Institut Universitaire de Technologie,
Aix-Marseille Université

RAPPORT DE STAGE de fin de deuxième année
Bachelor Universitaire de Technologie
Spécialité Réseaux et Télécommunications
parcours cybersécurité

Gestion des systèmes et des réseaux sur un serveur Windows

Clément Ismail

Hem France

Responsable entreprise : Yoni HADDAD

Responsable académique : Rabah IGUERNAISSI

2023

Table des matières

1 Introduction

Durant mon stage au sein du service informatique de l'entreprise Hem France, je me concentre sur un projet ambitieux : déployer un serveur Windows Server. Ce projet implique une série d'étapes cruciales telles que le choix du matériel approprié, l'installation et la configuration du serveur, la migration des données utilisateurs, et la création d'un VPN (Virtual Private Network) pour assurer un accès sécurisé aux ressources réseau

L'objectif principal de ce stage est de mettre en pratique mes compétences en administration système et en gestion de réseau, tout en contribuant à l'amélioration de l'infrastructure informatique de l'entreprise. Mes missions consisteront donc à sélectionner le matériel approprié, à installer et configurer le serveur Windows Server, à effectuer la migration des données des utilisateurs, à mettre en place un VPN sécurisé, et enfin, à réaliser un inventaire exhaustif du matériel réseau de l'entreprise, y compris la connexion d'un NAS (Network Attached Storage) au réseau.

Ce rapport sera structuré en quatre parties principales : tout d'abord, une présentation détaillée de l'entreprise Hem France et de ses besoins en matière d'infrastructure informatique ; ensuite, une analyse approfondie des différentes étapes impliquées dans le projet, de la planification à la mise en œuvre, en passant par les défis rencontrés et les solutions apportées ; suivie d'une section décrivant les résultats obtenus et les bénéfices pour l'entreprise ; enfin, une conclusion résumant les enseignements tirés de cette expérience et proposant des recommandations pour l'optimisation continue de l'infrastructure informatique de l'entreprise.

2 Présentation de l’entreprise

2.1 Qu'est-ce qu'est HEM France

HEM France est une entreprise spécialisée dans la distribution de produits de téléphonie, agissant principalement en tant que grossiste. Depuis sa fondation le 2 avril 2003, HEM France a su se faire une place importante dans le secteur, se distinguant par une expertise solide et une offre étendue.

HEM France, basée à Marseille au 27 Boulevard d'Arras, se concentre principalement sur la distribution de téléphones mobiles, d'accessoires pour smartphones, et d'autres équipements technologiques. En tant que grossiste, l'entreprise joue un rôle crucial en approvisionnant divers acteurs du marché, tels que les détaillants, les revendeurs, et d'autres professionnels de la téléphonie. La position de HEM France sur le marché est renforcée par ses partenariats avec de grandes marques et fabricants, lui permettant d'offrir une large gamme de produits à ses clients.

L'un des points forts de HEM France est la diversité de son catalogue. L'entreprise propose une vaste gamme de téléphones mobiles, incluant les dernières innovations technologiques, ainsi que des accessoires variés comme des coques, des chargeurs, des écouteurs, et bien d'autres. Cette variété permet à HEM France de répondre aux besoins spécifiques de ses clients, en offrant des solutions sur mesure en termes de prix, de fonctionnalité, et de disponibilité.

Outre la simple distribution de produits, HEM France se distingue également par les services annexes qu'elle propose. Cela inclut des services de logistique, assurant une livraison rapide et efficace à travers toute la France et potentiellement à l'international. L'entreprise offre aussi un support technique, essentiel pour ses clients qui peuvent avoir besoin d'assistance concernant les produits distribués. Cet engagement envers le service après-vente renforce la réputation de HEM France en tant que partenaire fiable.

HEM France ne se contente pas de distribuer des produits ; l'entreprise s'efforce également de rester à la pointe de l'innovation. Elle surveille de près les tendances du marché de la téléphonie pour s'assurer que ses clients ont accès aux dernières nouveautés. Cela inclut non seulement les nouveaux modèles de téléphones, mais aussi les avancées en matière d'accessoires et de technologies connectées.

En résumé, HEM France est un acteur clé dans le secteur de la téléphonie en France, se distinguant par sa capacité à offrir une large gamme de produits, des services de qualité, et une expertise solide. Son engagement envers l'innovation et la satisfaction client en fait un partenaire précieux pour de nombreux professionnels de la téléphonie, garantissant une distribution efficace et une adaptation constante aux besoins du marché.

