

NUMERICS

802.1x, 14, 109

- authentication server, 110
- authenticators, 110
- EAP, 112
 - EAP FAST*, 114
 - EAP MD5*, 113
 - EAP TLS*, 113
 - LEAP*, 113
 - messages*, 110
 - PEAP*, 113
- IBNS, 111
- machine authentication, 111
- NAC, 112
- PPP connections, 110
- supplicants, 110
- VPN, 114–115

A

ACL (Access Control List) rules

- firewall rules, configuring from topology maps, 197–198
- security policies, Cisco Security Manager, 199

Action filters (Guard), 35

Add Device function (Cisco ICS), 101

Admin tab (Cisco Security MARS), 223

Administration option (NAC Appliance Manager), 159

agentless host admission process (NAC), 131–133

AIP-SSM (Advanced Inspection and Protection Security Services Module), 43–44

Analysis button (Cisco Security Manager), 191

antispoofing (ASA), 42

antivirus programs, 10

Appliance (NAC), customer preferences comparison chart, 120, 139–140

Appliance Manager (NAC appliance)

- Administration option, 159
- Device Management category
 - CCA Servers option*, 143–145
 - Clean Access section*, 147–149
 - filters*, 146

Event log, 157

homepage organization, 142

Monitoring function, 156–157

monitoring summary, 141

switch management function, 152–153

user management function, 153

- quarantine roles*, 154

- user authentication*, 155

- user roles list*, 154

Application analysis (Cisco Security Agent Management Center), 172

Application Behavior Investigation option (Cisco Security Agent Management Center), 173

Application Deployment Investigation option (Cisco Security Agent Management Center), 173

ASA (Adaptive Security Appliance), 12

antispoofing, 42

ASDM, 41

- Content Security tab*, 66

- IPS*, 43–44, 48

- threat graphs*, 66

CSC-SSM, 64–65

- antispam configurations*, 74

- configuring*, 67

- file blocking*, 72

- file transfers*, 75

- InterScan (Trend Micro)*, 68, 74

- mail*, 73–74

- phishing*, 71

- scanning*, 72–73

- URL filtering*, 72

- web/http functions*, 68

HTTP inspection engine

- attacks*, 58

- HTTP maps*, 60, 63

- HTTP/Web service inspections*, 57

- protocol inspections*, 56

- RFC compliance*, 55

- TCP inspections*, 56

- TCP maps*, 58–59

- URL length*, 55

IPS signatures

- attack signatures*, 51

- configuring*, 50

- spyware detection signatures*, 52

- subcategories*, 51

protocol inspection services, 53–54
 Randomize Sequence Number feature, 58
 Service Policy Rules, 45–46, 49, 55
 SYN Cookie feature, 12–13

ASDM (Adaptive Security Device Manager), 41

Content Security tab, 66
 IPS, 43–44

- configuring*, 44
- connecting to*, 44
- inline IPS*, 48
- inspections*, 48
- preventions*, 48
- Service Policy rules*, 45–46, 49, 55
- signatures*, 50–52

