Numerics

3DES (Triple Data Encryption Standard), 48

Access Rights screen (VPN 3000 Series Concentrator), administration, 316–322
Action options, applying to filter rules, 273
adding filter rules to VPN Client, 272
addressing assignment method, configuring on VPN 3000 Series Concentrator, 147
admin password, configuring on VPN 3000 Series Concentrator, 150
Administer Sessions screen (VPN 3000 Series Concentrator), administration, 310
administering VPN 3000 Series Concentrators, 307
Access Rights screen, 316–322
Administer Session screen, 310
Certificate Manager screen, 323
File Management screen, 322
menu options, 308–310
Monitoring Refresh screen, 315
Ping screen, 315
Software Update screen, 310–312
System Reboot screen, 313–315
Administration screen, VPN 3000 Series Concentrator management interface, 97–98
AH (Authentication Header), 40
fields, 41
Always On option. See Stateful Firewall feature answers to problem scenarios, 478–486
applying filter rules
Action option, 273
Destination address option, 274
Destination port option, 274–276
Direction option, 273
ICMP Packet Type option, 276
Name option, 273
Protocol option, 273
Source address option, 274
TCP connection option, 273–274
TCP/UDP source option, 274
assessing knowledge of required topics, 11
authentication
IKE key types, 49
interactive hardware client authentication, 375–376
with preshared keys
group preshared keys, 133
unique preshared keys, 132–133
wildcard preshared keys, 133
Authentication Data field
AH, 41
ESP, 43
authentication process for identify certificates, 225
Automatic Client Update feature, 283–284
auto-update
monitoring events, 426–428
VPN 3002 Hardware Client configuration, 423–426
AYT (Are You There), 268
applying to firewall policy, 280
backup servers
VPN 3002 configuration, 412–413
branch office VPN routers, 28
browser-based manager, performing Quick Configuration for Cisco VPN 3000 Concentrator, 141, 144
address assignment method, 147
admin password, 150
interface settings, 144–146
internal authentication, 148
IPSec tunnel group, 149
system information, 146
tunneling protocol, 147
user authentication method, 148
business VPN applications, 21
business-to-business extranet VPNs, 25
remote access, 22–23
caveats of implementing, 23
client-initiated model, 23
NAS-initiated model, 23
site-to-site intranet VPNs, 24
business-to-business extranets, 25