2.2 Organigramme de l'entreprise

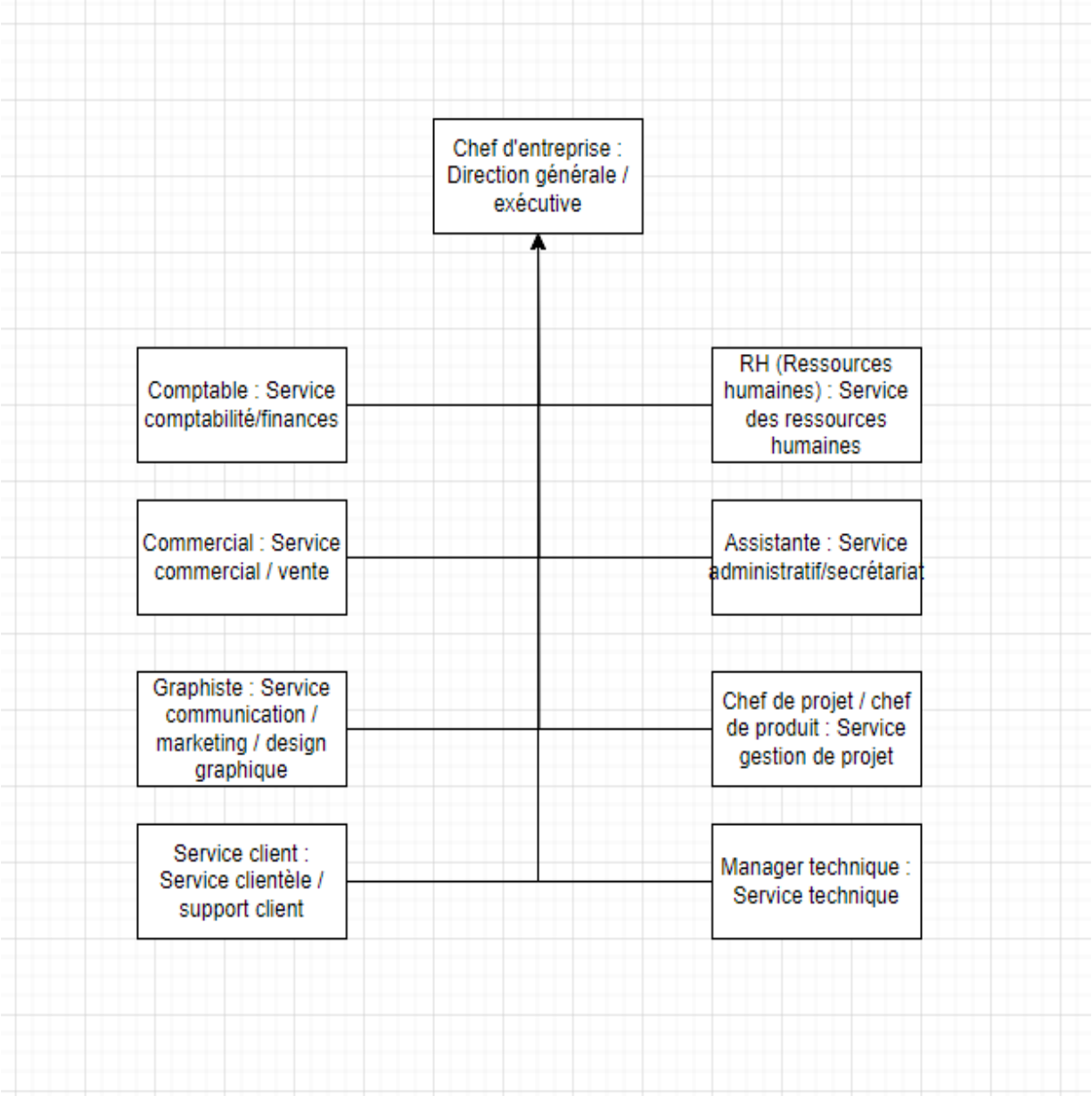

Figure 1 : Ceci est l'organigramme de Hem France

Le service comptabilité/finances est responsable de la gestion des finances de l'entreprise. Il s'occupe de suivre les dépenses et les recettes, de préparer les bilans comptables, d'analyser les finances pour soutenir les décisions stratégiques, et de gérer les relations avec les banques et les autorités fiscales.

Le service administratif/secrétariat assure le soutien administratif nécessaire au bon déroulement des opérations quotidiennes. Il gère l'accueil, le standard téléphonique, les courriers, organise les réunions, et soutient les autres départements en matière de gestion des plannings, de documents et de dossiers.

Le service gestion de projet/développement de produit se concentre sur la planification, l'exécution et la finalisation des projets, en respectant les délais, budgets et spécifications. Il coordonne les équipes et ressources, suit l'avancement des projets, et développe de nouveaux produits ou services jusqu'à leur lancement.

Le service clientèle/support client veille à la satisfaction des clients en répondant à leurs besoins, questions, et problèmes. Il gère les demandes, résout les réclamations, suit les commandes, et recueille les retours clients pour améliorer les produits ou services.

Le service des ressources humaines (RH) gère le capital humain de l'entreprise, y compris le recrutement, la formation, la gestion des performances, et les relations de travail. Il s'occupe également de la paie, des avantages sociaux, et de l'élaboration des politiques RH.

Le service commercial/vente est chargé de générer des revenus en vendant des produits ou services. Il prospecte de nouveaux clients, négocie des contrats, développe des stratégies de vente, et collabore avec le marketing pour promouvoir les offres de l'entreprise.

Le service communication/marketing/design graphique s'occupe de promouvoir l'image de marque et d'attirer des clients. Il développe des campagnes marketing, crée du contenu publicitaire, gère les réseaux sociaux, et conçoit les éléments graphiques qui renforcent l'identité visuelle de l'entreprise.

La direction générale/exécutive guide l'entreprise vers ses objectifs stratégiques. Elle prend les décisions clés, définit la vision globale, supervise les départements, et représente l'entreprise auprès des partenaires, actionnaires, et du public.

Le service technique/développement technologique/IT gère les infrastructures technologiques de l'entreprise et développe des solutions pour améliorer les opérations. Il assure la maintenance des systèmes informatiques, développe des logiciels, gère la sécurité des données, et soutient techniquement les utilisateurs internes et les clients.

2.3 Mon espace de travail

Figure 2 : Ceci est une représentation de mon espace de travail chez Hem France

Dans le cadre de mon stage, j'ai eu l'occasion de travailler dans un open-space un environnement qui favorisait la productivité et l'efficacité. Mon espace de travail était composé d'un bureau équipé de deux postes : un ordinateur fixe et un ordinateur portable. L’ordinateur me permettait de réaliser des tâches nécessitant une grande puissance de calcul.

3 Travail Réalisé

3.1 Découverte des appareils sur le réseau et inventaire du matériel

3.1.1 Utilisation d'outils de découverte réseau pour scanner

Les différents outils de scan

L'utilisation d'outils de scan de réseau tels qu'Advanced IP Scanner, Nmap, et Angry IP Scanner permet d'identifier et d'analyser les appareils connectés à un réseau. Voici une explication détaillée de l'utilisation de chacun de ces outils

Choix de l'outil de découverte réseau

Les outils de découverte réseau varient en termes de fonctionnalités et de complexité. Voici quelques exemples courants :

Nmap, ou Network Mapper, est un outil incontournable dans le domaine de la sécurité informatique et de la gestion des réseaux. Il est surtout connu pour sa capacité à explorer les réseaux et à fournir des informations détaillées sur les dispositifs connectés. En utilisant Nmap, les professionnels peuvent scanner les ports ouverts sur des hôtes cibles, identifier les services qui y sont associés et même déterminer les systèmes d'exploitation en cours d'exécution. Ce niveau de détail est possible grâce à des techniques sophistiquées telles que le fingerprinting des systèmes d'exploitation et le scan des services, qui permettent non seulement de détecter les vulnérabilités potentielles mais aussi de comprendre la configuration et la topologie du réseau. De plus, Nmap offre une extensibilité via son moteur de script (NSE), permettant aux utilisateurs de personnaliser leurs scans pour des tâches spécifiques comme la détection de vulnérabilités.

Advanced IP Scanner se distingue par sa simplicité et son efficacité pour les utilisateurs de Windows. Conçu pour des scans rapides et intuitifs des réseaux locaux, cet outil est idéal pour une analyse instantanée des adresses IP et des dispositifs connectés. Il permet de détecter facilement les équipements tels que les imprimantes et les routeurs, et fournit des informations sur les partages réseau disponibles. L'une de ses fonctionnalités notables est la possibilité d'administrer des machines à distance, telles que les redémarrer ou les éteindre, ce qui en fait un outil pratique pour les administrateurs réseau cherchant une solution rapide pour gérer leur infrastructure sans entrer dans les détails complexes de la configuration réseau.

Angry IP Scanner est un autre outil léger mais puissant qui s'adresse à ceux qui ont besoin d'une vue rapide et efficace des adresses IP en usage sur un réseau. Avec une interface utilisateur simple, Angry IP Scanner permet de scanner des plages d'adresses IP et de récupérer des informations sur les hôtes actifs, y compris les adresses MAC et les noms d'hôte. Sa légèreté et sa facilité d'utilisation en font un choix populaire pour des tâches rapides de gestion de réseau et de dépannage, sans les fonctionnalités avancées que l'on trouve dans des outils plus complexes.

SolarWinds Network Performance Monitor (NPM) est une solution hautement avancée, conçue principalement pour les grandes entreprises avec des réseaux complexes. Il excelle dans la découverte automatisée des dispositifs réseau et offre une surveillance continue et en temps réel des performances du réseau. SolarWinds NPM fournit des analyses détaillées et des rapports sur l'état du réseau, facilitant la détection précoce des problèmes de performance et leur résolution. Sa capacité à gérer les configurations des dispositifs et à générer des rapports détaillés en fait un outil essentiel pour les équipes informatiques qui ont besoin de maintenir la stabilité et l'efficacité de leurs infrastructures réseau à grande échelle.

Chacun de ces outils a ses propres avantages et est adapté à différents niveaux de complexité et de besoin en matière de gestion et de surveillance des réseaux.

