Index

Note: Page numbers followed by *f* and *t* indicate figures and tables, respectively.

A
abandon_time setting, for SMTP Security Server, 303
Accept action, in rules, 86
accept short circuit, in INSPECT, 523*t*
account names, in Windows NT, 555–556
account policies, in Windows NT, 555–556
Action, in rules, 86
action properties
  for Client Authentication, 227–229, 228*f*, 266*f*, 267*f*
  for encryption, in VPN, 396–397, 396*f*
  for Session Authentication, 225–226, 226*f*, 264*f*
  for URI resource, 275–276, 276*f*
  for User Authentication, 222–223, 222*f*, 262, 262*f*
address range objects, about, 73
address space. *See also* IP address
  adding, for firewalls, 15
  breakdown of, 337*t*
  sharing, in VPN, 405–406
address translation, introduction to, 335–338
address translation policy. *See* NAT rules
address translation tables, remote viewing of, 167
Administrative notifications, 134
administrative user
  adding, in management console installation, 45, 46*f*
  creating, 210
  logging actions of, 122
Administrator account, in Windows NT, 555
administrators, in operating system selection, 27, 29–30
aggressive mode, for IKE, 392
AIX
  FireWall-1 on, 30
  packet sniffer in, 355
alerts
  about, 133–136
  on Client Authentication, 229
  defining, 115–116, 116*f*
  by e-mail, 136
aliases, in SIC policy, 187, 188
anti-spoofing
  defining, 80–81, 81*f*
  in INSPECT, 534
  local interface, error on, 145
  for NAT, 350, 350*t*
    in double-blind network, 376
    in network migration, 372
    in simple network, 367, 367*t*
  in Office Mode, 445
  packet checked against, 342
AOL Instant Messenger, blocking, 149, 150*t*
application(s), Check Point
  alerts defined for, 115
  queried with `cpstat`, 119*t*–121*f*
  states of, 114, 114*t*–115*t*
application(s), in OS security, 37, 38
application layer gateways. *See* application proxies
application proxies
  authenticated requests forwarded to, 249
  filtering traffic through, error on, 257
  in FireWall-1, 8–9
  FireWall-1 as, 250
  vs. NAT, 336
  overview of, 4–5
  Passive FTP handled by, 6
  Stateful Inspection and, 5

application proxies (*cont.*)
traceroute handled by, 8
URI resource applied with, 273
<apply-to>, in SIC policy rules, 187
ARPs, for NAT
in double-blind network, 375, 375*f*
in network migration, 370–371
setting up, 345–347
in simple network, 366
troubleshooting, 356–357
assets, in security policy, 16
asymmetric connections, gateway cluster options for, 496–497
asymmetric encryption, definition of, 381
asymmetric routing
dynamic load balancing and, 507
in High Availability, 500–501
Office Mode and, 444
in State Synchronization, 498–499, 500–501
VPN and, 443
attributes, of dynamic tables, 528, 529*t*
authentication
certificates for, 163
configuring, for management users, 62–63, 62*f*
custom message on, 249
DLL for, SecureClient and, 460–461
expiration of, 229
failure of, settings for, 221, 223, 242
gateway support for, error on, 255
Global Properties for, 220–221, 220*f*
in OS security, 39
prompt for, absence of, 257
purpose of, 193
rule processing and, 90
in SecureClient, 439–441, 440*f*, 441*f*
in SecuRemote
timeout on, 433
in user creation, 429
settings for, for user, 212–218, 213*f*–216*f*
setting up, 208–221
troubleshooting, 255–259
in VPN, 379
of VPN, changing FQDN and, 175
Authentication Header, in IPSec, 385
authentication servers
firewall and, 37–38
integrating, 230–243
users in, FireWall-1 use of, 247
authentication services. *See also specific services*
unavailable, 256
Automatic ARP Configuration, 341–342

B

Backward Compatibility package, installation of, 42–43, 43*f*
banner, removal of, 250
buffer, HTTP, increasing size of, 293–294
buffer, log, full, 148
buffer, sync, error on, 516, 517–519

C

caching proxy server, requests forwarded to, 286
central gateway, in Star Community, 398
central license, 24
certificate(s)
for authentication, 163–164
configuring, for management users, 62–63, 63*f*
defining, for SecuRemote user, 430–431, 430*f*
expiration of, 220
generating, for user, 217–218, 217*f*
in L2TP, 447
on management station, deletion and, 175
vs. pre-shared secrets, 387
reserved, 430–431, 431*f*
in Windows, 447–449
certificate authority. *See also* ICA
definition of, 383
SecureClient options for, 462, 462*f*
certificate authority keys
exchanging, 392, 393*f*
in VPN, 387
certificate key, for licenses, 24
Certificate Revocation List (CRL), in LDAP, 236
characters, in naming, illegal, 104, 105*t*
Check Point applications
alerts defined for, 115
queried with `cpstat`, 119*t*–121*f*
states of, 114, 114*t*–115*t*
Check Point banner, removal of, 250
Check Point Express, license for, 23
Check Point gateway object
about, 67–69, 67*f*
configuring, for High Availability management modules, 180–181, 181*f*
defining, 92, 94, 94*f*

externally managed, about, 70
log forwarding with, 138–139, 138*f*
log rotation with, 137–138, 137*f*
SecuRemote behind, 470, 470*f*
for VPN, 394, 394*f,* 417
Check Point host object
for remote management, with NAT, 165
for secondary management module, 178–179, 178*f*
Check Point licenses. *See* license(s)
Check Point Management Interface (CPMI), 190–191
Check Point modules
connections between, 162, 162*f*
states of, 114, 114*t*
Check Point node objects, about, 69
Check Point objects, 70–73, 92. *See also* Check Point gateway object
checksum, from hash functions, 382
Cisco PIX, VPN issues with, 409
Class E addresses, 335–336
Cleanup rule, 88, 88*f,* 99
CLI. *See* command-line interface
Client Authentication
in cleartext, 256
explanation of, 202–205
over HTTP
custom pages for, 254–255
debugging, 320*t*
limitations of, 207
redirect on, 257
rule for, 227, 227*f*
error on, 256
sample configuration for, 265
security policy installation and, 257
setting up, 227–230
over Telnet, 202, 203–204
debugging, 320*t*
option for, 228
usage guidelines for, 207*t*
Client Encrypt action, for SecuRemote, 432, 432*f*
Clientless VPN
enabling, 243–244
in FireWall-1, 243–247
issues with, 246–247
client/server model, application proxies in, 4
clients file, for RADIUS, adding firewall to, 231
ClusterXL
error messages with, 514–520
license for, 494
load balancing with, 503–504
command line
blocking connections from, 129–131, 129*t*–130*t*
firewall configuration from, 190–191
`fw monitor` options from, 541*t*
license update from, 169–171
logs accessed from, 124–126
object created with, 143–145
for policy control, remote, 166
state tables viewed from, remotely, 167–169
system status accessed from, 116–118
command-line interface (CLI)
in AIX, 30
in IPSO, 31, 32
for SecureClient, 474–475, 474*t*–475*t*
in SPARC Solaris, 29
in Windows NT/2000, 29
Comment, in rules, 87
compiler, for INSPECT, 529–531
compressed connection, for SmartDashboard/ Policy Editor, 108
compression method, for VPN, selecting, 397
conditions, in INSPECT, 524–526
connection
accepting based on previous connection, INSPECT for, 537–538
blocking
from command line, 129–131, 129*t*–130*t*
with `fw sam`, 143
passwords erased and, 460
in SmartView Tracker, 128–129
sync buffer and, 518
disconnecting, at specific time, 143
firewall bypassed by, NAT and, 352–355
hiding, IP address for, 340
to HTTP Security Server, number of, 293
for L2TP, creating, 449–450
outbound, for SecuRemote, 536–537
to Security Servers, origin of, 318
to SMTP Security Server, number of, 305
successful, packet sniffer output for, 356
unidirectional, 152–153
connection mode, for SecureClient, 458*f,* 459

connections table
  creating, with INSPECT, 528
  of firewall module, remote viewing of, 167–169
  kbuf pointer in, incorrect, 519–520
  manipulating, in INSPECT, 527–528
Connect Mode, for SecureClient, 443
constants, in INSPECT, 526
content, CVP for scanning, 270, 282–284
Content Security
  e-mail error messages for, 305
  for FTP, 299–302
  for HTTP, 271–298
  with Session Authentication, 256, 319
  for SMTP, 302–316, 303*f*
    sample configuration for, 322–326
  for TCP, 316–318
  third-party software for, 269
  with User Authentication, 319
Content Vectoring Pool. *See* CVP
`cpconfig`, user configuration with, 58
`cpd`, 183
CPMI (Check Point Management Interface), 190–191
CPRID connections, accepting, 83, 96, 97*f*
`cprlic`, 170–171
`cpstat`, 118, 118*t*–121*t*
CPVP-VSC, license for, 426
CPVP-VSR, license for, 426
critical updates
  for Windows 2000, 557
  for Windows NT, 556
CRL (Certificate Revocation List), in LDAP, 236
cryptography, definition of, 380
CVP (Content Vectoring Protocol)
  about, 270
  with FTP Security Server, 300, 300*f*, 316–317, 317*f*
    sample configuration for, 328–329, 328*f*
  with HTTP Content Security, 282–284
    sample configuration for, 330, 333*f*
  with SMTP Security Server, 312, 325, 325*f*
  in URI resource, 276–277, 277*f*