C

CAs (Certificate Authorities), 50, 53
authentication process, 225
configuring on Cisco VPN 3000 Series
Concentrators, 241–242
CRLs, 226
enrollment process, 224, 455–457
manual SCEP authentication, 228–230
preshared key SCEP authentication, 230
via PKCS #10, 233–235
via SCEP, 228, 236 454–455
hierarchies, 225
Internet-based, 247
PKCS #10 certificate requests, 222–224
services, 221–222
vendors, 231
CBC (Cipher Block Chaining), 47
central CA structure, 225
central hub VPN routers, 28
certificate management, 454
Certificate Management screen, Cisco VPN 3000
Series Concentrator administration, 323
certification
exam overview, 4
overview of exams, 5
CSVPN, 6–10
preparing for exam, 11–12
recommended training path, 10
topics covered, 3
Cisco Easy VPN, 32–33
Cisco IDS Host Sensor, 35
Cisco Mobile Office, 33
Cisco Secure ACS, 34
Cisco VPN 3000 Concentrator Manager
Configuration screen
Policy Management section, 173
System section, 169–172
User Management section, 173
IPSec configuration, 152–154
modifying groups, 155–168
Cisco VPN 3000 Series concentrators, 30–31,
85–87, 232
administration, 307
Access Rights screen, 316–322
Administer Sessions screen, 310
Certificate Manager screen, 323
File Management screen, 322
menu options, 308, 310
Monitoring Refresh screen, 315
Ping screen, 315
requirements, 134
Software Update screen, 310–312
System Reboot screen, 313–315
Automatic Client Update feature, 283–284
capabilities, 89–90
CA support, configuring, 241–242
certificate validation, 237
Cisco VPN 3005, 101
Cisco VPN 3015, 102
Cisco VPN 3030, 103
Cisco VPN 3060, 104
Cisco VPN 3080, 104
Cisco VPN Client, 87, 109
compatibility, 88
configuration requirements, 135–136
CRLs, 237
fault tolerance, 94
identity certificates
  enrolling via PKCS #10, 233–236
  enrolling via SCEP, 236
IKE configuration, 239–240
IPSec configuration, 152–154
modifying groups, 155–168
LED indicators, 105–107
management interface, 94–95
  Administration screen, 97–98
  configuring, 96
  Monitoring screen, 98
  upgrading, 99–100
monitoring, 324–330, 333, 337
Routing Table screen, 326
Monitoring menu
  Event Log screen, 327
  Sessions screen, 328–330
  Statistics screen, 330, 333, 337
  System Status screen, 327
performance, 87
PKCS #10 certificate requests, 222
  fields, 222–224
placement, 87, 91
Quick Configuration option, 136
  CLI method, 137–141
  with browser-based manager, 141–152
routing options, 88
security, 90, 93
supported tunneling protocols, 88
upgrading, 99–100
VPN 3002 Hardware Client, 108
  configuring preshared keys, 366–368
VPN Client software
  filter rules, configuring, 269–276
  firewall features, 265–267
  Stateful Firewall, 267–268, 276
Cisco VPN 3002 Hardware Client, 32
Cisco VPN 3005 Concentrator, 101
Cisco VPN 3015 Concentrator, 102
Cisco VPN 3030 Concentrator, 103
Cisco VPN 3060 Concentrator, 104
Cisco VPN 3080 Concentrator, 104
Cisco VPN Client Cisco VPN Clients, 31–33
  version 3.6 firewall features, 265–266
Cisco VPN products
  Cisco PIX firewalls, 28, 30
  Cisco VPN 3000 Concentrators. See Cisco VPN
  3000 Series concentrators
  Cisco VPN Clients, 31–33
    Cisco Internet Mobile Office, 33
    wireless clients, 33
  Cisco VPN routers, 27–28
  management software, 33–36
CiscoView, 35
CiscoWorks 2000, 34–36
Cisco Secure ACS, 35
CLI (command-line interface)
  performing Quick Configuration for Cisco VPN
    3000 Concentrator, 137–138
    Private LAN Interface configuration, 139–141
  system date and time configuration, 138–139
Client Config tab (Groups screen), modifying IPSec
  groups, 159–160, 162
Client FW tab (Groups screen), modifying IPSec
  groups, 162–164
Client mode (VPN 3002 Hardware Client),
  configuring, 371–373
Client RRI, configuring, 410
client-initiated remote access model, 23
communications, SAs, 46–47
comp-lzs transform, 57
concentrators, enrolling with CA, 455–457.
  See also Cisco VPN 3000 Series Concentrators
Configuration screen (VPN Manager)
  Policy Management section, 173
  System section
    Address Management subsection, 170
    Client Update subsection, 172
    Events subsection, 171
    General subsection, 172
  Client Config tab (Groups screen), modifying IPSec
    groups, 159–160, 162
  Client FW tab (Groups screen), modifying IPSec
    groups, 162–164
  Client mode (VPN 3002 Hardware Client),
    configuring, 371–373
  Client RRI, configuring, 410
  client-initiated remote access model, 23
  communications, SAs, 46–47
  comp-lzs transform, 57
  concentrators, enrolling with CA, 455–457.
  See also Cisco VPN 3000 Series Concentrators
Configuration screen (VPN Manager)
Configuration screen (VPN Manager)

IP Routing subsection, 170–171
Load Balancing Cisco VPN Clients subsection, 172
Management Protocols subsection, 171
Servers subsection, 169–170
Tunneling Protocols subsection, 170
User Management section, 173
configuring
Cisco VPN 3000 Series Concentrators
debug levels, 369–371
IKE, 239–240
management interface, 96
Quick Configuration option, 136–152
requirements, 135–136
Cisco VPN 3002 Hardware Client
IPSec over TCP/IP, 418
IPSec over UDP, 419–420
IPSec, 152–154
modifying groups, 155–168
transforms, 54–55
valid transform sets, 55–56
LAN-to-LAN connections, 449
network lists, 449, 451
tunnels, creating, 453
with digital certificates, 462–463
split tunneling, 374
interactive hardware client authentication, 380–384
on head-end VPN 3000 Series Concentrator, 376–378
user authentication, 380–384
VPN 3002 backup servers, 412–413
VPN 3002 Hardware Client
Auto-Update, 423–426
Client mode, 371–373
load balancing, 414–416
Network Extension mode, 374
preshared keys, 366–368
RRI, 407–411
VPN Client, 181–185
Stateful Firewall feature, 276

