Index

4	ASA (Adaptive Security Algorithm), 161
acceptable-encryption policies, 74	assets, identifying, risk assessments, 78 attacks, 85
acceptable-use policies, 74	application layer attacks, 92
access, controlling, 127	mitigating, 117–118
access attacks, 91–92	applications, 37–38
access control	DoS (denial of service) attacks, 90–91, 109
Corportate Internet module, 203-204	mitigating, 115–117
medium-sized network design, 242–243	hosts, 35
access control lists (ACLs), SNMP, 144	IP spoofing, 102
Access Control Server (ACS). See ACS	ISP routers, 218
(Access Control Server)	mitigating, 127–128
access control servers, Campus modules,	management traffic attacks, mitigating, 140
49	man-in-the-middle attacks, 103–104
access filtering, Layer 3 switches, 278	mitigating, 130
access switches, campus module, medium-	networks, 36
sized network design, 249	packet sniffers, 102
access-group command, 226	mitigating, 128–129
accountability policies, 73	password attacks, 102–103
ACLs (access control lists), SNMP, 144	mitigating, 129
ACS (Access Control Server), 182–183	perimeter attacks, 158
campus module, 246	data manipulation, 158
Adaptive Security Algorithm (ASA), 161	DoS (denial of service), 158
agents, SNMP, 144	IP spoofing, 158
answers to Cisco SAFE Implementation	malicious destruction, 159
exam scenarios, 303-309	passive eavesdropping, 158
antispoofing, RFC 2827 filtering, 115-116	port scans, 158
antivirus policies, 74	rerouting attacks, 159
application layer attacks, 92	session hijacks, 158
mitigating, 117–118	unauthorized access, 158
applications	port redirection attacks, 104–105
as targets, 37–38	mitigating, 130–131
attacks on, 37–38	reconnaissance attacks, 89–90
hardening, 115	mitigating, 114–115
Architecture for Voice, Video, and Integrated	routers, 33
Data (AVVID). See AVVID	SAFE, mitigating, 17-18
	switches, 34
	Trojan-horse applications, 105

mitigating, 131	headend/standalone considerations,
trust exploitation attacks, 92–93	207
mitigating, 118	SAFE, 17, 31-32
unauthorized access attacks, 91–92	access authorization, 18
virus attacks, 105	architecture, 31
mitigating, 131	authentication, 18–19
audit policies, 75	axioms, 32-38
authentication	cost-effective deployment, 21
packet sniffers, 128	emerging networked application
policies, 73	support, 21
SAFE, 18–19	intrusion detection, 19–20
Auto Update Server Software (CiscoWorks),	policy-based attack mitigation,
185	17–18
availability statements, 73	security, 17–18
AVVID, 5, 186–188	security implementation, 18
Communication Services, 188	security management, 18
Network Infrastructure, 187	security reporting, 18
Service Control, 187	small network implementation, 217–218
Service Connect, 107	IDS services, 221
D	IOS Firewall routers, 219–224
В	ISP routers, 218–219
blind-TCP scans, 89	PIX Firewall, 224–228
blueprints (design)	branches
medium-sized network design, 233, 237–238	medium-sized network design, 251
branches, 251	small network design, 207
Campus module, 246–250	broadband access devices (remote-user
Corporate Internet module,	networks), 288
238–246	bugtraq, 117
WAN module, 250–251	
remote network design, 283, 287–292	C
configuration, 287–288	C
design guidelines, 290–292	Campus module, 205–207
devices, 288–289	design alternatives, 207
threat mitigation, 288, 290	design guidelines, 206
small network design, 199–200	medium-sized network design,
branches, 207	246–250
Campus module, 205–207	threat mitigation, 205–206
Corporate Internet module,	Campus module (SAFE), 47–48
200–204	alternative designs, 51
	devices, 49–51

CatOS switches, generic security	Computer Emergency Response Team
configuration, 349-351	(CERT), 117
CD One (CiscoWorks), 185	concentrators, VPNs, security, 179–180
CERT (Computer Emergency Response	confidentiality, integrity, and availability
Team), 117	(CIA), 77
CIA (confidentiality, integrity, and	configuration
availability), 77	CatOS switches, generic security
Cisco AVVID. See AVVID	configuration,
Cisco IOS Firewall, 160-161	349–351
medium-sized networks, 267–268	remote networks, 287–288
Cisco PIX Firewall, 161–162	routers, security, 347–349
