INDEX

Numerics

0 access-list acl_name, 165
0 access-list acl_name command, 165
3DES (triple Data Encryption Standard), 11, 47, 166

A

aaa-server command, 329
access rights, 299–300
access contol list. *See* ACLs
Access VPNs, 5
access-list command, 83, 130
access-list global configuration command, 163
ACLs (access control lists), 142, 300
    crypto, 86–88
    IPSec, 75–76
        configuring, 67
        PIX Firewalls, 224–225
        troubleshooting, 149
    PIX Firewall, 163–165
    wildcard preshared keys, 330
activity, monitoring, 285–294
adaptive security algorithm (ASA), 215
adding
    ACLs, 300
    IPSec LAN-to-LAN connections, 323
    permit statements, 75
    users, 250–251
addresses (IP)
    assigning, 243
    pools, 335
administration
    certificates, 304
    Cisco VPN 3000 Concentrator, 295–304
    files, 302–303
    sessions, 296
Administrators, 299
aggressive mode, IKE, 27
agreements, D-H key agreements, 18–20
AH (Authentication Header), 8, 72, 141
algorithms
    ASA, 215
    HMAC, 20
    HMAC-MD5-96, 21
    HMAC-SHA-1-96, 21
    IPSec, 71
    SHA, 166
Altiga Networks VPN command (Start menu), 254
applications
    IOS, 47–48
    VPN Concentrator, 52
        3000 series, 52–61
        5000 series, 61
applying
    crypto maps, 92–94
    interfaces (PIX Firewall), 174–175
ASA (adaptive security algorithm), 215
assignment, IP addresses, 243
authentication, 123
    CAs, 123, 197–198
    certificate-based, 37–39, 270
    HMAC, 166
    IPSec
        ACLs, 75–76
        checking current configuration, 74–75
        configuring, 67
        defining policies, 71–74
        preparing IKE, 68
        selecting IKE policies, 68–70
        testing peers, 75
    preshare method, 160
    SCEP, 190
    SHA, 166
    VPN 3000 Concentrator, 251
    Xauth, 328–329
Authentication Header (AH), 8, 72, 141

B

Baltimore Technologies, 114
Baltimore Technologies CA servers, 191
booting Cisco VPN 3000 Concentrator, 298
browsers. *See also* interfaces
    Browser Manager, 236
    VPN 3000 Concentrator, 239–251

C

CA (Certificate Authority)
    authentication, 197–198

Baltimore Technologies CA, 191
communication parameters, 196–197
configuring, 199
declaring, 196
devices, 115, 192
Entrust servers, 191
IKE, 24
interoperability, 125–127, 189–192
manual enrollment, 112
Microsoft Windows 2000 Certificate Services 5.0, 192
requests, 124
saving, 125
signed certificates, 198–199
site-to-site
configuring (PIX Firewall), 183, 193–201
IKE (PIX Firewall), 201–203
support (PIX Firewall), 183–191
support, 34–39, 105–112, 128
troubleshooting, 200–201
VeriSign OnSite servers, 191
ca authenticate command, 197–198
ca configure command, 196
ca crl request command, 200
ca enroll command, 198–199
ca generate rsa command, 195
ca identity command, 196
ca save all command, 199
ca zeroize rsa command, 200
CEP (Certificate Enrollment Protocol), 112
cepsetup.exe file, 115
Certificate Authority. *See* CA
Certificate Enrollment Protocol (CEP), 112
Certificate Management, 304
Certificate Revocation List (CRL), 107
certificates. *See also* CA
authentication, 37–39
chains, 264, 266
deleting, 200
digital (IKE), 24
enrollment, 260
signed, 198–199
VPN 3000 Concentrator
configuring support, 271–279
digital certificates for clients, 280–281
generating, 259–262
validating, 263–270
X.509v3, 189
CET (Cisco Encryption Technology), 171, 185
chains, certificates, 264, 266
Cisco Secure Intrusion Detection System), 6
Cisco VPN 3000 Concentrator
activity, 285–294
configuring, 295–304
Cisco VPN Concentrator, 52
3000 series, 52–61
5000 series, 61
Cisco Works 2000, 6
CLI (command-line interface), 236, 287. *See also* interfaces
PIX Firewall, 51
VPN 3000 Concentrator, 235–240
Client Config Security Policy Editor, 347
clients
IPSec, 67. *See also* IPSec
mobile VPN, 310
VPN
configuring, 250–255
IKE requirements, 332
VPN 3000 version 2.5, 340–342
clock set configuration command, 194
clock set privileged EXEC command, 118
clock timezone global configuration command, 118
clocks, configuring PIX Firewall, 194
command-line interface. *See* CLI
commands, 125, 131
aaa-server, 329
access-list, 83, 130
access-list global configuration, 163
ca authenticate, 197–198
ca configure, 196
ca crl request, 200
ca enroll, 198–199
ca generate rsa, 195
ca identity, 196
ca save all, 199
ca zeroize rsa, 200
clock set configuration, 194
clock set privileged EXEC, 118
clock timezone global configuration, 118
crl optional, 125
crypto ca, 34

