INDEX

Symbols

^z command, 92

Numerics

3DES (Triple Data Encryption Standard), 164

A

AAA (authentication, authorization, and accounting), 8, 259–262
    configuration, 276–300
    Floodguard, 320
    servers
        identifying, 276–279
        specifying, 275
    support, 28
    troubleshooting, 303–306
aaa accounting command, 277
aaa authentication command, 277
aaa authentication console command, 282
aaa authorization command, 277
aaa-server command, 276–277
access
    AAA, 259–262
    attacks, 5
    authentication console, 282
    inbound configuration, 112–118
    lists, 115–118
    modes, 92
    NAS, 260
    networks
        security, 3
        threats, 4
        types of attacks, 4–6
        vulnerabilities, 3
    object grouping, 119–122
    PDM requirements, 212
    remote, 48–50
        SSH, 49–50
        Telnet, 48–49
    rules, 385
    VPN, 161
access control list. *See* ACL
Access Control Server (ACS), 28
access list entries (ACEs), 115
access-group command, 177, 385
access-list command, 173
accounting. *See also* AAA
    configuration, 295–299
    troubleshooting, 305
    viewing, 297
ACEs (access list entries), 115
ACL (access control list), 15
    downloading, 300–302
    TurboACL, 118–119
ACS (Access Control Server), 28
activation keys
    license, 163
    upgrading, 51–53
ActiveX, filtering, 248
Adaptive Security Algorithm (ASA), 17, 25–26
addresses
    command, 55
    IP
        global, 382, 384
        mapping, 381
    static port translation, 113–114
    translation, 29, 71–79
        bidirectional, 79
        commands, 73
        configuring multiple, 77–78
        NAT, 74
        PAT, 75
        static, 75–76
        troubleshooting, 79–82
advanced protocol handling, 123–124
aggressive mode (IKE), 164
AH (Authentication Header), 163
algorithms
    ASA, 17, 25–26
    SHA-1, 164
    transform sets, 175
alias command, 319
applets, filtering, 246–247
applications
    AVVID, 9–10
    multimedia
        H.323, 315–317
        RTSP, 315
        support, 314–317
    threats, 4
    types of attacks, 4–6
    vulnerabilities, 3
architecture
    AVVID, 9–10
    point-to-point architecture, 7, 26–27, 31–41, 68–76, 117,
    selecting, 7, 26–34, 36–41, 68–78, 84–85
Architecture for Voice, Video, and Integrated Data. *See* AVVID
arguments, crypto maps, 178
ASA (Adaptive Security Algorithm), 17, 25–26
assigning users to groups, 288
attacks
    guards, 317–321
    Syslog, 130–132
    threats, 4
    types of, 4–6
        access, 5–6
        DoS, 6
        reconnaissance, 5
    vulnerabilities, 3
authentication. *See also* AAA
    CAs, 167
    configuration, 279–287, 385
    cut-through proxy, 18, 26–27
    HMAC, 164
    IPSec, 162–164

prompts, 285
services, 283
timeout, 286
troubleshooting, 304
X.509 certificate support, 28
Authentication Header (AH), 163
authentication telnet console command, 49
authentication, authorization, and accounting. *See* AAA
authorization. *See also* AAA
configuration, 287–295
CSACS, 288
cut-through proxy, 18, 26–27
rules for groups, 291
troubleshooting, 305
Auto Update, 57
AVVID (Architecture for Voice, Video, and Integrated Data), 9–10

B

basic configuration, 380–384
bidirectional network address translation, 79
block scans, 5
blocking applets, 246–247
boothelper disk, creating, 56–57