D

data, protection of, in security policy, 16–17
data integrity methods, for VPN
  selecting, 397
  settings for, 390
`dbedit`
  documentation of, 190
  object creation with, 143–145
  rulebase edited with, 103
defaultfilter.pf, sample of, 581–582
Defender, about, 196–197
Defender users, FireWall-1 use of, 247
defragmentation, virtual, error on, 146
delivery failure, e-mail stuck on, 313
demilitarized zone (DMZ)
  group for, 93, 93*f*
  need for, 14
denial-of-service (DoS) attacks
  ACK packets in, vanish action for, 523
  traceroute packets in, 8
Desktop Policy Server
  installation of, on IPSO, 40
  no response for, 480
Desktop Security
  policy for
    for client-to-site VPN, 484, 484*f*
    defining, 436–438, 436*f*, 437*f*
  for SecuRemote, setting up, 434–438
destination, in rules, 86
destination port static NAT, 340
destination static NAT, 340
detailed_av_err_mail setting, for SMTP Security Server, 305
detailed_rb_err_mail setting, for SMTP Security Server, 305
detailed_smtp_err_mail setting, for SMTP Security Server, 305
DHCP server
  link-local addresses and, 339
  for Office Mode, 445
DHCP traffic, accepting, 83, 98
DH (Diffie-Hellman) keys, definition of, 383
dial-up adapters
  installing SecureClient on, 439, 464
  mixing with NICs, SecuRemote and, 479
dial-up networking
  VPN integrated with, 443
  WINS server and, 456
Diffie-Hellman (DH) keys, definition of, 383
DLL, for authentication, SecureClient and, 460–461

- DMZ (demilitarized zone)
  - group for, 93, 93*f*
  - need for, 14
- DNS, split-horizon, 159
- DNS domain, defining, for Office Mode, 445
- DNS lookup
  - domains and, 71
  - enabling, 106
  - HTTP Security Server and, 297–298
  - service connection slowed by, 158
- DNS registration, disabling, in Windows 2000, 558
- DNS server, defining, for Office Mode, 445
- DNS traffic, encrypting
  - Global Properties for, 456
  - in SecureClient, 434
- domain. *See* Windows NT domain
- domain name
  - for external user group, 211
  - in INSPECT, 526
- domain objects, about, 71
- DoS (denial-of-service) attacks
  - ACK packets in, vanish action for, 523
  - traceroute packets in, 8
- downloads
  - policy on, 563–564
  - preventing, 287–288
- Drop action, in rules, 86
- drop short circuit, in INSPECT, 523, 523*t*
- Dst, in rule enforcement, 87
- dual NAT, 353–354, 353*f*
- dynamic load balancing, 507–508, 508*f*
  - with NAT, 509, 509*f*
- dynamic object
  - resolution failure for, log/alert on, 135
  - on ROBO Gateway, 190
- dynamic tables, creating, with INSPECT, 528

E

- Early Version Compatibility, for SecureClient, 438, 438*f*
- education, in network security, 18
- ELA (Event Log API), 270
- e-mail
  - alerts by, 136
  - in SMTP Security Server, 305
    - settings for, 303, 306
    - size of, 312
    - stuck, 313–316
- e-mail headers, rewriting, 308–309
- e-mail recipients, number of, under SMTP Security Server, 313–316
- embedded device objects, about, 70
- Encapsulating Security Payload (ESP)
  - in IPSec, 385
  - rules for, 407, 407*f*
- Encrypt/Client Encrypt action, in rules, 86
- Encrypt DNS Traffic, in Global Properties, 456
- encryption
  - asymmetric, definition of, 381
  - concepts in, 380–383
  - definition of, 380
  - for LDAP server, 239–240, 239*f*
  - licensing for, 383–384, 384*t*, 426
  - NAT and, 405
  - of Session Authentication, 256
  - symmetric, definition of, 381
  - User Authentication with, 406
  - in user properties, 218, 218*f*
  - in VPN, 379
    - configuring, 386–402
    - load balancing and, 510
  - VPN rules for, 396, 396*f*
    - for SecuRemote access, 431–432
- encryption algorithm, for VPN, selecting, 397
- encryption domain
  - address space shared in, 405–406
  - for client-to-site VPN, 482–483, 483*f*
  - compiled, in INSPECT, 531
  - definition of, 383
    - issues with, 410
  - determining, 387
    - for simplified mode, 397
    - for traditional mode, 389, 390*f*
  - disconnection from, issues with, 443
  - DNS requests forwarded inside, in Microsoft Networking, 453–456
  - downloading to SecuRemote client, 427
  - incorrect, 407–408
  - limiting access to, 403
  - multiple entry points to, 450–453
  - NIC IP address in, 479
  - SecuRemote used within, 443
  - selecting, 394, 395*f*
  - for site addition, 417
  - for three-site VPN, 413–414
  - unencrypted traffic in, 459

encryption keys, definition of, 380
encryption schemes, defining, for SecuRemote user, 428–430, 428*f,* 429*f*
End User License Agreement, IP address limits in, 22
end-user support, for SecuRemote, 426
entropy, in pseudo-random number generators, 380–381
entry points
  to encryption domain, multiple, 450–453
  SecureClient with multiple, 488–491, 488*f*
  in security, 14
error messages
  via e-mail, 305
  from security policy installation, 100–101, 101*f*
  in system log, 145–148
ESP (Encapsulating Security Payload)
  in IPSec, 385
  rules for, 407, 407*f*
evaluation licenses
  about, 24–25
  installation of, 45
  removal of, 170–171
Event Log API (ELA), 270
excessive log grace period, 135
exclusion, grouping by, 72, 73*f*
expiration date
  for management users, 62
  for users, 212
externally managed gateway objects, about, 70
externally managed node objects, about, 70
external user profile, 210, 211*f*

F
file descriptors, adjusting, for HTTP Security Server, 295–296
file downloads
  policy on, 563–564
  preventing, 287–288
filter, default
  changing, 539–540
  sample of, 581–582
fingerprints
  in encryption, 382
  validating, in SecureClient, 441, 441*f*
FIN packets, out of sequence, 157
firewall. *See also* FireWall-1; firewall module
  access to, by SecureClient with NAT, 469
  adding to RADIUS, 231
  authentication enabled on, 218–219, 219*f*
  authentication servers and, logon with, 37–38
  connections bypassing, NAT and, 352–355
  definition of, 1–2
  in encryption domains, 383
  gateway cluster and, switching to, 419–422, 420*f*
  limitations of, 2–3
  as MX, 310
  network logon to, 37–38
  number of, issues with, 189
  Passive FTP handled by, 5–6
  without security policy, 18
  security policy enforced with, 16
  Telnet to, error on, 258
  traceroute handled by, 6–8
  virtual, gateway clusters as, 401–402
FireWall-1
  alerts defined for, 116, 116*f*
  Clientless VPN in, 243–247
  components of, 161–163, 162*f*
  configuration of, common questions about, 141–145
  flexibility of, 10–11
  installation of, 39–52
    directory for, 43, 43*f*
    planning, 13–26
  integration with Windows NT domain, 247–248
  interoperability with, of third-party VPN products, 403
  kernel variables in, modifying, 141–142
  L2TP clients and, 446–450
  large-scale use of, management issues with, 188–191
  NAT in, 336, 339–343
  need for, 9–11
  operating system for
    installing, 34–39
    securing, 37–39, 545–561
    selecting, 27–34
  order of operations in, 341–343
  packet sniffer in, 355
  as proxy, 250

