Index

Numerics

802.11X, 364

A

acceptable-encryption policies, 74
acceptable-use policies, 74
access attacks, 91–92
access control, 127
 Corportate Internet module, 203–204
 medium-sized network design, 242–243
access control lists (ACLs), SNMP, 144
Access Control Server (ACS), 182–183
 Campus modules, 49
access filtering, Layer 3 switches, 278
access points, 362–363
access switches, Campus module (medium-sized network design), 249
access-group command, 226
accountability policies, 73
ACLs (access control lists), SNMP, 144
ACS (Access Control Server), 182–183
 campus module, 246
Adaptive Security Algorithm (ASA), 161
agents, SNMP, 144
antispoofing, RFC 2827 filtering, 115–116
antivirus policies, 74
application layer attacks, 92
 as threat to IP telephony networks, 340
 mitigating, 117–118
applications
 as targets, 37–38
 hardening, 115
Architecture for Voice, Video, and Integrated Data (AVVID), 5
ASA (Adaptive Security Algorithm), 161
assets, risk assessment, 78
attacks, 85
 application layer attacks, 92
  mitigating, 117–118
 applications, 37–38
 DoS attacks, 90–91, 109
  mitigating, 115–117
 hosts, 35
 IP spoofing, 102
  ISP routers, 218
  mitigating, 127–128
 management traffic attacks, mitigating, 140
 man-in-the-middle attacks, 103–104
  mitigating, 130
 mitigating, policy-based SAFE, 17–18
 networks, 36
 packet sniffers, 102
  mitigating, 128–129
 password attacks, 102–103
  mitigating, 129
 perimeter attacks, 158
  data manipulation, 158
  DoS, 158
  IP spoofing, 158
  malicious, 159
  passive, 158
  port scans, 158
  rerouting attacks, 159
  session hijacks, 158
  unauthorized, 158
 port redirection attacks, 104–105
  mitigating, 130–131
 reconnaissance attacks, 89–90
  mitigating, 114–115
 routers, 33
 switches, 34
 trojan-horse applications, 105
  mitigating, 131

trust exploitation attacks, 92–93

mitigating, 118

unauthorized access attacks, 91–92

virus attacks, mitigating, 131

viruses, 105

audit policies, 75

authentication

applying to user and device, 343

packet sniffers, 128

policies, 73

SAFE, 18–19

Auto Update Server Software (CiscoWorks), 185

availability statements, 73

AVVID (Architecture for Voice, Video, and Integrated Data), 5, 186

Communication Services, 188

Network Infrastructure, 187

Service Control, 187

axioms for SAFE IP Telephony design, 341–344

B

blind-TCP scans, 89

blueprints (SAFE), 17–19

axioms, 32–33

applications are targets, 37–38

hosts are targets, 35

networks are targets, 36–37

routers are targets, 33

switches are targets, 34

design fundamentals, 31–32

intrusion detection, 19–20

medium-sized network design, 233, 237–238

branches, 251

Campus module, 246–250

Corporate Internet module, 238–246

WAN module, 250–251

remote network design, 283, 287–292

configuration, 287–288

design guidelines, 290–292

devices, 288–289

threat mitigation, 288, 290

small network design, 199–200

branches, 207

Campus module, 205–207

Corporate Internet module, 200–204

headend/standalone considerations, 207

small network implementation, 217–218

IDS services, 221

IOS Firewall routers, 219–224

ISP routers, 218–219

PIX Firewall, 224–228

branches

medium-sized network design, 251

small network design, 207

broadband access devices (remote-user networks), 288

bugtraq, 117

Building Distribution module (Enterprise Campus layer), 310–311

design guidelines, 310

mitigating threats to, 310

building module (large IP telephony networks), 349

C

call interception, as threat to IP telephony networks, 338

caller identity spoofing, as threat to IP telephony networks, 339

Campus module (SAFE), 47–48, 205–207
- design alternatives, 51, 207
- design guidelines, 206
- devices, 49–51
- for medium-sized IP telephony networks, 348
- for small IP telephony networks, 347
- medium-sized network design, 246–250
- threat mitigation, 205–206

