VPN : accès distant et interconnexion de sites

Formation : BTS SIO — Option SISR

1. Rôle et fonctionnement

Un VPN établit un tunnel protégé entre deux points à travers un réseau intermédiaire. Le mode site à site relie des réseaux ; le mode accès distant raccorde un poste utilisateur à un périmètre défini. Le sujet est annoncé dans la feuille de route le laboratoire ; aucune recette de tunnel opérationnel n'est encore fournie.

IPsec protège les communications IP ; IKE négocie les paramètres et authentifie les pairs. D'autres solutions transportent le tunnel au-dessus de TLS. Le choix doit correspondre aux équipements et au besoin d'accès.

2. Préparer un tunnel

Documenter les pairs, les réseaux locaux et distants, la méthode d'authentification, les propositions cryptographiques et les routes. Vérifier l'absence de chevauchement entre les réseaux à relier. Définir les flux autorisés dans le tunnel et l'éventuelle exemption NAT selon la solution.

Un tunnel établi ne signifie pas que tous les sous-réseaux sont accessibles : routes, sélecteurs et filtrage doivent être cohérents aux deux extrémités.

3. Recette

Contrôle	Attendu
Authentification des pairs	Identités connues et validées
Établissement	Associations actives des deux côtés
Flux utile	Service prévu accessible
Flux interdit	Accès refusé et journalisé
Reconnexion	Rétablissement mesuré après coupure

4. Dépannage

Distinguer négociation impossible, tunnel établi sans trafic et trafic à sens unique. Vérifier les propositions, les routes retour et le NAT avant de modifier le chiffrement. Le VPN ne remplace pas un bastion : le premier transporte les flux, le second encadre les sessions d'administration.

5. Références

- strongSwan — principes IPsec/IKE

From:
https://wiki.ewengadonnaud.xyz/ - **Base de savoir réseaux/cyber/devops**

Permanent link:
https://wiki.ewengadonnaud.xyz/doku.php?id=reseau:vpn

Last update: **2026/10/18 01:23**