mitigating
*at host level*, 23–25
*at network level*, 25–26
Morris worm, characteristics of, 18
Nimda worm, characteristics of, 20–22
replacement login, example of, 17
signatures. *See* signatures
SQL Slammer worm, characteristics of, 21
**authentication**
802.1x, 78
role in layered defense, 79
**Auto mode (software bypass), 63**
**automated response to attacks, 26**
**automatic blocking, 143–144**
**automatic summarization, 46**

## B

**balanced systems, 186**
**behavioral security policies, 122–123**
**behavior-based detection, 44**
**benefits of IPSs, 137**
HIPS
*acceptable use policy enforcement, 95–96*
*attack prevention, 92*
*internal attack propagation prevention, 93*
*patch relief, 92–93*
*policy enforcement, 94–95*
security policy enforcement, 138
traffic normalization, 138
**"benevolent" worms, 16**
**blade-based sensors, 153–154**
**block response, 61**
**block signature action, 47**
**branch office IPS deployment, 236–237**
HIPS implementation, 238
limiting factors, 237
NIPS implementation, 239–240
security policy goals, 237
**buffer overflow vulnerabilities, 22**
**buffer overrun exploit, 105–107**

## C

**cabling, sensors, 221**
**capabilities**
of Cisco IPS network components, 211
of IPSs
*attack prevention, 27*
*regulatory compliance, 27*
**capturing network traffic**
devices for, 158–161
with IPSs, 154
*for Inline mode*, 155–157
*for promiscuous mode*, 157–158
with RSPAN, 162
with SPAN, 162
with VACLs, 164
**characteristics**
of attacks
*CIH virus*, 19
*Loveletter virus*, 19–20
*Morris worm*, 18
*Nimda worm*, 20–22
*replacement login attack*, 17
*SQL Slammer worm*, 21
of signatures, 34
**Chernobyl, 19**
**child processes, 107**
**CIH virus, 19**
**Cisco Catalyst 6500 series IDSM-2, 206–207**
**Cisco IDS Network Module, 207**

**Cisco IOS IPS sensors, 208**
**Cisco IPS 4200 series appliance sensors, 206**
**classifying IPS hosts, 185–187**
**client-server architecture, 8**
**client-server computing, 7–9**
**clipboard, 109**
**collaboration between layers, 81–82**
**COM (Component Object Model), 109**
**communications, securing management communication, 66–68**
**comparing IPS and IDS functionality, 136**
**complexity of attacks, 14–15**
**conducting pilot tests, 194–196**
**configuration updates, 62**
**configuring**
- policy groups, 191–193
- secondary policy groups, 192–193
- sensors, 221

**corporate security policies, 79–80**
- default policy configuration, customizing, 194
- reviewing, 212

**correlation tools, 65–66**
**criteria for sensor selection**
- form factor, 152–154
- interfaces, 151–152
- processing capacity, 150–151

**CSA (Cisco Security Agent), 77**
- phases of deployment, 177
  - *conducting pilot tests*, 194–196
  - *finalizing the project*, 198
  - *full deployment*, 197–198
  - *implementing management*, 189–194
  - *predeployment planning*, 180–184
  - *selection and classification of target hosts*, 184–188
  - *tuning*, 196
  - *understanding the product*, 178–179

**CSA MC (CSA Management Center), organizational units, 190–191**
**CS-MARs (Cisco Security Monitoring, Analysis and Response System), 82**
**customizing default corporate security policy configuration, 194**

## D

**day zero attacks, 77**
**default allow organizations, 214**
**default deny organizations, 214**
**defense-in-depth, 71**
- corporate security policy, 79–80
- examples of, 72–79

