Index

Numerics

3DES (triple data encryption standard), 21

A–B

aggressive mode negotiation, 89–90
AH (Authentication Headers), 6, 57–58
alternatives to IPsec VPN HA,
 stateful, 257–260
 stateless, 242
  HSRP, 244–245
  RRI, 245
applying crypto maps in SOHO environments, 432–446
asymmetric cryptography, 392
asymmetric key encryption, 36–39, 46
 impact on CPU processing, 404
asymmetric routing as cause of broken VPN tunnels, 220
authentication, 44
 of public key certificates, 402
authentication errors (IKE), troubleshooting, 146–165
authentication services (IKE)
 preshared keys, 83–85
 RSA encryption, 85
 RSA signatures, 86–87
 X.509 certificates, 86–87

BGP (Border Gateway Protocol), crypto path availability, 219
business drivers for VPNs, 29–30
 remote access VPNs, 30
 site-to-site VPNs, 30–31

C

CA hierarchy configuration, case study, 412–414
CAs (Certificate Authorities), 393, 397
 enrollment process, 395
 RA interoperability, configuring, 410–412
case studies, PKI
 CA hierarchy, 412–414
 configuring CA/RA interoperability, 410–412
 cryptographic endpoint integration, 407–409
CBC (cipher block chaining), 55
CBWFQ (class-based weighted fair queuing), impact of IPsec on, 181–182
CE (customer edge) routers, 18–20
characteristics of effective VPNs, 6–7
cipher text, 6
ciphers, 36
Cisco IPSec VPN 3000 series concentrators, 225
Cisco Security Wheel, 31
Cisco VPN 3000 series concentrators, clustering, 227–230
clustered spoke VPN design, 130
clustered VPN concentrator designs, 137–138
commands, redistribute static, 245, 269
comparing In-Path and Out-of-Path encryption, 361, 368–369
compulsory tunnels, 13
concentrator clustering, 225–230
configuring
 CA hierarchy, case study, 412–414
 CA/RA interoperability, case study, 410–412
 crypto maps, 66–68
 dynamic crypto maps, 425–430

geographic HA
DMVPNs, 287–294
IPsec+GRE, 279–280, 283–287
RRI with multiple IPsec peers, 267–278
ISAKMP, 94–95
RAVPN HA
DNS-based load balancing, 343–345
using multiple IPsec peers, 345, 348–355
with HSRP, 327–333
with VCA, 333–342
with VRRP, 315–326
site-to-site VPNs, 108–110
TED, 432
control messages, 16
creating
message digests, 42–44
transforms, 63–66
CRLs, 396
scalability, 404
crypto ACLs, 169
mismatches, troubleshooting, 169–170
crypto engines, 50
crypto maps, 236
configuring, 66–68
multiple peering statements, tunnel termination HA, 213
crypto path availability, 215–218
cryptographic endpoints, 397
cryptographic key derivation (SSL VPNs), 23–24
CSM (Content Switch Module), external load balancing, 231–232

D

data authentication, 44
data confidentiality, 6
in VPDN deployments, 10
data integrity, 7, 42–44
decryption, 6
deployment models
hub-and-spoke VPNs, 128–130
clustered spoke design, 130
redundant clustered spoke design, 131
IPsec+GRE, 121–122
sample configurations, 123–125
tunnel establishment, verifying, 126–127
RAVPNs, 132
clients, 132
clustered VPN concentrator designs, 137–138
standalone VPN concentrator designs, 133–136
site-to-site VPNs, 107
configuring, 108–110
over routed domain, 117–120
verifying configuration, 111–117
DES (data encryption standard), 21
Diffie, Whitfield, 392
Diffie-Hellman
key exchange, 51
secret key generation, 79–80, 82–83
DiffServ, impact of IPsec on, 181–182
digital signatures, generating, 44–46
distribute lists, 199
DMVPNs (Dynamic Multipoint VPNs), 27, 130
geographic HA, configuring, 287–294
DNS server load balancing, 225–227
in RAVPNs with geographic HA, 343–345

DPD (Dead Peer Detection), 92–94
peer availability, 217
dual-DMZ tunnel termination, 372–373, 377
dynamic crypto maps, 418
and RRI, 420
applying in SOHO environments, 432–446
configuring, 425–430
impact on ISAKMP/IKE, 418–419
impact on VPN behavior, 418–424
routing considerations, 419–420
security considerations, 421
key administration and scalability, 421–424
unrestricted peering and traffic flows, 424
TED, 430–432
verifying, 425–430

