



## Symbols & Numerics

---

**\*.rtr files, displaying output, 991**  
**.evt files, 887**

**50 percent rule, 148**  
**802.1x**  
 FAQs, 582–584  
 statistics, displaying, 555–557

## A

---

### AAA (Authentication, Authorization, and Accounting)

architectural components, 420  
 authentication, testing on VPN 3K, 593–594  
 authorization, troubleshooting on Cisco switches, 570–574  
 Auth-proxy, troubleshooting on Cisco routers, 457  
 communication protocols  
*RADIUS*, 425–427  
*TACACS+*, 421–424  
 configuring, best practices, 474  
 debug commands, 430–431  
 dial-up networking, troubleshooting on Cisco routers, 446–449, 452–457  
 FAQs, 472–474  
 on Cisco routers  
*accounting, configuring, 445*  
*command authorization, troubleshooting, 443–445*  
*exec authorization, troubleshooting, 440–443*  
*troubleshooting, 432–440*  
*VPDN case study, 458–462*  
 on Cisco switches  
*802.1x, FAQs, 582–584*  
*IBNS, 566–570*  
*IBNSs, 541–545*  
*switch management, 541, 558–566*  
 on VPN 3K  
*FAQs, 611–612*

*session timeouts, avoiding, 593*  
*troubleshooting, 587*

show commands, 429  
 X-Auth, troubleshooting on Cisco routers, 457

**access lists. *See* ACLs**

**Access-Accept messages (RADIUS), 427**  
**Access-Challenge messages (RADIUS), 427**

**accessing**  
 IDM sensor, 888  
 NM-CIDS console, 839

**Access-Reject messages (RADIUS), 427**

**accounting**  
 configuring  
*on Cisco routers, 445*  
*on Cisco switches, 565*  
 troubleshooting on Cisco switches, 566

**ACL Partition Manager (FWSM), 168–169**

**ACLs. *See also* VACLs**

Conduit to Access-list Converter, 53  
 downloadable, 652  
*PIX/IP ACLs, syntax, 606*  
*troubleshooting, 654–655*  
 effect on CBAC performance, 209  
 enabling/disabling on PIX Firewall, 35  
 established keyword, 180  
 implementing on PIX Firewalls, 34  
 IPS sensor blocking, 734–735  
 limitations of, 177  
 misconfigured, troubleshooting on CBAC, 202  
 on FWSM  
*ACL Partition Manager, 168–169*  
*compilation process, 170–172*  
*memory utilization, 164–166*  
 outbound, applying on PIX Firewall, 35–36  
 performance impact on PIX Firewall, 101  
 Reflexive, 180  
 time-range keyword, 34–35  
 wide holes, 181

**acquiring CSAgent software, 997–998**

**ACS. *See* CS ACS (Cisco Secure Access Control Server)**

**activating**  
 syslog on Cisco routers, 193  
 URL filtering, 186

**activation keys for PIX Firewall, 56**

**Active FTP connections, handling with CBAC, 180–181**

**active/active mode (PIX Firewall), 102**  
configuring, 105–106

**active/standby mode (PIX Firewall), 102**

**activities**

Router MC, dangling connections, 968  
unlocking with Firewall MC, 941

**AD (Active Directory). CS ACS integration, 627–629**

**adding**

devices to device table, 1052  
trusted hosts to sensors, 890–892

**Administer Sessions window (VPN 3000**

**Concentrator series), 352**

**agent kits (CSA Agent), generating, 997–998**

**aggressive mode negotiation, 231–232**

**AH (Authentication Header), 226**

**alert database, backing up, 1073**

**Alert Inserter, 1044**

**alerts, configuring, 192–193**

**AnalysisEngine, 678**

**Analyzer daemon, 1055**

**analyzing MDCTSupport file contents, 886–887**

**anti-spoofing, CBAC configuration**

**best practices, 219**

**anti-virus software. creating buffer overflow exclusions, 1018–1020**

**Apache certificate**

regenerating, 897  
trusted host issues, resolving on IDS MC, 897–898  
verifying on IDS MC, 896

**APIs, IDAPI, 678**

**application issues, troubleshooting on**

**CSAgent, 1016**

**application partition (NM-CIDS)**

re-imaging, 854–857  
recovering, 708–709

**application-layer protocols, traffic inspection, 183**

SMTP, 184

**applications comprising IPS software**

AnalysisEngine, 678  
CLI, 678  
MainApp, 677–678

**application-specific roles (ACS), 975**

**application-to-port mappings, modifying, 188–189**

**architectural components of AAA, 420**

**archive files, redirecting away from Database Disk, 1063**

**arguments**

for csutil.exe, 655–656  
for show crypto ipsec command, 299

**ARP spoofing, 80**

**ASA (Adaptive Security Algorithm), characteristics of, 29–30**

**assigning**

IP address to IDS-Sensor interface, 839  
privilege levels to VPN 3k users, 592

**asymmetric cryptographic algorithms, 224**

**asymmetric routing**

PIX Firewall support, 106  
troubleshooting on CBAC, 205

**attributes (VPN 3K), 589**

**audit reports (IDS MC), 885**

**audits, configuring, 193**

**AUS authentication**

with Firewall MC, troubleshooting, 940  
with firewalls, troubleshooting, 940–941

**authentication, 592**

AAA on VPN 3K, FAQs, 611–612  
on Firewall MC firewalls, troubleshooting, 939  
on Firewall MC with AUS, troubleshooting, 940  
on Router MC, troubleshooting, 967  
on VPN 3K, causes of failure, 607–608  
PEAP configuration case study, 574–576, 580  
testing, 593–594

**authentication server (IEEE 802.x framework), 543**

**authenticator, 542**

**authorization**

configuring on Cisco switches, 564–565  
NARs, 648  
*configuring, 648, 651*  
*troubleshooting, 651–652*  
troubleshooting on Cisco switches, 565, 570–574