C

cables, Crossover Ethernet, 149
caches
no url-cache command, 250
show url-cache command, 251
url-cache command, 250
CAs (Certification Authorities), 167
certificate revocation lists (CRLs), 102
certificates, X.509 support, 28
cgi-truncate parameter, 251
CIFS (Common Internet File System), 71
Cisco PIX Firewall
ASA, 17, 25–26
models
Cisco PIX 501 Firewall, 30–31
Cisco PIX 506 Firewall, 27, 31
Cisco PIX 515 Firewall, 28, 33–35
Cisco PIX 520 Firewall, 28, 35–38
Cisco PIX 525 Firewall, 28, 38–39
Cisco PIX 535 Firewall, 28, 39–41
Cisco Secure Access Control Server. *See* CSACS
Cisco Secure Intrusion Detection Sensor, 28
Cisco Secure Policy Manager (CSPM), 29
Cisco Secure Scanner, 8
clear command, 182
clear ntp command, 103
clear xlate command, 79
CLI (command-line interface), 29, 49
clients
DHCP, 102
HTTP, 56
VPN, 184–187
clock summer-time command, 104
command-line interface (CLI), 29, 49
commands
^z, 92
aaa accounting, 277
aaa authentication, 277
aaa authentication console, 282
aaa authorization, 277
aaa-server, 276–277
access modes, 92
access-group, 177, 385
access-list, 115–118, 173
address, 55
alias, 319
authentication telnet, 49
auth-prompt, 285
auto-update server, 57
clear, 182
clear ntp, 103
clear xlate, 79
clock summer-time, 104
conduit, 118
configuration, 92–100, 105–107
global, 96–97
interface, 93–94
ip address, 95–96
nameif, 94
nat, 96
configure terminal, 92
copy tftp flash, 53–54
crypto ipsec transform-set, 177
crypto-map, 176
debug, 99, 182, 395
debug aaa accounting, 305
debug aaa authorization, 305
disable, 92
enable, 92
enable password, 49
exit, 92
file, 55
filter activex, 248
filter java, 246
filter url, 249
fixup, 122–123
fixup protocol, 314
fixup protocol h323, 317
floodguard disable, 321
gateway, 55
interface, 54
ip audit, 322
ip verify reverse-path, 324–325
isakmp policy, 169
logging, 132–135
logging facility facility, 131
match-address, 178
nameif, 67, 83
nat 0, 115
no fixup protocol ftp, 124
no url-cache, 250
ntp, 103
ntp authenticate, 103
ntp authentication, 103
ntp trusted-key, 103
passwd, 48
permit any any, 173
ping, 55, 99
server, 55

show, 172, 181, 304, 395
show aaa-server, 304
show accounting, 305
show activation-key, 52
show perfmon, 252
show url-cache, 251
show url-server stats, 252
show version, 51
show xlate, 79
shun, 324
ssh, 49
static, 77
sysopt connection permit-ipsec, 180
sysopt security fragguard, 317
sysopt uauth allow-http-cache, 281
telnet, 48
timeout uauth, 286
translation, 73
url-cache, 250
url-server, 248
virtual telnet, 283
vpdn, 185–187
VPN groups, 185
write memory, 49, 100
write standby, 147
Common Internet File System (CIFS), 71
communications (VPN), 161
CAs, 167
clients, 184–187
configuration, 168–180
IKE, 164–167
IPSec, 162–164
scalability, 187
troubleshooting, 180–184
components, AAA, 259–262, 275
conduit command, 118
configuration, 105–107
AAA, 276–300
troubleshooting, 303–306
access rules, 385
accounting, 295–299
authentication, 279–287, 385
authorization, 287–295
Auto Update, 57
basic, 380–384
commands, 92–100
global, 96–97
interface, 93–94
ip address, 95–96
nameif, 94
nat, 96
RIP, 98
route, 98
Console, 134
crypto maps, 176
CSACS, 288
cut-through proxy, 300
DHCP, 100–102
clients, 102
servers, 101
DNS support, 82
downloadable PIX ACLs, 300–302
failover, 150–154, 395–397
filters
policies, 249
viewing, 251
IKE, 169–173
inbound access, 112–118
interfaces, 382–383
intrusion detection, 322–323
IPSec, 173–180
logging, 386
multiple translation types, 77–78
object grouping, 119–122
PDM, 210, 213–226
configuration, 213–226
requirements, 211–213
viewing logging, 133
VPN, 227–238
preshared keys, 171
redundancy, 18
replication, 147
routing, 382, 384
SA lifetimes, 175
saving, 100
SNMP requests/traps, 136
Syslog, 30, 132–136
testing, 99
time settings, 102–104
transform sets, 175
troubleshooting, 398–406
TurboACL, 119
VPN, 168–180, 386–389
troubleshooting, 394–395
tunneling, 389–394
configure terminal command, 92
connections
Cisco Secure PIX 501, 30–31
Cisco Secure PIX 506, 31
Cisco Secure PIX 515, 33–35
Cisco Secure PIX 520, 35–38
Cisco Secure PIX 525, 38–39
Cisco Secure PIX 535, 39–41
cut-through proxy, 18, 26–27, 260
embryonic (half-open), 70
filters
ActiveX, 248
Java applets, 246–247
URLs, 248–252
LAN failover, 149
security, 3
stateful failover, 148
Telnet, 48
threats, 4
troubleshooting, 79–82
types of attacks, 4–6
vulnerabilities, 3
Console, 134, 282
copy tftp flash command, 53–54
CRLs (certificate revocation lists), 102
Crossover Ethernet cables, 149
crypto access lists, creating, 173
crypto ipsec transform-set command, 177
crypto maps
arguments/options, 178
configuration, 176
crypto-map command, 176
CSACS (Cisco Secure Access Control Server), 262–268, 273
authorization, 288
downloadable PIX ACLs, 300–302
users, 288
verifying, 306
CSPM (Cisco Secure Policy Manager), 29
cut-through proxy, 18, 26–27, 260, 300

