

# Index

## • A •

- AAA (authentication, authorization, and accounting), 14–15, 18–19, 242, 296
- acceptable use policy, 104
- access, 15, 125
- access control lists (ACLs), 64, 210, 218
- Access Control Server (ACS), 217
- Access Requestor (AR), 228–229
- access teams, 137
- ACLs (access control lists), 64, 210, 218
- acquisitions, 20, 49
- ACS (Access Control Server), 217
- action logging, 17
- Active Directory (AD)
  - about, 79
  - in authentication, 151–152
  - as network deployment service, 71
  - with RADIUS, 245
  - validation against, 148
- Active X, 71, 72
- Address Resolution Protocol (ARP), 179, 194–196
- administrative privileges/rights, 123, 131
- administrative simplicity, 32
- adoption of NAC, 125
- agent-less mode, 21–22
- agents
  - about, 69–72
  - for authentication, 147–148
  - in NAC terrain, 121
  - with SNMP, 247
  - types of, 132
- airport analogy, 10–11
- alerting mechanism, 47
- alerts with SNMP, 248
- anomalous behavior, 16–17, 47–48
- anti-malware, 20–21, 42, 134–135
- antispysware, 84, 161
- antivirus software
  - checking from within the network, 121
  - endpoint security checks, 134–135
  - network enforcement, 263, 268–269
  - policies for, 104, 116–117, 162
  - for regulatory compliance, 41–42
  - scanning for, 160
  - servers for, 20–21
  - updating, 168
  - vendor evaluation, 83–84
- Apple iPhones, 156
- applets for authentication, 25
- appliance-based solutions, 18–22, 96
- application programming interfaces (APIs), 167
- applications
  - for access control, 12
  - access requirements for, 15–16, 31
  - checks, 13
  - customization of, 276
  - endpoint integrity, 81–82
  - enforcement, 181, 270–271
  - patches, 85–86, 162–163, 168
- apportionment, 15
- AR (Access Requestor), 228–229
- architectures
  - about, 215
  - Big Three collaboration, 236–240
  - Cisco Network Admission Control (Cisco NAC), 216–220, 236–238, 293, 299
  - Internet Engineering Task Force (IETF), 235
  - Microsoft Network Access Protection (NAP), 220–227
  - Trusted Network Connect (TNC), 227–234
- ARP (Address Resolution Protocol), 179, 194–196
- assessment
  - of authentication requests, 56
  - checks, 13
  - of pilot projects, 204
  - during planning, 289
- audit mode, 140
- audits. *See also* regulatory compliance
  - best practices for, 282
  - ramifications of, 40

audits (*continued*)

- for regulatory compliance, 41, 136–137
- of traffic, 143
- trails, 177

## authentication

- applicable user group policies, 56
  - during audit mode, 140
  - checking, 10–11
  - with Cisco NAC, 216–220
  - with clientless NAC solutions, 25
  - in closed access networks, 178
  - for EAP-compliant systems, 253
  - 802.1X-compliant systems, 73, 251
  - employee reaction to, 1
  - ensuring, 125
  - as essential trait, 30
  - identity, 144–153
  - with Microsoft NAP, 220–227
  - in NAC, 120
  - with off-shoring/outsourcing, 46
  - with out-of-band NAC appliances, 20–21
  - in phased deployment, 210
  - with policy servers, 18–19
  - with RADIUS, 74, 245
  - for regulatory compliance, 135
  - security team responsibilities, 122
  - servers for, 143
  - single sign on (SSO), 69
  - with SNMP, 247
  - with SSL VPN, 78
  - with Trusted Network Connect, 227–234
  - Trusted Platform Module for, 166
  - of users/machines, 54–55, 65
  - for WLAN access, 39
- authentication, authorization, and  
    accounting (AAA), 14–15, 18–19,  
    242, 296
- authentication servers, 188, 190
- authenticators
- about, 74
  - for EAP-compliant systems, 253
  - 802.1X-compliant systems, 188–190, 251,  
    255
- authorization
- about, 43
  - during audit mode, 140
  - with Cisco NAC, 216–220
  - ensuring, 125

- with Microsoft NAP, 220–227
  - with Trusted Network Connect, 227–234
  - of users, 80, 153–154
- automated remediation
- about, 76
  - advantages of, 169
  - as requirement, 31, 38
  - types of, 168
  - for updating, 58
  - user training in, 141
- automatic allocation, 249
- availability of policy engine, 67–68

## ● B ●

## backup

- corporate policies, 108–109
  - policy engine, 67, 68
  - software, 161, 275–276
- bandwidth connections, 86
- bar code tracking, 163
- baselines, 13, 39
- best practices
- day-to-day operation, 283
  - deployment success, 207–210
  - endpoint compliance, 280
  - existing authentication, leveraging, 280
  - future expansion, 284
  - helpdesk support, 282–283
  - ISO/IEC 27002 as, 116
  - logging, reporting, auditing, 282
  - maintenance and upgrades, 283–284
  - management, 281–282
  - planning, 279–280
  - policy enforcement, 281
- big wigs as allies, 110–111
- biometric identification, 54, 135
- BitTorrent, 84
- Bootstrap Protocol (BOOTP), 249
- Bradford Networks NAC, 294
- branch survivability, 67
- breaches of security, 1
- browser history, clearing, 89
- budgets
- elements of, 32
  - existing components, leveraging, 33
  - NAC delivery in phases, 130
  - options for, 29