VPNs with IPSec, 57–58
peer authentication, 61
SAs, 61
triggering IPSec process, 59–60
VPN termination, 62
connections (IPSec), SAs, 46–47
courses, recommended training for CCSP certification, 10
CPP (Central Protection Policy), 268
Policy Pushed option, applying to firewall policy, 280
creating
filtering rules for VPN Client, 272
tunnels, 453
between VPN 3000 Series Concentrator and Hardware Client, 366
split tunneling, 374–384
CRLs (Certificate Revocation Lists), 227, 237
CSVPN (Cisco Secure Virtual Private Networks) exam, 5–7
topics covered, 8–10
customizing firewall settings on VPN Client, 279–280

debug levels, setting on VPN 3000 Series Concentrator and Hardware Client, 369–371
defining policies
CPP, 268
firewall policies on VPN Client, Firewall Policy option, 280
deploying IPSec, 38
DES (Data Encryption Standard), 47
destination address options, applying to filter rules, 274
destination port options, applying to filter rules, 274–276
Detroit site (Value-Packed Nutrition Corporation), 474
devices, Cisco VPN 3000 Series Concentrators.
See Cisco VPN 3000 Series concentrators
dialup, client-initiated remote access model, 23
Diffie-Hellman protocol, 50–51
digital certificates, 50
CAs, 221–222
authentication process, 225
enrollment process, 224, 228–230
hierarchies, 225
configuring in LAN-to-LAN connections, 462–463
management applications, 247
PKCS #10 certificate requests, 222–224
revocation, 226
Direction options, applying to filter rules, 273
displaying VPN Client firewall statistics, 281–282
DSA (Directory System Agent) algorithms, 224

enabling IPSec on VPN 3002 Hardware Client
over TCP/IP, 418
over UDP, 419–420
encrypted nonces, 50
encryption
3DES, 48
DES, 47
enrolling digital certificates, 224
via PKCS #10, 233–235
via SCEP, 228, 454–455
manual authentication, 228–230
preshared key authentication, 230
enrolling identity certificates, 233–236
enterprise networks, SAFE, 86
ESP (Encapsulating Security Payload), 42
fields, 43
modes of operation, 44

establishing VPNs with IPSec, 57–58
peer authentication, 61
SAs, 61
triggering IPSec process, 59–60
Event Log screen (Monitoring Menu), Cisco VPN 3000 Series Concentrator, 327
event logging
VPN 3000 Series Concentrator
IKE Failures on Phase 1, 370
Incorrect User Name, 370
Incorrect User Password, 371
Work Group Name Incorrect, 370
VPN 3002 Hardware Client, Incorrect Group Password, 370
events, monitoring Auto-Update on VPN 3002 Hardware Client, 426–428
exams, 11–12
CSVPN exam, 6–10
overview of CCSP certification track, 4–5
external groups (IPSec), 154
extranet VPNs, 25
EzVPN, 32–33

features of VPN Client, 175–176
fields
of AH, 41
of ESP, 43
of PKCS #10 certificate requests, 222–224
File Management screen, Cisco VPN 3000 Series Concentrator administration, 322
Firewall feature (VPN Client), configuring filter rules, 269–276
firewalls
AYT, 268
Cisco PIX Firewalls, 28–30
configuring on VPN Client, 278–279
customizing on VPN Client, 279–280
Firewall Policy option, 280
General tab (Groups screen), modifying IPSec groups, 155–156