CatOS switches, generic security configuration, 357–359

CD One (CiscoWorks), 185

CERT (Computer Emergency Response Team), 117

CIA (confidentiality, integrity, and availability), 77

Cisco AVVID (Architecture for Voice, Video, and Integrated Data), 186–188
- Communication Services, 188
- Network Infrastructure, 187
- Service Control, 187

Cisco IOS firewalls, 160–161
- medium-sized networks, 267–268

Cisco PIX firewalls, 161–162

Cisco SAFE Implementation exam, scenarios, 391–392
- answers, 398–407
- branches (21-5), 394
- IKE configuration for IPSec VPNs (21-10), 397
- IPT solution for small networks (21-8), 397
- medium-sized company network design (18-6), 395–396
- medium-sized company network design (21-6), 395
- medium-sized company network design (21-7), 395
- medium-sized network design (18-2), 392
- medium-sized network design (18-3), 393
- medium-sized network design (21-2), 392–393
- medium-sized network design (21-3), 393
- secure wireless network design (21-9), 397
- small company network design (21-4), 394
- small network design (18-1), 391
- small network design (21-1), 391–392

Cisco Secure Access Control Server (ACS), 182–183

Cisco Secure IDS, 162–164, 166

Cisco Secure PIX Firewalls, 179

Cisco Secure Policy Manager (CSPM), 185–186

Cisco View (CiscoWorks), 184

Cisco VPN 3000 Series Concentrators, 179

Cisco VPN clients, 292

CiscoWorks VPN/Security Management Solution (VMS), 184–185

clients (VPNs)
- Cisco VPN clients, 292
- VPN hardware clients, 291–292
- security, 180–182

commands
- access-group, 226
- ip audit IDS in, 221
- permit ip any command, 73

communication policies, 75

Communication Services (AVVID), 188

Computer Emergency Response Team (CERT), 117

concentrators, security, 179–180

confidentiality, IP-based telephony support of, 342

confidentiality, integrity, and availability (CIA), 77

configuring
- CatOS switches, generic security configuration, 357–359
- remote networks, 287–288
- router security, 355–357
- VPNs, medium-sized networks, 271

connectivity, VPNs
- Corporate Internet module, 204
- IOS Firewall routers, 221

control protocols, network management protocols, 143–144

controlling voice-to-data segment interaction, 343

Core module (Enterprise Campus layer), 311

core switches (Campus module), medium-sized network design, 248–249

Corporate Internet module, 200–204
- access control, 203–204
- design alternatives, 204

- design guidelines, 202–204
- Enterprise Edge layer, 51–57, 320
    - *design guidelines for, 321–323*
- filtering, 203–204
- for small IP telephony networks, 346
- intrusion detection, 204
- medium-sized network design
    - *design alternatives, 245–246*
    - *design guidelines, 241–245*
    - *threat mitigation, 240–241*
- threat mitigation, 201–202
- VPN connectivity, 204

corporate servers, campus module, 49, 246

cost-effective deployment of SAFE, 21

cryptography, packet sniffers, 129

CSA software, host IPS, 165–166

- CSA MC, 166
- CSA software, 165–166

CSPM (Cisco Secure Policy Manager), 185–186

D

“day-zero” attacks, 165

DDoS (distributed denial of service) attacks, 91

- ISP routers, 218
- mitigating on medium-sized networks, 265

denial of service (DoS) attacks, 90–91, 109

- mitigating, 115–117

deployment models, 167, 345

designing

- Building Distribution module, guidelines, 311
- Building module, guidelines, 310
- Corporate Internet module, guidelines, 321–323
- E-Commerce module, guidelines, 315–316
- Management module, guidelines, 307–308
- medium-sized networks, 233, 237–238
    - *branches, 251*
    - *Campus module, 246–250*
    - *Corporate Internet module, 238–246*
    - *headend/standalone considerations, 251*
    - *WAN module, 250–251*
- remote networks, 283, 287–292
    - *configuring, 287–288*
    - *design guidelines, 290–292*
    - *devices, 288–289*
    - *threat mitigation, 288, 290*
- SAFE blueprints, 17, 31–32
    - *access authorization, 18*
    - *authentication, 18–19*
    - *axioms, 32–38*
    - Campus module, 51
    - *cost-effective deployment, 21*
    - *emerging networked application support, 21*
    - *intrusion detection, 19–20*
    - *policy-based attack mitigation, 17–18*
    - *security, 17–18*
- Server Module, guidelines, 312
- small network design, 199–200
    - *branches, 207*
    - *Campus module, 205–207*
    - *Corporate Internet module, 200–204*
    - *headend/standalone considerations, 207*
- VPNs
    - *and Remote Access Module, guidelines, 318–319*
    - *security, 188*
- WLANs, 365
    - *EAP WLAN design, 366–367*
    - *IPSec WLAN design, 368–371*
    - *large-enterprise WLAN design, 371–375*
    - *medium-sizednetworkdesign,376–378*
    - *remote network design, 379–380*
    - *small network design, 378–379*

