Index

A

acceptable-encryption policies, 74
acceptable-use policies, 74
access, controlling, 127
access attacks, 91–92
access control
    Corportate Internet module, 203–204
    medium-sized network design, 242–243
access control lists (ACLs), SNMP, 144
Access Control Server (ACS). *See* ACS (Access Control Server)
access control servers, Campus modules, 49
access filtering, Layer 3 switches, 278
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
answers to Cisco SAFE Implementation exam scenarios, 303–309
antispoofing, RFC 2827 filtering, 115–116
antivirus policies, 74
application layer attacks, 92
    mitigating, 117–118
applications
    as targets, 37–38
    attacks on, 37–38
    hardening, 115
Architecture for Voice, Video, and Integrated Data (AVVID). *See* AVVID
ASA (Adaptive Security Algorithm), 161
assets, identifying, risk assessments, 78
attacks, 85
    application layer attacks, 92
        mitigating, 117–118
    applications, 37–38
    DoS (denial of service) 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
    networks, 36
    packet sniffers, 102
        mitigating, 128–129
    password attacks, 102–103
        mitigating, 129
    perimeter attacks, 158
        data manipulation, 158
        DoS (denial of service), 158
        IP spoofing, 158
        malicious destruction, 159
        passive eavesdropping, 158
        port scans, 158
        rerouting attacks, 159
        session hijacks, 158
        unauthorized access, 158
    port redirection attacks, 104–105
        mitigating, 130–131
    reconnaissance attacks, 89–90
        mitigating, 114–115
    routers, 33
    SAFE, mitigating, 17-18
    switches, 34
    Trojan-horse applications, 105

mitigating, 131
trust exploitation attacks, 92–93
mitigating, 118
unauthorized access attacks, 91–92
virus attacks, 105
mitigating, 131
audit policies, 75
authentication
packet sniffers, 128
policies, 73
SAFE, 18–19
Auto Update Server Software (CiscoWorks), 185
availability statements, 73
AVVID, 5, 186–188
Communication Services, 188
Network Infrastructure, 187
Service Control, 187

B

blind-TCP scans, 89
blueprints (design)
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
SAFE, 17, 31-32
access authorization, 18
architecture, 31
authentication, 18–19
axioms, 32-38
cost-effective deployment, 21
emerging networked application support, 21
intrusion detection, 19–20
policy-based attack mitigation, 17–18
security, 17–18
security implementation, 18
security management, 18
security reporting, 18
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

C

Campus module, 205–207
design alternatives, 207
design guidelines, 206
medium-sized network design, 246–250
threat mitigation, 205–206
Campus module (SAFE), 47–48
alternative designs, 51
devices, 49–51

CatOS switches, generic security configuration, 349–351
CD One (CiscoWorks), 185
CERT (Computer Emergency Response Team), 117
CIA (confidentiality, integrity, and availability), 77
Cisco AVVID. ***See*** **AVVID**
Cisco IOS Firewall, 160-161
medium-sized networks, 267–268
Cisco PIX Firewall, 161–162
Cisco SAFE Implementation exam
scenarios, 299–300
answers, 303–309
branches (18-5), 302
medium-sized company network design (18-6), 302–303
medium-sized network design (18-2), 300–301
medium-sized network design (18-3), 301
small company network design (18-4), 301
small network design (18-1), 299–300
Cisco Secure Access Control Server (ACS), 182–183
Cisco Secure IDS, 162–165
Cisco Secure PIX Firewall, 179
Cisco Secure Policy Manager (CSPM), 185–186
Cisco Secure Scanner, 165–166
Cisco View (CiscoWorks), 184
Cisco VPN 3000 Series Concentrators, 179
Cisco VPN clients, 292
CiscoWorks VPN/Security Management Solution (VMS), 184–185
clients
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, VPNs, security, 179–180
confidentiality, integrity, and availability (CIA), 77
configuration
CatOS switches, generic security configuration, 349–351
remote networks, 287–288
routers, security, 347–349
connectivity, VPNs
Corporate Internet module, 204
IOS Firewall routers, 221
control protocols, network management protocols, 143–144
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
filtering, 203–204
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 Internet module (SAFE), 51–57
corporate servers
Campus module, 49, 246
cost-effective deployment (SAFE), 21
cryptography, packet sniffers, 129
CSPM (Cisco Secure Policy Manager), 185–186