Generating CAs via SCEP enrollment process, 455–457

Identity certificate installation, 458, 461

Group preshared keys, 133

Hierarchical CA structure, 225

HMAC (Hash-Keyed Message Authentication Code), 48

Hold-down routes, configuring, 411

HW Client tab (Groups screen), modifying IPSec groups, 164–166

ICMP Packet Type options, applying to filter rules, 276

Identity certificates, 224, 454

Authentication process, 225

Enrolling on Cisco VPN Concentrators via PKCS #10, 233–236

via SCEP, 236

Installing, 458–461

Identity tab (Groups screen), modifying IPSec groups, 155

IKE

Configuring on Cisco VPN 3000 Series Concentrators, 239–240

Identifying scenario requirements, 475

Key types, 49

IKE Failures on Phase 1 event log, 370

Implementing remote access VPNs, caveats, 23

Incorrect Group Password event log, 370

Incorrect User Name event log, 370

Incorrect User Password event log, 371

Installing

Identity certificates via SCEP, 458–461

VPN Client, 177–180

Interactive hardware client authentication, 375–376, 382–384

Interface settings, configuring on VPN 3000 Series Concentrator, 144–146

Internal authentication, configuring on VPN 3000 Series Concentrator, 148

Internal groups (IPSec), 154

Internet-based CAs, 247

Cisco VPN product support, 231

Intranet VPNs, 24

IP address translation, PAT, 417

IPSec, 36

CAs, 53

Configuring through Cisco VPN 3000 Concentrator Manager, 152–154

Groups, modifying, 155–167

Identifying scenario requirements, 476

IKE key types, 49

Over TCP/IP, configuring on VPN 3002 Hardware Client, 418

Over UDP, configuring on VPN 3002 Hardware Client, 419–420

Peer formation, 54

Planning for deployment, 38

RFCs, 36–37

SAs, 46–47

Forming, 54

Supported protocols, 38–39

3DES, 48

AH, 40–41

DES, 47

Diffie-Hellman, 50–51

ESP, 42–44

HMAC, 48

MD5, 49

Secure Hash Algorithm, 49
transforms, 54–55
valid transform sets, 55–56
transport mode, 44
troubleshooting connections on VPN 3002 Hardware Client, 420–422
tunnel groups, configuring on VPN 3000 Series Concentrator, 149
tunnel mode, 45
VPN establishment, 57–58
triggering IPSec process, 59–61
VPN termination, 62
IPSec tab (Groups screen), modifying IPSec groups, 157–158

K–L

key types (IKE), 49
LAN Extension mode (VPN 3002 Hardware Client), 374
LAN-to-LAN connections
configuring, 449
digital certificates, 462–463
network lists, configuring, 449–451
tunnels, creating, 453
LAN-to-LAN network RRI, configuring, 409
LED indicators (Cisco 3000 VPN Series Concentrators), 105–107
load balancing
configuring on VPN 3002 Hardware Client, 414–415
virtual clusters, 415–416
logging. See event logging

M

maintaining message integrity
HMAC, 48
MD5, 49
Secure Hash Algorithm, 49
management software, 33
Cisco Works 2000, 34–36
VDM, 33
man-in-the-middle attacks, 133
manual SCEP authentication, 228–230
MD5 (Message Digest 5), 49
Memphis site (Value-Packed Nutrition Corporation), 474
menu options, Cisco VPN 3000 Series Concentrator administration, 308–310
message encryption
3DES, 48
DES, 47
modifying IPSec groups, Groups screen tabs
Client Config tab, 159–162
Client FW tab, 162–164
General tab, 155–156
HW Client tab, 164–166
Identity tab, 155
IPSec tab, 157–158
PPTP/L2TP tab, 166–167
monitoring
Cisco VPN 3000 Series Concentrators, 324
Event Log screen, 327
Routing Table screen, 326
Sessions screen, 328–330
Statistics screen, 330–337
System Status screen, 327
VPN 3002 Hardware Client, Auto-Update events, 426–428
Monitoring Refresh screen, Cisco VPN 3000 Series Concentrator administration, 315
Monitoring screen, Cisco VPN 3000 Series Concentrator management interface, 98
Movian VPN Client, 33
Name options, applying to filter rules, 273
NAS-initiated remote access model, 23
NAT (network address translation), static NAT, 416
Network Extension mode (VPN 3002 Hardware Client), configuring, 374
Network Extension mode RRI, configuring, 410
network lists, configuring, 449–451
Next Header field (ESP), 43
nonces, 50

OSPF (Open Shortest Path First), setting up for RRI, 408
overview of required certification exams, 5
CSVPN, 6–10

