Conception du réseau et justification des choix techniques

PROJET VERGIS CORPORATION

Groupe Projet N°03 – Promotion X2027

INSTITUT UCAC-ICAM

Table des matières

I. Membres du groupe

Les membres du groupe sont :

- ☺ ATOUGA II Emmanuel Désiré (Chef)
- ☺ DZEMAZO DJOUTSA Erika Leslie
- ☺ DZOUG PEDJIOBAH Jefferson Bradley
- ☺ NKOULOU Joseph Emmanuel
- ☺ SIGHA ELOUNDOU Carla Wendy

II. Contexte du projet

Dans un univers futuriste où la compétition entre les géants technologiques fait rage, Vergis Corporation, pionnière sur la planète Tauron, cherche à renforcer son avantage en modernisant son infrastructure informatique. Récemment, la découverte du Processeur Méta-Cognitif (MCP) a positionné Vergis comme un concurrent sérieux face à Graystone Industries pour un contrat militaire crucial.

Cependant, des événements inattendus ont bouleversé l'équilibre. Graystone Industries, par le biais d'actions secrètes, a réussi à voler les plans du MCP, remportant ainsi le contrat. Tomas Vergis, PDG de Vergis Corporation, voit cette situation comme une opportunité de renforcer la sécurité de l'entreprise et de moderniser son infrastructure.

Nous sommes donc désignés pour repenser l'ensemble de l'architecture réseau, garantir une redondance fiable, sécuriser les accès, et concevoir de nouveaux bâtiments. Cette transformation devient cruciale pour l'avenir de Vergis Corporation dans un environnement technologique concurrentiel.

III. Objectifs attendus

Nous avons plusieurs objectifs pour ce projet :

- **Renforcer la Sécurité du Réseau** :

Mettre en place des mécanismes de sécurité robustes, y compris des ACL (Listes de Contrôle d'Accès) pour restreindre l'accès aux équipements critiques, aux services informatiques, et pour contrôler le flux de trafic.

- **Garantir une Redondance Quasi-Parfaite** :

Concevoir une architecture réseau offrant une redondance fiable pour minimiser les temps d'arrêt en cas de défaillance d'un composant. Utiliser des protocoles de redondance tels que HSRP, VRRP, ou GLBP selon les besoins.

- **Moderniser l'Infrastructure Informatique** :

Repenser l'ensemble de l'infrastructure informatique, en tenant compte de la croissance prévue de l'entreprise en cas de succès dans l'obtention du contrat. Intégrer de nouvelles technologies et concevoir une architecture évolutive.

- **Répondre aux Contraintes du Contrat Militaire** :

Assurer que l'infrastructure informatique répond aux exigences spécifiques du contrat militaire, notamment en facilitant le développement des Cyber Combat Units basées sur le prototype U-87 avec le Processeur Méta-Cognitif (MCP).

- **Implémenter des VLANs et Segmentation du Réseau** :

Établir des VLANs par service et un VLAN d'administration pour améliorer la segmentation et la sécurité du réseau.

- **Intégrer de Nouveaux Bâtiments** :

Concevoir et intégrer de nouveaux bâtiments, y compris une agence et un datacenter, en tenant compte des besoins spécifiques de chaque service et en garantissant une connectivité optimale.

- **Optimiser la Gestion des Adresses IP** :

Mettre en place un plan d'adressage IP efficace, en utilisant le VLSM (Variable Length Subnet Masking) et le CIDR (Classless Inter-Domain Routing) pour optimiser l'utilisation des adresses IP.

- **Mettre en Place des Mécanismes de Contrôle d'Accès Internet** :

Configurer des mécanismes de contrôle d'accès pour restreindre l'accès à Internet, conformément aux contraintes spécifiques du service logistique.

- **Établir une Connectivité MPLS et Sécuriser le Datacenter** :

Mettre en œuvre une connectivité MPLS entre les différents sites, en assurant la sécurité du Datacenter avec une DMZ, et en configurant un routage efficace.

