INDEX

Numerics access-class command interactive access control (infrastructure security), 62 802.1x, 219 accounting, 23 access layer (IP telephony), 271 ACL authentication negotiation schemes, 220 blocking unauthorized hosts/users from routers, authenticators, 26 components of, 219 exception ACL, configuring, 64 configuring Secure ACS Servers, 229, 232–233 ACL (Access Control Lists), 157 configuring with EAP-FAST in Unified controlling FWSM access via, 317-321 Wireless Solutions, 226 iACL (infrastructure Access Control Lists) EAP methods, 220-221 infrastructure security policy enforcement, IEEE 802.1x, 26 supplicants, 26 IPv6 filtering, 331–332 rACL (receive Access Control Lists) infrastructure security, 78–80 VACL, 157 action plans, building, 173-174 active-standby failovers identity and trust (SAVE framework), 183-184 ASA, configuring on infrastructure devices, configuring medium-sized business case studies, medium-sized business case studies, 394-396, 398-399 400-401 **AES (Advanced Encryption Standard)** AAA (Authentication, Authorization, encryption protocol Accounting), 23 WEP, 218 identity management solutions/systems, 26 AIP-SSM IBNS, 26 ASA, configuring on IEEE 802.1x, 26 medium-sized business case studies, **RADIUS**, 23, 25 391-394 TACACS+, 25 Aironet AP (Access Points) aaa authorization command, 65 managing, 216 aaa new-model command, 65 analyzing data access control postmortems, 169 small business case study, 352 anomaly detection access layer (IP telephony), 265, 272 IPS devices, 137-138 802.1x, 271 visibility (SAVE framework), 190 ARP, 270 anomaly detection systems, 22 **BPDU**, 268 anomaly detection zones DAI, 270 isolation and virtualization (SAVE framework), DHCP snooping, 269-270 198 NAC, 271 anomaly/telemetry detection port security, 268-269 CS-MARS, 121-122, 125 root guards, 268 Guard XT, 127, 129-131 VLAN assignment, 267 IPS, 137-138

NAM, 125-126

NetFlow, 108	ASA
Cisco platform support, 108	active-standby failovers, configuring
collecting CLI statistics, 112–114	medium-sized business case studies,
Egress NetFlow, 111	394–396, 398–399
enabling, 111–112	AIP-SSM, configuring
flows, elements of, 109	medium-sized business case studies,
flows, exporting data from, 110	391–394
flows, obtaining additional information	ASA security appliances
from, 109–110	enabling SYSLOG logging on, 117–118, 121
Ingress NetFlow, 111	Atlanta Office Cisco IOS configuration (small
IPFIX WG, 110	business case studies)
NDE packet templates, 110	configuring, 360
open source monitoring tools, 126–127	locking down IOS routers, 360, 363, 366,
SNMP, 118–119	368, 370–375
enabling IOS router/switch logging,	NAT configuration, 376
119–121	site-to-site VPN, 377, 380–381, 383, 385,
enabling logging on ASA security	387, 389
appliances, 121	attacks
enabling logging on PIX security	large business case studies, 419–420
appliances, 121	authentication, 23
SYSLOG, 115	HTTP
enabling IOS router/switch logging,	infrastructure security, 63
115–116	RADIUS, 23, 25
enabling logging on ASA security	routing protocols
appliances, 117–118	identity and trust (SAVE framework), 189
enabling logging on CATOS running	infrastructure security, 68–69
catalyst swtiches, 117	tunneled authentication, 224
enabling logging on PIX security	wireless networks, 216
appliances, 117–118	802.1x, 219–221, 226, 229, 232–233
TAD XT, 127–128, 131	configuring CSSC, 233–234, 236
anomaly-based analysis, 21	configuring WLC, 226, 228
antispoofing	EAP-FAST, 224–226, 229, 232–233
small business case study, 353	<i>EAP-GTC</i> , 225
antispoofing techniques, 141	EAP-MD5, 221–222
AP (Access Points)	EAP-TLS, 223
Aironet	EAP-TTLS, 224
managing, 216	LEAP, 222
autonomous mode, 215	PEAP, 223, 225
LWAPP, 215	WEP, 216–218
unified mode, 215	WPA, 218
Unified Wireless Architectures, 215	authentication banners
ARP (Address Resolution Protocol)	configuring
access layer (IP telephony), 270	infrastructure security, 62
proxy ARP	Authentication Servers (802.1x), 219
infrastructure security, disabling for, 73	authenticators (802.1x), 26, 219 authorization, 23

auto secure command	case studies
infrastructure security, 84–85	large businesses, 401, 403
autonomous mode (AP), 215	CSIRT, 403
Autopsy (Linux forensics tool), 162–163	incident response, 419–420
AutoSecure (Cisco IOS)	IPsec remote access VPN,
infrastructure security, 84–88	406, 408, 411–412, 415–417
	load-balancing, 415–417
	security policy creation, 404–406
В	medium-sized businesses, 389
	configuring AAA on infrastructure devices,
backscatter, 146	400–401
banners	configuring active-standby failovers on
authentication banners	ASA, 394–396, 398–399
configuring for infrastructure security, 62	configuring AIP-SSM on ASA, 391–394
base metrics (CVSS), 51	Internet edge routers, 391
BGP (Border Gateway Protocol)	small businesses, 341–343, 360
routers	access control, 352
hop-by-hop tracebacks, 146	antispoofing configuration, 353
black-box penetration testing, 46	Identity NAT, 351
bogon addresses, 37	IM, 354–355, 357–359
BOOTP servers	IP addressing/routing, 343
infrastructure security, disabling for, 73	locking down IOS routers, 360, 363, 366,
botnets	368, 370–375
	NAT configuration, 376
hop-by-hop tracebacks, 145	PAT, 347
BGP routers, 146 Shadowserver.com website, 145	site-to-site VPN, 377, 380–381, 383, 385,
tracebacks, 150	387, 389
bots, 99	Static NAT, 349
BPDU (Bridge Protocol Data Units)	catalyst switches
IP telephony	CATOS running switches
1 2	enabling SYSLOG logging on, 117
access layer, 268 broadcast amplification attacks. See smurf	CATOS (Catalyst Operating System)
attacks, 334	catalyst switches
attacks, 554	enabling SYSLOG logging on, 117
	CDP
C	visibility (SAVE framework), 191
O	CDP (Cisco Discovery Protocol)
CAM (Clean Access Manager) NAC Appliance	infrastructure security, disabling for, 71
CAM (Clean Access Manager), NAS Appliance,	CEF tables
27, 31	visibility (SAVE framework), 191
CAS (Clean Access Servers), NAC Appliance,	Centralized Deployment mode (CAS), 31
27–28	change management policies
Centralized Deployment mode, 31	large business case studies, 406
Edge Deployment mode, 30	changeto context command
Real IP mode, 29	FWSM configuration for data center
Virtual Gateway mode, 28	segmentation, 312
	000111011101111111111111111111111111111

checklists	flows, elements of, 109
incident-handling policies, 154–155	flows, exporting data from, 110
CIRCA (Cisco Incident Response	flows, obtaining additional information
Communications Arena), 54	from, 109–110
Cisco Catalyst switches	Ingress NetFlow, 111
data center segmentation, configuring for,	IPFIX WG, 110
309–310	NDE packet templates, 110
Cisco Guard	network visibility, 101, 103, 106-107
active verification	open source monitoring tools, 126–127
identity and trust (SAVE framework), 185	SNMP, 118–119
data center security, 302	enabling IOS router/switch logging,
Cisco IOS	119–121
AutoSecure	enabling logging on ASA security
infrastructure security, 84–88	appliances, 121
Cisco Personal Assistant	enabling logging on PIX security
securing, 289	appliances, 121
hardening operating environment,	SYSLOG, 115
289–290	enabling IOS router/switch logging,
server security policies, 291–293	115–116
Cisco Security Center, 50	enabling logging on ASA security
Cisco Unified CallManager (IP telephony),	appliances, 117–118
securing, 276–277	enabling logging on CATOS running
Cisco Unified CME (Communications Manager	catalyst switches, 117
Express)	enabling logging on PIX security
securing, 277–281	appliances, 117–118
Cisco Unity	TAD XT, 127–128, 131
securing, 281–282, 286–287	Clean Access Agents (NAC appliance), 27
TCP/UDP ports, 282–285	CLI
Cisco Unity Express	NetFlow statistics
securing, 287–288	collecting, 112–114
classifying security threats	CLI Views
CS-MARS, 121–122, 125	enable view command, 65
Guard XT, 127, 129–131	infrastructure security, 64–65
IDS, 131	isolation and virtualization (SAVE framework),
signature updates, 131–132	197
tuning, 133–134, 136	Lawful intercept views, 64
IPS, 131	parser view command, 65
anomaly detection, 137–138	Root views, 64
IDM, 132	Superviews, 64
signature updates, 131–132	username command, 65
tuning, 133–134, 136	collaboration (incident-handling policies/
NAM, 125–126	procedures), 153
NetFlow, 108	collecting data
Cisco platform support, 108	postmortems, 169
collecting CLI statistics, 112–114	Computer Fraud and Abuse Act, 156
Egress NetFlow, 111	confidentiality
enabling, 111–112	penetration tests, 48
	r

