Déploiement d'un Réseau d'Entreprise : NovaTech Solutions

Ce document présente une étude détaillée sur la conception et le déploiement d'une infrastructure réseau complète pour une entreprise fictive, NovaTech Solutions. L'objectif principal est de fournir un guide clair et structuré pour la mise en place d'un réseau performant, sécurisé et facile à administrer. Nous aborderons les aspects de conception, d'implémentation, d'administration et de sécurité, en tenant compte des besoins spécifiques de l'entreprise.

NovaTech Solutions est une entreprise fictive comptant 250 employés, répartis sur deux sites principaux : Paris et Lyon. L'entreprise a besoin d'une infrastructure réseau robuste pour supporter ses activités quotidiennes, notamment les applications critiques, la communication interne et l'accès sécurisé aux données. Ce document détaille les choix technologiques, les configurations et les procédures nécessaires pour répondre à ces besoins.

Conception de l'Infrastructure Réseau

La conception de l'infrastructure réseau de NovaTech Solutions est basée sur une analyse approfondie des besoins de l'entreprise. Il est essentiel de prendre en compte la bande passante requise pour les applications critiques, telles que la VoIP, la visioconférence et le transfert de fichiers volumineux. Une architecture réseau bien conçue garantit une performance optimale et une évolutivité future.

Nous optons pour une topologie centralisée avec une connexion VPN inter-sites. Cette architecture offre une gestion centralisée du réseau, une sécurité renforcée et une communication efficace entre les bureaux de Paris et Lyon. Les routeurs Cisco Catalyst 3945 sont choisis pour leur fiabilité et leurs fonctionnalités avancées. Les switches HP Aruba 2930F assurent une connectivité rapide et sécurisée au sein de chaque site. Un firewall Fortinet FortiGate 600E protège le réseau contre les menaces externes.

Le plan d'adressage IP est basé sur IPv4, avec une préparation pour une future migration vers IPv6. Des VLANs sont créés pour segmenter le réseau en fonction des départements (ventes, marketing, RH), améliorant ainsi la sécurité et la performance. Un diagramme détaillé du réseau logique et physique, réalisé avec Visio ou Lucidchart, fournit une représentation visuelle de l'infrastructure.

Implémentation du Réseau

L'implémentation du réseau implique la configuration précise des équipements sélectionnés. Les routeurs Cisco Catalyst sont configurés avec le protocole de routage OSPF pour une convergence rapide et une gestion efficace des routes. La qualité de service (QoS) est activée pour prioriser les applications VoIP et visioconférence, garantissant une qualité audio et vidéo optimale.

Les switches HP Aruba sont configurés avec des VLANs pour segmenter le réseau et améliorer la sécurité. Le protocole Spanning Tree (RSTP) est activé pour éviter les boucles de réseau et assurer une redondance. La sécurité des ports est renforcée avec 802.1X, exigeant une authentification avant l'accès au réseau.

Le firewall Fortinet FortiGate est installé et configuré avec des règles de pare-feu strictes pour contrôler le trafic entrant et sortant. Un VPN IPSec est mis en place pour sécuriser la communication entre les sites de Paris et Lyon. La détection d'intrusion (IPS) est activée pour identifier et bloquer les activités suspectes. Le câblage et l'installation physique respectent les normes TIA/EIA, avec une documentation complète pour faciliter la maintenance et le dépannage.

Mise en Place des Serveurs

Le choix du système d'exploitation serveur est Windows Server 2022, en raison de sa compatibilité avec les applications métiers de NovaTech Solutions et de sa facilité d'administration. Un serveur Active Directory est mis en place pour gérer les utilisateurs et les groupes, en utilisant des GPO (stratégies de groupe) pour configurer les paramètres de sécurité et les applications.

Un serveur DHCP et DNS est configuré et intégré avec Active Directory pour attribuer automatiquement les adresses IP et résoudre les noms de domaine. Un serveur de fichiers est mis en place pour partager les fichiers de manière sécurisée, avec des quotas pour limiter l'utilisation de l'espace disque et des sauvegardes régulières avec Veeam Backup & Replication pour protéger les données contre la perte.