Procédure de Scan

Installation et configuration : Téléchargez et installez l'outil de découverte réseau de votre choix. Configurez-le pour cibler le sous-réseau ou la plage d'adresses IP que vous souhaitez scanner. Par exemple, pour scanner un réseau local, vous pourriez spécifier une plage comme 192.168.1.0/24.

Lancement du scan : Exécutez le scan pour détecter les équipements. L'outil va interroger chaque adresse IP dans la plage spécifiée, en envoyant des requêtes pour identifier les équipements actifs, les ports ouverts, les services, et parfois même les systèmes d'exploitation utilisés.

Analyse des résultats : Une fois le scan terminé, examinez les résultats. Vous obtiendrez une liste des adresses IP, des noms d'hôtes (si disponibles), des adresses MAC, des types d'équipements, et des ports/services ouverts. Par exemple, Nmap peut fournir des détails très spécifiques sur les services actifs sur chaque port, comme HTTP, FTP, ou SSH.

3.1.2 Identification de tous les équipements et cartographie du réseau

Pour identifier tous les équipements et cartographier un réseau, commencez par collecter toutes les informations disponibles sur les appareils connectés, tels que les routeurs, switches, serveurs, et autres dispositifs. Pour cela, un scan du réseau est essentiel. Des outils comme Nmap ou Advanced IP Scanner permettent de détecter les équipements, leurs adresse IP (Internet Protocol), MAC (Media Access Control), et parfois des détails sur les systèmes d'exploitation et les services actifs.

Après avoir recueilli ces données, il est important de créer un inventaire complet. Cela inclut le modèle des équipements, leurs adresses réseau, et leur position dans l'infrastructure. Cette base de données doit être précise et régulièrement mise à jour pour refléter l'état actuel du réseau.

Une fois l'inventaire terminé, vous pouvez passer à la cartographie du réseau. En utilisant des logiciels spécialisés comme Microsoft Visio ou Lucidchart, vous créez une représentation visuelle de la topologie du réseau. Cette carte doit illustrer les connexions entre les équipements, les segments de réseau (comme les VLANs (Virtual Local Area Network)), et toute autre information pertinente pour la compréhension du réseau.

Après avoir créé cette carte, il est essentiel de la vérifier pour s'assurer qu'elle reflète fidèlement la réalité. Elle doit être mise à jour régulièrement pour inclure les nouvelles installations ou les changements dans la configuration du réseau. Documenter ces informations est crucial pour une gestion efficace du réseau, permettant une maintenance plus facile, une résolution rapide des problèmes, et une meilleure sécurité.

Cartographie du réseau

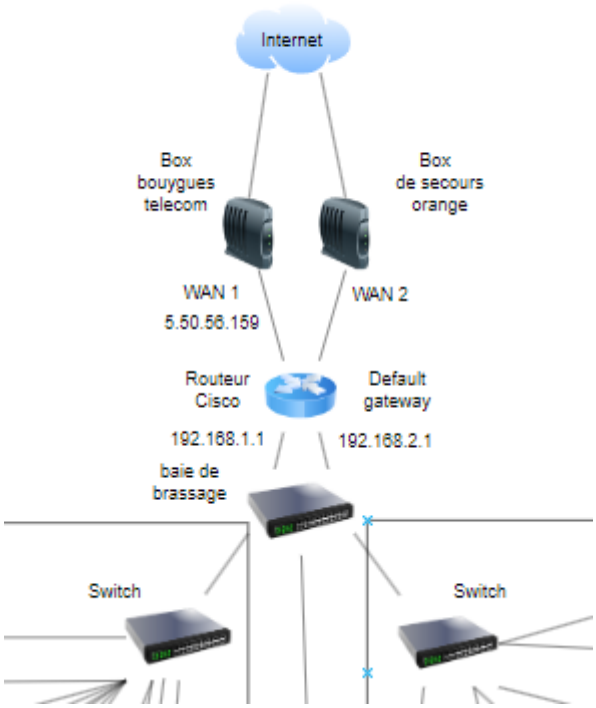

Figure 3 : Ceci est une partie du plan du réseau

Le réseau est structuré autour de deux connexions Internet distinctes, chacune fournie par une box avec sa propre adresse IP publique. Ces deux box sont connectées à un routeur central, un modèle Cisco R345P, qui assure la gestion du trafic réseau entre les différentes parties du réseau local et les connexions Internet.

Le routeur Cisco est relié à une baie de brassage, un équipement centralisé permettant de regrouper et d'organiser les connexions réseau. Depuis la baie de brassage, les connexions sont distribuées vers un switch de couche 2. Ce type de switch, opère au niveau de la couche de liaison de données du modèle OSI, gère la commutation de trames en fonction des adresses MAC et permet de segmenter le réseau en VLAN (Virtual Local Area Networks).

Le réseau comporte deux VLANs distincts : le premier utilise la plage d'adresses 192.168.1.0/24, destiné à un groupe spécifique d'utilisateurs ou d'équipements, tandis que le second, en 192.168.2.0/24, est réservé à un autre groupe, comme un réseau invité ou des dispositifs particuliers. Cette segmentation améliore la sécurité et l'efficacité du réseau en isolant les différents flux de trafic.

3.1.3 Les bénéfices des outils de découverte réseau

L'utilisation d'outils de découverte réseau pour scanner et cartographier l'infrastructure existante offre une multitude d'avantages et de bénéfices pour les organisations. En conclusion, voici quelques points clés à retenir :

Visibilité accrue de l'infrastructure : Les outils de découverte réseau permettent de visualiser l'ensemble de l'infrastructure, y compris les dispositifs connectés et les relations entre eux. Cela offre une compréhension approfondie de l'environnement informatique.
Détection des vulnérabilités : En identifiant tous les appareils connectés au réseau, ces outils aident à repérer les failles potentielles de sécurité. Cela permet aux équipes de sécurité informatique de prendre des mesures préventives pour renforcer la sécurité du réseau.
Gestion des actifs : En maintenant une liste précise des appareils réseau, les organisations peuvent mieux gérer leurs actifs informatiques. Cela facilite la planification des mises à jour, la maintenance préventive et la gestion des licences logicielles.
Optimisation des performances : La cartographie de l'infrastructure permet d'identifier les goulots d'étranglement et les inefficacités dans le réseau. En optimisant la configuration et en répartissant correctement la charge, les performances du réseau peuvent être améliorées.
Conformité réglementaire : Certains secteurs sont soumis à des réglementations strictes en matière de sécurité et de protection des données. En utilisant des outils de découverte réseau, les organisations peuvent mieux répondre aux exigences de conformité en identifiant et en sécurisant tous les dispositifs connectés.

En somme, l'utilisation d'outils de découverte réseau est essentielle pour maintenir un réseau informatique sécurisé, performant et conforme. En investissant dans ces outils et en les intégrant dans les pratiques de gestion des TI, les organisations peuvent renforcer leur posture de sécurité et optimiser leurs opérations informatiques.

3.2 Mise en place du serveur Windows Server et des profils locaux

3.2.1 Choix du bon matériel pour le Windows server

Lorsque je me lance dans la sélection du bon Windows Server, il y a plusieurs aspects à considérer pour m’assurer de faire le bon choix. Tout d’abord, je dois réfléchir à la taille et au type de mon organisation. Pour une petite entreprise avec moins de 50 utilisateurs, je pourrais envisager Windows Server Essentials. C'est une option simple et économique qui répondra à mes besoins de base. En revanche, si mon entreprise est de taille moyenne, avec entre 50 et 500 utilisateurs, ou si elle prévoit une croissance significative, je devrai probablement me tourner vers les éditions Standard ou Datacenter.