instrumentation and management (SAVE framework), 195 configuration rollback feature (IOS) instrumentation and management (SAVE framework), 195 Configure EAP Method screen (CSSC), 234 configuring authentication banners infrastructure security, 62 exception ACL, 64 NAT small business case study, 376 COPM (Cisco Operational Process Model), threat modeling, 45 COPM (Cisco Operational Process Model), threat modeling, 45 COPM (Coor operational Process Model), see SAVE, 177 COPM (Control Plane Policing) CPU traffic infrastructure security, 80 core layer (IP telephony), 265, 275 correlation (SAVE framework), 192 CSA-MC, 193 CS-MARS, 193 Peakflow SP, 193 Peakflow NS, 193 CPUU CoPP infrastructure security, 80 filtering traffic sent to infrastructure security, 78 interrupt time processors versus (infrastructure security, 78 packet registration infrastructure security, 78 processors versus (infrastructure security), 78 processors versus (infrastructure security), 78 pracket limiting traffic infrastructure security, 78 processors interrupt time versus (infrastructure security), 78 rACL Linfrastructure security, 78-80 rate limiting traffic infrastructure security, 78-80 rate limiting traffic infrastructure security, 78 seheduler allocate command configuring cagent kits, 326 CCSA (Cisco Security Agents) data centers, deploying for, 325 CCSA (Cisco Security Agents) data centers, deploying for, 325 CCSA (Cisco Security Agents) data centers, deploying for, 325 CCSA (Cisco Security Agents) data centers, deploying for, 325 CCSA (Cisco Security Agents) data centers, deploying for, 325 CCSA (Cisco Security Agents) data centers, deploying for, 325 CCSA (Cisco Security Agents) data centers, deploying for, 325 CCSA (Cisco Security Agents) data centers, deploying for, 325 CCSA (Cisco Security Agents) data centers, deploying for, 325 CCSA (Cisco Security Agents) data centers, deploying for, 325 CCSA (Cisco Security Agents) data centers, deploying for, 325 CCSA (Cisco Security Agents) data centers, deploying for, 325 CCSA (C	configuration logger (IOS)	CPU threshold notifications, 76
eonfiguration rollback feature (IOS) instrumentation and management (SAVE framework), 195 Configure EAP Method screen (CSSC), 234 configuring authentication banners infrastructure security, 62 exception ACL, 64 NAT small business case study, 376 COPM (Cisco Operational Process Model), threat modeling, 45 COPM (Cisco Operational Process Model), threat modeling, 45 COPM (Cisco Operational Process Model), threat modeling, 45 COPM (Cisco Operational Process Model), safe functure security, 80 CPU traffic infrastructure security, 80 CS-MARS, 193 CS-MARS, 193 CS-MARS, 193 Peakflow SP, 193 Peakflow SP, 193 Peakflow X, 193 CPU COPP (COPP (CoPP (CoPP (CoPP (Corp) (CoPP (Corp) (Correlation (SAVE framework), 192 (CSA-MC, 193 (CS-MARS, 193 (CS-MARS, 193 (CS-MARS, 193 (CSM (Cisco Security Manager)		
eonfiguration rollback feature (IOS) instrumentation and management (SAVE framework), 195 Configure EAP Method screen (CSSC), 234 configuring authentication banners infrastructure security, 62 exception ACL, 64 NAT small business case study, 376 COPM (Cisco Operational Process Model), threat modeling, 45 COPM (Cisco Operational Process Model), threat modeling, 45 COPM (Cisco Operational Process Model), threat modeling, 45 COPM (Cisco Operational Process Model), safe functure security, 80 CPU traffic infrastructure security, 80 CS-MARS, 193 CS-MARS, 193 CS-MARS, 193 Peakflow SP, 193 Peakflow SP, 193 Peakflow X, 193 CPU COPP (COPP (CoPP (CoPP (CoPP (Corp) (CoPP (Corp) (Correlation (SAVE framework), 192 (CSA-MC, 193 (CS-MARS, 193 (CS-MARS, 193 (CS-MARS, 193 (CSM (Cisco Security Manager)	framework), 195	CSA (Cisco Security Agent), 11
framework), 195 Configure EAP Method screen (CSSC), 234 configuring authentication banners infrastructure security, 62 exception ACL, 64 NAT small business case study, 376 COPM (Cisco Operational Process Model), threat modeling, 45 COPM (Cisco Operational Process Model), See SAVE, 177 COPP (Control Plane Policing) CPU traffic infrastructure security, 80 core layer (IP telephony), 265, 275 correlation (SAVE framework), 192 CSA-MC, 193 CS-MARS, 193 Peakflow SP, 193 Peakflow SP, 193 Peakflow X, 193 CPU COPP infrastructure security, 80 filtering traffic sent to infrastructure security, 78 interrupt time processors versus (infrastructure security, 78 packet registration infrastructure security, 78 processors interrupt time versus (infrastructure security, 78 processors interrupt time versus (infrastructure security, 78 processors interrupt time versus (infrastructure security, 78 rACL infrastructure security, 78 racl infrastructure security, 78 scheduler allocate command data centers, deploying agent kits, 326 CSA-MC (Cisco Security Agent Management Console correlation (SAVE framework), 193 CSIRT postmortems large business case studies, 419–420 CSIRT (Computer Security Incident Response Teams), 52 incident response collaborative teams, 54 large business case studies, 403 responsibilities of, 54 CSM CSM (Cisco Security Manager) instrumentation and management (SAVE framework), 195 CS-MARS CS-MARS, 193 CS-MARS	configuration rollback feature (IOS)	endpoint security, 92–94
Configure EAP Method screen (CSSC), 234 configuring authentication banners infrastructure security, 62 exception ACL, 64 NAT Small business case study, 376 COPM (Cisco Operational Process Model), threat modeling, 45 COPM (Cisco Operational Process Model), See SAVE, 177 CoPP (Control Plane Policing) CPU traffic infrastructure security, 80 core layer (IP telephony), 265, 275 correlation (SAVE framework), 193 CS-MARS, 193 Peakflow X, 193 CPU COPP infrastructure security, 80 filtering traffic sent to infrastructure security, 78 interrupt time processors versus (infrastructure security), 78 packet registration infrastructure security, 78 processors interrupt time versus (infrastructure security), 78 processors interrupt time versus (infrastructure security), 78 rACL infrastructure security, 78 scheduler allocate command configuring agent kits, 326 CSA architectures, 325–326 phased deployments, 326–327 CSA-MC (Cisco Security Agent Mangement Console) CSA-MC (Cisco Security Agent Mangement Console) CSIRT (Computer Security Incident Response Teams), 52 incident response collaborative teams, 54 large business case studies, 419–420 CSIRT (Computer Security Incident Response Teams), 52 incident response collaborative teams, 54 large business case studies, 419–420 CSIRT (Computer Security Incident Response Teams), 52 incident response collaborative teams, 54 large business case studies, 403 responsibilities of, 54 selecting personnel for, 53 tasks of, 54 CSM CSM data center security SSM (Cisco Security Manager) instrumentation and management (SAVE framework), 195 CS-MARS (Cisco Security Monitoring, Analysia and Response System), 121–122, 125 CSSC Configure EAP Method screen, 234 configuring wireless networks, 233–234, 236 Network Authentication screen, 234 configuring wireless networks, 233–234, 236 Network Profile screen, 233 CVSS (Common Vulnerability Scoring System) 50 base metrics, 51	instrumentation and management (SAVE	CSA (Cisco Security Agents)
authentication banners infrastructure security, 62 exception ACL, 64 NAT small business case study, 376 COPM (Cisco Operational Process Model), threat modeling, 45 COPW (Cisco Operational Process Model), threat modeling, 45 COPU (Control Plane Policing) CPU traffic infrastructure security, 80 core layer (IP telephony), 265, 275 correlation (SAVE framework), 192 CSA-MC, 193 CS-MARS, 193 Peakflow X, 193 CPU COPP COPP COPP infrastructure security, 80 filtering traffic sent to infrastructure security, 78 interrupt time processors versus (infrastructure security), 78 packet registration infrastructure security, 78 interrupt time processors versus (infrastructure security), 78 processors interrupt time versus (infrastructure security, 78 processors interrupt time versus (infrastructure security),	framework), 195	data centers, deploying for, 325
authentication banners infrastructure security, 62 exception ACL, 64 NAT small business case study, 376 COPM (Cisco Operational Process Model), threat modeling, 45 COPM (Cisco Operational Process Model), threat modeling, 45 COPM (Cisco Operational Process Model), threat modeling, 45 COPM (Cisco Operational Process Model), See SAVE, 177 COPP (Control Plane Policing) CPU traffic infrastructure security, 80 Core layer (IP telephony), 265, 275 correlation (SAVE framework), 192 CSA-MC, 193 CS-MARS, 193 Peakflow SP, 193 Peakflow SP, 193 Peakflow X, 193 CPU COPP infrastructure security, 80 filtering traffic sent to infrastructure security, 78 interrupt time processors versus (infrastructure security), 78 packet registration infrastructure security, 78 processors interrupt time versus (infrastructure security), 78 processors interrupt time vers	Configure EAP Method screen (CSSC), 234	configuring agent kits, 326
infrastructure security, 62 exception ACL, 64 NAT Small business case study, 376 COPM (Cisco Operational Process Model), threat modeling, 45 COPM (Cisco Operational Process Model). See SAVE, 177 CoPP (Control Plane Policing) CPU traffic infrastructure security, 80 core layer (IP telephony), 265, 275 correlation (SAVE framework), 192 CSA-MCR, 193 CS-MARS, 193 Peakflow SP, 193 Peakflow X, 193 CPU COPP COPP COPP infrastructure security, 80 filtering traffic sent to infrastructure security, 78 interrupt time processors versus (infrastructure security, 78 interrupt time versus (infrastructure security, 78 processors interrupt time versus (infrastructure security), 78 pracket registration infrastructure security, 78 processors interrupt time versus (infrastructure security), 78 pracket registration infrastructure security, 78 processors interrupt time versus (infrastructure security), 78 processors interrupt time versus (infrastructure security), 78 pracket registration infrastructure security, 78 processors interrupt time versus (infrastructure security), 78 processors interrupt time versus (infrastructure security), 78 processors interrupt time versus (infrastructure security, 78 processors interrupt time versus (configuring	CSA architectures, 325–326
infrastructure security, 62 exception ACL, 64 NAT Small business case study, 376 COPM (Cisco Operational Process Model), threat modeling, 45 COPM (Cisco Operational Process Model). See SAVE, 177 CoPP (Control Plane Policing) CPU traffic infrastructure security, 80 core layer (IP telephony), 265, 275 correlation (SAVE framework), 192 CSA-MCR, 193 CS-MARS, 193 Peakflow SP, 193 Peakflow X, 193 CPU COPP COPP COPP infrastructure security, 80 filtering traffic sent to infrastructure security, 78 interrupt time processors versus (infrastructure security, 78 interrupt time versus (infrastructure security, 78 processors interrupt time versus (infrastructure security), 78 pracket registration infrastructure security, 78 processors interrupt time versus (infrastructure security), 78 pracket registration infrastructure security, 78 processors interrupt time versus (infrastructure security), 78 processors interrupt time versus (infrastructure security), 78 pracket registration infrastructure security, 78 processors interrupt time versus (infrastructure security), 78 processors interrupt time versus (infrastructure security), 78 processors interrupt time versus (infrastructure security, 78 processors interrupt time versus (authentication banners	phased deployments, 326–327
