



Numbers

5500 series Adaptive Security Appliances, NADs (Network Access Devices), 21

802.1X

- disassociated wireless client, 119
- wired clients.
 - CTA Windows installation, 35–42*
 - troubleshooting, 82, 85–86*

A

Access Control Server. See ACS

access-group Policy-ACL command, 164

ACLs, Layer 3 NAC configuration, 161–163

ACS (Access Control Server), 22. See also Cisco

Secure Access Control Server

- agentless hosts, 298–299
 - Agentless Host for L3, 299*
 - configuration, 300–305*
 - NAC-L2-802.1X enabled networks, 299–300*
- configuration, 248
 - digital certificates, 252–253, 256–258*
 - global authentication protocols, 259–262*
 - NADs (network access devices), 250–251*
 - NAPs (network access profiles), 262–264*
 - NDGs (Network Device Groups), 249–250*
 - RADIUS attributes, 251–252*
- event sending to CS-MARS, 509
 - 802.1X NADs configuration, 513–514*
 - defining as reporting device, 509–511*
 - logging configuration, 511–513*
 - pnlog agent installation, 514–517*
- installation
 - post tasks, 246–247*
 - previous version upgrade, 246*
 - server system requirements, 242–243*
 - Windows, 243–245*
- large enterprise NAC configuration, 463
 - database replication, 466–471*
 - NAC-L2-802.1X, 464–466*
- logging options, 307
 - failed attempts configuration, 307–309*

- passed authentications configuration, 309–311*

- RADIUS accounting logging, 311–313*

- NAFs (network access filters), 295–297

- NAPs (network access profiles), 286–288

- Authentication policy, 289–290*

- Authorization policy, 294–295*

- Posture Validation policy, 290–293*

- Protocols policy, 288–289*

- posture enforcement

- downloadable IP ACLs, 276–279*

- policy-based ACLs, 281*

- RACs (RADIUS authorization*

- components), 282–286*

- VLAN assignment, 280–281*

- posture validation, 264–266

- antivirus servers, 274*

- audit servers, 274*

- deleting rule, 276*

- notification string, 276*

- policies, 266–267, 270–272*

- rule cloning, 275–276*

- rule ordering, 275*

- replication, 313

- small business configuration, 399–405, 413–414

- troubleshooting

- certificate issues, 318*

- enabling service debug logging, 314–317*

- invalid protocol data, 317*

- RADIUS dictionary missing, 318*

- RADIUS posture validation incorrect mapping, 318*

- user database, 305–306

- vendor attributes, 306

ACS dictionary, attribute definitions, 61–62

Activity, Security Posture

- NAC, 530

- NAC Infected/Quarantine, 531

Adaptive Security Appliances. See ASA

address assignment

- IPSec remote-access tunnels, 186–187

- security appliance configuration, 218–219

Administrative Client, Cisco Secure Services

- configuration, 94–102

- installation, 93–94

agent kits, CSA (Cisco Security Agent), 333–336**agentless hosts**

ACS, 298–299
Agentless Host for L3, 299
 configuration, 300–305
NAC-L2-802.1X enabled networks, 299–300

architecture, 358–361
 audit servers, configuration, 361–374

CS-MARS reports, 532–533

handling options

audit servers, 357–358
MAC authentication bypass, 356
NAD exception lists, 355–356

monitoring

CS-ACS logs, 376
NADs, 377–378
QualysGuard Scanner Appliance, 375–376

Altiris Quarantine solution

medium enterprise configuration, 433–434

remediation solutions, 381–384

adding Notification Server, 386
exception policies, 387
importing attribute files, 385
Network Access Agent and Posture Plug-in, 386–387
Network Discovery, 384
posture policy on Notification Server, 387–388

analysis, NAC components, 23–24**antivirus policies, maintaining, 492****antivirus servers, ACS posture validation, 274****antivirus software**

HCAP (Host Credential Authorization Protocol), 345–352
 posture plug-ins, 344–345
 supported vendors, 343

architectures

agentless hosts, 358–361
 CSA (Cisco Security Agent), 324–325
CSA MC rule definitions, 325–327
global event correlation, 327–328

Layer 3 NAC, 155–158

NAC-L2-802.1X, 139–141

NAC-L2-IP, 123–125

security appliance, 211–212

VPN 3000 series concentrators, 175
L2TP over IPSec clients, 179–180
software clients, 176–178

ASA (Adaptive Security Appliances), 21, 211

5500 series, 21

architecture, 211–212

configuration, 212–213

NAC-related parameters, 221–228

VPN, 213–221

VPN client, 221

event sending to CS-MARS, 524

configuring forward events, 526–527
defining reporting device, 524–526

testing, 229

NAC session monitoring, 235–238

remote-access IPSec tunnel from agentless client, 232–234

remote-access IPSec tunnel from CTA client, 234–235

remote-access IPSec tunnel without NAC, 230–232

attribute files, Altiris, 385**audit servers**

ACS posture validation, 274

configuration, 361

configuring QualysGuard Scanner Appliance, 363–366

CS-ACS server configuration, 366–374

QualysGuard Scanner Appliance installation, 362–363

medium enterprise configuration, 432–433

NAP setup, 370

audits servers, agentless hosts, handling options, 357–358**authentication**

Layer 3 NAC configuration, 159–160

users

IPSec remote-access tunnels, 183–185

security appliance configuration, 217

authentication bypass, agentless host**handling, 356****Authentication policy, ACS NAPs, 289–290****Authorization policy, ACS NAPs, 294–295**

