Cahier des charges - Sécurisation du Réseau SafeTech

Contexte

La société SafeTech entreprend une restructuration visant à renforcer la sécurité de son réseau informatique. Dans ce contexte, nous sommes chargés de repenser, développer et mettre en place des solutions techniques pour sécuriser la navigation sur Internet, garantir la sécurité des données et assurer une intervention rapide en cas d'incidents réseau sur le parc informatique. Cette mission est confiée par le Directeur des Systèmes d'Information (DSI).

2. Besoins des Utilisateurs

2.1. Les Professionnels

- Besoins :
  - Accès sécurisé à des ressources matérielles et logicielles spécifiques en toute confidentialité.
  - Possibilité de travailler de manière efficace et sans interruption.
- Stratégie GPO 1 :
  - Définir une stratégie GPO (Gestion des Objets de Groupe) qui permet aux professionnels d'accéder de manière sécurisée à des ressources matérielles et logicielles définies.
  - Cette stratégie doit garantir une expérience utilisateur fluide et sécurisée.
- Stratégie GPO 2 :
  - Créer une deuxième stratégie GPO pour les professionnels, spécifiant d'autres règles d'accès aux ressources, notamment pour des applications spécifiques ou des imprimantes réseau.

2.2. Les Visiteurs

- Besoins :
  - Accès limité à certaines ressources pour des raisons de sécurité.
  - Sécurité renforcée pour prévenir tout accès non autorisé.
- Stratégie GPO 1 :
  - Créer une stratégie GPO spécifique pour les visiteurs, définissant des règles d'accès restreint aux ressources.
  - Limiter l'accès aux sites web et aux applications non essentiels.
  - Imposer des politiques de sécurité strictes, telles que des mots de passe complexes et des délais de verrouillage de session.
- Création de deux groupes utilisateurs :
  - Professionnels (Pierre) avec des accès avancés.
  - Visiteurs (Clément) avec des accès restreints.
- Configuration de deux lecteurs réseau respectifs pour les utilisateurs, donnant accès à des dossiers personnels pour stocker des fichiers de travail.

3. Sécurisation du Réseau

3.1. VLAN

- Besoins :
  - Isolation des réseaux pour les Professionnels et les Visiteurs afin de prévenir les menaces internes.
  - Gestion optimale du trafic pour garantir des performances élevées.
- Création de deux VLAN distincts :
  - VLAN 80 (Professionnels) avec des règles strictes de communication.
  - VLAN 90 (Visiteurs) avec une segmentation totale du trafic.
- Mise en place du routage inter-VLAN et du Network Address Translation (NAT) avec les adresses réseaux : 192.168.80.0/24 et 192.168.90.0/24.

3.2. Serveur DHCP

- Besoins :
  - Attribution automatique des adresses IP dans les VLAN.
  - Gestion centralisée des adresses IP pour éviter les conflits.
- Configuration d'un serveur DHCP avec des paramètres spécifiques pour chaque VLAN.
- Définition de deux plages d'adresses IP réservées pour les deux VLAN.

3.3. Réservation d'Adresses DHCP

- Besoins :
  - Réservation d'adresses IP pour des utilisateurs spécifiques.
- Réservation d'adresses DHCP pour un Professionnel nommé Jean et un Visiteur nommé Clément pour garantir des adresses IP fixes.

4. Outils de Gestion

4.1. GLPI

- Besoins :
  - Gestion efficace des incidents réseau.
  - Communication transparente entre les utilisateurs et l'équipe d'assistance.
- Déploiement de GLPI pour la gestion des incidents.
- Configuration pour l'envoi de courriers électroniques à l'administrateur lors de la clôture d'incidents, assurant ainsi un suivi optimal des problèmes et leur résolution rapide.

4.2. OCS Inventory

- Besoins :
  - Inventaire complet des équipements du parc informatique.

- Déploiement d'OCS Inventory pour inventorier les routeurs, les commutateurs, les bornes WiFi et d'autres équipements du parc informatique, fournissant une vue d'ensemble précise de l'infrastructure.

5. Supervision

5.1. NAGIOS

- Besoins :
  - Surveillance proactive des ressources réseau.
  - Détection rapide des pannes ou des problèmes de service DHCP.
- Configuration de NAGIOS pour superviser en temps réel les ressources du service DHCP, garantissant une disponibilité continue et une intervention immédiate en cas de problèmes.

6. Schéma de l'architecture: