



Numerics

3DES algorithm, 15

A

access attacks, 5
 access lists, creating, 345
 Access Rights window (Cisco VPN 3000 Concentrator), 344–346
 Acme Limited case study, 387
 central site infrastructure, 389–390
 remote agent infrastructure, 391
 remote-access design considerations, 388–389
 VPN Concentrator configuration, 391–406
 adding custom CPP policies, 199–206
 Administer Sessions screen (Cisco VPN 3000 Concentrator), 339–340
 Administration index screen (Cisco VPN 3000 Concentrator)
 Access Rights window, 344–346
 File Management window, 347–350
 Monitoring Refresh window, 344
 Ping window, 344
 Reboot Status window, 344
 Software Update window, 340, 343
 System Reboot window, 343
 AES (Advanced Encryption Standard) algorithm, 15
 AH (Authentication Header), 26–29
 anti-replay protection, IPSec functionality, 26
 attacks, 4
 access, 5
 DoS, 5
 authentication
 certificate-based, 141–142
 interactive unit authentication, configuring on
 Cisco 3002 Hardware Client, 244–251
 user authentication, configuring on Cisco 3002
 Hardware Client, 252–255, 259
 AYT (Are You There), 189
 configuring, 190–194
 operation, 194

B

backup server, configuring
 on Cisco 3000 VPN Concentrator, 264
 on Hardware Client, 265
 on Software Client, 266
 bandwidth management, 352
 bandwidth aggregation, configuring, 361
 bandwidth policing, configuring, 353–356
 bandwidth reservation, configuring, 356–360
 statistics, monitoring, 361–362
 banner support, configuring on movianVPN, 441
 browser interface, Quick Configuration window, 93–103

C

CA-based LAN-to-LAN VPNs, troubleshooting
 initial failures, 381
 ongoing failures, 384
 CAs, 142
 configuring VPN 3000 Concentrator support
 file-based enrollment, 155–166
 group matching policy, configuring, 157–158
 VPN client enrollment, 173–174
 file enrollment, 174, 177–179
 network enrollment, 180–183
 case studies
 Acme Limited, 387
 central site infrastructure, 389–390
 remote agent infrastructure, 391
 remote-access design considerations, 388–389
 VPN Concentrator configuration, 391–406
 central site VPN concentrator connection, configuring on LAN-to-LAN VPNs, 301–311
 Certicom, 444
 certificate-based authentication, configuring on movianVPN, 438–439
 certificates
 connecting remote-access VPNs, 184–185
 CRLs, enabling, 167