B

best practices

- CSA MC management, 489–491
- maintaining policies, 491
 - antivirus*, 492
 - operating system*, 491–492
 - remediation servers*, 492
- NAC deployment, 481–482
 - final deployment strategy*, 487–488
 - initial tuning*, 486
 - lab testing*, 483–485
 - pilot site*, 486
 - readiness assessment*, 482–483
 - test plans*, 485
 - user assessment*, 483
- provisioning software to client machines, 488–489
- technical support, 492–493
- training and education, 493
 - end-user*, 493–494
 - engineering staff*, 494
 - help desk staff*, 494

branch offices, large enterprise network topology, 454–456

brokers, CTA (Cisco Trust Agent), 12

business requirements, medium enterprise, 424–425

C

CA certificates, CTA lab environment deployment, 46

- Linux, 47
- Mac, 47
- post installation tasks, 47
- Windows, 46–47

call centers, headquarter network topology, 458

catalyst switches, NADs (Network Access Devices), 17–20

CatOS (Cisco Catalyst switch), 130

- medium enterprise configuration, 427–430
- NAC-L2-802.1X configuration, 144
- NAC-L2-IP configuration, 130–132

Cisco 5500 series Adaptive Security Appliances NADs (Network Access Devices), 21

Cisco Adaptive Security Appliances. *See* ASA

Cisco Catalyst switch. *See* CatOS

Cisco Easy VPN Client, VPN configuration, 189–192, 221

Cisco IOS

- NAC-L2-802.1X configuration, 142–144
- NAC-L2-IP configuration, 126–129
- router report to CS-MARS, 499–500
 - defining as reporting device*, 500–502
 - forward events configuration*, 502–504

Cisco IOS routers, NADs (Network Access Devices), 16–17

Cisco Network Admission Control, Volume I, 5, 18, 30

Cisco PIX Security Appliances. *See* PIX Security Appliances

Cisco Secure Access Control Server, 241–242. *See also* ACS

- agentless hosts, 298–299
 - Agentless Host for L3*, 299
 - configuration*, 300–305
 - NAC-L2-802.1X enabled networks*, 299–300
- configuration, 248
 - digital certificates*, 252–253, 256–258
 - global authentication protocols*, 259–262
 - NADs (network access devices)*, 250–251
 - NAPs (network access profiles)*, 262–264
 - NDGs (Network Device Groups)*, 249–250
 - RADIUS attributes*, 251–252
- HCAP (Host Credential Authorization Protocol), 346–352
- installation
 - post tasks*, 246–247
 - previous version upgrade*, 246
 - server system requirements*, 242–243
 - Windows*, 243–245
- logging options, 307
 - failed attempts configuration*, 307–309
 - passed authentications configuration*, 309–311
 - RADIUS accounting logging*, 311–313
- medium enterprise configuration, 435
 - ADF file import*, 435
 - Altiris server setup*, 438
 - authorization rules*, 442–443
 - external antivirus policy server*, 437–438

- network access filter configuration, 435–436*
- posture-validation policies, 436–437*
- posture-validation rules, 441–442*
- QualysGuard Scanner setup, 438–439*
- shared components profile, 439–441*
- NAFs (network access filters), 295–297
- NAPs (network access profiles), 286–288
 - Authentication policy, 289–290*
 - Authorization policy, 294–295*
 - Posture Validation policy, 290–293*
 - Protocols policy, 288–289*
- posture enforcement
 - downloadable IP ACLs, 276–279*
 - policy-based ACLs, 281*
 - RACs (RADIUS authorization components), 282–286*
 - VLAN assignment, 280–281*
- posture validation, 264–266
 - antivirus servers, 274*
 - audit servers, 274*
 - deleting rule, 276*
 - notification string, 276*
 - policies, 266–267, 270–272*
 - rule cloning, 275–276*
 - rule ordering, 275*
- replication, 313
- troubleshooting
 - certificate issues, 318*
 - enabling service debug logging, 314–317*
 - invalid protocol data, 317*
 - RADIUS dictionary missing, 318*
 - RADIUS posture validation incorrect mapping, 318*
- user database, 305–306
- vendor attributes, 306
- Cisco Secure Services Client, 91–92**
 - current status viewing, 113–114
 - deployment
 - creating license file, 111*
 - End-User Client, 103–113*
 - installation, 92
 - Administrative Client, 93–94*
 - configuring Administrative Client, 94–102*
 - system requirements, 93*
 - troubleshooting
 - disassociated wireless client, 119*
 - GUI does not start, 118*
 - icon in system tray, 118*
 - password prompt, 119*
 - suspended client, 119*
 - System Report Utility, 115–117*
 - viewing client log, 117*
- WZC (Windows Wireless Zero configuration), 115
- Cisco Security Agent. See CSA**
- Cisco Security Agent, 324**
- Cisco Security Agent Management Center. See CSA MC**
- Cisco Security Monitoring, Analysis, and Response System. See CS-MARS**
- Cisco Trust Agent. See CTA**
- Cisco VPN 3000 series concentrators. See VPN 3000 series concentrators**
- Cisco Web site, 12**
- clear eou command, 135**
- clientless hosts, Layer 3 NAC configuration, 165–166**
- clients**
 - end-user, small business configuration, 405–406
 - provisioning software, 488–489
 - VPN 3000 series concentrators, 176–178
- clients logs, troubleshooting Cisco Secure Services Client, 117**
- clogcli utility, CTA logging, 68–69**
- commands, Layer 3 NAC monitoring, 168–169**
- communications**
 - CTA (Cisco Trust Agent), 12
 - troubleshooting CTA (Cisco Trust Agent), 78–79
- components, NAC (Network Admissions Control)**
 - analysis, 23–24
 - Cisco Secure Access Control Server, 22
 - CSA (Cisco Security Agent), 14–15
 - CTA (Cisco Trust Agent), 12–14
 - monitoring, 23–24
 - NADs (Network Access Devices), 15–22
 - reporting, 23–24
- Computer Associates, supported antivirus vendors, 343**
- conference center, headquarter network topology, 459**

