

Les VPN

Objectif :

Vous souhaitez permettre à vos collaborateurs et à vos sites distants d'accéder aux ressources de votre organisation à moindre coût et de manière sécurisée ?

La mise en œuvre d'un réseau privé virtuel est la solution sur les réseaux filaires comme sur les réseaux sans-fil.

Cette formation VPN vous permettra d'apprendre:

- A vous défendre contre ce qui menace vos communications, en particulier avec les mobiles
- Les motivations pour avoir un VPN - coût, sécurité et choix de technologie
- Les procédés d'encodage et de décodage des messages
- Les procédés d'encapsulation en particulier les offres opérateurs mpls
- Ce que sont les vpn Ipsec et ssl/tls, leurs avantages et limites respectifs
- A décrire les fonctions , les charges, les attributs, les phases et échanges du protocole ISAKMP (Ipsec Security Associations and Key Management Protocol)
- Les défis à détecter et la correction des erreurs dans les réseaux sécurisés

Participants :

Les professionnels de la sécurité, les administrateurs, les ingénieurs réseau, les responsables de sites web, les consultants e-commerce et développeurs, les responsables de communication et les responsables informatiques.

Pré-requis :

Bonne compréhension des protocoles TCP/IP, pratique de l'Internet et des applications standards.

Durée : 3 jours (21 heures) Référence : RVPN

Contenu de la formation :

VPN: Assurer des communications sûres dans un environnement hostile

Organisations étendues et mobilité
Menaces sur les communications
Objectifs de la sécurité des communications

Réseaux Virtuels Privés

Qu'est ce qu'un VPN ?
Quelles utilisations ?
Comment construire ou acquérir un VPN?

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

Gestion de clés publiques (PKI)

- Objectif de la PKI
- Caractéristiques et éléments de la PKI
- Exemples de PKI

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)

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

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

Modèles propriétaires : LEAP/WPA/VNC/?

- La sécurité nécessaire des communications sans fils
- Des solutions cryptographiques propriétaires controversées
- Quelle harmonisation ?

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

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