as reverse proxy, 250
technologies in, 8–9
upgrading, 52–53
firewall-1.conf, 567–569
FireWall-1 control connections, accepting, 83, 96, 96*f*
FireWall-1 host, license for, 22
FireWall-1 Password
about, 194
enabling, on firewall, 219
settings for, for user, 215, 215*f*
firewall-1.schema, 571–573
firewall Internet gateway. *See* single-gateway products
firewall module
dynamic addressing used by, SIC and, 184
in FireWall-1, 161
installation of, 49–52
license for, 20–26
updating remotely, 169–171
logging on, local, 164–165
one-time password for, 163–164, 164*f*
security policy on, remotely controlling, 166–167
state tables of, remote viewing of, 167–169
synching clock of, to management station, 184
firewall object
for NAT implementation, 350, 351*t*
in double-blind network, 376, 376*t*
in network migration, 372, 373*t*
in simple network, 367, 368*t*
for SecuRemote, configuring, 427
floating evals, 24–25
FQDN (fully qualified domain name), changing, 48, 48*f*
FTP commands, FTP Security Server and, 300–301
FTP connections
with random source port, 157
over SSL, 157–158, 158*t*
FTP proxy, FireWall-1 as, 250
FTP resource, for Content Security, 299–300, 299*f*, 300*f*
sample configuration for, 327–329, 327*f*, 328*f*, 329*f*
FTP Security Server
about, 299–302
debugging, 320*t*
sample configuration for, 326–329
site access through, 301–302
FTP service
Client Authentication over, 228
ident required by, 157
ports for, problems with, 157
problems with, 156–158
User Authentication for, 198–201
rule order and, 224
FTP traffic, Content Security for, 299–302
sample configuration for, 326–329
full sync
definition of, 494
error on, 514
fully qualified domain name (FQDN), changing, 48, 48*f*, 175
`fw`, *vs.* `fwm`, 167
`fw fetch`, 167
`fw log`, 124–126, 126*t*
`fw logswitch`, 136–137
`fwm`
vs. `fw`, 167
user configuration with, 58–59, 59*t*
`fwm load`, 166
`fw monitor`
example code for, 542
guidelines for use of, 543
INSPECT used with, 540–542, 541*t*
NAT issues and, 355
`fwm unload`, 167
`fw` parameter, of `cpstat`, application flavors for, 120*t*
`fw putkey`, 163
`fw sam`, 129–131, 129*t*–130*t*
connection blocking with, 143
FWZ, about, 384–385

G

gateway
IP addresses for, in INSPECT, 534
management module moved from, 176–178
management of, with ROBO Gateway Profile, 189–190
packets from, accepting, 83, 97, 97*f*
rule enforcement by, specifying, 87
in VPN Communities, 401, 407

gateway cluster
- creating, 421, 421*f*
- firewall switching to, 419–422, 420*f*
- for High Availability VPNs, 401–402
- IP address for, 495–496
- IP Pool NAT in, 452
- policies installed in, inconsistencies in, 514–515, 516
- SecureClient with, sample configuration for, 484–487, 485*f*
- SecuRemote failover with, 450
  - sample configuration for, 488–491, 490*f*
- software mismatch within, 519–520
- for State Synchronization
  - configuration of, 495–497, 495*f,* 496*f,* 497*f*
  - working mode of, error on, 514
- third-party, interoperability with, 403

gateway cluster objects
- about, 70
- configuring, 495–497, 495*f,* 496*f,* 497*f*

Gateway Components, installation of, 40

gateway object. *See also* Check Point gateway object
- for gateway cluster creation, 419–420, 485
- IP Pool NAT settings for, 452, 452*f*
- Office Mode configured on, 444–446, 444*f*
- for SecuRemote, configuring, 427–428
- User Authentication configured on, 223

GINA DLL, enabling, for SecureClient, 465

Global Properties
- for authentication, 220–221, 220*f*
- for High Availability management modules, 179–180
- IP Pool NAT in, 451, 451*f*
- for LDAP, 235–236, 235*f*
- for rulebase
  - about, 82–85, 82*f,* 84*f,* 85*f*
  - alerts settings in, 133–136, 133*f,* 134*f*
  - application of, 106
  - tweaking, 96–98
- for SecuRemote, 432–434, 433*f*
  - encryption in, 429–430, 429*f*
- VPN modes in, 388–389, 388*f*

Gnutella, blocking, 288–289

group, user. *See* user groups

group objects
- about, 72, 72*f*
- configuring, for management users, 62, 62*f*
- creating, with `dbedit`, 144
- defining, 92, 93, 93*f*
- for DMZ, 93, 93*f*
- for VPN domain, 390

GUIdbedit tool, rulebase edited with, 103, 103*f*

H

HA. *See* High Availability

hackers, firewall design and, 3

hard drive partitioning
- for Linux, 559
- for SPARC Solaris, 545

hardware support, in SPARC Solaris, 29

hardware token
- in Defender, 196–197
- in SecurID, 196, 196*f*

hash functions
- for dynamic load balancing, 507, 508*f,* 509
  - with VPN, 510
- in encryption, 382

High Availability (HA), 270
- asymmetric routing in, 500–501
- hardware-based solutions for, 502
- implementation of, 499–512
- licensing for, 494
- load balancing in, 503–512
- SecuRemote in, 450–453
- S/Key and, 196
- software-based solutions for, 502
- solution providers for, 502–503
- State Synchronization in, 493–499

High Availability management modules. *See also* secondary management module
- about, 178–183
- certificate authority errors in, 184–185
- failover in, 182–183, 182*f*
- synchronizing, 179, 179*f*

High Availability VPNs, gateway clusters for, 401–402

host
- grouping, for load balancing, 504
- for Management GUIs
  - configuring, 63–64
  - fetching, 108
- number of, error on, 146–147
- specification of, in rules, 86

hostid, license based on, 24
host objects. *See also* node host objects
  creating, with `dbedit`, 144
hosts file, in Windows NT, 554
hotfix accumulators, about, 145
hotfixes, for Windows 2000, 557
hot standby, definition of, 494
HTML, weeding, 276
HTTP buffer, increasing size of, 293–294
HTTP connection
  authenticated, logging on, 135
  file descriptors for, 295–296
  tunneled, blocking, 288–289
HTTP proxy, FireWall-1 as, 250
HTTP Security Server
  about, 271–298
  CVP with, 282–284
  debugging, 319–320, 320*t*
  enabling, 271–272
  error messages in, 292–293
  instances of, increasing, 294
  memory for, 295, 298
  performance tuning, 293–296
  port for, 297–298
  requests forwarded by, to caching proxy server, 286
  sample configuration for, 330–333
  schemes permitted by, 291–292
  troubleshooting, 297–298
  UFP with, 278–282
  Web site access through
    issues with, 290, 290*t*–291*t*
    troubleshooting, 298
HTTP server, user authentication properties for, 223
HTTP service
  authenticating over different ports, 251
  authentication with, on remote site, 253
  Client Authentication over, 202, 204, 204*f*, 228
    custom pages for, 254–255
    debugging, 320*t*
  for Clientless VPN, 244–246, 245*f*, 246*t*
  connections dropped with, 258
  User Authentication for, 198–199, 199*f*
    rule order and, 224
HTTPS server, internal, authenticating access to, 251–252, 253*f*
HTTPS service
  Client Authentication over, 202
  User Authentication for, 198–199
HTTPS traffic, outbound
  authenticating, 251
  Content Security for, 288
HTTP traffic
  Content Security for, 271–298
    sample configuration for, 330–333
  filtering, 272–278
    on other ports, 285–286
    UFP for, 271, 278–282
hub-and-spoke model, for VPN, 404–405

I

IANA (Internet Assigned Numbers Authority), 335
ICA (Internal Certificate Authority)
  in High Availability management configuration, 184–185
  random number generator for, 47, 47*f*
  SIC for, 163
ICA certificates
  exporting, 392
  on management station, deletion and, 175
  revoking, 185–186
ICANN (Internet Corporation for Assigned Names and Numbers), 335
ICMP packets
  blocking, 150
  NAT support for, 352
ICMP Redirect, dual NAT and, 353–354, 354*f*
ICMP requests, accepting, 83, 98, 98*f*
ICMP service object, about, 77
ICMP traceroute, firewall handling of, 7–8
identifiers, in INSPECT, 525, 525*t*
ident packets
  accepting, 99–100, 99*f*
  rejecting, 158–159
  required by FTP, 157
If Via, in rules, 86
IGMP packets, accepting, 99, 99*f*
IKE
  about, 386
  aggressive mode for, 392
  debugging with, 408
  maximum concurrent connections for, 408
  rules for, 407, 407*f*

IKE (*cont.*)
over TCP, SecureClient options for, 460
in traditional mode, settings for, 390–392, 391*f*
IKE pre-shared secrets
encryption key for, 242
with L2TP, 447
simplified mode and, 388
for VPN gateways, 401
IKE rekey, VPN failure after, 409–410
incremental sync, definition of, 494
individuals, in security policy, 17
information confidentiality, policy on, 564
INSPECT
definition of, 521
documentation of, 521
purpose of, 522
rulebase converted to, 529–536, 530*f*
sample of, 536–543
syntax for, 522–529
installation image, for SecureClient, 465–468
Install On
in rules, 87
in S/Key, 214
Insufficient Information problem, 223–225
interface
definition of, 143
different rules for, INSPECT for, 538–539
fetching, 108
support for, 143
Internal Certificate Authority. *See* ICA
Internet, DNS definitions for, 159
Internet Assigned Numbers Authority (IANA), 335
Internet connection, sharing, SecuRemote and, 473
Internet Corporation for Assigned Names and Numbers (ICANN), 335
Internet Explorer, HTTP Security Server and, 298
Internet Relay Chat (IRC), ident used by, 100
Internet Service Providers, policy on, 565
interoperable device objects, about, 72
Intranet, DNS definitions for, 159
IP address
for connection hiding, 340
determining, with IP Pool NAT, 477
in domain objects, 71
for gateway cluster, 402, 402*f*
more than four, 515
in State Synchronization configuration, 495–496
in INSPECT, 526
Internet, in internal network, 443
license based on, 24–25
for Management GUIs, configuring, 63–64
for management station, moving management module and, 174–176
for MX records, in SMTP Security Server, 306, 308
for NAT
binding to loopback interface, 354–355
determining, 345
in double-blind network, 375
in network migration, 370
in simple network, 366
of NIC, in encryption domain, 479
in node-limited license, 21–22, 147
for remote management, installation of, 46, 46*f*
virtual, for High Availability, 499–500
for VPN clients
assigned in Office Mode, 443–444, 445
conflicting, 442
IP Options
dropping, logging on, 134
enabling, 84
packet checked against, 342
IP Pool NAT
allocating to Office Mode clients, 446
asymmetric routing and, 443
determining IP address with, 477
for SecuRemote connections, 451, 451*f*
in VPN, 397
IP routing, enabling
in Windows 2000, 558
in Windows NT, 553
IPSec
about, 385–386
starting, for L2TP, 449
UDP encapsulation for
fragmentation with, 477–478
SecureClient option for, 460
IPSec rekey, IKE rekeys and, 409–410

