

Numerics

802.1x, 219

- access layer (IP telephony), 271
- authentication negotiation schemes, 220
- authenticators, 26
- components of, 219
- configuring Secure ACS Servers, 229, 232–233
- configuring with EAP-FAST in Unified Wireless Solutions, 226
- EAP methods, 220–221
- IEEE 802.1x, 26
- supplicants, 26

A

AAA

- identity and trust (SAVE framework), 183–184
- infrastructure devices, configuring
 - medium-sized business case studies*, 400–401

AAA (Authentication, Authorization, Accounting), 23

- identity management solutions/systems, 26
 - IBNS*, 26
 - IEEE 802.1x*, 26
- RADIUS, 23, 25
- TACACS+, 25

aaa authorization command, 65

aaa new-model command, 65

access control

- small business case study, 352

access layer (IP telephony), 265, 272

- 802.1x, 271
- ARP, 270
- BPDU, 268
- DAI, 270
- DHCP snooping, 269–270
- NAC, 271
- port security, 268–269
- root guards, 268
- VLAN assignment, 267

access-class command

- interactive access control (infrastructure security), 62

accounting, 23

ACL

- blocking unauthorized hosts/users from routers, 6
- exception ACL, configuring, 64

ACL (Access Control Lists), 157

- controlling FWSM access via, 317–321
- iACL (infrastructure Access Control Lists)
 - infrastructure security policy enforcement*, 82
- IPv6 filtering, 331–332
- rACL (receive Access Control Lists)
 - infrastructure security*, 78–80
- VACL, 157

action plans, building, 173–174

active-standby failovers

- ASA, configuring on
 - medium-sized business case studies*, 394–396, 398–399

AES (Advanced Encryption Standard) encryption protocol

- WEP, 218

AIP-SSM

- ASA, configuring on
 - medium-sized business case studies*, 391–394

Aironet AP (Access Points)

- managing, 216

analyzing data

- postmortems, 169

anomaly detection

- IPS devices, 137–138
- visibility (SAVE framework), 190

anomaly detection systems, 22

anomaly detection zones

- isolation and virtualization (SAVE framework), 198

anomaly/telemetry detection

- CS-MARS, 121–122, 125
- Guard XT, 127, 129–131
- IPS, 137–138
- NAM, 125–126

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

- auto secure command**
 - infrastructure security, 84–85
- autonomous mode (AP), 215**
- Autopsy (Linux forensics tool), 162–163**
- AutoSecure (Cisco IOS)**
 - infrastructure security, 84–88

B

- backscatter, 146**
- banners**
 - authentication banners
 - configuring for infrastructure security, 62
- base metrics (CVSS), 51**
- BGP (Border Gateway Protocol)**
 - routers
 - hop-by-hop tracebacks, 146
- black-box penetration testing, 46**
- bogon addresses, 37**
- BOOTP servers**
 - infrastructure security, disabling for, 73
- botnets**
 - hop-by-hop tracebacks, 145
 - BGP routers, 146
 - Shadowserver.com website, 145
 - tracebacks, 150
- bots, 99**
- BPDU (Bridge Protocol Data Units)**
 - IP telephony
 - access layer, 268
- broadcast amplification attacks. See smurf attacks, 334**

C

- CAM (Clean Access Manager), NAS Appliance, 27, 31**
- CAS (Clean Access Servers), NAC Appliance, 27–28**
 - Centralized Deployment mode, 31
 - Edge Deployment mode, 30
 - Real IP mode, 29
 - Virtual Gateway mode, 28

- case studies**
 - large businesses, 401, 403
 - CSIRT, 403
 - incident response, 419–420
 - IPsec remote access VPN, 406, 408, 411–412, 415–417
 - load-balancing, 415–417
 - security policy creation, 404–406
 - medium-sized businesses, 389
 - configuring AAA on infrastructure devices, 400–401
 - configuring active-standby failovers on ASA, 394–396, 398–399
 - configuring AIP-SSM on ASA, 391–394
 - Internet edge routers, 391
 - small businesses, 341–343, 360
 - access control, 352
 - antispoofing configuration, 353
 - Identity NAT, 351
 - IM, 354–355, 357–359
 - IP addressing/routing, 343
 - locking down IOS routers, 360, 363, 366, 368, 370–375
 - NAT configuration, 376
 - PAT, 347
 - site-to-site VPN, 377, 380–381, 383, 385, 387, 389
 - Static NAT, 349
- catalyst switches**
 - CATOS running switches
 - enabling SYSLOG logging on, 117
- CATOS (Catalyst Operating System)**
 - catalyst switches
 - enabling SYSLOG logging on, 117
- CDP**
 - visibility (SAVE framework), 191
- CDP (Cisco Discovery Protocol)**
 - infrastructure security, disabling for, 71
- CEF tables**
 - visibility (SAVE framework), 191
- Centralized Deployment mode (CAS), 31**
- change management policies**
 - large business case studies, 406
- changeto context command**
 - FWSM configuration for data center segmentation, 312