Je dois également prendre en compte les besoins spécifiques en ressources. Si je gère beaucoup de données ou si mes opérations nécessitent des performances élevées, il est essentiel que je choisisse une édition capable de gérer cette charge. Par exemple, si je prévois d'utiliser des machines virtuelles, l'édition Datacenter pourrait être plus appropriée, car elle offre des licences illimitées pour la virtualisation.

En termes de services et d'applications, je dois réfléchir à ce que j'utilise actuellement et à ce que je prévois d'utiliser. Si j'héberge des applications web ou si j'utilise des services spécifiques, je devrai choisir une version qui supporte ces besoins. La version la plus récente, Windows Server 2022, offre de nombreuses améliorations en termes de sécurité et de gestion, et elle est bien intégrée avec les solutions cloud, ce qui pourrait être un atout si je cherche à évoluer vers une infrastructure hybride.

Je ne dois pas oublier le budget. Il est crucial de choisir une édition qui correspond non seulement à mes besoins techniques, mais aussi à mes capacités financières. Les éditions Essentials sont plus abordables et adaptées pour des besoins limités, tandis que les éditions Standard et Datacenter offrent des fonctionnalités plus avancées, mais à un coût plus élevé.

Enfin, en réfléchissant à ces différents aspects, je pourrai choisir la version de Windows Server qui répondra le mieux à mes exigences actuelles et futures. Pour une intégration fluide avec le cloud et une gestion centralisée, je pourrais envisager Windows Server 2022 avec Azure Arc, surtout si mon organisation adopte une stratégie cloud hybride.

En résumé, je dois évaluer soigneusement les besoins de mon organisation, la taille et le type de mon infrastructure, ainsi que mon budget pour faire un choix éclairé. Je consulterai également la documentation officielle de Microsoft et, si nécessaire, je contacterai un conseiller pour obtenir des conseils personnalisés.

J'ai finalement choisi d'opter pour la licence Windows Server Standard avec un serveur PowerEdge R350. Cette combinaison me semble être le meilleur choix pour répondre aux besoins actuels de mon entreprise tout en restant dans mon budget.

L'édition Standard de Windows Server complémente bien cette configuration en offrant une solution efficace pour les environnements physiques et peu virtualisés, tout en permettant une gestion simplifiée et une sécurité renforcée.

3.2.2 Installation et configuration du serveur

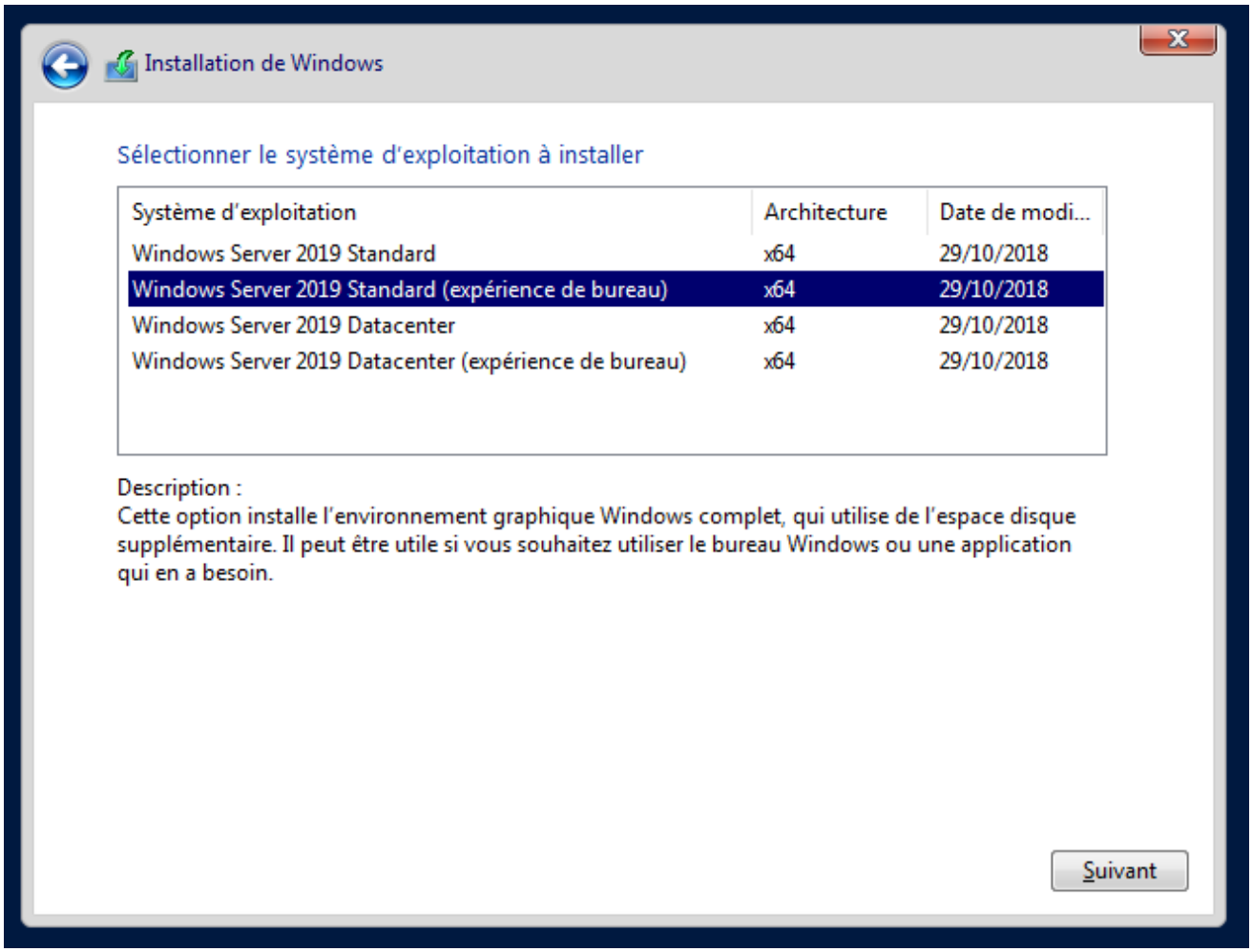

Figure 4 : Ceci est fenêtre d'installation de Windows Server

Pour installer et configurer Windows Server, commencez par préparer votre matériel en vérifiant qu'il répond aux exigences nécessaires pour faire fonctionner le serveur. Téléchargez l'image ISO de Windows Server depuis le site de Microsoft ou un autre canal officiel, puis créez un support d'installation, comme une clé USB bootable ou un DVD.

Démarrez le serveur à partir de ce support d'installation en accédant au BIOS pour modifier l'ordre de démarrage. Configurez les options de langue et de clavier, puis lancez l'installation. Choisissez l'édition de Windows Server que vous souhaitez installer, acceptez les termes de la licence, et sélectionnez le disque sur lequel vous voulez installer le système. Laissez l'installation se dérouler, puis définissez un mot de passe pour le compte administrateur une fois le processus terminé.

Après l'installation, configurez les paramètres réseau en attribuant une adresse IP statique, définissez la passerelle par défaut et configurez les serveurs DNS. Renommez le serveur pour qu'il reflète son rôle ou sa fonction dans votre réseau, puis activez Windows Server avec la clé de produit fournie.