 threat graphs, 66

attack diagrams (Cisco Security MARS), 216

attack reports (Guard), generating, 38

attack signatures (IPS), 51

attack-drop.sdf files, 222

Audit admission validations (Cisco Secure ACS), 124

authentication

machine-based (802.1x), 111
 NAC Appliance Manager, 155

authentication server (802.1x), 110

authenticator (802.1x), 110

Automatic Outbreak Management Task (Cisco ICS), 99

B - C

behavior diagrams (Cisco ICS), 84

bootstrapping (Guard), 33

bump-in-the-wire, 140

Burst filters (Guard), 35

bypass filters (Traffic Anomaly Detector), 28

Catalyst Anomaly Guard service module (Guard), 32

CCA (Cisco Clean Access). See NAC (Network Admission Control) appliance

CCA Servers option (NAC Appliance Manager), 143–145

Checkup posture states, 126

Cisco ICS (Incident Control Service), 13, 79

Add Device function, 101

Device List, 100

Global Settings tab, 106

logs, 102

Event Log Query function, 104–105

Incident Log Query function, 103

Log Maintenance function, 106

Outbreak Log Query function, 104

New Outbreak Management Task list, 87, 90

OPACL, 80

automatic deployment of, 90–92

information, displaying, 87

target devices, selecting, 88

OPSig, 80

outbreak management, 80, 89–92

outbreak reports, 93–94

outbreak settings, 92

accessing, 94–95

Automatic Outbreak Management Task, 99

Exception Lists, 96

OPACL, 95

Report, 97

watch list, 98

summary page, 81

threats

behavior diagrams, 84

statistics, 86

technical details, 85

Update Settings tab, 106

Cisco Secure ACS

admission control policy comparisons, 126–127

admission validations, 123–124

Checkup posture states, 126

enforcement actions, 127

Healthy posture states, 126–129

Infected posture states, 127

network admission decisions, 127

Policy decision point, 124

policy servers, forwarding endpoint information to, 127

Quarantine posture states, 126

enforce quarantine access actions, 133

enforce redirection (optional) actions, 133

Healthy posture states, changing to, 128–129

Transition posture states, 126

Unknown posture states, 127

Cisco Security Agent, 14

- day-zero protection, 163
- features of, 163
- Management Center, 164
 - analysis, running, 172*
 - Application analysis, 172*
 - Application Behavior Investigation option, 173*
 - Application Deployment Investigation option, 173*
 - attaching rules to security policies, 169*
 - deploying device/device group kits, 166*
 - displaying device group end-station hostnames, 166*
 - Event Log, 171*
 - Event Monitor, 171*
 - generating/deploying rules, 169–170*
 - Learn mode, 173*
 - reviewing security policies, 167*
 - send polling hintcapabilities, 170*
 - Test mode, 173*
- Status area, 174–175
- System Security area, 175

Cisco Security Manager, 14, 179–180

- Cisco Security MARS linkages, 224–225
- Device View, 181
 - ACLs, 184, 187–188*
 - adding devices, 182*
 - Analysis button, 191*
 - firewalls, 188*
 - Hit Count button, 191–192*
 - interface roles, configuring, 186–187*
 - policy queries, invoking, 189*
- features, of, 180
- Map View, 193–198
- Object Manager, 202–204
- Policy View, 198
 - ACL rules, security policies, 199*
 - IPS management, 202*
 - policy inheritance, 200*
 - security policies, 201*
- value override per device, 204

Cisco Security MARS (Cisco Security Monitoring, Analysis, and Response System)

- Admin tab, 223
- CLI commands, 214
- Cisco Security Manager linkages, 224–225

- dashboard, 211
- features of, 209
- incidents, 212
 - attack diagrams, 216*
 - displaying paths of, 213*
 - hotspot graphs, 216*
 - mitigating attacks, 213*
- input/event sources, 210
- Management tab, 222
- Netflow, 219
- report groups, 219–222
- rules, 217, 219

CiscoWorks VMS. See Cisco Security Manager Clean Access section (NAC Appliance Manager), 147–149**CLI (command-line interface) commands**

- commands, Cisco Security MARS, 214
- Service Policy rules, 49

cloud networks, adding topology maps to, 195–196**content filtering (mail), CSC-SSM, 74****Content Security tab (ASDM), 66****CSC-SSM (Content Security and Control Security Service Module), 64–65**

- configuring, 67
- file blocking, 72
- file transfers, 75
- InterScan (Trend Micro), 68, 74
- mail, 73–74
- phishing, 71
- scanning, 72–73
- URL filtering, 72
- web/http functions, 68

CTA (Cisco Trust Agent), 123**D****dashboard (Cisco Security MARS), 211**

- attack diagrams, 216
- hotspot graphs, 216
- incidents, 212–213

day-zero protection (Cisco Security Agent), 163

DDoS (distributed denial-of-service) attacks, 6, 19

mitigation, 11

Guard, 21, 32

*attach reports, generating, 38**bootstrapping, 33**Catalyst Anomaly Guard service module, 32**WBM, 33**zone creation, 34**zone filters, 34–35**zone learning phases, 36**zone protect mode, 36**zone synchronization, 34**zone traffic diversion, 36*

HTTP inspection engine, 58

mitigation overview, 21

Traffic Anomaly Detector, 21

*configuring, 23**detecting anomalies, 30**diagnostic information, 30**dynamic filters, 30**policy templates, 28–29**zone creation, 24–27**zone filters, 27–28**zone learning phases, 29**zone policy construction phase, 29**zone threshold-tuning phase, 29*

types of, 19–21

device filters (NAC Appliance Manager), 146**Device List (Cisco ICS), 100****Device Management category (NAC Appliance Manager)**

CCA Servers option, 143

*NAT Gateway mode, 144**OOB deployments, 144–145**Real IP Gateway mode, 144**Virtual IP Gateway mode, 144*

