

## VPN - PRÉSERVER SES INFORMATIONS SUR INTERNET

Durée

3 jours

Référence Formation

3-SR-VPN

### Objectifs

Connaitre les menaces de vos communications internes, inter site, nomades

Appréhender les opportunités technologiques

Bonnes pratiques pour leur mise en service, leur suivi et leur contrôle

### Participants

### Pré-requis

Professionnels de la sécurité, les administrateurs, les ingénieurs réseau, les techniciens informatique Bonne compréhension des protocoles TCP/IP, pratique de l'Internet et des applications standards

### PROGRAMME

- 1. VPN : Assurer des communications sûres dans un environnement hostile  
Organisations étendues et mobilité  
Menaces sur les communications  
Objectifs de la sécurité des communications
- 2. Réseaux Virtuels Privés  
Qu'est ce qu'un VPN ?  
Quelles utilisations ?  
Comment construire ou acquérir un VPN?
- 3. Première approche de la cryptographie  
Transformation des messages - chiffrement et déchiffrement  
Deux types de chiffrement  
Signatures numériques  
Certificats numériques  
Implantation des protections  
Vieillessement et révocation automatique et manuelle des clés
- 5. Gestion de clés publiques (PKI)  
Objectif de la PKI  
Caractéristiques et éléments de la PKI  
Exemples de PKI
- 6. Première approche de l'encapsulation et de l'étiquetage  
TCP/IP et le modèle OSI  
Serial Line Interface Protocol (SLIP), «Point to point protocole» (PPP), «Point to point Tunneling Protocol» (PPTP)  
Level 2 Forwarding (L2F), Layer 2 Tunneling Protocol (L2TP)  
Multiprotocol Label Switching (MPLS)  
Protocole de réservation de ressource (RSVP), services différenciés (DiffServ), et services intégrés IETF (IntServ)
- 7. Sécurité du protocole IP (Ipsec)  
Qu'est ce que l'Ipsec ?  
Association de sécurité (SA), Base de données de sécurité (SADB), Base de données des procédures (SPD)  
Mode opératoire et services de sécurité d'Ipsec  
Phases et échange de clés Internet (IKE)

Risques et limites d'IPSEC  
Principaux matériels/logiciels permettant de créer des VPN IPSEC  
·8. Sécurité des couches applicatives : SSL, SSH et TLS  
Qu'est ce que SSL/TLS ?  
Mode opératoire et services de sécurité de SSL/TLS  
Risques et limites de SSL/SSH  
Principaux matériels/logiciels permettant de créer des VPN SSL/TLS/SSH  
·9. Modèles propriétaires : LEAP/WPA/VNC/...  
La sécurité nécessaire des communications sans fils  
Des solutions cryptographiques propriétaires controversées  
Quelle harmonisation ?  
·10. Architecture de communications sécurisées  
Applications à servir, répartition des risques, politique, et architecture  
Lieu d'installation des services de protection  
Sécurité des communications et disponibilité  
Approche de choix de solutions  
·11. Gestion et maintenance des communications sécurisées  
Principes pour maintenir et gérer des communications sécurisées  
Recherche et correction des fautes  
Performance  
Gestion des clés  
Directions futures  
Services de sécurité dans IPV6

## Moyens pédagogiques

Accueil des stagiaires dans une salle dédiée à la formation équipée d'un vidéo projecteur, tableau blanc et paperboard ainsi qu'un ordinateur par participant pour les formations informatiques.  
Positionnement préalable oral ou écrit sous forme de tests d'évaluation, feuille de présence signée en demi-journée, évaluation des acquis tout au long de la formation.  
En fin de stage : QCM, exercices pratiques ou mises en situation professionnelle, questionnaire de satisfaction, attestation de stage, support de cours remis à chaque participant.  
Formateur expert dans son domaine d'intervention  
Apports théoriques et exercices pratiques du formateur  
Utilisation de cas concrets issus de l'expérience professionnelle des participants  
Réflexion de groupe et travail d'échanges avec les participants

Pour les formations à distance : Classe virtuelle organisée principalement avec l'outil ZOOM. Assistance technique et pédagogique : envoi des coordonnées du formateur par mail avant le début de la formation pour accompagner le bénéficiaire dans le déroulement de son parcours à distance.