- generating, 143, 145–146
 - installing, 148
 - PKCS#10, 144
 - renewing, 166
 - signature validation, 149
 - validity period, 151
 - VPN client enrollment, 173–174
 - file enrollment, 174, 177–179
 - network enrollment, 180–183
 - X.509, 147–148
- CIC (Cisco Info Center), 62
- Cisco 3002 Hardware Client, 209–210
- Client mode, 211
 - interactive unit authentication, configuring, 244–251
 - monitoring client user statistics, 259
 - Network Extension mode, 211
 - user authentication, configuring, 252–259
- Cisco AVVID architecture, 7
- business integrators, 10
 - clients, 8
 - intelligent network services, 9
 - Internet business solutions, 10
 - Internet middleware layer, 9–10
 - network platforms, 9
 - SAFE blueprint, 10
 - characteristics, 12
- Cisco Resource Manager Essentials, 63
- Cisco View, 63
- Cisco VPN 3000 Concentrator
- Administration index screen, 339
 - Access Rights window, 344–346
 - Administer Sessions window, 340
 - File Management window, 347–350
 - Monitoring Refresh window, 344
 - Ping window, 344
 - Reboot Status window, 344
 - Software Update window, 340, 343
 - System Reboot window, 343
 - dynamic routing, 72–73
 - OSPF, 77–84
 - RIP, 73–74, 77
 - firewall features
 - AYT, 190, 192–194
 - CPP, 196–197
 - stateful firewall, 195
 - LAN-to-LAN VPNs, configuring with digital certificates, 320–322
 - Monitoring index screen, 325
 - Dynamic Filters window, 327
 - Filterable Event Log window, 328–330
 - LED Status window, 332
 - memory Status window, 333
 - Routing Table window, 326
 - Sessions window, 334
 - Statistics window, 338
 - System Status window, 330–332
 - placement of, 58–59, 62
 - series models, 41–43
 - Cisco VPN 3005, 43
 - Cisco VPN 3015, 44–45
 - Cisco VPN 3020, 45
 - Cisco VPN 3030, 46
 - Cisco VPN 3060, 47–48
 - Cisco VPN 3080, 48–49
 - session statistics, monitoring, 292–294
 - static routing, 67–69
 - configuring, 69–72
 - tunnel default route, 69
- Cisco VPN 3002 Hardware Client
- auto-update feature
 - configuring, 234–238
 - monitoring, 239–240
 - configuring mode of operation, 230, 234
 - connecting to VPN 3000 Concentrator, 212–230
- Cisco VPN Monitor, 63
- Cisco Works, 63
- CLI configuration for VPN Concentrator, 57
- Client mode (Cisco 3002 Hardware Client), 211
- Client RRI, 274–275
- clusters, 266–267
 - configuring, 270–271
 - load balancing, connection process, 267
 - VCA, enabling between concentrators, 268–269
- columns, 43
- comparing
 - features of Cisco VPN 3000 Concentrator Series models, 41–43
 - Hardware and Software Clients, 56
- confidentiality
 - DH key exchange, 19

- encryption algorithms, 17
- IPSec services, 16–17
- key exchange, 18
- configuring
 - AYT, 190, 192–194
 - bandwidth management
 - bandwidth aggregation, 361
 - bandwidth policing, 353–356
 - bandwidth reservation, 356–360
 - Cisco VPN 3002 Hardware Client, 212–214
 - auto-update feature, 234–238
 - group and user information, 225–227, 230
 - identity and system information, 216
 - interactive unit authentication, 244–251
 - network information, 218–220, 223–224
 - quick configuration, 213
 - user authentication, 252–255, 259
 - VPN operation mode, 230, 234
 - clusters, 270–271
 - CPP, 197
 - IPSec backup server on Cisco 3000 VPN
 - Concentrator, 264
 - Hardware Client, 265
 - Software Client, 266
 - IPSec over TCP
 - Concentrator configuration, 290
 - VPN Software Client configuration, 291
 - IPSec over UDP, 287
 - concentrator configuration, 288
 - VPN Software Client configuration, 288
 - LAN-to-LAN VPNs
 - central site VPN Concentrator connection, 301–311
 - remote site VPN Concentrator connection, 312–313
 - movianVPN, 425
 - banner support, 441
 - certificate-based authentication, 438–439
 - DNS support, 437–438
 - external authentication, 439–440
 - gateway access, 426
 - IPSec, 433–434
 - NAT Traversal, 440–441
 - Perfect Forward Secrecy, 436–437
 - policies, 428–433, 442–443
 - split tunneling, 435–436
 - NAT-T
 - Concentrator, 289
 - VPN Software Client, 290
 - OSPF on VPN concentrator, 77–84
 - remote-access VPNs
 - groups, 107–126
 - IKE proposals, 104–106
 - with digital certificates, 139–146, 149–151
 - with preshared keys, 87–89
 - connecting browser interface, 92, 95–103
 - establishing management session, 90–92
 - RIP on VPN concentrator, 73–74, 77
 - static routing on VPN Concentrator, 69–72
 - VCA message transmissions between concentrators, 269
 - VPN 3000 Concentrators
 - for remote-access VPNs, 169, 171
 - file-based enrollment, 155–166
 - for CA support, 154
 - Windows Software Client, 128–135
- connecting
 - Cisco VPN Hardware client to VPN 3000 Concentrator, 212–234
 - remote-access VPNs with certificates, 184–185
- continuous security policies, 5–7
- CPP (Central Policy Protection), 190, 196
 - configuring, 197
 - custom policies, creating, 199–206
- creating
 - access lists, 345
 - custom CPP policies, 199–206
 - movianVPN policies, 428–432
- CRLs, 151
 - enabling, 167
- custom CPP policies, creating, 199–206