devices

- on medium-sized networks, 264
- on remote networks, 288–289
- rogue, 344
- SAFE Campus module, 49–51

dial-in servers, Corporate Internet module, 53–55, 239

distributed DoS attacks, 91

DNS servers, Corporate Internet module, 53–54, 239

DoS (denial of service) attacks, 90–91, 109

- as threat to IP telephony networks, 340

E

EAP, 364
- large-enterprise WLAN design, 372–373
- medium-sized WLAN design, 376
- small WLAN design, 379
- WLAN design model, 366–367

EAP-TLS (EAP-Transport Layer Security), 365

EAS (Advance Encryption Standard), 365

E-Commerce module (Enterprise Edge layer), 314–316

Edge Distribution module (Enterprise Campus layer), 313

edge routers
- Corporate Internet module, 53–55, 239
- medium-sized networks
  - *ISP traffic filtering, 266*
  - *public VLAN traffic filtering, 267*

encryption, WEP
- alternatives to, 364–365
- enhancements to, 365

Enterprise Campus layer
- Building Distribution module, 310
  - *design guidelines, 311*
- Building module, 310
- Core module, 311
- Edge Distribution module, 313
- Management module, 305
  - *design guidelines, 307–308*
  - *mitigating threats in, 307*
- Server module, 312

Enterprise Edge layer, 314
- Corporate Internet module, 320
  - *design guidelines, 321–323*
- E-Commerce module, 314
  - *mitigating threats to, 315–316*
- VPN and Remote Access module, 317
  - *design guidelines for, 318–319*
- WAN module, 323

external security threats, 22

extranet policies, 74

F

file/web servers, corporate Internet module, 239

file-management protocols, 144

filtering
- access filtering, Layer 3 switches, 278
- Corporate Internet module, 203–204
- inside interface filtering, PIX Firewall, 269–270
- internal traffic filtering
  - *IOS Firewall routers, 222*
  - *PIX Firewall, 226*
- ISP traffic filtering, edge routers, 266
- medium-sized network design, 242–243
- outside interface filtering, PIX Firewall, 225, 268–269
- public services segment filtering, PIX Firewall, 270–271
- public services traffic filtering, PIX Firewall, 226
- public VLAN traffic filtering, edge routers, 267
- remote-access segment filtering, PIX Firewall, 271

firewalls
- Cisco IOS firewalls, 160–161
- Cisco PIX firewalls, 161–162
- Corporate Internet module, 53–54, 239
- packet filtering, 160, 168
- perimiter firewalls, 160–162
- PIX Firewall on small networks, 224–228
- proxy servers, 160, 168
- remote-site firewalls, 290–291
- stateful
  - *controlling voice-to-data segment interaction, 343*
  - *packet filtering, 160, 168*
- VPNs, security, 178

FTP servers, Corporate Internet module, 53–54

G

Gramm-Leach-Bliley Act (GLBA) and the Sarbanes-Oxley Public Company Accounting Reform and Investor Protection Act, 71

H

H.323, 336–337
hardening applications, 115
hardware clients, 181–182
hardware-based VPN WLAN design, 380
headend/standalone considerations, small network design, 207
Health Insurance Portability and Accountability Act (HIPAA), 71
HIDS (host-based intrusion detection system), 48, 163
  medium-sized networks, 275
host-based intrusion detection systems (HIDS). *See* HIDS (host-based intrusion detection system)
host-based IPS (intrusion prevention system), 165
  CSA MC, 166
  CSA software, 165–166
hosts
  as targets, 35
  attacks on, 35
  Corporate Internet module, 54
HTTP servers, Corporate Internet module, 53–54