D

Data Encryption Standard (DES), 164, 211
DDoS (distributed denial of service) attacks, 6
debug aaa accounting command, 305
debug aaa authorization command, 305
debug command, 99, 182
default security policies, 67
demilitarized zone (DMZ) segment, 77
denial of service (DoS) attacks, 6
deny keyword, 173
DES (Data Encryption Standard), 164, 211
design, security, 8
devices (PDM), 210–226
    configuration, 213–226
    requirements, 211–213
DHCP (Dynamic Host Configuration Protocol)
    clients, 102
    servers, 101
disable command, 92
disabling Syslog messages, 138–139
distributed denial of service (DDoS) attacks, 6
DMZ (demilitarized zone) segment, 77
DNS (Domain Name Service), 318–319
    support, 82
    queries, 5
DoS (denial of service) attacks, 6
downloadable PIX ACLs, 300–302
dynamic shunning, 323

E

embedding, secure real-time embedded systems, 17
embryonic (half-open) connections, 70
enable command, 92
enable password command, 49
Encapsulating Security Payload (ESP), 162
encapsulation of upper-level data, 68
encryption
    3DES, 164
    DES, 164, 211
    X.509 certificate support, 28
environments, ROBO, 31
ESP (Encapsulating Security Payload), 162
Ethernet, PPPoE, 188
events
    failover, 146–147
    Syslog, 30, 130–132
exit command, 92

F

fabrication, access attacks, 6
failover
    configuration, 147, 150–154, 395–397
    event monitoring, 146–147
    LAN, 149
    redundancy, 18
    stateful, 148
features, PIX Firewalls, 27–28
file command, 55
File Transfer Protocol (FTP), 123–124
filter activex command, 248
filter java command, 246
filter url command, 249
filters
    ActiveX, 248
    Java applets, 246–247
    packets, 15–16
    policies, 249
    URLs, 248–252
    viewing, 251
firewalls, 15–16
    basic configuration, 380–384
    managing, 29
    packet filtering, 15–16
    PIX, 17–18
        ASA, 17, 25–26
        Cisco 501, 30–31
        Cisco 506, 31
        Cisco 515, 33–35
        Cisco 520, 35–38
        Cisco 525, 38–39
        Cisco 535, 39–41
        models, 27–28
    proxy servers, 16
    stateful inspection, 16
    troubleshooting, 398–406
fixup command, 122–123
fixup protocol command, 314
fixup protocol h323 command, 317
Flood Defender, 320
Floodguard, 320
floodguard disable command, 321
formatting
    boothelper disk, 56–57
    crypto access lists, 173
fragmentation guard, 317
frames, 67
FTP (File Transfer Protocol), 123–124