**defining goals of IPS deployment, 213–216**
**delivery mechanism of attacks, 13**
**deny response, 61**
**deploying IPSs**
- at medium financial enterprises, 240
  - *HIPS implementation*, 241–242
  - *limiting factors*, 241
  - *NIPS implementation*, 242–243
  - *security goals*, 241
- at branch offices, 236–237
  - *HIPS implementation*, 238
  - *limiting factors*, 237
  - *NIPS implementation*, 239–240
  - *security policy goals*, 237
- at home office, 250
  - *HIPS implementation*, 251–252
  - *limiting factors*, 251
  - *NIPS implementation*, 252
  - *security policy goals*, 251
- at medium educational institutions, 243
  - *HIPS implementation*, 245–246
  - *limiting factors*, 244
  - *NIPS implementation*, 246–247
  - *security policy goals*, 245
- at small offices, 247
  - *HIPS implementation*, 248–249
  - *limiting factors*, 248
  - *NIPS implementation*, 250
  - *security policy goals*, 248
- host IPS, 53
  - *determining factors*, 54–55
- network IPS, 55
  - *determining factors*, 56–58
- on large enterprise, 229–230
  - *HIPS implementation*, 231–233
  - *limiting factors*, 231
  - *NIPS implementation*, 233, 236
  - *security policy goals*, 231
- sensors
  - *large deployments*, 169
  - *small deployments*, 168

- **deployment phases**
  - of CSA, 177
    - *conducting pilot tests, 194–196*
    - *finalizing the project, 198*
    - *full deployment, 197–198*
    - *implementing management, 189–194*
    - *predeployment planning, 180–184*
    - *selection and classification of target hosts, 184–188*
    - *tuning, 196*
    - *understanding the product, 178–179*
  - of IPS, 204
    - *finalizing the project, 225*
    - *predeployment planning, 212–220*
    - *sensor deployment, 221–222*
    - *tuning, 222–224*
    - *understanding the product, 205–211*
- **devices**
  - failure
    - *inline sensor failure, 62*
    - *management console failure, 63–64*
  - intrinsic IPS, 80–81
- **device-to-device communication, securing, 68**
- **directory traversal attacks, 40**
- **DMZ firewall, role in layered defense, 75**
- **drive-by spamming, 14**
- **drop signature action, 46**
- **dropping**
  - all packets from source IP address, 137
  - all packets on connection, 137

# E

- **encoding mechanisms, 40**
- **encryption, role in layered defense, 78–79**
- **endpoint agents, access control process, 101**
  - access resource, identifying, 102
  - consulting the security policy, 119–124
  - determining system state, 115–116, 119
  - gathering operation data, 110–115
  - taking action, 124
- **enforcing security policies, 138**
- **EtherChannel, 63**
- **event correlation, 65–66**
- **event horizon, 36**
- **events, 109**
- **evolution of security threats, 6**
  - client-server computing, 7–9
  - Internet, 9
  - mobile computing, 10–11
  - wireless connnectivity, 10
- **examples**
  - of attacks
    - *CIH virus, 19*
    - *Loveletter virus, 19–20*
    - *Morris worm, 18*
    - *Nimda worm, 20–22*
    - *replacement login, 17*
    - *SQL Slammer worm, 21*
  - of effective defense-in-depth, 72
    - *external attack against corporate database*, 72–77
    - *internal attacks against management servers, 77–79*
- **exploits, 104**

# F

- **false negatives, 59**
- **false positives, 59**
- **finalizing CSA deployment, 198**
- **firewalls, 6**
- **flows, 164**
- **form factor as sensor selection criteria, 152–154**
- **forwarding devices, 136**
- **full CSA deployment, 197–198**
- **future of IPS, intrinsic IPS, 80–81**

# G-H

- **generating alerts, 141**
- **goals of IPS deployment**
  - defining, 213–216

- **HIDS (host-based intrusion detection systems), 25**
- **hierarchical management model, 127**
- **HIPS (host-based intrusion prevention systems), 89, 101**
  - benefits of
    - *acceptable use policy enforcement*, 95–96
    - *attack prevention*, 92

*internal attack propagation prevention*, 93
*patch relief*, 92–93
*policy enforcement*, 94–95
endpoint agents, 101
*access control process*, 101–124
limitations of, acceptable use policy enforcement, 96–97
management infrastructure, 125
*management center*, 127–129
*management interface, 129*
required capabilities, 90–92
role in layered defense, 79
security policies
*anomaly-based*, 120
*atomic-rule based*, 121
*behavioral*, 122–123