Cisco SAFE Implementation exam	connectivity, VPNs
scenarios, 299-300	Corporate Internet module, 204
answers, 303–309	IOS Firewall routers, 221
branches (18-5), 302	control protocols, network
medium-sized company network	management protocols, 143-144
design (18-6), 302–303	core switches, campus module, medium-
medium-sized network design (18-2),	sized network design,
300–301	248–249
medium-sized network design	Corporate Internet module, 200-204
(18-3), 301	access control, 203-204
small company network design	design alternatives, 204
(18-4), 301	design guidelines, 202-204
small network design (18-1),	filtering, 203–204
299–300	intrusion detection, 204
Cisco Secure Access Control Server (ACS),	medium-sized network design
182–183	design alternatives, 245–246
Cisco Secure IDS, 162–165	design guidelines, 241–245
Cisco Secure PIX Firewall, 179	threat mitigation, 240–241
Cisco Secure Policy Manager (CSPM),	threat mitigation, 201–202
185–186	VPN connectivity, 204
Cisco Secure Scanner, 165–166	Corporate Internet module (SAFE), 51-57
Cisco View (CiscoWorks), 184	corporate servers
Cisco VPN 3000 Series Concentrators, 179	Campus module, 49, 246
Cisco VPN clients, 292	cost-effective deployment (SAFE), 21
CiscoWorks VPN/Security Management	cryptography, packet sniffers, 129
Solution (VMS), 184–185	CSPM (Cisco Secure Policy Manager),
clients	185–186
Cisco VPN clients, 292	
VPN hardware clients, 291–292	D
security, 180–182	U
commands	data manipulation attacks, 158
access-group, 226	DDoS (distributed denial of service)
ip audit IDS in, 221	attacks, 91
permit ip any command, 73	ISP routers, 218
communication policies, 75	mitigating, medium-sized networks, 265
Communication Services (AVVID), 188	denial of service (DoS), 158
	attacks, 90–91, 109
	mitigating, 115–117

design	DoS (denial of service), 158
medium-sized network design, 233,	attacks, 90–91, 109
237–238	mitigating, 115
branches, 251	
Campus module, 246–250	
Corporate Internet module,	E-F
238–246	edge routers
headend/standalone	8
considerations, 251	Corporate Internet module, 53, 55, 239 medium-sized networks, 266–267
WAN module, 250–251	ISP traffic filtering, 266
remote network design, 283, 287–292	public VLAN traffic filtering, 267
configuration, 287–288	external security threats, 22
design guidelines, 290–292	extranet policies, 74
devices, 288–289	extranct poncies, 74
threat mitigation, 288, 290	file/web servers, Corporate Internet module,
SAFE blueprints, 17, 31-32	239
access authorization, 18	file-management protocols, network
architecture, 31	management protocols, 144
authentication, 18–19	filtering
axioms, 32–38	access filtering, Layer 3 switches, 278
cost-effective deployment, 21	Corporate Internet module, 203–204
emerging networked application	inside interface filtering, PIX Firewall, 269-
support, 21	270
intrusion detection, 19–20	internal traffic filtering
policy-based attack mitigation, 17–18	IOS Firewall routers, 222
security, 17–18	PIX Firewall, 226
security implementation, 18	ISP traffic filtering, edge routers, 266
security management, 18	medium-sized network design, 242–243
security reporting, 18	outside interface filtering, PIX Firewall,
SAFE Campus module, 51	225, 268–269
small network design, 199–200	public services segment filtering, PIX
branches, 207	Firewall, 270–271
Campus module, 205–207	public services traffic filtering, PIX
Corporate Internet module, 200–204	Firewall, 226
headend/standalone considerations,	public VLAN traffic filtering, edge routers,
207	267
VPN security, 188	remote-access segment filtering, PIX
devices	Firewall, 271
medium-sized networks, 264	firewalls
remote networks, 288–289 SAFE Campus module, 49–51	Corporate Internet module, 53–54, 239
dial-in servers, Corporate Internet	IOS Firewalls, 160–161, 222
module, 53-55, 239	packet filtering, 160
distributed DoS attacks. See DDoS	perimeter firewalls, 160–162
(distributed denial of service) attacks	PIX Firewall,161-162, 268-271
DNS servers	small networks, 224–228, 268-271
Corporate Internet module, 53–54, 239	proxy servers, 160
±	

remote-site firewalls, 290-291	ISP routers, 265–266
stateful packet filtering, 160	Layer 3 switches, 277–278