**Authorization cache, 212**

**auth-proxy, 177**

authentication methods, 212  
configuring, 213–215  
on Cisco routers, troubleshooting, 457  
operation, 212

supported Cisco router platforms, 213  
troubleshooting, 216–217  
**avoiding AAA session timeouts on VPN 3K, 593**

## B

### backing up data

alert database, 1073  
CiscoWorks Common Services, 874–875  
command syntax, 656  
CS ACS, 665  
CSA MC database, 1023–1024  
IPS sensor configuration, 782–783  
Router MC database, 972

### backup files, redirecting away from Database Disk, 1063

### backup/restore operations, troubleshooting on Router MC, 973

### base group attributes (VPN 3K), 589

### baselining, importance of, 6

### best practices

for AAA configuration, 474  
for CBAC  
    *anti-spoofing configuration, 219*  
    *router security, 218–219*  
for CiscoWorks Common Services management, 881  
for CS ACS Server, 670–671  
for CSA MC installation, 1036  
for IDS MC configuration, 929  
for IDSM-2 blade implementation, 829  
for implementing AAA on VPN 3K, 612  
for IPS deployment, 781–785  
for protecting PIX Firewall, 110–111  
for Security Monitor operation, 1077

### Bidirectional replication, 647

### BIN directory (CSA MC), 985

### blat, 1070

### blocking issues on IPS sensors,

ACLs, 734–735  
configuring, 737–740  
for specific signatures, troubleshooting, 753  
implementing, 736–737  
MBS, 737, 741–743  
supported managed devices and versions, 735  
verifying blocking processes, 923–924

### blocking forwarding sensor, 737

### blue screen, troubleshooting, 990

### browsers. *See* web browsers

### buffer overflow exclusions, creating, 1018–1020

### Bugs Tracker, 54

### bulk importing NASSs, 667

### Bypass mode (IPS sensor), 682

## C

### capture command, 47–49

### capturing

debug command output, 199  
IPS traffic  
    *on MPLS IP IDS, 776–777*  
    *on RSPAN, 773–775*  
    *on SPAN, 763–770*  
    *on VACL, 775–776*  
    *on hub, 763*  
packets on FWSM, 123–124  
sniffer traces, 199

### “cascade” replication, 645

### case studies

Hairpinning, configuring, 335–337  
PEAP configuration, 574–576, 580  
RADIUS configuration on Cisco IOS routers, 462–463  
troubleshooting VPDN on Cisco IOS routers, 464–472  
user permissions on Router MC, 974  
    *ACS roles, 975, 978*  
    *CiscoWorks Server roles, 975*  
VPDN configuration on Cisco IOS routers, 458–462

### Catalyst 2900/3500XL switches, configuring IPS traffic capture with SPAN, 765–767

### Catalyst 2900/3600XL switches, configuring SPAN, 765–767

### Catalyst 2950 switches, configuring IPS traffic capture with SPAN, 767–770

### Catalyst 2950/3550 and 3750 switches, configuring SPAN, 767–770

### Catalyst 3550 switches, configuring IPS traffic capture with SPAN, 767–770

### Catalyst 3750 switches, configuring IPS traffic capture with SPAN, 767–770

### Catalyst 4000/6000 switches running CatOS, configuring SPAN, 770–771

**Catalyst 4000/6000 switches running Native IOS, configuring SPAN, 771–772**

**Catalyst 6500, IDSM-2 blade**

- Command and Control port, configuring, 801–805
- event generation, troubleshooting, 817–818
- front panel indicator lights, 789
- hardware issues on CatOS, troubleshooting, 797–800
- hardware issues on Native IOS, troubleshooting, 793–797
- hardware requirements, 788
- installing, 789
- Maintenance Partition, upgrading, 823–824
- Promiscuous mode
  - configuring, 805–813*
  - troubleshooting, 814–816*
- re-imaging, 818–823
- removing from switch, 790
- serial cable, connecting, 826
- signature update, installing, 824–825
- slot assignment, 788
- sniffing ports, 791
- supported ports, 790
- TCP reset, 818
- upgrading to version 5.x, 826
- user passwords, recovering, 827–829
- VACL Capture, 827
- versus IDS Appliance, 787

**categorizing CS ACS problem areas, 625**

**CatOS, Native IOS show commands, 792**

**CBAC (Context-Based Access Control), 177**

- Active FTP connections, handling, 180–181
- anti-spoofing configuration, best practices, 219
- asymmetric routing, troubleshooting, 205
- Cisco IOS code base, upgrading, 209
- connection states, 194–195
- connectivity, troubleshooting, 201–203
- CPU utilization, verifying, 205–206
- FAQs, 217–218
- half-open connections, manipulating threshold values, 208
- HTTP inspection, verifying dropped packets, 208

- interaction with IPsec, 193
- interoperability with NAT, 188
- IP fragmentation, mitigating, 191
- Java blocking, configuring, 184
- misconfigured ACLs, troubleshooting, 202
- misconfigured IP inspection, troubleshooting, 203
- misconfigured NAT, troubleshooting, 202
- multi-channel protocols
  - inspecting, 187, 205*
  - securing, 180*
- packet drops, troubleshooting, 210
- packet flow across routers, 196
- performance, troubleshooting, 205–210
- protecting inside network, 179–180
- router security configuration, best practices, 218–219
- single channel protocol inspection, 182
  - application-layer protocols, 183*
  - ICMP, 182*
  - SMTP, 184*
  - UDP, 182*
- switching path, troubleshooting performance issues, 209
- TCP SYN flood attacks, mitigating, 189–191
- troubleshooting, 199
- UDP connection timeout, selecting, 207–208
- UDP inspection, troubleshooting, 203–205
- URL filtering
  - configuring, 185–187*
  - troubleshooting, 211*

