AC32.04 – Permettre aux Collaborateurs de Se Connecter de Manière Sécurisée au Système d'Information de l'Entreprise Contexte

La sécurité des connexions à distance est un enjeu majeur pour garantir la confidentialité et l'intégrité des données échangées entre les collaborateurs et l'entreprise. Dans le cadre de la **SAE CTF**, l'objectif était de configurer un **VPN OpenSSL** afin de permettre aux collaborateurs d'accéder en toute sécurité au système d'information de l'entreprise à partir de n'importe quel réseau, tout en assurant une authentification forte et un chiffrement des données.

Savoir mis en œuvre

- **Installation et configuration d'un VPN OpenSSL** : Mise en place de **OpenSSL** pour créer des certificats et gérer l'authentification des utilisateurs à travers des connexions VPN sécurisées.
- **Création des certificats SSL** : Génération de certificats pour le serveur et pour les clients VPN, permettant ainsi de garantir la confidentialité et l'intégrité des échanges.
- **Configuration du serveur VPN** : Configuration d'un serveur **OpenVPN** pour assurer le tunnel chiffré entre le client et le serveur, et permettre une communication sécurisée à travers un réseau non sécurisé.
- **Règles de sécurité** : Mise en place de règles strictes pour gérer les accès, avec l'utilisation de certificats et de clés privées, garantissant l'identification et l'authentification des utilisateurs.

Savoir-faire mis en œuvre

- **Installation du serveur OpenVPN** : Configuration d'un serveur VPN sur une machine dédiée en utilisant **OpenSSL** pour générer des certificats SSL nécessaires à l'authentification.
    - Création d'une **Autorité de Certification (CA)** interne pour signer les certificats du serveur et des clients.
    - Configuration des règles de pare-feu pour autoriser les connexions VPN tout en maintenant la sécurité du réseau interne.
- **Configuration des clients VPN** : Déploiement des certificats sur les postes des collaborateurs, installation du client OpenVPN et configuration de la connexion à distance.

- **Sécurisation de l’accès distant** : Mise en place de **chiffrement de bout en bout** pour protéger les données échangées, et utilisation de l'authentification basée sur des certificats pour éviter l’utilisation de mots de passe vulnérables.
- **Tests de la solution** : Validation de la connexion sécurisée en simulant des scénarios où des utilisateurs se connectent depuis des réseaux externes, tout en vérifiant que les données sont correctement chiffrées.

Savoir-être mis en œuvre

- **Précision** dans la configuration des certificats et des règles de sécurité pour garantir l'intégrité de l'architecture VPN.
- **Rigueur** dans l’application des bonnes pratiques pour sécuriser les accès distants et minimiser les risques d'intrusion.
- **Sens de l’analyse** pour vérifier que chaque connexion VPN respecte les critères de sécurité définis (certificats valides, chiffrement efficace, etc.).
- **Proactivité** dans la gestion des mises à jour de sécurité des outils et des certificats pour garantir la pérennité de la solution VPN.

Tâches réalisées et résultats Tâches effectuées :

Création d'une infrastructure de certificats : Mise en place d’une **CA** interne avec **OpenSSL** pour signer les certificats du serveur et des clients VPN. **Installation et configuration du serveur OpenVPN** : Mise en place de la solution **OpenVPN**, avec configuration des règles de pare-feu et de routage pour gérer le trafic VPN. **Déploiement des clients VPN** : Installation et configuration des clients VPN sur les ordinateurs des collaborateurs avec les certificats nécessaires. **Tests de sécurité** : Vérification de la sécurité du tunnel VPN en analysant les logs, en simulant des attaques de type **Man-in-the-Middle** et en s’assurant que toutes les connexions sont correctement chiffrées. **Mise à jour et maintenance** : Mise à jour régulière des certificats et de l’infrastructure pour maintenir la sécurité à long terme.

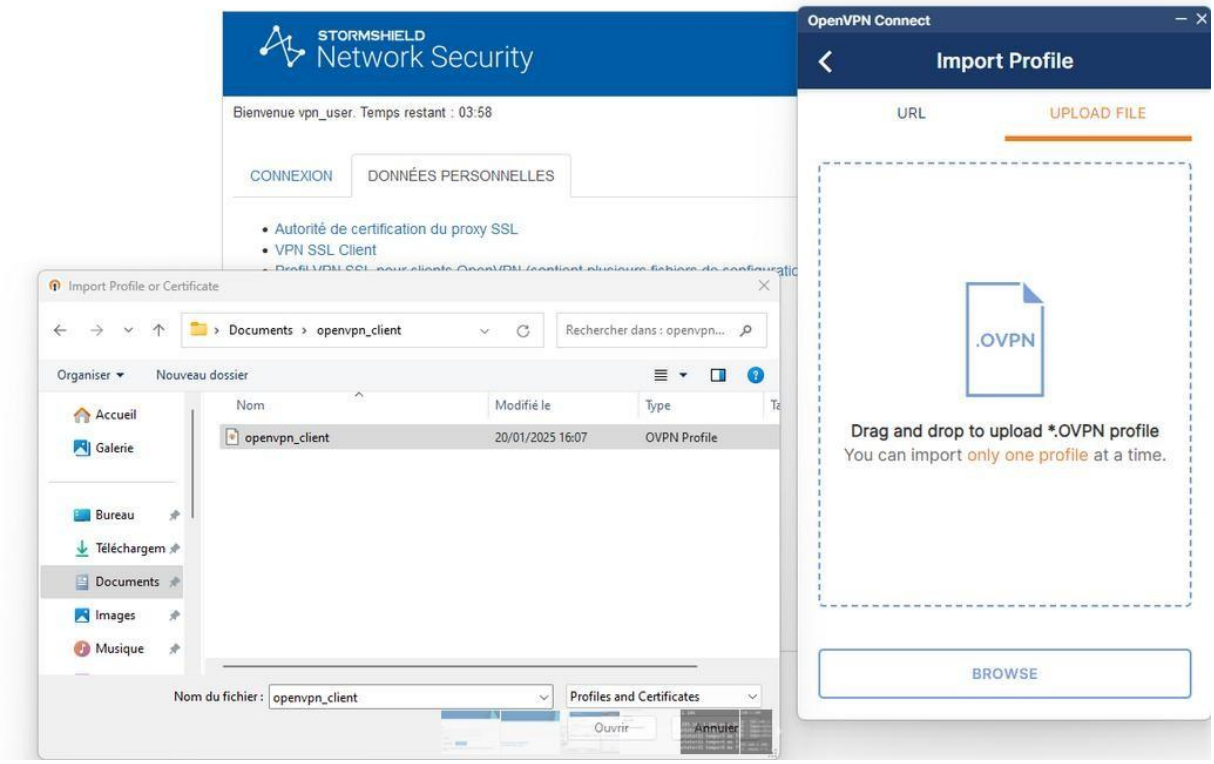
Résultats :

