Mise en œuvre de VPNs

Durée : 3 jours Référence : VPN

Cette formation vous apportera toutes les connaissances nécessaires à la conception, l'établissement et l'administration d'un réseau privé virtuel, VPN, sous différents couches OSI.

Contenu

- Introduction
- VPN à différentes couches OSI
- La cryptographie dans les réseaux privés virtuels
- Fonctionnement des VPN PPTP
- Fonctionnement des VPN L2TP
- Fonctionnement des VPN IPsec
- Fonctionnement des VPN SSL-TLS
- Les solutions du marché
- Travaux pratiques

Participants

Techniciens, Administrateurs et ingénieurs réseau et responsables sécurité.

Pré-requis

Connaissances de TCP/IP, systèmes et réseaux.

Programme

Introduction

- Faiblesses des communications TCP/IP
- Besoins d'interconnexions et réseaux d'entreprise du LL(LS) à l'xDSL
- Apports et réponses apportés par les VPN

VPN à différentes couches OSI

- VPN au niveau 2

PPTP, L2F, L2TP

- VPN au niveau 2.5
  MPLS, les offres opérateurs
- VPN au niveau 3 et +
  IPSEC, SSL/TLS, SSH

La cryptographie dans les réseaux privés virtuels

- Cryptographie symétrique, Cryptographie asymétrique, fonctions de hachage
- Compléments sur Diffie-Hellman
- Compléments sur les certificats numériques et les autorités de certification
- Compléments sur les algorithmes les plus utilisés DES, 3DES, AES, SAH1, SHA2, MD5…

Fonctionnement des VPN PPTP

- Composants d'un tunnel PPTP
- Mécanismes de mise en oeuvre
- La connexion de contrôle
- Le protocole GRE dans PPTP
- VPN avec PPTP

Fonctionnement des VPN L2TP

- Composants d'un tunnel L2TP
- LAC (L2TP Access Concentrator), LNS (L2TP Network Server)
- Les mécanismes du L2TP
- L2TP/IPsec (L2TP over IPSEC)
- VPN L2TP/IPsec en poste à site

Fonctionnement des VPN IPsec

- Construction d'un tunnel IPsec
- AH (Authentication Header), ESP (Encapsulating Security Payload)

  Intégration de l'en-tête AH et ESP dans un paquet IP en mode tunnel
  Avantages et Limites du protocole AH et ESP
- Paramètres de sécurité d'un tunnel
  Contenu d'une SAD ou SADB (Security Association Database)

Création des SA

SPD (Security Policy Database), PAD (Peer Authorization Database)

- Présentation du protocole IKE (Internet Key Exchange) et ISAKMP

  IKE v1, v2

  ISAKMP

- Notions avancées

  Mode transport

  IKE Keep-Alive et DPD (Dead Peer Detection), IKE KEEP-ALIVE, Dead Peer Detection (DPD)

- NAT-Traversal ou NAT-T

Fonctionnement des VPN SSL-TLS

- Principes de fonctionnement de SSL
- Les principaux protocoles mis en œuvre
- PKI et Certificats
- Protocoles Handshake et Change Cipher Spec
- Exemples de données échangées entre un client et un serveur
- VPN Clientless (VPN SSL)
- Établissement d'une session SSL entre un navigateur et un serveur

Les solutions du marché

- Les solutions matériels

  VPN Firewall, concentrateurs VPN, VPN Appliances, SSL Apliances…

- Les solutions logiciels

  open swan, ZyXEL, open, free net BSD, Linux, Windows, ….

Travaux pratiques

- Implémentation d'IPsec en site à site

  Mise en œuvre entre deux sites avec adresses IP fixes – Avec une adresse IP fixe et une adresse IP dynamique – avec ou sans DYNDNS

- Implémentation d'IPsec en poste à site

  Mise en œuvre entre un poste anonyme et un site à adresse IP fixe et dynamique avec secret partagé

- Implémentation d'IPsec en poste à poste

  Mise en œuvre entre deux machines sous Windows/linux

- Implémentation de VPN SSL/TLS

  Connexion avec un client spécifique et authentification classique par nom d'utilisateur et mot de passe

  Configuration du VPN, Téléchargement du client depuis le pare-feu, Mise en place des certificats sur le pare-feu

  Connexion sans client (clientless) et authentification par nom d'utilisateur

  Exemple d'utilisation d'un pare-feu, Configuration du VPN, Mise en place des certificats sur le pare-feu

  Exemple d'utilisation d'un boitier dédié SSL

  Exemple d'utilisation d'un pare-feu