G

gateways
    command, 55
    VPNs, 30
        clients, 184–187
        configuration, 168–180
        scalability, 187
        troubleshooting, 180–184
global command, 96–97
global information, recording, 380
global IP addresses, 382, 384
grouping
    objects, 119–122
    rules, 291
    users, 288
    VPN, 185
guards, 318–319
    attack, 317–321
    DNS, 318–319
    fragmentation, 317
    mail, 319–320

H

H.323 collection of protocols, 315–317
handling protocols, 123–124
hardware, CSACS, 262
headers, AH, 163
HMAC (Keyed-Hash Message Authentication Code), 164
horizontal scans, 5
HTML (Hypertext Markup Language), ActiveX filters, 248
HTTP (Hypertext Transfer Protocol)
    clients, 56
    Virtual, 285

I

ICMP object groups, 121
identifying
    filters, 248
    servers, 276–279
IKE (Internet Key Exchange)
    configuration, 169–173
    Policy Panel, 229
    VPN, 164–167
implementation
    security designs, 8
    troubleshooting, 398–406
inbound access configuration, 112–118
inbound connections, cut-through proxy, 18, 26–27
information security, 3
inspection
    advanced protocol handling, 123–124
    FTP, 123–124
installation
    CSACS, 263–268
    operating systems, 50–53
    PDM, 213–226
integrated data, AVVID, 9–10
integrity, X.509 certificate support, 28
Intel Internet Video Phone, 124
interception, 5, 114–115
interface command, 54, 93–94
interfaces. *See also* access
    CLI, 29, 49
    configuration, 382–383
    failover, 146–147
    PDM, 210–226
        configuration, 213–226
        requirements, 211–213
    static NAT, 112–113
Intranet VPNs, 161
intrusion detection, 28, 321–324
    configuration, 322–323
    dynamic shunning, 323
    optimizing, 8
IP (Internet Protocol)
    addresses
        global, 382, 384
        mapping, 381
    fragmentation guard, 317
ip address command, 95–96
ip audit command, 322
ip verify reverse-path command, 324–325
IPSec (Internet Protocol Security)
    configuration, 173–180
    VPN, 162–164
isakmp policy command, 169

J

Java applets, filtering, 246–247

K

Keyed-Hash Message Authentication Code (HMAC), 164
keywords
    deny, 173
    permit, 173

L

L2TP (Layer 2 Tunneling Protocol), 185–187
LAN failover, 149
Layer 2 Tunneling Protocol (L2TP), 185–187
levels of security (Syslog), 67, 131–132
lifetimes, SA, 175
Linux, PDM requirements, 213
lists
    access, 115–118
    ACL, 15
    CRLs, 102
logging
    configuration, 386
    facilities, 131
    Syslog, 130–132
    viewing, 133
long URLs, filtering, 251
longurl-truncate parameter, 251

M

mail guard, 319–320
main mode (IKE), 164
management
    firewalls, 29
    PDM, 210–226
        configuration, 213–226
        requirements, 211–213
mapping
    static IP addresses, 381
    static NAT, 112–113
match address command, 178
MD5 (Message Digest 5), 164
memory requirements, 50
Message Digest 5 (MD5), 164
messages
    digest, 164
    HMAC, 164
    Syslog, 130–132
        Console, 134
        disabling, 138–139
        organizing, 137

reading, 138
viewing, 134
Microsoft NetMeeting, 124, 283
Microsoft Netshow, 124
models, PIX Firewalls, 27–28
modes
access, 92
LAN failover, 149
monitor, 54–56
stateful failover, 148
modification
access attacks, 5
activation keys, 51–53
monitor mode, 54–56
monitoring
failover events, 146–147
networks, 8
Syslog, 130–132
multimedia
H.323, 315–317
RTSP, 315
support, 124, 314–317