correlation (SAVE framework), 193 Small business case study, 376 COPM (Cisco Operational Process Model), threat modeling, 45 COPM (Cisco Operational Process Model). See SAVE, 177 CoPP (Control Plane Policing) CPU traffic infrastructure security, 80 core layer (IP telephony), 265, 275 correlation (SAVE framework), 192 CSA-MC, 193 CS-MARS, 193 Peakflow SP, 193 Peakflow X, 193 COPP COPP COPP infrastructure security, 80 filtering traffic sent to infrastructure security, 78 interrupt time processors versus (infrastructure security, 78 processors interrupt time versus (infrastructure security), 78 processors interrupt time versus (infrastructure security), 78 rACL infrastructure security, 78 racle limiting traffic infrastructure security, 78 rate limiting traffic infrastructure security, 78 scheduler allocate command correlation (SAVE framework), 193 CSIRT postmortems large business case studies, 419–420 CSIRT (Computer Security Incident Response Teams), 52 incident response collaborative teams, 54 large business large business case studies, 419–420 CSIRT (Computer Security Incident Response Teams), 52 incident response collaborative teams, 54 large business case studies, 403 responsibilities of, 54 selecting personnel for, 53 tasks of, 54 CSM CSM CSM CSM CSM CSM CSM CS	infrastructure security, 62	CSA-MC (Cisco Security Agent Mangement
Small business case study, 376 COPM (Cisco Operational Process Model), threat modeling, 45 COPM (Cisco Operational Process Model). See SAVE, 177 CoPP (Control Plane Policing) CPU traffic infrastructure security, 80 CSA-MC, 193 CS-MARS, 193 Peakflow SP, 193 Peakflow SP, 193 Peakflow X, 193 COPP COPP COPP CoPP infrastructure security, 80 filtering traffic sent to infrastructure security, 78 interrupt time processors versus (infrastructure security), 78 packet registration infrastructure security, 78 processors interrupt time versus (infrastructure security), 78 pracket registration infrastructure security, 78 processors interrupt time versus (infrastructure security), 78 processors interrupt time versus (infrastructure security), 78 processors interrupt time versus (infrastructure security, 78 processors interrupt ti	exception ACL, 64	Console)
COPM (Cisco Operational Process Model), threat modeling, 45 COPM (Cisco Operational Process Model). See SAVE, 177 CoPP (Control Plane Policing) CPU traffic infrastructure security, 80 core layer (IP telephony), 265, 275 correlation (SAVE framework), 192 CSA-MC, 193 CS-MARS, 193 Peakflow SP, 193 Peakflow X, 193 COPP COPP CoPP CoPP Infrastructure security, 80 filtering traffic sent to infrastructure security, 78 interrupt time processors versus (infrastructure security, 78 packet registration infrastructure security, 78 processors interrupt time versus (infrastructure security, 78 processors interrupt time versus (NAT	correlation (SAVE framework), 193
threat modeling, 45 COPM (Cisco Operational Process Model). See SAVE, 177 CoPP (Control Plane Policing) CPU traffic infrastructure security, 80 CS-MARS, 193 Peakflow SP, 193 Peakflow X, 193 CPU CoPP CoPP infrastructure security, 80 filtering traffic sent to infrastructure security, 78 packet registration infrastructure security, 78 packet registration infrastructure security, 78 processors interrupt time versus (infrastructure security), 78 processors interrupt time versus (infrastructure security), 78 processors interrupt time versus (infrastructure security, 78 processors interrupt time versus (infrastruc	small business case study, 376	CSIRT
COPM (Cisco Operational Process Model). See SAVE, 177 CoPP (Control Plane Policing) CPU traffic infrastructure security, 80 core layer (IP telephony), 265, 275 correlation (SAVE framework), 192 CSA-MC, 193 CS-MARS, 193 Peakflow SP, 193 Peakflow X, 193 CPU CoPP infrastructure security, 80 filtering traffic sent to infrastructure security, 78 interrupt time processors versus (infrastructure security, 78 packet registration infrastructure security, 78 processors interrupt time versus (infrastructure security), 78 rACL infrastructure security, 78 rACL infrastructure security, 78 rate limiting traffic infrastructure security, 78 scheduler allocate command CSIRT (Computer Security Incident Response Teams), 52 incident response collaborative teams, 54 large business case studies, 403 responsibilities of, 54 selecting personnel for, 53 tasks of, 54 CSM CSM CSM (Cisco Security Manager) instrumentation and management (SAVE framework), 195 CS-MARS CS-MARS (Cisco Security Monitoring, Analysi and Response System), 121–122, 125 CSSC Configuring wireless networks, 233–234, 236 Network Authentication screen, 234 Network Profile screen, 233 CVSS (Common Vulnerability Scoring System) 50 base metrics, 51 environmental metrics, 52 temporal metrics, 51	COPM (Cisco Operational Process Model),	postmortems
COPM (Cisco Operational Process Model). See SAVE, 177 CoPP (Control Plane Policing) CPU traffic infrastructure security, 80 core layer (IP telephony), 265, 275 correlation (SAVE framework), 192 CSA-MC, 193 CS-MARS, 193 Peakflow SP, 193 Peakflow X, 193 CPU CoPP infrastructure security, 80 filtering traffic sent to infrastructure security, 78 interrupt time processors versus (infrastructure security, 78 packet registration infrastructure security, 78 processors interrupt time versus (infrastructure security), 78 rACL infrastructure security, 78 rACL infrastructure security, 78 rate limiting traffic infrastructure security, 78 scheduler allocate command CSIRT (Computer Security Incident Response Teams), 52 incident response collaborative teams, 54 large business case studies, 403 responsibilities of, 54 selecting personnel for, 53 tasks of, 54 CSM CSM CSM (Cisco Security Manager) instrumentation and management (SAVE framework), 195 CS-MARS CS-MARS (Cisco Security Monitoring, Analysi and Response System), 121–122, 125 CSSC Configuring wireless networks, 233–234, 236 Network Authentication screen, 234 Network Profile screen, 233 CVSS (Common Vulnerability Scoring System) 50 base metrics, 51 environmental metrics, 52 temporal metrics, 51	threat modeling, 45	large business case studies, 419–420
SAVE, 177 CoPP (Control Plane Policing) CPU traffic infrastructure security, 80 core layer (IP telephony), 265, 275 correlation (SAVE framework), 192 CSA-MC, 193 CS-MARS, 193 Peakflow SP, 193 Peakflow X, 193 COPP CoPP CoPP infrastructure security, 80 filtering traffic sent to infrastructure security, 78 processors versus (infrastructure security, 78 packet registration infrastructure security, 78 processors interrupt time versus (infrastructure security, 78 rACL infrastructure security, 78 raCL infrastructure security, 78 rate limiting traffic infrastructure security, 78 rate limiting traffic infrastructure security, 78 scheduler allocate command Teams), 52 incident response collaborative teams, 54 large business case studies, 403 responsibilities of, 54 CSM CSM CSM CSM CSM (Cisco Security Manager) instrumentation and management (SAVE framework), 195 CS-MARS CS-MARS CS-MARS CS-MARS (Cisco Security Monitoring, Analysi and Response System), 121–122, 125 CSSC Configure EAP Method screen, 234 configuring wireless networks, 233–234, 236 Network Authentication screen, 234 Network Profile screen, 233 CVSS (Common Vulnerability Scoring System) 50 base metrics, 51 environmental metrics, 52 temporal metrics, 51		CSIRT (Computer Security Incident Response
CPU traffic large business case studies, 403 responsibilities of, 54 selecting personnel for, 53 tasks of, 54 CSA-MC, 193 CS-MARS, 193 Peakflow SP, 193 Peakflow X, 193 COPP COPP Infrastructure security, 80 filtering traffic sent to infrastructure security, 78 packet registration infrastructure security, 78 processors interrupt time versus (infrastructure security, 78		
CPU traffic infrastructure security, 80 responsibilities of, 54 selecting personnel for, 53 tasks of, 54 CSA-MC, 193 CS-MARS, 193 data center security Peakflow SP, 193 SYN cookies, 299 Peakflow X, 193 CSM (Cisco Security Manager) COPP infrastructure security, 80 rate limiting traffic infrastructure security, 78 scheduler allocate command infrastructure security, 78 scheduler allocate command CYU tasks of, 54 CSM CSM CSM CSM (Cisco Security Manager) CSM (Cisco Security Manager) CS-MARS CS-MARS CS-MARS CS-MARS CS-MARS CS-MARS CS-MARS (Cisco Security Monitoring, Analysi and Response System), 121–122, 125 CSSC Configure EAP Method screen, 234 Network Authentication screen, 234 Network Profile screen, 233 CYSS (Common Vulnerability Scoring System) 50 and Response System) SSC Configure EAP Method screen, 234 Network Profile screen, 233 CYSS (Common Vulnerability Scoring System) Society infrastructure security, 78 Environmental metrics, 51 environmental metrics, 52 temporal metrics, 51		incident response collaborative teams, 54
infrastructure security, 80 core layer (IP telephony), 265, 275 correlation (SAVE framework), 192 CSA-MC, 193 CS-MARS, 193 Peakflow SP, 193 Peakflow X, 193 COPP COPP infrastructure security, 80 filtering traffic sent to infrastructure security, 78 processors versus (infrastructure security, 78 packet registration infrastructure security, 78 processors interrupt time versus (infrastructure security, 78 base metrics, 51 environmental metrics, 52 temporal metrics, 51		
core layer (IP telephony), 265, 275 correlation (SAVE framework), 192	infrastructure security, 80	
correlation (SAVE framework), 192 CSA-MC, 193 CS-MARS, 193 Peakflow SP, 193 Peakflow X, 193 COPU COPP infrastructure security, 80 filtering traffic sent to infrastructure security, 78 interrupt time processors versus (infrastructure security), 78 packet registration infrastructure security, 78 processors interrupt time versus (infrastructure security), 78 rACL infrastructure security, 78–80 rate limiting traffic infrastructure security, 78 scheduler allocate command tasks of, 54 CSM data center security SYN cookies, 299 CSM (Cisco Security Manager) instrumentation and management (SAVE framework), 195 CS-MARS CS-MARS (Cisco Security Monitoring, Analysi and Response System), 121–122, 125 CSSC Configure EAP Method screen, 234 configuring wireless networks, 233–234, 236 Network Authentication screen, 234 Network Profile screen, 233 CVSS (Common Vulnerability Scoring System) 50 base metrics, 51 environmental metrics, 52 temporal metrics, 51		
CSA-MC, 193 CS-MARS, 193 Peakflow SP, 193 Peakflow X, 193 CPU COPP infrastructure security, 80 filtering traffic sent to infrastructure security, 78 interrupt time processors versus (infrastructure security), 78 packet registration infrastructure security, 78 processors interrupt time versus (infrastructure security), 78 processors interrupt time versus (infrastructure security, 78 processors interrupt time versus (infr		