D

data manipulation attacks, 158
DDoS (distributed denial of service) attacks, 91
ISP routers, 218
mitigating, medium-sized networks, 265
denial of service (DoS), 158
attacks, 90–91, 109
mitigating, 115–117

design
medium-sized network design, 233, 237–238
branches, 251
Campus module, 246–250
Corporate Internet module, 238–246
headend/standalone considerations, 251
WAN module, 250–251
remote network design, 283, 287–292
configuration, 287–288
design guidelines, 290–292
devices, 288–289
threat mitigation, 288, 290
SAFE blueprints, 17, 31-32
access authorization, 18
architecture, 31
authentication, 18–19
axioms, 32–38
cost-effective deployment, 21
emerging networked application support, 21
intrusion detection, 19–20
policy-based attack mitigation, 17–18
security, 17–18
security implementation, 18
security management, 18
security reporting, 18
SAFE Campus module, 51
small network design, 199–200
branches, 207
Campus module, 205–207
Corporate Internet module, 200–204
headend/standalone considerations, 207
VPN security, 188
devices
medium-sized networks, 264
remote networks, 288–289
SAFE Campus module, 49–51
dial-in servers, Corporate Internet module, 53-55, 239
distributed DoS attacks. *See* DDoS (distributed denial of service) attacks
DNS servers
Corporate Internet module, 53–54, 239
DoS (denial of service), 158
attacks, 90–91, 109
mitigating, 115

E-F

edge routers
Corporate Internet module, 53, 55, 239
medium-sized networks, 266–267
ISP traffic filtering, 266
public VLAN traffic filtering, 267
external security threats, 22
extranet policies, 74

file/web servers, Corporate Internet module, 239
file-management protocols, network 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
Corporate Internet module, 53–54, 239
IOS Firewalls, 160–161, 222
packet filtering, 160
perimeter firewalls, 160–162
PIX Firewall,161-162, 268-271
small networks, 224–228, 268-271
proxy servers, 160

remote-site firewalls, 290–291
stateful packet filtering, 160
VPNs, security, 178
FTP servers, Corporate Internet module, 53–54

G-H

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

hardening applications, 115
hardware clients, 181–182
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
hosts
as targets, 35
attacks on, 35
Corporate Internet module, 54
HTTP servers, Corporate Internet module, 53–54

I

identity management, VPNs, security, 182–183
IDSs (intrusion detection systems), 37-38
Campus module, medium-sized network design, 249
configuration, PIX Firewall, 227
management console (MC), 165
medium-sized network design, 243–244
sensors, 163-165
Host Sensor (CiscoWorks), 185
small network services, 221
IIS directory traversal vunerability, 92
implementation
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
inside interface filtering, PIX Firewall, 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
Corporate Internet module, 204
SAFE, 19–20
intrusion detection systems (IDSs). ***See*** **IDSs (intrusion detection systems)**
IOS Firewall routers, small networks, 219–224
internal traffic filtering, 222
public services traffic filtering, 223
public traffic filtering, 223–224
VPNs, 221
IOS Firewalls, 160–161
medium-sized networks, 267–268
IP (Internet Protocol), security, SAFE, 10–11
ip audit IDS in command, 221
IP spoofing, 102, 158
ISP routers, 218
mitigating, 127–128
medium-sized networks, 265
remote-user networks, 289
ISP routers
Corporate Internet module, 53, 55
medium-sized networks, 265–266
small network implementation, 218–219
ISP traffic filtering, edge routers, medium-sized networks, 266

L

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, medium-sized networks, 277–278
logging protocols, network management protocols, 143

M

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 traffic attacks, mitigating, 140
managers, SNMP, 144
man-in-the-middle attacks, 103-104
mitigating, 130
remote-user networks, 289
medium-sized network design, 233, 237–238
branches, 251
Campus module, 246–250
Corporate Internet module, 238–246
design alternatives, 245–246
design guidelines, 241–245
threat mitigation, 240–241
headend/standalone cosiderations, 251
SAFE, 8
WAN module, 250–251
medium-sized 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
mitigation
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
packet sniffers, 128–129
password attacks, 129
port redirection attacks, 130–131
reconnaisance attacks, 114–115
threats
Campus module, 205–206
Corporate Internet module, 201–202, 240-241
medium-sized network design, 247–251
remot networks, 288, 290
Trojan-horse applications, 131
trust exploitation attacks, 118
unauthorized access, 117
virus attacks, 131
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

N

Network Infrastructure (AVVID), 187
network intrusion detection system (NIDS). *See* NIDS (network intrusion detection system)
network management, 139
in-band network management, 139
out-of-band network management, 139–140
policies, 73
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, remote-user networks, 289
network scanners, 165
network security database, 166
Network Time Protocol (NTP), 141, 145
NIDS (network intrusion detection system), 47, 163
Campus module, 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