Clean Access section, 147–149

filters, 146

Device View (Cisco Security Manager), 181

ACLs, 184, 187–188

adding devices, 182

Analysis button, 191

firewalls, 188

Hit Count button, 191–192

interface roles, configuring, 186–187

policy queries, invoking, 189

DoS (denial-of-service) attacks, 5**Dst Port filters (Guard), 35****DTM report groups (Cisco Security MARS), 220–222****dynamic filters (Traffic Anomaly Detector), 28–30**

E–F

EAP (Extensible Authentication Protocol), 802.1x, 112

EAP FAST, 114

EAP MD5, 113

EAP TLS, 113

LEAP, 113

messages, 110

PEAP, 113

endpoint security application, 122**enforce quarantine access actions (Quarantine posture states), 133****enforce redirection (optional) actions (Quarantine posture states), 133****enforcement actions (NAD), 127****Event log**

Cisco Security Agent, 171

NAC Appliance Manager, 157

Query function (Cisco ICS), 104–105

Event Monitor (Cisco Security Agent), 171**Exception Lists (Cisco ICS), 96****false positives, 25****files (CSC-SSM)**

blocking, 72

transfers, security, 75

filters

flex filters (Traffic Anomaly Detector), 28

Fragments filters (Guard), 35

NAC Appliance Manager, 146

firewalls, 9

ACL rules, configuring from topology maps, 197–198

Device View (Cisco Security Manager), 188

Fragments filters (Guard), 35**Framework (NAC)**

agentless host admission process, 131–133

benefits of, 120–121

components of, 121–124

customer preferences comparison chart, 120

deployment

- LAN access compliance, 135*
- remote access compliance, 135*
- rules for, 134*
- WAN access compliance, 135*

endpoint security application, 122

management systems, 124

network access devices, 123

noncompliant endpoint admission process, 124–125

- admission control policy comparisons, 126–127*
- Cisco Secure ACS decisions, 127*
- Cisco Secure ACS enforcement actions, 127*
- endpoint change from Quarantine to Healthy posture state, 128–129*
- endpoint compliance change polls, 130–131*
- endpoint network access, 126*
- NAD enforcement of actions, 128*
- NAD policy server notifications, 126*
- policy servers, forwarding endpoint information to, 127*
- posture agent actions, 128*

operational overview, 124–131

policy servers, 123–126

posture agents, 123, 128

reporting tools, 124

Revalidation configurable timers, 130–131

Status Query configurable timers, 130

web resources, 121

G–H

Global Settings tab (Cisco ICS), 106

Guard, 32

- attack reports, generating, 38
- bootstrapping, 33
- Catalyst Anomaly Guard service module, 32
- DDoS attacks, 21
- WBM, 33

zones

- creating, 34*
- filters, 34–35*
- learning phase, 36*
- protect mode, 36*
- synchronizing, 34*
- traffic diversion, 36*

Healthy posture states, 126–129

Hit Count button (Cisco Security Manager), 191–192

hotspot graphs (Cisco Security MARS), 216

HTTP insection engine, 55

- attacks, 58
- HTTP maps, 60, 63
- HTTP/Web server inspections, 57
- protocol inspections, 56
- RFC compliance, 55
- TCP inspections, 56
- TCP maps, 58–59
- URL length, 55

I–J–K

IBNS (Identity-Based Networking Services), 111

ICS (Incident Control Service). *See* Cisco ICS (Incident Control Service)

Identity admission validations (Cisco Secure ACS), 123

IDS (intrusion detection systems), 9

Incident Log Query function (Cisco ICS), 103

incidents, Cisco Security MARS, 212

- attack diagrams, 216
- displaying paths of, 213
- hotspot graphs, 216
- mitigating attacks, 213

Infected posture states, 127

inheritance policies (Cisco Security Manager), 200

inline IPS (Intrusion Prevention Service), 48

InterScan (Trend Micro)

- antispam configurations, 74
- CSC-SSM, 68–71

IPS (Intrusion Prevention Service), 12, 43

- ASDM connections to, 44
- configuring, 44

- inline IPS, 48
- inspections, 48
- Policy View (Cisco Security Manager),
 - managing via, 202
- preventions, 48
- Service Policy rules, 45–46, 49, 55
- signatures
 - attack signatures, 51*
 - configuring, 50*
 - spyware detection signatures, 52*
 - subcategories, 51*

ISR (Integrated Services Routers), 220-222

L–M

LEAP (802.1x), 113

Learn mode (Cisco Security Agent Management Center), 173

learning phase (zones)