IPSO
  FireWall-1 on, 31–32
    installation of, 40
  firewall module on, installation of, 49–52
  packet sniffer in, 355
  preinstallation of, 35–36
  proxy ARP on, 347
  static routes on, 348–349
  tweaking, 577
IPv4 address space, 335–336
IPv6 address space, 336
IPxxx. *See* IPSO
IRC (Internet Relay Chat), ident used by, 100
ISPs (Internet Service Providers), policy on, 565

J
JAVA code, blocking, 276

K
KaZaA, blocking, 288–289
kernel URL logging, HTTP Security Server and, 295
kernel variables, modifying, 141–142
KEY, in connections table, 527
key exchange, for VPN, settings for, 390

L
L2TP clients, configuring for, 446–450
label, in domain names, 454–456
lab network, for testing OS configuration, 36
Large Scale Manager
  gateway management with, 189
  purpose of, 56
LDAP (Lightweight Directory Access Protocol)
  about, 197–198
  Global Properties for, 235–236, 235*f*
  integrating, 234–243
  license for, 24
LDAP account unit
  authentication properties for, 241–242, 241*f*
  properties of, 236–237, 237*f*
  server added to, 237–238, 237*f*
LDAP group
  properties for, 242–243, 242*f*
  rule for, 243
  in user creation, setting for, 210
LDAP server
  adding to account unit, 237–238, 237*f*
  branches of, specifying, 240, 240*f*
  encryption properties for, 239–240, 239*f*
  properties of, 238–239, 238*f*
  schema checking for, 234–235
  SecureClient options for, 462
LDAP users, FireWall-1 use of, 247
LEA (Log Export API), 270
license(s)
  adding, 171
  for evaluation, 24–25
  for firewall module, installation of, 50–51
  for High Availability, 494
  for High Availability management modules, 178
  installation of, 171
  issues with, 24–25, 109
  for management console, installation of, 45, 45*f*
  obtaining, 24–26
  for planning and installation, 20–26
  for State Synchronization, error on, 516
  third-party software and, 269
  updating, remotely, 169–171
license key, for licenses, 24
Lightweight Directory Access Protocol. *See* LDAP
link-local addresses, 339
Linux
  FireWall-1 on, 32–34
  packet sniffer in, 355
  securing, 559–561
  tweaking, 560–561
load balancing
  dynamic, 507–508, 508*f*
    with NAT, 509, 509*f*
  in High Availability, 503–512
  static, 504–505, 505*f*
  with switches, 506, 507*f*
localhost, connection to Management GUIs, 64
local interface anti-spoofing, error on, 145
local license, 24
location, in user properties, 216, 216*f*
log
  on Client Authentication, 229
  grace period in, 135
  for High Availability management modules, 181, 181*f*

log (*cont.*)
  location of, 139–140, 139*f*
  maintenance of, 136–140
  number of, issues with, 190
  rule viewed from, 126–127
log, system, error messages in, 145–148
log buffer, full, 148
Log Export API (LEA), 270
logging
  enabling
    for Linux, 560–561
    in SPARC Solaris, 551
  on firewall module, local, 164–165
  guidelines for, 123–124
  of implied rules, 84, 98
  in OS security, 38–39
  in rules, 86–87
  to syslog, 142–143
  in usage policy, 565
login accounts, generic, issues with, 39
login name, for management users, 61
Log Manager. *See* SmartView Tracker
logon, SecureClient options for, 464–465, 464*f*
Log Viewer. *See* SmartView Tracker
Lumeta, for network topology, 14

M
MAC address
  for ARP
    determining, 345–347
    in double-blind network, 375
    in network migration, 370–371
    in simple network, 366
    verifying, 357–359
  for State Synchronization, changing, 512–513
machine name
  for Windows 2000, 557
  for Windows NT, 553
mail alerts, 136
management (organizational), security policy supported by, 16, 18
management console. *See also* management station; SmartConsole
  installation of, 40–49
  license for, 22
  purpose of, 20–21
  in single-gateway products, 22
Management GUI applications. *See also specific applications*
  about, 55–66
  administrator accounts for, 39
  backward compatibility of, 106
  demonstration mode of, 66
  hosts for, configuring, 63–64
  installation of, 44, 44*f*
  license for, 23
    error on, 109
  purpose of, 21
  reliance on, issues with, 190–191
  over slow connections, 107–108
  status of, 113, 113*f*
  users for, configuring, 58
management module
  in FireWall-1, 162
  highly available (*See* High Availability management modules)
  moving, 172–178
    from standalone gateway, 176–178
  NAT on, remote management from, 165
  one-time password for, 163–164, 164*f*
  testing, after migration, 176
management object
  deleting, after moving, 175
  IP address of, moving management module and, 174–176
  log rotation with, 137
management station. *See also* management console
  fingerprint of, 48, 48*f*
  installation of, 40–49
  limitations on moving, 176
  synching clock of, to firewall module, 184
management users
  configuring
    in Policy Editor, 60–63, 60*f,* 61*f,* 62*f,* 63*f*
    in SmartDashboard, 58
manual rules, for NAT, 339
max_conns_per_site setting, for SMTP Security Server, 305
max_conns setting, for SMTP Security Server, 305
max_ips_per_mx_node setting, for SMTP Security Server, 306
max_mail_size setting, for SMTP Security Server, 305

max_mails_per_conn setting, for SMTP Security Server, 305
max_mx_node_per_mail setting, for SMTP Security Server, 305
maxrecipients setting, for SMTP Security Server, 306
MD5 Challenge, authentication with, 447
memory
  for HTTP Security Server, 295, 298
  used for state tables, 576, 576*f*
Meshed Community, creating, 397–401, 398*f*, 399*f*, 400*f*
<methods>, in SIC policy rules, 188
Microsoft Internet Explorer, HTTP Security Server and, 298
Microsoft Networking, SecureClient and, 453–457
Microsoft Visio, for network topology, 14
MIME type, filtering on, 309–310
modules. *See also specific modules*
  connections between, 162, 162*f*
  states of, 114, 114*t*
Motif GUI, license for, 23
MTA, connection failure at, 312
MTU Adjuster, 478, 478*f*
multicast addresses, 335–336
MX records, under SMTP Security Server
  firewall as, 310
  IP address of, 306, 308
  number of, 305–306
  subject of, 310

N

NAT (Network Address Translation)
  disadvantages of, 337–338
  for double-blind network, 374–377, 374*f*
  dual, 353–354, 353*f*
  dynamic load balancing with, 509, 509*f*
  encryption and, 405
  in FireWall-1, 336, 339–343
  firewall bypassed and, 352–355
  for firewalls, 15
  implementation of, 343–351, 344*f*
    samples of, 365–377
  IP addresses for
    binding to loopback interface, 354–355
    determining, 345
  L2TP and, 450
  limitations of, 351–355
  network migration with, 369–373, 369*f*
  network objects for, 349, 349*t*
  proxy ARPs for, setting up, 345–347
  purpose of, 336
  remote management with, 165
  SecureClient with, firewall access by, 469
  SecuRemote with, 468–469
  simple network with, sample of, 365–369, 365*f*
  State Synchronization and, 499
  static host routes for, setting up, 348–349
  troubleshooting, with packet sniffer, 355–364
  types of, 339–340
  with VPN, 405–406
    IP conflicts with, 442
  in VPN Community, disabling, 400–401
NAT rules
  compiled, in INSPECT, 532–534, 532*f*
  creating, 350–351, 351*f*
  in double-blind network, 377, 377*f*
  dual, 353–354, 353*f*
  encryption and, 405, 405*f*
  manual, 339
  in network migration, 373, 373*f*
  packet checked against, 342
  in simple network, 368, 368*f*
NetBIOS
  name resolution in, SecuRemote and, 456–457
  over TCP, disabling, in Windows 2000, 558
network
  double-blind, NAT for, 374–377, 374*f*
  Internet IP addresses routed through, 443
  migrating, with NAT, 369–373, 369*f*
  size of, security needs and, 9–11
  unsecured operating systems on, 36
Network Address Translation. *See* NAT
network objects
  about, 70–71, 70*f*
  compiled, in INSPECT, 531
  creating, with `dbedit`, 144–145
  defining, 92, 93*f*
  for encryption domain, 389
    for site addition, 417
    for three-site VPN, 413–414
  for NAT implementation, 349, 349*t*
    in double-blind network, 376, 376*t*
    in network migration, 371, 371*t*–372*t*
    in simple network, 367, 367*t*
  number of, issues with, 188