Pour personnaliser le serveur selon vos besoins, utilisez le Gestionnaire de serveur pour ajouter et configurer les rôles et fonctionnalités nécessaires, comme Active Directory, DNS ou DHCP. Chaque rôle peut nécessiter une configuration spécifique ; par exemple, pour Active Directory, vous devrez promouvoir le serveur en tant que contrôleur de domaine.

Assurez-vous que le serveur est à jour en installant les dernières mises à jour disponibles, et configurez la sécurité en ajustant les paramètres du pare-feu, en installant un logiciel antivirus, et en mettant en place des politiques de sécurité appropriées. Gérez les utilisateurs et les permissions pour contrôler l'accès aux ressources du serveur.

Pour protéger vos données, configurez des sauvegardes régulières à l'aide de Windows Server Backup ou d'un autre logiciel de sauvegarde. Surveillez les performances du serveur avec des outils de gestion pour anticiper et résoudre les problèmes potentiels.

Enfin, activez l'accès à distance via le Bureau à distance (RDP) pour faciliter la gestion du serveur depuis d'autres emplacements, et configurez un VPN si nécessaire pour établir des connexions sécurisées à distance. En suivant ces étapes, vous établirez un environnement serveur stable et sécurisé.

3.2.3 Migration des Données des Utilisateurs entre Deux Profils Locaux

La migration des données des utilisateurs entre deux profils locaux est une opération courante lorsqu'un utilisateur change de poste de travail ou de périphérique. Cette migration implique le transfert sécurisé et efficace des fichiers, des paramètres et des préférences utilisateur d'un profil local vers un autre, tout en préservant l'intégrité et la disponibilité des données.

Identification et Sélection des Données à Migrer

La première étape de la migration consiste à identifier et sélectionner les données à migrer. Cela peut inclure les fichiers personnels, les documents de travail, les paramètres de l'application, les favoris de navigateur, les profils utilisateur et d'autres informations pertinentes pour l'utilisateur. Il est important de consulter l'utilisateur pour comprendre ses besoins et ses préférences afin de garantir une migration complète et précise.

Préparation des Données

Avant de commencer la migration, il est essentiel de préparer les données pour garantir un transfert efficace et sans erreur. Cela peut inclure la sauvegarde des données existantes pour éviter toute perte accidentelle, la suppression des fichiers inutiles ou obsolètes pour réduire le volume de données à migrer, et la consolidation des paramètres et des préférences utilisateur pour simplifier le processus de migration.

Transfert des Données

Une fois les données préparées, le transfert des données peut commencer. Cela peut être réalisé en utilisant des outils de migration intégrés, tels que l'Assistant de Transfert de Fichiers et de Paramètres de Windows, des solutions tierces ou des méthodes manuelles. Il est important de choisir une méthode de transfert sécurisée et fiable pour garantir que les données sont transférées sans altération et protégées contre tout accès non autorisé.

Validation et Vérification

Après le transfert des données, il est crucial de procéder à une validation et une vérification rigoureuse pour s'assurer que toutes les données ont été migrées correctement. Cela peut inclure la comparaison des données source et cible pour détecter les écarts ou les erreurs, la vérification des autorisations d'accès pour garantir que l'utilisateur a toujours accès aux fichiers appropriés, et la réalisation de tests de fonctionnalité pour confirmer que les applications et les services fonctionnent comme prévu dans le nouveau profil.

Assistance Utilisateur et Suivi

Une fois la migration terminée, il est important de fournir une assistance et un suivi continus à l'utilisateur pour résoudre les éventuels problèmes et répondre à ses questions. Cela peut inclure des sessions de formation supplémentaires, la création de guides utilisateur et la mise en place d'un système de support technique pour assurer une transition en douceur vers le nouveau profil.

En suivant ces étapes, la migration des données des utilisateurs entre deux profils locaux peut être réalisée de manière efficace et transparente, garantissant ainsi une expérience utilisateur cohérente et sans interruption lors du changement de poste de travail ou de périphérique.

3.2.4 Utilisation de User Profile Wizard

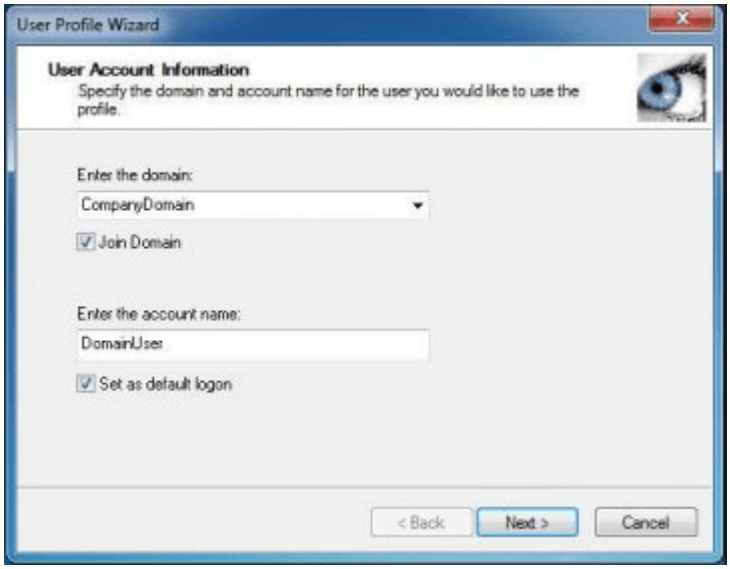

Figure 5 : Ceci est fenêtre du logiciel User Wizard profil

Le User Profile Wizard est un outil utilisé pour migrer des profils d'utilisateurs entre différents comptes sur un même ordinateur ou entre différentes machines. Voici une explication détaillée de son utilisation pour migrer des profils d'utilisateurs entre deux utilisateurs

Pour utiliser User Profile Wizard afin de migrer un profil utilisateur d'un ancien compte vers un nouveau, commencez par télécharger le logiciel depuis le site officiel de ForensIT. Une fois le téléchargement terminé, lancez le fichier d'installation et suivez les instructions habituelles pour installer le logiciel sur votre ordinateur.

Avant de commencer la migration, assurez-vous que les deux comptes utilisateurs, l'ancien et le nouveau, sont déjà créés. Cela peut se faire soit sur l'ordinateur local, soit sur le domaine,

selon votre configuration. Connectez-vous ensuite à l'ordinateur avec un compte disposant des droits d'administrateur, car la migration des profils nécessite des privilèges élevés.

Lancez User Profile Wizard. À l'ouverture de l'application, vous verrez l'écran d'accueil vous invitant à commencer le processus de migration. Vous devrez alors sélectionner le profil utilisateur que vous souhaitez transférer. Ce profil est celui qui contient toutes les configurations, fichiers et paramètres que vous souhaitez migrer vers un nouveau compte.

Après avoir sélectionné l'ancien profil, choisissez le nouveau compte utilisateur vers lequel vous souhaitez transférer les données. Vous devrez indiquer le nom d'utilisateur du nouveau compte, ainsi que le domaine ou l'ordinateur local si le compte est local.

Une fois que vous avez configuré ces options, lancez le processus de migration. User Profile Wizard commencera à transférer toutes les informations de l'ancien profil vers le nouveau compte. Il est important de surveiller la progression de la migration pour vous assurer qu'aucun problème ne survient.

Après la fin du processus, vérifiez que le nouveau compte utilisateur fonctionne correctement. Connectez-vous avec ce compte pour vous assurer que tous les fichiers, paramètres et configurations ont été correctement transférés. Si tout semble en ordre, vous pouvez choisir de supprimer l'ancien profil pour libérer de l'espace, bien que cela ne soit pas obligatoire.

