HAMDI Locqmen
AZIZ Souhayl

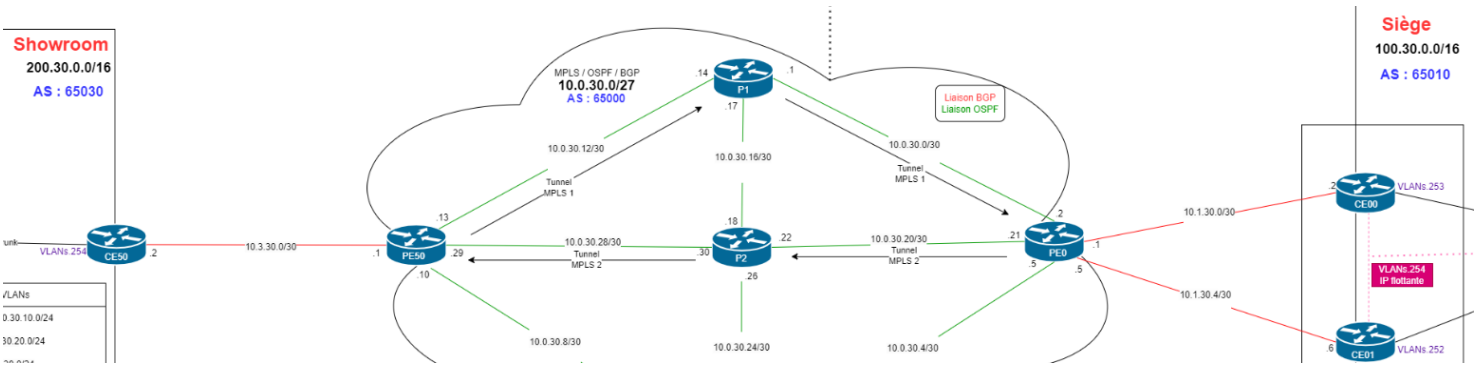
Rapport d'Audit de Sécurité et Propositions d'Amélioration

L'objectif de ce rapport est de présenter les actions réalisées et les recommandations supplémentaires pour renforcer la sécurité du réseau multi-site de Beerok. Cette démarche vise à garantir la protection des données, la continuité de service et la sécurisation des accès au réseau pour les employés et les visiteurs.

Actions Réalisées

1. **Mise en place d'un tunnel MPLS** :

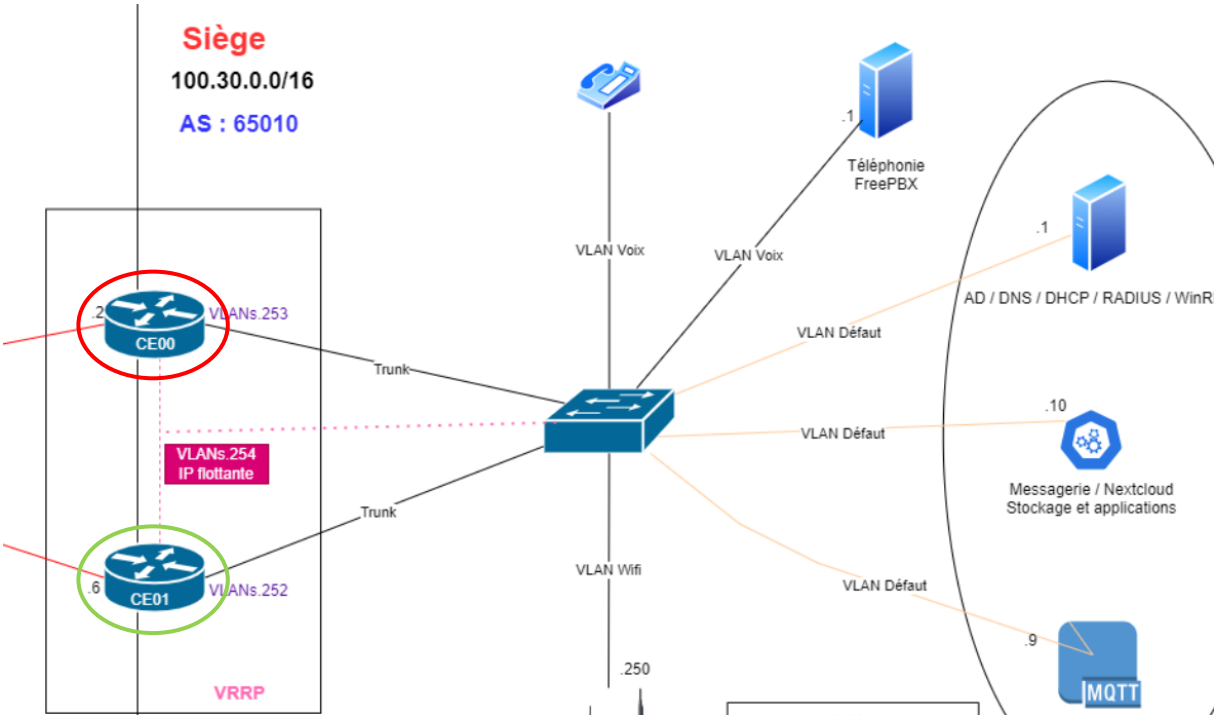
Un tunnel MPLS (Multiprotocol Label Switching) a été mis en place entre le siège et le showroom, utilisant des chemins explicites différents pour sécuriser les communications dans les deux sens. Cette solution offre une transmission de données sécurisée et privée, rendant difficile toute interception ou espionnage des communications entre les sites. De plus, MPLS permet une gestion efficace du trafic réseau, assurant ainsi une latence réduite et une bande passante optimisée.



