Formation Réseaux Virtuels Privés (VPN)

Durée :	3 jours
Public :	Administrateurs réseaux
Pré-requis :	Connaissances en TCP/IP, réseau
Objectifs :	Maîtriser la mise en place de VPN sécurisés
Sanction :	Attestation de fin de stage mentionnant le résultat des acquis
Taux de retour à l'emploi:	Aucune donnée disponible
Référence:	RéS610-F
Note de satisfaction des participants:	Pas de données disponibles

Introduction

Réseaux d'entreprise : composantes, mobilité
Menaces sur les communications réseaux
VPN : définition, utilisations, construction

Cryptage

Chiffrage des données dans un VPN
Signatures et certificats
Clés publiques (PKI)

Sécurisation d'un VPN

Gestion des authentifications : PPP, PAP, CHAP, Radius, Tacacs
Panorama de serveurs d'authentifications
IPSec (Internet Protocol Security) : présentation, modes opératoires, mise en place
Multiprotocol Label Switching (MPLS)
Sécurité des applications : SSL, TLS, SSH

Mise en place / maintenance

Choix de l'architecture, intégration à l'existant
Gestion de la sécurité : communications, clés, sécurité IPv6
Solutions matérielles : routeurs, concentrateurs VPN, clients matériels
Solutions logicielles : Open Source, FreeS/WAN (Linux), Cisco, Microsoft
VPN administrés : Smartpipe, Openreach, Interasys
Administration courante et audit de VPN