I

identity management, VPN security, 182–183
IDSs (intrusion detection systems) , 37–38
  Campus module, medium-sized network design, 249
  configuring, PIX Firewall, 227
  medium-sized network design, 243–244
  sensors, 163–164
  services for small networks, 221
IDS Host Sensor (CiscoWorks), 185
IDS management console (MC), 164, 166
IIS directory traversal vunerability, 92
implementing
  medium-sized networks, 259, 264
    devices, 264
    edge routers, 266–267
    HIDS, 275
    IOS Firewall, 267–268
    ISP routers, 265–266
    Layer 3 switches, 277–278
    NIDS, 272–275
    PIX Firewall, 268–272
    VPN 3000 Concentrator, 276
  small networks, 217–218
    IDS services, 221
    IOS Firewall routers, 219–224
    ISP routers, 218–219
    PIX Firewall, 224–228
in-band network management, 139
information technology systems, 73
information-sensitivity policies, 74
initialization-collision attacks, preventing, 368
inside interface filtering on medium-sized networks, 269–270
internal routers, Corporate Internet module, 53, 56
internal security threats, 22
internal traffic filtering
  IOS Firewall routers, 222
  PIX Firewall, 226
internal-lab security policies, 75
Internet DMZ equipment policies, 75
intrusion detection systems (IDSs). *See* IDSs (intrusion detection systems)
IOS Firewall routers, 160–161
  small networks, 219–224
    internal traffic filtering, 222
    public services traffic filtering, 223
    public traffic filtering, 223–224
    VPNs, 221
  medium-sized networks, 267–268
ip audit IDS in command, 221
IP phones, voice/data segmentation, 342
IP spoofing, 102, 158
  as threat to IP telephony networks, 339
  ISP routers, 218
  mitigating, 127–128
    on medium-sized networks, 265
    on remote-user networks, 289
"IP Telephony Security in Depth" whitepaper, 335
IPSec
  designing large-enterprise WLANs, 373–375
  medium WLAN design, 377–378
  VPNs, 364
  WLAN design model, 368–371
    alternative designs, 371
    threats mitigated by, 370

ISP routers
Corporate Internet module, 53, 55
medium-sized networks, 265–266
small network implementation, 218–219
ITU H.323 standard, 336

L

large IP telephony network design, 349
building module, 349
server module, 350–351
large-enterprise WLAN design, 371
EAP model, 372–373
IPSec model, 373, 375
Layer 2 hubs (remote-user networks), 288
Layer 2 services, medium-sized network design, 245
Layer 2 switches
Campus modules, 49–50, 246
Corporate Internet module, 53–55, 239
Layer 3 switches
Campus modules, 49–50, 246
configuring on medium-sized networks, 277–278
LEAP (Lite-EAP), 364
logging protocols, network management protocols, 143

M

man-in-the-middle attacks, 103–104
Management Center for IDS Sensors (CiscoWorks), 185
Management Center for PIX Firewalls (CiscoWorks), 185
Management Center for VPN Routers (CiscoWorks), 185
management hosts, Campus modules, 49–51
Management module (Enterprise Campus layer), 305
design guidelines, 307–308
mitigating threats in, 307
management traffic attacks, mitigating, 140
management VLANs on wireless networks, 375
managers (SNMP), 144
man-in-the-middle attacks, mitigating, 130
on remote-user networks, 289
medium-sized networks
designing, 233, 237–238
branches, 251
Campus module, 246–250
Corporate Internet module, 238–246
headend/standalone cosiderations, 251
WAN module, 250–251
implementing, 259, 264
devices, 264
edge routers, 266–267
HIDS, 275
IOS Firewall, 267–268
ISP routers, 265–266
Layer 3 switches, 277–278
NIDS, 272–275
PIX Firewall, 268–272
VPN 3000 Concentrator, 276
IP telephony networks, Campus module, 348
MGCP (Media Gateway Control Protocol), 337
midsize networks, SAFE implementation, 8
mitigating
attacks
application layer attacks, 117–118
DoS (denial of service) attacks, 115–117
IP spoofing, 127–128
management traffic attacks, 140
man-in-the-middle attacks, 130
password attacks, 129
port redirection attacks, 130–131
reconnaisance attacks, 114–115
trust exploitation attacks, 118
trojan-horse applications, 131
unauthorized access, 117
virus attacks, 131
threats
to Campus module, 205–206
to Corporate Internet module, 201–202, 240–241
to medium-sized network designs, 247–251
to Building module, 310
to E-Commerce module, 315
to remote networks, 288, 290
to Management module, 307

modules, SAFE, 47
Campus module, 47–51
Corporate Internet module, 51–57
WAN module, 58
Monitoring Center for Security (CiscoWorks), 185
monitoring protocols, network management protocols, 143–144
mutual authentication WLAN design model, 366–367