D

- data integrity, IPsec functionality, 20–21
- DES algorithm, 15
- DH (Diffie-Hellman), 15
 - key exchange, 19
- diagnostic tools for movianVPN, 441–442
- digital certificates
 - certificate generation, 143–146
 - certificate validation, 149–151
 - configuring remote-access VPNs, 139–143
 - PKI, 142–143
 - VPN client enrollment, 173–174
 - file enrollment, 174, 177–179
 - network enrollment, 180–183
 - X.509, 147–148
- digital signatures, 140
- displaying Software Client firewall status parameters, 199
- DMZs (demilitarized zones), VPN Concentrator placement, 61
- DNS support
 - configuring on movianVPN, 437–438
 - split DNS, 123, 126
- DoS attacks, 5
- DPD (dead peer detection) messages, 112
- dynamic filter statistics, monitoring on Cisco VPN 3000, 327
- dynamic routing on Cisco VPN 3000 Concentrator, 72–73
 - OSPF, 77–84
 - RIP, 73–74, 77

E

- enabling CRLs, 167
- encrypted nonces, 26
- encryption algorithms, 17
- ESP, 27–30
- event log statistics, monitoring on Cisco VPN 3000, 328–330
- external authentication, configuring on movianVPN, 439–440
- external threats, 4

F

- features of Cisco VPN 3000 Concentrator Series models, 41–43
 - Cisco VPN 3005, 43
 - Cisco VPN 3015, 44–45
 - Cisco VPN 3020, 45
 - Cisco VPN 3030, 46
 - Cisco VPN 3060, 47–48
 - Cisco VPN 3080, 48–49
- file enrollment, 174, 177–179
- File Management window (Cisco VPN 3000 Concentrator), 347–350
- file-based enrollment (CAs), 155–166
- firewall-based VPNs, 14
- firewalls
 - AYT
 - configuring, 190–194
 - operation, 194
 - CPP, creating custom policies, 200–206
 - VPN Concentrator placement, 60

G

- general statistics, monitoring on Cisco VPN 3000 Concentrator, 338
- groups, configuring for remote-access VPNs, 107–126
- group matching policy (CAs), configuring, 157–158

H

- Hardware Client, 55, 209–210
 - auto-update feature, configuring, 234–238
 - auto-update feature, monitoring, 239–240
 - Client mode, 211
 - comparing with Software Client, 56
 - connecting to VPN 3000 Concentrator, 212–234
 - interactive unit authentication, configuring, 243–251
 - IPsec backup server, 264
 - configuring, 265
 - load balancing, configuring, 272
 - monitoring client user statistics, 259
 - Network Extension mode, 211
 - user authentication, configuring, 252–255, 259
- HMAC algorithms, 22

identity certificates, renewing, 166

IKE proposals, configuring for remote-access VPNs, 104, 106

initial VPN failures, troubleshooting, 365

- on CA-based LAN-to-LAN VPNs, 381
- on LAN-to-LAN VPNs, 372–376, 381
- on remote-access VPNs, 368–371

installing

- certificates, 148
- root certificates, 159–162

integrators of Cisco AVVID partnerships, 10

intelligent network services, 9

interactive unit authentication, configuring on Cisco 3002 Hardware Client, 244–251

- accessing username password prompt, 245, 249–251

interface OSPF configuration, 81–84

internal threats, 4–5

IP address, configuring on 3002 Hardware Client, 218–224

IPSec, 15

- AH, 26, 28–29
- Backup Server
 - configuring on Hardware Client, 265
 - configuring on Software Client, 266
- configuring on movianVPN, 433–434
- ESP, 27, 29–30
- functions performed, 16
- functions provided
 - anti-replay protection, 26
 - confidentiality, 16–19
 - data integrity, 20–21
 - origin authentication, 23–26
- operation, 31
 - data transfer, 37
 - defining interesting traffic, 32
 - IKE phase 1, 33–34
 - IKE phase 2, 34–36
 - tunnel termination, 38
- over TCP
 - configuring, 290–291
 - routing packets through nonroutable IP address space, 285–286
- over UDP
 - configuring, 287–288