En suivant ces étapes, vous devriez pouvoir migrer efficacement les profils utilisateurs à l'aide de User Profile Wizard. Assurez-vous de bien vérifier chaque étape pour garantir une transition fluide et sans problème.

Attention au risque :

Utiliser User Profile Wizard pour migrer des profils d’utilisateurs peut grandement simplifier le transfert de données et de configurations d’un compte à un autre, mais cela comporte certains risques qui méritent une attention particulière.

L'un des principaux risques est la **perte de données**. Malgré le fait que User Profile Wizard soit conçu pour transférer les paramètres et les fichiers d’un profil à un autre, il peut arriver que des erreurs se produisent pendant le processus de migration. Cela peut entraîner la perte de données importantes. Pour éviter cela, il est crucial de faire une sauvegarde complète de toutes les données avant de commencer la migration.

Un autre problème potentiel est lié à la **compatibilité**. Les profils utilisateur peuvent contenir des paramètres ou des configurations spécifiques qui ne sont pas toujours parfaitement compatibles avec le nouveau compte ou le nouvel environnement. Par exemple, certaines applications ou paramètres peuvent ne pas fonctionner comme prévu après la migration. Pour réduire ce risque, il est utile de vérifier les configurations et de s'assurer que le nouvel environnement est bien adapté aux besoins de l’ancien profil.

Les **permissions et l'accès** représentent également une préoccupation. Les paramètres de sécurité et les droits d’accès peuvent ne pas être transférés correctement, ce qui peut entraîner des problèmes pour accéder à des fichiers ou utiliser des ressources. Il est important de vérifier que le nouveau compte utilisateur dispose des permissions nécessaires après la migration.

De plus, certaines **configurations du profil** peuvent ne pas se transférer intégralement. Les paramètres spécifiques des applications ou les préférences de l'utilisateur peuvent nécessiter des ajustements manuels après la migration pour garantir que tout fonctionne correctement.

Il peut aussi y avoir des **conflits avec les comptes existants**. Si le nouveau compte a déjà des données ou des configurations, la migration peut écraser ces informations, ce qui pourrait causer des problèmes. Il est donc conseillé de bien comprendre l'état du nouveau compte avant de commencer le transfert.

Les **problèmes de performance** peuvent aussi se manifester, surtout si vous migrez des profils volumineux ou complexes. Cela peut ralentir le système pendant et après la migration. Pour minimiser cet impact, il est recommandé de planifier la migration à un moment où le système n'est pas trop sollicité.

Enfin, **l'environnement dans lequel vous travaillez** peut également affecter le succès de la migration. Dans des environnements complexes, comme ceux avec des configurations de domaine multiples ou des politiques de sécurité strictes, des problèmes inattendus peuvent survenir. Tester la migration dans un environnement contrôlé ou de test peut aider à anticiper et résoudre ces problèmes.

En prenant ces risques en compte et en appliquant des pratiques de sauvegarde et de vérification rigoureuses, vous pouvez réduire les chances de rencontrer des problèmes lors de l'utilisation de User Profile Wizard pour migrer des profils utilisateurs.

3.3 Installation et configuration d'un Serveur VPN

3.3.1 C'est quoi un serveur VPN ?

Un serveur VPN (Virtual Private Network) pour une entreprise est un dispositif ou un service qui permet de sécuriser et de protéger les communications entre les employés et les ressources de l'entreprise sur Internet. Voici quelques points clés pour comprendre son rôle :

Sécurité des Données : Le serveur VPN chiffre les données transmises entre les ordinateurs des employés et les serveurs de l'entreprise. Cela rend les informations illisibles pour quiconque pourrait intercepter les communications, comme des cybercriminels ou des hackers.

Accès à Distance : Avec un VPN, les employés peuvent accéder aux ressources internes de l'entreprise (comme les fichiers, les applications, les systèmes de gestion, etc.) de manière sécurisée, même lorsqu'ils sont en déplacement ou travaillent à distance. Cela est particulièrement utile pour les entreprises avec des équipes distribuées ou des travailleurs à domicile.

Confidentialité : Le serveur VPN masque l'adresse IP des utilisateurs, offrant un anonymat supplémentaire en ligne et aidant à protéger la vie privée des employés lorsqu'ils accèdent à Internet à travers le réseau de l'entreprise.

Contrôle d'Accès : Les entreprises peuvent configurer des règles spécifiques pour gérer qui peut accéder à quoi au sein du réseau. Cela permet de s'assurer que seules les personnes autorisées ont accès aux informations sensibles ou aux systèmes critiques.

En résumé, un serveur VPN pour une entreprise est un outil essentiel pour assurer la sécurité, la confidentialité, et l'efficacité des opérations en ligne. Il permet de créer un réseau sécurisé pour que les employés puissent travailler de manière sûre et efficace, même en dehors des locaux de l'entreprise.

3.3.2 Choix du protocole VPN adapté aux besoins de l'entreprise

Lorsqu'il s'agit de choisir un protocole VPN adapté aux besoins d'une entreprise, plusieurs facteurs doivent être pris en compte. Chaque protocole VPN a ses propres avantages et inconvénients, et le choix doit être basé sur les besoins spécifiques de l'entreprise en termes de sécurité, de performance, de compatibilité et de facilité de déploiement.

PPTP (Point-to-Point Tunneling Protocol)

Le PPTP est un protocole de tunneling qui se distingue par sa simplicité d'utilisation et sa configuration facile. Il est compatible avec une vaste gamme de systèmes d'exploitation et d'appareils, ce qui en fait un choix pratique pour de nombreux utilisateurs. Cependant, malgré ces avantages, le PPTP est souvent critiqué pour ses vulnérabilités de sécurité. Les failles connues dans ce protocole peuvent exposer les données des utilisateurs à des risques importants, ce qui le rend peu fiable pour les environnements où la sécurité est une priorité. Son utilisation est généralement déconseillée dans des contextes nécessitant une protection renforcée des données.

L2TP/IPsec (Layer 2 Tunneling Protocol avec IPsec)

Le L2TP/IPsec combine le Layer 2 Tunneling Protocol (L2TP) avec IPsec pour offrir une solution plus sécurisée que le PPTP. L2TP, en lui-même, ne fournit pas de chiffrement des données, mais lorsqu'il est associé à IPsec, il offre une protection significative en chiffrant les données échangées. Cette combinaison améliore considérablement la sécurité, mais elle peut entraîner une certaine dégradation des performances en raison du double processus d'encapsulation : d'abord par L2TP, puis par IPsec. De plus, la configuration du L2TP/IPsec est plus complexe comparée à celle du PPTP, ce qui peut poser des défis supplémentaires pour les administrateurs et les utilisateurs. Néanmoins, il reste une option populaire pour ceux qui recherchent un compromis entre sécurité et compatibilité.

OpenVPN

OpenVPN est reconnu pour son niveau élevé de sécurité et sa flexibilité. Utilisant le protocole SSL/TLS pour le chiffrement des données, il offre une protection robuste contre les interceptions et les attaques. Ce protocole est extrêmement versatile et peut être configuré pour répondre à des besoins spécifiques grâce à ses nombreuses options de personnalisation. Cependant, cette flexibilité et ce niveau de sécurité élevé viennent avec un coût en termes de complexité de configuration. OpenVPN nécessite l'installation de logiciels clients supplémentaires, ce qui peut compliquer son déploiement, surtout dans des environnements où les utilisateurs ne sont pas techniquement expérimentés. Malgré ces défis, il reste un choix privilégié dans des contextes où la sécurité des données est cruciale.

