

Sommaire

Partie 1 – Concepts fondamentaux des VPN

1. Introduction aux réseaux privés virtuels
2. Besoins de sécurisation des communications
3. Services de sécurité : confidentialité, intégrité, authentification
4. Architecture générale d'un VPN

Partie 2 – Protocoles et technologies

5. Cryptographie appliquée aux VPN
6. Chiffrement symétrique et asymétrique
7. Certificats numériques et PKI
8. Protocoles d'authentification
9. Gestion des clés

Partie 3 – VPN IPSec

10. Architecture IPSec
11. Protocoles AH et ESP
12. IKE et négociation des associations de sécurité
13. VPN site-à-site avec IPSec
14. VPN nomade avec IPSec

Partie 4 – VPN SSL

15. Principes des VPN SSL
16. Accès distant sécurisé
17. Portails SSL
18. Authentification et contrôle d'accès

Partie 5 – VPN PPTP et L2TP

19. Présentation de PPTP
20. Présentation de L2TP
21. Comparaison des solutions VPN
22. Cas d'utilisation pratiques

Partie 6 – Mise en œuvre sous différents systèmes

23. Configuration sous Windows
24. Configuration sous Linux
25. Configuration sous FreeBSD
26. Interconnexion de réseaux hétérogènes

Partie 7 – Équipements et solutions professionnelles

27. Routeurs et pare-feu Cisco
28. Boîtiers VPN dédiés

- 29. Gestion des certificats
- 30. Mise en production d'un VPN d'entreprise

Partie 8 – VPN et IPv6

- 31. Introduction à IPv6
- 32. Déploiement de VPN en environnement IPv6
- 33. Compatibilité IPv4 / IPv6

Partie 9 – Administration et maintenance

- 34. Supervision des VPN
- 35. Journalisation et audit
- 36. Diagnostic des pannes
- 37. Résolution des problèmes courants
- 38. Optimisation des performances

Partie 10 – Études de cas

- 39. VPN site à site
- 40. VPN poste à site
- 41. VPN poste à poste
- 42. Scénarios d'entreprise et tests de validation

Annexes

- Rappels TCP/IP
- Commandes de configuration
- Glossaire
- Bibliographie
- Index.