- Guard, 36
- Traffic Anomaly Detector, 29

Log Maintenance function (Cisco ICS), 106

machine authentication (802.1x), 111

mail, security, 73-74

Management Center (Cisco Security Agent), 164

- analysis, running, 172
- Application analysis, 172
- Application Behavior Investigation option, 173
- Application Deployment Investigation option, 173
- attaching rules to security policies, 169
- deploying device/device group kits, 166
- displaying device group end-station hostnames, 166
- Event Log, 171
- Event Monitor, 171
- generating/deploying rules, 169–170
- Learn mode, 173
- reviewing security policies, 167
- send polling hintcapabilities, 170
- Test mode, 173

Management tab (Cisco Security MARS), 222

Map View (Cisco Security Manager), topology maps, 193

- adding cloud networks to, 195–196
- firewall ACL rules, 197–198
- showing devices on, 194

maximum services option (policy templates), 29

minimum threshold option (policy templates), 29

Monitoring function (NAC Appliance Manager), 156–157

N

NAC (Network Admission Control), 13, 119

- 802.1x, 112
- Appliance, customer preferences comparison chart, 120, 139-140

Appliance Manager

- Administration option, 159*
- Device Management category, 143–149*
- Event log, 157*
- homepage organization, 142*
- Monitoring function, 156–157*
- monitoring summary, 141*
- switch management function, 152–153*
- user authentication, 155*
- user management function, 153–154*

Framework

- agentless host admission process, 131–133*
- benefits of, 120–121*
- components of, 121–124*
- customer preferences comparison chart, 120*
- deployment, 134-135*
- endpoint security application, 122*
- management systems, 124*
- network access devices, 123*
- noncompliance endpoint admission process, 124–131*
- operational overview, 124–131*
- policy servers, 123–126*
- posture agents, 123, 128*
- reporting tools, 124*
- Revalidation configurable timers, 130–131*

Status Query configurable timers, 130
web resources, 121
 overview of, 119–120
NAD (Network Admission Devices)
 Cisco Secure ACS actions, enforcement of, 128
 enforcement actions, 127
NAT Gateway mode (CCA Servers option), 144
Netflow, Cisco Security MARS, 219
network access devices (NAC Framework), 123
network attacks
 attacks, 6, 11
 DoS attacks, 5
 phishing, 7
 spyware, 6
 Trojan horses, 5
 viruses, 4
 worms, 4-5
network defenses
 antivirus programs, 10
 firewalls, 9
 IDS, 9
 router ACLs, 9
 VPN, 10
New Outbreak Management Task list
 (Cisco ICS), 87, 90

O–P

Object Manager (Cisco Security Manager), 202–204
OOB (out-of-band) deployments (CCA Servers option), 144–145
OPACL (outbreak prevention access control lists), 80, 95
 automatic deployment of, 90-92
 information, displaying, 87
 target devices, selecting, 88
OPSig (outbreak prevention signatures), 80
Outbreak Log Query function (Cisco ICS), 104
outbreak management (Cisco ICS)
 behavior diagrams, 84
 New Outbreak Management Task list, 87, 90
 OPACL, 87, 90, 92
 outbreak reports, 93–94
 outbreak settings, 92-99
 overview of, 80–81

 statistics (threats), 86
 summary page, 81
 tasks, running/stopping, 89-90
 technical details (threats), 85
outbreak reports (Cisco ICS), 93-94

PEAP (802.1x), 113
phishing, 7, 71
policies
 construction phase (zones), 29
 inheritance, CS Manager, 200
 queries
 Device View (Cisco Security Manager), 189
 wildcards, 190
 templates, 28-29
Policy decision point (Cisco Secure ACS), 124
Policy servers, 123–124
 endpoint information, forwarding to (NAC), 127
 NAD notifications, 126
Policy View (Cisco Security Manager), 198
 ACL rules, security policies, 199
 IPS management, 202
 policy inheritance, 200
 security policies, 201
Posture admission validations (Cisco Secure ACS), 123
posture agents
 actions of, 128
 CTA, 123
PPP connections (802.1x), 110
protect mode (zones), Guard, 36
Protocol filters (Guard), 35
protocol inspection services, 53–54

Q–R

Quarantine posture states, 126
 enforce quarantine access actions, 133
 enforce redirection (optional) actions, 133
 Healthy posture states, changing to, 128–129
quarantine roles (NAC appliance), 154

Randomize Sequence Number feature (ASA), 58
Rate filters (Guard), 35

Real IP Gateway mode (CCA Servers option), 144
report groups, Cisco Security MARS, 219-222
Report Settings (Cisco ICS), 97
reports, generating attack reports (Guard), 38
Revalidation configurable timers (NAC), 130-131
RFC, HTTP inspection engine, 55
routers
 ACLs, 9
 ISR, 220-222
RTP (Real-Time Protocol), 46
rules, Cisco Security MARS, 217, 219