VPNs, security, 178	NIDS, 272–275
FTP servers, Corporate Internet module,	PIX Firewall, 268–272
53–54	VPN 3000 Concentrator, 276
	small networks, 217-218
G-H	IDS services, 221
	IOS Firewall routers, 219–224
Gramm-Leach-Bliley Act (GLBA), and the	ISP routers, 218–219
Sarbanes-Oxley Public Company	PIX Firewall, 224–228
Accounting Reform and Investor	in-band network management, 139
Protection Act, 71	information technology systems, 73
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	information-sensitivity policies, 74
hardening applications, 115	inside interface filtering, PIX Firewall,
hardware clients, 181–182	medium-sized networks, 269–270
headend/standalone considerations, small	internal routers, Corporate Internet
network design, 207	module, 53, 56
Health Insurance Portability and	internal security threats, 22
Accountability Act (HIPAA), 71	internal traffic filtering
HIDS (host-based intrusion detection system), 48, 163	IOS Firewall routers, 222
medium-sized networks, 275	PIX Firewall, 226
hosts	internal-lab security policies, 75
as targets, 35	Internet DMZ equipment policies, 75
attacks on, 35	intrusion detection
Corporate Internet module, 54	Corporate Internet module, 204
HTTP servers, Corporate Internet module,	SAFE, 19–20
53–54	intrusion detection systems (IDSs). See IDSs (intrusion detection systems)
	IOS Firewall routers, small networks, 219-
	224
	internal traffic filtering, 222
identity management VDNg geomity	public services traffic filtering, 223
identity management, VPNs, security, 182–183	public traffic filtering, 223–224
IDSs (intrusion detection systems), 37-38	VPNs, 221
Campus module, medium-sized network	IOS Firewalls, 160–161
design, 249	medium-sized networks, 267–268
configuration, PIX Firewall, 227	IP (Internet Protocol), security, SAFE,
management console (MC), 165	10–11
medium-sized network design,	ip audit IDS in command, 221
243–244	IP spoofing, 102, 158
sensors, 163-165	ISP routers, 218
Host Sensor (CiscoWorks), 185	mitigating, 127-128
small network services, 221	medium-sized networks, 265
IIS directory traversal vunerability, 92	remote-user networks, 289
implementation	ISP routers
medium-sized networks, 259, 264	Corporate Internet module, 53, 55
devices, 264	medium-sized networks, 265-266
edge routers, 266–267	small network implementation, 218-219
HIDS, 275	ISP traffic filtering, edge routers, medium-
IOS Firewall. 267–268	sized networks, 266

L	Layer 3 switches, 277–278
Layer 2 hubs (remote-user networks), 288	NIDS, 272–275
Layer 2 services, medium-sized network	PIX Firewall, 268–272
design, 245	VPN 3000 Concentrator, 276
Layer 2 switches	mitigation
Campus modules, 49–50, 246	application layer attacks, 117–118
Corporate Internet module, 53, 55, 239	DoS (denial of service) attacks,
Layer 3 switches	115–117
Campus modules, 49–50, 246	IP spoofing, 127–128
configuring, medium-sized networks,	management traffic attacks, 140 man-in-the-middle attacks, 130
277–278	· · · · · · · · · · · · · · · · · · ·
logging protocols, network management	packet sniffers, 128–129 password attacks, 129
protocols, 143	port redirection attacks, 130–131
r	reconnaisance attacks, 114–115
	threats
M	Campus module, 205–206
Management Center for IDS Sensors	Corporate Internet module,
(CiscoWorks), 185	201–202, 240-241
Management Center for PIX Firewalls	medium-sized network design,
(CiscoWorks), 185	247–251
Management Center for VPN Routers	remot networks, 288, 290
(CiscoWorks), 185	Trojan-horse applications, 131
management hosts, Campus modules,	trust exploitation attacks, 118
49, 51	unauthorized access, 117
management traffic attacks, mitigating, 140	virus attacks, 131
managers, SNMP, 144	modules (SAFE), 47
man-in-the-middle attacks, 103-104	Campus module, 47–51
mitigating, 130	Corporate Internet module, 51–57
remote-user networks, 289	WAN module, 58
medium-sized network design, 233,	Monitoring Center for Security
237–238	(CiscoWorks), 185
branches, 251	monitoring protocols, network
Campus module, 246–250	management protocols, 143-144
Corporate Internet module, 238–246	
design alternatives, 245–246	B.I.