- **Présenter une Maquette de la Nouvelle Infrastructure :**

Produire une maquette détaillée de la nouvelle infrastructure informatique, incluant la configuration réseau, les plans d'adressage, la segmentation, et les mécanismes de sécurité, dans un délai court pour répondre aux besoins urgents de Vergis Corporation.

IV. Conception du réseau

Nous pensons réaliser notre réseau comme suit :

- **Architecture en Étoile avec Redondance** :

Adopter une architecture en étoile pour le réseau, avec un site principal (Tauron City Centre) comme point central, relié au site secondaire (nouveau bâtiment) et à l'agence. Intégrer des mécanismes de redondance pour garantir une disponibilité maximale.

- **Segmentation par VLANs** :

Implanter des VLANs par service pour améliorer la segmentation et la sécurité du réseau. Chaque service aura son VLAN dédié, avec un VLAN d'administration pour les opérations réseau.

- **Protocole de Routage** :

Choix entre EIGRP (Enhanced Interior Gateway Routing Protocol) et OSPF (Open Shortest Path First) pour le routage interne. La décision sera basée sur des critères de performance, de simplicité, et d'évolutivité, avec une justification détaillée.

- **VLSM et CIDR** :

Utilisation de VLSM pour optimiser l'utilisation des adresses IP, permettant une gestion efficace des sous-réseaux. Le recours au CIDR sera envisagé pour simplifier la notation et la configuration des routes.

- **Sécurité des Accès et des Services** :

Mise en place d'ACLs pour contrôler l'accès aux équipements d'interconnexion, aux services informatiques, et pour réguler le flux de trafic entre les services. Les chercheurs auront un accès spécifique au serveur FTP, avec des restrictions sur certains protocoles.

- **Connectivité MPLS et DMZ au Datacenter** :

Établissement d'une connectivité MPLS entre les différents sites, avec un Datacenter sécurisé en périphérie. Configuration d'une DMZ pour héberger un site vitrine et des serveurs spécifiques.

- **Répartition des Charges avec HSRP** :

Utilisation du protocole HSRP pour assurer une redondance au niveau des passerelles par défaut, garantissant une bascule transparente en cas de défaillance.

- **Intégration de Nouveaux Bâtiments** :

Conception des nouveaux bâtiments (agence, réplique du bâtiment principal, datacenter) avec une attention particulière aux besoins spécifiques de chaque service. Assurer une connectivité optimale tout en prenant en compte la croissance anticipée.

- **Optimisation de la Gestion des Adresses IP** :

Élaboration d'un plan d'adressage IP efficace, utilisant le VLSM et le CIDR, pour éviter le gaspillage d'adresses et faciliter la gestion future.

- **Sécurisation des Accès Internet** :

Mise en place de mécanismes de contrôle d'accès pour restreindre l'accès à Internet selon les contraintes spécifiques du service logistique.

V. Justification des choix techniques

a. Classe d'adresse utilisée

Premièrement, il a fallu choisir la classe d'adresse que nous devions utiliser pour adresser notre réseau. Le choix entre les adresses de classe B et de classe C dépend de la taille prévue du réseau et du nombre d'hôtes nécessaires dans chaque sous-réseau.

Adresse	Avantages	Inconvénients
Adresse de classe B	• 65 534 hôtes • Adapté aux réseaux vastes	• Gaspillage d'adresses. • Gestion difficile des sous réseaux.
Adresse de classe C	• Économise d'adresse IP. • Plus facile à gérer et à subdiviser en sous-réseaux.	• Limite le nombre d'hôtes par réseau (environ 254 adresses). • Moins adapté aux grandes entreprises avec de nombreux périphériques.

La configuration actuelle de l'entreprise (un peu moins de 600 hôtes) nous positionne donc tout naturellement sur le choix des adresses de classe C. Nous avons donc soigneusement planifié la gestion des adresses IP pour éviter tout gaspillage et permettre une évolutivité future.