crypto ca authenticate name, 123
crypto ca certificate query, 118
crypto ca enroll global configuration, 124
crypto ca identity, 123–124
crypto ca identity global configuration, 122
crypto dynamic-map, 311, 336
crypto ipsec security-association lifetime, 83, 130
crypto ipsec security-association lifetime global configuration, 86, 170
crypto ipsec transform-set, 34, 83, 130
crypto ipsec transform-set global configuration, 83, 167
crypto isakmp client configuration address-pool, 335
crypto isakmp enable, 77
crypto isakmp identity global configuration, 80
crypto isakmp key, 77
crypto isakmp policy, 34, 77–78, 129
crypto key generate rsa, 120, 127
crypto map, 34, 83, 130
crypto map client authentication, 329–330
crypto map client-configuration address, 333
crypto maps, 172
debug, 68, 96–99
debug crypto ca, 204
debug crypto ipsec, 131
debug crypto isakmp, 131, 145–146, 220
debug crypto key-exchange, 131
debug crypto pki, 131
enrollment mode ra command, 123
generate RSA keys, 120
interface, 83, 130
ip address-pool global configuration, 335
ip domain-name global configuration, 119
ip local pool, 333
ISAKMP, 144
isakmp, 219
isakmp client configuration address-pool local, 333
isakmp show, 95
no ca enroll, 199
no ca save, 199
no certificate, 124
no isakmp enable interface-name, 159
no isakmp identity hostname, 203
no sysopt connection permit-ipsec, 163
peer default ip address pool interface configuration, 335
permit any, 336
ping, 75
Program menu, 254
show, 68, 74, 139
  information, 141
  IPSec, 95–96
  PIX Firewall, 215–217
  viewing, 140
show access-list, 68
show ca mypubkey rsa, 200
show clock, 194
show crypto ca certificates, 127
show crypto engine, 216
show crypto engine connections active, 141, 150
show crypto ipsec a, 141
show crypto ipsec sa, 131, 216
show crypto ipsec security-association lifetime, 176
show crypto ipsec transform-set, 74, 140, 215
show crypto isakmp, 147
show crypto isakmp key, 148
show crypto isakmp policy, 74, 77, 131, 216
show crypto key mypubkey rsa, 127
show crypto map, 74, 140, 174, 215, 327
show crypto map interface serial 0, 150
show ip route, 151
show running-config, 74
sysopt connection permit-ipsec, 163, 215
vpngroup, 340, 343
write memory, 199
write terminal, 161
communication, 196–197
  monitoring, 206
  parameters, 196–197
components
  IPSec crypto, 17–21
  VPN, 45–46
Concentrator series, 6
configuration
  access, 301
  CAs
    IKE, 201–203
    saving, 199
    support, 105–106, 116–127, 193–201