checklists

- incident-handling policies, 154–155

CIRCA (Cisco Incident Response Communications Arena), 54**Cisco Catalyst switches**

- data center segmentation, configuring for, 309–310

Cisco Guard

- active verification
 - identity and trust (SAVE framework), 185*
- data center security, 302

Cisco IOS

- AutoSecure
 - infrastructure security, 84–88*

Cisco Personal Assistant

- securing, 289
 - hardening operating environment, 289–290*
 - server security policies, 291–293*

Cisco Security Center, 50**Cisco Unified CallManager (IP telephony), securing, 276–277****Cisco Unified CME (Communications Manager Express)**

- securing, 277–281

Cisco Unity

- securing, 281–282, 286–287
- TCP/UDP ports, 282–285

Cisco Unity Express

- securing, 287–288

classifying security threats

- CS-MARS, 121–122, 125

- Guard XT, 127, 129–131

- IDS, 131

- signature updates, 131–132*

- tuning, 133–134, 136*

- IPS, 131

- anomaly detection, 137–138*

- IDM, 132*

- signature updates, 131–132*

- tuning, 133–134, 136*

- NAM, 125–126

- 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 from, 109–110*

- Ingress NetFlow, 111*

- IPFIX WG, 110*

- NDE packet templates, 110*

- network visibility, 101, 103, 106–107

- open source monitoring tools, 126–127

- SNMP, 118–119

- enabling IOS router/switch logging, 119–121*

- enabling logging on ASA security appliances, 121*

- enabling logging on PIX security appliances, 121*

- SYSLOG, 115

- enabling IOS router/switch logging, 115–116*

- enabling logging on ASA security appliances, 117–118*

- enabling logging on CATOS running catalyst switches, 117*

- enabling logging on PIX security appliances, 117–118*

- TAD XT, 127–128, 131

Clean Access Agents (NAC appliance), 27**CLI**

- NetFlow statistics

- collecting, 112–114*

CLI Views

- enable view command, 65

- infrastructure security, 64–65

- isolation and virtualization (SAVE framework), 197

- Lawful intercept views, 64

- parser view command, 65

- Root views, 64

- Superviews, 64

- username command, 65

collaboration (incident-handling policies/procedures), 153**collecting data**

- postmortems, 169

Computer Fraud and Abuse Act, 156**confidentiality**

- penetration tests, 48

- configuration logger (IOS)**
 - 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). 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*, 78–80
 - rate limiting traffic
 - infrastructure security*, 78
 - scheduler allocate command
 - infrastructure security*, 81
 - scheduler interval command
 - infrastructure security*, 81
- CPU threshold notifications, 76**
- crystal-box (grey-box) penetration testing, 46**
- CSA (Cisco Security Agent), 11**
 - endpoint security, 92–94
- CSA (Cisco Security Agents)**
 - data centers, deploying for, 325
 - configuring agent kits*, 326
 - CSA architectures*, 325–326
 - phased deployments*, 326–327
- CSA-MC (Cisco Security Agent Mangement 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
 - selecting personnel for, 53
 - tasks of, 54
- CSM**
 - data center security
 - SYN cookies*, 299
- CSM (Cisco Security Manager)**
 - instrumentation and management (SAVE framework), 195
- CS-MARS**
 - correlation (SAVE framework), 193
 - tracebacks, 148
- CS-MARS (Cisco Security Monitoring, Analysis 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