**home office IPS deployment, 250**
HIPS implementation, 251–252
limiting factors, 251
NIPS implementation, 252
security policy goals, 251

**Host IPS**
deploying, 53–55
role in layered defense, 77
signature tuning, 59–60

**host-based signatures**
atomic, 35
stateful, 36
triggering mechanisms, 39

**host-level attack mitigation, 23**
antivirus, 23–24
HIDS, 25
personal firewalls, 24

**hosts, classifying, 185–187**

**hubs, 158**

**hybrid IPS/IDS systems, 140, 145**

## I

**IDSM-2 sensors, 207**

**impact of attack, 16**

**incident response plans, 66**

**individual management method, 65**

**information theft, 12**

**inline mode sensor operation, 208**
capturing network traffic, 155, 157
sensor failure, 62

**inline on a stick, 152**

**inline prevention, 26**

**insecure management protocol, 67**

**installing**
IPS MC, 222
sensors, 221–222

**integrated IPS software, 154**

**interfaces as sensor selection criteria, 151–152**

**Internet as security threat, 9**

**Internet perimeter firewall, role in layered defense, 74**

**Internet perimeter router, role in layered defense, 73**

**intrinsic IPS, 80–81**

**IP blocking, 143–146**

**IP logging, 142**

**IP spoofing, 144**

**IPSs**
hosts, classifying, 185–187
integrated software, 154
network management options, 209–211
network traffic, capturing, 154–158
phases of deployment, 204
*finalizing the project*, 225
*predeployment planning*, 212–220
*sensor deployment*, 221–222
*tuning*, 222–224
*understanding the product*, 205–211
response methods
*alerting actions*, 166
*blocking actions*, 167
*dropping actions*, 167
*logging actions*, 167
sensors
*Cisco Catalyst 6500 series IDSM-2*, 206–207
*Cisco IDS Network Module*, 207
*Cisco IOS IPS sensors*, 208
*Cisco IPS 4200 series appliance sensors*, 206
*Cisco product availability*, 205
*large deployments*, 169
*selecting location for placement*, 216–218
*small deployments*, 168
signature updates, 212

**IPS MC (IPS Management Center), installing, 222**

# K-L

**kernel, 109**
modification, 111
modules, 108

**large enterprise IPS deployment, 229–230**
HIPS implementation, 231–233
limiting factors, 231
NIPS implementation, 233, 236
security policy goals, 231
sensor deployment, 169
**layered defense. *See also* defense-in-depth**
against corporate database attacks, 72–77
against management server attacks, 77–79
**least privilege, 124**
**lifecycle of attacks, 103**
application execution, 107
file resources, 108
memory resources, 105, 107
network resources, 104–105
persistence process, 107, 109
**limitations**
of IPS, 138–140, 145
of HIPS, acceptable use policy enforcement, 96–97
**line cards, 153–154**
**location state conditions, 116**
**log response, 61**
**log signature action, 47**
**logging**
attacker traffic, 142
traffic between attacker and victim, 143
victim traffic, 142
**Loveletter virus, 19–20**

# M

**MAC (mandatory access control), 124**
**mainframes, 7**
**malicious mobile code, 103**
**malware, 232**
**management communication**
device-to-device, securing, 68
OOB, securing, 67
securing, 66
**management console failure, 63–64**
**management infrastructure, 125**
management center, 125–129
management interface, 129
**management method, selecting, 65**
**manager-of-managers, 127**
**McAfee Entercept, 122**
**medium educational institution IPS deployment, 243**
HIPS implementation, 245–246
limiting factors, 244
NIPS implementation, 246–247
security policy goals, 245
**medium financial enterprise IPS deployment, 240**
HIPS implementation, 241–242
limiting factors, 241
NIPS implementation, 242–243
security goals, 241
**Microsoft Component Object Model, 109**
**mirroring traffic, 158**
**mitigating attacks**
at host level, 23
*antivirus*, 23–24
*HIDS*, 25
*personal firewalls*, 24
at network level, 25
*inline prevention*, 26
*promiscuous monitoring*, 25
*system log analysis*, 25
**mobile computing as security threat, 10–11**
**modems, 13**
**monitoring IPS activities, 64**
**Morris worm, 16, 18**
**Morris, Robert, 16**