E–F–G

eliminating single points of failure for site-to-site VPNs, 209
enabling TED, 432
encryption, 6
asymmetric, 36–39
In-Path versus Out-of-Path, 361, 368–369
Out-of-Path, 370
symmetric, 21, 39–41
enrollment process, 395
for RSA signatures, 398, 402
for X.509 certficates, 398, 402
ESP (Encapsulating Standard Protocol), 6
confidentiality services, 55–56
data integrity and authentication services, 56–57
extensions for IKE
mode config, 96–98
xauth, 98–99
external load balancers, 230–232

failover
stateful HA failover process, 261–263
stateless HA failover process, 246–257
firewalled VPN environments
ICMP unreachables, troubleshooting, 174
troubleshooting, 171–174
tunnel termination, 370–378
floating static routes, 238
flow-based QoS, impact of IPsec on, 180–181
format of L2F packets, 10
forwarding public key certificates, 403
fragmentation
on Cisco IOS VPN endpoints, 189–193
PMTUD, 184–188
preventing
with IPsec Prefragmentation, 193–196
with manual MTU adjustment, 196
Virtual Fragmentation Reassembly, 174

generating
Diffie-Hellman secret keys, 79–83
digital signatures, 44–46
geographic HA, 267
DMVPNs, 287–294
IPsec+GRE, 279–280, 283–287
RRI with multiple IPsec peers, 267–277
goals of VPN implementation, 6–7
GRE-offload, 306, 379–383. ***See also* IPsec+GRE model**
with cleartext firewall paths, 385
with dynamic crypto maps, 383–384
with high-speed tunnel termination, 385
with IKE x-Auth, 384–385

H

HA (High Availability)
geographic HA, 267
DMVPNs, 287–294
IPsec+GRe, 279–287
RRI with multiple IPsec peers, 267–277
in RAVPNs, 314
concentrator redundancy with multiple peers, 345, 348–355
DNS-based load balancing, 343–345
HSRP, 327–333

VCA, 333–342
VRRP, 315, 320, 323–326
load-balanced designs
concentrator clustering, 227–230
DNS server load balancing, 225–227
external load balancers, 230–232
load sharing with peer statements, 222–224
routing, 224
peer availability, 216
on-demand DPD, 217
SSO, 259
stateful HA
alternatives to, 257–260
failover process, 261–263
stateless HA
alternatives to, 242–245
failover process, 246–257
tunnel termination redundancy, 210
on HSRP/VRRP virtual interfaces, 211
using RP-based IPsec HA, 214–215
with multiple peer statements, 212–214
handshake process (SSL VPNs), 22–24
hardware-based VPN clients, 133
hashes, 42
Hellman, Martin, 392
HMAC (hashed message authentication codes), 24, 42
home gateways, 10
HSRP (Hot Standby Routing Protocol), 244
RAVPN concentrator HA, 327–333
timers, tuning, 255
HSRP/VRRP virtual interfaces, tunnel termination point HA, 211
hub-and-spoke IPsec model, 128–130
clustered spoke design, 130–131
site-to-site VPNs, 26

I

ICMP messages
rate-limiting, 187
unreachables, troubleshooting in firewalled VPN environments, 174
identifying IPsec transform set mismatches, 168
IKE, 78
authentication errors, troubleshooting, 146–165
authentication services
pre-shared keys, 83–85
RSA encryption, 85
RSA signatures, 86–87
X.509 certificates, 86–87
Diffie-Hellman secret key generation, 79–83
keepalives, removing stale SAs from SADB, 217
key mismatches, troubleshooting, 150–151
mode config extension, 96–98
Phase I negotiation
aggressive mode negotiation, 89–90
main mode negotiation, 88–89
Phase II negotiation
DPD, 92
IKE keepalives, 92–94
PFS, 91–92
quick mode negotiation, 90
SA negotiation and maintenance, 79
SA proposal mismatches, troubleshooting, 142–146
x-auth, 421
xauth extension, 98–99
impact of vendor interoperability on path availability, 301–305
In-Path encryption, 368–369
integrity, 7
IntServ, impact of IPsec on, 183
invalid SPI recovery, 308–309
IPComp, 58–59
IPPCP (IP Payload Compression Protocol), 58–59
IPsec Prefragmentation, 193–196
IPsec+GRE model, 121–122, 190
geographic HA, configuring, 279–280, 283–287
sample configurations, 123–125
tunnel establishment, verifying, 126–127
ISAKMP, 78
configuring, 94–95
ITU-T X.509v3–compliant certificates, 396
IV (Initialization Vector), 57