**CEP (Certificate Enrollment Protocol), PKI**

- configuring, 258–261
- troubleshooting, 261–265

**CFG directory (CSA MC), 985**

**challenge-response-based authentication, 546**

**changing database maximum event limit, 1066**

**check pointing CiscoWorks Common Services database, 951**

**checking status of Firewall MC processes, 931**

**CIDEE (Cisco Intrusion Detection Event Exchange), 679–680**

**CIFS access, configuring on VPN 3000**

**Concentrator series, 394**

**circular blocks, 737**

**Cisco AV-Pairs, 653**

**Cisco IOS routers**

AAA

- accounting, configuring, 445*
- Auth-proxy, troubleshooting, 457*
- command authorization, 443–445*
- dial-up networking, troubleshooting, 446–457*
- exec authorization, 440–443*
- router management, troubleshooting, 432–440*
- VPDN case study, 458–462*
- X-Auth, troubleshooting, 457*

IPsec VPNs

- PKI, troubleshooting, 258–265*
- Remote Access client VPN connections, troubleshooting, 265–270*
- NM-CIDS, managing, 848–849
- RADIUS configuration, case study, 462–463
- VPDN troubleshooting, case study, 464–472
- VPNs, DMVPN, 270–280

**Cisco IOS Software, upgrading code base on**

**CBAC routers, 209**

**Cisco PIX firewalls. *See* PIX firewalls**

**Cisco Secure ACS mode (CiscoWorks Common Services), 862**

**Cisco Security Agent Management Center (CSA MC) license key, 865**

**Cisco switches**

AAA

- 802.1x FAQs, 582–584*
  - authorization, troubleshooting, 570–574*
  - IBNS, 566–570*
  - PEAP configuration, case study, 574–580*
  - switch management, 541, 558–566*
- IBNSs, 541–542
- IEEE 802.1x framework, 542–545*

**CiscoWorks Common Services database**

- backing up, 874–875
- FAQs, 877–881
- installing, 870–871
  - database management, 873*
  - minimum requirements, 870*
  - problems, troubleshooting, 871–873*
  - user management issues, 873*
- license key, upgrading, 868
- licenses, troubleshooting, 869
- managing, best practices, 881
- MDCSUPPORT, 863
  - files collected by, 864*

- MDCSupportInformation.zip file,
  - file summary, 864
- Privileges, 862
- resolving DNS errors, 1048
- restore procedures, 875–876, 950
- Roles, 862
- running on multi-homed machines, 879
- user authentication, case study, 876–877
- user management, 862

**CiscoWorks Common Services Desktop,**

**launching on browser, 861**

**CiscoWorks MDCSupportInformation.zip, file contents, 933**

**classifier, 84**

**clear crypto sa command, 238**

**CLI (command-line interface), 678**

- IPS sensors, licensing, 719–720

**clientless SSL VPN mode (VPN 3000**

**Concentrator series)**

- configuring, 390
- troubleshooting, 391–395

**closing NM-CIDS sessions, 843**

**cluster redundancy on VPN 3000 Concentrator series, 412–414**

**collecting MDCSupport file on Windows platform, 886**

**combined sensor mode (IPS), 683**

**Command and Control port**

- on IDSM-2
  - 5-minute output rate, checking, 803–805*
  - configuring, 801–803*
- on NM-CIDS, 834
  - configuring, 844–845*

**command authorization, troubleshooting on**

**Cisco routers, 443–445**

**commands**

- capture, 47–49
- clear crypto sa, 238
- debug, 300
  - debug aaa accounting, 430
  - debug aaa authentication, 430
  - debug aaa authorization, 430
  - debug application-protocol, 47
  - debug commands, FWSM-related, 122–123
  - debug fixup tcpludp, 47
  - debug icmp trace, 46–47
  - debug ip inspect, 197–198

- debug pix process, 47
  - debug sanity, 24
  - debug tunnel, 257–258
  - diagnostic level complete, 795
  - for PIX flash file system, 33
  - intrusion-detection module, 808
  - ip port-map, 189
  - iplog, 691
  - nslookup, 19
  - packet, 692
  - ping, 17
  - recover application-partition, 709
  - service-module, connecting to NM-CIDS, 840
  - show authorization, 554
  - show aaa servers, 430
  - show aaa user, 430
  - show accounting, 554
  - show asp drop, 41–42
  - show blocks, 43
  - show commands
    - for IPsec Phase 1 tunnel negotiations, 233–235*
    - for IPsec Phase 2 tunnel negotiations, 235–236*
    - FWSM-related, 120–122*
  - show configuration, 687
  - show connection, 40
  - show cpu usage, 42
  - show crypto ipsec, 299–300
  - show crypto map, 237
  - show dot1x all, 556
  - show dot1x statistics, 557
  - show events, 687
  - show interfaces, 689
  - show ip inspect, 194–195
  - show local-host, 40–41
  - show localusers, 552
  - show module, 791
  - show output filters, 44–45
  - show radius, 553
  - show radius statistics, 430
  - show running config, 15, 300
  - show running logging, 52
  - show security acl, 792
  - show service-policy, 41, 94
  - show span, 792
  - show statistics, 687–688
  - show tacacs, 430, 553
  - show tech-support, 45, 689
  - show test, 792
  - show traffic, 42
  - show trunk, 792
  - show users, 430
  - show version, 15, 200, 686–690, 791
  - show vlan brief, 558
  - show xlate, 39–40
  - tcpdump, 690
  - telnet, 18
  - time-range, 34–35
  - traceroute, 18
  - winmsd, 988
- common services license key, 865**
- commonly asked questions. See FAQs**
- communication architecture**
- for CSA MC, 986
  - of Firewall MC, 932
  - of Router MC, 960
  - on IDS MC, 884–885
- communication protocols, 678–681**
- RADIUS, 425–426
    - authentication operation, 426–427*
    - authorization operation, 426–427*
    - configuring, case study, 462–463*
  - TACACS+, 421
    - AAA packet flows, 423*
    - accounting operation, 424*
    - authentication operation, 422–423*
    - authorization operation, 424*
    - versus RADIUS, 428–429*
- compacting**
- CiscoWorks Common Services database, 952–953
  - CS ACS database, 660
  - CSA MC database, 1029–1031
- comparing RADIUS and TACACS+, 428–429**
- compilation process for ACLs on FWSM, 170–172**
- components of CSA, 983, 985**
- Conduit to Access-list Converter, 53**
- configuration files**
- for VPN 3000 Concentrator series, 354
  - sysvars.cf, 991