configuration

- ACS, 248
 - agentless host policy*, 300–305
 - digital certificates*, 252–253, 256–258
 - global authentication protocols*, 259–262
 - NADs (network access devices)*, 250–251
 - NAPs (network access profiles)*, 262–264
 - NDGs (Network Device Groups)*, 249–250
 - RADIUS attributes*, 251–252
- audit servers, 361
 - configuring QualysGuard Scanner Appliance*, 363–366
 - CS-ACS server configuration*, 366–374
 - QualysGuard Scanner Appliance installation*, 362–363
- Cisco Secure Services, 92
 - Administrative Client*, 93–102
 - system requirements*, 93
- CSA (Cisco Security Agent), 331
 - agent kits*, 333–336
 - creating groups*, 331–333
 - NAC Posture changes*, 336–338
- large enterprise NAC, 463
 - ACS*, 463–471
 - end-user clients*, 472
 - switches*, 472
- Layer 3 NAC, 158–159
 - AAA authentication*, 159–160
 - clientless host parameters*, 165–166
 - defining RADIUS server*, 160–161
 - exception policies*, 163–165
 - intercept ACLs*, 162–163
 - interface ACL*, 161–162
 - optimizing parameters*, 166–168
 - parameters*, 162
- NAC for small business, 399
 - Cisco Secure ACS*, 399–405
 - end-user clients*, 405–406
 - switches*, 406–410
 - web server*, 411
- NAC-L2-802.1X
 - CatOS*, 144
 - Cisco IOS*, 142–144
 - wireless access points*, 147–150
- NAC-L2-IP
 - CatOS*, 130–132
 - Cisco IOS*, 126–129
 - nonresponsive hosts*, 132–133
- security appliance, 212–213
 - NAC-related parameters*, 221–228
 - VPN*, 213–221
 - VPN client*, 221
- VPN 3000 series concentrators, 181
 - Cisco Easy VPN Client*, 189–192
 - NAC-related parameters*, 193–200
 - VPN configuration*, 182–189
- WZC (Windows Wireless Zero configuration), 115
- CSA (Cisco Security Agent), 14–15, 323–324**
 - architecture, 324–325
 - CSA MC rule definitions*, 325–327
 - global event correlation*, 327–328
 - configuring features, 331
 - agent kits*, 333–336
 - creating groups*, 331–333
 - NAC Posture changes*, 336–338
 - CSA MC installation, 328–331
 - event sending to CS-MARS, 518
 - defining as reporting device*, 518–520
 - forward event configuration*, 520–521
- CSA MC (Cisco Security Agent Management Center), 15, 323**
 - architecture, 324–325
 - global event correlation*, 327–328
 - rule definitions*, 325–327
 - installation, 328–331
 - management, 489–491
- CS-ACS (Cisco Secure Access Control Server), 181**
 - BPN 3000 series concentrators user authentication, 181
 - configuration, 366–367
 - defining QualysGuard Scanner Appliance*, 368–369
 - loading ADF*, 367
 - NAP audit server setup*, 370
 - NAP authorization policy*, 373
 - QualysGuard root certificate*, 373–374
 - shared profile configuration*, 371–372
 - monitoring logs, 376
- CSA-MC, medium enterprise configuration, 443**
- CS-MARS (Cisco Security Monitoring, Analysis, and Response System), 497**
 - ACS event sending configuration, 509
 - 802.1X NADs configuration*, 513–514
 - defining as reporting device*, 509–511

- logging configuration*, 511–513
- pnlog agent installation*, 514–517
- ASA (Adaptive Security Appliance), 524
 - configuring forward events*, 526–527
 - defining reporting device*, 524–526
- basics, 497–499
- Cisco IOS router setup, 499–500
 - defining as reporting device*, 500–502
 - forward events configuration*, 502–504
- CSA event sending configuration, 518
 - defining as reporting device*, 518–520
 - forward event configuration*, 520–521
- generating reports, 528–529
 - agentless hosts*, 532–533
 - scheduling*, 533–534
 - top hosts*, 531
 - top tokens*, 530
- PIX, 524
 - configuring forward events*, 526–527
 - defining reporting device*, 524–526
- QualysGuard, 527–528
- switch setup, 504
 - defining as reporting device*, 505–507
 - forward events configuration*, 508–509
- troubleshooting
 - monitored device discovery*, 537
 - specific device events not showing*, 535–536
 - unknown reporting device events showing*, 536–537
- VPN 3000 concentrators, 521
 - defining as reporting device*, 521–522
 - forward event configuration*, 523–524
- CTA (Cisco Trust Agent), 12–14, 29–30, 331**
 - ctad.ini file, 48–49, 55–56
 - deployment, 30–31
 - installation packages*, 32–34
 - lab environment*, 34–47
 - minimum system requirements*, 32
 - operating systems*, 31–32
 - production networks*, 70–77
 - logging service, 63–64
 - clogcli utility*, 68–69
 - ctalogd.ini file creation*, 64–68
 - posture plug-ins, 344–345
 - Scripting Interface, 57
 - executing*, 62–63
 - use requirements*, 58–62