design guidelines, 241–245	N
threat mitigation, 240–241	Network Infrastructure (AVVID), 187
headend/standalone cosiderations, 251	network intrusion detection system (NIDS).
SAFE, 8	See NIDS (network intrusion detection
WAN module, 250–251	system)
medium-sized network implementation,	network management, 139
259, 264	in-band network management, 139
devices, 264	out-of-band network management,
edge routers, 266–267	139–140
HIDS, 275	policies, 73
IOS Firewall, 267–268	protocols, 140–141
ISP routers, 265–266	control protocols, 143–144
	file-management protocols, 144

logging protocols, 143	DoS (denial of service), 158
monitoring protocols, 143–144	firewalls, 160–162
remote-access protocols, 141–143	IP spoofing, 158
reporting protocols, 143	malicious destruction, 159
time-synchronization protocols, 145	passive eavesdropping, 158
traffic attacks, mitigating, 140	port scans, 158
network modules (SAFE), 47	products, 166–167
Campus module, 47–51	rerouting attacks, 159
Corporate Internet module, 51–57	routers, 159–160
WAN module, 58	session hijacks, 158
network posture visibility, reducing, 114	unauthorized access, 158
network reconnaissance attacks,	perimeter traffic flow filtering, medium-sized
mitigating, remote-user networks, 289	network design, 242
network scanners, 165	permissive security policies, 72
network scarners, 105 network security database, 166	permit ip any command, 73
Network Time Protocol (NTP), 141, 145	personal firewall software (remote-user
NIDS (network intrusion detection system),	networks), 288
47, 163	Pfleeger, Charles, 78
	9 ,
Campus module, 49–50, 246	PIX (Private Internet Exchange) Firewalls, 161-162, 178
Corporate Internet module, 53, 56, 239	
medium-sized networks, 272–275	medium-sized networks, 268–272
nondistributed DoS attacks, 90–91	inside interface filtering, 269-270
NTP (Network Time Protocol), 141, 145	outside interface filtering, 268–269
	public services segment filtering,
)-P	270–271
	remote-access segment filtering, 271
OOB (out-of-band) networks, 18	VPN configuration, 217
OTP (one-time password) servers, Campus	small networks, 224–228
modules, 49	IDS configuration, 227
Campus module, 246	internal traffic filtering, 226
out-of-band (OOB) networks, 18	outside interface filtering, 225
out-of-band network management, 139-140	VPN configuration, 227–228
outside interface filtering, PIX Firewall,	policies, security, 67, 72
225	acceptable-encryption policies, 74
medium-sized networks, 268-269	acceptable-use policies, 74
	accountability policies, 73
packet filtering, 160	antivirus policies, 74
packet sniffers, 102	audit policies, 75
mitigating, 128–129	authentication policies, 73
passive eavesdropping, 158	availability statements, 73
password attacks, 102–103	communication policies, 75
mitigating, 129	extranet policies, 74
password-protection policies, 75	goals, 76–77
passwords, testing, 129	implementing, 79–80
perimeter security, 158	information technology systems, 73
Cisco Secure IDS, 162–165	information-sensitivity policies, 74
Cisco Secure Scanner, 165–166	internal-lab security policies, 75
data manipulation, 158	Internet DMZ equipment policies, 75
	network maintenance policies, 73
	password-protection policies, 75

permissive policies, 72	threat mitigation, 288, 290
primary characteristics, 75	remote-access policies, 74
remote-access policies, 74	remote-access protocols, network
restrictive policies, 72	management protocols, 141-143
risk assessments, 77–78	remote-access segment filtering, PIX firewall,
subpolicies, 73–75	medium-sized networks, 271