- savings, 110–111
    - with standards, 242
    - for WLANs, 38
  - business continuity, 97
  - business partners, 99
- C ●
- cache cleaning, 81, 88–89
  - captive portals, 21–22, 71–72, 146
  - certificate revocation lists (CRLs), 79
  - certificates
    - in authentication, 14, 152
    - collecting, 68
    - for credentials collecting, 148
    - endpoint integrity with, 87–88
    - as identification, 164–165
  - checks as essential trait, 30
  - choke points, 20
  - Cisco Access Control Server (Cisco ACS), 217–218
  - Cisco Network Admission Control (Cisco NAC), 216–220, 236–238, 293, 299
  - Cisco Trust Agent (CTA), 217
  - clean machines, 55
  - CLI (command line interface), 191–192
  - client-based NAC solutions, 23–25
  - client-based SSL VPN access, 91–93
  - clientless access, 71–72
  - clientless mode, 21–22
  - clientless NAC solutions, 25
  - clientless SSL VPNs, 90–91
  - clients
    - about, 68–72
    - in NAC, 121
    - types of, 132
  - closed access networks, 177–178, 185
  - colleague coercion, 111
  - collect posture, 68
  - command line interface (CLI), 191–192
  - compliance. *See* regulatory compliance
  - components
    - about, 63
    - clients, 68–72
    - enforcement, 72–76
    - policies, 63–68
    - remediation, 76
  - conference rooms, deployment in, 208
  - configuration
    - static, 177
    - of switches, 186–187
    - of VLANs, 188
  - consensus building, 129, 138
  - consulting, 210–211
  - consumerization of IT, 274
  - contamination, 24
  - continuity, 48, 97
  - contractors
    - quarantine scenarios, 170–172
    - usability testing involvement, 142
  - controls, policy, 64–65
  - cookies, clearing, 89
  - coordination of SSL VPN/NAC, 95–96
  - corporate security policies
    - about, 103
    - enforcement, 108–114
    - planning, 286
    - plans from, 52–53
    - resources, 116
    - types of, 103–107
    - updating, 114–116
    - writing, 116–118
  - corporate security standards, 37
  - corporate switching infrastructure, 59
  - costs
    - elements of, 32
    - NAC delivery in phases, 130
    - options for, 29
    - savings opportunities, 33, 110–111
    - with standards, 242
    - for WLANs, 38
  - credentials
    - collecting, 145–147
    - with RADIUS, 245
    - transporting, 149
  - CRLs (certificate revocation lists), 79
  - cross-functional teams, 286
  - cross-platform approaches, 92, 146
  - cross-pollination, 138
  - cryptographic processors, 166
  - CTA (Cisco Trust Agent), 217
  - customers, 44, 99
  - customization
    - of applications, 276
    - of endpoint integrity checks, 31
    - of policies, 13, 88

customization (*continued*)  
 scanning, 166–167  
 of security checks, 13

## • D •

### data

access to, 16  
 backup policy, 104–105  
 control of, 12, 31  
 logging, 179  
 protection in transit, 41  
 role-based access, 43  
 survivability of, 67  
 data leakage prevention (DLP), 272–273  
 data link layer (Layer 2), 26–27  
 data-nappers, 37, 131  
 day-to-day operations, best practices, 283  
 decision making mode, 179–180  
 deployment  
   during audit mode, 141  
   blended authentication solutions, 148  
   of client/host-based NAC solutions, 25  
   flexibility, 32  
   helpdesk role, 139  
   of inline NAC appliances, 20  
   Internet, 90  
   of out-of-band NAC appliances, 20, 22  
   in phases, 129–130  
   of pilot projects, 204  
   in public areas, 208  
   time/cost savings, 15  
   types of, 25–26  
   of upgrades, 128–129  
 deployment success  
   about, 197  
   best practices for, 207–210  
   pre-enforcement evaluation, 205–207  
   professional services/consulting, 210–211  
   steps for, 198–205  
 desktop management, 130–133  
 desktop virtualization solutions, 274–275  
 destination IP, 181, 183  
 destination port, 181, 183  
 devices  
   administrative rights, 123  
   authentication of, 10–11

classification of, 263–265  
 compliance, 41  
 control over, 1  
 identity, 16, 30–31  
 management of, 19  
 updating, 13  
 DHCP. *See* Dynamic Host Configuration Protocol (DHCP)  
 dialog boxes for credentials, 147  
 differentiated access for different users, 14, 39, 46, 154, 182  
 differentiating managed/unmanaged machines, 163–164  
 digital certificates, 79  
 disaster recovery, 20  
 disk encryption, 161–162, 166, 272  
 disruptions, limiting, 22  
 dissolvable agents/clients, 72, 121  
 distributed enforcement architecture, 96  
 DLP (data leakage prevention), 272  
 domain name systems (DNSs), 249  
 draft IETF specifications, 235  
 driver installation, 92  
 dynamic access control, 94  
 dynamic allocation, 249  
 dynamic changes, 30–31  
 Dynamic Host Configuration Protocol (DHCP)  
   about, 248–250  
   enforcement with, 192–193, 224, 227  
   as industry standard, 244  
   with IP addresses, 75  
 dynamic VLANs, 187