Peakflow SP, 193 Peakflow X, 193 CPU CoPP infrastructure security, 80 filtering traffic sent to infrastructure security, 78 interrupt time processors versus (infrastructure security), 78 packet registration infrastructure security, 78 processors interrupt time versus (infrastructure security), 78 processors interrupt time versus (infrastructure security), 78 processors interrupt time versus (infrastructure security), 78 processors interrupt time versus (infrastructure security), 78 rACL infrastructure security, 78-80 rate limiting traffic infrastructure security, 78 scheduler allocate command SYN cookies, 299 CSM (Cisco Security Manager) instrumentation and management (SAVE framework), 195 CS-MARS CS-MARS (Cisco Security Monitoring, Analysi and Response System), 121–122, 125 CSSC Configure EAP Method screen, 234 configuring wireless networks, 233–234, 236 Network Authentication screen, 234 Network Profile screen, 233 CVSS (Common Vulnerability Scoring System) 50 base metrics, 51 environmental metrics, 52 temporal metrics, 51		CSM
Peakflow SP, 193 Peakflow X, 193 CPU CoPP infrastructure security, 80 filtering traffic sent to infrastructure security, 78 interrupt time processors versus (infrastructure security), 78 packet registration infrastructure security, 78 processors interrupt time versus (infrastructure security), 78 processors interrupt time versus (infrastructure security), 78 processors interrupt time versus (infrastructure security), 78 processors interrupt time versus (infrastructure security), 78 rACL infrastructure security, 78-80 rate limiting traffic infrastructure security, 78 scheduler allocate command SYN cookies, 299 CSM (Cisco Security Manager) instrumentation and management (SAVE framework), 195 CS-MARS CS-MARS (Cisco Security Monitoring, Analysi and Response System), 121–122, 125 CSSC Configure EAP Method screen, 234 configuring wireless networks, 233–234, 236 Network Authentication screen, 234 Network Profile screen, 233 CVSS (Common Vulnerability Scoring System) 50 base metrics, 51 environmental metrics, 52 temporal metrics, 51	CS-MARS, 193	data center security
CSM (Cisco Security Manager) instrumentation and management (SAVE framework), 195 infrastructure security, 80 filtering traffic sent to correlation (SAVE framework), 193 infrastructure security, 78 interrupt time CS-MARS (Cisco Security Monitoring, Analysic and Response System), 121–122, 125 security), 78 packet registration Configure EAP Method screen, 234 infrastructure security, 78 processors wersus (infrastructure security, 78 processors wersus (infrastructure security, 78 processors Wireless networks, 233–234, 236 interrupt time versus (infrastructure security), 78 rACL Security, 78 racl imiting traffic base metrics, 51 infrastructure security, 78 scheduler allocate command temporal metrics, 52 temporal metrics, 51	Peakflow SP, 193	•
CPU CoPP infrastructure security, 80 filtering traffic sent to infrastructure security, 78 interrupt time processors versus (infrastructure security), 78 packet registration infrastructure security, 78 processors processors processors processors processors security, 78 processors processo		CSM (Cisco Security Manager)
CoPP infrastructure security, 80 filtering traffic sent to infrastructure security, 78 interrupt time processors versus (infrastructure security), 78 packet registration infrastructure security, 78 processors interrupt time versus (infrastructure security), 78 processors interrupt time versus (infrastructure security), 78 processors interrupt time versus (infrastructure security), 78 rACL infrastructure security, 78 racl infrastructure security, 78 rate limiting traffic infrastructure security, 78 scheduler allocate command framework), 195 CS-MARS CS-MARS (Cisco Security Monitoring, Analysi and Response System), 121–122, 125 CSSC Configure EAP Method screen, 234 configuring wireless networks, 233–234, 236 Network Authentication screen, 234 Network Profile screen, 233 CVSS (Common Vulnerability Scoring System) 50 base metrics, 51 environmental metrics, 52 temporal metrics, 51	CPU	
filtering traffic sent to infrastructure security, 78 interrupt time processors versus (infrastructure security), 78 packet registration infrastructure security, 78 processors interrupt time versus (infrastructure security), 78 processors interrupt time versus (infrastructure security), 78 processors interrupt time versus (infrastructure security), 78 rACL infrastructure security, 78 rate limiting traffic infrastructure security, 78 scheduler allocate command correlation (SAVE framework), 193 tracebacks, 148 CS-MARS (Cisco Security Monitoring, Analysi and Response System), 121–122, 125 CSSC Configure EAP Method screen, 234 configuring wireless networks, 233–234, 236 Network Authentication screen, 234 Network Profile screen, 233 CVSS (Common Vulnerability Scoring System) 50 base metrics, 51 environmental metrics, 52 temporal metrics, 51	CoPP	
filtering traffic sent to infrastructure security, 78 interrupt time processors versus (infrastructure security), 78 packet registration infrastructure security, 78 processors interrupt time versus (infrastructure security), 78 processors interrupt time versus (infrastructure security), 78 processors interrupt time versus (infrastructure security), 78 rACL infrastructure security, 78 rate limiting traffic infrastructure security, 78 scheduler allocate command correlation (SAVE framework), 193 tracebacks, 148 CS-MARS (Cisco Security Monitoring, Analysi and Response System), 121–122, 125 CSSC Configure EAP Method screen, 234 configuring wireless networks, 233–234, 236 Network Authentication screen, 234 Network Profile screen, 233 CVSS (Common Vulnerability Scoring System) 50 base metrics, 51 environmental metrics, 52 temporal metrics, 51	infrastructure security, 80	CS-MARS
infrastructure security, 78 interrupt time processors versus (infrastructure security), 78 packet registration infrastructure security, 78 processors interrupt time versus (infrastructure security), 78 processors interrupt time versus (infrastructure security), 78 rACL infrastructure security, 78 rate limiting traffic infrastructure security, 78 scheduler allocate command tracebacks, 148 CS-MARS (Cisco Security Monitoring, Analysi and Response System), 121–122, 125 CSSC Configure EAP Method screen, 234 configuring wireless networks, 233–234, 236 Network Authentication screen, 234 Network Profile screen, 233 CVSS (Common Vulnerability Scoring System) 50 base metrics, 51 environmental metrics, 52 temporal metrics, 51		correlation (SAVE framework), 193
interrupt time processors versus (infrastructure security), 78 packet registration infrastructure security, 78 processors interrupt time versus (infrastructure security), 78 processors interrupt time versus (infrastructure security), 78 rACL infrastructure security, 78—80 rate limiting traffic infrastructure security, 78 scheduler allocate command CS-MARS (Cisco Security Monitoring, Analysi and Response System), 121–122, 125 CSSC Configure EAP Method screen, 234 configuring wireless networks, 233–234, 236 Network Authentication screen, 234 Network Profile screen, 233 CVSS (Common Vulnerability Scoring System) 50 base metrics, 51 environmental metrics, 52 temporal metrics, 51		
processors versus (infrastructure security), 78 packet registration infrastructure security, 78 processors interrupt time versus (infrastructure security), 78 rACL infrastructure security, 78-80 rate limiting traffic infrastructure security, 78 scheduler allocate command and Response System), 121–122, 125 CSSC Configure EAP Method screen, 234 configuring wireless networks, 233–234, 236 Network Authentication screen, 234 Network Profile screen, 233 CVSS (Common Vulnerability Scoring System) 50 base metrics, 51 environmental metrics, 52 temporal metrics, 51		CS-MARS (Cisco Security Monitoring, Analysi
security), 78 packet registration infrastructure security, 78 processors interrupt time versus (infrastructure security), 78 rACL infrastructure security, 78—80 rate limiting traffic infrastructure security, 78 scheduler allocate command CSSC Configure EAP Method screen, 234 configuring wireless networks, 233—234, 236 Network Authentication screen, 234 Network Profile screen, 233 CVSS (Common Vulnerability Scoring System) 50 base metrics, 51 environmental metrics, 52 temporal metrics, 51		
infrastructure security, 78 processors interrupt time versus (infrastructure security), 78 rACL infrastructure security, 78–80 rate limiting traffic infrastructure security, 78 scheduler allocate command configuring wireless networks, 233–234, 236 Network Authentication screen, 234 Network Profile screen, 233 CVSS (Common Vulnerability Scoring System) 50 base metrics, 51 environmental metrics, 52 temporal metrics, 51		
infrastructure security, 78 processors interrupt time versus (infrastructure security), 78 rACL infrastructure security, 78–80 rate limiting traffic infrastructure security, 78 scheduler allocate command configuring wireless networks, 233–234, 236 Network Authentication screen, 234 Network Profile screen, 233 CVSS (Common Vulnerability Scoring System) 50 base metrics, 51 environmental metrics, 52 temporal metrics, 51	packet registration	Configure EAP Method screen, 234
processors interrupt time versus (infrastructure security), 78 rACL infrastructure security, 78–80 rate limiting traffic infrastructure security, 78 scheduler allocate command wireless networks, 233–234, 236 Network Authentication screen, 234 Network Profile screen, 233 CVSS (Common Vulnerability Scoring System) 50 base metrics, 51 environmental metrics, 52 temporal metrics, 51		
interrupt time versus (infrastructure security), 78 rACL infrastructure security, 78–80 rate limiting traffic infrastructure security, 78 scheduler allocate command Network Authentication screen, 234 Network Profile screen, 233 CVSS (Common Vulnerability Scoring System) 50 base metrics, 51 environmental metrics, 52 temporal metrics, 51		
security), 78 rACL infrastructure security, 78–80 rate limiting traffic infrastructure security, 78 scheduler allocate command Network Profile screen, 233 CVSS (Common Vulnerability Scoring System) 50 base metrics, 51 environmental metrics, 52 temporal metrics, 51		
rACL infrastructure security, 78–80 rate limiting traffic infrastructure security, 78 scheduler allocate command CVSS (Common Vulnerability Scoring System) 50 base metrics, 51 environmental metrics, 52 temporal metrics, 51		Network Profile screen, 233
infrastructure security, 78–80 rate limiting traffic infrastructure security, 78 scheduler allocate command 50 base metrics, 51 environmental metrics, 52 temporal metrics, 51		CVSS (Common Vulnerability Scoring System)
rate limiting traffic base metrics, 51 infrastructure security, 78 environmental metrics, 52 scheduler allocate command temporal metrics, 51	infrastructure security, 78–80	
infrastructure security, 78 environmental metrics, 52 scheduler allocate command temporal metrics, 51		base metrics, 51
scheduler allocate command temporal metrics, 51		*
•		*
infrastructure security, 81	infrastructure security, 81	•
scheduler interval command	•	