Les tunnels MPLS sont indiqué sur ce plan à l'aide de flèche noir.

2. **Configuration de deux routeurs avec VRRP au siège** :

Deux routeurs au niveau du siège ont été configurés avec le protocole VRRP (Virtual Router Redundancy Protocol) pour assurer une redondance. Cette configuration permet d'avoir un routeur de secours prêt à prendre le relais en cas de défaillance du routeur principal, minimisant ainsi les interruptions de service et assurant une continuité du service. De plus, la redondance des routeurs garantit que le réseau reste opérationnel même en cas de panne matérielle, ce qui améliore la haute disponibilité.



Ici, si le routeur principal (CE00) tombe en panne, alors le routeur secondaire (CE01) prendra le relai et assurera la continuité des services tout en étant transparent vis-à-vis des utilisateurs.

3. **Portail captif avec authentification RADIUS** :

Un portail captif sur Wi-Fi a été mis en place, nécessitant une authentification via un serveur RADIUS lié à votre Active Directory (annuaire des utilisateurs de votre entreprise) pour contrôler l'accès au réseau. Cette solution renforce le contrôle d'accès en permettant uniquement aux utilisateurs authentifiés d'accéder au réseau, réduisant ainsi les risques d'accès non autorisés. De plus, l'authentification via RADIUS permet de conserver des logs d'accès, ce qui facilite la traçabilité et l'audit des connexions.

Propositions d'Amélioration

1. **Implémentation d'une Connexion VPN** :

Pour plus de sécurité, nous conseillons la mise en place d'une connexion VPN (Virtual Private Network) pour permettre aux employés de se connecter de manière sécurisée au réseau de l'entreprise depuis les magasins ou en déplacement.

La mise en place d'un VPN permet de sécuriser les accès distants en chiffrant les communications, ce qui protège les données sensibles contre toute interception. Cela offre également une grande flexibilité aux employés, qui peuvent accéder aux ressources de l'entreprise de manière sécurisée, où qu'ils se trouvent. La mise en place d'un VPN assurera que les données échangées entre les employés distants et le réseau de l'entreprise restent intègres et confidentielles

2. **Configuration d'une Politique de Sécurité** :

Il est essentiel de définir et de mettre en œuvre une politique de sécurité pour l'entreprise, qui inclut des règles et des procédures pour la gestion des accès, la protection des données et la réponse aux incidents. Une telle politique clarifie les rôles et les responsabilités de chaque employé en matière de sécurité, réduit les risques de comportements inappropriés ou négligents, et aide l'entreprise à se conformer aux normes et régulations en vigueur, assurant ainsi une meilleure protection globale. Nous proposons de vous aider à mettre en place cette politique de sécurité en se conformant aux recommandations de l'ANSSI.

3. **Politique de Mot de Passe sur l'Active Directory** :

Nous vous recommandons également de configurer une politique de mot de passe sur l'Active Directory (AD) pour imposer des mots de passe forts et gérer régulièrement leur renouvellement. Cela renforce la sécurité des comptes utilisateurs en réduisant les risques de compromission, car des mots de passe complexes et régulièrement changés sont plus difficiles à deviner ou à casser. En d'autres termes, cette politique garantit que l'entreprise suit les bonnes pratiques de sécurité standard, vous permettant de bénéficier d'une meilleure protection des données et des systèmes.

4. **Système de Sauvegarde des Données avec un NAS Synology** :

Enfin, nous vous recommandons la mise en place d'un système de sauvegarde des données en utilisant un NAS (Network Attached Storage) Synology pour stocker et protéger les données de l'entreprise. Ce système permet de protéger les données critiques contre les pertes dues à des défaillances matérielles ou à la corruption des données grâce à des sauvegardes régulières. En cas d'incident, les données peuvent être rapidement restaurées, ce qui minimise les temps d'arrêt. De plus, le NAS centralise toutes les sauvegardes, ce qui simplifie la gestion et la récupération des données. Nous vous recommandons aussi cela car il vous permet de garder la main sur vos données plutôt que de les stocker sur des cloud.

Conclusion

Les mesures déjà implémentées permettent déjà une bonne sécurité du réseau Beerok. Les propositions d'amélioration suggérées visent à compléter cette sécurisation et à assurer une protection continue contre les menaces de cybersécurité. La mise en œuvre de ces recommandations permettra à Beerok de maintenir un environnement de travail sécurisé et résilient face aux défis actuels de la cybersécurité.

Nous restons à votre disposition pour toute clarification ou assistance supplémentaire concernant ces propositions.