

Sumário

Dedicatória	5
Agradecimentos	6
Sobre o autor	7
Depoimentos	13
Prefácio	15
Objetivos do Livro	17

Parte I – Introdução 19

1 Fundamentos da Rede Privada Virtual.....	21
Introdução à VPN	21
Riscos protegidos pela VPN	26
Privacidade	27
Integridade	28
Autenticidade	28
Não-repúdio	28
Facilidade	29
Conceitos necessários.....	29
Criptografia	30
Padronização e interoperabilidade	37
Firewall	39
Appliance	44
O que a VPN não protege?	44
Custos x benefícios	48
Por onde começar?.....	49
2 Revisão de conceitos da infra-estrutura Internet	51
Endereçamento e IPv4.....	51
IPv6.....	54
DHCP e DNS	55

Parte II – Tecnologia necessária 57

3 Encapsulamento e protocolos para VPN	59
Introdução	59
PPP (Point-to-Point Protocol)	61
PPTP (Point-to-Point Tunneling Protocol)	63
L2F (Layer Two Forwarding Protocol)	66

L2TP (Layer Two Tunneling Protocol)	67
IPSec	68
MPLS	70
SecureShell (SSH)	73
4 IPSec	75
Introdução	75
Protocolos do IPSec	76
Authentication Header	76
Encapsulation Security Payload	79
Associação de Segurança	81
Banco de dados de Segurança	83
Gerenciamento de Chaves	84
Internet Key Exchange	84
Conclusão	88
5 Autenticação	89
Introdução	89
Two-Party Authentication	90
Senha (Password)	91
Challenge/Response	92
One-Time Password	93
One-Time Password por Tokens	93
Smartcards	94
Biometria	95
Autenticação em Protocolo Ponto-a-Ponto (PPP)	98
TACACS	101
RADIUS	102
Session Key (S/KEY) e OTP	104
Trusted Third-Party Authentication	104
Kerberos	104
X.509 Public Key Infrastructure (PKI)	107
6 Public Key Infrastructure (PKI)	109
Introdução	109
Certificação e Autoridade Certificadora	113
Protocolos no ambiente PKI	115
Validação	117
Revogação de Certificados	117

Mercado de PKI	118
Infra-estrutura de Chave Pública Brasil (ICP – Brasil)	118
CA Autônoma	121
Utilização de PKI em VPN	121
Autenticação	122
Gerência de Chaves	124
Controle de Acesso	124
7 DNS e NAT	125
Split DNS	125
NAT e VPN	126
Static NAT	127
NAT Hide	127
NAPT	128
Dynamic NAT	130
Considerações	131
8 Usando Plataformas de Mercado	135
Introdução	135
Linux	135
FreeS/WAN	136
VTun	143
SSH	143
Windows	148
Autenticação e criptografia de dados em conexões VPN no Windows	148
Criptografia de dados	151
IPSec	152
Requisitos de criptografia do Windows 2000	156
SNMP	158
Gateways de segurança	158
Serviços DHCP, DNS e WINS	158
Associações de segurança	159
Snap-in	165
Microsoft Management Console (MMC)	165
Configurando o monitor IPSec	167
Ambientes Híbridos	170
Gateway VPN integrado com Firewall	171
Gateway VPN em frente ao Firewall	172
Gateway VPN atrás do Firewall	173
Gateway VPN em paralelo ao Firewall	174
Gateway VPN numa interface do Firewall	176

Parte III – Gerência de VPNs	179
9 Administração e Gerência de VPNs	181
Custos dos Componentes	181
Equipe	184
Treinamento	184
Equipamentos e Softwares	185
Riscos Inerentes	185
Ameaças x Vulnerabilidade	185
O perfil do hacker	186
Hackers x crackers	186
Script Kiddies	186
Funcionários insatisfeitos e ex-funcionários	186
Anatomia de um ataque de hacker	187
Tipos de ataques	187
Política de Segurança	190
Vulnerabilidade em servidores de mensagem instantânea	192
Tecnologias de segurança de redes	192
Gerência Interna x Gerência Terceirizada	195
Gerência Centralizada de VPNs	199
Regras de negócio	200
Utilizando o modelo	205
Violação de Nível de Serviço Acordado	206
Considerações finais e tendências de mercado	208
Parte IV – Estudos de Casos	211
10 Estudo de Casos	213
VPN em Empresa de Pequeno Porte	213
Case 01 – Solução In House	213
Case 02 – Solução Outosource	214
VPN em Empresa de Grande Porte	215
Case 01 – Solução baseada em circuitos virtuais	215
Case 02 – Solução baseada em segmentação de tráfego	216
Case 03 – Solução baseada em IPSec	218
VPN entre filiais com mesmo endereçamento IP	221
VPN com Usuários Remotos	222
Como ampliar a segurança da VPN para usuários remotos	225
A Referências	227
Índice remissivo	231