- network topology
  - anti-spoofing settings in, 80–81, 81*f*
  - for Check Point gateway, 68–69, 69*f*
  - creating, 91
  - defining, error on, 148
  - in firewall planning, 13–15
  - for gateway cluster, 486, 486*f*
  - in rulebase creation, 91–92, 92*f*
  - SecureClient options for, 461, 461*f*
  - SecureClient request for, port for, 473
  - as VPN domain, 389, 390*f*
- network traffic, order of operations in, 341–343
- newline characters, FTP problems with, 156–157
- NIC, mixing with dial-up adapters, SecuRemote and, 479
- node gateway objects, about, 70
- node host objects, about, 70
- node-limited firewalls
  - in HA configuration, 494
  - host number error in, 146–147
  - license for, 21–22
  - in single-gateway products, 22
- node objects (workstation objects)
  - about, 70–73
  - defining, 92, 94*f*
  - externally managed, about, 70
  - in FireWall-1 upgrade, 52–53
  - for RADIUS server, creating, 232–233
  - for TACACS, 233, 233*f*
- Nokia Crypto Cluster, VPN issues with, 409
- Nokia IP Clustering, load balancing in, 504
- Nokia IP Security Platform. *See* IPSO
- NT domain. *See* Windows NT domain
- numbers, in INSPECT, 526

O

- objects
  - creation of, from command line, 143–145
  - defining, 92–94
  - naming, 104, 105*t*–106*t*
  - types of, 66–73
  - viewing, in SmartDashboard, 57
- objects_5_0.C
  - corruption of, 147–148
  - editing, 102–103
  - in rulebase compiling, 529–530
- objects list, in SmartDashboard, 57
- objects tree, in SmartDashboard, 57
- OBSEC Management Interface (OMI), 270
- Office Mode, for SecureClient, 442–446
  - anti-spoofing in, 445
  - configuring, 444–446, 444*f*
  - connections in, 446
  - issues resolved by, 442–444
  - limitations of, 446
  - Microsoft Networking and, 453
  - with multiple interfaces, 445
- OMI (OBSEC Management Interface), 270
- one-request method, for UFP caching, 294–295
- one-time password (OTP)
  - for firewall module, 163–164, 164*f*
  - for management module, 163–164, 164*f*
  - *vs.* static password, 194
- OpenLDAP v1, file for, 567–569
- OpenLDAP v2, file for, 571–573
- Open Platform for Security (OPSEC), about, 270
- operating system. *See* OS
- OPSEC (Open Platform for Security), about, 270
- OPSEC application
  - for CVP server, 283, 283*f*
  - for UFP server, 279–280, 279*f*, 281*f*
- organization, security needs of, 9–11
- OS (operating system)
  - for FireWall-1
    - configuration of, 36
    - installing, 34–39
    - securing, 37–39, 545–561
    - selecting, 27–34
  - firewall limitations and, 2–3
  - of management module, moving module and, 172–173
  - patches for, 38
- OSE device objects, about, 71
- os parameter, of `cpstat`, application flavors for, 119*t*
- OS password
  - about, 194
  - enabling, on firewall, 219
- Other type services, INSPECT for, 536
- OTP. *See* one-time password
- ownership, in security policy, 17

P

- packages
  - for Linux, 559–560
  - for SPARC Solaris, 546–550

- packet
  - accepting based on previous packet, INSPECT for, 537–538
  - fragmentation of, in VPN, 411
  - inspection of, with `fw monitor`, 541
  - processing of, in FireWall-1, 342
  - virtual defragmentation of, error on, 146
- packet filters
  - overview of, 3–4
  - Passive FTP handled by, 6
  - Stateful Inspection and, 5
  - traceroute handled by, 7–8
- packet integrity check, in VPN, 379
- packet sniffer
  - for NAT troubleshooting, 355–364
  - password discovered with, 194
- Passive FTP, firewall handling of, 5–6
- password(s)
  - about, 193–198
  - erased, SecureClient and, 460
  - for management users, 59
  - in S/Key, 214
    - resetting, 253–254
  - user, changing, 253
- password, one-time. *See* one-time password (OTP)
- password number, in S/Key, 195
- <peers>, in SIC policy rules, 187
- permissions, defining, for management users, 61, 61*f*
- .pf file, in rulebase compiling, 529–531
- `ping`, fragmented packet troubleshooting with, 477–478
- PKI (Public Key Infrastructure), 270
- Pnote devices, errors on, 517
- Point-to-Point Tunneling Protocol (PPTP), INSPECT for, 537
- Policy Editor. *See also* SmartDashboard
  - about, 56–58, 57*f*
  - crashing of, 108–109
  - demonstration mode of, 66
  - NAT rules in, 339
  - purpose of, 55
  - restrictions on, 65, 65*f*
  - on SPARC Solaris, 30
  - troubleshooting, 107
- policy names, in FireWall-1 upgrade, 53
- policy routing, load balancing with, 505, 506*f*
- policy server, SecureClient and, 434
  - logon to, 459
- <ports>, in SIC policy rules, 187
- postmaster, e-mail address for, 306
- postmaster setting, for SMTP Security Server, 306
- PPPoE, SecuRemote and, 476
- PPTP (Point-to-Point Tunneling Protocol), INSPECT for, 537
- pre-shared secrets
  - *vs.* certificates, 387
  - for IKE
    - encryption key for, 242
    - simplified mode and, 388
    - for VPN gateways, 401
- privacy, in usage policy, 565
- private key, in public-key cryptography, 381
- protocol(s). *See also specific protocols*
  - NAT incompatibility with, 351–352
  - for State Synchronization, 494
  - for Windows 2000, 556–557
  - for Windows NT, 552
- proxied conns, entries in, increasing, 293
- proxies. *See* application proxies
- proxy ARPs. *See also* ARPs
  - setting up, for NAT implementation, 345–347
- pseudo-random number generator, in encryption, 380–381
- public key
  - certification of, 383
  - in public-key cryptography, 381
- public-key cryptography, asymmetric encryption in, 381
- Public Key Infrastructure (PKI), 270

R

- RADIUS (Remote Access Dial-In User Service)
  - about, 197
  - integrating, 231–233
  - settings for, for User Authentication, 215, 215*f*
- RADIUS server, on NT domain, 248
- RADIUS server object, creating, 232–233, 232*f*
- RADIUS service, creating, 232
- RADIUS users, FireWall-1 use of, 247
- random keystrokes
  - in firewall installation, 51
  - in management console installation, 47, 47*f*
- random number generator, seeding, 47, 47*f*
- registers, in INSPECT, 526

- registry, hacking, in securing Windows NT, 554–555
- Reject action, in rules, 86
- reject short circuit, in INSPECT, 523*t*
- Remote Access, SCV for, 435–436, 435*f*
- Remote Access community, gateway object for, for SecuRemote, 427
- Remote Access Dial-In User Service. *See* RADIUS
- remote administration
  - IP address for, installation of, 46, 46*f*
  - in Windows NT/2000, 28–29
- remote management
  - capabilities of, 165–171
  - with NAT, 165
  - troubleshooting, 183–188
- Remote Procedure Call (RPC), support for, 149
- Reporting Tool, purpose of, 56
- resend_period setting, for SMTP Security Server, 303
- resources, definition of, 271, 271*t*. *See also specific types*
- reverse proxy, FireWall-1 as, 250
- revision control, for security policy, setting for, 85
- RFC1918 addresses, 338
- RIP, accepting, 97, 97*f*
- rlogin Security Server, debugging, 320*t*
- rlogin service
  - Client Authentication over, 228
  - User Authentication for, 198–199
    - rule order and, 224
- Roaming user profiles, with SecureClient, 465
- ROBO Gateway Profile, 189–190
- routers
  - firewalls compared to, 1–2
  - packet filtering in, 3
- routing
  - asymmetric
    - Office Mode and, 444
    - VPN and, 443
  - in firewall OS, 39
  - for Office Mode network, 446
- RPC (Remote Procedure Call), support for, 149
- RPC locator, Windows 2000 and, 558–559
- RPC service object, about, 77, 77*f*
- RST packets
  - dropping, 155
  - SYN packets followed by, in NAT troubleshooting, 359–361
- rule(s). *See also* NAT rules; VPN rules
  - changing, responsibility for, 17
  - for Client Authentication, 227, 227*f*, 266*f*
    - error on, 256
  - for Clientless VPN, 244, 244*f*
  - for client-to-site VPN, 483, 483*f*
  - conflicting, 101, 101*f*
  - defining, 94–95
  - for Desktop Security, 436–438, 436*f*, 437*f*
  - for FTP Content Security, 300, 300*f*, 329*f*
  - for groups, 218
  - hierarchical management of, 189
  - for HTTP Content Security, 278, 278*f*
    - with CVP, 284, 285*f*
    - with UFP, 282, 282*f*
  - implied, logging, 84, 98
  - for interfaces, 106–107
  - for LDAP group, 243
  - for multiple-entry point SecureClient, 491, 491*f*
  - for NAT implementation, 350, 350*f*
  - necessary, 99–100
  - number of, issues with, 188
  - order of, 88–90, 89*f*
    - guidelines for, 90
    - Security Servers and, 319
    - setting, 82
    - in User Authentication, 223–225
  - parts of, 85–87
  - sample, 87–88, 88*f*
  - for SecureClient with gateway cluster, 486–487, 487*f*
  - for Session Authentication, 225, 225*f*
  - in SIC policy, 187
  - for SMTP Content Security, 310*f*, 326*f*, 329*f*
  - for TCP Content Security, 317, 317*f*
  - for User Authentication, 221–223, 222*f*
  - for users, 218
- rulebase
  - about, 85–90
  - components of, 66–85
  - converted to INSPECT, 529–536, 530*f*
  - creating, 90–101
    - network topology in, 91–92, 92*f*
    - objects in, defining, 92–94
  - disappearance of, 107
  - e-mail directed through, 308
  - e-mail not allowed by, notification on, 305