IKEv2/IPsec (Internet Key Exchange version 2 avec IPsec)

IKEv2/IPsec est souvent apprécié pour sa rapidité et sa robustesse. Il est particulièrement efficace dans les environnements mobiles grâce à sa capacité à maintenir une connexion stable même lors de changements de réseau, comme lorsqu'un appareil passe de données cellulaires à un réseau Wi-Fi. Cette caractéristique le rend particulièrement adapté aux situations où la continuité de la connexion est essentielle. Cependant, bien que bien supporté par les systèmes d'exploitation modernes, son support peut être limité sur des systèmes plus anciens. De plus, la configuration initiale d'IKEv2/IPsec peut être complexe, nécessitant une compréhension approfondie des paramètres de sécurité et des options de connexion.

WireGuard

WireGuard est un protocole relativement récent qui se distingue par ses performances exceptionnelles et sa conception simplifiée. Avec un code source beaucoup plus réduit que les autres protocoles VPN, WireGuard offre une solution efficace et rapide pour le chiffrement des données. Sa conception épurée se traduit par une implémentation plus rapide et une gestion des clés plus efficace. En tant que protocole open source, WireGuard est accessible et transparent, ce qui contribue à sa popularité croissante. Cependant, malgré ses nombreux avantages, WireGuard est encore relativement nouveau et peut ne pas être aussi largement supporté que les protocoles plus anciens comme OpenVPN. Il peut également manquer de certaines fonctionnalités avancées présentes dans des solutions plus matures, ce qui pourrait limiter son utilisation dans certains contextes.

Facteurs à considérer pour le choix du protocole VPN :

Niveau de sécurité requis : Pour des informations hautement sensibles, les protocoles comme OpenVPN, IKEv2/IPsec, ou WireGuard sont recommandés.
Performance et vitesse : Pour des besoins de performance élevée, WireGuard et IKEv2/IPsec sont préférables.
Compatibilité des appareils : Si une large gamme d'appareils doit être supportée, L2TP/IPsec et OpenVPN offrent une meilleure compatibilité.
Facilité de configuration : Pour des déploiements rapides avec peu de ressources techniques, PPTP (bien que peu sécurisé) ou L2TP/IPsec peuvent être envisagés.
Support et maintenance : OpenVPN, étant open source avec une large communauté, offre de nombreux ressources et support communautaire.

3.3.3 Configuration des paramètres de sécurité (certificats, authentification)

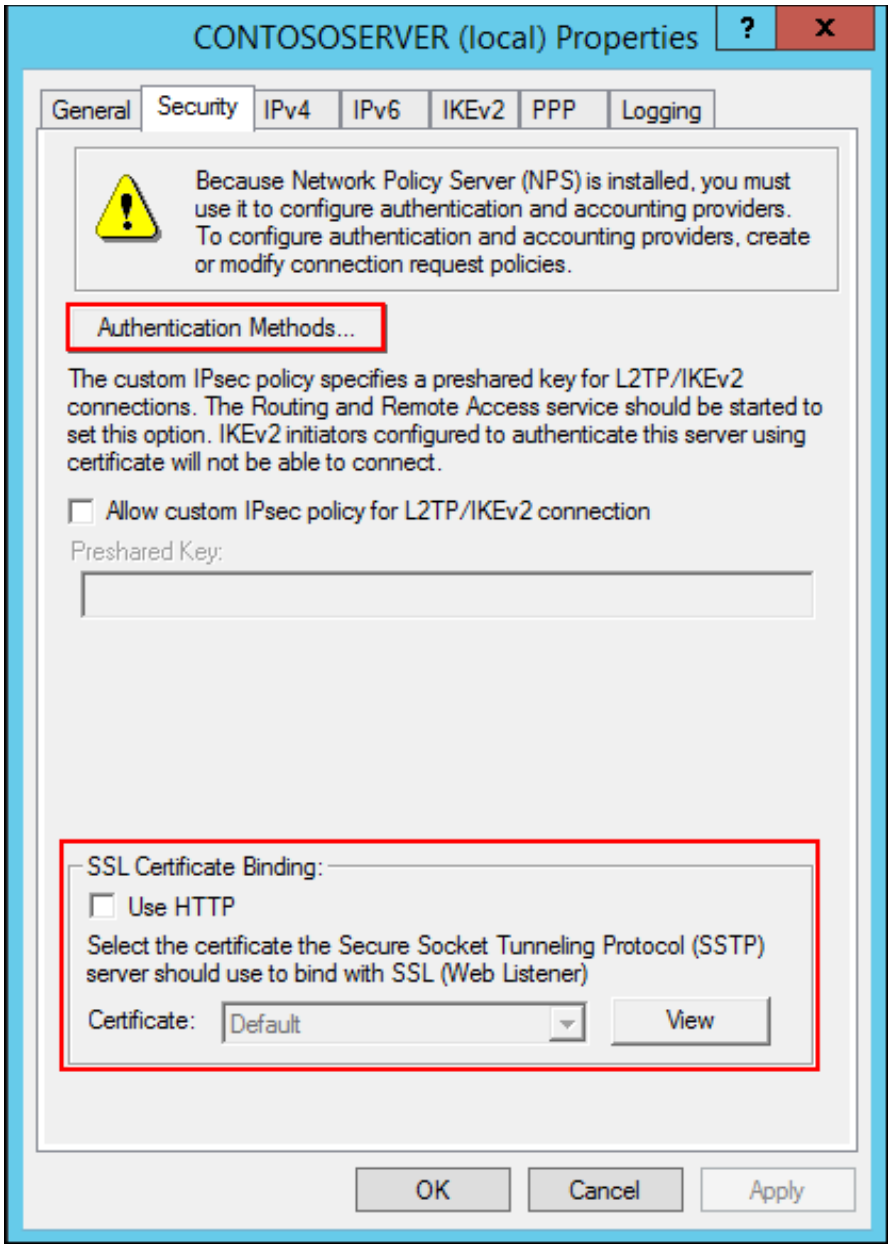

Figure 6 : Ceci est fenêtre de configuration de VPN sur Windows Server

La configuration des paramètres de sécurité, en particulier l'authentification, pour un serveur VPN L2TP/IPsec avec PSK sur Windows, est une étape essentielle pour garantir une connexion sécurisée et fiable. Voici une approche détaillée pour cette configuration :

Préparation de l'infrastructure VPN :

Serveur Windows : Assurez-vous d'avoir un serveur Windows correctement configuré pour héberger le service VPN. Cela peut être un serveur dédié ou une machine Windows disposant des fonctionnalités de serveur VPN activées.

Adresse IP statique : Le serveur Windows doit disposer d'une adresse IP statique pour garantir une connectivité constante et prévisible

Configuration du service VPN sur Windows Server :

Installation du service VPN : Installez le service VPN sur le serveur Windows en utilisant les fonctionnalités de gestion des rôles et fonctionnalités de Windows Server. Activez le support pour le protocole L2TP/IPsec.

Configuration des paramètres VPN : Une fois le service VPN installé, configurez les paramètres VPN pour utiliser le protocole L2TP/IPsec avec PSK comme méthode d'authentification.