**configuring**

- AAA
  - best practices, 474*
  - on Cisco switches, enable password authentication, 563*
- accounting
  - on Cisco IOS routers, 445*
  - on Cisco switches, 565*
- active/active failover on PIX Firewall, 105–106
- alerts, 192–193
- audits, 193
- auth-proxy, 213–215
- basic router security, best practices, 218–219
- blocking, 737–743
- CBAC anti-spoofing, best practices, 219
- clientless SSL VPN mode on VPN 3000 Concentrator series, 390
- Command and Control interface (NM-CIDS), 844–845
- connectivity
  - on FWSM, 135–139*
  - on PIX Firewall, 69–72*
- CS ACS
  - AAA Client definition for VPN 3K, 609*
  - domain controller mode, 628*
  - replication, 640, 644–647*
- email notification, 1068–1070
- Firewall MC, Recovery Server, 953–954
- FWSM
  - failover, 149–155*
  - multiple SVI interfaces, 157, 161–162*
- GRE over IPsec, 256–257
- Hairpinning, 335–337
- IDM sensors, trusted hosts, 889–890
- IDS MC, best practices, 929
- IDS-2
  - Command and Control port, 801–805*
  - Promiscuous mode, 805–813*
- IPS sensor, Inline mode, 757–762
- IPsec LAN-to-LAN VPN tunnels, 302, 305–308
  - crypto maps, creating, 305–306*
  - transform sets, 304*
  - tunnel groups, 305*
- IPsec over TCP, 339
- Java blocking, 184
- LAN-to-LAN tunnels on VPN 3000 Concentrator series, 356
- LLQ on PIX Firewall, 93–94
- local user authentication on VPN 3K, 597–599
- login authentication, 559–560
- MAPI Proxy on VPN 3000 Concentrator, 399–400
- MBS, 741–743
- MPLS IP IDS, IPS traffic capture, 776–777
- NARs, 648, 651
- NAT-T, 338–339
- NDS database with CS ACS, 630
  - troubleshooting, 631–636*
- NM-CIDS, time stamping, 857–858
- packet capturing on NM-CIDS, 846–848
- PEAP
  - case study, 574–576, 580*
  - Machine Authentication, 567–570*
- PIX Firewall
  - multiple context mode, 87–90*
  - policing, 90–92*
  - Remote Access VPN, 323–327*
- PKI, 258–261
- RADIUS
  - dynamic filters, 604*
  - on Cisco IOS routers, case study, 462–463*
- Remote Access VPN connections on VPN 3000 Concentrator series, 364–365
- RSPAN, IPS traffic capture, 773–775
- sensors
  - on IDS MC, 906*
  - shunning, case study, 920–925*
- SPAN
  - IPS traffic capture, 763–770*
  - on Catalyst 2900/3600XL, 765–767*
  - on Catalyst 2950/3550 and 3750, 767–770*
  - on Catalyst 4000/6000 running CatOS, 770–771*
  - on Catalyst 4000/6000 running Native IOS, 771–772*
- Split Tunneling, 342–344
- SSL VPN on VPN 3000 Concentrator, Thick Client mode, 402–403
- syslog on PIX Firewall, 50–53
- TACACS+ on VPN 3K, 590–592
- traceback on PIX Firewall, 53



- transparent firewalls, 193
  - on *PIX Firewall*, 79–82
- URL filtering, 185–187
- VACL, IPS traffic capture, 775–776
- VPN 3000 Concentrator series
  - Cisco Secure ACS*, 590–591
  - event classes, 348
  - group authentication with *RADIUS*, 599–600
  - Group feature, 608
  - Group Lock feature, 601
  - local group and user authentication, 595
  - RADIUS Server*, 609
- Windows NT/2000 Authentication, Unknown User Policy, 609–610
- connecting**
  - IPS sensor to network, 784
  - serial cable to *IDS-2*, 826
  - to *NM-CIDS* console, 840–842
- connection block, 734**
- connection states, CBAC, 194–195**
- connectivity**
  - on *CBAC*, troubleshooting, 201–203
  - on *FWSM*
    - configuring, 135–139
    - troubleshooting, 134, 139–142
  - on IPS sensors, troubleshooting, 720–725
  - on *PIX Firewall*
    - configuring, 69–72
    - displaying details, 40
    - troubleshooting, 72–76
  - testing with ping command, 17
- console access to *NM-CIDS*, troubleshooting, 843–844**
- console port (*NM-CIDS*), 835**
- Context-Based Access Control. *See* *CBAC***
- CONTINUE packets (*TACACS+*), 422**
- control connection, 181**
- cooperation between *SecOP* and *NetOP* personnel, 7**
- core dumps**
  - generating, 22
    - with *Flash disk*, 23
    - with *FTP*, 22
    - with *rcp*, 23
    - with *TFTP*, 22
  - testing configuration of, 24
- corrupt *IDS MC* licenses, troubleshooting, 904**
- CP (control plane), *FWSM* architecture, 113–114**
- CPU utilization**
  - on *CBAC*, verifying, 205–206
  - on *FWSM*, troubleshooting, 143
  - on *PIX Firewall*
    - displaying, 42
    - troubleshooting, 95–98
- Cr directory (*CSA MC*), 986**
- creating**
  - buffer overflow exclusions, 1018–1020
  - crypto maps for LAN-to-LAN tunnels, 305–306
  - database rules, 1064
  - DMVPN* spoke-to-spoke tunnels, 275
  - dump text files, 657
  - dynamic crypto maps, 327
  - exceptions, 1016
  - securitylog.txt file, 991
  - transform sets, 304
- CRSHDUMP.TXT file, 354**
- Crypto Errors (*CS ACS*), resolving, 661**
- crypto maps, creating for LAN-to-LAN tunnels, 305–306**
- crypto socket creation problems (*NHRP*), troubleshooting, 279**
- cryptographic algorithms, 224**
- cryptographic-based authentication (*EAP*), 546**
- CS ACS (*Cisco Secure Access Control Server*)**
  - AAA Client definition for *VPN 3K*, configuring, 609
  - Active Directory integration, 627–629
  - application-specific roles, 975
  - as proxy server, 665
  - associated registries, 663
  - backing up, 665
  - best practices, 670–671
  - categorizing problem areas, 625
  - configuring, 590–591
  - FAQs, 661–670
  - database, compacting, 660
  - default *NAS*, adding, 663
  - domain controller mode, configuring, 628
  - domain stripping, 665
  - external user database integration, required components, 620
  - GUI, recovering lost passwords, 663
  - installing on Windows platform, 625–627
  - “Logged in Users” report, 668