certificates, 271–279
Cisco VPN 3000 Concentrator, 295–304
crypto access lists, 163–165
crypto maps, 171–173
dates/time, 118
digital certificates, 280–281
dynamic crypto maps
    IOS, 313–314
    PIX Firewall, 310–312
global IPSec SA lifetimes, 170
host names, 119
IKE, 77–81, 106–111, 129
    PIX Firewall, 158–162
    policies, 129
    verifying, 82
IOS
    PFS, 338
    Secure VPN 1.1 clients, 352–353
IPSec, 67, 82–94, 106–111, 130
    ACLs, 75–76
    checking current, 74–75
    clients, 251–255
    defining policies, 71–74
    networks, 135–136, 138–142
    PIX Firewall, 162, 209–217, 315–320
    preparing IKI, 68
    SA lifetimes, 86
    selecting IKE policies, 68–70
    troubleshooting, 143–152
    testing peers, 75
    verifying, 175–176
    VPN 3000 Concentrator, 244–249
ISAKMP, 68
MTU, 255
PIX Firewall
    CA site-to-site, 183
    IPSec, 157–169, 171–177
    PFS, 337
    preshared keys, 157
    Secure VPN 1.1clients, 345–351
    VPN 3000 Client version 2.5, 340–342
preshared keys, 80–81, 160
transform sets, 83–84, 168
VPN 3000 Concentrator, 235–239
    browsers, 239–251
    PIX Firewall, 320–328
    remote access, 233
    testing, 177–180
connections
    IPSec, 141
    LAN-to-LAN, 323
copy running-config startup-config, 125
copy running-config startup-config command, 125
CRL (Certificate Revocation List), 107, 125–127, 267
crl optional command, 125
crypto map command, 83
crypto access lists
    creating, 86–88
    PIX Firewall, 163–165
crypto ca authenticate name command, 123
crypto ca certificate query command, 118
crypto ca commands, 34
crypto ca enroll global configuration command, 124
crypto ca identity command, 123–124
crypto ca identity global configuration command, 122
crypto components, IPSec, 17–21
crypto dynamic-map command, 311, 336
crypto ipsec security-association lifetime command, 83, 130
crypto ipsec security-association lifetime global configuration command, 86, 170
crypto ipsec transform-set command, 34, 83, 130
crypto ipsec transform-set global configuration command, 83, 167
crypto isakmp client configuration address-pool local command, 335
crypto isakmp enable command, 77
crypto isakmp identity global configuration command, 80
crypto isakmp key command, 77
crypto isakmp policy command, 34, 77–78, 129
crypto key generate rsa command, 120, 127
crypto map client authentication command, 329–330
crypto map client-configuration address command, 333
crypto map command, 34, 130
crypto maps, 140, 172
    applying, 92–94
    creating, 89–91
    dynamic, 309–310
        IOS, 313–314
        PIX Firewall, 310–312

interfaces, 150, 225
PIX Firewall, 171–175
crypto system error messages, ISAKMP, 99
cryptographic service provider (CSP), 115
CSIDS (Cisco Secure Intrusion Detection System), 6
CSP (cryptographic service provider), 115

D

Data Encryption Standard (DES), 8, 11, 17
databases, Security Parameter Database, 30
date/time, Pix Firewall, 194
dates, configuring, 118
DDR (dial-on-demand routing), 149
debug command, 68, 96–99
debug crypto ca command, 204
debug crypto ipsec command, 131
debug crypto isakmp command, 131, 145–146, 220
debug crypto key-exchange command, 131
debug crypto pki command, 131
declarations, CAs, 122, 196
defining
policies
IKE, 70
IPSec, 71–74
traffic, 26
transform sets, 83–84
deleting
certificates, 200
RSA keys, 200
demilitarized Zone (DMZ), 174
DES (Data Encryption Standard), 8, 11, 17
devices, enrolling CAs, 115, 192
D-H (Diffie-Hellman), 8, 12 18–20, 141
dialers, VPN, 255
dialog boxes, DUN properties, 254
dial-on-demand routing (DDR), 149
Diffie-Hellman (D-H), 8, 12, 18–20, 141
digital certificates, 263. *See also* certificates
enrollment, 260
IKE, 24
VPN 3000 Concentrator
digital signatures, 36
digital subscriber line (DSL), 5
disabling IKE, 77, 159
DMZ (Demilitarized Zone), 174
domain names
configuring, 119, 195
routers, 119
DRAM (dynamic random-access memory), 30
DSA (Directory System Agent), 259
DSL (digital subscriber line), 5
DUN (Dial Up Networking), 254
dynamic crypto maps, 309–310
IOS, 313–314
PIX Firewall, 310–312
dynamic random-access memory (DRAM), 30
dynomap 210, 313

