

A photograph of a man in a dark suit and glasses sitting at a desk, working on a laptop. The office is dimly lit, with a warm, orange glow from the desk lamp and the laptop screen. Another person is visible in the background, also working.

SECURITY

IPSec VPN Design

The definitive design and deployment guide
for secure virtual private networks

Contents

	Introduction	xvi
Chapter 1	Introduction to VPNs	3
	Motivations for Deploying a VPN	3
	VPN Technologies	5
	Layer 2 VPNs	6
	Layer 3 VPNs	6
	GRE Tunnels	6
	MPLS VPNs	6
	IPSec VPNs	7
	Remote Access VPNs	8
	Summary	9
Chapter 2	IPSec Overview	11
	Encryption Terminology	11
	Symmetric Algorithms	12
	Asymmetric Algorithms	13
	Digital Signatures	14
	IPSec Security Protocols	15
	IPSec Transport Mode	16
	IPSec Tunnel Mode	17
	Encapsulating Security Header (ESP)	18
	Authentication Header (AH)	19
	Key Management and Security Associations	21
	The Diffie-Hellman Key Exchange	21
	Security Associations and IKE Operation	23
	IKE Phase 1 Operation	25
	Main Mode	26
	Aggressive Mode	27
	Authentication Methods	28
	IKE Phase 2 Operation	30
	Quick Mode	30
	IPSec Packet Processing	32
	Security Policy Database	32
	Security Association Database (SADB)	33
	Cisco IOS IPSec Packet Processing	34
	Summary	39
Chapter 3	Enhanced IPSec Features	41
	IKE Keepalives	41
	Dead Peer Detection	43
	Idle Timeout	47

Reverse Route Injection	50
RRI and HSRP	53
Stateful Failover	56
SADB Transfer	57
SADB Synchronization	57
IPSec and Fragmentation	65
IPSec and PMTUD	66
Look Ahead Fragmentation	69
GRE and IPSec	70
IPSec and NAT	76
Effect of NAT on AH	76
Effect of NAT on ESP	76
Effect of NAT on IKE	77
IPSec and NAT Solutions	77
NAT Traversal (NAT-T)	77
IPSec Pass-through	83
IKE Passing Through PAT	83
ESP Passing Through PAT	83
Restricted ESP Through PAT Mode	84
Summary	87

Chapter 4	IPSec Authentication and Authorization Models	89
	Extended Authentication (XAUTH) and Mode Configuration (MODE-CFG)	89
	Mode-Configuration (MODECFG)	94
	Easy VPN (EzVPN)	95
	EzVPN Client Mode	96
	Network Extension Mode	99
	Digital Certificates for IPSec VPNs	103
	Digital Certificates	103
	Certificate Authority—Enrollment	104
	Certificate Revocation	105
	Summary	107

Chapter 5	IPSec VPN Architectures	109
	IPSec VPN Connection Models	109
	IPSec Model	110
	The GRE Model	111
	The Remote Access Client Model	112
	IPSec Connection Model Summary	112
	Hub-and-Spoke Architecture	114
	Using the IPSec Model	115
	Transit Spoke-to-Spoke Connectivity Using IPSec	120

Internet Connectivity	126
Scalability Using the IPSec Connection Model	127
GRE Model	128
Transit Site-to-Site Connectivity	140
Transit Site-to-Site Connectivity with Internet Access	141
Scalability of GRE Hub-and-Spoke Models	143
Remote Access Client Connection Model	144
Easy VPN (EzVPN) Client Mode	145
EzVPN Network Extension Mode	151
Scalability of Client Connectivity Models	155
Full-Mesh Architectures	156
Native IPSec Connectivity Model	156
GRE Model	165
Summary	170