- NARs, 648
  - configuring*, 648, 651
  - troubleshooting*, 651–652
- NASs, bulk importing, 667
- Novell IDS integration, 630
  - troubleshooting*, 631–636
- packet flow, 619–620
- password encryption, 668
- RADIUS Server, communicating with VPN 3K, 597–599
- replication
  - configuring*, 640, 644
  - troubleshooting*, 644–647
- SDI integration, 636–638
  - troubleshooting*, 638–639
- services, CSAdmin, 615–616
- setup procedures for Router MC, 979–980
- Shared File Components, 653–654
- uninstalling, 661
- upgrading on Windows platform, 625–626
- user/NAS import options, 658
  - exporting user and group information*, 660
  - importing NAS to CS ACS database*, 659
  - importing users to existing database*, 658
- user names, defining, 980
- users, deleting, 659
- CSA Agent, 983**
  - application issues, troubleshooting, 1016
  - communication with CSA MC,
    - troubleshooting, 1014–1015
  - csainfo.bat utility, 989
  - debug mode, turning on, 989–991
  - disk usage, monitoring, 992
  - installation
    - minimum requirements*, 998–999
    - troubleshooting*, 997, 1001
  - license, procuring, 1007
  - log files, 988–992
  - policies, 987
  - polling issues, troubleshooting, 1014–1015
  - registration, troubleshooting, 1014–1015
  - removing from Windows systems, 999–1000
  - rtrformat utility, 990
  - shims, disabling, 1016–1017
  - software, procuring, 997–998
  - stopping service, 991
  - update issues, troubleshooting, 1004–1005
- CSA MC (Cisco Security Agent Management Console), 983**
  - communication architecture, 986
  - database
    - compacting*, 1029–1031
    - manual backups, performing*, 1023–1024
    - purging events from*, 1028–1029
    - repairing*, 1031–1032
    - restoring*, 1025–1027
  - database maintenance, 1023
  - default installation directory, 985
  - directory structure, 985–986
  - disaster recovery, 1036–1037
  - DRP, 1023
  - installation
    - best practices*, 1036
    - minimum requirements*, 995
    - troubleshooting*, 993
  - launching
    - problems with, troubleshooting*, 1010–1013
    - slow launches, troubleshooting*, 1013–1014
  - license key, installing, 869
  - licenses, 1005–1006
    - importing*, 1007–1008
    - procuring*, 1007
    - troubleshooting*, 1009–1010
  - local database installation, troubleshooting, 994
  - log directory, 988
  - log files, 987
  - management model, 983–985
  - manually removing components, 996–997
  - registration, 868
  - remote database installation,
    - troubleshooting, 994
  - uninstalling, 995
  - upgrading, 1002
    - on same system*, 1002–1003
    - on separate system*, 1003–1004
- CSAdmin, 615–616**
- csainfo.bat utility, 989**
- csalog.txt file, 989**
- csauser.dll, disabling, 1018**
- CSAuth, 616**
- CSDBSync, 616**
- CSLog, 616**

**CSMon, 616–617**  
**CSRADIUS service, 618**  
**CSSupport utility, files included in Package.cab file, 622–624**  
**CSTacacs service, 618**  
**csutil.exe, 655, 658**  
     options, 655–656