N–O

Network Infrastructure (AVVID), 187
network intrusion detection system (NIDS). ***See*** **NIDS (network intrusion detection system)**
network maintenance policies, 73
network management, 139
in-band network management, 139
out-of-band network management, 139–140
protocols, 140–141
control protocols, 143–144
file-management protocols, 144
logging protocols, 143
monitoring protocols, 143–144
remote-access protocols, 141–143
reporting protocols, 143
time-synchronization protocols, 145
traffic attacks, mitigating, 140
network modules (SAFE), 47
Campus module, 47–51
Corporate Internet module, 51–57
WAN module, 58
network posture visibility, reducing, 114
network reconnaissance attacks, mitigating on remote-user networks, 289
Network Time Protocol (NTP), 141, 145
networks
as targets, 36–37
security threats, 21
external threats, 22
internal threats, 22
structured threats, 21
unstructured threats, 22
NIDS (network intrusion detection system), 47, 163
Campus modules, 49–50, 246
Corporate Internet module, 53, 56, 239
medium-sized networks, 272–275
nondistributed DoS attacks, 90–91
NTP (Network Time Protocol), 141, 145

OOB (out-of-band) networks, 18
OTP (one-time password) servers, campus module, 49, 246
out-of-band (OOB) networks, 18
out-of-band network management, 139–140
outside interface filtering, PIX Firewall, 225
on medium-sized networks, 268–269

P

packet filtering, 160, 168
packet sniffers, 102
mitigating, 128–129
password attacks, 102–103
mitigating, 129
password-protection policies, 75
passwords, testing, 129
PC-based IP phones, susceptibility to attacks, 342
PEAP (Protected EAP), 365
perimeter security, 158
Cisco Secure IDS, 162–166
data manipulation, 158
DoS, 158
firewalls, 160–162
IP spoofing, 158
malicious destruction, 159
passive eavesdropping, 158
port scans, 158
product selection, 166–167
products, 167
rerouting attacks, 159
routers, 159–160
session hijacks, 158
traffic flow filtering on medium-size networks, 242
unauthorized access, 158
permissive security policies, 72
permit ip any command, 73
personal firewall software (remote-user networks), 288

Pfleeger, Charles, 78
PIX Firewall, 161–162
medium-size networks, 268–272
inside interface filtering, 269–270
outside interface filtering, 268–269
public services segment filtering, 270–271
remote-access segment filtering, 271
VPN configuration, 271
small networks, 224–228
IDS configuration, 227
internal traffic filtering, 226
outside interface filtering, 225
VPN configuration, 227–228
policies 67, 72
acceptable-encryption policies, 74
acceptable-use policies, 74
accountability policies, 73
antivirus policies, 74
audit policies, 75
authentication policies, 73
availability statements, 73
communication policies, 75
extranet policies, 74
goals, 76–77
implementing, 79–80
information technology systems, 73
information-sensitivity policies, 74
internal-lab security policies, 75
Internet DMZ equipment policies, 75
network maintenance policies, 73
password-protection policies, 75
permissive policies, 72
primary characteristics, 75
remote-access policies, 74
restrictive policies, 72
risk assessments, 77–78
subpolicies, 73–75
violations-reporting policies, 74
VPN security policies, 75
wireless networking policies, 75
port redirection attacks, 104–105
mitigating, 130–131
port scans, 158
potential threats to wireless networks, 363
alternatives to WEP, 364–365
preventing initialization-collision attacks, 368
protocols, network management, 140–141
control protocols, 143–144
file-management protocols, 144
logging protocols, 143
monitoring protocols, 143–144
remote-access protocols, 141–143
reporting protocols, 143
time-synchronization protocols, 145
proxy servers, 160, 168
public services segment filtering (PIX Firewall), medium-sized networks, 270–271
public services traffic filtering
IOS Firewall routers, 223
PIX Firewall, 226
public traffic filtering, IOS Firewall routers, 223–224
public VLAN traffic filtering on medium-sized networks, 267