- troubleshooting
 - 802.1X wired client*, 82, 85–86
 - communication*, 78–79
 - disconnected client*, 87
 - installation*, 77–78
 - posture token validation*, 81–82
 - system logs*, 80–81
- user notifications, 48
- wired client comparison to Cisco Secure Services Client, 91

- ctad.ini files, CTA (Cisco Trust Agent), 48–51, 55–56**
- ctalogd.ini files, creating, 64–68**

D

- data center, headquarter network topology, 460**
- database replication, large enterprise NAC configuration, 466–471**
- debug commands, troubleshooting**
 - large enterprise NAC, 474
 - NAC-L2-IP, 137–139
- debug eou all command, 170–171**
- deployment**
 - Cisco Secure Services
 - creating license file*, 111
 - End-User Client*, 103–113
 - CTA (Cisco Trust Agent), 30–31
 - installation packages*, 32–34
 - lab environment*, 34–47
 - minimum system requirements*, 32
 - operating systems*, 31–32
 - production networks*, 70–77
 - NAC in medium enterprise, 419–421
 - management network*, 422–423
 - quarantine network*, 423
 - user network*, 421
 - phases, final strategy, 487–488
- device authorize command, 163–164**
- digital certificates, ACS configuration, 252–253, 256–258**
- downloadable IP ACLs, ACS posture enforcement, 276–279**
- dynamic crypto maps, security appliance configuration, 220**
- Dynamic Link Library files, posture plug-in, 344**

E

- education, best practices, 493**
 - end-user, 493–494
 - engineering staff, 494
 - help desk staff, 494
- End-User Client, Cisco Secure Services**
 - creating configuration files, 103–111
 - deployment, 112–113
 - prerequisites, 103
- end-user clients**
 - large enterprise NAC configuration, 472
 - medium enterprise configuration, 443
 - small business configuration, 405–406
 - training best practices, 493–494
- enforcement actions, large enterprise business requirements, 453**
- engineering, headquarter network topology, 459**
- engineering staff, training best practices, 494**
- eou allow clientless command, 165**
- eou allow ip-station-id command, 162, 359, 500**
- eou clientless password command, 166**
- eou clientless username command, 166**
- eou default command, 168**
- EoU logging, troubleshooting, NAC-L2-IP, 136–137**
- eou logging command, 170**
- eou max-retry 2 command, 167**
- eou port command, 167**
- eou rate-limit command, 168**
- eTrust AntiVirus, 343**
- eTrust Patrol, 343**
- exception lists**
 - NAD, agentless hosts, 355–356
 - security appliance configuration, 228
 - security appliances, 212
- exception policies**
 - Altiris remediation, 387
 - Layer 3 NAC configuration, 163–165
- exceptions list, VPN 3000 series concentrators, 194–198**
- external antivirus policy servers, Cisco Secure ACS, 346–352**
- external groups, 182**

F–G

- finance, headquarter network topology, 459**
- GAME protocol (Generic Authorization Message Exchange protocol), 11**
- Generic Authorization Message Exchange protocol (GAME protocol), 11**
- global authentication protocols, ACS configuration, 259–262**
- global parameters, NAC, VPN 3000 series concentrators, 193**
- groups**
 - CSA (Cisco Security Agent), 331–333
 - IPSec remote-access tunnels, 182
- GUI, troubleshooting Cisco Secure Services Client, 118**

H

- HCAP (Host Credential Authorization Protocol), 345–352**
- headquarters, large enterprise network topology, 457–458**
 - call center, 458
 - conference center, 459
 - data center, 460
 - engineering, 459
 - finance, 459
 - human resources, 459
 - remote access VPNs, 460
 - sales department, 459
 - VLAN assignment, 461–463
- help desk staff, training best practices, 494**
- Host Credential Authorization Protocol (HCAP), 345–352**
- human resources, headquarter network topology, 459**

I–K

- identity policy command, 164**
- identity profile eapoudp command, 163**
- IEEE 802.1X, 30**

.inf files, CTA Scripting Interface, 60–62**Information Files, posture plug-in, 344****installation**

ACS

- post tasks, 246–247*
- previous version upgrade, 246*
- server system requirements, 242–243*
- Windows, 243–245*

Cisco Secure Services, 92

- Administrative Client, 93–94*
- configuring Administrative Client, 94–102*
- system requirements, 93*

CSA MC, 328–331

CTA (Cisco Trust Agent)

- packages, 32–34*
- troubleshooting, 77–78*

internal groups, 182**IOS routers, NADs (Network Access Devices), 16–17****IP address assignment, security appliance configuration, 218–219****ip admission IOS-NAC command, 162****ip admission name command, 162****ip radius source-interface command, 161****IPSec**