## D

### daemons

Analyzer, 1055  
 Notifier, 1055

**daily alarm reports, scheduling, 1073**

**dangling connections on Router MC, 968**

**data connection, 181**

**data not passing through IPsec LAN-to-LAN VPN tunnels, troubleshooting, 322–323**

### databases

backing up, command syntax, 656  
 CiscoWorks Common Services, 873

*backing up, 874–875*

*check pointing, 951*

*compacting, 952–953*

*restoring, 875–876, 950*

compacting, 660, 1068

CSA MC database

*compacting, 1029–1031*

*purging events, 1028–1029*

*repairing, 1031–1032*

*restoring database, 1025–1027*

disk utilization, monitoring, 1066

DRP, 1023

maximum event limit, changing, 1066

pruning issues, troubleshooting, 1067–1068

restoring, 657

Router MC

*backing up, 972*

*restoring, 973*

rules, creating, 1064

**DB directory (CSA MC), 986**

**debug aaa accounting command, 430**

**debug aaa authentication command, 430**

**debug aaa authorization command, 430**

**debug application-protocol command, 47**

**debug commands, 195, 197, 300**

    FWSM-related, 122–123

    guidelines for using, 16

    output, capturing, 199

**debug fixup tcpudp command, 47**

**debug icmp trace command, 46–47**

**debug information**

    on Firewall MC, viewing, 932

    on Router MC, 961–962

**debug ip inspect command, 197–198**

**debug logging level (Router MC), 961**

**debug mode (CSA Agent), turning on, 989**

**debug pix process command, 47**

**debug sanity command, 24**

**debug tunnel command, 257–258**

**debugging**

    IDS MC, 887–888

    turning off, 555

**decryption, 223**

**default event limit (database), changing, 1066**

**default installation directory for CSA MC, 985**

**defining**

    tunnel groups for LAN-to-LAN tunnels, 305

    usernames in ACS, 980

**deleting**

    CS ACS users, 659

    users in multiple group, 669

**deployed jobs, stopping, 942**

**deploying**

    device configurations from Firewall MC, 947

    device configurations from Router MC,

        970–971

    IDS MC configuration, 917–920

**deployment architecture of IPS, 676–677**

**destination ports, 764**

**detecting IOS Firewall feature set, 200**

**device groups, defining in ACS, 980**

**devices**

    adding to device table, 1052

    configuration files

*deploying, 947*

*importing, 943–946, 969–970*

    flow rates, monitoring, 1064–1065

**diagnostic commands, show ip inspect, 194–195**

**diagnostic level complete command, 795**

**dial-up networking on Cisco routers**

    accounting, 457

    troubleshooting, 446–456

**Digital Certificates**

- on VPN 3000 Concentrator series, 383–384
  - troubleshooting*, 384–389
- on VPN 3000 Concentrator series VPN client, 382–383

**digital signatures, 225**

**directory structure of CSA MC, 985–986**

**disabling**

- CSAgent shims, 1016–1017
- csausser.dll, 1018

**disconnecting from NM-CIDS console, 842–843**

**disk space, reclaiming, 1011**

**disk usage, monitoring, 992**

**displaying**

- \*.rtr file output, 991
- 802.1X statistics, 555–557
- Firewall MC debug information, 932
- Router MC debug information, 961–962
- server selftest information, 988
- Windows system information, 988

**DMVPN (Dynamic Multipoint VPN), 270**

- configurable dynamic routing protocols, 280
- crypto socket creation problems,
  - troubleshooting*, 279
- dynamic spoke-to-spoke configuration, 273–276
- mGRE interface, 271
- NHRP, 271
  - mapping problems, troubleshooting*, 278–279

**DNS errors, resolving, 1048**

**Doc directory (CSA MC), 986**

**documenting network topology, importance of, 6**

**domain controller mode (CS ACS),**

**configuring, 628**

**domain stripping on CS ACS, 665**

**DoS attacks**

- fragmentation, mitigating with CBAC, 191
- TCP SYN flood, mitigating with CBAC, 189–191

**downgrading PIX Firewall, 66**

**downloadable ACLs, 652**

- PIX/IP, syntax, 606
- troubleshooting*, 654–655

**DPD (Dead Peer Discovery), 345**

**driver\_install.log file, 989**

**DRP (disaster recovery plan), 1023**

- application partition, recovery procedures, 708–709
- implementing, 707

**dump text files, creating, 657**

**dynamic crypto maps, creating, 327**

**dynamic filters**

- active, viewing, 603
- configuring on VPN 3K, 602
- fields, 604
- on RADIUS, configuring, 604
- rules, syntax, 603

**dynamic routing protocols for DMVPN networks, 280**

**dynamic spoke-to-spoke DMVPN configuration, 273–276**

**dynamically mapped users, replication, 670**

**E**

**EAP (Extensible Authentication Protocol), 545–546**

**EAPOL (EAP over LANs), 544**

**egress traffic, 764**

**email notification**

- configuring, 1068, 1070
- troubleshooting*, 1071–1072

**E-mail Proxy (VPN 3000 Concentrator)**

- configuring, 401
- troubleshooting*, 401–402

**enable password authentication**

- configuring, 563
- troubleshooting*, 562–564

**enabling**

- Firewall MC, Recovery Server, 954
- SSL, 1049

**encryption, 223**

- of CS ACS passwords, 668

**error messages, troubleshooting**

- Internal Server Error*, 1050
- Page Cannot Be Found Error*, 1050

**escalation procedures, documenting, 7**

**ESMTP (Extended Simple Mail**

**Transfer Protocol), traffic inspection, 183–184**

**ESP (Encapsulating Security Header), 226**

**established keyword (ACLs), 180**

**establishing LAN-to-LAN tunnels, 240–246**

**Ethernet, 125, 199**

- web site, 20

**Ethernet, interface IDS-Sensor, 834****event classes, configuring on VPN 3000**

- Concentrator series, 348**

**Event Limiting, 991****event log (VPN 3000 Concentrator series), viewing, 350–352****Event Viewer**

- launching, 1055
- test events, generating, 1057
- troubleshooting, 1057

**events**

- Large ICMP events, generating, 1057
- maximum event limit (database), changing, 1066
- purging from CSA MC database, 1028–1029
- writing to securitylog.txt file, 991

**exception memory command, generating core dump, 23****exceptions, creating, 1016****exec authorization, troubleshooting on Cisco routers, 440–443****expired IDS MC licenses, troubleshooting, 905**  
**exporting user and group information from CS ACS database, 660****F****fact gathering stage, production network troubleshooting, 10–11****Failed Attempts logs, 621****failover, 102**

- on FWSM

- configuring, 149–155*
- forced reboot conditions, 147*
- initialization phase, 146*
- monitoring, 147–148*
- troubleshooting, 144–146, 155–157*