## • E •

EAP (Extensible Authentication Protocol), 69, 73, 151, 217, 252  
 EAP Quarantine EC, 224  
 EAP over RADIUS, 150, 220  
 EAPoL (Extensible Authentication Protocol over LAN), 150, 189  
 EAP-Protected Extensible Authentication Protocol (EAP-PEAP), 252  
 EAP-Tunneled Transport Layer Security (EAP-TTLS), 252  
 ease of operation, 32

- ECs (enforcement clients), 221–222
  - 802.1Q, 188
  - 802.1X standard
    - about, 244, 251–252, 254–255, 295
    - authentication servers in, 190
    - Cisco NAC with, 216–220
    - compatibility with, 33
    - in corporate switching infrastructure, 59
    - for credentials collecting, 149–150
    - in deployment, 64
    - EAP with, 151
    - encryption levels with, 39, 42, 136
    - enforcement with, 26, 73–75, 179, 224, 227
    - NAP with, 221, 223
    - for port-based control, 22, 188–190
    - RADIUS with, 245
    - for scalability, 96
    - supplicant functionality, 69
    - switch port controls, 185
    - usage, 74
  - e-mail use policy, 105
  - emergencies, 48
  - employee quarantine scenarios, 170
  - encapsulation only mode, 194
  - encryption
    - for data transit, 41–42
    - disk, 161, 166, 272
    - with IPsec, 193–194
    - IPsec VPN with, 76
    - policies for, 162
    - for regulatory compliance, 135–136
    - with SNMP, 247
    - vendor evaluation, 84
  - endpoint clients, 68
  - endpoint devices
    - cordoning off, 122
    - identity of, 144
    - regulatory compliance, 134, 280
  - endpoint enforcement, 59, 73, 180–182
  - endpoint integrity
    - about, 296–297
    - applications, 159–162
    - assessment of, 11, 13, 31
    - checks, 121
    - as essential trait, 30
    - with integration, 242
    - with NAC, 64, 271–276
    - scanning for, 271
    - with SSL VPN, 80–90
    - verification, 166
  - endpoint posture, 65
  - enforcement. *See also* policy enforcement
    - corporate security policies, 108–114
    - Layer 3, 69
    - methods, 72–76, 223
    - mode, 176–178
    - NAC extensions, 265–271
    - support for, 69
  - enforcement clients (ECs), 221–222
  - enforcement points
    - hardware for, 16
    - policies, 15, 58–59
    - port disabling, 17
    - pre-admission, 144–145
  - enforcement servers (ESs), 223
  - environmental factors in access
    - determination, 55
  - ethernet switches, 26
  - evaluate only mode, 175–176, 207
  - evaluation
    - of authentication request, 56
    - before enforcement, 205–207
  - event-driven monitoring, 60–61, 172
  - executive summary, 201–203
  - ex-employees, 1
  - existing network components
    - authentication, 280
    - leveraging, 33–34, 153, 234
    - NAC compatibility with, 31
  - expulsion
    - device, 17
    - network, 11–12
  - extensibility of Trusted Network Connect, 229, 233–234
  - Extensible Authentication Protocol (EAP), 69, 73, 151, 217, 252
  - Extensible Authentication Protocol over LAN (EAPoL), 150, 189
  - extranet policy, 105
- F ●**
- failure points, 20
  - file checks, 13
  - firewalls
    - for dynamic policy enforcement, 183–184
    - enabling, 160–161, 168

firewalls (*continued*)  
 enforcement with, 73, 179, 266–267  
 evaluation of, 177  
 functionality, 179  
 as inline enforcement, 75  
 interaction with, 16  
 with out-of-band NAC appliances, 20–21  
 policies for, 162  
 for segmentation, 46  
 vendor evaluation, 84  
 first responders, 124  
 five-tuple concept, 181, 183  
 fixed telecommuters, 99  
 forbidden Web content, 269  
 Forrester NAC Wave, 293  
 full agents, 70–71  
 full production, 288–289  
 functionality in phased deployment, 210  
 future expansion, 284

## • G •

Gartner NAC Marketscope, 292  
 gateways, 249  
 GINA (Graphical Identification and Authentication), 69  
 goals of test plans, 203  
 Google Android, 156  
 government regulatory requirements, 133–137  
 GPOs (Group Policy Objects), 69  
 granular access control  
 with inline NAC appliances, 19  
 intrusion detection systems, 267  
 port forwarding with, 93  
 with rewriters, 91  
 with SSL VPNs, 99  
 teams, 137  
 within your internal groups, 210  
 Graphical Identification and Authentication (GINA), 69  
 Group Policy Objects (GPOs), 69  
 group standards, 244  
 guest users  
 about, 43–45  
 access for, 15

with client/host-based solutions, 24–25  
 credentials of, 151  
 in phased deployment, 210  
 quarantine scenarios, 170–171  
 in testing solutions, 142  
 guest VLANs, 188, 191

## • H •

hackers, 37, 44  
 hands-on remediation, 38  
 hardware appliances, 185, 218  
 hardware-based authentication, 14  
 Health Insurance Portability and Accountability Act (HIPAA), 40, 116, 143, 266  
 helpdesk  
 calls during phased deployment, 130  
 implementation role of, 139–140  
 in proof-of-concept testing, 198  
 support for, 282–283  
 HIPAA (Health Insurance Portability and Accountability Act), 40, 116, 143, 266  
 home PCs, 81, 94–95, 99  
 host-based solutions, 23–25, 179–181  
 hosted virtual desktop environments, 275  
 hotfixes, 41–42