E

editing transform sets, 84
enabling IKE, 77, 159
Encapsulating Security Payload (ESP), 8, 72, 141
encryption
3DES, 166
DES, 17
IPSec
ACLs, 75–76
checking current configuration, 74–75
configuring, 67, 82–94, 106–111
defining policies, 71–74
encrypted tunnels, 29
preparing IKE, 68
selecting IKE policies, 68–70
testing peers, 75
PIX Firewall, 157–169, 171–177
RSA, 24
traffic, 140
enrollment
CA devices, 115, 192
certificates, 260
SCEP, 190
enrollment mode ra command, 123
entries, creating, 313
Entrust CA servers, 113, 191
error messages, 99
ESP (Encapsulating Security Payload), 8, 72, 141
Event Log, monitoring, 287
exceptions, security gateways, 329
execution, IOS in routers, 47–48

Extended Authentication. *See* Xauth
external authentication, 251. *See also* authentication
Extranet VPNs, 5

F

FDQN (fully qualified domain name), 23, 193
File Management, 302–303
firewalls. *See also* PIX Firewall
    ACLs, 224–225
    crypto map placement, 225
    IPsec
        differing preshared keys, 223
        troubleshooting, 209–220, 222–227
    ISAKMP policies, 218–223
    PIX, 49, 51
    routing, 225–226
Flash memory
    deleting, 200
    managing, 193
flowcharts, IPSec, 32, 34
formatting
    crypto ACLs, 86–88
    crypto maps, 89–91
    dynamic crypto map entries, 313
    policies (IKE), 78–79
fully qualified domain name (FQDN), 23, 193

G

gateways
    security, 329
    transport/tunnel modes, 13–16
general purpose keys, generating, 121
General Statistics, monitoring, 294
generate RSA keys command, 120
generation
    certificates, 259–262
    general purpose keys, 121
    RSA key pairs, 120, 195
    special usage keys, 120
global IPSec, configuring, 86
GRE (Generic Route Encapsulation), 47
groups
    IPSec, 244–249
    VPN 3000 Concentrator, 250–251
GUI (graphical user interface), 238. *See also* interfaces

H

HMAC (hashed message authentication code), 12, 20–21, 166
host names
    PIX Firewall, 195
    routers, 119

I

IE (Internet Explorer), 280. *See also* browsers
IETF (Internet Engineering Task Force), 112, 249
IKE (Internet Key Exchange), 12, 111
    CAs, 24
    certificates, 263
    configuring, 77–82, 106–111, 129
    digital certificates, 24
    IPSec
        ACLs, 75–76
        checking current configuration, 74–75
        configuring, 67
        defining policies, 71–74
        operations. 27–28
        preparing, 68
        selecting policies, 68–70
        testing peers, 75
    managing, 206
    mode configuration, 331–336
    monitoring, 206
    overview, 22–23
    PIX Firewall
        configuring, 158–162
        verifying policies, 160–162
    policies, 108–111, 129
        CAs, 186–188
        site-to-site, 202–203
    preshared keys, 23
    proposals, 279
    routers, 32, 34
    RSA
        encryption, 24