importing, 107
for multiple-entry point SecureClient, 491, 491*f*
for NAT implementation, 350, 350*f*
in double-blind network, 377, 377*f*
in network migration, 373, 373*f*
in simple network, 368, 368*f*
number of, issues with, 188–189
order of operations in, 88–90, 89*f*
packet checked against, 342
sample of, 95*f*
for SecureClient with gateway cluster, 486–487, 487*f*
for SecuRemote, 431–432, 432*f*
for Session Authentication, 264*f*
for User Authentication, 262, 262*f*
rulebasese.fws, editing, 102–103
rundir setting, for SMTP Security Server, 304

S

SA (Security Associations)
about, 386
simplification of subnets in, 410
SAA (Secure Authentication API), 270
Safe@ products, license for, 23
SAM. *See* SmartDefense
SAMP (Suspicious Activity Monitoring Protocol), 270
SANS Institute, security policy documents of, 20
satellite gateway, in Star Community, 398
scan_period setting, for SMTP Security Server, 303
scheduled event object, 78, 79*f*
schema checking, for LDAP server, 234–235
script, as alert action, 135–136
SCV (Secure Configuration Verification), for Remote Access, 435–436, 435*f*
SDL. *See* Secure Domain Logon
secondary management module
failover to, 182–183, 182*f*
installing, 178–179, 178*f*
secret key, in S/Key, 195
settings for, 214
Secure Authentication API (SAA), 270
SecureClient
adding site to, 441–442, 441*f*
anti-spoofing in, 445
certificate obtained with, 430–431
command line interface for, 474–475, 474*t*–475*t*
configuring, 439, 440*f*
connection mode for, 458*f*, 459
custom prepackaged version of, 442, 457–468
DNS traffic encrypted for, 434
with gateway clusters, sample configuration for, 484–487, 485*f*
installation of, 438–442
image for, 465–468, 466*f*
options for, 463–464, 463*f*
profiles for, 457, 458*f*
introduction to, 425–426
license for, 24, 426
Microsoft Networking and, 453–457
with multiple entry points, sample configuration for, 488–491, 488*f*
with NAT, firewall access by, 469
Office Mode for, 442–446
options for, 459–462, 460*f*
policy server and, 434
profiles for installation of, 457, 458*f*
sample configurations for, 481–491
vs. SecuRemote, 425–426
third-party VPN and, 473
topology request by, port for, 473
traceroute with, 411
SecureClient Packaging Tool, 56, 457–468
Secure Configuration Verification (SCV), for Remote Access, 435–436, 435*f*
Secure Domain Logon (SDL)
platforms compatible with, 457
for SecureClient
Microsoft Networking and, 453
options for, 465
Secure Internal Communication. *See* SIC
SecuRemote. *See also* SecureClient
binding to all adapters, 479
behind Check Point gateway, 470, 470*f*
communication ports blocked in, 476
configuring, 426–442
custom adapters and, 476
disabling at startup, 472
encrypted session to, initiating, 469–470
failover of, gateway cluster for, 450, 488–491, 490*f*
interface bound to, 439

SecuRemote (*cont.*)
  introduction to, 425–426
  IP Pool NAT for, 451, 451*f*
  license for, 24, 426
  with NAT, 468–469
  NetBIOS name resolution and, 456–457
  NT file permissions and, 478
  outbound connections allowed to, code for, 536–537
  behind proxy, 471–472, 471*f*, 472*f*
  sample configurations for, 481–491
  vs. SecureClient, 425–426
  site added to, 476
  troubleshooting, 476–480
  user creation for, 428–431, 428*f*
SecuRemote DNS server, 454, 454*f*, 455*f*
Secure Platform (SPLAT), for Linux installation, 32–34
secure server, license for, 22
Secure Sockets Layer. *See* SSL
SecureUpdate. *See* SmartUpdate
SecurID
  about, 196, 196*f*
  authentication failure with, 258–259
  integrating, 230–231
  settings for, 216
SecurID users, FireWall-1 use of, 247
Security Associations (SA)
  about, 386
  simplification of subnets in, 410
Security Focus, 38
security policy
  configuring, frequently asked questions about, 101–107
  default filter and
    changing, 539–540
    sample of, 581–582
  developing, 15–20
  enforcement of, 16
  example of, 19–20
  files in, 102
  firewall implementation and, 18
  firewall limitations in, 2
  guidelines for, 16–18
  in INSPECT, 534–536
  installation of, 100–101, 100*f*
    Client Authentication and, 257
    errors on, 147–148
    on gateway cluster, inconsistencies in, 514–515, 516
    setting for, 85
  large-scale environment, 188
  management support for, 16
  reinstallation of, 104
  remotely controlling, on firewall module, 166–167
  responsibility for, 17, 19–20
  revision control for, 85
  in rule generation, 94–95
  specifics in, 17–18
Security Servers. *See also specific servers*
  connections to
    failover of, 494
    origin of, 318
  debugging, 319–321, 320*t*
  enabling, 221
  issues with, 318–319
  rule order and, 319
  State Synchronization and, 499
seed value, in S/Key, 195
  settings for, 212
selection criteria, in SmartView Tracker, 123–124
server object
  for LDAP account unit, 236
  for RADIUS, 232–233, 232*f*
  for TACACS, 233, 233*f*
service(s)
  "any," 104, 104*t*
  Client Authentication for, 202
  common questions about, 148–150
  disabling
    in SPARC Solaris, 550–551, 551*t*
    in Windows 2000, 557–558
    in Windows NT, 554
  excepting from State Synchronization, 513
  in FireWall-1 upgrade, 53
  not running, RST packets from, 360–361
  in OS security, 38
  of Other type, INSPECT for, 536
  removing, from Linux, 560
  Session Authentication for, 201
  slow, 158
  User Authentication for, 198
  through VPN, not encrypting, 399–400
  in Windows 2000, 556–557
  in Windows NT, 553

Service, in rules, 86
Service Level Agreement (SLA), violation of, log/alert on, 134
service objects
about, 73–77
creating, 73
service packs
for Windows 2000, 557
for Windows NT, 556
service port, error message about, 145–146
<services>, in SIC policy rules, 187
Session Authentication
in cleartext, 256
for Client Authentication, 202, 228
with Content Security, 256, 319
encryption for, 256
error on, 255
explanation of, 201, 201*f,* 202*f*
limitations of, 207–208
rule for, 225, 225*f*
sample configuration for, 263–264
setting up, 225–227
SSL for, 226
usage guidelines for, 207*t*
short circuit, in INSPECT, 523, 523*t*
SIC (Secure Internal Communication)
about, 163–164
debugging, 186–188
dynamic addressing and, 184
failure of, in remote management, 183–184
general failure of, 184
one-time password for, establishing, 51–52
for OPSEC application, 280
random number generator for, 47, 47*f*
resetting, 185–186
with secondary management station, 179
SIC certificates, clock sync and, 184
SIC key, copying, to destination management module, 173–174
SIC name, in moving management module, 175
SIC policy, debugging, 187–188
Sign On Method, for Client Authentication, 228–229, 228*f*
silent installation, for SecureClient, 462–463, 463*f*
Simple Object Access Protocol (SOAP), for URI resource, 278, 278*f*
single-gateway products
about, 22
in HA configuration, 494
S/Key
about, 195–196
enabling, on firewall, 219
resetting passwords for, 253–254
settings for, 212–215, 213*f*
S/Key generator, 195, 195*f*
SLA (Service Level Agreement), violation of, log/alert on, 134
small-office environments, Check Point Express for, 23
SmartCenter. *See* SmartConsole
SmartClients
backward compatibility of, 106
installation of, directory for, 44, 44*f*
license for, 22–23
SmartConsole. *See also* management console
files modified by, 65
in FireWall-1, 162
license for, 22–23
reliance on, 190–191
SmartDashboard. *See also* Policy Editor
about, 56–58, 57*f*
authentication configured in, 163–164
crashing of, 108–109
purpose of, 55
reliance on, 190–191
restrictions on, 65, 65*f*
rules viewed in, 126–127
troubleshooting, 107
users created in, 208
SmartDefense (SAM)
FTP commands enabled in, 301, 301*f*
log/alert settings for, 134
SmartDirectory, license for, 24
SmartMap, crashing of, 108–109
"smart" SMTP server, 311, 311*f*
SmartUpdate (SecureUpdate)
license update with, 169, 171, 172*f*
purpose of, 56
SmartView Monitor, purpose of, 56
SmartView Status. *See also* Status Manager
about, 111–118, 112*f*
purpose of, 56
SmartView Tracker (Log Viewer)
about, 121–131, 121*f*