## • I •

IAS (Internet Authentication Server), 224–225  
 icons used in this book, 4–5  
 identity  
 authentication of, 14–15, 144–153  
 internal stores, 143  
 for regulatory compliance, 135  
 identity-aware firewalling, 266  
 identity-enabling application access, 16  
 IDP (intrusion detection and prevention), 260–261  
 IDSs (intrusion detection systems), 11–12, 47–48, 267–268  
 IEC (International Electromechanical Commission), 116

- IEEE standards, 251–255. *See also* 802.1X standard; *specific standards*
- IETF (Internet Engineering Task Force), 235, 244–251, 292
- IETF Request for Comment (RFC) 3580, 190
- IF-MAP (Interface for Metadata Access Point), 233–234
- IMCs (integrity measurement collectors), 230
- implementation
  - by network security teams, 125
  - pilot projects, 199–201
  - planning for, 285–289
- IMVs (integrity measurement verifiers), 231–232
- in sync (corporate security policies), 115–116
- industry regulatory requirements, 133–137
- industry standards. *See* standards
- infections, 167–172
- information transfer among
  - components, 26
- infrastructure-based solutions, 96
- inline enforcement, 65, 75–76, 179
- inline NAC appliances, 19–20, 59, 96, 182–185
- insider threats
  - about, 42, 47–48
  - encryption for, 136
  - with user monitoring, 16, 17
- installer services, 92, 127
- integrated NAC features
  - capabilities, 22
  - deployment, 26
  - solutions, 138, 242
- integrity measurement collectors (IMCs), 230
- integrity measurement verifiers (IMVs), 231–232
- interaction of pilot team, 203–204
- Interface for Metadata Access Point (IF-MAP), 233
- interfaces, open, 231
- International Electrotechnical Commission (IEC), 116
- International Standards Organization (ISO), 116
- Internet Authentication Server (IAS), 224–225
- Internet directories, clearing, 89
- Internet Engineering Task Force (IETF), 235, 244–251, 292
- Internet Protocol addresses. *See* IP addresses
- Internet Protocol Security (IPSec)
  - about, 244, 250–251
  - for business-critical applications traffic, 193–194
  - encryption with, 42, 136
  - enforcement, 22–23, 76, 179, 223, 227
- interoperability
  - with existing network components, 31–32
  - of network architecture firms, 236, 238–240
  - of standards, 241–242
  - with third-party applications, 222
- intrusion detection and prevention (IDP), 260–261
- intrusion detection systems (IDSs), 11–12, 47–48, 267–268
- intrusion prevention systems (IPSs), 11–12, 31–32, 47–48, 260–261, 267–268
- inventory
  - of devices, 263–265
  - of users/machines, 53–55
- IP addresses
  - assigning, 192
  - checks, 13
  - delivery of, 249–250
  - as Layer 3, 194
  - tracking, 31
  - of users, 184
- IP information, 249
- IPSec. *See* Internet Protocol Security (IPSec)
- IPSs (intrusion prevention systems), 11–12, 31–32, 47–48, 260–261, 267–268
- IPv4 address configuration, 224
- ISO (International Standards Organization), 116
- ISO/IEC 27002, 116

## • J •

Java, 71–72

Juniper Networks Unified Access Control (UAC), 3, 293, 298–299

## • K •

Kerberos tickets, 148, 152

kiosks, 81, 99

## • L •

lab testing, 129, 139

LANs (local area networks). *See* local area networks (LANs)

laptop data backup, 104–105

Layers 2/3, 26–28, 91–93, 194

LDAP (lightweight directory access protocol), 78–79, 152, 245

leveraging

access policies, 15

authentication, 280

existing network components, 31, 33–34, 280

standards, 244

lifecycle

assessment assembly, 56

enforcement points, 58–59

inventory, 53–55

monitoring, 59–61

of NAC products, 127

policies, 51–53

remediation, 57–58

lightweight agents, 71

lightweight directory access protocol (LDAP), 78–79, 152, 245

limited production, 288

Linux operating systems

policies for, 84, 161

security concerns with, 156, 158

software appliances on, 184

load balancing devices, 20

lobbies, deployment in, 208

local area networks (LANs)