- remote-access tunnels, 182
 - address assignment, 186–187*
 - group configuration, 182*
 - mode-config assignment, 189*
 - user authentication, 183–185*
- security appliance configuration, defining policy, 219
- tunnels, VPN 3000 series concentrators, 179–180

IPSec tunnels

- remote-access from agentless client
 - security appliances, 232–234*
 - VPN 3000 series concentrators, 203–205*
- remote-access from CTA client
 - security appliances, 234–235*
 - VPN 3000 series concentrators, 205–207*
- remote-access without NAC
 - security appliances, 230–232*
 - VPN 3000 series concentrators, 200–203*

ISAKMP

- security appliance configuration, preshared keys, 217
- VPN security appliance configuration, 214

L

L2TP over IPSec clients, VPN 3000 series concentrators, 179–180**lab environments, CTA deployment, 34**

- CA certificate, 46–47
- Linux installation, 45
- Mac installation, 42–44
- Windows installation, 34–42

lab testing, NAC deployment phase, 483–485**large enterprises**

- business requirements
 - enforcement actions, 453*
 - security policies, 452–453*
- NAC configuration, 463
 - ACS, 463–471*
 - end-user clients, 472*
 - switches, 472*
- network topology
 - branch office, 454–456*
 - headquarters, 457–463*
 - regional office, 456*
- troubleshooting
 - ACS logs, 475*
 - debug commands, 474*
 - show commands, 473–474*

Layer 3 NAC

- architecture, 155–158
- configuration, 158–159
 - AAA authentication, 159–160*
 - clientless host parameters, 165–166*
 - defining RADIUS server, 160–161*
 - exception policies, 163–165*
 - intercept ACLs, 162–163*
 - interface ACL, 161–162*
 - optimizing parameters, 166–168*
 - parameters, 162*
- monitoring commands, 168–169
- troubleshooting, 170–171

license files, Cisco Secure Services Client deployment, 111

Linux, CTA (Cisco Trust Agent)

- CA certificate, 47
- installation packages, 33
- lab environment installation, 45
- operating system support, 31
- production environment deployment, 76–77

logging, ACS, 307

- failed attempts configuration, 307–309
- passed authentication configuration, 309–311
- RADIUS accounting logging, 311–313

logging services, CTA (Cisco Trust Agent), 63–64

- clogcli utility, 68–69
- ctalogd.ini file creation, 64–68
- troubleshooting, 80–81

M**MAC**

- agentless hosts handling, authentication bypass, 356

CTA (Cisco Trust Agent)

- CA certificate, 47
- installation packages, 33
- lab environment installation, 42–44
- operating system support, 31

- NAC-L2-802.1X authentication bypass, 144–145

- production environment deployment, 75–76

management networks, medium enterprise NAC deployment, 422–423**McAfee, supported antivirus vendors, 343****medium enterprises**

- business requirements, 424–425
- configuration steps, 427
 - Altiris Quarantine solution configuration, 433–434*
 - audit server configuration, 432–433*
 - CatOS configuration, 427–430*
 - Cisco Secure ACS configuration, 435–443*
 - CSA-MC server configuration, 443*
 - end-user clients, 443*
 - Trend Micro Policy Server configuration, 434*
 - VPN 300 concentrator configuration, 430–431*

- major NAC solution highlights, 425–427

- NAC deployment overview, 419, 421

- management network, 422–423*

- quarantine network, 423*

- user network, 421*

- troubleshooting

- NAC on Catalyst 6500 switch, 444–446*

- NAC on VPN 3000 concentrator, 446–448*

- secure ACS logging, 448*

Meetinghouse AEGIS SecureConnect client. See Cisco Secure Services Client**mode-config assignment, IPsec remote-access tunnels, 189****monitoring**

- agentless hosts, 375–376

- CS-ACS logs, 376*

- NADs, 377–378*

- Layer 3 NAC, 168–169

- medium enterprises

- NAC on Catalyst 6500 switch, 444–446*

- NAC on VPN 3000 concentrator, 446–448*

- secure ACS logging, 448*

- NAC components, 23–24

- security appliances, 229

- NAC sessions, 235–238*

- remote-access IPsec tunnel from agentless client, 232–234*

- remote-access IPsec tunnel from CTA client, 234–235*

- remote-access IPsec tunnel without NAC, 230–232*

- VPN 3000 series concentrators, 200

- remote-access IPsec tunnel from agentless client, 203–205*

- remote-access IPsec tunnel from CTA client, 205–207*

- remote-access IPsec tunnel without NAC, 200–203*

N**NAC (Network Admission Control), 5**

- basics, 5–7

- Phase I, 7–8*

- Phase II, 9–11*

- program participation, 12*

components

- analysis*, 23–24
- Cisco Secure Access Control Server*, 22
- CSA (Cisco Security Agent)*, 14–15
- CTA (Cisco Trust Agent)*, 12–14
- monitoring*, 23–24
- NADs (Network Access Devices)*, 15–22
- reporting*, 23–24

NAC agentless host (NAH), 11**NAC Layer 2 802.1X**

- agentless hosts, 299–300
- architecture, 139–141
- configuration
 - CatOS*, 144
 - Cisco IOS*, 142–144
- Mac authentication bypass, 144–145
- troubleshooting, 145–147
- wireless access point configuration, 147–150