infrastructure security, 81

deep packet inspection, 10 deep-packet inspection, 9

device authorize command, 272

ר	device security policies
	large business case studies, 405
DAI (Dynamic Address Inspection)	DHCP
access layer (IP telephony), 270	snooping
dark IP addresses, 37	identity and trust (SAVE framework),
data analysis	186–187
postmortems, 169	DHCP snooping
telemetry	access layer (IP telephony), 269-270
infrastructure security, 89	diagrams (networks)
data centers, 297	high-level enterprise diagrams, 101, 103
CSA, deploying, 325	layered diagrams, 106
configuring agent kits, 326	digital certificates
CSA architectures, 325–326	identity and trust (SAVE framework), 188
phased deployments, 326–327	Directed Broadcasts (IP)
DoS attacks, 297	infrastructure security, disabling for, 72
Cisco Guard, 302	distance vector protocols (IGP), 67
Flexible NetFlow, 301	distribution layer (IP telephony), 265, 273
IDS, 300	GLBP, 274
IPS, 300	HSRP, 273–274
NetFlow, 301	distribution layer switches
SYN cookies, 297–299	NetFlow
infrastructure protection, 302–303	configuring at, 103
network intrusion detection/prevention systems,	DMZ (demilitarized zones), 10
deploying, 322	DMZ servers
monitoring, 325	Static NAT
sending selective traffic to IDS/IPS	small business case study, 349
devices, 322, 324	documentation
tuning, 325	incident-handling policies, 154–155
segmentation, 303–304	DoS (Denial of Service) attacks
FWSM, 306–314, 316–322	data center security, 297
tiered access control, 303–304	Cisco Guard, 302
worms, 297	Flexible NetFlow, 301
Cisco Guard, 302	IDS, 300
Flexible NetFlow, 301	infrastructure protection, 302–303
IDS, 300	IPS, 300
infrastructure protection, 302–303	NetFlow, 301
IPS, 300	SYN cookies, 297–299
NetFlow, 301	dot-dot attacks
data collection	tracebacks, 148
postmortems, 169	dotlx port-control auto command, 271
data transmission	DREAD model (threat modeling), 44–45
telemetry	
infrastructure security, 89	E

Ε

EAP methods

802.1x, 220-221

EAP-FAST, 224–225	filtering
configuring 802.1x in Unified Wireless	CPU traffic
Solutions, 226	infrastructure security, 78
configuring Secure ACS Servers, 229, 232–233	IPv6, 331
EAP-GTC, 225	ACL, 331–332
EAP-MD5, 221-222	routes
EAP-TLS, 223	infrastructure security, 69
EAP-TTLS (EAP Tunneled TLS Authentication	Finger Protocol
Protocol), 224	infrastructure security, disabling for, 72
eavesdropping attacks	firewalls, 5
IP telephony, 293–294	data center security
Edge Deployment mode (CAS), 30	SYN cookies, 297–299
EGP (Exterior Gateway Protocols), 67	network firewalls, 6
Egress NetFlow, 111	deep packet inspection, 10
enable view command, 65	DMZ, 10
EnCase (Guidance Software), 165	<i>NAT</i> , 7–8
endpoint security	packet filters, 7
CSA, 92–94	router configurations, 6
patch management, 90–91	stateful firewalls, 9
engineering (social), 49	personal firewalls, 11
Enterprise	CSA, 11
tracebacks, 147	segmentation
CS-MARS, 148	isolation and virtualization (SAVE
dot-dot attacks, 148	framework), 200
environmental metrics (CVSS), 52	FIRST (Forum for Incident Response and
escalation procedures (incident-handling policies/	Security Teams)
procedures), 154	tracebacks, 142
escalation procedures (NAC), 97	Flexible NetFlow
ethical hacking. See penetration testing, 46	data center security, 301
exception ACL, configuring, 64	forensics, 160
exec-timeout command	Linux forensics tools, 162–163
modifying idle timeouts, 63	netstat command, 163
extension headers	pstree command, 163
IPv6, 332	log files, 161
external databases (802.1x), 219	Windows forensics tools
	EnCase, 165
_	Systernals, 164
:	fragment command
	FWSM, data center segmentation, 322
failovers	fragmentation
active-standby failovers	IPv6, 333
medium-sized business case studies, 394–	FWSM
396, 398–399	data center segmentation, 306, 308
feedback	configuring Cisco Catalyst switches
looped feedback	309–310
postmortems, 167	configuring NAT, 313–314, 316
positionens, 107	y.g,, ,

configuring security context interfaces, 312–313 controlling access via ACL, 317–321 creating security contexts, 310–312 Routed mode, 306	HTTP authentication infrastructure security, 63
Transparent mode, 306–307 Virtual Fragment Reassembly, 322 FWSM (Firewall Services Module) data center security SYN cookies, 298	iACL (infrastructure Access Control Lists) infrastructure security policy enforcement, 82 IB (in-band) mode (NAC appliance), 29 iBGP (interal Border Gateway Protocol), 36 IBNS (Identity-Based Networking Services), 26
GLBP (Gateway Load Balancing Protocol) distribution layer (IP telephony), 274 grey-box (crystal-box) penetration testing, 46 set port dotlx, 271 Guard (Cisco)	IC3 (Internet Crime Complaint Center), 156 ICMP redirect messages infrastructure security, disabling for, 73 ICMP filtering IPv6, 332 ICV (Integrity Check Values), 216–217
active verification identity and trust (SAVE framework), 185 Guard XT (Traffic Anomaly Detectors XT) identifying/classifying security threats, 127, 129–131	IDENT (Indentity Protocol) infrastructure security, disabling for, 74 identifiers (local) IPV6, 331 identifying security threats CS-MARS, 121–122, 125
1	Guard XT, 127, 129–131 IDS, 131 signature updates, 131–132
hacking ethical hacking. See penetration testing, 46 headers extension headers IPv6, 332 manipulation attacks IPv6, 333	tuning, 133–134, 136 IPS, 131 anomaly detection, 137–138 IDM, 132 signature updates, 131–132 tuning, 133–134, 136 NAM, 125–126
heuristic-based analysis, 21 High Availability (NAC Appliance), 31 high-level enterprise diagrams, 101, 103 HIPAA (Health Industry Portability and Accountability Act), 156 hop-by-hop tracebacks, 142 botnets, 145 BGP routers, 146	NetFlow, 108 Cisco platform support, 108 collecting CLI statistics, 112–114 Egress NetFlow, 111 enabling, 111–112 flows, elements of, 109 flows, exporting data from, 110 flows, obtaining additional information
zombies, 145 HSRP (Hot Standby Router Protocol) distribution layer (IP telephony), 273–274	from, 109–110 Ingress NetFlow, 111 IPFIX WG, 110 NDE packet templates, 110

network visibility, 101, 103, 106–107	heuristic-based analysis, 21
open source monitoring tools, 126–127	identifying/classifying security threats, 131
SNMP, 118–119	signature updates, 131–132
ASA security appliances, enabling logging	tuning, 133–134, 136
on, 121	pattern matching, 20
IOS router/switch logging, enabling,	protocol analysis, 21
119–121	signatures, 20
PIX security appliances, enabling logging	IEEE 802.1x, 26
on, 121	IGP (Interior Gateway Protocols)
SYSLOG, 115	distance vector protocols, 67
ASA security appliances, enabling logging	link state protocols, 67
on, 117–118	IKE
CATOS running catalyst switches,	identity and trust (SAVE framework), 188
enabling logging on, 117	IM (Instant Messaging)
IOS router/switch logging, enabling,	small business case study, 354-355, 357-359
115–116	IMS (Internet Motion Sensor), security
PIX security appliances, enabling logging	intelligence, 50
on, 117–118	incident response
TAD XT, 127–128, 131	large business case studies, 419–420
identity and trust (SAVE framework), 183	incident response collaborative teams (CSIRT),
AAA, 183–184	54
Cisco Guard active verification, 185	Incident Response Reports, 169
DHCP snooping, 186–187	Lessons Learned section, 171
digital certificates, 188	ratings systems, 173
IKE, 188	incident-handling
IP Source Guard, 187–188	ACL, 157
NAC, 188	VACL, 157
routing protocol authentication, 189	forensics, 160
strict Unicast RPF, 189	Linux forensics tools, 162–163
identity management solutions/systems, 26	log files, 161
IBNS, 26	Windows forensics tools, 164–165
IEEE 802.1x, 26	law enforcement, 155
Identity NAT	Computer Fraud and Abuse Act, 156
small business case study, 351	HIPAA, 156
idle timeouts	IC3, 156
modifying, 63	Infragard, 156
IDM (IPS Device Manager)	U.S. Department of Justice website, 156
signature updates, 132	policies/procedures
IDS	checklists, 154–155
data center network intrusion detection/	collaboration, 153
prevention systems	documentation, 154–155
sending selective traffic to, 322, 324	escalation procedures, 154
IP telephony eavesdropping attacks, 294	patch management, 154
visibility (SAVE framework), 190–191	private VLAN, 158
IDS (Intrusion Detection Systems), 19, 22	RTBH, 158, 160
anomaly-based analysis, 21	Infragard, 156
data center security, 300	