O-P

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

packet filtering, 160
packet sniffers, 102
mitigating, 128–129
passive eavesdropping, 158
password attacks, 102–103
mitigating, 129
password-protection policies, 75
passwords, testing, 129
perimeter security, 158
Cisco Secure IDS, 162–165
Cisco Secure Scanner, 165–166
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
perimeter traffic flow filtering, medium-sized network design, 242
permissive security policies, 72
permit ip any command, 73
personal firewall software (remote-user networks), 288
Pfleeger, Charles, 78
PIX (Private Internet Exchange) Firewalls, 161-162, 178
medium-sized 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, 217
small networks, 224–228
IDS configuration, 227
internal traffic filtering, 226
outside interface filtering, 225
VPN configuration, 227–228
policies, security, 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
posture, networks, visibility reduction, 114
Private Internet Exchange (PIX) Firewalls. ***See*** **PIX (Private Internet Exchange) Firewalls**
protocols, network management 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
proxy servers, 160
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, edge routers, medium-sized networks, 267

R

reconnaissance attacks, 89–90
remote access, medium-sized network design, 244
remote network design, 283, 287–292
configuration, 287–288
design guidelines, 290–292
Cisco VPN clients, 292
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, PIX firewall, medium-sized 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, 38
protocols, network management protocols, 143
SAFE, 18
rerouting attacks, 159
Resource Manager Essentials, 184
restrictive security policies, 72
RFC 2827 filtering
antispoofing, 115–116
IP spoofing, 127
medium-sized networks, 266
routers
as targets, 33
attacks on, 33
configuring, security, 347–349
edge routers
Corporate Internet module, 53, 55
medium-sized networks, 266–267
internal routers, Corporate Internet module, 53, 56
ISP routers
Corporate Internet module, 53, 55
medium-sized networks, 265–266
perimeter routers, 159–160
remote-site routers, 291
VPNs, security, 178

S

SAFE, 5-6, 13, 27
architecture, 31
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
blueprint
design philosophy, 199

design, 17, 31–32
policy-based attack mitigation, 17–18
security, 17–18
Enterprise blueprint, 6–7
Extending the Security Blueprint to Small, Midsize, and Remote-User Networks, 7
IP telephony security, 10–11
IP Telephony Security in Depth, 10
medium-sized 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-sized 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
midsize networks, 8
network modules, 47
Campus module, 47–51
Corporate Internet module, 51–57
WAN module, 58
remote network design, 283, 287–292
configuration, 287–288
design guidelines, 290–292
devices, 288–289
threat mitigation, 288-290
remote-user networks, 9
security
access authorization, 18
authentication, 18–19
cost-effective deployment, 21
emerging networked application support, 21
implementation, 18
intrusion detection, 19–20
management, 18
policy-based attack mitigation, 17–18
reporting, 18
threats, 21-22
small network design, 7-8, 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
VPNs, 9
white papers, 6-11
Wireless LAN Security in Depth, 10
WLANs, 10
SAFE Code-Red Attack Mitigation, 11
SAFE Implementation exam, scenarios, 299–300
answers, 303–309
branches (18-5), 302
medium-sized company network design (18-6), 302–303
medium-sized network design (18-2), 300–301
medium-sized network design (18-3), 301
small company network design (18-4), 301
small network design (18-1), 299–300
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
scanners, Cisco Secure Scanner, 165