configuration data for, 249

with inline NAC appliances, 96

teams, 137

virtual local area networks (VLANs), 46, 64, 186–188

wired/wireless, 38–39

wireless local area networks (WLANs), 2, 38, 97

local authentication, 78

location

in phased deployment, 207–208

of policy engine, 66–67

logging

for audits, 179

best practices for, 282

capabilities, 206

for compliance, 43

malicious traffic, 261–262

login, 10–11, 145

lying endpoint, 24, 166, 234

## • M •

MAC (Media Access Control) addresses, 13, 87, 164, 190–191, 194

machines

certificate checks, 13

identity, 54–55, 86–87, 163–164

remediation, 57

Macintosh operating systems, 84, 156, 158, 161

maintenance best practices, 283–284

malevolent users, 123–124

malware

about, 36–37

anti-malware applications, 20–21, 42, 134–135

checks for, 11, 121

downtime from malware, 186

lying endpoint, 24

managed devices

about, 45

insiders with, 47

laptops, 94, 98, 127

PCs, 81

switches, 187

management

best practices for, 281–282

buy-in, 110

simplicity, 32

- manual remediation
    - about, 76, 168–169
    - as backup, 58
    - as fall-back, 169
    - forced, 17
    - user training in, 141
  - Media Access Control (MAC) addresses, 13, 87, 164, 190–191, 194
  - mergers, 20, 49
  - Metadata Access Point (MAP), 233
  - methods, 249
  - metrics (budget), 110–111
  - Microsoft Active Directory. *See* Active Directory (AD)
  - Microsoft Network Access Protection (NAP), 220–227, 236–240, 299
  - Microsoft patches, 85, 163
  - Microsoft Vista, 236
  - milestones, 204–205
  - mobile devices
    - about, 98–99
    - backup, 104–105
    - network security and, 38
    - platform options, 84, 156, 161
    - usage policies, 105–106, 116–118
    - users, 98–99
  - monitoring
    - for compliance, 59–61
    - continuous, 66
    - event-driven, 172
  - multiple authentication servers, 152
  - multiple NAC solutions, 138
  - multiple-factor authentication, 79
  - multiple-owner devices, 120
  - must-have traits of NAC solutions, 30–32
- **N** •
- NAA (Network Access Authority), 231
  - NAC (network access control)
    - about, 9
    - appliances, 184–185
    - description of, 10–17
    - extensions
      - endpoint, 271–276
      - enforcement, 265–271
      - network data collection, 259–265
    - reasons for deploying
      - about, 35–37
      - compliance, 40–43
      - guest users, 43–45
      - insider threats, 47–48
      - keeping business running, 48–49
      - malware, 37–38
      - off-shoring/outsourcing, 45–46
      - wireless networks, 38–39
    - solution choices, 28–32, 127–128
    - types of, 18–28
  - NADs (Network Access Devices), 217–218
  - NAP (Network Access Protection), 293, 299
  - native authentication data stores, 18–19
  - natural disasters, 48, 97
  - NBA (network behavior analysis), 16
  - NBAD (network behavior anomaly detection), 16, 47
  - NEA WG (Network Endpoint Assessment Working Group), 235, 244, 257, 292
  - Nessus, 165
  - Network Access Authority (NAA), 231
  - network access control. *See* NAC (network access control)
  - Network Access Devices (NADs), 217–218
  - Network Access Protection (NAP), 293, 299
  - Network Admission Control (Cisco NAC), 216–220, 236–238, 293, 299
  - network behavior analysis (NBA), 16
  - network behavior anomaly detection (NBAD), 16, 47
  - Network Endpoint Assessment Working Group (NEA WG), 235, 244, 257, 292
  - network layer (Layer 3), 26–28, 65, 69, 72
  - Network Management System (NMS), 247
  - Network Policy Server (NPS), 224–225
  - Network World*, 291
  - networking team, 126–130
  - networks
    - access control policies, 106
    - administrative rights, 123, 198
    - antivirus enforcement, 263, 268–269
    - architects/designers, 198
    - attacks against, 127–128
    - changes to, 22
    - data collection, 259–265

networks (*continued*)

- diagrams, 179
- endpoint enforcement, 73
- equipment-based NAC solutions, 22–23
- infrastructure, 122, 126
- inventory, 263–265
- policies, 64, 181, 242
- security teams, 122–126
- sniffing, 194
- switches, 185–192

new-hire training, 112

NMAP, 165

NMS (Network Management System), 247

non-persistent agents, 147

non-Windows operating systems, 84

NPS (Network Policy Server), 224–225

NTLM authentication protocol, 152



OCSP (Online Certificate Status Protocol), 79

off-shoring, 45–46

one-time passwords (OTPs), 79

Online Certificate Status Protocol (OCSP), 79

online information sources

- Bradford Networks NAC, 294
- Cisco NAC, 293
- Forrester NAC Wave, 293
- Gartner NAC Marketscope, 292
- Internet Engineering Task Force (IETF), 292
- Juniper Networks UAC, 293
- Network Access Protection (NAP), 293
- Network Endpoint Assessment Working Group (NEA WG), 292
- Network World*, 291
- Symantec NAC, 294
- Trusted Computing Group, 291–292

open access network, 176–177

open interfaces, 231

open standards, 68, 167, 227, 241, 255–257

Open Systems Interconnection (OSI) Basic Reference Model, 26

operating modes, 175–180

operating systems

- checks, 13
- patches, 85–86, 162–163, 168
- security concerns with, 158
- vendor evaluation, 82–83
- verifying, 159

optimization of enforcement, 190

organizational linking, 243

OSI (Open Systems Interconnection) Basic Reference Model, 26

OTPs (one-time passwords), 79

out-of-band NAC appliances, 20–22, 26

outsourcing, 45–46

overlay NAC deployment, 26



pairing of NAC solutions, 22

partners, 44, 99

passwords

- authentication of, 10–11, 14, 152
- collecting, 68
- policies, 106–107, 109
- for regulatory compliance, 135

Patch Tuesday, 85, 163

patches

- checking for, 42
- device adherence, 41
- managing, 275
- Microsoft, 85, 163
- operating systems, 85–86
- opportunities for, 54
- policies for, 162
- as remediation, 168

Payment Card Industry (PCI), 143

Payment Card Industry Data Security Standards (PCI DSS), 40, 116

PC security

- about, 155–156
- infections, 167–172
- PC choices, 156–158
- scans, 172–173
- trustworthy choices, 159–167