infrastructure devices	SNMP access control, 66
AAA, configuring on	SSH versus Telnet, 59–60
medium-sized business case studies,	telemetry, 89
400–401	Ingress NetFlow, 111
infrastructure security, 57	instrumentation and management (SAVE
automated security tools	framework), 193
Cisco IOS AutoSecure, 84–88	Cisco IOS configuration logger logs, 195
SDM, 88–89	Cisco IOS configuration rollback feature, 195
disabling unnecessary services, 70	Cisco IOS CR XML interface, 196
BOOTP servers, 73	CSM, 195
CDP, 71	embedded device managers, 195
Finger protocol, 72	RMON, 196
ICMP redirect messages, 73	SNMP, 196
IDENT, 74	Syslog, 196
IP Directed Broadcasts, 72	intelligence (security), 50
IP source routing, 73	Cisco Security Center, 50
IPv6, 75	CVSS, 50
MOP, 72	base metrics, 51
PAD, 73	environmental metrics, 52
proxy ARP, 73	temporal metrics, 51
TCP/UDP small servers, 74	IMS (Internet Motion Sensor), 50
locking unused network access device ports, 75	research initiatives/organizations, 50
policy enforcement, 81	interactive access control (infrastructure
iACL, 82	security), 62–64
Unicast RPF, 83–84	Internet edge routers
resource exhaustion control, 75	medium-sized business case studies, 391
CoPP, 80	Internet usage policies
CPU packet generation, 78	large business case studies, 406
filtering CPU traffic, 78	IOS
processors versus interrupt time, 78	configuration logger
rACL, 78–80	instrumentation and management (SAVE
rate limiting CPU traffic, 78	framework), 195
resource threshold notifications, 76–77	configuration rollback feature
scheduler allocation command, 81	instrumentation and management (SAVE
scheduler interval command, 81	framework), 195
router planes, 57–58	CR XML interface
routing protocols, 67	instrumentation and management (SAVE
authentication, 68–69	framework), 196
route filtering, 69	role-based CLI Access
static routing peers, 68	isolation and virtualization (SAVE
TTL security checks, 70	framework), 197
strong device access control, 59	IOS routers
authentication banner configuration, 62	small business case study, 360, 363, 366, 368,
CLI Views, 64–65	370–375
interactive access control, 62–64	SNMP logging, enabling, 119–121
local password management, 61	SYSLOG logging, enabling, 115–121
wear passivora nanagement, or	5 1 5 1 5 1 5 5 1 5 5 1 5 5 1 5 1 5 1 5

IOS switches	ip verify source vlan dhcp-snooping interface
SNMP logging, enabling, 119–121	subcommand
SYSLOG logging, enabling, 115–116	enabling IP Source Guard, 187
IP	IPFIX WG (IETF Internet Protocol Flow
source routing	Information Export Work Group), 110
infrastructure security, disabling for, 73	IPS
IP addresses	data center network intrusion detection/
dark IP addresses, 37	prevention systems
IP addressing	sending selective traffic to, 322, 324
small business case study, 343	IP telephony eavesdropping attacks, 294
IP Directed Broadcasts	visibility (SAVE framework), 190-191
infrastructure security, disabling for, 72	IPS (Intrusion Prevention Systems), 19, 22
ip http access-class command	data center security, 300
interactive access control (infrastructure	identifying/classifying security threats, 131
security), 63	anomaly detection, 137–138
ip http authentication command	signature updates, 131–132
enabling HTTP authentication, 63	tuning, 133–134, 136
ip http max-connections command	IDM, 132
interactive access control (infrastructure	wireless IPS, 239–240
security), 63	configuring sensors in WLC, 241–242
IP routing	configuring signatures, 242–243
small business case study, 343	IPsec
IP Source Guard	IPv6, 335–337
identity and trust (SAVE framework), 187-188	remote access VPN
IP telephony, 261–262, 265	large business case studies, 406, 408,
access layer, 265, 272	411–412, 415–417
ARP, 270–271	IPsec (IP Security)
BPDU, 268	technical overview of, 14
DAI, 270	main mode negotiation, 15–16
DHCP snooping, 269–270	phase 1 negotiation, 14, 16
NAC, 271	phase 2 negotiation, 16–17
port security, 268–269	Transport mode, 17
root guards, 268	Tunnel mode, 17
VLAN assignment, 267	WEP, 218
Cisco Personal Assistant, 289	IPv4 (Internet Protocol version 4)
hardening operating environment,	IPv6 versus, 329
289–290	IPv6 (Internet Protocol version 6), 329
server security policies, 291–293	filtering, 331
Cisco Unified CallManager, 276–277	ACL, 331–332
Cisco Unified CME, 277–281	extension headers, 332
Cisco Unity, 281–282, 286–287	ICMP filtering, 332
Cisco Unity Express, 287–288	fragmentation, 333
core layer, 265, 275	header manipulation attacks, 333
distribution layer, 265, 273	IPsec, 335–337
GLBP, 274	IPv4 versus, 329
HSRP, 273–274	local identifiers, 331
eavesdropping attacks, 293–294	reconnaissance, 330
	security through obscurity, 330

routing security, 334	layer 2 routing
smurf attacks, 334	visibility (SAVE framework), 191
spoofing, 333	layer 3 routing
subnet prefixes, 331	visibility (SAVE framework), 191
IPv6 (IP Version 6)	layered diagrams, 106
infrastructure security, disabling for, 75	LEAP, 222
ipv6 access-list command, 331	Lessons Learned section (Incident Response
ISAC (Information Sharing and Analysis	Reports), 171
Centers), 54	link state protocols (IGP), 67
isolation and virtualization (SAVE framework),	Linux
196	forensics tools
anomaly detection zones, 198	Autopsy, 162–163
Cisco IOS role-based CLI Access, 197	netstat command, 163
CLI Views, 197	pstree command, 163
firewall segmentation, 200	Sleuth Kit, 162
network device virtualization, 198–199	load balancers
VLAN segmentation, 199	data center security
VRF segmentation, 200	SYN cookies, 297–299
VRF-Lite segmentation, 200	load-balancing
ITU-T X.805	large business case studies, 415–417
SAVE versus, 178, 180–181	local identifiers
	IPv6, 331
	log files (forensics), 161
	logging on host command
	enabling SYSLOG logging on ASA/PIX
large business case studies, 401, 403	security appliances, 117
CSIRT, 403	logging on command
incident response, 419–420	enabling SYSLOG logging on ASA/PIX
IPsec remote access VPN, deploying, 406, 408,	security appliances, 117
411–412, 415–417	logging trap command
load-balancing, 415–417	enabling SYSLOG logging on ASA/PIX
security policy creation, 404	security appliances, 117
change management policies, 406	SYSLOG logging, 116
device security policies, 405	logic attacks
Internet usage policies, 406	defining, 99
patch management policies, 406	examples of, 99
perimeter security policies, 404	login block-for command
physical security policies, 404	interactive access control (infrastructure
remote access VPN policies, 405	security), 64
law enforcement, 155	login delay command
Computer Fraud and Abuse Act, 156	interactive access control (infrastructure
HIPAA, 156	security), 63
IC3, 156	login quiet-mode access-class global command
Infragard, 156	configuring exception ACL, 64
U.S. Department of Justice website, 156	looped feedback
Lawful intercept view (CLI Views), 64	postmortems, 167
	m/p, 271

segmentation, 313-314, 316

network firewalls, 7–8

LWAPP (Lightweight Acess Point Protocol), 215 LWAPP (Lightweight Acess Point Protocol),	appliance configuration, 246–248, 251, 253–254
236–239	escalation procedures, 97
	identity and trust (SAVE framework), 188
	NAC Appliance, 27, 33
M	CAM, 27, 31
•••	CAS, 27–31
main mode negotiation (IPsec), 15–16	Clean Access Agents, 27
medium-sized business case studies, 389	High Availability, 31
AAA, configuring on infrastructure devices,	IB mode, 29
400–401	OOB mode, 29–30
active-standby failovers, configuring on ASA,	NAC Framework, 33–34, 36
	NAD, 34
394–396, 398–399 AIP-SSM, configuring on ASA, 391–394	NAH, 35
Internet edge routers, 391	phased deployments, 94–95
-	staff and support, 96–97
memory threshold natifications 77	WLC configuration, 255, 257, 259
threshold notifications, 77 memory free low-watermark io threshold	NAC Appliance, 27, 33
·	CAM, 27, 31
command	CAS, 27, 31
memory threshold notifications, configuring for	Centralized Deployment mode, 31
infrastructure security, 77	Edge Deployment mode, 30
memory free low-watermark processor threshold	Real IP mode, 29
global command	Virtual Gateway mode, 28
memory threshold notifications, configuring	
for infrastructure security, 77	Clean Access Agents, 27
memory reserve critical kilobytes command	High Availability, 31
memory threshold notifications, configuring	IB mode, 29
for infrastructure security, 77	OOB mode, 29–30
MFP (Management Frame Protection), 243	NAC Framework, 33–34, 36
mls flow ip interface-full command	NAD, 34
collecting CLI NetFlow statistics, 114	NAH, 35
mode multiple command	NAD (NAC Framework), 34
FWSM configuration for data center	NAH (NAC Agentless Hosts), 35
segmentation, 311	NAM (Network Analysis Module), 125–126
monitoring tools (open source)	visibility (SAVE framework), 191
identifying/classifying security threats,	NANOG (North American Network Operators
126–127	Group)
MOP (Maintenance Operations Protocol)	tracebacks, 142
infrastructure security, disabling for, 72	NAS (network access servers). See also RADIUS,
	23
A I	NAT
V	configuring
	small business case study, 376
NAC (Network Admission Control), 27, 94, 245	NAT (Network Address Translation)
access layer (IP telephony), 271	FWSM configuration for data center