- routing packets through nonroutable IP address space, 283–284
- transport mode, 30
- tunnel mode, 31

K-L

key exchange, 18

LAN-to-LAN VPNs, 299, 301

- CA-based
 - initial failures, troubleshooting, 381
 - ongoing failures, troubleshooting, 384
- central site VPN Concentrator connection
 - configuring, 301–311
 - configuring on VPN 3000 with digital certificates, 320, 322
- initial failures, troubleshooting, 372–376, 381
- multiple subnet administration, 314–315
 - NAD, 318
 - network lists, 315–317
- ongoing failures, troubleshooting, 381
- remote site VPN Concentrator connection,
 - configuring, 312–313

layers of Cisco SAFE blueprint, 11

LED status, monitoring on Cisco VPN 3000, 332

Linux Cisco VPN Client, 52

load balancing, 266–267

- clusters, configuring, 270–271
- configuring, 269
 - on Hardware Client, 272
 - on Software Client, 273
- connection process, 267

RRI, 274

- Client RRI, 274–275
- network extension RRI, 275

VCA, 268–269

M

Mac OS Cisco VPN Client, 53–54

MD5 (Message Digest 5) algorithm, 15

memory status, monitoring on Cisco VPN 3000, 333

messages, DPD, 112

Microsoft Windows Cisco VPN Client.

See Windows Cisco VPN Client

mode of operation (VPN 3002 Hardware Client),
configuring, 230, 234

monitoring

bandwidth statistics, 361–362

Cisco 3002 Hardware Client, auto-update feature,
239–240

client user statistics on Cisco 3002 Hardware
Client, 259

session statistics, 292–294

Monitoring Refresh window (Cisco VPN 3000
Concentrator), 344

movianCrypt, 443

movianDM, 444

movianMail, 443

movianVPN, 425

banner support, configuring, 441

certificate-based authentication, configuring,
438–439

diagnostic tools, 441–442

DNS support, configuring, 437–438

external authentication, configuring,
439–440

gateway access, configuring, 426

IPSec, configuring, 433–434

NAT Traversal, configuring, 440–441

Perfect Forward Secrecy, configuring,
436–437

policies

configuring, 428–433

required information, 442–443

security applications, 443–444

split tunneling, configuring, 435–436

typical work setup, 426–427

multiple subnets, administering on LAN-to-LAN
VPNs, 314–315

NAD, 318

network lists, 315–317

N

NAD, configuring LAN-to-LAN VPNs, 318

NAT, 280

routing packets through nonroutable private
address space, 280–281

with two hosts, 281

NAT-T (NAT Traversal)