generating, 195
signatures, 24
SAs, 71
Xauth, 328–329
information show commands, 141, 216–217
initial configurations, routers, 137
interface command, 83, 130
interfaces, 299
crypto maps, 92–94, 174–175
GUI, 238
IP, 240
monitoring, 292
PIX Firewall, 51
refreshing, 299
troubleshooting, 150, 225
Internet Engineering Task Force (IETF), 112
Internet Key Exchange. *See* IKE
Internet Protocol Security. *See* IPSec
Internet Security Association Key Management Protocol. *See* ISAKMP
Internet service provider (ISP), 331
interoperability, 113–115
CA, 189–192
monitoring, 113–127
Intranet VPNs, 5
IOS
dynamic crypto maps, 313–314
PFS, 338
preshared key wildcards, 330
routers, 47–48
Secure VPN 1.1, 352–353
IP (Internet Protocol)
addresses
assigning, 243
pools, 335
interfaces, 240
traffic
applying crypto maps, 91–94
creating crypto ACLs, 86–88
ip address-pool local global configuration command, 335
ip domain-name global configuration command, 119
ip local pool command, 333
IPSec (Internet Protocol Security)
3DES, 11
ACLs
PIX Firewalls, 224–225
troubleshooting, 149
AH, 9
CAs, 13
configuring, 82–94, 106–111, 130, 175–176
crypto components, 17, 19–21
debug commands, 96–99
DES, 11
D-H, 12
encryption
ACLs, 75–76
checking current configuration, 74–75
configuring, 67
defining policies, 71–74
PIX Firewall, 157–167, 169–177
preparing IKE, 68
selecting IKE policies, 68–70
testing peers, 75
ESP, 10
flowcharts, 32, 34
IKE, 12, 77–81
LAN-to-LAN connections, 323
managing, 206
MD5, 12
NAT, 338–339
network configurations, 135–142
PIX Firewalls, 209–217
troubleshooting, 143–152
operations, 25
defining traffic, 26
encrypted tunnel, 29
IKE, 27–28
tunnel termination, 29
peers, 147–148, 223
PIX Firewall
CA site-to-site, 184–185
configuring, 162, 315–320
configuring preshared keys, 157
testing, 204–206
RSA signatures, 12
SAs, 30–34, 86, 279
SHA-1, 12
show commands, 95–96
site-to-site CA (PIX Firewall), 203
testing, 94–99, 131
transforms, 16

transport/tunnel modes, 13–16
verifying, 131, 327
VPN 3000 Concentrator
clients, 251–255
configuring, 244–249
scaling, 309
ISAKMP (Internet Security Association Key Management Protocol), 108–111, 143
configuring, 68
commands, 144
crypto system error messages, 99
policies, 143–146, 218–223
isakmp client configuration address-pool local command, 333
isakmp command, 219
isakmp show command, 95
ISP (Internet service provider), 331

J–K

keys. *See also* IKE; preshared keys
agreements, 18
general purpose
generating, 121
PFS, 337
IOS, 338
PIX Firewall, 337
preshared, 23, 80, 141
RSA
deleting, 200
generating, 120, 195
special usage, 120
wildcards, 330

L

LAN to LAN connections, adding, 323
LDAP (Lightweight Directory Access Protocol), 107, 185
LED (light emitting diode), monitoring, 289–290
length, 121
lifetimes
global IPSec SA, 170
SAs, 86
Lightweight Directory Access Protocol (LDAP), 107, 185
loading certificates, 271–276
local IPSec peers, 138
login, VPN 3000 Concentrator, 237
logs, monitoring, 287

M

main mode, IKE, 27
maintenance
CAs, 125–127
support, 200–201
management, 296
certificates, 304
Cisco VPN 3000 Concentrator, 295–304
files, 302–303
IKE, 206
IPSec, 206
memory (Flash), 193–194
NVRAM, 117
sessions,296
manual enrollment
CAs, 112
SCEP, 190
maps, crypto. *See* crypto maps
MD5 (Message Digest 5 (MD5), 8, 12
memory
DRAM, 30
Flash
deleting, 200
managing, 193–194
NVRAM, 117
menus (Program), VPN clients, 254–255
Message Digest 5 (MD5), 8, 12
messages, error (ISAKMP), 99
methods, preshare authentication, 160
Microsoft Windows 2000 Certificate Services 5.0, 192
mobile VPN clients, 310
modes
IKE configuration, 331–334
IOS, 336
modulus length, 121
monitoring
activity, 285–294

CAs, 125–127
Event Log, 287
General Statistics, 294
IKE, 206
interfaces, 292
IPSec, 206
LED status, 289–290
power supply status, 291
Routing Table, 286
Sessions, 292–293
support, 200–201
System Status, 288–291
Monitoring Refresh, 299
mscep.dll, 115
MTU (maximum transmission unit), 255
MyMap, 140

N

names, PIX Firewall configuration, 195
NAT (Network Address Translation), 15, 215, 338–339
negotiation, transform sets, 169
Network Address Translation. *See* NAT
Network Auto Discovery check box, 324
Network Time Protocol (NTP), 118
networks
IPSec configurations, 135–142
PIX Firewalls, 209–217
troubleshooting, 143–152
topologies, 320
no ca enroll command, 199
no ca save command, 199
no certificate command, 124
no isakmp enable interface-name command, 159
no isakmp identity hostname command, 203
no sysopt connection permit-ipsec command, 163
NTP (Network Time Protocol), 118
NVRAM (Non-Volatile Random Access Memory), managing, 117