Génération de la Pre-Shared Key (PSK) :

Création d'une PSK : Générez une PSK robuste et complexe à utiliser pour l'authentification entre le serveur VPN et les clients. Cette clé partagée doit être protégée et connue uniquement des administrateurs autorisés.

Configuration des paramètres de sécurité sur le serveur Windows :

Authentification : Configurez le serveur VPN pour utiliser la PSK comme méthode d'authentification. Cette étape garantit que seuls les clients disposant de la PSK correcte peuvent établir une connexion VPN.

Cryptage : Choisissez les algorithmes de cryptage appropriés, tels que AES, pour sécuriser les données transitant à travers le tunnel VPN. Assurez-vous que le niveau de cryptage est conforme aux normes de sécurité de votre entreprise.

Intégrité des données : Activez la vérification de l'intégrité des données pour détecter toute altération non autorisée des paquets VPN en transit.

Configuration avancée : Explorez les options de configuration avancée disponibles sur Windows Server pour renforcer la sécurité du VPN. Cela peut inclure la configuration de listes de contrôle d'accès (ACL) pour contrôler le trafic entrant et sortant, ainsi que l'activation de fonctionnalités telles que Perfect Forward Secrecy (PFS) pour améliorer la sécurité.

En suivant ces étapes de configuration et de validation, vous pouvez mettre en place un serveur VPN L2TP/IPsec avec PSK sécurisé sur Windows, adapté aux besoins de sécurité de votre entreprise. Il ne faut pas oubliez de surveiller régulièrement le système et de mettre à jour les paramètres de sécurité en fonction des exigences et des évolutions de votre entreprise.

3.4 Les Apports du stage

Le stage réalisé chez HEM France a constitué une étape fondamentale dans mon parcours professionnel, offrant une multitude d'apprentissages significatifs. Tout d'abord, il a permis une application concrète des connaissances théoriques acquises au cours de ma formation académique. En travaillant directement sur des projets tels que la configuration de serveurs et la gestion des réseaux, j'ai pu associer la théorie à des situations réelles, ce qui a grandement enrichi ma compréhension des outils et technologies.

En outre, cette expérience m'a permis de développer des compétences techniques spécifiques, comme la configuration de serveurs Windows et la mise en place de réseaux VPN. Ces compétences pratiques sont directement applicables dans le monde professionnel et m'ont donné une maîtrise approfondie de technologies courantes. Parallèlement, le stage a favorisé le développement de compétences professionnelles essentielles, telles que la gestion du temps, la résolution de problèmes complexes, et le travail sous pression, compétences cruciales pour toute carrière dans le secteur.

L'immersion dans la culture et les dynamiques de l'entreprise a également été un aspect important du stage. En observant le fonctionnement interne de l'entreprise et en participant à diverses activités, j'ai pu comprendre les processus décisionnels et les interactions entre les différents départements. Cette compréhension m'a aidé à apprécier l'importance de la collaboration interfonctionnelle et de l'alignement avec les objectifs et les valeurs de l'entreprise.

De plus, le stage a renforcé mon réseau professionnel. Travailler aux côtés de professionnels expérimentés m'a permis de créer des relations précieuses, de bénéficier de conseils avisés, et d'obtenir des retours constructifs. Ce réseau constitue une ressource importante pour l'avenir et ouvre des perspectives intéressantes pour ma carrière.

L'expérience m'a également offert une vision réaliste du métier, clarifiant mes objectifs de carrière et identifiant les domaines dans lesquels je dois m'améliorer. En me confrontant à des situations variées, le stage a renforcé ma confiance en moi et mes compétences interpersonnelles, tout en m'encourageant à adopter une attitude proactive face aux défis.

En somme, le stage chez HEM France a été une expérience extrêmement formatrice. Il a permis de combiner efficacement théorie et pratique, de développer des compétences techniques et professionnelles, et d'acquérir une compréhension approfondie du fonctionnement d'une entreprise. Ces apprentissages sont précieux pour mon développement professionnel et personnel et me préparent de manière solide pour mon avenir dans le secteur.

4 Conclusion

Ce rapport a permis de mettre en lumière les diverses tâches effectuées au sein de l'entreprise HEM France, ainsi que les compétences acquises au cours de cette expérience professionnelle.

La découverte des appareils sur le réseau et l'inventaire du matériel ont été essentiels pour obtenir une vue d'ensemble claire de l'infrastructure informatique existante. L'utilisation d'outils de découverte réseau s'est avérée cruciale, facilitant ainsi l'identification des équipements et la cartographie du réseau, tout en soulignant les nombreux avantages offerts par ces outils en termes de gestion et de sécurité.

L'installation et la configuration d'un serveur Windows Server, accompagnées de la migration des données des utilisateurs, ont renforcé mes compétences techniques, notamment dans le choix du matériel adéquat, la configuration précise du serveur, et la gestion des profils utilisateurs grâce à des outils comme User Profile Wizard.

Enfin, la mise en place d'un serveur VPN a permis de sécuriser les communications internes de l'entreprise, en choisissant un protocole VPN adapté et en configurant les paramètres de sécurité appropriés. Cette étape a démontré l'importance de la sécurité dans la gestion des infrastructures réseau d'une entreprise.

En somme, cette expérience a été riche en apprentissages, tant sur le plan technique que pratique, me permettant de développer une compréhension approfondie des défis rencontrés dans le domaine de l'informatique en entreprise et des solutions à apporter pour y faire face. Les compétences acquises au cours de ce stage seront sans nul doute précieuses pour mes futures missions professionnelles.

5 Remerciements

Je souhaite exprimer ma profonde gratitude à toutes les personnes qui ont contribué au succès de mon stage chez HEM France.

Je tiens à remercier particulièrement Monsieur Yoni Haddad, mon superviseur, pour sa confiance, son encadrement et ses conseils avisés tout au long de cette expérience. Son expertise et sa disponibilité ont été d'une grande aide pour mener à bien mes missions.

Je remercie également toute l'équipe de HEM France pour leur accueil chaleureux, leur soutien, et leur collaboration. Leur esprit d'équipe et leur volonté de partager leurs connaissances ont grandement facilité mon intégration et enrichi mon apprentissage.

Enfin, je souhaite exprimer ma gratitude à mes professeurs et formateurs, dont les enseignements comme les cours sur le CCNA et le soutien continu ont été essentiels à ma préparation pour ce stage. Leur guidance m'a permis de tirer le meilleur parti de cette expérience.

À tous, je vous adresse mes sincères remerciements pour votre aide et votre soutien précieux.

6 Glossaire

BUT, Bachelor Universitaire de Technologie

VPN, Virtual Private Network

NAS, Network Attached Storage

Open-space, Espace de travail collectif dans lequel les différents postes ne sont pas séparés par des cloisons

Fingerprinting, Technique utilisée dans la sécurité informatique pour identifier le système d'exploitation d'un appareil connecté à un réseau, souvent à partir des réponses aux requêtes réseau.

IP, Internet Protocol

MAC, Media Access Control

VLAN, Virtual Local Area Network

ISO, est un fichier informatique qui contient une image mémoire du système de fichiers d'un CD ou d'un DVD

BIOS, basic input/output system(programme de démarrage)

DNS, Domain Name System

DHCP, Dynamic Host Configuration Protocol

RDP, Remote Desktop Protocol

7 Bibliographie

Empson, S. (April 17, 2005). *CCNA Command Quick Reference (Cisco Networking Academy Program)* .