N

N2H2, 248
nameif command, 67, 83, 94
NAS (Network Access Server), 260, 275–279
NAT (Network Address Translation), 74
bidirectional, 79
static, 112–113
nat 0 access-list address translation rule, 112
nat 0 command, 115
nat command, 96
nat/global command, 67
NDG (Network Device Group), 294
negotiation, IKE, 164–167
nesting object groups, 122
NetBIOS Domain Name System, 71
NetMeeting, 283
Network Access Server (NAS), 260, 275–279
Network Address Translation. *See* NAT
network architecture
point-to-point architecture, 7, 26–34, 36–41, 68–78, 84–85
selecting, 7, 26–34, 36–41, 68–78, 84–85
Network Device Group (NDG), 294
network object group, 120
Network Time Protocol (NTP), 102–103
networks
address translation, 29
firewalls, 15–16
packet filtering, 15–16
PIX, 17–18
proxy servers, 16
stateful inspection, 16
monitoring, 8
SAFE, 10
security policies, 3–8
threats, 4
types of attacks, 4–6
VPN, 161
CAs, 167
certificates, 28
clients, 184–187
configuration, 168–180, 386–389
groups, 185
IKE, 164–167
IPSec, 162–164
scalability, 187
troubleshooting, 180–184, 394–395
tunneling, 30, 389–394
vulnerabilities, 3
no fixup protocol ftp command, 124
no url-cache command, 250
node communication, 69
nonce values, 165
NTP (Network Time Protocol), 102–103
ntp authenticate command, 103
ntp authentication command, 103
ntp trusted-key command, 103

O

objectives of network security policies, 7–8
objects, grouping, 119–122
Open System Interconnection (OSI), 15
operating systems
CSACS, 262
installing, 50–53
PDM requirements, 212
upgrading, 53–56
optimizing security, 8
options
crypto maps, 178
VPN groups, 185
organization, Syslog messages, 137
OSI (Open System Interconnection), 15
outbound connections, cut-through proxy, 18, 26–27

P

packets, 67
ActiveX filters, 248
failover, 146–147
filtering, 15–16
parameters
AAA authentication, 280
access-list, 173
cgi-truncate, 251
isakmp policy, 170
longurl-truncate, 251
passwd command, 48
password recovery, 58–59
PAT (Port Address Translation), 72, 75
patches, 4. *See also* vulnerabilities
PDM (PIX Device Manager), 29, 210–226, 282, 324
configuration, 213–226
logging, 133
requirements, 211–213
VPN configuration, 227–238
perimeter security
packet filtering, 15–16
PIX, 17–18
proxy servers, 16
stateful inspection, 16

permit any any command, 173
permit keyword, 173
PFSS (PIX Firewall Syslog Server), 130, 136
phase 1 negotiation, 164
physical security, AAA, 259–262
physical site surveys, performing, 7, 26–34, 36–41, 68–78, 84–85
ping command, 55, 99
ping sweeps, 5
pipes, 131
PIX Device Manager. *See* PDM
PIX Firewall Syslog Server (PFSS), 130, 136
PIX Firewalls, 17–18
  Cisco 501, 30–31
  Cisco 506, 31
  Cisco 515, 33–35
  Cisco 520, 35–38
  Cisco 525, 38–39
  Cisco 535, 39–41
  models, 27–28
point-to-point architecture, 7, 26–34, 36–41, 68–78, 84–85
Point-to-Point Protocol over Ethernet (PPPoE), 188
Point-to-Point Tunneling Protocol (PPTP), 185–187
policies
  filtering, 249
  security, 7–8, 67
Port Address Translation (PAT), 72
ports
  address translation, 29
  fixup command, 122–123
  redirection, 77
  static address translation, 113–114
PPPoE (Point-to-Point Protocol over Ethernet), 188
PPTP (Point-to-Point Tunneling Protocol), 185–187
preshared keys, 165, 171
processes, security, 7
prompts, authentication, 285
protocols
  advanced handling, 123–124
  Auto Update, 57
  FTP, 123–124
  H.323 collection of, 315–317
  L2TP, 185–187
  NTP, 102–103
  object-type, 121
  PPTP, 185–187
  RTSP, 315
  SCEP, 29
  SNMP, 29
  TCP, 68, 114–115
  transport, 67–71
  UDP, 68
proxy servers, 16
public address translation, 29
public keys, CAs, 167