D

DAI (Dynamic Address Inspection)

access layer (IP telephony), 270

dark IP addresses, 37

data analysis

postmortems, 169

telemetry

infrastructure security, 89

data centers, 297

CSA, deploying, 325

configuring agent kits, 326

CSA architectures, 325–326

phased deployments, 326–327

DoS attacks, 297

Cisco Guard, 302

Flexible NetFlow, 301

IDS, 300

IPS, 300

NetFlow, 301

SYN cookies, 297–299

infrastructure protection, 302–303

network intrusion detection/prevention systems,

deploying, 322

monitoring, 325

sending selective traffic to IDS/IPS

devices, 322, 324

tuning, 325

segmentation, 303–304

FWSM, 306–314, 316–322

tiered access control, 303–304

worms, 297

Cisco Guard, 302

Flexible NetFlow, 301

IDS, 300

infrastructure protection, 302–303

IPS, 300

NetFlow, 301

data collection

postmortems, 169

data transmission

telemetry

infrastructure security, 89

deep packet inspection, 10

deep-packet inspection, 9

device authorize command, 272

device security policies

large business case studies, 405

DHCP

snooping

identity and trust (SAVE framework),

186–187

DHCP snooping

access layer (IP telephony), 269–270

diagrams (networks)

high-level enterprise diagrams, 101, 103

layered diagrams, 106

digital certificates

identity and trust (SAVE framework), 188

Directed Broadcasts (IP)

infrastructure security, disabling for, 72

distance vector protocols (IGP), 67

distribution layer (IP telephony), 265, 273

GLBP, 274

HSRP, 273–274

distribution layer switches

NetFlow

configuring at, 103

DMZ (demilitarized zones), 10

DMZ servers

Static NAT

small business case study, 349

documentation

incident-handling policies, 154–155

DoS (Denial of Service) attacks

data center security, 297

Cisco Guard, 302

Flexible NetFlow, 301

IDS, 300

infrastructure protection, 302–303

IPS, 300

NetFlow, 301

SYN cookies, 297–299

dot-dot attacks

tracebacks, 148

dotlx port-control auto command, 271

DREAD model (threat modeling), 44–45

E

EAP methods

802.1x, 220–221

EAP-FAST, 224–225
 configuring 802.1x in Unified Wireless Solutions, 226
 configuring Secure ACS Servers, 229, 232–233

EAP-GTC, 225

EAP-MD5, 221–222

EAP-TLS, 223

EAP-TTLS (EAP Tunneled TLS Authentication Protocol), 224

eavesdropping attacks
 IP telephony, 293–294

Edge Deployment mode (CAS), 30

EGP (Exterior Gateway Protocols), 67

Egress NetFlow, 111

enable view command, 65

EnCase (Guidance Software), 165

endpoint security
 CSA, 92–94
 patch management, 90–91

engineering (social), 49

Enterprise
 tracebacks, 147
 CS-MARS, 148
 dot-dot attacks, 148

environmental metrics (CVSS), 52

escalation procedures (incident-handling policies/procedures), 154

escalation procedures (NAC), 97

ethical hacking. See penetration testing, 46

exception ACL, configuring, 64

exec-timeout command
 modifying idle timeouts, 63

extension headers
 IPv6, 332

external databases (802.1x), 219

F

failovers
 active-standby failovers
 medium-sized business case studies, 394–396, 398–399

feedback
 looped feedback
 postmortems, 167

filtering
 CPU traffic
 infrastructure security, 78

IPv6, 331
 ACL, 331–332

routes
 infrastructure security, 69

Finger Protocol
 infrastructure security, disabling for, 72

firewalls, 5
 data center security
 SYN cookies, 297–299

network firewalls, 6
 deep packet inspection, 10
 DMZ, 10
 NAT, 7–8
 packet filters, 7
 router configurations, 6
 stateful firewalls, 9

personal firewalls, 11
 CSA, 11

segmentation
 isolation and virtualization (SAVE framework), 200

FIRST (Forum for Incident Response and Security Teams)
 tracebacks, 142

Flexible NetFlow
 data center security, 301

forensics, 160
 Linux forensics tools, 162–163
 netstat command, 163
 pstree command, 163

log files, 161

Windows forensics tools
 EnCase, 165
 Systemals, 164

fragment command
 FWSM, data center segmentation, 322

fragmentation
 IPv6, 333

FWSM
 data center segmentation, 306, 308
 configuring Cisco Catalyst switches, 309–310
 configuring NAT, 313–314, 316

configuring security context interfaces, 312–313
controlling access via ACL, 317–321
creating security contexts, 310–312
Routed mode, 306
Transparent mode, 306–307
Virtual Fragment Reassembly, 322