scenarios, Cisco SAFE Implementation exam, 299–300
answers, 303–309
branches (18-5), 302
medium-sized company network design (18-6), 302–303
medium-sized network design (18-2), 300–301
medium-sized network design (18-3), 301
small company network design (18-4), 301
small network design (18-1), 299–300
script kiddies, 22
Secure IDS, 162–165
Secure PIX Firewalls, 179
Secure Scanner, 165–166
Secure Shell (SSH), 18
Secure Socket Header (SSH), 141–142
Secure Sockets Layer (SSL), 18, 141–142
security
access authorization, 18
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
authentication, 18–19
CatOS switches, generic security configuration, 349–351
cost-effective deployment, 21
emerging networked application support, 21
firewalls, remote-site firewalls, 290–291
IDSs (intrusion detection systems), 37–38
implementation, 18
intrusion detection, 19–20
IP spoofing, 102
IP telephony, 10–11
management, 18, 38
management traffic attacks, mitigating, 140
mitigation
application layer attacks, 117–118
DoS (denial of service) attacks, 115–117
reconnaissance attacks, 114–115
trust exploitation attacks, 118
unauthorized access, 117
need for, 71–72
NIDS (network intrusion detection system), Campus modules, 50
packet sniffers, 102
password attacks, 102–103
perimeter security, 158
Cisco Secure IDS, 162–165
Cisco Secure Scanner, 165–166
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
policy-based attack mitigation, 17–18
reporting, 18
routers, configuring for, 347–349
threats, 21-22
VPNs (Virtual Private Networks), 178
AVVID, 186–188
clients, 180–182
concentrators, 179–180
design considerations, 188
firewalls, 178
identity management, 182–183
management, 184–186
routers, 178
***Security in Computing*, 78**
Security Wheel concept, 79–80
sensors, IDS sensors, 163–165
Service Control (AVVID), 187
session hijacks, 158
Simple Network Mail Protocol (SNMP). *See* SNMP (Simple Network Mail Protocol),
small network design, 8, 199–200
branches, 207
Campus module, 205–207
design alternatives, 207
design guidelines, 206
threat mitigation, 205–206
Corporate Internet module, 200–204
design alternatives, 204
design guidelines, 202–204
threat mitigation, 201–202
headend/standalone considerations, 207
SAFE Implementation exam scenario, 299–300
small network implementation, 217–218
IDS services, 221
IOS Firewall routers, 219–224
internal traffic filtering, 222
public services traffic filtering, 223
public traffic filtering, 223–224
VPNs, 221
ISP routers, 218–219
PIX Firewall, 224–228
IDS configuration, 227
internal traffic filtering, 226
outside interface filtering, 225
public services traffic filtering, 226
VPN configuration, 227–228
SMTP servers
Corporate Internet module, 53–54, 239
SNMP (Simple Network Management Protocol), 141–144
ACLs (access control lists), 144
agents, 144
management hosts, 246
managers, 144
SNMPv3 (Simple Network Management Protocol v3), 18
software clients, 180
SSH (Secure Socket Header), 141-142
SSL (Secure Sockets Layer), 18, 141-142
stateful packet filtering, 160
string attacks, 92
structured security threats, 21
subnets, intrusion detection, 19–20
subpolicies, security policies, 73–75
switched infrastructures, packet sniffers, 128
switches
as targets, 34
attacks on, 34
CatOS switches, generic security configuration, 349–351
Layer 2 switches
Campus modules, 49–50
Corporate Internet module, 53-55
Layer 3 switches, Campus modules, 49–50
Sysadmin, Campus modules, 49
Syslog (system log), 141-143
campus module, 246
Campus modules, 49

T

TCP intercept, 116
Telnet, 141–142
testing passwords, 129
TFTP (Trivial File Transfer Protocol), 141, 144
threads, identifying, risk assessments, 78
threats, 21
external threats, 22
internal threats, 22
mitigation
Campus module, 205–206
Corporate Internet module, 201–202, 240–241
medium-sized network design, 247–251
remote networks, 288-290
structured threats, 21
unstructured threats, 22
time-synchronization protocols, network management protocols, 145
traffic-rate limiting, 117
Trivial File Transfer Protocol (TFTP), 141, 144
Trojan-horse applications, 105
mitigating, 131
Trojan-horse attacks, mitigating, remote-user networks, 289
trust exploitation attacks, 92–93
mitigating, 118

U-Z

unauthorized access, 158
mitigating, 117
remote-user networks, 289
unauthorized access attacks, 91–92
uncontrollable information, 89
unstructured security threats, 22
user workstations, Campus modules, 49

violations-reporting policies, 74
Virtual Private Networks (VPNs). *See* VPNs (Virtual Private Networks)
virus attacks, 105
mitigating, 131
remote-user networks, 289
VLANs (virtual LANs), segregation, Layer 3 switches, 277–278
VMS (VPN/Security Management Solution), 184–185
VPN concentrators
Corporate Internet module, 53, 56, 239
VPN 3000 Series Concentrator, 276
VPN firewall routers (remote-user networks), 288
VPN hardware clients, 288–292
VPN Monitor (CiscoWorks), 184
VPN/Security Management Solution (VMS), 184–185
VPNs (Virtual Private Networks), 9, 178
configuration
medium-sized networks, 271
PIX Firewall, 227–228
connectivity
Corporate Internet module, 204
IOS Firewall routers, 221
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

WAN module, 58
medium-sized network design, 250–251
white papers (SAFE), 6-11
wireless networking policies, 75
WLANs (wireless LANs), 10
workstations, Campus modules, 49