violations-reporting policies, 74	remote-access VPN clients (remote-user
VPN security policies, 75	networks), 288
wireless networking policies, 75	remote-site firewalls, 290–291
port redirection attacks, 104–105	remote-site routers, 291
mitigating, 130–131	remote-user networks (SAFE), 9
port scans, 158	reporting, 38
posture, networks, visibility reduction, 114	protocols, network management protocols,
Private Internet Exchange (PIX) Firewalls.	143
See PIX (Private Internet Exchange)	SAFE, 18
Firewalls	rerouting attacks, 159
protocols, network management protocols,	Resource Manager Essentials, 184
140–141	restrictive security policies, 72
control protocols, 143–144	RFC 2827 filtering
file-management protocols, 144	antispoofing, 115–116
logging protocols, 143	IP spoofing, 127
monitoring protocols, 143–144	medium-sized networks, 266
remote-access protocols, 141–143	routers
reporting protocols, 143	as targets, 33
time-synchronization protocols, 145	attacks on, 33
proxy servers, 160	configuring, security, 347–349
public services segment filtering, PIX	edge routers
Firewall, medium-sized networks,	Corporate Internet module, 53, 55
270–271	medium-sized networks, 266–267
public services traffic filtering	internal routers, Corporate Internet module,
IOS Firewall routers, 223	53,56
PIX Firewall, 226	ISP routers
public traffic filtering, IOS Firewall routers,	Corporate Internet module, 53, 55
223–224	medium-sized networks, 265–266
public VLAN traffic filtering, edge routers,	perimeter routers, 159–160
medium-sized networks, 267	remote-site routers, 291
	VPNs, security, 178
1	S
reconnaissance attacks, 89–90	SAFE 5 6 13 27
remote access, medium-sized network design,	SAFE, 5-6, 13, 27
244	architecture, 31 axioms, 32–33
remote network design, 283, 287–292	applications are targets, 37–38
configuration, 287–288	hosts are targets, 35
design guidelines, 290–292	nosis are targets, 35 networks are targets, 36–37
Cisco VPN clients, 292	routers are targets, 33
remote-site firewalls, 290–291	switches are targets, 34
remote-site routers, 291	blueprint
VPN hardware clients, 291–292	design philosophy, 199
devices, 288–289	uesign phhosophy, 199

design, 17, 31–32	reporting, 18
policy-based attack mitigation, 17–18	threats, 21-22
security, 17–18	small network design, 7-8, 199-200
Enterprise blueprint, 6–7	branches, 207
Extending the Security Blueprint to Small,	Campus module, 205–207
Midsize, and Remote-User Networks, 7	Corporate Internet module, 200–20-
IP telephony security, 10–11	small network implementation, 217-218
IP Telephony Security in Depth, 10	IDS services, 221
medium-sized network design, 233,	IOS Firewall routers, 219–224
237–238	ISP routers, 218–219
branches, 251	PIX Firewall, 224–228
Campus module, 246–250	VPNs, 9
Corporate Internet module, 238–246	white papers, 6-11
headend/standalone	Wireless LAN Security in Depth, 10
considerations, 251	WLANs, 10
WAN module, 250–251	SAFE Code-Red Attack Mitigation, 11
medium-sized network implementation,	SAFE Implementation exam, scenarios,
259, 264	299–300
devices, 264	answers, 303–309
edge routers, 266–267	branches (18-5), 302
HIDS, 275	medium-sized company network design
IOS Firewall, 267–268	(18-6), 302–303
ISP routers, 265–266	medium-sized network design (18-2),
Layer 3 switches, 277–278	300–301
NIDS, 272–275	medium-sized network design
PIX Firewall, 268–272	(18-3), 301
VPN 3000 Concentrator, 276	small company network design
midsize networks, 8	(18-4), 301
network modules, 47	small network design (18-1),