R

reconnaissance attacks, 89–90
remote network design, 283, 287–292
configuration, 287–288
design guidelines, 290–292
Cisco VPN clients, 292
medium-sized networks, 244
remote-site firewalls, 290–291
remote-site routers, 291
VPN hardware clients, 291–292
devices, 288–289
threat mitigation, 288–290
remote-access policies, 74
remote-access protocols, network management protocols, 141–143
remote-access segment filtering on medium-size networks, 271
remote-access VPN clients (remote-user networks), 288
remote-site firewalls, 290–291
remote-site routers, 291
remote-user networks, SAFE, 9
reporting protocols, network management protocols, 143
repudiation as threat to IP telephony networks, 339
Resource Manager Essentials, 184
restrictive security policies, 72

RFC 2827 filtering
antispoofing, 115–116
IP spoofing, 127
on medium-sized networks, 266
rogue access points, 363
rogue devices, 344
routers
as targets, 33
configuring security, 355–357
edge routers
Corporate Internet module, 53, 55
on medium-sized networks, 266–267
internal routers on Corporate Internet module, 53, 56
ISP routers
Corporate Internet module, 53, 55
on medium-sized networks, 265–266
perimeter routers, 159–160
remote-site routers, 291
VPNs, security, 178

S

SAFE, 5, 13, 27, 335
axioms, 32–33
applications are targets, 37–38
hosts are targets, 35
networks are targets, 36–37
routers are targets, 33
switches are targets, 34
design, 17, 31–32
philosophy behind, 199
policy-based attack mitigation, 17–18
security, 17–18
Enterprise blueprint, 6–7
IP Telephony design, 10–11
axioms, 341–344
large IP telephony networks, 349–351
medium-sized IP telephony networks, Campus module, 348
network components, 335–336
small IP telephony networks, 345–347
VoIP protocols, 336–337
medium-size network design, 233, 237–238
branches, 251
Campus module, 246–250
Corporate Internet module, 238–246
headend/standalone considerations, 251
WAN module, 250–251
medium-size network implementation, 259, 264
devices, 264
edge routers, 266–267
HIDS, 275
IOS Firewall, 267–268
ISP routers, 265–266
Layer 3 switches, 277–278
NIDS, 272–275
PIX Firewall, 268–272
VPN 3000 Concentrator, 276
network modules, 47
Campus module, 47–51
Corporate Internet module, 51–57
WAN module, 58
remote network design, 9, 283, 287–292
configuration, 287–288
design guidelines, 290–292
devices, 288–289
threat mitigation, 288, 290
securtity
access authorization, 18
authentication, 18–19
cost-effective deployment, 21
emerging networked application support, 21
implementing, 18
intrusion detection, 19–20
managing, 18
policy-based attack mitigation, 17–18
reporting, 18
small network design, 199–200
branches, 207
Campus module, 205–207
Corporate Internet module, 200–204
small network implementation, 217–218
IDS services, 221
IOS Firewall routers, 219–224
ISP routers, 218–219
PIX Firewall, 224–228
white papers
"A Security Blueprint for Enterprise Networks,“ 6–7