Un serveur d'applications est déployé pour héberger les applications métiers de NovaTech Solutions, telles que le CRM et l'ERP. Le dimensionnement des ressources (CPU, mémoire, stockage) est effectué en fonction des besoins de ces applications pour garantir une performance optimale. La virtualisation peut être envisagée pour optimiser l'utilisation des ressources et faciliter la gestion des serveurs.

Gestion des Utilisateurs et des Postes de Travail

La gestion des utilisateurs et des postes de travail est un aspect crucial de l'administration du réseau. La création des comptes utilisateurs respecte les politiques de mot de passe strictes, avec l'authentification multi-facteurs (MFA) activée pour renforcer la sécurité. Les postes de travail sont configurés de manière centralisée avec Microsoft Deployment Toolkit (MDT), assurant une installation uniforme et rapide.

Un antivirus (Bitdefender) est installé sur tous les postes de travail pour protéger contre les logiciels malveillants. Les mises à jour des logiciels sont gérées de manière centralisée pour garantir la sécurité et la compatibilité. La gestion des droits et permissions est basée sur le principe du moindre privilège, limitant l'accès des utilisateurs aux ressources dont ils ont besoin pour effectuer leur travail. Le contrôle d'accès basé sur les rôles (RBAC) simplifie l'attribution des droits en fonction des fonctions des utilisateurs.

Un support technique est mis en place pour aider les utilisateurs en cas de problème. Un helpdesk est disponible pour répondre aux questions et résoudre les incidents. Une documentation complète est fournie aux utilisateurs pour les aider à utiliser les applications et les ressources du réseau. Des formations sont organisées pour sensibiliser les utilisateurs aux bonnes pratiques de sécurité.

Sécurité du Réseau

La sécurité du réseau est une priorité absolue pour NovaTech Solutions. Des politiques de sécurité claires sont définies, décrivant les règles et procédures à suivre pour protéger le réseau contre les menaces. Les utilisateurs sont sensibilisés à ces politiques et formés aux bonnes pratiques de sécurité, telles que l'utilisation de mots de passe forts et la vigilance face aux tentatives de phishing.

Le réseau est segmenté en VLANs pour isoler les différents départements et limiter l'impact d'une éventuelle compromission. Une zone démilitarisée (DMZ) est créée pour les serveurs exposés, tels que le serveur web et le serveur de messagerie, afin de les protéger contre les attaques directes. Des outils SIEM (Security Information and Event Management) sont utilisés pour surveiller le réseau en temps réel et détecter les anomalies. Les journaux d'audit sont analysés régulièrement pour identifier les activités suspectes.

Des tests d'intrusion sont effectués régulièrement pour identifier les vulnérabilités du réseau. Des simulations d'attaques sont réalisées avec des outils tels que Kali Linux et Metasploit pour évaluer la résistance du réseau aux attaques. Un plan de reprise d'activité (PRA) est mis en place pour assurer la continuité des activités en cas d'incident majeur. Le PRA comprend la sauvegarde des données, la redondance des équipements et les procédures de restauration.

Documentation du Réseau

Une documentation complète du réseau est essentielle pour faciliter l'administration, le dépannage et l'évolution de l'infrastructure. La documentation comprend un schéma détaillé du réseau, représentant la topologie logique et physique. Un plan d'adressage IP est fourni, indiquant les adresses IP attribuées à chaque équipement et VLAN. Les configurations des équipements (routeurs, switches, firewalls) sont documentées de manière précise et accessible.

Les procédures d'administration sont décrites en détail, notamment la création d'utilisateurs, la gestion des serveurs et la configuration des applications. Un plan de sécurité est inclus, détaillant les politiques, les procédures d'urgence et les mesures de protection du réseau. La documentation est mise à jour régulièrement pour refléter les changements apportés à l'infrastructure.

Conclusion

Ce document a présenté une approche complète pour le déploiement d'un réseau d'entreprise pour NovaTech Solutions. Les objectifs de performance, de sécurité et d'administration ont été pris en compte tout au long de la conception et de l'implémentation. L'infrastructure réseau proposée offre une base solide pour supporter les activités actuelles et futures de l'entreprise.

Les perspectives d'évolution incluent la virtualisation des serveurs, le passage au cloud computing pour certaines applications et l'intégration de l'IoT (Internet des Objets) pour les nouveaux services. Une surveillance continue du réseau et une adaptation aux nouvelles menaces sont essentielles pour garantir la sécurité et la performance à long terme.