FWSM (Firewall Services Module)

data center security
SYN cookies, 298

G**GLBP (Gateway Load Balancing Protocol)**

distribution layer (IP telephony), 274

grey-box (crystal-box) penetration testing, 46**set port dotlx, 271****Guard (Cisco)**

active verification
identity and trust (SAVE framework), 185

Guard XT (Traffic Anomaly Detectors XT)

identifying/classifying security threats, 127,
 129–131

H**hacking**

ethical hacking. See penetration testing, 46

headers

extension headers
IPv6, 332
 manipulation attacks
IPv6, 333

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
 zombies, 145

HSRP (Hot Standby Router Protocol)

distribution layer (IP telephony), 273–274

HTTP

authentication
infrastructure security, 63

I**iACL (infrastructure Access Control Lists)**

infrastructure security policy enforcement, 82

IB (in-band) mode (NAC appliance), 29**iBGP (internal Border Gateway Protocol), 36****IBNS (Identity-Based Networking Services), 26****IC3 (Internet Crime Complaint Center), 156****ICMP**

redirect messages
infrastructure security, disabling for, 73

ICMP filtering

IPv6, 332

ICV (Integrity Check Values), 216–217**IDENT (Identity Protocol)**

infrastructure security, disabling for, 74

identifiers (local)

IPv6, 331

identifying security threats

CS-MARS, 121–122, 125

Guard XT, 127, 129–131

IDS, 131

signature updates, 131–132

tuning, 133–134, 136

IPS, 131

anomaly detection, 137–138

IDM, 132

signature updates, 131–132

tuning, 133–134, 136

NAM, 125–126

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 from, 109–110

Ingress NetFlow, 111

IPFIX WG, 110

NDE packet templates, 110

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

infrastructure devices

- AAA, configuring on
 - medium-sized business case studies, 400–401*
- infrastructure security, 57**
 - automated security tools
 - Cisco IOS AutoSecure, 84–88*
 - SDM, 88–89*
 - disabling unnecessary services, 70
 - BOOTP servers, 73*
 - CDP, 71*
 - Finger protocol, 72*
 - ICMP redirect messages, 73*
 - IDENT, 74*
 - IP Directed Broadcasts, 72*
 - IP source routing, 73*
 - IPv6, 75*
 - MOP, 72*
 - PAD, 73*
 - proxy ARP, 73*
 - TCP/UDP small servers, 74*
 - locking unused network access device ports, 75
 - policy enforcement, 81
 - iACL, 82*
 - Unicast RPF, 83–84*
 - resource exhaustion control, 75
 - CoPP, 80*
 - CPU packet generation, 78*
 - filtering CPU traffic, 78*
 - processors versus interrupt time, 78*
 - rACL, 78–80*
 - rate limiting CPU traffic, 78*
 - resource threshold notifications, 76–77*
 - scheduler allocation command, 81*
 - scheduler interval command, 81*
 - router planes, 57–58
 - routing protocols, 67
 - authentication, 68–69*
 - route filtering, 69*
 - static routing peers, 68*
 - TTL security checks, 70*
 - strong device access control, 59
 - authentication banner configuration, 62*
 - CLI Views, 64–65*
 - interactive access control, 62–64*
 - local password management, 61*

SNMP access control, 66

SSH versus Telnet, 59–60

telemetry, 89

Ingress NetFlow, 111**instrumentation and management (SAVE framework), 193**

- Cisco IOS configuration logger logs, 195
- Cisco IOS configuration rollback feature, 195
- Cisco IOS CR XML interface, 196
- CSM, 195
- embedded device managers, 195
- RMON, 196
- SNMP, 196
- Syslog, 196

intelligence (security), 50

- Cisco Security Center, 50
- CVSS, 50
 - base metrics, 51*
 - environmental metrics, 52*
 - temporal metrics, 51*
- IMS (Internet Motion Sensor), 50
- research initiatives/organizations, 50

interactive access control (infrastructure security), 62–64**Internet edge routers**

- medium-sized business case studies, 391

Internet usage policies

- large business case studies, 406

IOS

- configuration logger
 - instrumentation and management (SAVE framework), 195*
- configuration rollback feature
 - instrumentation and management (SAVE framework), 195*
- CR XML interface
 - instrumentation and management (SAVE framework), 196*
- role-based CLI Access
 - isolation and virtualization (SAVE framework), 197*