NAC Layer 2 IP

- agentless hosts, 299
- architecture, 123–125
- configuration
 - CatOS*, 130–132
 - Cisco IOS*, 126–129
 - nonresponsive hosts*, 132–133
- troubleshooting
 - debug commands*, 137–139
 - EoU logging*, 136–137
 - show commands*, 133–136

NAC Posture, CSA (Cisco Security Agent), 336–338**NAC-L2-802.1X, 9**

- agentless hosts, 299–300
- architecture, 139–141
- attributes, 18
- configuration
 - CatOS*, 144
 - Cisco IOS*, 142–144
- large enterprise NAC configuration, 464–466
- Mac authentication bypass, 144–145
- troubleshooting, 145–147
- wireless access point configuration, 147–150

NAC-L2-IP, 9

- agentless hosts, 299
- architecture, 123–125
- attributes, 18

configuration

- CatOS*, 130–132
- Cisco IOS*, 126–129
- nonresponsive hosts*, 132–133

troubleshooting

- debug commands*, 137–139
- EoU logging*, 136–137
- show commands*, 133–136

NAC-L3-IP, agentless hosts, 299**NAC-related parameters**

- security appliance configuration, 221–222
 - authentication configuration*, 224
 - exception list*, 228
 - global parameter setup*, 222–223
 - user group policy*, 225–227
- VPN 3000 series concentrators, 193
 - global parameter setup*, 193
 - NAC exception list*, 194–198
 - user group enabling*, 198–200

NADs (Network Access Devices), 15–16, 250

- ACS configuration, 250–251
- agentless host handling, exception lists, 355–356
- catalyst switches, 17–20
- Cisco 5500 series Adaptive Security Appliances, 21
- Cisco IOS routers, 16–17
- monitoring agentless hosts, 377–378
- PIX 500 series security appliances, 21
- VPN 3000 series concentrators, 20, 175
 - architecture*, 175–180
 - configuration steps*, 181–200
 - testing solutions*, 200–207
- wireless device support, 21–22

NAFs (network access filters), 295–297**NAH (NAC agentless host), 11****NAPs (network access profiles), 286**

- ACS, 286–288
 - Authentication policy*, 289–290
 - Authorization policy*, 294–295
 - configuration*, 262–264
 - Posture Validation policy*, 290–293
 - Protocols policy*, 288–289

NDGs (Network Device Groups), 249–250**Network Access Agent and Posture Plug-in,****Altiris remediation, 386–387****network access devices. See NADs****network access filters (NAFs), 295–297**

network access profiles. *See* NAPs
 Network Admission Control. *See* NAC
 Network Device Groups (NDGs), 249–250
 Network Discovery, Altiris, 384
 network profiles, configuring Administrative Client, 94–100
 network topology, large enterprises
 branch office, 454–456
 headquarters, 457–463
 regional office, 456
 networks, small businesses, 397–398
 no eou revalidate command, 167
 nonresponsive hosts, NAC-L2-IP configuration, 132–133
 Notification Server, Altiris remediation
 adding, 386
 posture policy, 387–388
 notification strings, ACS posture validation, 276

O–P

operating systems

CTA deployment, 31–32
 maintaining policies, 491–492

parameters

Layer 3 NAC, 162
 Layer 3 NAC configuration, 166–168

passwords, troubleshooting Cisco Secure Services Client, 119

PatchLink, remediation solutions, 388–389

periodic revalidations, NAC Phase II, 11

Phase I, NAC rollout, 7–8

Phase II, NAC rollout, 9–11

phases, deployment best practices, 481–482

final deployment strategy, 487–488
 initial tuning, 486
 lab testing, 483–485
 pilot site, 486
 readiness assessment, 482–483
 test plans, 485
 user assessment, 483

pilot sites, NAC deployment phase, 486

PIX, event sending to CS-MARS, 524

configuring forward events, 526–527
 defining reporting device, 524–526

PIX 500 series security appliances, NADs (Network Access Devices), 21

PIX security appliances

architecture, 211
 NAC exception lists, 212
 stateful failover, 211
 configuration, 212–213
 NAC-related parameters, 221–228
 VPN, 213–221
 VPN client, 221
 testing, 229
 NAC session monitoring, 235–238
 remote-access IPSec tunnel from agentless client, 232–234
 remote-access IPSec tunnel from CTA client, 234–235
 remote-access IPSec tunnel without NAC, 230–232

pn (Protego Networks), 497

policies

ACS NAPs
 Authentication, 289–290
 Authorization, 294–295
 Posture Validation, 290–293
 Protocols, 288–289
 ACS posture validation, 266–267, 270–272
 maintaining, 491
 antivirus, 492
 operating system, 491–492
 remediation servers, 492

policy-based ACLs, ACS posture enforcement, 281

posture enforcement, ACS

downloadable IP ACLs, 276–279
 policy-based ACLs, 281
 RACs (RADIUS authorization components), 282–286
 VLAN assignment, 280–281

posture plug-ins, antivirus software, 344–345

posture tokens, CTA (Cisco Trust Agent)

troubleshooting, 81–82

posture validation,

ACS, 264–266
 antivirus servers, 274
 audit servers, 274
 deleting rule, 276
 notification string, 276