Nous avons utilisé le concept du **VLSM** (Variable Length Subnet Masking) pour diviser un espace d'adresses IP en sous-réseaux de tailles différentes, adaptées aux besoins spécifiques de chaque sous-réseau. Grâce au VLSM, les adresses IP peuvent être allouées de manière plus précise en fonction de la taille réelle des sous-réseaux, évitant ainsi le gaspillage d'adresses IP.

(Voir plan d'adressage en annexe).

b. Protocole de routage utilisé

Le routage est le processus qui permet de déterminer le chemin optimal pour transmettre des données d'un point à un autre à travers un réseau informatique.

Il implique la sélection des itinéraires les plus efficaces pour acheminer les paquets de données d'une source vers une destination, en tenant compte de divers paramètres tels que la distance, la bande passante, la charge du réseau, et d'autres métriques.

Dans notre cas, nous avions le choix entre deux protocoles de routage, **EIGRP** et **OSPF**. Nous allons donc faire une étude comparative de ces deux protocoles afin de voir lequel est le plus adapté à notre situation :

Spécifications	**OSPF**	**EIGRP**
Protocole de routage	Etat de lien	Hybride
Métrique	Bande passante	Bande passante, cout
Algorithme	Djikstra	Vecteur de distance DUAL
Propriétaire Cisco	Non	Oui
Convergence	Rapide	Très rapide
Distance administrative	110	90 (interne) 170 (externe)

Bien qu'**EIGRP** soit un protocole de routage puissant avec des fonctionnalités avancées, son utilisation se limite au niveau des routeurs Cisco ; ce qui n'est pas très avantageux pour des organisations comme Vergis Corporation qui utilisent une multitude d'équipements de différentes marques.

OSPF reste préféré dans des environnements réseau modernes en raison de sa convergence rapide, de sa gestion efficace de la topologie, de sa flexibilité et de son utilisation plus efficiente de la bande passante. La préférence pour OSPF est renforcée pour des réseaux de taille importante, complexes et évolutifs.

c. Redondance du réseau

La redondance dans un réseau informatique joue un rôle crucial en garantissant la disponibilité continue des services, la résilience face aux pannes et la stabilité opérationnelle. Elle consiste à fournir des chemins ou des ressources de secours afin de maintenir la connectivité et les performances du réseau même en cas de défaillance d'un composant.

Nous avons principalement étudié les protocoles de redondance **HSRP**, **VRRP** et **GLBP**. Nous allons donc les comparer afin de déterminer lequel est le plus adapté dans notre situation.

Spécifications	HSRP	VRRP	GLBP
Propriétaire cisco	Oui	Non	Oui
Prise en charge IPV6 & IPV6	Oui	Seulement le VRRPv3	Oui
Rapidité	Moins rapide	Rapide	Moins rapide
Mise en place	Facile	Facile	Modéré
Adresse IP virtuelle	Oui	Oui	Oui

Pour les besoins spécifiques de Vergis Corporation, où la priorité est une redondance fiable et une configuration simple, **HSRP** semble être plus approprié. Son fonctionnement stable et sa simplicité en font un choix solide pour assurer la continuité des services, ce qui est crucial dans le contexte de l'entreprise en compétition pour un contrat militaire.

d. Méthodes utilisées pour assurer la sécurité du réseau

Afin de réguler les accès sur le réseau et filtrer le traffic, nous avons mis en place des ACL (Listes de contrôle d'accès). Les ACL seront mises en œuvre de manière stratégique pour répondre aux contraintes de sécurité de Vergis Corporation. Elles ont été configurées comme suit :

- **Contrôle d'accès aux équipements d'interconnexion**
  Des ACL seront configurées pour restreindre l'accès aux équipements d'interconnexion, notamment les routeurs et les commutateurs. Seuls les informaticiens auront la permission d'accéder en SSH à ces équipements. Cela garantira une gestion sécurisée des infrastructures réseau.