IOS routers

- small business case study, 360, 363, 366, 368, 370–375
- SNMP logging, enabling, 119–121
- SYSLOG logging, enabling, 115–116

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

- routing security, 334
- smurf attacks, 334
- spoofing, 333
- subnet prefixes, 331

IPv6 (IP Version 6)

- infrastructure security, disabling for, 75

ipv6 access-list command, 331**ISAC (Information Sharing and Analysis Centers), 54****isolation and virtualization (SAVE framework), 196**

- anomaly detection zones, 198
- Cisco IOS role-based CLI Access, 197
- CLI Views, 197
- firewall segmentation, 200
- network device virtualization, 198–199
- VLAN segmentation, 199
- VRF segmentation, 200
- VRF-Lite segmentation, 200

ITU-T X.805

- SAVE versus, 178, 180–181

L**large business case studies, 401, 403**

- CSIRT, 403
- incident response, 419–420
- IPsec remote access VPN, deploying, 406, 408, 411–412, 415–417
 - load-balancing, 415–417*
- security policy creation, 404
 - change management policies, 406*
 - device security policies, 405*
 - Internet usage policies, 406*
 - patch management policies, 406*
 - perimeter security policies, 404*
 - physical security policies, 404*
 - remote access VPN policies, 405*

law enforcement, 155

- Computer Fraud and Abuse Act, 156
- HIPAA, 156
- IC3, 156
- Infragard, 156
- U.S. Department of Justice website, 156

Lawful intercept view (CLI Views), 64**layer 2 routing**

- visibility (SAVE framework), 191

layer 3 routing

- visibility (SAVE framework), 191

layered diagrams, 106**LEAP, 222****Lessons Learned section (Incident Response Reports), 171****link state protocols (IGP), 67****Linux**

- forensics tools
 - Autopsy, 162–163*
 - netstat command, 163*
 - pstree command, 163*
 - Sleuth Kit, 162*

load balancers

- data center security
 - SYN cookies, 297–299*

load-balancing

- large business case studies, 415–417

local identifiers

- IPv6, 331

log files (forensics), 161**logging on host command**

- enabling SYSLOG logging on ASA/PIX
- security appliances, 117

logging on command

- enabling SYSLOG logging on ASA/PIX
- security appliances, 117

logging trap command

- enabling SYSLOG logging on ASA/PIX
- security appliances, 117
- SYSLOG logging, 116

logic attacks

- defining, 99
- examples of, 99

login block-for command

- interactive access control (infrastructure security), 64

login delay command

- interactive access control (infrastructure security), 63

login quiet-mode access-class global command

- configuring exception ACL, 64

looped feedback

- postmortems, 167

m/p, 271

LWAPP (Lightweight Access Point Protocol), 215
LWAPP (Lightweight Access Point Protocol), 236–239

M

main mode negotiation (IPsec), 15–16

medium-sized business case studies, 389

AAA, configuring on infrastructure devices, 400–401

active-standby failovers, configuring on ASA, 394–396, 398–399

AIP-SSM, configuring on ASA, 391–394

Internet edge routers, 391

memory

threshold notifications, 77

memory free low-watermark io threshold

command

memory threshold notifications, configuring for infrastructure security, 77

memory free low-watermark processor threshold

global command

memory threshold notifications, configuring for infrastructure security, 77

memory reserve critical kilobytes command

memory threshold notifications, configuring for infrastructure security, 77

MFP (Management Frame Protection), 243

mls flow ip interface-full command

collecting CLI NetFlow statistics, 114

mode multiple command

FWSM configuration for data center segmentation, 311

monitoring tools (open source)

identifying/classifying security threats, 126–127

MOP (Maintenance Operations Protocol)