S

Secure ACS (Cisco)

admission validations, 123-124
 Policy decision point, 124

security

ASA
antispoofing, 42
ASDM, 41-44, 48
CSC-SSM, 64-68, 71-75
HTTP inspection engine, 55-60, 63
IPS, 43-44, 48-52
protocol inspection services, 53-54
Randomize Sequence Number geature, 58
Service Policy rules, 45-46, 49, 55
 Cisco ICS, 79
Add Device function, 101
behavior diagrams, 84
Device List, 100-102
Event Log Query function, 104-105
Global Settings tab, 106
Incident Log Query function, 103
Log Maintenance function, 106
New Outbreak Management Task list, 87, 90
OPACL, 80, 87, 90-92
OPSig, 80
Outbreak Log Query function, 104
outbreak management, 80
Outbreak Management tab, 92
outbreak management tasks, 89-90
outbreak reports, 93-94
outbreak settings, 92-99

statistics (threats), 86
summary page, 81
technical details (threats), 85
Update Settings tab, 106
 Cisco Security Agent
day-zero protection, 163
features of, 163
Management Center, 164-173
Status area, 174-175
System Security area, 175
 attacks, HTTP inspection engine, 58
 files
blocking, 72
transfers, CSC-SSM, 75
 mail, 73-74
 phishing, 71
 policies
ACL rules, 199
Policy View, 201
 TrendLabs (Trend Micro), role in outbreak management, 80
 URL
blocking, InterScan (Trend Micro), 70
filtering, 72
Security Manager (Cisco). See Cisco Security Manager, 179
self-defending networks, 10
 802.1x, 14
 ASA, 12-13
 CSA, 14
 Cisco Security Manager, 14
 mitigation, 11
 ICS, 13
 IPS, 12
 NAC, 13
Service Policy rules (ASA), 45-46, 49, 55
show module command (AIP-SSM), 43-44
SMTP mail, scanning, 73
Source IP filters (Guard), 35
Source Subnet filters (Guard), 35
spam (mail), 74
spyware, 6, 52
state option (policy templates), 29
Status area (Cisco Security Agent), 174-175
Status Query configurable timers (NAC), 130
subnet filters (NAC Appliance Manager), 146
summary page (Cisco ICS), 81

supplicants (802.1x), 110
switch management function (NAC Appliance Manager), 152–153
SYN Cookie feature (ASA), 12–13
System Security area (Cisco Security Agent), 175

T

TCP (transfer control protocol), HTTP inspection engine, 56-59
Test mode (Cisco Security Agent Management Center), 173
threats (security)
 behavior diagrams, 84
 Cisco ICS
 statistics, 86
 technical details, 85
 graphs, ASDM, 66
threshold-tuning phase (zones), 29
topology maps, 193
 adding cloud networks to, 195–196
 firewall ACL rules, 197–198
 showing devices on, 194
Traffic Anomaly Detector
 configuring, 23
 DDoS attacks, 21
 detecting anomalies, 30
 diagnostic information, 30
 dynamic filters, 30
 policy templates, 28–29
 zones
 creating, 24-27
 filters, 27–28
 learning phase, 29
 policy construction phase, 29
 threshold-tuning phase, 29
Transition posture states, 126
TrendLabs (Trend Micro), role in outbreak management, 80
Trojan horses, 5

U–V–W

Unknown posture states, 127
Update Settings tab (Cisco ICS), 106

URL (uniform resource locators)
 blocking, InterScan (Trend Micro), 70
 filtering, 72
 HTTP inspection engine, 55
user filters (Traffic Anomaly Detector), 27
user management function (NAC Appliance Manager), 153
 quarantine roles, 154
 user authentication, 155
 user roles list, 154

value override per device (Cisco Security Manager), 204
Virtual IP Gateway mode (CCA Servers option), 144
viruses, 4, 10
VPN (Virtual Private Networks), 10, 114-115

watch list settings (Cisco ICS), 98
wildcards, policy queries, 190
worms, 4-5

X–Y–Z

zombies, 5
zones
 Guard
 creating in, 34
 filters, 34-35
 learning phase, 36
 protect mode, 36
 synchronizing in, 34
 traffic diversion, 36
 policies
 construction phase, 29
 templates, 28–29
 threshold-tuning phase, 29
 Traffic Anomaly Detector
 creating in, 24–27
 filters, 27-28
 learning phase, 29