# N

**NetFlow, role in layered defense, 76**
**network adapters, 94**
**network flows, 164**
**network IPS**
deploying, 55
*determining factors*, 56–58
role in layered defense, 75, 78
signature tuning, 59–60
**network taps, 159**

**network traffic**
analyzing, 114
*via anomaly operations*, 165
*via atomic operations*, 164
*via normalizing operations*, 165–166
*via protocol decode operations*, 165
*via stateful operations*, 164–165
capturing, 154
*devices for*, 158–161
*with inline mode IPS*, 155–157
*with promiscuous mode IPS*, 157–158
*with RSPAN*, 162
*with SPAN*, 162
*with VACLs*, 164
**network-based signatures**
atomic signatures, 35
stateful signatures, 37
triggering mechanisms, 39
**network-level attack mitigation, 25**
inline prevention, 26
promiscuous monitoring, 25
system log analysis, 25
**Nimda worm, 20–22**
**NIPS, selecting management architecture, 218–220**
**normalizing traffic, 138, 165–166**
**NTP (Network Time Protocol), 65**

## O

**Off mode (software bypass), 63**
**On mode (software bypass), 63**
**OOB (out-of-band) management communication, securing, 67**
**operating systems**
events, 109
kernel, 109–111
**organizational units (CSA MC), 190–191**
**OSI reference model, 26**
**OTPs (one-time passwords), 79**

## P

**parent processes, 107**
**passwords, OTPs, 79**
**pattern detection, 40–41**
**pattern matching, regular expressions, 40**
**pattern-based security policies, 122**
**PCs, zombies, 12**
**peer-to-peer networks, 9**
**permissive systems, 186**
**persistence process**
application execution, 107
file modification, 108
system configuration, 108
**personal firewalls, 24**
**phases of deployment, 177**
for CSA
*conducting pilot tests, 194–196*
*finalizing the project, 198*
*full deployment, 197–198*
*implementing management, 189–194*
*predeployment planning, 180–184*
*selection and classification of target hosts, 184–188*
*tuning, 196*
*understanding the product, 178–179*
for IPS, 204
*finalizing the project, 225*
*predeployment planning, 212–218, 220*
*sensor deployment, 221–222*
*tuning, 222–224*
*understanding the product, 205–211*
**pilot test, conducting, 194, 196**
**placing IPS sensors in network, 216–218**
**policy groups**
configuring, 191–193
secondary groups, 192–193
**port security, 78**
**PortMapper, 45**
**predeployment planning phase of IPS deployment, 212–220**
**processing capacity as sensor selection criteria, 150–151**
**promiscuous mode sensor operation, 25, 246**
capturing network traffic, 157–158
**protocol decodes, 38, 165**
**Pull model (management console), 64**
**Push model (management console), 64**

## R

**RBAC (role-based access control) matrix, 124**
**regular expressions, 40**
**regulatory compliance, 27**

**remote delivery mechanisms, 14**
**replacement login, example of, 17**
**required HIPS capabilities, 90–92**
**reset signature action, 47**
**resetting TCP connections, 143**
**responses to suspicious activity**
alerting actions, 166
blocking actions, 167
dropping actions, 167
logging actions, 167
**restrictive systems, 186**
**reviewing corporate security policies, 212**
**RFI ( Request for Information), sample questions, 261–269**
**rootkit, 109, 119**
**RPC (Remote Procedure Call), 45**
**RRs (risk ratings), 223**
**RSPAN (Remote Switch Port Analyzer), capturing network traffic, 162**
**rule modules, 190**