K–L

keepalives (IKE), 92–94
key management
- need for, 77
- PKI, 391–393
  - *CAs, 397*
  - *CRLs, 396*
  - *cryptographic endpoints, 397*
  - *public key certificates, 394–395*
  - *registration authorities, 395–396*

L2F (Layer 2 Forwarding), home gateways, 10
L2TP (Layer 2 Tunneling Protocol)
- control messages, 16
- payload packets, 16
- tunnel negotiation process, 17

LAC (L2TP Access Concentrator), 16
lack of RP support, effect on IPS HA design, 302–304
Layer 2 Forwarding Protocol, 10
- packet format, 10
- tunnel establishment process, 11–12

life cycle of public key certificates, 397
- RSA signatures, 397, 401
- X.509 certificates, 398, 401

limitations of vendor HA interoperability
- inability to specify multiple peers, 297–300
- lack of peer availability mechanisms, 300–301

LLQ (low-latency queuing), impact of IPsec on, 181–182
LNS (L2TP Network Server), 16
load balanced designs
- concentrator clustering, 227–230
- DNS server load balancing, 225–227
  - *configuring in RAVPNs with geographic HA, 343–345*
- external load balancers, 230–232
- load sharing with peer statements, 222–224
- routing, 224

load sharing with peer statements, 222–224
local IPsec HA, 235
Lookahead Fragmentation, 194
LZS (Lempel Ziv Stac), 58–59

M–N–O

main mode negotiation, 88–89
manual keying, 68–77
manual MTU adjustment, preventing fragmentation, 196
MD5 (Message Digest 5), 43
message digests, creating and verifying, 42–44
messages (ICMP), rate-limiting, 187
mismatched crypto ACLs, troubleshooting, 169–170
mismatched IKE SA proposals, troubleshooting, 142–146, 165–168
mismatched transform sets, identifying, 168
mode config extension (IKE), 96–98
MODP (prime modulus), 51
MP-BGP (Multiprotocol Border Gateway Protocol), 18
MPLS VPNs, 18–20
- VRFs, 19

MPPE (Microsoft Point-to-Point Encryption), 13
MTUs (maximum transmission units), manual adjustment, 196

NAS (Network Access Server), 10
NAT (Network Address Translation)
- SPI-based, troubleshooting, 179–180
- troubleshooting, 174–178

NAT Detect, 179
NAT-on-a-stick, IPsec VPN tunnel termination, 362–368
NAT-T, troubleshooting, 178–179
NHRP (next hop routing protocol), 27
nonces, 85

obtaining public key certificates, 403
OCSP (Online Certificate Status Protocol), 405
“on-a-stick” designs, 386
- NAT-on-a-stick, 362–368
- router-on-a-stick, 359–362

on-demand DPD, 217
OSI reference model, 9
Out-of-Path encryption, 368–370

P

P (provider) routers, 18
packets, L2F, 10
path availability, 218, 284
 and vendor HA availability, 301–305
path symmetry, managing, 219
payload packets, 16
PE (provider edge) routers, 18
peer availability, 215–216, 297
 on-demand DPD, 217
peer mismatches (IKE), troubleshooting, 150–151
periodic DPD, 218
PFS (perfect forward secrecy), 69, 91–92
PKI (Public Key Infrastructure), 391–393
 CAs, 397
 case studies
  CA hierarchy, 412–414
  configuring CA/RA interoperability, 410–412
  cryptographic endpoint integration, 407–409
 CRLs, 396
 cryptographic endpoints, 397
 enrollment process, 163
 public key certificates, 394–395
 registration authorities, 395–396
PMTUD (Path MTU Discovery), 184–188
PPTP (Point-to-Point Tunneling Protocol), 12
 compulsory tunnels, 13
 data structure, 14
 tunnel negotiation process, 14
 voluntary tunnels, 13
preshared keys, 83–85
preventing fragmentation
 with IPsec Prefragmentation, 193–196
 with manual MTU adjustment, 196
proxies, 169
PSKs (preshared keys), troubleshooting mismatched peer addresses, 149–150
public key certificates, 394–395
 authentication, 402
 forwarding, 403
 life cycle of, 397
 obtaining, 403
 registration process, 402
 RSA signatures, life cycle of, 397, 401
 signing, 403
 X.509 certificates, life cycle of, 398, 401
public key cryptography, 392
public key encryption, 45–46
 Diffie-Hellman key exchange, 51
 RSA, 48–50
 RSA signatures, 50