Chapter 6 Designing Fault-Tolerant IPSec VPNs 173

Link Fault Tolerance	173
Backbone Network Fault Tolerance	174
Access Link Fault Tolerance	175
Multiple IKE Identities	176
Multiple IKE Identities Associated with Dial Backup	182
Single IKE Identity	183
Single IKE Identity Using Multi-link PPP on the Access Links	188
Access Link Fault Tolerance Summary	189
IPSec Peer Redundancy	189
Simple Peer Redundancy Model	189
Virtual IPSec Peer Redundancy Using HSRP	194
IPSec Stateful Failover	196
Peer Redundancy Using GRE	200
Virtual IPSec Peer Redundancy Using SLB	204
Server Load Balancing Concepts	205
IPSec Peer Redundancy Using SLB	205
Cisco VPN 3000 Clustering for Peer Redundancy	210
Peer Redundancy Summary	212
Intra-Chassis IPSec VPN Services Redundancy	212
Stateless IPSec Redundancy	213
Stateful IPSec Redundancy	213
Summary	214

Chapter 7 Auto-Configuration Architectures for Site-to-Site IPSec VPNs 217

- IPSec Tunnel Endpoint Discovery 217
 - Principles of TED 218
 - Limitations with TED 220
 - TED Configuration and State 221
 - TED Fault Tolerance 225
- Dynamic Multipoint VPN 227
 - Multipoint GRE Interfaces 229
 - Next Hop Resolution Protocol 232
 - Dynamic IPSec Proxy Instantiation 236
 - Establishing a Dynamic Multipoint VPN 237
 - DMVPN Architectural Redundancy 248
 - DMVPN Model Summary 254
- Summary 255

Chapter 8 IPSec and Application Interoperability 257

- QoS-Enabled IPSec VPNs 258
 - Overview of IP QoS Mechanisms 258
 - IPSec Implications for Classification 259
 - QoS Applied to IPSec Transport Mode 260
 - QoS Applied to IPSec Tunnel Mode 261
 - IPSec Transport Mode - QoS Attribute Preservation of GRE Tunnels 261
 - Transitive QoS Applied to IPSec 264
 - Internal Preservation of QoS Attributes 264
 - IPSec Implications on QoS Policies 266
 - IPSec Implications of Packet Size Distribution on Queue Structures 266
 - IPSec Implications of Packet Size on Queue Bandwidth Assignments 266
- VoIP Application Requirements for IPSec VPN Networks 267
 - Delay Implications 267
 - Jitter Implications 269
 - Loss Implications 270
 - Mitigating Anti-replay Loss in Combined Voice/Data Flows 270
 - Mitigating Anti-replay Loss in Separate Voice/Data Flows 270
 - Engineering Best Practices for Voice and IPSec 271
- IPSec VPN Architectural Considerations for VoIP 271
 - Decoupled VoIP and Data Architectures 272
 - VoIP over IPSec Remote Access 274
 - VoIP over IPSec-Protected GRE Architectures 275
 - VoIP Hub-and-Spoke Architecture 277
 - VoIP over DMVPN Architecture 278
 - VoIP Bearer Path Optimization with DMVPN 279
 - VoIP Bearer Path Synchronization with DMVPN 279
 - VoIP Traffic Engineering Summary 279

Multicast over IPSec VPNs	280
Multicast over IPSec-protected GRE	280
Multicast on Full-Mesh Point-to-Point GRE/IPSec Tunnels	282
DMVPN and Multicast	285
Multicast Group Security	287
Group Security Key Management	287
Group Security Association	289
Multicast Group Security Summary	291
Multicast Encryption Summary	291
Summary	291

Chapter 9 Network-Based IPSec VPNs 293

Fundamentals of Network-Based VPNs	293
The Network-Based IPSec Solution: IOS Features	296
The Virtual Routing and Forwarding Table	296
Crypto Keyrings	297
ISAKMP Profiles	297
Operation of Network-Based IPSec VPNs	299
A Single IP Address on the PE	300
Front-Door and Inside VRF	300
Configuration and Packet Flow	301
Generic MPLS VPN Configuration on the PE	305
Mapping an IPSec Tunnel from a Site into IVRF at the PE	306
Mapping an IPSec Tunnel from a Telecommuter into an IVRF at the PE	315
Termination of IPSec on a Unique IP Address Per VRF	321
Network-Based VPN Deployment Scenarios	324
IPSec to MPLS VPN over GRE	324
DMVPN and VRF	327
IPSec to L2 VPNs	330
PE-PE Encryption	334
Summary	339