"Extending the Security Blueprint to Small, Midsize, and Remote-User Networks," 7–9
"IP Telephony Security in Depth," 10–11
"SAFE Code-Red Attack Mitigation," 11
"SAFE L2 Application Note," 11
"SAFE Nimda Attack Mitigation," 11
"SAFE RPC DCOM/W32/Blaster Attack Mitigation," 11
"SAFE SQL Slammer Worm Attack Mitigation," 11
"Wireless LAN Security in Depth," 10
WLANs, 10
SAFE Implementation exam scenarios, 391–402
script kiddies, 22
SDP (Session Description Protocol), 337
Secure IDS, 162–166
Secure PIX Firewalls, 179
Secure Shell (SSH), 18
Secure Socket Header (SSH), 141–142
Secure Sockets Layer (SSL), 18, 141–142
security
attacks, 85
application layer attacks, 92
applications, 37–38
DoS (denial of service) attacks, 90–91, 109
hosts, 35
IP spoofing, 127–128
man-in-the-middle attacks, 103–104, 130
networks, 36
packet sniffers, 128–129
password attacks, 129
port redirection attacks, 104–105, 130–131
reconnaisance attacks, 89–90
routers, 33
switches, 34
trojan-horse applications, 105, 131
trust exploitation attacks, 92–93
unauthorized access attacks, 91–92
virus attacks, 105, 131
CatOS switches, generic security configuration, 357–359
firewalls, remote-site firewalls, 290–291
IDSs, 37–38
IP spoofing, 102
managing, 38
management traffic attacks, mitigating, 140
mitigating
application layer attacks, 117–118
DoS attacks, 115–117
reconnaissance attacks, 114–115
trust exploitation attacks, 118
unauthorized access, 117
need for, 71–72
NIDS, Campus modules, 50
packet sniffers, 102
password attacks, 102–103
perimiter security, 158
Cisco Secure IDS, 162–166
data manipulation, 158
DoS (denial of service), 158
firewalls, 160–162
IP spoofing, 158
malicious destruction, 159
passive eavesdropping, 158
port scans, 158
products, 166–167
rerouting attacks, 159
routers, 159–160
session hijacks, 158
unauthorized access, 158
policies, 67, 72
acceptable-encryption policies, 74
acceptable-use policies, 74
accountability policies, 73
antivirus policies, 74
audit policies, 75
authentication policies, 73
availability statements, 73
communication policies, 75
extranet policies, 74
goals, 76–77
implementing, 79–80
information technology systems, 73
information-sensitivity policies, 74
internal-lab security policies, 75
Internet DMZ equipment policies, 75
network maintenance policies, 73
password-protection policies, 75
permissive policies, 72
primary characteristics, 75
remote-access policies, 74

restrictive policies, 72
risk assessments, 77–78
subpolicies, 73–75
violations-reporting policies, 74
VPN security policies, 75
wireless networking policies, 75
routers, configuring for, 355–357
SAFE. *See* SAFE
threats, 21
external threats, 22
internal threats, 22
structured threats, 21
unstructured threats, 22
VPNs (virtual private networks), 178
AVVID, 186–188
clients, 180–182
concentrators, 179–180
design considerations, 188
firewalls, 178
identity management, 182–183
managing, 184–186
routers, 178
Security Wheel concept, 79–80
segmenting telephony traffic, 341
selecting perimiter security products, 166–167
sensors (IDS), 163–164
Server module (Enterprise Campus layer), 312
Server module (large IP telephony networks), 350–351
Service Control (AVVID), 187
Simple Network Management Protocol (SNMP). *See* SNMP (Simple Network Mail Protocol)
Simple Network Management Protocol v3 (SNMPv3), 18
single-site campus deployment model, 345
SIP (Session Initiation Protocol), 337
small networks
designing, 199–200
branches, 207
Campus module, 205–207
Corporate Internet module, 200–204
headend/standalone considerations, 207
IP telephony networks, 345–347
implementing, 217–218
IDS services, 221
IOS Firewall routers, 219–224
ISP routers, 218–219
PIX Firewall, 224–228
SMTP servers, Corporate Internet module, 53–54, 239
SNMP (Simple Network Management Protocol), 141–144
ACLs (access control lists), 144
agents, 144
management hosts, campus module, 246
managers, 144
SNMPv3 (Simple Network Management Protocol v3), 18
software clients, 180
software-based VPN WLAN design, 380
SSH (Secure Shell), 18
SSH (Secure Socket Header), 141
SSL (Secure Sockets Layer), 18, 141–142
stateful firewalls, controlling voice-to-data segment interaction, 343
stateful packet filtering, 160, 168
string attacks, 92
structured security threats, 21
subnets, intrusion detection, 19–20
subpolicies, 73–75
susceptibility of wireless networks, 363
alternatives to WEP, 364–365
switched infrastructures, packet sniffers, 128
switches
as targets, 34
CatOS switches, generic security configuration, 357–359
Layer 2 switches
Campus modules, 49–50
Corporate Internet module, 53, 55
Layer 3 switches, Campus modules, 49–50
Sysadmin, Campus modules, 49
Syslog, 141–143
Campus modules, 49, 246