PCI (Payment Card Industry), 143

PCI DSS (Payment Card Industry Data Security Standards), 40, 116

- PDP (Policy Decision Point), 228–229, 234, 297
- peer-to-peer applications, 84, 161–162
- penalties for non-compliance, 41
- PEP (Policy Enforcement Point), 228–229, 234, 297–298
- peripheral protection, 273–274
- persistence after signout, 72
- persistent agents, 147
- phased deployment, 32, 129–130, 207–208.  
*See also* deployment success
- physical security policy, 107
- pilot projects
  - helpdesk role, 139
  - implementation, 199–201, 287
  - pre-deployment testing, 129, 201–205
- PKI (private key infrastructure), 88, 165
- planning
  - assessment/evaluation, 289
  - best practices for, 279
  - corporate security policy, 286
  - cross-functional teams, 286
  - limited/full production, 288–289
  - pilot implementation, 287
  - proof-of-concept testing, 287
  - understanding NAC, 285–286
  - vendor info and RFPs, 287
- platforms
  - cross-platform approaches, 92, 146
  - for mobile devices, 84, 156, 161
  - platform-dependant credentialing, 148
  - security concerns, 156, 158
- point person from each team, 138
- policies. *See also* corporate security policies
  - about, 13
  - changes, 30–31
  - components, 63–68
  - consistency, 96, 123
  - firewalls and, 266
  - lifecycle, 51–53
  - for operating systems, 161
  - regulatory compliance, 134
  - reuse, 33
  - role-based, 267
  - for threat mitigation, 16
  - updating, 20–21
  - user groups, 56
  - of vendors, 82–84
- Policy Decision Point (PDP), 228–229, 234, 297
- policy enforcement
  - about, 175
  - alternatives, 192–196
  - best practices for, 281
  - endpoint/software, 180–182
  - inline NAC appliances, 182–185
  - network switch infrastructure, 185–192
  - operating modes, 175–180
- Policy Enforcement Point (PEP), 228–229, 234, 297–298
- policy engines, 125, 150–153
- policy management, 19
- policy servers, 18–19
- pornographic material, 269
- port-based network access control, 22, 26, 33
- ports
  - client application forwarding, 91, 93
  - configuration of, 188
  - disabling, 17
  - segmentation of, 186
  - usage of, 13
- post-admission host/client checks, 14
- post-authentication scans, 173
- posture plug-ins, 217
- pre-admission host/client checks, 14
- pre-enforcement evaluation, 205–207
- pre-testing, 129
- privacy, 76
- private key infrastructure (PKI), 88, 165
- problem documentation, 200
- process checks, 13
- productivity with NAC systems, 179
- product/version, 13
- professional services, 210–211
- prompts, authentication, 54
- proof of compliance, 41
- proof-of-concept testing, 198–200, 287
- proprietary methods, 151
- proprietary standards, 241

protected workspaces, 89–90  
 protection, 10, 159–160  
 protocols, 181, 249

## • Q •

quarantine  
 for anomalous behavior, 17  
 challenges, 2  
 of devices, 12  
 with integration, 242  
 IP addresses, 193  
 as necessary option, 31  
 network, 37–38  
 for non-compliance, 135, 167  
 options, 169–172  
 user training, 141  
 VLANs in, 74

## • R •

RADIUS servers  
 about, 243, 245–246  
 authentication, 74, 79, 152  
 Cisco ACS as, 217  
 802.1X-compliant systems, 64, 188, 190  
 enforcement, 18–19  
 MAC address authentication with, 190  
 random assessment checks, 11  
 ransom for data, 37, 131  
 RDP (Remote Desktop Protocol), 275  
 real-time monitoring/protection, 13, 160  
 reasonable policies, 108–109  
 redundancy  
 endpoint enforcement, 180  
 inline NAC appliances, 20  
 policy engine, 67–68  
 registry checks, 13  
 registry setting identification, 86, 164  
 regulatory compliance  
 about, 133–137  
 data logging, 179  
 device adherence, 43  
 enforcement options, 65  
 evaluate only mode, 175  
 identity policies, 31  
 with NAC, 40–43, 143

network security team responsibility  
 for, 125  
 remediation and, 57–58  
 remediation  
 anomalous behavior, 17  
 during audit mode, 140  
 compliance and, 57–58  
 integrating, 242, 275  
 as necessary option, 31  
 for non-compliance, 135, 167  
 types of, 38, 76, 168–169  
 user training in, 141  
 remote access. *See also* SSL VPN  
 about, 49  
 with inline NAC appliances, 96  
 policies, 107  
 scanning, 165  
 teams, 137  
 users, 141  
 Remote Access Quarantine EC, 224  
 Remote Authentication Dial-In User  
 Service. *See* RADIUS servers  
 Remote Desktop Protocol (RDP), 275  
 reporting  
 best practices for, 282  
 capabilities/requirements, 206  
 templates, 34  
 tools, 43, 207  
 Requests for Comments (RFCs), 69, 73,  
 190, 244  
 Requests for Proposals (RFPs), 201, 287  
 resources. *See also* online information  
 sources  
 for corporate security policies, 116  
 protection of, 143  
 reuse policies, 33  
 reviewing threat landscapes, 124  
 rewriters, 91  
 RFCs (Requests for Comments), 69, 73,  
 190, 244  
 RFPs (Requests for Proposals), 201, 287  
 RIM BlackBerry, 156  
 risk mitigation, 178  
 role mapping, 154  
 role playing, 208–209  
 role-based policies, 43, 267  
 routers, 16  
 rules, evaluation of, 175