- **Accès aux services informatiques**
  Des ACL seront mises en place pour autoriser ou restreindre l'accès aux différents services informatiques, tels que le support, l'infrastructure et le développement. Seuls les utilisateurs autorisés auront accès à ces services, contribuant ainsi à la confidentialité et à la sécurité des informations.

- **Contrôle des flux de traffic**

Les ACL seront utilisées pour contrôler le flux de trafic entre les différents services. Chaque VLAN sera associé à une ACL spécifique pour réguler les communications. Cela garantira que seuls les services autorisés peuvent communiquer entre eux, renforçant ainsi la sécurité du réseau

- **Accès aux services spécifiques pour les chercheurs**

  Pour répondre à la contrainte de permettre l'accès des chercheurs au serveur FTP de recherche, des ACL spécifiques seront configurées. Cela limitera l'accès au serveur aux chercheurs désignés tout en empêchant l'accès non autorisé à d'autres employés.

- **Restriction des protocoles**

  Les ACL seront utilisées pour restreindre certains protocoles spécifiques. Par exemple, le trafic TFTP et SMTP ne sera pas autorisé sur le sous-réseau des chercheurs, renforçant ainsi la sécurité en évitant l'utilisation non autorisée de ces protocoles.

- **Contrôle des accès internet**

  Les ACL seront utilisées pour restreindre certains protocoles spécifiques. Par exemple, le trafic TFTP et SMTP ne sera pas autorisé sur le sous-réseau des chercheurs, renforçant ainsi la sécurité en évitant l'utilisation non autorisée de ces protocoles.

- **Protection du Datacenter**

  Des ACL seront mises en place au niveau du Datacenter pour réguler l'accès aux différentes ressources, y compris le serveur FTP pour les commerciaux, les applications métiers RH, et l'intranet. Cela garantira que seuls les utilisateurs autorisés peuvent accéder à ces services sensibles.

L'utilisation judicieuse des ACL permettra à Vergis Corporation de mettre en œuvre une politique de sécurité robuste, répondant aux contraintes spécifiques tout en assurant une protection efficace de son réseau informatique.

VI. Conclusion

En concluant ce projet de modernisation, notre équipe a accompli une transformation significative de l'infrastructure informatique de Vergis Corporation. Nous avons relevé le défi de renforcer la sécurité, d'assurer une redondance quasi-parfaite, et de concevoir une architecture évolutive pour répondre aux besoins actuels et futurs de l'entreprise.

La mise en œuvre de technologies telles que les VLANs, les ACLs, le routage dynamique, et la segmentation du réseau a permis d'atteindre une organisation efficace et sécurisée des ressources. L'utilisation judicieuse du protocole HSRP pour la redondance des passerelles par défaut garantit une continuité opérationnelle sans faille.

La conception des nouveaux bâtiments, intégrant une agence, une réplique du bâtiment principal et un datacenter, offre une infrastructure physique adaptée à la croissance anticipée de l'entreprise. L'utilisation de MPLS pour la connectivité entre les sites et la sécurisation du Datacenter avec une DMZ reflètent notre engagement envers la robustesse et la protection des données.

En optimisant la gestion des adresses IP avec VLSM et CIDR, nous avons démontré notre souci d'efficacité et de conservation des ressources. Les mécanismes de contrôle d'accès, notamment les ACLs, assurent la confidentialité des données sensibles tout en permettant une communication fluide entre les différents services.

En somme, cette modernisation positionne Vergis Corporation à l'avant-garde de la compétition technologique. Nous sommes convaincus que cette infrastructure repensée propulsera l'entreprise vers de nouveaux sommets, offrant une base solide pour la réalisation de ses objectifs stratégiques et la concrétisation de ses ambitions dans un monde en constante évolution.