T

TCP intercept, 116
Telnet, 141–142
testing passwords, 129
TFTP (Trivial File Transfer Protocol), 141, 144

threats, 21
external, 22
internal, 22
mitigating
Campus module, 205–206
Corporate Internet module, 201–202, 240–241
medium-sized network design, 247–251
remote networks, 288–290
structured, 21
to IP telephony networks, 338
application layer attacks, 340
call interception, 338
caller identity spoofing, 339
DoS, 340
IP spoofing, 339
repudiation, 339
toll fraud, 339
trust exploitation, 340
unauthorized access, 339
viruses, 338
unstructured, 22
time-synchronization protocols, network management protocols, 145
TKIP (Temporal Key Integrity Protocol), 365
toll fraud as threat to IP telephony networks, 339
traffic-rate limiting, 117
Trivial File Transfer Protocol (TFTP), 141, 144
Trojan-horse attacks, 105
mitigating, 131
on remote-user networks, 289
trust exploitation attacks, 92–93
as threat to IP telephony networks, 340
mitigating, 118

U

unauthorized access attacks, 91–92
as threat to IP telephony networks, 339
mitigating, 117
on remote-user networks, 289
uncontrollable information, 89
unstructured security threats, 22
user workstations, Campus modules, 49

V

violations-reporting policies, 74
virtual private networks (VPNs). ***See*** **VPNs (virtual private networks)**
viruses, 105
as threat to IP telephony networks, 338
mitigating, 131
on remote-user networks, 289
VLANs
management VLANs, on wireless networks, 375
segregation, Layer 3 switches, 277–278
VMS (VPN/Security Management Solution), 184–185
voice and data traffic segmentation, 341
voice servers, securing, 344
VoIP (voice over IP)
H.323, 336–337
MGCP, 337
SIP, 337
VPN 3000 Series Concentrators, 276
VPN and Remote Access module (Enterprise Edge layer), 317–319
VPN Monitor (CiscoWorks), 184
VPN/Security Management Solution (VMS), 184–185
VPNs (virtual private networks), 178
concentrators, Corporate Internet module, 53, 56, 239
configuring
on medium-sized networks, 271
on PIX Firewall, 227–228
connectivity
Corporate Internet module, 204
IOS Firewall routers, 221
firewall routers (remote-user networks), 288
hardware clients, 291–292
IPSec, 364
SAFE, 9
security, 178
AVVID, 186–188
clients, 180–182
concentrators, 179–180
design considerations, 188
firewalls, 178
identity management, 182–183
management, 184–186
policies, 75
routers, 178

vulnerability of wireless networks, 363
alternatives to WEP, 364–365

W

WAN centralized call-processing deployment model, 345
WAN distributed call-processing deployment model, 345
WAN module, 58
medium-sized network design, 250–251
Enterprise Edge layer, 323
WEP
alternatives to, 364–365
enhancements to, 365
white papers, SAFE, 335
"A Security Blueprint for Enterprise Networks," 6–7
"Extending the Security Blueprint to Small, Midsize, and Remote-User Networks," 7–9
"IP Telephony Security in Depth," 10–11
"SAFE Code-Red Attack Mitigation," 11
"SAFE L2 Application Note," 11
"SAFE Nimda Attack Mitigation," 11
"SAFE RPC DCOM/W32/Blaster Attack Mitigation," 11
"SAFE SQL Slammer Worm Attack Migration," 11
"SAFE VPN IPSec Virtual Private Networks," 9
"Wireless LAN Security in Depth," 10
wireless networking
wireless networks
access points, 362–363
management VLANs, 375
policies, 75
vulnerability of, 363
WEP, alternatives to, 364–365
WLANs
designing, 365
EAP WLAN design, 366–367
IPSec WLAN design, 368–371
large-enterprise WLAN design, 371–375
medium-sized network design, 376–378
remote network design, 379–380
small network design, 378–379
WLANs
designing, 365
EAP WLAN design, 366
threats mitigated by, 367
IPSec WLAN design, 368–369
alternative designs, 371
threats mitigated by, 370
large-enterprise WLAN design, 371
EAP model, 372–373
IPSec model, 373–375
management VLANs, 375
medium-sized network design, 376
EAP WLAN design, 376
IPSec WLAN design, 377–378
remote network design, 379–380
SAFE, 10
small network design, 378–379
workstations, Campus modules, 49