administrative tasks, 96

NDE packet templates (NetFlow), 110 NetFlow, 108	visibility, 101, 103, 106–107 threat modeling (risk analysis), 45
as anomaly detection systems, 22	no ip bootp server global command
Cisco platform support, 108	BOOTP servers, disabling for infrastructure
CLI statistics, collecting, 112–114	security, 73
data center security, 301	no ip identd global command
distribution layer switches	IDENT, disabling for infrastructure security, 74
configuring at, 103	no ip redirects interface subcommand
Egress NetFlow, 111	ICMP redirect messages, disabling for
enabling, 111–112	infrastructure security, 73
Flexible NetFlow, 301	no ipv6 address interface subcommand
flows	disabling IPv6 for infrastructure security, 75
elements of, 109	no ipv6 enable interface subcommand
exporting data from, 110	disabling IPv6 for infrastructure security, 75
IPFIX WG, 110	no service pad global command
obtaining additional information from, 109–110	PAD, disabling for infrastructure security, 73
Ingress NetFlow, 111	
NDE packet templates, 110	O
netstat command	
Linux forensics, 163	OOB (out-of-band) mode (NAC appliance), 29-30
network access devices	open source
locking down unused ports (infrastructure	monitoring tools
security), 75	identifying/classifying security threats,
Network Authentication screen (CSSC), 234	126–127
network devices	
isolation and virtualization (SAVE framework), 198–199	Р
network firewalls, 6	
deep packet inspection, 10	packet filters, 7
DMZ, 10	packet registration
NAT, 7–8	CPU traffic
packet filters, 7	infrastructure security, 78
router configurations, 6	PAD (Packet Assembler/Disassembler)
stateful firewalls, 9	infrastructure security, disabling for, 73
network intrusion detection/prevention systems	parser view command, 65
data centers, deploying for, 322	passwords
monitoring, 325	local password management
sending selectiv traffic to IDS/IPS devices,	infrastructure security, 61
322, 324	PAT
tuning, 325	small business case study, 347
Network Profile screen (CSSC), 233	patch management
networks	endpoint security, 90–91
diagrams	security policies, building, 56
high-level enterprise diagrams, 101, 103	patch management policies
layered diagrams, 106	large business case studies, 406
• • •	range business case studies, 700

patches	TCP ports
managing (incident-handling policies), 154	Cisco Unity, 282–285
pattern matching	UDP ports
stateful pattern-matching recognition, 20	Cisco Unity, 282–285
pattern matching (IDS), 20	unused network access device ports
Peakflow SP	locking for infrastructure security, 75
correlation (SAVE framework), 193	postmortems, 167
Peakflow X	action plans, building, 173-174
correlation (SAVE framework), 193	data analysis, 169
PEAP, 223, 225	data collection, 169
penetration testing, 46	Incident Response Reports, 169
black-box testing, 46	Lessons Learned section, 171
confidentiality requirements, 48	ratings systems, 173
crystal-box (grey box) testing, 46	large business case studies, 419–420
infrastructure device configuration audits, 47	looped feedback, 167
open-source tools, 46–48	typical questions answered in, 168
scheduling, 48	prosecuting attacks, 155
white-box testing, 46	Computer Fraud and Abuse Act, 156
perimeter security policies	HIPAA, 156
large business case studies, 404	IC3, 156
personal firewalls, 11	Infragard, 156
CSA, 11	U.S. Department of Justice website, 156
phase 1 negotiation (IPsec), 14, 16	protocol analysis, 21
phase 2 negotiation (IPsec), 16–17	proxy ARP (Address Resolution Protocol)
phishing attacks, 49	infrastructure security, disabling for, 73
phone tapping attacks	pstree command
IP telephony, 293–294	Linux forensics, 163
physical security policies	
large business case studies, 404	
ping-of-death attacks, 99	Q
PIX security appliances	
enabling SNMP logging on, 121	quarantining, 157
enabling SYSLOG logging on, 117–118	
PKI	D
digital certificates	R
identity and trust (SAVE framework), 188	
policies (security), building, 54–55	rACL (receive Access Control Lists)
flexibility, 56	CPU traffic
patch management, 56	infrastructure security, 78–80
security changes, 56	RADIUS (Remote Authentication Dial-In User
SME (subject matter experts), 56	Service), 23, 25
updates, 56	RADIUS (Remote Authentication Dial-In User
policy enforcement (SAVE framework), 202–203	Service).
port-control auto command, 271	RADIUS servers
ports	WLC
security	adding to, 226, 228
access layer (IP telephony), 268–269	

Raleigh Office Cisco ASA configuration (small business case studies), 343	crystal-box (grey-box) testing, 46 infrastructure device configuration audits,
configuring	47
access control, 352	open-source tools, 46–48
antispoofing configuration, 353	scheduling, 48
Identity NAT, 351	white-box testing, 46
IM, 354–355, 357–359	threat modeling, 44
IP addressing/routing, 343	COPM, 45
PAT, 347	DREAD model, 44–45
Static NAT, 349	•
rate limits	network visibility, 45
CPU traffic	vulnerabilities, defining, 43 RMON
infrastructure security, 78	instrumentation and management (SAVE
ratings systems (Incident Response Reports), 173	framework), 196
Real IP mode (CAS), 29	role-based CLI. See CLI Views, 64
reconnaissance	root guards
IPv6, 330	IP telephony
security through obscurity, 330	access layer, 268
redirect messages (ICMP)	Root views (CLI Views), 64
infrastructure security, disabling for, 73	route filtering
remote access VPN	infrastructure security, 69
large business case studies,	Routed mode (FWSM), 306
406, 408, 411–412, 415–417	router planes
remote access VPN policies	infrastructure security, 57–58
large business case studies, 405	routers
remote-access VPN (Virtual Private Networks),	ACL
13	blocking unauthorized hosts/users, 6
resource attacks	BGP routers
defining, 99	hopy-by-hop tracebacks, 146
examples of, 99	IOS routers
resource exhaustion, controlling (infrastructure	enabling SNMP logging, 119–121
security), 75	enabling SYSLOG logging, 115–116
CoPP, 80	network firewalls
CPU packet generation, 78	configuring, 6
filtering CPU traffic, 78	sinkhole routers, 37
processors versus interrupt time, 78	routing protocols
rACL, 78–80	authentication
rate limiting CPU traffic, 78	identity and trust (SAVE framework), 189
resource threshold notifications, 76–77	EGP, 67
scheduler allocate command, 81	IGP
scheduler interval command, 81	distance vector protocols, 67
RF (radio frequencies)	link state protocols, 67
WLC, 238	infrastructure security, 67
risk analysis, 43	authentication, 68–69
penetration testing, 46	route filtering, 69
black-box testing, 46	static routing peers, 68
confidentiality requirements, 48	TTL security checks, 70

routing security	ITU-T X.805 versus, 178, 180-181
IPv6, 334	policy enforcement, 202-203
routing tables	visibility, 189
visibility (SAVE framework), 191	anomaly detection, 190
RTBH (Remotely Triggered Black Hole), 158, 160	CDP, 191
RTBH (Remotely Triggered Black Holes), 36	CEF tables, 191
iBGP, 36	IDS, 190–191
sinkholes, 36–37	IPS, 190–191
	layer 2 routing information, 191
	layer 3 routing information, 191
5	NAM, 191
	routing tables, 191
SAVE (Security Assessment, Validation, and	visualization techniques, 203–205, 207
Execution) framework, 177	scheduler allocate command
correlation, 192	infrastructure security, 81
CSA-MC, 193	scheduler interval command
CS-MARS, 193	infrastructure security, 81
Peakflow SP, 193	scheduling
Peakflow X, 193	penetration tests, 48
identity and trust, 183	SDM (Secure Device Manager)
AAA, 183–184	infrastructure security, 88–89
Cisco Guard active verification, 185	Secure ACS Servers
DHCP snooping, 186–187	configuring 802.1x with EAP-FAST,
digital certificates, 188	229, 232–233
IKE, 188	security intelligence, 50
IP Source Guard, 187–188	Cisco Security Center, 50
NAC, 188	CVSS, 50
routing protocol authentication, 189	base metrics, 51
strict Unicast RPF, 189	environmental metrics, 52
instrumentation and management, 193	temporal metrics, 51
Cisco IOS configuration logger logs, 195	IMS (Internet Motion Sensor), 50
Cisco IOS configuration rollback feature,	research initiatives/organizations, 50
195	security policies
Cisco IOS XR XML interface, 196	change management policies large business case studies, 406
CSM, 195	device security policies
embedded device managers, 195	large business case studies, 405
RMON, 196	Internet usage policies
SNMP, 196 Syslog, 196	large business case studies, 406
isolation and virtualization, 196	large business case studies, 404
	change management policies, 406
anomaly detection zones, 198 Cisco IOS role-based CLI Access, 197	device security policies, 405
CLI Views, 197	Internet usage policies, 406
firewalls segmentation, 200	patch management policies, 406
network device virtualization, 198–199	perimeter security policies, 404
VLAN segmentation, 199	physical security policies, 404
VRF segmentation, 200	remote access VPN policies, 405
VRF-Lite segmentation, 200	
THE DESTITION, 200	

patch management policies	show ip dhcp snooping command
large business case studies, 406	verifying DHCP snooping VLAN
perimeter security policies	configurations, 187
large business case studies, 404	show ip flow export command
physical security policies	collecting CLI NetFlow statistics, 114
large business case studies, 404	show snmp group command
remote access VPN policies	viewing SNMP group information, 120
large business case studies, 405	signature updates
security policies, building, 54–55	IPS/IDS devices, 131–132
flexibility, 56	signatures
patch management, 56	IDS, 20
security changes, 56	sinkholes, 36–37
SME (subject matter experts), 56	site-to-site VPN
updates, 56	small business case study, 377, 380–381, 383,
security through obscurity, 330	385, 387, 389
seeds, 216	site-to-site VPN (Virtual Private Networks), 12
segmentation	Sleuth Kit (Linux forensics tool), 162
data center security, 303-304	small business case studies, 341–342
FWSM, 306-314, 316-322	Atlanta Office Cisco ISO configuration, 360
firewalls	locking down IOS routers, 360, 363, 366,
isolation and virtualization (SAVE	368, 370–375
framework), 200	NAT configuration, 376
VLAN	site-to-site VPN, 377, 380–381, 383, 385,
isolation and virtualization (SAVE	387, 389
framework), 199	Raleigh Office Cisco ASA configuration, 343
VRF	access control, 352
isolation and virtualization (SAVE	antispoofing configuration, 353
framework), 200	Identity NAT, 351
VRF-Lite	<i>IM</i> , 354–355, 357–359
isolation and virtualization (SAVE	IP addressing/routing, 343
framework), 200	PAT, 347
service password-encryption global command	Static NAT, 349
local password management (infrastructure	SME (subject matter experts)
security), 61	security policies, building, 56
service tcp-keepalives-in command	smurf attacks
enabling TCP keepalives on incoming sessions,	IPv6, 334
63	SNMP, 118–119
service timestamps log datetime command	access control
enabling SYSLOG logging on IOS routers, 116	infrastructure security, 66
set port disable command	ASA security appliances, enabling logging on,
network access device ports, locking for	121
infrastructure security, 75	instrumentation and management (SAVE
Shadowserver.com website	framework), 196
botnet activity, 145	IOS router/switch logging, enabling, 119–121
show ip cache flow command	PIX security appliances, enabling logging on,
collecting CLI NetFlow statistics, 112, 114	121
Enterprise tracebacks, 147	snmp deny version command, 121