Q

queries, DNS, 5

R

RADIUS (Remote Authentication Dial-In User Service), 262
reading Syslog messages, 138
RealNetworks RealAudio and RealVideo, 124
Real-Time Streaming Protocol (RTSP), 315
reconnaissance attacks, 5
recording global information, 380
recovery, passwords, 58–59
redirection, ports, 77
redundancy, 18
remote access, 48–50. *See also* access
  SSH, 49–50
  Telnet, 48–49
  VPN, 161
Remote Authentication Dial-In User Service (RADIUS), 262
remote office/branch office (ROBO), 31
remote procedure calls (RPC), 71
replication, configuration, 147
reports, Syslog, 130–132
requests, SNMP, 136
requirements
  memory, 50
  PDM, 211–213
resources
  modification access attacks, 5
  unauthorized access to, 5
Restricted Bundle, 41
RIP command, 98
ROBO (remote office/branch office), 31
route command, 98
routing, configuration, 380, 382, 384
RPC (remote procedure call), 71
RTSP (Real-Time Streaming Protocol), 315
rules
  access, 385
  groups, 291

S

SA (security association), 162, 175
SAFE (Secure Blueprint for Enterprise Networks), 10
saving configuration, 100
scalability, VPN, 187
scanning
  block, 5
  Cisco Secure Scanner, 8
  horizontal, 5
  vertical scans, 5
SCEP (Simple Certificate Enrollment Protocol), 29
searching TurboACL, 118–119
Secure Blueprint for Enterprise Networks (SAFE), 10
Secure Hash Algorithm 1 (SHA-1), 164
Secure Intrusion Detection Sensor, 28
secure real-time embedded systems, 17
Secure Shell (SSH) remote access, 49–50
security
  AAA, 259–262
  ASA, 17, 25–26
  attack guards, 317–321
  design, 8
  firewalls, 15–16

packet filtering, 15–16
PIX, 17–18
proxy servers, 16
stateful inspection, 16
intrusion detection, 321–324
configuration, 322–323
dynamic shunning, 323
IPSec, 162–164
levels, 131–132
networks, 3
optimizing, 8
policies, 7–8, 67
process, 7
static NAT, 112–113
testing, 8
threats, 4
traffic
levels, 67
transport protocols, 67–71
types of attacks, 4–6
vulnerabilities, 3
security association (SA), 162
segments, 67, 77
selecting VPN configuration, 168
sending Syslog messages, 134
server command, 55
servers
AAA
configuration, 276–300
identifying, 276–279
specifying, 275
ACS, 28
Auto Update, 57
CSACS, 262–268, 273
authorization, 288
installing, 263–268
users, 288
verifying, 306
DHCP configuration, 101
filters, 248
NAS, 260, 275–279
NetMeeting, 284
PFSS, 130, 136
proxy, 16
Syslog configuration, 135–136
services
authentication, 283
fixup command, 122–123
object-type, 121
SHA-1 (Secure Hash Algorithm), 164
show aaa-server command, 304
show accounting command, 305
show activation-key command, 52
show command, 172, 181, 304, 395
show perfmon command, 252
show url-cache command, 251
show url-server stats command, 252
show version command, 51
show xlate command, 79
shun command, 324
Simple Certificate Enrollment Protocol (SCEP), 29
Simple Network Management Protocol. *See* SNMP
site surveys, performing, 7, 26–34, 36–41, 68–78, 84–85
Site to Site VPN, 161, 227
SNMP (Simple Network Management Protocol), 29
requests, 136
traps, 136
specifying AAA servers, 275
spoofing, 15
SSH (Secure Shell) remote access, 49–50
standby unit, configuration replication, 147
state tables, 17, 25–26
stateful failover, 18, 148
stateful inspection, 16
static command, 77
static IP address mapping, 381
static NAT, 112–113
static port address translation, 113–114
static translation, 72, 75–76
statistics
show url-server stats command, 252
viewing filters, 251
structured threats, 4
Sun Solaris, PDM requirements, 213
support
AAA, 28
DNS, 82
multimedia, 124, 314–317
H.323, 315–317
RTSP, 315
PPPoE, 188
Syslog, 30
X.509 certificates, 28
Syslog, 130–132
configuration, 132–135
messages
disabling, 138–139
organizing, 137
reading, 138
security levels, 131–132
servers, 135–136
support, 30
sysopt connection permit-ipsec command, 180
sysopt security fragguard command, 317
sysopt uauth allow-http-cache command, 281
system clock, 104
system requirements, CSACS, 262

