

## Formation Réseaux Virtuels Privés (VPN)

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