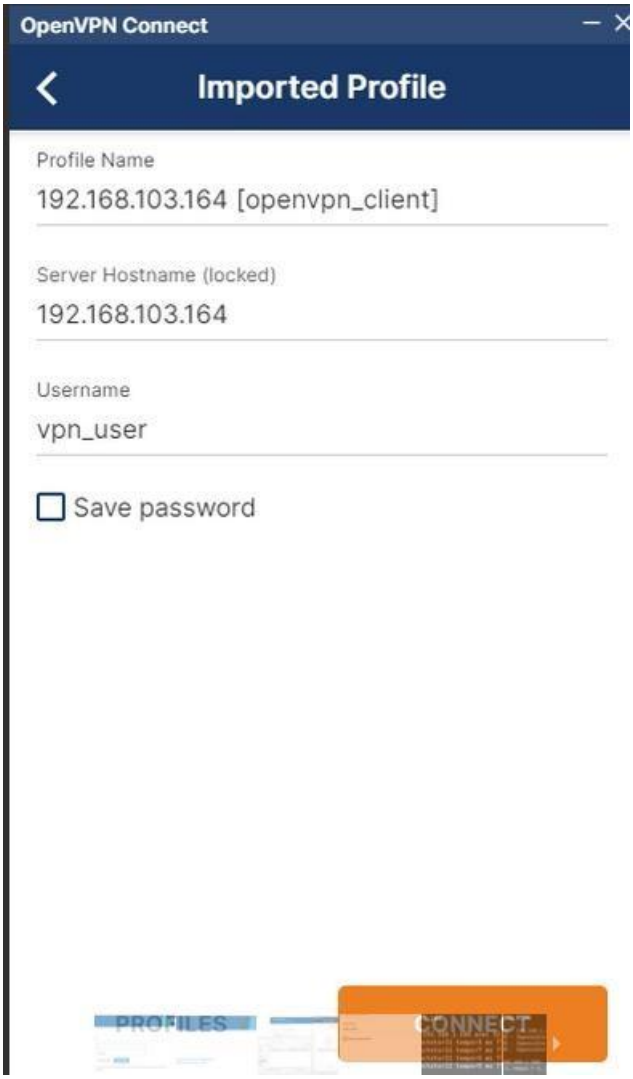
- **Accès sécurisé au réseau de l’entreprise** pour tous les collaborateurs, garantissant la confidentialité et l’intégrité des données échangées via VPN.
- **Authentification forte** grâce à l’utilisation de certificats SSL pour l’authentification des utilisateurs.

- **Tunnel chiffré sécurisé** permettant de protéger les communications, même lorsqu'elles transitent par des réseaux publics ou non sécurisés.
- **Solution flexible et évolutive** qui peut être déployée à grande échelle avec une gestion centralisée des certificats et des connexions.

Analyse réflexive :

Pour sécuriser l'accès au système d'information de l'entreprise, j'ai mis en place un VPN OpenVPN avec une infrastructure de certificats gérée via OpenSSL. La première étape a consisté à créer une autorité de certification interne afin de générer et signer les certificats nécessaires pour le serveur et les clients. Ensuite, j'ai installé et configuré le serveur VPN en définissant les règles de pare-feu et de routage pour sécuriser les connexions distantes. Après cela, j'ai déployé les certificats sur les postes des collaborateurs et configuré les clients VPN. Enfin, j'ai réalisé des tests de sécurité pour vérifier le chiffrement des connexions et la résistance aux attaques de type Man-in-the-Middle. Cette approche garantit un accès sécurisé, mais nécessite une vigilance constante pour maintenir un haut niveau de sécurité. Pour améliorer la solution, l'automatisation du renouvellement des certificats et une supervision en temps réel des connexions pourraient être mises en place afin d'anticiper les incidents et d'optimiser la gestion des accès distants.




OpenVPN Connect
Imported Profile
Profile Name
192.168.103.164 [openvpn_client]
Server Hostname (locked)
192.168.103.164
Username
vpn_user
Save password
PROFILES
CONNECT