O

operations (IPSec), 25
defining traffic, 26
encrypted tunnel, 29
IKE, 27–28
tunnel termination, 29
verifying, 327
optimization
IPSec algorithms, 71
VPN routers, 48
options
IPSec clients, 252–253
isakmp command, 219
output, show ca mypubkey rsa command, 200
overview
CAs, 34–39
IKE, 22–23
VPN, 5–6

P

parameters
CA, 196–197
crypto maps, 171
IKE
CA site-to-site (PIX Firewall), 187
configuring, 77–81
defining, 70
PIX Firewall, 158–162
policies, 109
IPSec
client options, 252–253
configuring, 71
ISAKMP, 110
SAs, 32
VPN 3000 Concentrator, 235–239
peer default ip address pool interface configuration command, 335
peers
IPSec, 71, 138
differing preshared keys between, 147–148, 223
testing, 75
perfect forward secrecy. *See* PFS
permit any command, 336

PERMIT statements, 75, 142
PFS (perfect forward secrecy), 29, 150, 173
  IOS, 338
  PIX Firewall, 337
Ping, 75
  Cisco VPN 3000 Concentrator, 299
  remote IPSec peers, 138
PIX Firewall, 6, 49
  ACLs, 224–225
  CA site-to-site
    configuring, 183, 193–201
    IKE, 201–203
    support, 183–191
  crypto access lists, 163–165
  crypto maps, 171, 173
    applying to interfaces, 174–175
    placement, 225
  date/time, 194
  dynamic crypto maps, 309–312
  global IPSec SA lifetimes, 170
  IKE
    configuring, 158–162
    modes, 333–334
  IPSec
    configuring, 157–169, 171–177, 315–320
    differing preshared keys between peers, 223
    networks, 209–218
    preparing, 158
    site-to-site CA, 203
    testing, 204–206
    verifying, 175–176
    troubleshooting, 218–227
  ISAKMP policies, 218–223
  PFS, 337
  preshared keys, 157
  routing, 225–226
  Secure VPN 1.1, 345–347, 349, 351
  VPN, 51, 177–180
  VPN 3000 Client version 2.5, 340
  VPN 3000 Concentrator, 320–328
  Xauth, 328–329
PKCS #10 (Public-Key Cryptography Standard #10), 189
PKCS #7 (Public-Key Cryptography Standard #7), 189
PKCS (Public Key Cryptography Standards), 259
PKI (public key infrastructure), 38, 251
PL2 (Private Link), 51
placement of crypto maps, troubleshooting, 150, 225
policies
  IKE, 108, 110–111, 129
    CA site-to-site (PIX Firewall), 186, 188
    creating, 78–79
    PIX Firewall, 159
    selecting, 68–70
    site-to-site CA (PIX Firewall), 202–203
    verifying, 160–162
  IPSec, 68–74
  ISAKMP, 143–146, 218–223
  security, 83–84
pools, IP addresses, 335
power supplies, monitoring, 291
PPP (Point-to-Point Protocol), 331
PPTP (Point-to-Point Tunneling Protocol), 51, 294
preparation
  IKE, 68
  IPSec, 158
preshare authentication method, 160
preshared keys, 141. *See also* IKE
  configuring, 80–81
  IKE, 23
  IPSec, 147–148, 223
  PIX Firewall, 157, 160
  VPN 3000, 233
  wildcards, 330
private LANs, configuring, 235–237, 239
processes
  certificate authentication, 270
  certificate loading, 271–276
  D-H, 19–20
products, VPN, 45–46
Program menu
  commands, 254
  VPN clients, 254–255
properties
  DUN, 254
  IPSec, 253
  VPN Concentrator 3000, 240
proposals, IKE, 279
protection suites, 187
protocols
  CEP, 112
  IPSec
    3DES, 11