infrastructure security, disabling for, 72

N

NAC (Network Admission Control), 27, 94, 245

access layer (IP telephony), 271

administrative tasks, 96

appliance configuration,

246–248, 251, 253–254

escalation procedures, 97

identity and trust (SAVE framework), 188

NAC Appliance, 27, 33

CAM, 27, 31

CAS, 27–31

Clean Access Agents, 27

High Availability, 31

IB mode, 29

OOB mode, 29–30

NAC Framework, 33–34, 36

NAD, 34

NAH, 35

phased deployments, 94–95

staff and support, 96–97

WLC configuration, 255, 257, 259

NAC Appliance, 27, 33

CAM, 27, 31

CAS, 27–28

Centralized Deployment mode, 31

Edge Deployment mode, 30

Real IP mode, 29

Virtual Gateway mode, 28

Clean Access Agents, 27

High Availability, 31

IB mode, 29

OOB mode, 29–30

NAC Framework, 33–34, 36

NAD, 34

NAH, 35

NAD (NAC Framework), 34

NAH (NAC Agentless Hosts), 35

NAM (Network Analysis Module), 125–126

visibility (SAVE framework), 191

NANOG (North American Network Operators Group)

tracebacks, 142

NAS (network access servers). See also RADIUS, 23

NAT

configuring

small business case study, 376

NAT (Network Address Translation)

FWSM configuration for data center

segmentation, 313–314, 316

network firewalls, 7–8

NDE packet templates (NetFlow), 110**NetFlow, 108**

- as anomaly detection systems, 22
- Cisco platform support, 108
- CLI statistics, collecting, 112–114
- data center security, 301
- distribution layer switches
 - configuring at, 103*
- Egress NetFlow, 111
- enabling, 111–112
- Flexible NetFlow, 301
- flows
 - elements of, 109*
 - exporting data from, 110*
 - IPFIX WG, 110*
 - obtaining additional information from, 109–110*
- Ingress NetFlow, 111
- NDE packet templates, 110

netstat command

- Linux forensics, 163

network access devices

- locking down unused ports (infrastructure security), 75

Network Authentication screen (CSSC), 234**network devices**

- isolation and virtualization (SAVE framework), 198–199

network firewalls, 6

- deep packet inspection, 10
- DMZ, 10
- NAT, 7–8
- packet filters, 7
- router configurations, 6
- stateful firewalls, 9

network intrusion detection/prevention systems

- data centers, deploying for, 322
 - monitoring, 325*
 - sending selectiv traffic to IDS/IPS devices, 322, 324*
 - tuning, 325*

Network Profile screen (CSSC), 233**networks**

- diagrams
 - high-level enterprise diagrams, 101, 103*
 - layered diagrams, 106*

- visibility, 101, 103, 106–107

threat modeling (risk analysis), 45

no ip bootp server global command

- BOOTP servers, disabling for infrastructure security, 73

no ip identd global command

- IDENT, disabling for infrastructure security, 74

no ip redirects interface subcommand

- ICMP redirect messages, disabling for infrastructure security, 73

no ipv6 address interface subcommand

- disabling IPv6 for infrastructure security, 75

no ipv6 enable interface subcommand

- disabling IPv6 for infrastructure security, 75

no service pad global command

- PAD, disabling for infrastructure security, 73

O**OOB (out-of-band) mode (NAC appliance), 29–30****open source**

- monitoring tools
 - identifying/classifying security threats, 126–127*

P**packet filters, 7****packet registration**

- CPU traffic
 - infrastructure security, 78*

PAD (Packet Assembler/Disassembler)

- infrastructure security, disabling for, 73

parser view command, 65**passwords**

- local password management
 - infrastructure security, 61*

PAT

- small business case study, 347

patch management

- endpoint security, 90–91
- security policies, building, 56

patch management policies

- large business case studies, 406

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

Raleigh Office Cisco ASA configuration (small business case studies), 343

configuring

- access control*, 352
- antispoofing configuration*, 353
- Identity NAT*, 351
- IM*, 354–355, 357–359
- IP addressing/routing*, 343
- PAT*, 347
- Static NAT*, 349

rate limits

CPU traffic

- infrastructure security*, 78

ratings systems (Incident Response Reports), 173**Real IP mode (CAS), 29****reconnaissance**

IPv6, 330

- security through obscurity*, 330

redirect messages (ICMP)

- infrastructure security, disabling for, 73

remote access VPN

- large business case studies, 406, 408, 411–412, 415–417

remote access VPN policies

- large business case studies, 405

remote-access VPN (Virtual Private Networks), 13**resource attacks**

- defining, 99
- examples of, 99

resource exhaustion, controlling (infrastructure security), 75

- CoPP, 80
- CPU packet generation, 78
- filtering CPU traffic, 78
- processors versus interrupt time, 78
- rACL, 78–80
- rate limiting CPU traffic, 78
- resource threshold notifications, 76–77
- scheduler allocate command, 81
- scheduler interval command, 81