Pad Length field (ESP), 43
Padding field (ESP), 43
PAT (Port Address Translation), 417
static NAT, 416
Payload field (ESP), 43
Payload Length field (AH), 41
peer authentication, IKE key types, 49
PEM (Privacy Enhanced Mail), 234
performance, Cisco VPN 3000 Series Concentrators, 87
Ping screen, Cisco VPN 3000 Series Concentrator administration, 315
PKCS #10 certificate requests, 222–224
PKI, CAs
authentication process, 225
CRLs, 226
enrollment process, 224, 228–230

hierarchies, 225
PKCS #10 certificate requests, 222–224
services, 221–222
placement of Cisco 3000 Series Concentrators, 91
planning IPSec deployment, 38
polling, AYT, 268
Port Address Translation mode (VPN 3002 Hardware Client), 371–373
Portland site, 476
Value-Packed Nutrition Corporation, 474
PPTP/L2TP tab (Groups screen)
modifying IPSec groups, 166–167
prechapter tests, 11
preparing for exam, 11–12
preshared keys, 50
group, 133
SCEP authentication, 230
unique, 132–133
VPN 3002 Hardware Client configuration, 366
verifying tunnel operation, 368
wildcard, 133
Private LAN Interface, CLI Quick Configuration, 139–141
Protocol options, applying to filter rules, 273

Quick Configuration option (Cisco VPN 3000 Concentrator), 136
CLI method, 137–141
with browser-based manager, 141–152

recommended training path for CCSP certification, 10
redundancy, configuring VPN 3002 backup servers, 412–413
remote access VPsNs, 22–23
requirements for Cisco VPN 3000 Concentrator configuration, 135–136
Reserved field (AH), 41
revocation of certificates, 226
RFCs, IPSec-related, 36–37
Richmond sitem (Value-Packed Nutrition Corporation), 475
RIPv2, setting up for RRI, 407
RME (Cisco Works Resource Management Essentials), 36
root certificates, 224
routers, Cisco VPN routers, 27–28
Routing Table screen (Monitoring Menu), Cisco VPN 3000 Series Concentrator, 326
RRI (Reverse Route Injection), configuring
  Client RRI, 410
  hold-down routes, 411
  LAN-to-LAN Network RRI, 409
  Network Extension mode RRI, 410
OSPF, 408
RIPv2, 407
RSA digital signatures, 50

SAFE, 86
SAs (Security Associations), 39, 46–47
  forming, 54
saving Cisco VPN 3000 Concentrator configuration settings, 150–151
scenarios
  Value-Packed Nutrition Corporation answers, 478–486
  Detroit site, 474
  IKE configuration, 475
  IPSec configuration, 476
  Memphis site, 474
  Portland site, 474
  Richmond site, 475
  Seattle site, 474
SCEP (Simple Certificate Enrollment Protocol), 228, 454–455
  CA generation
    enrollment process, 455–457
    identity certificate installation, 458, 461
  enrollment process, 236
  manual authentication, 228–230
  preshared key authentication, 230
Seattle site (Value-Packed Nutrition Corporation), 474
Secure Hash Algorithm, 49
security, firewalls
  AYT, 268
  Cisco PIX Firewalls, 28–30
    configuring on VPN Client, 278–279
    customizing on VPN Client, 279–280
    Firewall Policy option, 280
Security Parameters Index field
  AH, 41
  ESP, 43
self-signing certificates, 454
Sequence Number Field
  AH, 41
  ESP, 43
Sessions screen (Monitoring Menu), Cisco VPN 3000 Series Concentrator, 328–330
setting debug levels on VPN 3000 Series Concentrator and Hardware Client, 369–371
site-to-site intranet VPsNs, 24
small remote office VPN routers, 28
Software Update screen, Cisco VPN 3000 Series Concentrator administration, 310, 312
SOHO remote-access VPN routers, 27
Source Address options, applying to filter rules, 274
SPI (Security Parameters Index), 46
split tunneling, 268, 374
  configuring on head-end VPN 300 Series Concentrator, 376–378
  interactive hardware client authentication, 380–384
  user authentication, 380–84
Stacker LZS compression, 57
starting VPN Client from Windows-based PCs, 174
Stateful Firewall feature (VPN Client), 267–268
configuring, 276
Statistics screen (Monitoring Menu), Cisco VPN
3000 Series Concentrator, 330–335
study tips
- exam preparation, 11–12
- prechapter tests, 11
subordinate certificates, 454
supported IPSec protocols, 38–39
3DES, 48
- AH, 40–41
- DES, 47
- Diffie-Hellman, 50–51
- ESP, 42
  - fields, 43
  - modes of operation, 44
HMAC, 48
IKE key types, 49
MD5, 49
Secure Hash Algorithm, 49
system information, configuring on VPN 3000
Series Concentrator, 146
System Reboot screen, Cisco VPN 3000 Series
Concentrator administration, 313–314
system requirements for VPN Client
installation, 177
System Status screen (Monitoring Menu), Cisco
VPN 3000 Series Concentrator, 327
system time and date, CLI Quick Configuration,
138–139