policies, 266–267, 270, 272

rule cloning, 275–276

rule ordering, 275

creating policies, 436–437

Layer 3 NAC, 156

rule configuration, 441–442

posture validation option, 184

Posture Validation policy, ACS NAPs, 290–293

postures

CTA Scripting Interface, 57

executing, 62–63

use requirements, 58–62

NAC-L2-802.1X validation

architecture, 139–141

configuration, 142–144

Mac authentication bypass, 144–145

troubleshooting, 145–147

wireless access point configuration,

147–150

NAC-L2-IP validation

architecture, 123–125

configuration, 126–133

troubleshooting, 133–139

production networks, CTA (Cisco Trust Agent)

deployment, 70–72

Linux, 76–77

Mac, 75–76

Windows, 72–75

Protego Networks (pn), 497

Protocols policy, ACS NAPs, 288–289

Q–R

QualysGuard Scanner Appliance

configuration, 363–366

defining, 368–369

event sending to CS-MARS, 527–528

installation, 362–363

monitoring agentless hosts, 375–376

root certificate, 373–374

quarantine networks, medium enterprise NAC

deployment, 423

RACs (RADIUS authorization components),

282–286

RADIUS

ACS configuration, 251–252

Layer 3 NAC configuration, 160–161

RADIUS authorization components (RACs),
282–286

radius-server host command, 160

radius-server key command, 160

readiness assessment, NAC deployment phase,
482–483

regional offices, large enterprise network
topology, 456

remediations

Altiris, 381–384

adding Notification Server, 386

exception policies, 387

importing attribute files, 385

Network Access Agent and Posture Plug-
in, 386–387

Network Discovery, 384

posture policy on Notification Server,
387–388

PatchLink, 388–389

servers, maintaining policies, 492

remote access VPNs, headquarter network
topology, 460

remote-access attributes, security appliance
configuration, 214–216

replication

ACS, 313

large enterprise NAC configuration, 466–471

reporting, NAC components, 23–24

reports, CS-MARS, 528–529

agentless hosts, 532–533

scheduling, 533–534

top hosts, 531

top tokens, 530

revalidation timers, 200, 226

routers, NADs (Network Access Devices), 16–17

S

sales department, headquarter network
topology, 459

Scripting Interfaces, CTA (Cisco Trust Agent), 57

executing, 62–63

use requirements, 58–62

SDNI (Self-Defending Network Initiative), 5 section, 49–55**SecureMe, Inc.**

- business requirements, 424–425
- large enterprise network topology
 - branch office, 454–456*
 - headquarters, 457–463*
 - regional office, 456*
- major NAC solution highlights, 425–427
- NAC configuration steps, 427
 - Altiris Quarantine solution configuration, 433–434*
 - audit server configuration, 432–433*
 - CatOs configuration, 427–430*
 - Cisco Secure ACS configuration, 435–443*
 - CSA-MC server configuration, 443*
 - end-user clients, 443*
 - Trend Micro Policy Server configuration, 434*
 - VPN 3000 concentrator configuration, 430–431*
- NAC deployment overview, 419–421
 - management network, 422–423*
 - quarantine network, 423*
 - user network, 421*
- troubleshooting
 - NAC on Catalyst 6500 switch, 444–446*
 - NAC on VPN 3000 concentrator, 446–448*
 - secure ACS logging, 448*

security, CTA (Cisco Trust Agent), 12**security appliances**

- architecture, 211
 - NAC exception lists, 212*
 - stateful failover, 211*
- configuration, 212–213
 - NAC-related parameters, 221–228*
 - VPN, 213–221*
- testing, 229
 - NAC session monitoring, 235–238*
 - remote-access IPSec tunnel from agentless client, 232–234*
 - remote-access IPSec tunnel from CTA client, 234–235*
 - remote-access IPSec tunnel without NAC, 230–232*

security policies, large enterprise business requirements, 452–453**Self-Defending Network Initiative (SDNI), 5****service password-encryption command, 161****Shared Object files, posture plug-in, 344****show commands**

- Layer 3 NAC monitoring, 168
- troubleshooting
 - large enterprise NAC, 473–474*
 - NAC small business deployment, 411–412*
 - NAC-L2-IP, 133–136*

show eou all command, 134, 168, 377–378, 411, 444**show eou config command, 136, 445****show eou ip command, 169, 411, 445****show policy group all command, 444****small business**

- configuring NAC, 399
 - Cisco Secure ACS, 399–405*
 - end-user clients, 405–406*
 - switches, 406–410*
 - web server, 411*
- NAC requirements, 395–397
- network topology, 397–398
- troubleshooting NAC deployment, 411
 - ACS logging, 413–414*
 - certificate issues, 414–415*
 - EAP over UDP logging, 413*
 - show commands, 411–412*

software, provisioning to client machines, 488–489**software clients, VPN 3000 series concentrators, 176–178****stateful failovers, security appliances, 211****status, Cisco Secure Services, 113–114****status query timers, 200, 226****Sullivan, Chad, Cisco Security Agent, 324****switches**

- catalyst switches, 17–20
- large enterprise NAC configuration, 472
- report to CS-MARS setup, 504
 - defining as reporting device, 505–507*
 - forward events configuration, 508–509*
- small business configuration, 406–410

Symantec, supported antivirus vendors, 343**System Report Utility, troubleshooting Cisco Secure Services Client, 115–117****system requirements**