RF (radio frequencies)

WLC, 238

risk analysis, 43

- penetration testing, 46
 - black-box testing*, 46
 - confidentiality requirements*, 48

- crystal-box (grey-box) testing*, 46
- infrastructure device configuration audits*, 47

- open-source tools*, 46–48

- scheduling*, 48

- white-box testing*, 46

threat modeling, 44

- COPM*, 45

- DREAD model*, 44–45

- network visibility*, 45

- vulnerabilities, defining, 43

RMON

- instrumentation and management (SAVE framework), 196

role-based CLI. See CLI Views, 64**root guards**

IP telephony

- access layer*, 268

Root views (CLI Views), 64**route filtering**

- infrastructure security, 69

Routed mode (FWSM), 306**router planes**

- infrastructure security, 57–58

routers

ACL

- blocking unauthorized hosts/users*, 6

BGP routers

- hop-by-hop tracebacks*, 146

IOS routers

- enabling SNMP logging*, 119–121
- enabling SYSLOG logging*, 115–116

network firewalls

- configuring*, 6

sinkhole routers, 37

routing protocols

authentication

- identity and trust (SAVE framework)*, 189

EGP, 67

IGP

- distance vector protocols*, 67

- link state protocols*, 67

infrastructure security, 67

- authentication*, 68–69

- route filtering*, 69

- static routing peers*, 68

- TTL security checks*, 70

- routing security**
 - IPv6, 334
- routing tables**
 - visibility (SAVE framework), 191
- RTBH (Remotely Triggered Black Hole), 158, 160**
- RTBH (Remotely Triggered Black Holes), 36**
 - iBGP, 36
 - sinkholes, 36–37

S

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

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

snmp-server enable traps cpu threshold command
 CPU threshold violation notification,
 configuring for infrastructure security, 76

snooping (DHCP)
 identity and trust (SAVE framework), 186–187

social engineering, 49

source routing (IP)
 infrastructure security, disabling for, 73

spoofing
 IPv6, 333

SRTP (Source Real-Time Transport Protocol)
 IP telephony eavesdropping attacks, 294

SSH
 Telnet versus, 59–60

ssh timeout command
 modifying idle timeouts, 63

SSL (Secure Sockets Layer)
 VPN, 18

stateful firewalls, 9

stateful pattern-matching recognition, 20

Static NAT
 small business case study, 349

strong device access control (infrastructure security), 59
 authentication banner configuration, 62
 CLI Views, 64–65
 interactive access control, 62–64
 local password management, 61
 SNMP access control, 66
 SSH versus Telnet, 59–60

subnet prefixes
 IPv6, 331

Superviews (CLI Views), 64

supplicants (802.1x), 26, 219

switches
 catalyst switches
enabling SYSLOG logging on CATOS running switches, 117
 distribution layer switches
configuring NetFlow at, 103
 IOS switches
enabling SNMP logging, 119–121
enabling SYSLOG logging, 115–116

switchport port-security violation restrict command
 IP telephony security, 269

SYN cookies
 data center security, 297–299

SYN-flooding, 297

Syslog
 instrumentation and management (SAVE framework), 196

SYSLOG (System Logs), 115
 ASA security appliances, enabling logging on, 117–118
 CATOS running catalyst switches, enabling logging on, 117
 IOS router/switch logging, enabling, 115–116
 PIX security appliances, enabling logging on, 117–118

Systemals (Windows forensics tools), 164

T

TACACS+, 25

TAD XT (Traffic Anomaly Detectors XT)
 identifying/classifying security threats, 127–128, 131

TCP Client
 IDENT
infrastructure security, disabling for, 74

TCP ports
 Cisco Unity, 282–285

TCP small servers
 infrastructure security, disabling for, 74

TEAP (Tunneled EAP). See EAP-FAST, 224

telemetry
 infrastructure security, 89

telemetry/anomaly detection
 CS-MARS, 121–122, 125
 Guard XT, 127, 129–131
 IPS, 137–138
 NAM, 125–126
 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 from, 109–110