SmartView Tracker (*cont.*)
  active mode in, 127–131, 127*f*, 127*t*–128*t*
  audit mode in, 131, 132*f*, 132*t*
  bottleneck in, 190
  demonstration mode of, 66
  fields in, 122*t*–123*t*
  IP resolution timeout for, 135
  purpose of, 56
SMTP resources, for Content Security, 306–310, 307*f*, 308*f*, 309*f*
  sample configuration for, 323–326, 324*f*, 325*f*, 326*f*
SMTP Security Server
  about, 302–316, 303*f*
  CVP with, 312, 325, 325*f*
  debugging, 320*t*
  mail stuck in, 313–316
  MX records used by, issues with, 311
  parameters for, 302–306, 304*f*
  sample configuration for, 322–326
  spam and, 311–312
  troubleshooting, 312–316
SMTP server, "smart," 311, 311*f*
SMTP traffic
  Content Security for, 302–316, 303*f*
    sample configuration for, 322–326
  ident used by, 100
`snoop`
  expressions for, 364, 364*t*
  flags for, 363, 363*t*
  for NAT troubleshooting, 355–361
SOAP (Simple Object Access Protocol), for URI resource, 278, 278*f*
social engineering, 2
SOCKS, ICMP proxied by, 8
software, uninstalling, for security, 37
Solaris x86, FireWall-1 on, 29. *See also* SPARC Solaris
Sonicwall, VPN issues with, 409–410
source, in rules, 86
source hide NAT, 340
source static NAT, 339–340
spam, SMTP Security Server and, 311–312
SPARC Solaris
  FireWall-1 on, 29–30
  packet sniffer in, 355
  patching, 546
  securing, 545–552
  tweaking, 551–552, 577
specific sign-on, for Client Authentication, 202–205, 206*f*, 227
SPLAT (Secure Platform), for Linux installation, 32–34
split-horizon DNS, 159
  NAT and, 352–353
spool files, in SMTP Security Server, 313–316
spool_limit_scan_period setting, for SMTP Security Server, 304
spool_limit setting, for SMTP Security Server, 304
Src, in rule enforcement, 87
SSH, for Management GUI access, 64
SSL (Secure Sockets Layer)
  FTP over, 157–158, 158*t*
  for LDAP server, 239–240, 239*f*
  for Session Authentication, 226
  in SIC, 163
standard sign-on, for Client Authentication, 202–205, 205*f*, 227
Star Community, 398, 404–405, 404*f*
Stateful ICMP replies, accepting, 98
Stateful Inspection
  in FireWall-1, 8–9
  overview of, 5
  Passive FTP handled by, 6
  of TCP connections, problems with, 150–156
  traceroute handled by, 8
statements, in INSPECT, 524
State Synchronization
  asymmetric routing and, 500–501
  checking, 512
  configuration of, 495–497
  definition of, 494
  error messages with, 514–520
  frequently asked questions about, 512–513
  in High Availability, 493–499
  limitations of, 498–499
  MAC address used by, changing, 512–513
  network used for, 497, 498*f*
  platform interoperability in, 513
  protocol for, 494
  service not synchronized with, 513

state tables. *See also* address translation tables; connections table
  of firewall module, remote viewing of, 167–169
  memory used for, 576, 576*f*
  number of entries in, 575–576
static host routes
  for load balancing, 504
  for NAT implementation, 348
    in double-blind network, 375, 375*f*
    in network migration, 371
    in simple network, 367
static load balancing, 504–505, 505*f*
static password, problems with, 194
static tables, creating, with INSPECT, 528
status information, interval for fetching, 135
Status Manager, 135. *See also* SmartView Status
Stealth rule, 99, 99*f*
streaming media, preventing access to, 287–288
subnet
  firewall and, 15
  simplification of, in IPSec SAs, 410
support, end-user, for SecuRemote, 426
Suspicious Activity Monitoring Protocol (SAMP), 270
SVN Foundation
  alerts defined for, 115–116, 115*f*
  status of, 113, 113*f*
switches, load balancing with, 506, 507*f*
symmetric encryption, definition of, 381
SYN-ACK packets, unexpected, 155
sync buffer, error on, 516, 517–519
SYN packets
  dropping, 155
  in NAT troubleshooting, 357–359
    followed by RST, 359–361
syslog, logging to, 142–143
system log, error messages in, 145–148

T

table, for SecuRemote clients, 469–470
TACACS/TACACS+ (Terminal Access Controller Access Control System)
  about, 197
  integrating, 233–234
  settings for, for user, 216, 216*f*
TACACS users, FireWall-1 use of, 247
TCP ACK packet, Stateful Inspection of, 151
TCP connection
  bidirectional, 153–154
  conflicting, 154–155
  Stateful Inspection of, problems with, 150–156
  timeout on
    adjusting, 156
    disabling, 156
    issues with, 154–155
  unidirectional, 153
`tcpdump`
  expressions for, 362, 362*t*
  flags for, 361, 361*t*
  for NAT troubleshooting, 355–361
TCP/IP stack, SecuRemote bound to, 426
TCP packet
  NAT support for, 352
  out of state, 151–152
TCP port, of management module, 162
TCP resource, for Content Security, 316–318, 317*f*
TCP Security Server
  about, 316–318
  with CVP, 316–317, 317*f*
  debugging, 320*t*
  with UFP, 318
TCP Sequence Verifier, 154, 155
TCP service
  DNS over, accepting, 83, 98, 98*f*
  IKE over, SecureClient options for, 460
  NetBIOS over, disabling, in Windows 2000, 558
TCP service object, about, 73–75, 74*f*, 75*f*
TCP traffic, Content Security for, 316–318
Telnet Security Server, debugging, 320*t*
Telnet service
  Client Authentication over, 202, 203–204, 228
    debugging, 320*t*
  User Authentication for, 198–199
    error on, 258
    rule order and, 224
Terminal Access Controller Access Control System. *See* TACACS/TACACS+
third-party software
  for AIX, 30
  for Content Security, 269
  for High Availability, 502–503
  for IPSO, 32

third-party software (*cont.*)
  for SPARC Solaris, 29
  for Windows NT/2000, 28
time, in user properties, 217, 217*f*
time objects
  about, 77–78, 78*f*, 79*f*
  in rules, 87
timeout
  for Client Authentication, 229, 229*f*
  on SecuRemote authentication, 433
  on TCP
    adjusting, 156
    disabling, 156
    issues with, 154–155
  on UDP, adjusting, 156
  for User Authentication, 223, 262, 263*f*
TIMEOUT, in connections table, 527
timeout setting, for SMTP Security Server, 303
token, hardware
  in Defender, 196–197
  in SecurID, 196, 196*f*
topology. *See* network topology
traceroute
  firewall handling of, 6–8
  through VPN, 410–411
  in Windows, problem with, 148–149
Track, in rules, 86–87
Traffic Monitoring, purpose of, 56
training
  for AIX, 30
  for SPARC Solaris, 29–30
Translate Destination on Client Side option, 342–343
transparent connection, URI resource applied with, 273
trust, levels of, in firewall usage, 1
trust, zones of. *See* zones of trust
tunnel connection
  over HTTP, blocking, 288–289
  URI resource applied with, 273
two-request method, for UFP caching, 294–295

