

AC33.07 – Mettre en œuvre des outils avancés de sécurisation d'une infrastructure réseau

Contexte

Cette compétence concerne la mise en œuvre d'outils et de solutions avancées pour sécuriser une infrastructure réseau. Il s'agit notamment de **protéger les flux réseau** et d'implémenter des **mécanismes de sécurité** comme des **firewalls**, des **systèmes de détection/prévention d'intrusions** (IDS/IPS), ainsi que la mise en place de **VPNs** de différents types (IPSec, OpenVPN, TLS, MPLS).

Savoir mis en œuvre

- **Sécurisation du trafic réseau** : Utilisation de **firewalls** et de **mécanismes avancés** pour contrôler le trafic entrant et sortant.
 - **Détection et prévention des intrusions (IDS/IPS)** : Installation et configuration de systèmes permettant de détecter les activités malveillantes.
 - **Mise en place de VPNs** : Configuration de **VPNs IPSec, OpenVPN, TLS et MPLS** pour garantir la sécurité des communications entre différents sites.
 - **Gestion des accès et des profils utilisateurs** : Définition des **règles d'accès** pour les utilisateurs et les périphériques.
 - **Sécurisation des accès Wi-Fi** : Mise en place de politiques de sécurité pour protéger les réseaux sans fil.
-

Savoir-faire mis en œuvre






- **Configuration avancée de firewalls** pour filtrer le trafic réseau et empêcher l'accès non autorisé.
 - **Mise en place de systèmes IDS/IPS** pour surveiller et analyser les flux réseau en temps réel.
 - **Interconnexion des sites via VPNs** de différents types pour assurer une communication sécurisée entre les sites distants.
 - **Gestion des profils d'utilisateurs** : Attribuer des droits d'accès selon les rôles, avec une gestion fine des permissions.
 - **Configuration de la sécurité des réseaux sans fil (Wi-Fi)** en utilisant des protocoles de sécurité comme WPA3.
-

Savoir-être mis en œuvre




- **Précision** dans la configuration des outils pour éviter les erreurs de sécurité.
 - **Proactivité** pour tester et déployer des solutions de sécurité avant que des incidents ne surviennent.
 - **Capacité d'adaptation** aux nouvelles menaces et aux outils de sécurisation émergents.
 - **Esprit de collaboration** pour travailler avec les autres membres de l'équipe afin d'assurer une sécurité optimale.
-