Q–R

QoS (quality of service), impact of IPsec on
 DiffServ, 181–182
 flow-based, 180–181
 IntServ, 183
quick mode negotiation, 90

RAs (registration authorities), 395–396
 CA interoperability, configuring, 410–412
rate-limiting ICMP messages, 187
RAVPNs (remote-access VPNs)
 deployment model, 132
  clients, 132
  clustered VPN concentrator designs, 137–138
  standalone VPN concentrator designs, 133–136
 HA, 314
  DNS-based load balancing, 343–345
  geographic HA, DNS-based load balancing, 345, 348–355
  HSRP, 327–333
  VCA, 333–342
  VRRP, 315, 320, 323–326
reconvergence of routing protocols, impact on IPsec reconvergence, 238–240
recursive routing
 effect on IPsec VPNs, 197–200
 symptoms of, 197–198
redistribute static command, 245, 269
redistribution
 distribute lists, 199
 of VPN routes, 253
redundant clustered spoke VPN design, 131
registration authorities, 395–396
 CA interoperability, configuring, 410–412

registration process for public key certificates, 402
remote-access VPNs
  business drivers, 30
  SSL, 28
removing stale SAs from SADB, 217
round-robin approach to DNS resolution, 227
route descriptors, 20
router-on-a-stick, IPsec VPN tunnel termination, 359–362
routing, 224
RP-based IPsec HA, 214–215
RRI (Reverse Route Injection), 245
  and dynamic crypto maps, 420
  impact on vendor interoperability, 304–305
RSA encryption, 48–50, 85
  IKE authentication errors, troubleshooting, 151–158
  signatures, 23, 50, 86–87, 396
    enrollment process, 398, 402
    IKE authentication errors, troubleshooting, 158–165
    life cycle of, 397, 401
RSVP (Resource Reservation Protocol), impact of IPsec on, 183

S

sample IPsec+GRE model configurations, 123–125
SAs (security associations)
  IPsec tunnel security parameters, 59, 62–63
  need for, 77
  proposal mismatches, troubleshooting, 165–168
  security parameters, manual keying, 68–77
  transport mode, 52
  tunnel mode, 54
scalability of CRLs, 404
SCEP (Simple Certificate Enrollment Protocol), 402
SCTP (Stream Control Transmission Protocol), 260
security wheel, 32
sender non-repudiation, 7
serialization delay, 196
session authentication (SSL VPNs), 24
SHA (Secure Hash Algorithm), 43
shared secret keys, 39
signing public key certificates, 403
single points of failure for site-to-site VPNs, 208–209
site-to-site IPsec VPNs, 25, 107
  business drivers, 30–31
  configuration, verifying, 111–117
  configuring, 108–110
  hub-and-spoke networks, 26
  over routed domains, 117, 120
  single points of failure, eliminating, 208–209
site-to-site IPsec+GRE model. ***See*** **IPsec+GRE model**
software-based VPN clients, 132
SOHO deployments, applying dynamic crypto maps case study, 432–446
SPI (security parameter index), 56
SPI-based NAT, troubleshooting, 179–180
SSL VPNs, 21
  cryptographic key derivation, 23–24
  handshake process, 22–24
  HMAC, 24
  RAVPN architectures, 28
  session authentication, 24
  transport layer security, 25
  tunnel establishment process, 22
SSO (stateful switchover), 259
stale SAs
  impact on IPsec reconvergence, 240
  removing from SADB, 217
standalone VPN concentrator designs, 133–137
stateful IPSec HA, 212
  alternatives to, 257–260
  failover process, 261–263
stateless IPsec HA, 212
  alternatives to, 242
    HSRP, 244–245
    RRI, 245
  failover process, 246–257
  goals of, 243–244
static crypto maps, 417–418
symmetric encryption, 21, 39–41
  shared secret keys, Diffie-Hellman secret key generation, 79–83
symptoms of recursive routing, 197–198

