VPN – Réseaux Privés Virtuels

Date et durée

Code formation : SEC11FR
Durée : 4 jours
Nombre d'heures : 28 heures

Description

Le VPN, pour Virtual Private Network, est une technologie permettant de créer un lien direct et exclusif entre deux postes séparés, l'idée de base étant de sécuriser les données échangées de toute intrusion extérieure. Cette formation vous apprendra à comprendre et mettre en oeuvre diverses configurations de VPN.

Objectifs

Au cours de cette formation le stagiaire assimilera les éléments théoriques nécessaires permettant la mise en œuvre concrète des différentes configurations de VPN.
Les travaux pratiques sont basés sur des matériels Cisco et des postes sous Linux et sous Windows.

Pré-requis

Connaissance de base de TCP/IP

Cette formation s'adresse aux profils suivants

Administrateur système
Directeur des Systèmes d'Information (DSI)
Ingénieur système

Programme

- Typologie et généralités sur les VPN
- Sécurité du protocole IP (Ipsec)
  - Le protocole IPsec et sa mise en œuvre
    - Tunnel site à site
    - Tunnel poste à site
    - Tunnel poste à poste
  - Avantages et limitations du protocole IPsec
  - Utilisation avancée d'IPsec et résolution de problèmes
  - IPsec et les translations d'adresses
- Sécurité des couches applicatives : SSL et TLS
  - Le protocole SSL/TLS
  - Le protocole OpenVPN
  - Mises en œuvre :
    - Sans client
    - Client léger

        - Tunnel intégral avec client lourd
- Autres protocoles
    - L2TP
    - PPTP
    - Etc…
- Clients VPN autonomes ou managés
- Méthodes d'authentifications :
    - Locale
    - Centralisée (AD, LDAP, Radius)
    - Certificats
    - Authentification forte des nomades