Campus module, 47–51	299–300
Corporate Internet module, 51–57	SAFE L2 Application Note, 11
WAN module, 58	SAFE Nimda Attack Mitigation, 11
remote network design, 283, 287–292	SAFE RPC DCOM/W32/Blaster Attack
configuration, 287–288	Mitigation, 11
design guidelines, 290–292	SAFE SQL Slammer Worm Attack
devices, 288–289	Mitigation, 11
threat mitigation, 288-290	scanners, Cisco Secure Scanner, 165
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	

scenarios, Cisco SAFE Implementation	IDSs (intrusion detection systems), 37–38
exam, 299–300	implementation, 18
answers, 303–309	intrusion detection, 19–20
branches (18-5), 302	IP spoofing, 102
medium-sized company network design	IP telephony, 10–11
(18-6), 302–303	management, 18, 38
medium-sized network design (18-2),	management traffic attacks, mitigating, 140
300–301	mitigation
medium-sized network design	application layer attacks, 117–118
(18-3), 301	DoS (denial of service) attacks,
small company network design	115–117
(18-4), 301	reconnaissance attacks, 114–115
small network design (18-1), 299-300	trust exploitation attacks, 118
script kiddies, 22	unauthorized access, 117
Secure IDS, 162–165	need for, 71–72
Secure PIX Firewalls, 179	NIDS (network intrusion detection system),
Secure Scanner, 165–166	Campus modules, 50
Secure Shell (SSH), 18	packet sniffers, 102
Secure Socket Header (SSH), 141–142	password attacks, 102-103
Secure Sockets Layer (SSL), 18, 141–142	perimeter security, 158
security	Cisco Secure IDS, 162–165
access authorization, 18	Cisco Secure Scanner, 165–166
attacks, 85	data manipulation, 158
application layer attacks, 92	DoS (denial of service), 158
applications, 37–38	firewalls, 160–162
DoS (denial of service) attacks,	IP spoofing, 158
90–91, 109	malicious destruction, 159
hosts, 35	passive eavesdropping, 158
IP spoofing, 127–128	port scans, 158
man-in-the-middle attacks,	products, 166–167
103–104, 130	rerouting attacks, 159
networks, 36	routers, 159–160
packet sniffers, 128–129	session hijacks, 158
password attacks, 129	unauthorized access, 158
port redirection attacks, 104–105,	policies, 67, 72
130–131	acceptable-encryption policies, 74
reconnaisance attacks, 89–90	acceptable-use policies, 74
routers, 33	accountability policies, 73
switches, 34	antivirus policies, 74
Trojan-horse applications, 105, 131	audit policies, 75
trust exploitation attacks, 92–93	authentication policies, 73
unauthorized access attacks, 91–92	availability statements, 73
virus attacks, 105, 131	communication policies, 75
authentication, 18–19	extranet policies, 74
CatOS switches, generic security	goals, 76–77
configuration, 349–351	implementing, 79–80
cost-effective deployment, 21	information technology systems, 73
emerging networked application support, 21	information-sensitivity policies, 74
firewalls, remote-site firewalls, 290-291	internal-lab security policies, 75

Internet DMZ equipment policies, 75	internal traffic filtering, 222
network maintenance policies, 73	public services traffic filtering, 223
password-protection policies, 75	public traffic filtering, 223–224
permissive policies, 72	VPNs, 221
primary characteristics, 75	ISP routers, 218–219
remote-access policies, 74	PIX Firewall, 224–228
restrictive policies, 72	IDS configuration, 227
risk assessments, 77–78	internal traffic filtering, 226
subpolicies, 73–75	outside interface filtering, 225
violations-reporting policies, 74	public services traffic filtering, 226
VPN security policies, 75	VPN configuration, 227–228
wireless networking policies, 75	SMTP servers