AH, 9
CAs, 13
crypto components, 17–21
DES, 11
D-H, 12
ESP, 10
IKE, 12
MD5, 12
RSA signatures, 12
SHA-1, 12
transforms, 16
transport/tunnel modes, 13–16
ISAKMP, 68
LDAP, 107, 185
NTP, 118
PPP, 331
PPTP, 51
SCEP, 112, 185–190
SNMP, 288
TFTP, 302
public interfaces, configuring, 240
public IP interfaces, 241
public key infrastructure. *See* PKI
Public-Key Cryptography Standard #10 (PKCS #10, 111
Public-Key Cryptography Standard #7 (PKCS #7), 111

Q

Quick Configuration, VPN 3000 Concentrator, 239

R

RA (registration authority), 107
ranges, validating, 266
RAS (Rivest, Shamir, and Adelman) signatures, 8
rebooting Cisco VPN 3000 Concentrator, 298
refreshing, 299
registration authority (RA), 107
remote access, VPN 3000, 233
remote IPSec peers, pinging, 138
remote users, 254
requests, CA signed certificates, 198–199
requirements, VPN client IKE, 332
revisions, transform sets, 84
rights, access, 299–300
Rivest, Shamir, and Adelman. *See* RSA
ROBO (remote office, branch office), 49
routers, 6
CA interoperability, 113–115
date/time, 118
domain names, 119
dynamic crypto maps, 309–310
IOS, 313–314
PIX Firewall, 310–312
host names, 119
IKE, 32, 34
initial configurations, 137
IOS, 47–48
IPSec
configuring, 139–142
troubleshooting, 143–152
PIX Firewall, 315–320
routing
DDR, 149
PIX Firewalls, 225–226
troubleshooting, 151–152
Routing Table, monitoring, 286
RSA (Rivest, Shamir, and Adelman), 259
deleting keys, 200
encryption, 24
generating keys, 120, 195
signatures, 12, 24

S

SAs (security associations), 22, 141
global IPSec lifetimes, 170
IKE, 71
IPSec, 30–34, 279
lifetimes, 86
scaling IPSec-based VPNs, 309
SCEP (Simple Certificate Enrollment Protocol), 112, 185–190
Secure Hash Algorithm-1 (SHA-1), 8
Secure PIX Firewall. *See* PIX Firewall
Secure Policy Manage, 6
Secure VPN 1.1
IOS, 352–353
PIX Firewall, 345–351

Secure VPN clients, 6
security
gateways, 329
IPSec
3DES, 11
AH, 9
CAs, 13
crypto components, 17, 19–21
DES, 11
D-H, 12
ESP, 10
IKE, 12
MD5, 12
RSA signatures, 12
SHA-1, 12
transforms, 16
transport/tunnel modes, 13–16
PIX Firewall, 49–51
policies, 83–84
Security Associate Program, 190
security associations. *See* SAs
Security Parameter Database, 30
Security Policy editor, 349
selection
CA servers, 185
policies, 68–74
transforms, 71
SEP (Scalable Encryption Processing), 52
seq-num (sequence number), 171
servers
Baltimore Technologies CA, 191
CA
router interoperability, 113–115
selecting, 185
Entrust CA, 113, 191
Microsoft Windows 2000 Certificate Services, 192
VeriSign OnSite CA, 113, 191
Windows 2000 CA, 114
sessions, monitoring, 292–296
sets, transforms, 16
setting date/time, PIX Firewall, 194
SHA (Secure Hash Algorithm), 166
SHA-1 (Secure Hash Algorithm-1), 8, 12
show access-lists command, 68
show ca mypubkey rsa command, 200
show clock command, 194
show commands, 68, 74, 139
information, 141
IPsec, 95–96
PIX Firewall, 215–217
viewing, 140
show crypto ca certificates command, 127
show crypto engine command, 216
show crypto engine connections active command, 141, 150
show crypto ipsec sa command, 131, 141, 216
show crypto ipsec security-association lifetime command, 176
show crypto ipsec transform set, 131
show crypto ipsec transform set command, 131
show crypto ipsec transform-set command, 74, 215
show crypto isakmp command, 147
show crypto isakmp key command, 148
show crypto isakmp policy command, 74, 131, 216
show crypto isakmp policy map command, 140
show crypto key mypubkey rsa command, 127
show crypto map command, 74, 131, 140, 174, 215
show crypto map interface serial 0 command, 150
show ip route command, 151
show running-config command, 74
shutdown, Cisco VPN 3000 Concentrator, 298
signatures
digital, 36
requesting certificates, 198–199
validating, 265
Simple Certificate Enrollment Protocol (SCEP), 112
Simple Network Management Protocol (SNMP), 288
site-to-site CA, 190–191
configuring, 183, 193–201
IKE, 201, 203
support, 183–189
site-to-site preshared keys. configuring, 157. *See also* preshared keys
site-to-site VPNs, configuring, 320–328
small office, home office (SOHO), 5
SNMP (Simple Network Management Protocol), 288
software
IOS, 47
VPN Concentrator, 52
3000 series, 52–61
5000 series, 61