- ACS installation, 242–243
- CTA (Cisco Trust Agent), 32

T

technical support, best practices, 492–493
testing

- NAC deployment phase, planning, 485
- security appliance, 229
 - NAC session monitoring, 235–238*
 - remote-access IPSec tunnel from agentless client, 232–234*
 - remote-access IPSec tunnel from CTA client, 234–235*
 - remote-access IPSec tunnel without NAC, 230–232*
- VPN 3000 series concentrators, 200
 - remote-access IPSec tunnel from agentless client, 203–205*
 - remote-access IPSec tunnel from CTA client, 205–207*
 - remote-access IPSec tunnel without NAC, 200–203*

third-party software, maintaining policies, 492**Top Hosts (Total View) reports, 531****top hosts reports, CS-MARS, 531****Top Tokens (Total View) reports, 530****top tokens reports, CS-MARs, 530****topology, large enterprises**

- branch office, 454–456
- headquarters, 457–463
- regional office, 456

traffic filtering, security appliance configuration, 221**training, best practices, 493**

- end-user, 493–494
- engineering staff, 494
- help desk staff, 494

Trend Micro Policy Server

- medium enterprise configuration, 434
- supported antivirus vendors, 343

troubleshooting

- ACS
 - certificate issues, 318*
 - enabling service debug logging, 314–317*
 - invalid protocol data, 317*
 - RADIUS dictionary missing, 318*
 - RADIUS posture validation incorrect mapping, 318*

Cisco Secure Services

- disassociated wireless client, 119*
- GUI does not start, 118*
- icon in system tray, 118*
- password prompt, 119*
- suspended client, 119*
- System Report Utility, 115–117*
- viewing client log, 117*

CS-MARS

- monitored device discovery, 537*
- specific device events not showing, 535–536*
- unknown reporting device events showing, 536–537*

CTA (Cisco Trust Agent)

- 802.1X wired client, 82, 85–86*
- communication, 78–79*
- disconnected client, 87*
- installation, 77–78*
- posture token validation, 81–82*
- system logs, 80–81*

large enterprise NAC

- ACS logs, 475*
- debug commands, 474*
- show commands, 473–474*

Layer 3 NAC, 170–171

medium enterprises

- NAC on Catalyst 6500 switch, 444–446*
- NAC on VPN 3000 concentrator, 446–448*
- secure ACS logging, 448*

NAC for small business, 411

- ACS logging, 413–414*
- certificate issues, 414–415*
- EAP over UDP logging, 413*
- show commands, 411–412*

NAC-L2-802.1X, 145–147

NAC-L2-IP

- debug commands, 137–139*
- EoU logging, 136–137*
- show commands, 133–136*

security appliances, 229

- NAC session monitoring, 235–238*
- remote-access IPSec tunnel from agentless client, 232–234*
- remote-access IPSec tunnel from CTA client, 234–235*

remote-access IPSec tunnel without NAC,
230–232

VPN 3000 series concentrators, 200
remote-access IPSec tunnel from agentless client, 203–205
remote-access IPSec tunnel from CTA client, 205–207
remote-access IPSec tunnel without NAC, 200–203

trusted servers, configuring Administrative Client, 101–102

tuning, NAC deployment phase, 486

tunnels, security appliance configuration, 216

U

upgrades, ACS installation, 246

user databases, ACS, 305–306

user networks, medium enterprise NAC deployment, 421

user notifications, CTA (Cisco Trust Agent), 48
users

authentication

IPSec remote-access tunnels, 183–185
security appliance configuration, 217

NAC deployment phase, 483

training best practices, 493–494

V

vendor attributes, ACS, 306

VirusScan, 343

VLAN assignment

ACS posture enforcement, 280–281

headquarter network topology, 461–463

VPN

configuration, VPN 3000 concentrator,
182–189

security appliance configuration, 213–214, 221
defining tunnel type, 216
dynamic crypto map, 220
enabling ISAKMP, 214
IP address assignment, 218–219
IPSec policy, 219
ISAKMP preshared keys, 217
remote-access attributes, 214–216

traffic filtering, 221

user authentication, 217

VPN 3000 series concentrators, 175

architecture, 175

L2TP over IPSec clients, 179–180

software clients, 176–178

configuration steps, 181

Cisco Easy VPN Client, 189–192

NAC-related parameters, 193–200

VPN configuration, 182–189

event sending to CS-MARS, 521

defining as reporting device, 521–522

forward event configuration, 523–524

medium enterprise configuration, 430–431

NADs (Network Access Devices), 20

testing solutions, 200

remote-access IPSec tunnel from agentless client, 203–205

remote-access IPSec tunnel from CTA client, 205–207

remote-access IPSec tunnel without NAC, 200–203

W–Z

web servers, small business configuration, 411

Web sites, Cisco, 12

Windows

ACS, installation, 243–245

CTA (Cisco Trust Agent)

802.1X wired supplicant, 35–42

CA certificate, 46–47

installation packages, 33

lab environment installation, 34–35

operating system support, 31

production environment deployment, 72–75

Windows Wireless Zero configuration (WZC), 115

wired supplicants, CTA Windows installation, 35–42

wireless clients, troubleshooting Cisco Secure Services, 119

wireless devices, NADs (Network Access Devices), 21–22

WZC (Windows Wireless Zero configuration), Cisco Secure Services, 115