T

TED (Tunnel Endpoint Discovery), 430–432
timers (HSRP), tuning, 255
topologies. *See* VPN topologies
transform sets, identifying mismatches, 168
transforms
AH, 57–58
creating, 63–66
ESP
confidentiality services, 55–56
data integrity and authentication services, 56–57
IPComp, 58–59
LZS, 58–59
transport layer VPNs, SSL VPNs, 21
cryptographic key derivation, 23–24
handshake process, 22–24
HMAC, 24
session authentication, 24
transport layer security, 25
tunnel establishment process, 22
transport mode, 52, 55
troubleshooting
IKE
authentication errors, 146–165
peer mismatches, 150–151
SA proposal mismatches, 142–146, 165–168
mismatched crypto ACLs, 169–170
NAT issues in IPsec VPN designs, 174–178
SPI-based NAT, 179–180
NAT-T issues in IPsec VPN designs, 178–179
VPNs in firewalled environments, 171–174
TTI (Trusted Transitive Introduction), 434
tunnel mode, 54–55
tunnel termination. *See also* tunnels
dual-DMZ firewall design, 372–373, 377
firewalled, 370–378
GRE-offload, 379–383
with cleartext firewall paths, 385
with dynamic crypto maps, 383–384
with high-speed tunnel termination, 385
with IKE x-Auth, 384–385
“on a stick” termination
NAT-on-a-stick, 362–368
router-on-a-stick, 359–362
termination redundancy, 210
on HSRP/VRRP virtual interfaces, 211
using RP-based IPsec HA, 214–215
with multiple peer statements, 212–214
tunnels
L2F establishment process, 11–12
load-balanced designs
concentrator clustering, 227–230
DNS, 225–227
external load balancers, 230–232
load sharing with peer statements, 222–224
routing, 224
negotiation process, 17
PPTP
compulsory, 13
tunnel negotiation process, 14
voluntary, 13
SA security parameters, 59, 62–63

V

“validity period” field (ITU-T X.509v3-compliant certificates), 396
VCA (Virtual Cluster Agent) protocol, 228
RAVPN concentrator HA, 333–342
vendor HA interoperability
design considerations, 306
interoperability with stateful IPsec HA, 309–311
invalid security parameter index recovery, 308–309
Phase1/2 SA lifetime expiry, 307
SADB management, 307–308
impact on path availability, 301–305
limitations of
inability to specify multiple peers, 297–300
lack of peer availability mechanisms, 300–301
verifying
dynamic crypto maps, 425–430
IPsec+GRE model, tunnel establishment, 126–127
message digests, 42–44
site-to-site VPN configuration, 111–117
TED, 432
Virtual Fragmentation Reassembly, 174
voluntary tunnels, 13

VPDNs (virtual private dialup networks), 10
L2TP, 16
control messages, 16
payload packets, 16
tunnel negotiation process, 17
Layer 2 Forwarding Protocol, 10
packet format, 10
tunnel establishment process, 11–12
PPTP, 12
compulsory tunnels, 13
data structure, 14
tunnel negotiation process, 14
voluntary tunnels, 13
VPN clients, 28
VPN concentrators, 28
VPN routes, redistribution, 253
VPN topologies
hub-and-spoke, 128–130
clustered spoke design, 130
redundant clustered spoke design, 131
IPsec+GRE model, 121–122
sample configurations, 123–125
tunnel establishment, verifying, 126–127
RAVPNs, 132
clients, 132
clustered VPN concentrator designs, 137–138
standalone VPN concentrator designs, 133–136
site-to-site, 107
configuring, 108–110
over routed domain, 117, 120
verifying configuration, 111–117
VPN tunnel termination
dual-DMZ firewall design, 372–373, 377
firewalled, 370–378
GRE-offload, 379–383
with cleartext firewall paths, 385
with dynamic crypto maps, 383–384
with high-speed tunnel termination, 385
with IKE x-Auth, 384–385
"on a stick" termination
NAT-on-a-stick, 362–368
router-on-a-stick, 359–362
termination redundancy, 210
on HSRP/VRRP virtual interfaces, 211
using RP-based IPsec HA, 214–215
with multiple peer statements, 212–214
VPN3000 Clustering, 227–230
VRFs (VPN Routing and Forwarding Instances), 19
VRRP, RAVPN concentrator HA, 315, 320, 323–326

W-X-Y-Z

wildcard preshared keys, 83

X.509 certificates, 86–87
enrollment process, 398, 402
life cycle of, 398, 401
x-auth, 421
xauth extension (IKE), 98–99