SOHO (small office, home office), 5, 49
special usage keys, generating, 120
statements, PERMIT, 75, 142
statistics, PPTP, 294
status
    LED, 289–290
    power supplies, 291
    System Status, 288–291
support
    CAs, 34–39, 107–112, 128
        configuring, 105–106, 119–127
        troubleshooting, 200–201
    configuring, 116–127
    PIX Firewall, 183–189
    VPN 3000 Concentrator, 271–279
sysopt connection permit-ipsec command, 163, 215
System Reboot, Cisco VPN 3000 Concentrator, 298
System Status, monitoring, 288–291
systems properties, VPN Concentrator 3000, 240

T

tables, monitoring, 286
tasks, configuring, 105–106
technologies
    Baltimore, 114
    Entrust, 113
    VPN, 5–6
termination of tunnels, 29
testing
    IPSec, 94–99, 131
    peers, 75
    PIX Firewall, 204–206
    VPN, 177–180
TFTP (Trivial File Transfer Protocol), 302
time, 118, 194
topologies, 320
traffic
    defining, 26
    IP
        applying crypto maps, 89–94
        creating crypto ACLs, 86–88
    IPSec, 140
transform sets
    configuring, 83–84
    IPSec, 16
    PIX Firewall, 166–169
    selecting, 71
transport modes, 13, 15–16
Triple DES (3DES), 8
Trivial File Transfer Protocol (TFTP), 302
troubleshooting
    ACLs
        IPSec, 149
        PIX Firewalls, 224–225
    CA support, 200–201
    IPSec, 94–97, 99, 204–206
    network configurations, 135–136, 138–152
    routing, 151–152, 225–226
    VPN, 177–180
Tunnel Endpoint Discovery, 336
tunnels
    GRE, 47
    IPSec encrypted tunnel, 29
    mode, 13–16
    terminating, 29

U

UniCERT CA module, 114
unistallation of VPN 3000 Concentrator clients, 255
Universal Time Code (UTC), 118
update, 297
users
    adding250–251
    remote, 254
UTC (Universal Time Code), 118

V

VACs (VPN Accelerator Cards), 48
validation
    certificates, 263–270
    ranges, 266
verification
    CA support configuration, 199
    IKE, 82, 160–162
    IPSec, 94–99, 131, 327
    VPN, 177–180
VeriSign OnSite CA server, 113, 191
viewing show commands, 140, 215

VPN (virtual private network)
3000 series, 52–61
5000 series, 61
clients, 332
components, 45–46
dialers, 255
IOS, 47–48
IPSec, 309
mobile clients, 310
overview of, 5–6
PIX Firewall
testing, 177–180
troubleshooting, 204–206
VPN 3000 Client version 2.5, configuring, 340–342
VPN 3000 Concentrator
adding users, 250–251
browsers, 239–251
certificates
configuring support, 271–279
generating, 259–262
validating, 263–270
configuring, 235–239
digital certificates, 280–281
IP addresses, 243
IPSec
configuring, 244–249
configuring clients, 251–255
PIX Firewall, 320–328
Quick Configuration, 239
remote access, 233
vpngroup command, 340, 343

W

wildcards, preshared keys, 330
Windows 2000 CA server, 114
write memory command, 199
write terminal command, 161

X–Z

X.509v3 certificates, 111, 189
Xauth (Extended Authentication), 328–329