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

traffic flows

SAVE framework, 204–205

transmitting data

telemetry

infrastructure security, 89

Transparent mode (FWSM), 306–307**transport input command**

interactive access control (infrastructure security), 62

Transport mode (IPsec), 17**TTL (Time-to-Live) security checks**

routing protocols

infrastructure security, 70

tuning

data center network intrusion detection/
prevention systems, 325

IPS/IDS devices, 133–134, 136

Tunnel mode (IPsec), 17**tunneled authentication, 224****U****UDP ports**

Cisco Unity, 282–285

UDP small servers

infrastructure security, disabling for, 74

unauthorized hosts/users

blocking from routers via ACL, 6

Unicast RPF

identity and trust (SAVE framework), 189

Unicast RPF (Reverse Path Forwarding)

infrastructure security policy enforcement,
83–84

unified mode (AP), 215**Unified Wireless Networks**

AP, 215

architecture of, 212, 214–215

configuring 802.1x with EAP-FAST, 226

LWAPP, 236–239

MFP, 243

NAC, 245

*appliance configuration, 246–248, 251,
253–254*

WLC configuration, 255, 257, 259

wireless IPS, 239–240

configuring sensors in WLC, 241–242

configuring signatures, 242–243

Wireless Location Appliance, 244

updates

security policies, 56

signatures

IPS/IDS devices, 131–132

U.S. Department of Justice website, 156**username command**

associating local users CLI Views, 65

V**VACL (VLAN ACL), 157****Virtual Fragment Reassembly**

FWSM data center segmentation, 322

Virtual Gateway mode (CAS), 28**visibility (networks), 101, 103, 106–107****visibility (SAVE framework), 189**

anomaly detection, 190

CDP, 191

CEF tables, 191

IDS, 190–191

IPS, 190–191

layer 2 routing information, 191

layer 3 routing information, 191

NAM, 191

routing tables, 191

VLAN

DHCP snooping, 186–187

IP telephony

access layer, 267

private VLAN, 158

segmentation

*isolation and virtualization (SAVE
framework), 199*

VPN (Virtual Private Networks), 12

IPsec

technical overview of, 14–17

remote access VPN policies

large business case studies, 405

remote-access VPN, 13

site-to-site VPN, 12

small business case study,

377, 380–381, 383, 385, 387, 389

SSL VPN, 18

VPN (virtual private networks)

- remote access VPN
 - large business case studies, 406, 408, 411–412, 415–417*

VRF

- segmentation
 - isolation and virtualization (SAVE framework), 200*

VRF-Lite

- segmentation
 - isolation and virtualization (SAVE framework), 200*

vulnerabilities (risk analysis), defining, 43

W

websites

- security intelligence, 50
 - Cisco Security Center, 50*
 - IMS (Internet Motion Sensor), 50*

WEP (Wired Equivalent Privacy), 216

- AES encryption protocol, 218
- ICV, 216–217
- IPsec, 218
- limitations of, 217
- seeds, 216
- TKIP, 218

white-box penetration testing, 46

Windows

- forensics tools
 - EnCase, 165*
 - Systemals, 164*

wireless IPS (Intrusion Prevention Systems), 239–240

- configuring
 - sensors in WLC, 241–242*
 - signatures, 242–243*

Wireless Location Appliance, 244

wireless networks, 211

- authentication, 216
 - 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*

EAP-TLS, 223

EAP-TTLS, 224

LEAP, 222

PEAP, 223, 225

WEP, 216–218

WPA, 218

Secure ACS Servers

- configuring for 802.1x and EAP-FAST, 229, 232–233*

Unified Wireless Networks

- AP, 215*
- architecture of, 212, 214–215*
- configuring 802.1x with EAP-FAST, 226*
- LWAPP, 236–239*
- MFP, 243*
- NAC, 245–248, 251, 253–255, 257, 259*
- wireless IPS, 239–243*
- Wireless Location Appliance, 244*

WLC

- configuring via NAC, 255, 257, 259
- RF, 238

WLC (wireless LAN context)

- adding RADIUS servers to, 226, 228
- configuring, 226, 228

worms

- data center security, 297
 - Cisco Guard, 302*
 - Flexible NetFlow, 301*
 - IDS, 300*
 - infrastructure protection, 302–303*
 - IPS, 300*
 - NetFlow, 301*

WPA (Wi-Fi Protected Access), 218

Z

zombies, 99

- hop-by-hop tracebacks, 145
- tracebacks, 150