T

tables, state, 17, 25–26
TACACS+ (Terminal Access Controller Access Control System), 262
TCP (Transmission Control Protocol), 68, 114–115
technologies, VPN, 161
Telnet, 48–49
messages, 134
Virtual Telnet, 283
Terminal Access Controller Access Control System (TACACS+), 262
testing
configuration, 99
security, 8
threats, 4
time settings
configuration, 102–104
NTP, 102–103
system clock, 104
timeout uauth command, 286
tokens, X.509 certificate support, 28
traffic
cut-through proxy, 260

firewalls, 15–16
packet filtering, 15–16
PIX, 17–18
proxy servers, 16
stateful inspection, 16
security
levels, 67
transport protocols, 67–71
Transform Set Panel, 229
transform sets
configuration, 175
crypto ipsec transform-set command, 177
translation
addresses, 29, 71–79
commands, 73
NAT, 74
PAT, 75
static, 75–76
troubleshooting, 79–82
bidirectional, 79
multiple configuration, 77–78
slots, 70
static port addresses, 113–114
transport protocols, 67–71
traps, SNMP, 136
Triple Data Encryption Standard (3DES), 164
Trojan horses, 6
troubleshooting
AAA, 303–306
accounting, 305
address translation, 79–82
authentication, 304
authorization, 305
basic configuration, 398–406
boothelper disk, 56–57
object grouping, 119–122
security, 8
Syslog, 130–132
VPN, 180–184, 394–395
tunneling, VPN, 389–394
TurboACL, 118–119
types of attacks, 4–6
access, 5–6
DoS, 6
reconnaissance, 5

U

UDP (User Datagram Protocol), 68
unauthorized access, 5
Unicast RPF (Unicast Reverse Path Forwarding), 324–325
unstructured threats, 4
updating, Auto Update, 57
upgrading
activation keys, 51–53
operating systems, 53–56
upper-level data encapsulation, 68
url-cache command, 250
URLs (Uniform Resource Locators), filtering, 248–252
url-server command, 248
users
accounting, 295–299
authentication, 279–287
authorization, 287–295

V

VDOnet VDOLive, 124
verification
CSACS, 306
IKE configuration, 172
VPN, 394–395
X.509 certificate support, 28
vertical scans, 5
video, AVVID, 9–10
viewing
accounting, 297
filters, 251
logging, 133
messages, 134
virtual circuits, 68
Virtual HTTP, 285
virtual private networks. *See* VPNs
virtual reassembly, 317
virtual service authentication, 283
viruses, 6
Virtual Telnet, 283
VocalTech, 124
voice, AVVID, 9–10
vpdn commands, 185–187
VPN (Virtual Private Network)
CAs, 167
certificates, 28
clients, 184–187
configuration, 168–180, 386–389
troubleshooting, 394–395
tunneling, 389–394
gateways, 30
groups, 185
IKE, 164–167
IPSec, 162–164
PDM configuration, 227–238
scalability, 187
technologies, 161
troubleshooting, 180–184
vulnerabilities, 3
VXtreme WebTheatre, 124

W

Websense, 248
White Pine CuSeeMe, 124
White Pine Meeting Point, 124
Windows 2000
CSACS, 263–268
PDM requirements, 212
Windows NT
CSACS, 263–268
PDM requirements, 212
worms, 6
write memory command, 49, 100
write standby command, 147

X-Z

X.509 certificates support, 28
Xing StreamWorks, 124