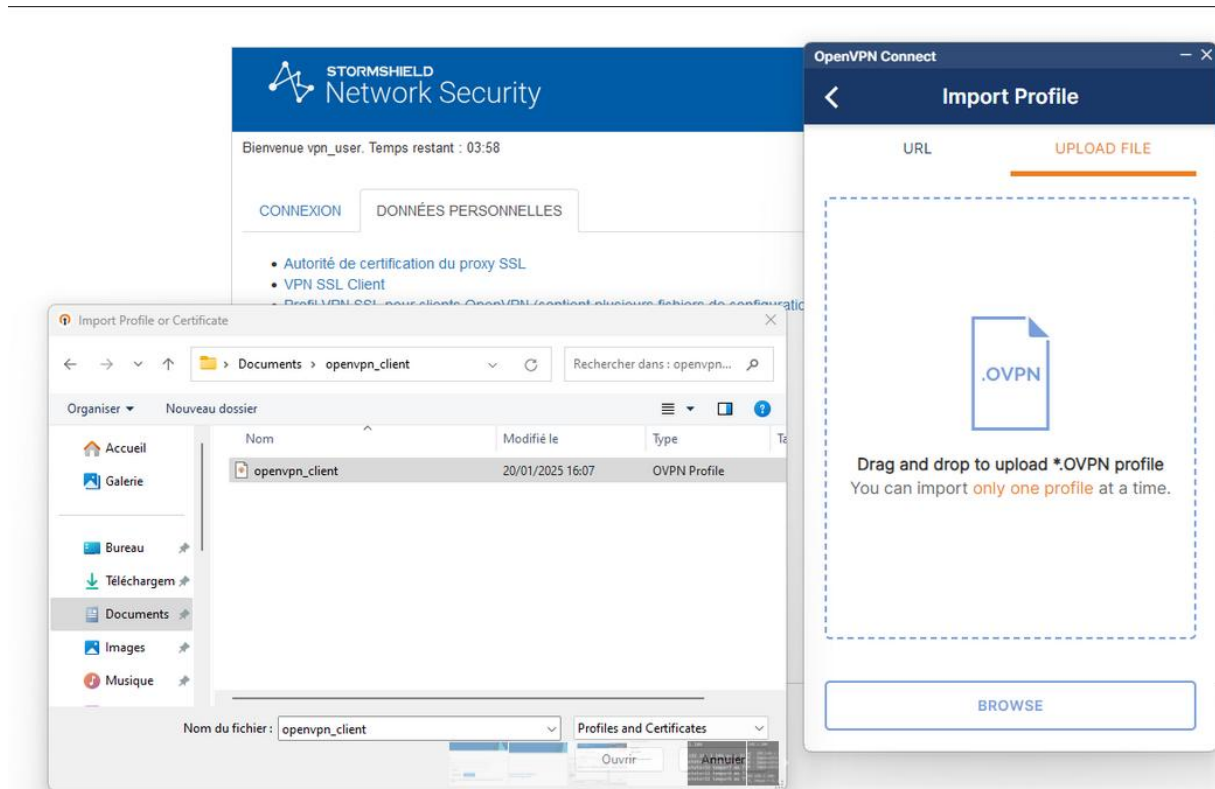
Tâches réalisées et résultats

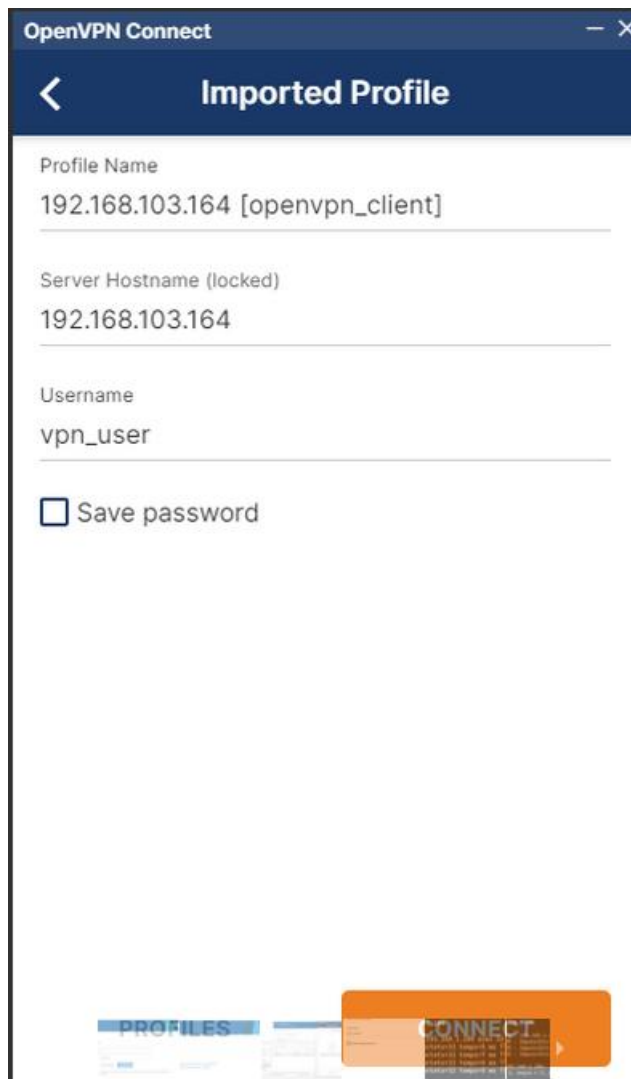
Tâches effectuées :

-  **Mise en place de filtres avancés** avec des firewalls pour contrôler le trafic réseau.
-  **Installation et configuration d'IDS/IPS** pour détecter les intrusions potentielles.
-  **Création de VPNs** (IPSec, OpenVPN, TLS, MPLS) pour connecter les sites de manière sécurisée.
-  **Gestion des accès utilisateur** avec des solutions d'authentification avancées.
-  **Configuration de la sécurité Wi-Fi** avec des mécanismes comme WPA3 pour assurer des connexions sûres.

Résultats :

-  **Réseau sécurisé** grâce à la mise en place de mécanismes de filtrage, détection et prévention des intrusions.
-  **Sites interconnectés de manière sécurisée** via des VPNs.
-  **Protection des données et des utilisateurs** grâce à une gestion fine des profils d'accès et à une politique de sécurité Wi-Fi solide.





```
C:\Users\Admin>ping 192.168.1.104
```

```
Envoi d'une requête 'Ping' 192.168.1.104 avec 32 octets de données :  
Réponse de 192.168.1.104 : octets=32 temps=5 ms TTL=64  
Réponse de 192.168.1.104 : octets=32 temps=7 ms TTL=64  
Réponse de 192.168.1.104 : octets=32 temps=4 ms TTL=64  
Réponse de 192.168.1.104 : octets=32 temps=5 ms TTL=64
```