snmp-server enable traps cpu threshold	SYN cookies
command	data center security, 297–299
CPU threshold violation notification,	SYN-flooding, 297
configuring for infrastructure security, 76	Syslog
snooping (DHCP)	instrumentation and management (SAVE
identity and trust (SAVE framework), 186–187	framework), 196
social engineering, 49 source routing (IP)	SYSLOG (System Logs), 115 ASA security appliances, enabling logging on.
infrastructure security, disabling for, 73	117–118
	CATOS running catalyst switches, enabling
spoofing IPv6, 333	logging on, 117
SRTP (Source Real-Time Transport Protocol)	IOS router/switch logging, enabling, 115–116
IP telephony eavesdropping attacks, 294	PIX security appliances, enabling logging on,
SSH	117–118
Telnet versus, 59–60	Systenals (Windows forensics tools), 164
ssh timeout command	Systemas (Windows forensies tools), 104
modifying idle timeouts, 63	
SSL (Secure Sockets Layer)	T
VPN, 18	•
stateful firewalls, 9	TACACS+, 25
stateful pattern-matching recognition, 20	TAD XT (Traffic Anomaly Detectors XT)
Static NAT	identifying/classifying security threats,
small business case study, 349	127–128, 131
strong device access control (infrastructure	TCP Client
security), 59	IDENT
authentication banner configuration, 62	infrastructure security, disabling for, 74
CLI Views, 64–65	TCP ports
interactive access control, 62-64	Cisco Unity, 282–285
local password management, 61	TCP small servers
SNMP access control, 66	infrastructure security, disabling for, 74
SSH versus Telnet, 59–60	TEAP (Tunneled EAP). See EAP-FAST, 224
subnet prefixes	telemetry
IPv6, 331	infrastructure security, 89
Superviews (CLI Views), 64	telemetry/anomaly detection
supplicants (802.1x), 26, 219	CS-MARS, 121–122, 125
switches	Guard XT, 127, 129–131
catalyst switches	IPS, 137–138
enabling SYSLOG logging on CATOS	NAM, 125–126
running switches, 117	NetFlow, 108
distribution layer switches	Cisco platform support, 108
configuring NetFlow at, 103	collecting CLI statistics, 112–114
IOS switches	Egress NetFlow, 111
enabling SNMP logging, 119–121	enabling, 111–112
enabling SYSLOG logging, 115–116	flows, elements of, 109
switchport port-security violation restrict	flows, exporting data from, 110
command	flows, obtaining additional information
IP telephony security, 269	from, 109–110

Ingress NetFlow, 111	telnet timeout command
IPFIX WG, 110	modifying idle timeouts, 63
NDE packet templates, 110	templates
open source monitoring tools, 126–127	NDE packet templates (NetFlow), 110
SNMP, 118–119	temporal metrics (CVSS), 51
enabling IOS router/switch logging,	threat modeling, 44
119–121	COPM, 45
enabling logging on ASA security	DREAD model, 44–45
appliances, 121	network visibility, 45
enabling logging on PIX security	threats (security)
appliances, 121	identifying/classifying
SYSLOG, 115	CS-MARS, 121–122, 125
enabling IOS router/switch logging,	Guard XT, 127, 129–131
115–116	IDS, 131–134, 136
enabling logging on ASA security	IPS, 131–134, 136–138
appliances, 117–118	NAM, 125–126
enabling logging on CATOS running	NetFlow, 108–114
catalyst switches, 117	network visibility, 101, 103, 106–107
enabling logging on PIX security	open source monitoring tools, 126–127
appliances, 117–118	SNMP, 118–121
TAD XT, 127–128, 131	SYSLOG, 115–118
telephony (IP), 261–262, 265	TAD XT, 127–128, 131
access layer, 265, 272	threshold notifications
802.1x, 271	infrastructure security, 76–77
ARP, 270	tiered access control
BPDU, 268	data centers, 303–304
DAI, 270	timeouts
DHCP snooping, 269–270	idle timeouts
NAC, 271	modifying, 63
	TKIP (Temporal Key Integrity Protocol)
port security, 268–269	WEP, 218
root guards, 268 VLAN assignment, 267	WPA, 218
Cisco Personal Assistant, 289	,
	topology maps SAVE framework, 203
hardening operating environment, 289–290	
	tracebacks, 141
server security policies, 291–293	backscatter, 146
Cisco Unified CallManager, 276–277	botnets, 150
Cisco Unified CME, 277–281	Enterprise, 147
Cisco Unity, 281–282, 286–287	CS-MARS, 148
Cisco Unity Express, 287–288	dot-dot attacks, 148
core layer, 265, 275	hop-by-hop, 142
distribution layer, 265, 273	botnets, 145–146
GLBP, 274	zombies, 145
HSRP, 273–274	requirements, 142
eavesdropping attacks, 293–294	service provider environments, 142, 145–146
Telnet	zombies, 150
SSH versus, 59–60	

traffic flows	wireless IPS, 239–240
SAVE framework, 204–205	configuring sensors in WLC, 241–242
transmitting data	configuring signatures, 242–243
telemetry	Wireless Location Appliance, 244
infrastructure security, 89	updates
Transparent mode (FWSM), 306-307	security policies, 56
transport input command	signatures
interactive access control (infrastructure	IPS/IDS devices, 131–132
security), 62	U.S. Department of Justice website, 156
Transport mode (IPsec), 17	username command
TTL (Time-to-Live) security checks	associating local users CLI Views, 65
routing protocols	
infrastructure security, 70	
tuning	V
data center network intrusion detection/	
prevention systems, 325	VACL (VLAN ACL), 157
IPS/IDS devices, 133–134, 136	Virtual Fragment Reassembly
Tunnel mode (IPsec), 17	FWSM data center segmentation, 322
tunneled authentication, 224	Virtual Gateway mode (CAS), 28
	visibility (networks), 101, 103, 106–107
	visibility (SAVE framework), 189
J	anomaly detection, 190
	CDP, 191
UDP ports	CEF tables, 191
Cisco Unity, 282–285	IDS, 190–191
UDP small servers	IPS, 190–191
infrastructure security, disabling for, 74	layer 2 routing information, 191
unauthorized hosts/users	layer 3 routing information, 191
blocking from routers via ACL, 6	NAM, 191
Unicast RPF	routing tables, 191
identity and trust (SAVE framework), 189	VLAN
Unicast RPF (Reverse Path Forwarding)	DHCP snooping, 186–187
infrastructure security policy enforcement,	IP telephony
83–84	access layer, 267
unified mode (AP), 215	private VLAN, 158
Unified Wireless Networks	segmentation
AP, 215	isolation and virtualization (SAVE
architecture of, 212, 214–215	framework), 199
configuring 802.1x with EAP-FAST, 226	VPN (Virtual Private Networks), 12
LWAPP, 236–239	IPsec
MFP, 243	technical overview of, 14–17
NAC, 245	remote access VPN policies
appliance configuration, 246–248, 251,	large business case studies, 405
253–254	remote-access VPN, 13
WLC configuration, 255, 257, 259	site-to-site VPN, 12
J U	small business case study,
	377, 380–381, 383, 385, 387, 389
	SSI VPN 18

802.1x, 219–221, 226, 229, 232–233 configuring CSSC, 233–234, 236 configuring WLC, 226, 228 EAP-FAST, 224–226, 229, 232–233

EAP-GTC, 225 EAP-MD5, 221–222

VPN (virtual private networks)	EAP-TLS, 223
remote access VPN	EAP-TTLS, 224
large business case studies, 406, 408,	LEAP, 222
411–412, 415–417	PEAP, 223, 225
VRF	WEP, 216–218
segmentation	WPA, 218
isolation and virtualization (SAVE	Secure ACS Servers
framework), 200	configuring for 802.1x and EAP-FAST,
VRF-Lite	229, 232–233
segmentation	Unified Wireless Networks
isolation and virtualization (SAVE	AP, 215
framework), 200	architecture of, 212, 214–215
vulnerabilities (risk analysis), defining, 43	configuring 802.1x with EAP-FAST, 226
	LWAPP, 236–239
	MFP, 243
W	NAC, 245–248, 251, 253–255, 257, 259
• •	wireless IPS, 239–243
websites	Wireless Location Appliance, 244
security intelligence, 50	WLC
Cisco Security Center, 50	configuring via NAC, 255, 257, 259
IMS (Internet Motion Sensor), 50	RF, 238
WEP (Wired Equivalent Privacy), 216	WLC (wireless LAN context)
AES encryption protocol, 218	adding RADIUS servers to, 226, 228
ICV, 216–217	configuring, 226, 228
IPsec, 218	worms
limitations of, 217	data center security, 297
seeds, 216	Cisco Guard, 302
TKIP, 218	Flexible NetFlow, 301
white-box penetration testing, 46	IDS, 300
Windows	infrastructure protection, 302–303
forensics tools	IPS, 300
EnCase, 165	NetFlow, 301
Systernals, 164	WPA (Wi-Fi Protected Access), 218
wireless IPS (Intrusion Prevention Systems),	(\(\text{111}\)(\(11110\text{11110\text{
239–240	
configuring	Z
sensors in WLC, 241–242	-
signatures, 242–243	zombies, 99
Wireless Location Appliance, 244	hop-by-hop tracebacks, 145
wireless Location Appliance, 244 wireless networks, 211	tracebacks, 150
authentication, 216	Hacebacks, 150
authentication, 210	