

Sommaire

1. Introduction aux réseaux privés virtuels

- Définition et objectifs des VPN
- Besoins des entreprises
- VPN et réseaux publics
- Avantages et limites

2. Principes de sécurité des VPN

- Confidentialité
- Intégrité des données
- Authentification
- Contrôle d'accès
- Non-répudiation

3. Cryptographie appliquée aux VPN

- Chiffrement symétrique
- Chiffrement asymétrique
- Fonctions de hachage
- Signatures numériques
- Gestion des clés

4. Protocoles et techniques de tunneling

- Principe du tunneling
- Encapsulation des données
- Protocoles de transport
- VPN basés sur IP

5. Protocoles de sécurité

- IPsec
- SSL/TLS
- Authentification et négociation
- Échange de clés

6. Architectures VPN

- VPN d'accès distant
- VPN site à site
- Intranets
- Extranets
- Interconnexion de réseaux

7. Conception d'une solution VPN

- Analyse des besoins

- Choix de l'architecture
- Sécurité et performances
- Dimensionnement

8. Déploiement et administration

- Mise en œuvre d'un VPN
- Configuration
- Gestion des utilisateurs
- Surveillance et maintenance

9. Solutions et outils du marché

- Comparaison des solutions VPN
- Matériels et logiciels
- Critères de choix

10. Mise en œuvre d'un projet VPN en entreprise

- Étude du contexte
- Déploiement
- Tests
- Exploitation et maintenance

11. Bibliographie et index