policy-based attack mitigation, 17–18	Corporate Internet module, 53–54, 239
reporting, 18	SNMP (Simple Network Management
routers, configuring for, 347–349	Protocol), 141–144
threats, 21-22	ACLs (access control lists), 144
VPNs (Virtual Private Networks), 178	agents, 144
AVVID, 186–188	management hosts, 246
clients, 180–182	managers, 144
concentrators, 179–180	SNMPv3 (Simple Network Management
design considerations, 188	Protocol v3), 18
firewalls, 178	software clients, 180
identity management, 182–183	SSH (Secure Socket Header), 141-142
management, 184–186	SSL (Secure Sockets Layer), 18, 141-142
routers, 178	stateful packet filtering, 160
Security in Computing, 78	string attacks, 92
Security Wheel concept, 79–80	structured security threats, 21
sensors, IDS sensors, 163–165	subnets, intrusion detection, 19-20
Service Control (AVVID), 187	subpolicies, security policies, 73-75
session hijacks, 158	switched infrastructures, packet sniffers,
Simple Network Mail Protocol (SNMP). See	128
SNMP (Simple Network Mail	switches
Protocol),	as targets, 34
small network design, 8, 199-200	attacks on, 34
branches, 207	CatOS switches, generic security
Campus module, 205–207	configuration,
design alternatives, 207	349–351
design guidelines, 206	Layer 2 switches
threat mitigation, 205–206	Campus modules, 49–50
Corporate Internet module, 200–204	Corporate Internet module,
design alternatives, 204	53-55
design guidelines, 202–204	Layer 3 switches, Campus modules, 49-50
threat mitigation, 201–202	Sysadmin, Campus modules, 49
headend/standalone considerations, 207	Syslog (system log), 141-143
SAFE Implementation exam scenario,	campus module, 246
299–300	Campus modules, 49
small network implementation, 217–218	
IDS services, 221	
IOS Firewall routers, 219–224	

	VLANs (virtual LANs), segregation, Layer
	3 switches, 277–278
TCP intercept, 116	VMS (VPN/Security Management
Telnet, 141–142	Solution), 184–185
testing passwords, 129	VPN concentrators
TFTP (Trivial File Transfer Protocol),	Corporate Internet module, 53, 56, 239
141, 144	VPN 3000 Series Concentrator, 276
threads, identifying, risk assessments, 78	VPN firewall routers (remote-user
threats, 21	networks), 288
external threats, 22	VPN hardware clients, 288–292
internal threats, 22	VPN Monitor (CiscoWorks), 184
mitigation	VPN/Security Management Solution
Campus module, 205–206	(VMS), 184–185
Corporate Internet module,	VPNs (Virtual Private Networks), 9, 178
201–202, 240–241	
medium-sized network design,	configuration
247–251	medium-sized networks, 271
remote networks, 288-290	PIX Firewall, 227–228
structured threats, 21	connectivity
unstructured threats, 22	Corporate Internet module, 204
*	IOS Firewall routers, 221
time-synchronization protocols, network	security, 178
management protocols, 145	AVVID, 186–188
traffic-rate limiting, 117	clients, 180–182
Trivial File Transfer Protocol (TFTP),	concentrators, 179–180
141, 144	design considerations, 188
Trojan-horse applications, 105	firewalls, 178
mitigating, 131	identity management, 182–183
Trojan-horse attacks, mitigating,	management, 184–186
remote-user networks, 289	policies, 75
trust exploitation attacks, 92-93	routers, 178
mitigating, 118	10mers, 170
	WAN module, 58
	medium-sized network design, 250–251
U-Z	
~ _	white papers (SAFE), 6-11
unauthorized access, 158	wireless networking policies, 75
mitigating, 117	WLANs (wireless LANs), 10
remote-user networks, 289	workstations, Campus modules, 49
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	
remote-user networks, 209	