Concentrator, configuring, 289

configuring on movianVPN, 440–441

routing packets through nonroutable IP address
space, 284

VPN Software Client, configuring, 290

necessity of VPNs in corporate networks, 14

network enrollment, 180–183

Network Extension mode (Cisco 3002 Hardware
Client), 211

network extension RRI, 275

network lists, configuring on LAN-to-LAN VPNs,
315, 317

network management options, 62–63

nonroutable IP address space

routing packets through with IPSec over TCP,
285–286

routing packets through with IPSec over UDP,
283–284

routing packets through with NAT, 280

routing packets through with NAT-T, 284

O

obtaining Cisco Software Client, 54

ongoing VPN failures, troubleshooting, 366

on CA-based LAN-to-LAN VPNs, 384

on LAN-to-LAN VPNs, 381

on remote-access VPNs, 371

operation of IPSec, 31

data transfer, 37

defining interesting traffic, 32

IKE phase 1, 33–34

IKE phase 2, 34–36

tunnel termination, 38

origin authentication, IPSec functionality, 23

preshared keys, 24

RSA encrypted nonces, 26

RSA signatures, 24–25

OSPF (Open Shortest Path First), configuring on VPN
concentrator, 77–84

P

- packets, routing through nonroutable IP address space
 - with IPSec over TCP, 285–286
 - with IPSec over UDP, 283–284
 - with NAT, 280–281
 - with NAT-T, 284
- PAT (Port Address Translation), 282
 - Client mode operation, 211
 - translation tables, 282–283
- Perfect Forward Secrecy, configuring on movianVPN, 436–437
- Ping window (Cisco VPN 3000 Concentrator), 344
- PKCS#10 certificate requests, 144
- PKI, 142–143
- placement of VPN Concentrator, 58–59, 62
- policies
 - creating for movianVPN, 428–432, 442–443
 - testing for movianVPN, 432–433
- presared keys, 24
 - connecting browser interface, 92, 95–98, 101–103
 - remote-access VPN configuration, 87–92
- presared key LAN-to-LAN VPNs
 - initial failures, troubleshooting, 372–376, 381
 - ongoing failures, troubleshooting, 381

Q-R

- Quick Configuration window (Hardware Client), 213
 - remote-access VPN configuration, 93, 95, 97–98, 101–103
- Reboot Status window (Cisco VPN 3000 Concentrator), 344
- reconnaissance attacks, 4
- redundancy, columns, 43
- remote access, Cisco 3002 Hardware Client, 209–210
 - Client mode, 211
 - connecting to VPN 3000 Concentrator, 212, 215–217, 220–224, 227, 230, 234
 - Network Extension mode, 211
- remote site VPN concentrator connection, configuring on LAN-to-LAN VPNs, 312–313

- remote-access VPNs, 12
 - configuring with digital certificates, 139–143
 - certicate generation, 143–146
 - certicate validation, 149–151
 - configuring with presared keys, 87–89
 - browser configuration, 92, 95–98, 101–103
 - establishing management session, 90–92
 - connecting with certificates, 184–185
 - groups, configuring, 107–126
 - Hardware Client, 55
 - IKE proposals, configuring, 104, 106
 - parameters, 112–113, 116
 - software clients, 50
 - Linux client, 52
 - MacOS client, 53–54
 - Solaris client, 52
 - Windows client, 50–51
 - troubleshooting, 366
 - initial failures, 368–371
 - ongoing failures, 371
 - VPN 3000 Concentrator configuration, 169–171
- renewing certificates, 166
- RIP, 73
 - configuring on VPN concentrator, 73–74, 77
- root certificates, installing, 159–162
- routing table statistics, monitoring on Cisco VPN 3000, 326
- RRI (Reverse Route Injection), 274
 - Client RRI, 274–275
 - network extension RRI, 275
- RSA encrypted nonces, 26
- RSA signatures, 24–25
- rule parameters for CPP policies, creating, 200–202

S

- SAFE blueprint, 10
 - characteristics, 12
- script kiddies, 3
- security applications for movianVPN, 443–444
- Security Wheel, 5–7
- SEP (Scalable Encryption Processor), 42
 - columns, 43

SEP-E, 42
 session statistics, monitoring on Cisco VPN 3000, 334
 SHA-1 (Secure Hash Algorithm 1), 15
 signatures
 RSA, 24–25
 validating, 149
 site-to-site VPNs, 13
 Software Client, 50. *See also* Hardware client
 comparing with Hardware Client, 56
 custom CPP policies, creating, 199–206
 firewall features, 189
 AYT, 190, 192–194
 CPP, 196–197
 stateful firewall, 195
 firewall status parameters, 197
 displaying, 199
 IPSec backup server, 264
 configuring, 266
 Linux client, 52
 load balancing, configuring, 273
 Mac OS client, 53–54
 obtaining, 54
 session statistics, monitoring, 292–294
 Solaris client, 52
 Windows, configuring, 128–135
 Windows client, 50–51
 Software Update window (Cisco VPN 3000
 Concentrator), 340, 343
 Solaris Cisco VPN Client, 52
 Split DNS, 123, 126
 split tunneling, 116–121, 189
 configuring on movianVPN, 435–436
 stateful firewall, 189, 195
 static routing on Cisco VPN 3000 Concentrator, 67–69
 configuring, 69–72
 statistics, monitoring on Cisco VPN 3000
 Concentrator, 325
 bandwidth, 361–362
 dynamic filters, 327
 event log, 328–330
 general statistics, 338
 LED status, 332
 memory status, 333
 routing table, 326
 sessions status, 334
 system status, 330–332