U
UAA (User Authority API), 270
UAM (User-to-Address Mapping), 270
UDP connection
  timeout on, adjusting, 156
  unidirectional, 153
UDP packets
  fragmentation of, troubleshooting, 477–478
  NAT support for, 352
UDP service
  DNS over, accepting, 83, 97–98, 97*f*
  State Synchronization and, 494
UDP service object, about, 76, 76*f*
UDP traceroute, firewall handling of, 7–8
UFP (URL Filtering Protocol)
  about, 270
  caching, 294–295
  OPSEC application for, 279–280, 279*f*, 281*f*
UNIX. *See also* Linux
  command-line mail in, 136
  proxy ARP on, 347
  static routes on, 348
Upgrade Verification Utilities, 53
URI resources, for Content Security, 272–278, 273*f*, 274*f*, 275*f*
  with CVP, 283–284, 284*f*, 285*f*
  rule for, 278, 278*f*
  sample configuration for, 330–333, 331*f*, 332*f*
  with UFP, 280–282, 281*f*
URI specification file, 275
URL, filtering by. *See also* UFP; URI resources
  specifying match for, 274
URL Filtering Protocol. *See* UFP
usage policy
  redirection to, 286–287
  sample of, 563–565
user
  access permissions of, in Windows NT, 555
  adding to RADIUS, 231–232
  in authentication server, FireWall-1 use of, 247
  authentication settings for, 212–218, 213*f*–216*f*
  creation of, 208–218, 208*f*–212*f*
  Office Mode allowed for, 445
  for SecuRemote, creation of, 428–431, 428*f*, 482
  for VPN, creation of, 417–418
  Windows usernames for, access based on, 248
user access, to operating system, securing, 39
User Authentication
  in cleartext, 256
  for Client Authentication, 202, 228
  with Content Security, 319

on each URL, 256
with encryption, 406
in SecuRemote, 426
explanation of, 198–201
failure of, settings for, 221, 223
file downloads allowed with, 287–288, 287*f*
prompt for, absence of, 257
rule for, 221–223, 222*f*
rule order in, 223–225
sample configuration for, 260–262
setup for, 221–225
usage guidelines for, 207*t*
in usage policy, 564
User Authority API (UAA), 270
UserAuthority server, for Session Authentication, 226
User/Client/Session Auth action, in rules, 86
user database
import/export of, 248–249, 248*t,* 249*t*
in User Authentication, 222
user groups
adding users to, 212, 213*f*
creation of, 210, 218, 219*f*
Office Mode allowed for, 445
for policy server, for Desktop Security, 434, 434*f*
User Monitor, purpose of, 56
user password, changing, 253
users file, for RADIUS, adding users to, 231–232
user template, 209, 210
with LDAP server, 241
User-to-Address Mapping (UAM), 270

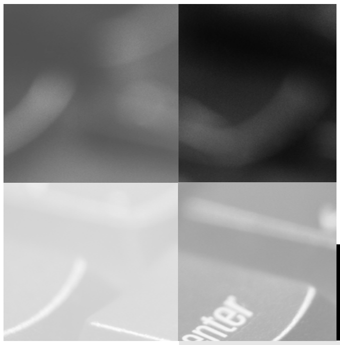
V
VALUE, in connections table, 527
vanish short circuit, in INSPECT, 523, 523*t*
variables, in INSPECT, 526
virtual defragmentation, error on, 146
virtual IP addresses, for High Availability, 499–500
virtual LANs (VLANs), zones of trust in, 15
Virtual Link, statistics for, logging, 135
virtual memory, for HTTP Security Server, 295
Virtual Private Network. *See* VPN
Virtual Router Redundancy Protocol (VRRP)
configuring, 419
for SecureClient with gateway clusters, 484–487
Visitor Mode, 471–472, 471*f,* 472*f*
Visual Policy Editor (VPE)
crashing of, 108–109
in SmartDashboard, 57
VLANs (virtual LANs), zones of trust in, 15
VPE. *See* Visual Policy Editor
VPN (Virtual Private Network). *See also* SecureClient; SecuRemote
adding site to, 415–418, 416*f*
asymmetric routing and, 443
authentication of, changing FQDN and, 175
blocked communication in, 408
certificate criteria for, 394–395, 395*f*
client software for (*See* SecureClient; SecuRemote)
client-to-site, sample configuration for, 481–484, 481*f*
configuration error on, log/alert on, 134
with dial-up networking, 443
encryption in, configuring, 386–402
failover of, with ClusterXL, 504
frequently asked questions about, 403–407
interoperability issues with, 409
introduction to, 379–383
IP addresses for, at different sites, 403–404
key exchange for, log/alert on, 133, 134
license for, 24, 383–384
limiting access to, 403
load sharing in, 511*f*
with ClusterXL, 504
dynamic, 510–512, 511*f*
with policy routing, 505, 506*f*
with NAT, 405–406
packet fragmentation in, 411
packet handling errors in, log/alert on, 134
planning for, 386–387, 387*f*
sample configurations for, 412–422
sharing address space in, 405–406
simplified mode for
configuring, 397–401
Remote Access community rules for, 431, 432*f*
SecuRemote configuration in, 427
vs. traditional mode, 388–389
status of, 113, 113*f*
third-party products for
interoperability with, 403
SecureClient and, 473
three-site, configuration for, 412–415, 413*f*

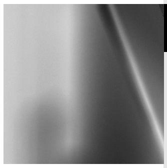
VPN (Virtual Private Network) (*cont.*)
  traceroute through, 410–411
  traditional mode for
    configuring, 389–397
    SecuRemote configuration in, 427, 427*f*
    vs. simplified mode, 388–389
VPN-1
  alerts defined for, 116, 116*f*
  Pro *vs.* Net, 384
VPN-1 control connections, accepting, 83, 96, 96*f*
VPN-1 Embedded NG, license for, 23
VPN Community
  creating, 397–401
  gateway in multiple, 407
  logging traffic on, 135
  NAT disabled in, 400–401
  in simplified mode, 388
  for site addition, 417
  specification of, in rules, 86
  for three-site VPN, 414, 414*f*
vpn parameter, of `cpstat`, application flavors for, 120*t*–121*t*
VPN Routing, 404–405
VPN rules
  for client-to-site VPN, 483, 483*f*
  for encryption, 396, 396*f*
    for SecuRemote access, 431–432
  in FireWall-1, 379
  for multiple-entry point SecureClient, 491, 491*f*
  for SecureClient with gateway cluster, 486–487, 487*f*
  in simplified mode, 401, 401*f*
  for site addition, 417, 417*f*, 418, 418*f*
  for three-site VPN, 415, 415*f*
VRRP (Virtual Router Redundancy Protocol)
  configuring, 419
  for SecureClient with gateway clusters, 484–487
VRRP packets, accepting, 99, 99*f*

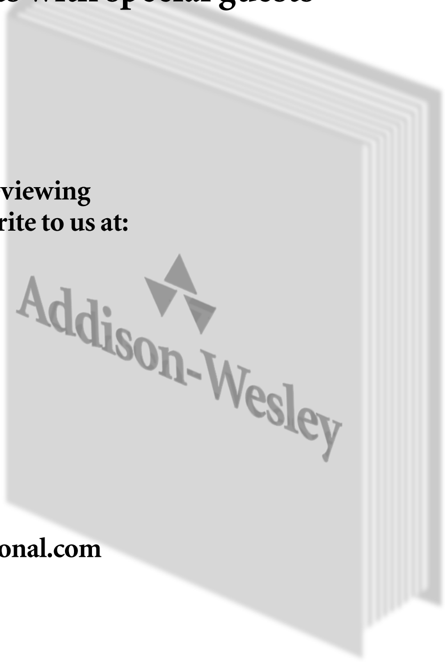
W
wait mode, for Client Authentication, 230
warm standby, definition of, 493
Web sites, access to, through HTTP Security Server, 298
.W file, 529–530
wildcards, definition of, 271, 271*t*
Windows
  ClusterXL failure on, 515
  VPN client software for (*See* SecureClient; SecuRemote)
Windows 9x/ME, Office Mode and, 446
Windows 2000
  command-line mail in, 136
  FireWall-1 on, about, 28–29
  management console on, installation of, 40–49
  packet sniffer in, 355
  proxy ARP on, 347
  securing, 556–559
  static routes on, 348
  traceroute in, problem with, 148–149
Windows NT
  command-line mail in, 136
  file permissions in, SecuRemote issues with, 478
  FireWall-1 on, about, 28–29
  management console on, installation of, 40–49
  packet sniffer in, 355
  proxy ARP on, 347
  securing, 552–556
  static routes on, 348
  traceroute in, problem with, 148–149
  tweaking, 577–579
Windows NT domain
  FireWall-1 integration with, 247–248
  in securing Windows 2000, 557
  in securing Windows NT, 553
Windows NT domain users, FireWall-1 use of, 247
Windows user names, access based on, 248
WINS client, disabling, in Windows NT, 553
WINS requests, forwarding in encryption domain, 456–457
WINS server, defining, for Office Mode, 445
WINS TCP/IP, disabling, in Windows NT, 553
wizards, enabling, 84
words, in naming, reserved, 104, 105*t*–106*t*
workstation objects. *See* node objects
wrapper, for FireWall-1 installation, 40

Y
Yahoo Messenger, blocking or enabling, 150, 150*t*

Z
ZeBeDee, for Management GUI access, 64
zones of trust
  determining, 14–15
  in VLANs, 15






Addison-Wesley