target audience of book, 5
TCP connection options, applying to filter rules,
273–274
TCP/UDP source options, applying to filter
rules, 274
terminating VPNs with IPSec, 62
testing centers, registration process, 4
Thompson Prometric testing centers, 4
topics covered in CCSP exam, 3
transforms, 54–55
valid transform sets, 55–56
transport mode (IPSec), 44
troubleshooting IPSec connections on VPN 3002
Hardware Client, 420–422
tunnel mode (IPSec), 45
 tunnels
- between VPN 3000 Series Concentrator and
  Hardware Client, 366
- configuring on VPN 3000 Series
  Concentrator, 147
- creating, 453
- split tunneling, 374
  - configuring on head-end VPN 3000 Series
    Concentrator, 376–378
  - interactive hardware client authentication,
    380–384
  - user authentication, 380–384
unique preshared keys, 132–133
Unity Client, 31
upgrading Cisco VPN 3000 Series Concentrator,
99–100
user authentication configuration
  - VPN 3000 Series Hardware Client, 382–384
  - VPN 3000 Series Concentrator, 148
valid transform sets, 55–56
Value-Packed Nutrition Corporation
  answers to problem scenarios, 478–486
  Detroit site, 474
  Memphis site, 474
  Portland site, 474, 476
  Richmond site, 475
  Seattle site, 474
VDM (Cisco VPN Device Manager), 33
vendors supporting Cisco VPN products, 231
verifying tunnel operation between VPN 3000 Series
  Concentrator and Hardware Client, 368
viewing VPN Client firewall statistics, 281–282
virtual cluster masters, 415
VMS (Cisco Works VPN/Security Management
  Solution), 35–36
VPN 3000 Series Concentrator. See Cisco VPN
3000 Series concentrators
VPN 3002 backup servers, configuring, 412–413
VPN 3002 Hardware Client
  auto-update
    configuring, 423–426
    monitoring events, 426–428
  Client mode, 371–373
IPSec
  over TCP/IP, configuring, 418
  over UDP, configuring, 419–420
  troubleshooting connections, 420–422
load balancing, 414–415
  virtual clusters, 415–416
Network Extension mode, 374
preshared keys, configuring, 366
  verifying tunnel operation, 368
RRI, configuring, 407–411
setting debug levels, 369–371
VPN Client
  Automatic Client Update feature, 283–284
  configuring, 181–185
  features, 175–176
  filter rules, configuring, 269–276
  firewall settings
    configuring, 278–279
    customizing, 279–280
    policy options, 280
    statistics, viewing, 281–282
  installing, 177, 180
  starting from Windows-based PC, 174
Stateful Firewall feature, 267–268
  configuring, 276
VPN Concentrators, configuring LAN-to-LAN
connections with digital certificates, 462–463
VPN Manager. See browser-based manager
VPNs, 21
  business-to-business extranet VPNS, 25
    establishing with IPSec, 57–58
    peer authentication, 61
    SAs, 61
    triggering IPSec process, 59–60
  remote access, 22–23
    caveats of implementing, 23
    client-initiated model, 23
    NAS-initiated model, 23
  site-to-site intranet VPNS, 24
    terminating with IPSec, 62
VUE testing centers, 4
W-Z

WEP (Wired Equivalent Privacy), 86
wildcard preshared keys, 133
wireless communications
    Movian VPN Client, 33
    WEP, 86
Work Group Name Incorrect event log, 370

X.509 Identity Certificate fields, 245