## • S •

- SAML (Security Assertion Markup Language), 80
- sample pilot test plan, 201–205
- sandboxes, 81, 89, 274–275
- SANS Institute, 116
- Sarbanes-Oxley (SOX), 40, 116, 143, 266
- saved credentials, 147
- scalability, 20, 22, 96
- scanning
  - about, 121–122, 172–173
  - customization, 166–167
  - functionality, 159
  - post-authentication, 173
  - remote, 165
  - time-based, 172
  - verification of, 160
- schedule of pilot projects, 204
- secret files as identification, 87, 164
- Secure Sockets Layer (SSL), 150–151
- Secure Sockets Layer virtual private network. *See* SSL VPN
- security
  - in closed access networks, 178
  - configuration change, 107
  - events staging, 124
  - extensions, 31–32
  - limitations, 25
  - of machines, 55
  - updating, 13, 20–21
- Security Assertion Markup Language (SAML), 80
- security event management (SEM), 234
- security information and event management (SIEM), 31–32, 47, 136, 234, 261–262
- security state data
  - with Cisco NAC, 216–220
  - with Microsoft Network Access Protection (NAP), 220–227
  - with Trusted Network Connect (TNC), 227–234
- segmentation
  - data, 43
  - by function, 266
  - of information, 46
  - network, 15, 31, 39, 41, 47, 135
  - of ports/switches, 186
  - self-remediation
    - about, 76, 168–169
    - as fall-back, 169
    - as requirement, 31, 38
    - user training in, 141
- SEM (security event management), 234
- server-based enforcement, 182
- service packs, 159
- severity classifications, patches, 86, 163
- SHAs (System Health Agents), 221–222
- shopping for NAC solutions, 28–32
- SHVs (System Health Validators), 222
- SIEM (security information and event management), 31–32, 47, 136, 234, 261–262
- signatures, 16, 41–42, 160
- Simple Network Management Protocol (SNMP)
  - about, 243, 246–248
  - enforcement, 179
  - switch control, 185, 191–192
- simultaneous network access, 20
- single point of failure, 20
- Single Sign-On (SSO), 80, 148, 182
- smart cards, 10–11, 148
- SMS (Systems Management Server), 69, 71, 221
- SNMP. *See* Simple Network Management Protocol (SNMP)
- software appliances, 184–185
- software enforcement, 73, 180–182
- SoH (Statement of Health), 237–240, 298
- Solaris, 156
- source IP, 181, 183
- source port, 181, 183
- SOX (Sarbanes-Oxley), 40, 116, 143, 266
- spoofing attacks, 194
- SQL (Structured Query Language), 245
- SSL (Secure Sockets Layer), 150–151
- SSL VPN
  - about, 77–78
  - endpoint security with, 80–90
  - NAC with, 95–97
  - remote access policy enforcement, 90–95
  - use cases, 97–99
  - user identity with, 78–80
- SSO (Single Sign-On), 80, 148, 182
- stakeholders in pilot test plan, 202

- standards. *See also* 802.1X standard;
    - technology standards
    - checks, 13
    - corporate security, 37, 116
    - draft IETF specifications, 235
    - enforcement, 22–23
    - industry, 13, 33, 243–244
    - open, 68, 167, 227, 241, 255–257
    - proprietary, 241
  - state change in device security, 11
  - Statement of Health (SoH), 237–240, 298
  - static configuration, 177
  - static VLANs, 187
  - storage devices, 1
  - stringency of security policy, 158
  - Structured Query Language (SQL), 245
  - supplicant functionality, 69
  - supplicants
    - about, 74
    - for EAP-compliant systems, 253
    - 802.1X-compliant systems, 188–189, 251, 255
  - switch-based NAC solutions, 22–23
  - switch-dependent features, 190–191
  - switches
    - ethernet, 26–27
    - with out-of-band NAC appliances, 20–21
    - segmentation of, 186
  - switching infrastructure, 59
  - Symantec NAC, 294
  - Symbian phones, 156
  - System Health Agents (SHAs), 221–222
  - System Health Validators (SHVs), 222
  - Systems Management Server (SMS), 69, 71, 221
- T •
- tailgating, 107
  - TCG (Trusted Computing Group), 14, 166, 244, 255–257, 291–292
  - TCP/IP (Transmission Control Protocol/Internet Protocol), 248–249
  - team building, 138
  - team interaction, 203–204
  - technological territory
    - about, 119
    - compliance, 133–137
    - desktop management, 130–133
    - helpdesk, 139–140
    - network security team, 122–126
    - networking team, 126–130
    - other members, 137–138
    - terrain analysis, 119–122
    - users, 140–142
  - technologies for policy enforcement, 179
  - technology standards
    - about, 241
    - IEEE standards, 251–255
    - IETF standards, 245–251
    - open standards, 255–257
    - role of, 242–244
  - telecommunications teams, 137
  - telecommuters, 50, 99, 141
  - test plan document, 201–205
  - testing of NAC solutions
    - contractors in, 142
    - helpdesk role, 139
    - remote users in, 141
  - theft of sensitive data, 44
  - third party products/services
    - audits, 41
    - organizations, 137
    - plug-ins, 217
    - providers, 127, 218–219
    - security applications, 81, 159
    - servers, 152, 217, 225
    - verification, 167
  - threats
    - evolution of, 15
    - insider, 17
    - mitigation policies for, 16
    - network security reviews, 124
  - time-based monitoring, 60
  - time-based scans, 172
  - TNC (Trusted Network Connect), 227–234, 238–240, 298
  - TNC client (TNCC), 231–232