status parameters for Software
 Client Firewall, 197
 displaying, 199
 structured threats, 4
 System Reboot window (Cisco VPN 3000
 Concentrator), 343
 system statistics, monitoring on Cisco VPN 3000,
 330–332
 LED status, 332
 memory status, 333
 system-wide OSPF configuration, 77–79

T

testing movianVPN policies, 432–433
 threats
 external, 4
 internal, 4–5
 structured, 4
 unstructured, 3
 traffic
 bandwidth aggregation, configuring, 361
 bandwidth policing, configuring, 353–356
 bandwidth reservation, configuring, 356–360
 translation tables (PAT), 282–283
 transport mode (IPSec), 30
 troubleshooting
 CA-based LAN-to-LAN VPNs
 initial failures, 381
 ongoing failures, 384
 VPNs
 initial failures, 365
 LAN-to-LAN, 372–376, 381
 ongoing failures, 366
 remote-access, 366–371
 tunnel default routes on VPN Concentrator, 69
 tunnel mode (IPSec), 31
 tunneling
 DPD messages, 112
 split tunneling, 116–118, 121
 tunnels, 209

U

- unit authentication, configuring on Cisco 3002
 - Hardware Client, 244–251
 - accessing username password prompt, 245, 249–251
- unstructured threats, 3
- update feature
 - configuring on Hardware Client, 234–238
 - monitoring, 239–240
- user and group information, configuring on VPN 3002
 - Hardware Client, 225–227, 230
- user authentication, configuring on Cisco 3002
 - Hardware Client, 252–255, 259
 - accessing username password prompt, 253, 256, 259

V

- validating digital certificates, 149
- VCA (Virtual Cluster Agent), 268–269
- VPN Client enrollment, 173–174
 - file enrollment, 174, 177–179
 - network enrollment, 180–183
- VPN Software Client
 - custom CPP policies, creating, 199–206
 - firewall features, 189
 - AYT, 190–194
 - CPP, 196–197
 - stateful firewall, 195
 - firewall status parameters, 197
 - displaying, 199
- VPNs
 - firewall-based, 14
 - initial failures, troubleshooting, 365
 - LAN-to-LAN, 299, 301
 - configuring, 301–313, 320–322
 - initial failures, troubleshooting, 372–376, 381
 - multiple subnet administration, 314–315
 - NAD, 318
 - network lists, 315, 317
 - ongoing failures, troubleshooting, 381
 - need for in corporate networks, 14

- ongoing failures, troubleshooting, 366
- remote-access, 12
 - troubleshooting, 366–371
- site-to-site, 13

W

- web browser configuration for VPN Concentrator, 57
- web-based management tools, Cisco VPN Monitor, 63
- Windows Cisco VPN Client, 50–51
- Windows Software Client, configuring, 128–135
- wireless access, MovianVPN
 - banner support, configuring, 441
 - certificate-based authentication, configuring, 438–439
 - configuring, 425–426
 - diagnostic tools, 441–442
 - DNS support, configuring, 437–438
 - external authentication, configuring, 439–440
 - IPSec, configuring, 433–434
 - NAT Traversal, configuring, 440–441
 - Perfect Forward Secrecy, configuring, 436–437
 - policies
 - creating, 428–432, 442–443
 - testing, 432–433
 - security applications, 443–444
 - split tunneling, configuring, 435–436
 - typical work setup, 426–427

X-Y-Z

- X.509 certificates, 147–148