## S

**sample RFI questions, 261–269**
**sandbox, 113**
**scenarios for IPS deployment**
at branch offices, 236–240
at home office, 250–252
at large enterprises, 229–233, 236
at medium educational institutions, 243–247
at medium financial enterprises, 240–243
at small offices, 247–250
**secondary policy groups, configuring, 192–193**
**securing management communication, 66**
device-to-device, 68
OOB, 67
**security policies**
anomaly-based, 120
atomic rule-based, 121–122
behavioral, 122–123
pattern-based, 122
**selecting**
location for IPS sensor placement, 216–218
management method, 65
NIPS management architecture, 218–220
sensors, criteria
*form factor, 152–154*
*interfaces, 151–152*
*processing capacity, 150–151*
**sensors**
alerts, risk ratings, 223
Cisco Catalyst 6500 series IDSM-2, 206–207
Cisco IDS Network Module, 207
Cisco IOS IPS sensors, 208
Cisco IPS 4200 series appliance sensors, 206
Cisco product availability, 205
configuring, 221
inline mode
*failure of, 62*
*functionality, 208*
installing, 221–222
large deployments, 169
promiscuous mode, 246
selection criteria
*form factor*, 152–154
*interfaces*, 151–152
*processing capacity*, 150–151
small deployments, 168
**shared IPS/IDS capabilities, 145**
alert generation, 141
initiating IP blocking, 143–144
IP logging, 142
logging attacker traffic, 142
logging traffic between attacker and victim, 143
logging victim traffic, 142
resetting TCP connections, 143
**shims, 111**
**signature updates, 212**
**signatures, 33**
alerts, 45
allow signature action, 47
atomic signatures, 34–35
*host-based*, 35
*network-based*, 35
block signature action, 47
cabling, 221
characteristics of, 34
drop signature action, 46
event horizon, 36
event responses, 61
log signature action, 47

reset signature action, 47
stateful, 36
*host-based*, 36
*network-based*, 37
*with anomaly-based triggering mechanism*, 43
triggering mechanisms, 37–39
*anomaly-based detection*, 42–43
*behavior-based detection*, 44
*pattern detection*, 40–41
tuning, 59–60
**single packets, dropping, 136**
**single-server management model, 127**
**small IPS sensor deployments, 168**
**small office IPS deployment, 247**
HIPS implementation, 248–249
limiting factors, 248
NIPS implementation, 250
security policy goals, 248
**social engineering, 105**
**software bypass, 63**
**software updates, 61**
**source IP addresses**
dropping all packets from, 137
spoofing, 144
**Spacefiller, 19**
**spam, 14**
**SPAN (Switch Port Analyzer), capturing network traffic, 162**
**spyware, 248**
**SQL Slammer worm, 230**
**stack memory, 106**
**standalone appliance sensors, 153**
**stateful operation method of network traffic analysis, 164–165**
**stateful signatures, 36**
host-based, 36
network-based, 37
**summary alerts, 46**
**suspicious activity, IPS response methods**
alerting actions, 166
blocking actions, 167
dropping actions, 167
logging actions, 167
**switch ports, role in layered defense, 78**
**switches, 136**
capturing network traffic, 160
**symbolic links, 110**
**system call interception, 111–113**
**system log analysis, 25**
**system state conditions, 118–119**

# T

**TCP connections**
resetting, 143
three-way handshake, 74
**TCP Reset interface, 207**
**TCP/IP, 10**
**threats to security, evolution of, 6**
client-server computing, 7, 9
Internet, 9
mobile computing, 10–11
wireless connnectivity, 10
**three-way handshake, 74**
**tiered management model, 127**
**traffic mirroring, 158**
**traffic flows, 164**
**traffic normalization, 138**
**triggers, 37–39**
anomaly-based detection, 42–43
behavior-based detection, 44
pattern detection, 40–41
**Trojan horses, 19**
rootkits, 119
**true negatives, 60**
**true positives, 60**
**tuning phase of CSA deployment, 196**

# U

**uRPF (unicast reverse path forwarding), 73**
**user state conditions, 117**

# V

**VACLs (VLAN access control lists), capturing network traffic, 164**
**virtual operating systems, 113**
**viruses, 18**
CIH virus, characteristics of, 19
Loveletter virus, characteristics of, 19–20
**vulnerabilities, 93, 104**

W-X-Y-Z

**war-dialers, 13**

**wireless connnectivity as security threat, 10**

**wireless network adapters, 94**

**worms, 19**

Nimda, characteristics of, 20–22

SQL Slammer, characteristics of, 21

**zombies, 12**