- on PIX Firewall

- active/active failover, configuring, 102, 105–106*
- active/standby mode, 102*
- asymmetrical routing support, 106*
- failover groups, 104*
- hardware and licensing requirements, 104*

**failover groups, 104****failure of VPN 3K authentication, causes of, 607–608****FAQs**

- regarding 802.1x, 582–584
- regarding AAA, 472–474
  - on VPN 3K, 611–612*
- regarding CBAC, 217–218
- regarding CS ACS, 661–670
- regarding CSA Agent/CSA MC, 1032–1035
- regarding CiscoWorks Common Services, 877–881
- regarding FWSM, 173–174
- regarding IDS MC, 925–929
- regarding IPS, 777–781
- regarding PIX Firewall, 109–110
- regarding VPN 3000 Concentrator series, 406–410

**Fast Path packet flow through FWSM, 116–118****features of Router MC, 960****Field Notices, 54****fields**

- of dynamic filters, 603–604
- of EAP frames, 546

**file systems (PIX), commands, 33****files in MDCSupport, analyzing, 886–887****filters, configuring dynamic filters on VPN 3K, 602****Firewall MC**

- activities, unlocking, 941
- authentication problems, resolving, 939–940
- browser-related problems, resolving, 937
- CiscoWorks Common Services database
  - check pointing, 951*
  - compacting, 952–953*
- Common Services, installing, 935
- communication architecture, 932
- debug information, viewing, 932
- device configurations
  - deploying, 947*
  - importing, 943–946*
- initialization, 936, 964
- installation issues, troubleshooting, 934
- interoperability with other applications, 936
- jobs, rolling back, 942
- MDCSupport utility, generated files, 933
- processes, 931
- purge-mc-tasks utility, 942

Recovery Server  
*configuring, 953–954*  
*enabling, 954*  
 terminal activities, removing, 941–942

**Firewall module administration on FWSM, troubleshooting, 128–133**

**firewalls**  
 and IPsec, 284–285  
 deploying between IPsec peers, 340  
 on IPsec endpoints, 340

**Flash disk, generating core dumps, 23**

**flow rates, monitoring, 1064–1065**

**fragmentation, mitigating with CBAC, 191**

**front panel indicator lights**  
 IDSM-2, 789  
 NM-CIDS, 833

**FTP, 21**  
 generating core dumps, 22  
 packet flow through FWSM, 118

**FWSM**  
 access-lists  
*ACL Partition Manager, 168–169*  
*compilation process, 170–172*  
*memory utilization, 164–166*  
 connectivity  
*configuring, 135–139*  
*troubleshooting, 134, 139–142*  
 CP, 113–114  
 CPU utilization, troubleshooting, 143  
 debug commands, 122–123  
 failover  
*configuring, 149–155*  
*forced reboot conditions, 147*  
*initialization phase, 146*  
*monitoring, 147–148*  
*troubleshooting, 144–146, 155–157*  
 FAQs, 173–174  
 Firewall module administration issues,  
 troubleshooting, 128–133  
 hardware issues, troubleshooting, 127–128  
 image upgrades, performing, 133–134  
 intermittent packet drops, troubleshooting, 144  
 licensing issues, troubleshooting, 126–127  
 Maintenance Partition, 130–132  
 multiple SVI interfaces, configuring, 157–162  
 NP, 114–116  
 packet capturing, 123–124

packet flows, 116  
*Fast Path packet flow, 116–118*  
*FTP session packet flow, 118*  
*Session Management Path packet flow, 118*  
 password recovery, 132  
 show commands, 120–122  
 syslog, 125

---

## G

**generating**  
 agent kits, 997–998  
 core dumps, 22  
*with exception memory command, 23*  
*with Flash disk, 23*  
*with FTP, 22*  
*with rep, 23*  
*with TFTP, 22*  
 Large ICMP events, 1057  
 test events on Event Viewer, 1057

**GRE over IPsec**  
 configuring, 256–257  
 troubleshooting, 257–258

**group attributes (VPN 3K), 589**

**group authentication with RADIUS, configuring on VPN 3K, 599–600**

**group configuration on VPN 3K, 608**

**Group Lock feature (VPN 3K), 601, 607**

**groups, 985**

**GUI (Firewall MC)**  
 lost passwords, recovering, 663  
 removing terminal activities from  
 Firewall MC, 941–942

---

## H

**Hairpinning, 334**  
 configuring, 335–337

**half-open connections, manipulating threshold values on CBAC routers, 208**

**hardware**  
 IPS support, 683–685  
 on FWSM, troubleshooting, 127–128

**hardware requirements**  
 for IDSM-2, 788

- for NM-CIDS support, 832
- for PIX Firewall failover, 104
- Headless CSAgent software, procuring, 997**
- high availability of PIX firewall for VPN connections, 344–345**
- high CPU utilization, troubleshooting**
  - on FWSM, 143
  - on PIX Firewall, 95–98
- host block, 734**
- hosts, 985**
- HTTP inspection, Java filtering, 204**
- HTTPS, tasks performed on IDS MC, 885**
- hubs, capturing IPS traffic, 763**

---

- IBNSs (Identity-Based Network Services), 541–542, 555**
  - 802.1X statistics, displaying, 555–557
  - IEEE 802.1x framework, 542–545
    - standard operation, 544–545*
  - machine authentication, 566–567
    - PEAP, configuring, 567–570*
- ICMP (Internet Control Message Protocol), traffic inspection, 182**
- IDAPI (Intrusion Detection Application Programming Interface), 678**
- IDENT protocol, troubleshooting on PIX Firewall, 102**
- identifying registered CSA MC agents, 1008**
- IDIOM, 681**
- IDM (IPS Device Manager)**
  - IPS sensors, licensing, 719
  - sensors
    - accessing, 888, 901–902*
    - trusted hosts, adding, 890–892*
    - trusted hosts, configuring, 889–890*
- IDS MC**
  - Apache certificate
    - regenerating, 897*
    - trusted host issues, resolving, 897–898*
    - verifying, 896*
  - audit reports, 885
  - communication architecture, 884–885
  - configuration deployment, 917
    - troubleshooting, 918–920*