- TNC Server (TNCS), 231–232
  - tokens
    - authentication of, 10–11, 14
    - for regulatory compliance, 135
  - TPM (Trusted Platform Module), 14, 166, 234
  - tracking usage, 16
  - traffic
    - audits, 143
    - increases, 20
    - malicious, 260–261
    - monitoring, 25
    - on software appliances, 184–185
  - training
    - of helpdesk staff, 139
    - of pilot participants, 200
    - on policies, 111–112
    - of users, 141
  - transition to NAC solutions, 142
  - Transmission Control Protocol/Internet Protocol (TCP/IP), 248–249
  - traps on SNMP-enabled network switches, 248
  - Trojan Horses, 36–37
  - Trusted Computing Group (TCG), 14, 166, 244, 255–257, 291–292
  - Trusted Network Connect (TNC), 227–234, 238–240, 298
  - Trusted Platform Module (TPM), 14, 166, 234
  - trustworthy PC choices, 159–167
  - two-factor authentication, 10–11, 14, 40, 68, 135, 152–153
- **U** •
- unauthenticated VLANs, 191
  - Unified Access Control (UAC), 3, 293, 298–299
  - unified threat management (UTM)-enabled firewalls, 11–12
  - unique codes for authentication, 152
  - Unix, 156
  - unmanaged devices, 24–25, 43, 45, 120, 186
  - unmanned machines, 54
  - untagged ports, 188
  - updating
    - antivirus software, 168
    - best practices for, 282
    - corporate security policies, 114–116
    - of equipment, 205
    - managed laptops, 98
    - of NAC solutions, 129
    - non-compliant equipment, 225
    - policies, 53, 123
    - software/machines, 58
    - SSL VPN, 92
  - urgency levels, 209
  - URL/Web-filtering enforcement, 269
  - use cases, 97–99
  - user groups policies, 56
  - user identity
    - about, 54–55, 143–144
    - authentication, 10–11, 14, 65, 68, 144–153, 210
    - authorization, 80, 153–154
    - certificates, 165
    - credentials, 68
    - defining, 143
    - monitoring, 16
    - in NAC policy, 64
    - policies based on, 30–31
    - for regulatory compliance, 135
    - with SSL VPN, 78–80
  - user roles
    - access determined by, 15, 31, 43–46
    - anomalous behavior with, 17
  - user-driven remediation, 31, 38
  - users
    - audit trails, 177
    - productivity, 179
    - in proof-of-concept testing, 198
    - quarantine scenarios, 170–172
    - in regulatory compliance, 134
    - seamless connections, 145–146
    - technological territory, 140–142
  - UTM (unified threat management)-enabled firewalls, 11–12

## • U •

validation  
 of device health, 224  
 of endpoint machines, 81  
 of identity, 151–153

valuation, 289

value of NAC solutions, 32

value-added resellers (VARs), 137

vendors  
 in credentialing, 151  
 DHCP network control, 192–193  
 evaluation of, 67, 82–84, 206  
 host-based enforcement differences, 180  
 information, 287  
 multiple device support, 156  
 patches, 85  
 in proof-of-concept testing, 198  
 requests for proposals for, 201  
 selecting, 127  
 of software appliances, 184  
 of SSL VPN, 81, 91  
 switch controls, 191  
 System Health Agents development, 222  
 verification of credentials, 146

version verification, 160

virtual environments, 181

virtual local area networks (VLANs), 46, 64, 186–188

virtual private networks (VPNs)  
 customer use of, 44  
 802.1X standards, 74  
 enforcement, 224, 227, 270  
 IPsec enforcement with, 76  
 remote employees, 1

virtual sandboxes, 274–275

virtualization software, 274–275

virus signatures, 160

Vista, 221–223, 236

VLANs (virtual local area networks), 46, 64, 186–188

Voice over Internet Protocol (VoIP)  
 phones, 137

VPNs. *See* virtual private networks (VPNs)

vulnerabilities. *See also* threats  
 with administrative privileges and  
 rights, 131  
 checks for, 11  
 of LANs, 39  
 remote scanning for, 165  
 reviewing for, 124  
 with SNMP, 247  
 of Windows operating systems, 84, 158,  
 161, 163

## • W •

weak security, 177

Web portals  
 for authentication, 146–147  
 for credentials, 150

Web-based interface for network access,  
 121

Wi-Fi protection, 78

Windows  
 policies for, 161  
 vulnerabilities, 158

Windows Graphical Identification and  
 Authentication (GINA), 147

Windows Mobile, 156

Windows operating systems, 84

Windows Security Center (WSC), 222

Windows Server 2008, 221–223, 236

Windows Vista, 221–223

Windows XP Service Pack 3, 221–224

wireless access, 26–27, 209, 224

wireless local area networks (WLANs), 2,  
 38, 97

wireless networks, 38–39, 137, 245

worldwide compliance regulations, 40

WSC (Windows Security Center), 222

## • X •

x86 hardware, 184–185

X.509 digital certificates, 54, 79–80, 87–88,  
 165

XP Service Pack 3, 221–224