- configuring, best practices, 929
- corrupt licenses, troubleshooting, 904
- database pruning, 920
- debugging, 887–888
- device table, adding devices to, 1052
- expired licenses, troubleshooting, 905
- FAQs, 925–929
- installing, 902–903
- MDCSupport file
  - collecting on Windows platform, 886*
  - file contents, analyzing, 886–887*
- processes, starting/stopping, 884
- resolving connection problems with sensor, 893
- secure communication with sensor,
  - verifying, 893
- sensors
  - configuring, 906*
  - import process, troubleshooting, 907–908, 1051*
  - shunning, case study, 920–925*
  - updating signature level, 899–901*
  - upgrading, 908–917*
  - service pack version, verifying, 895–896
  - VMS Server, IP addressing, modifying, 898
- IDS Sensor Software, naming conventions, 700**
  - platform-dependent images, 700–701
  - platform-independent images, 701–702
- IdsAlarms.exe utility, 1076**
- IDSdbcompact utility, 1068**
- IDS M-2 (Intrusion Detection Services Module 2) blade**
  - Command and Control port
    - 5-minute output rate, checking, 803–805*
    - configuring, 801–803*
  - event generation, troubleshooting, 817–818
  - front panel indicator lights, 789
  - hardware issues, troubleshooting
    - on CatOS, 797–800*
    - on Native IOS, 793–797*
  - hardware requirements, 788
  - implementing, best practices, 829
  - installing, 789
  - Maintenance Partition, upgrading, 823–824
  - Promiscuous mode, 805
    - configuring, 805–813*
    - troubleshooting, 814–816*
  - re-imaging, 818–823
  - removing from switch, 790

- serial cable, connecting, 826
- signature update, installing, 824–825
- slot assignment, 788
- sniffing ports, 791
- supported ports, 790
- TCP reset, 818
- upgrading to version 5.x, 826
- user passwords, recovering, 827–829
- VACL Capture, 827
- versus IDS Appliance, 787
- IKE (Internet Key Exchange), 229**
  - phase 1, 229–232
  - phase 2, 232–233
- images**
  - for NM-CIDS, 849
  - upgrading on FWSM, 133–134
- implementing**
  - AAA on VPN 3K, best practices, 612
  - access lists on PIX Firewalls, 34–35
    - outbound ACLs, 35–36*
    - time-range keyword, 34–35*
  - disaster recovery plan, 707–709
  - IDS-2, best practices, 829
- importing**
  - CSA MC license, 1007–1008
  - device configurations
    - with Firewall MC, 943–946*
    - with Router MC, 969–970*
  - IDS sensors from IDS MC, 1051
    - troubleshooting, 907–908*
  - NAS to CS ACS database, 659
  - users to existing CS ACS database, 658
- inaccessible sensors, troubleshooting, 901–902**
- inbound connections, 69**
  - configuring on PIX Firewall, 69–72
- information logging level (Router MC), 961**
- ingress traffic, 764**
- initial IPS sensor setup problems, troubleshooting, 693–696**
- initialization problems, resolving**
  - on Firewall MC, 936
  - on Router MC, 964
- Inline Bypass sensor mode (IPS), 682**
- Inline mode (IPS sensor), 681–682**
  - configuring, 757–762
  - troubleshooting, 762–763
- inside network, protecting, 178–180**
- inspecting**
  - multi-channel protocols, 187
  - single channel protocols, 182
    - application-layer protocols, 183*
    - ICMP, 182*
    - SMTP, 183*
    - UDP, 182*
    - URL filtering, 185–187*
- installation failures on Router MC, troubleshooting, 963**
- installing. See also removing; uninstalling**
  - CiscoWorks Common Services, 870–871
    - database management, 873*
    - minimum requirements, 870*
    - problems, troubleshooting, 871–873*
    - user management issues, 873*
    - with Terminal Services in Remote Administration mode, 935*
  - CS ACS on Windows platform, 625–627
  - CSA MC
    - best practices, 1036*
    - license key, 869*
    - minimum requirements, 995*
    - problems, troubleshooting, 993–994*
  - CSAgent
    - minimum requirements, 998–999*
    - problems, troubleshooting, 997, 1001*
  - Firewall MC, 934
  - IDS MC, 902–903
  - IPS Sensor Appliances, 703
    - with CD-ROM, 703–704*
    - with TFTP server, 704–707*
  - ISDM-2 blade, 789
  - NM-CIDS, 833
  - Security Monitor, 1047
  - signature update on IDSM-2, 824–825
- integrating CS ACS**
  - with Novell IDS, 630–636
  - with AD, 627–629
  - with SDI, 636–639
- interfaces supported on IPS, 683– 685**
- intermittent packet drops on FWSM, troubleshooting, 144**
- Internal Server Error messages, troubleshooting, 1050**
- interoperability**
  - of Firewall MC with other applications, 936
  - of NAT and CBAC, 188



**inter-process communication, 678****intrusion-detection module command, 808****IOS Firewall feature set, 177**

- auth-proxy, 212
  - authentication methods, 212*
  - configuring, 213–215*
  - troubleshooting, 216–217*
- detecting with show version command, 200
- supported Cisco router platforms, 213

**IP addresses**

- assigning to IDS-Sensor interface, 839
- DNS errors, resolving, 1048
- on VMS Server, modifying, 898

**IP fragmentation, mitigating with CBAC, 191****IP inspection on CBAC routers, troubleshooting, 202****ip port-map command, 189****iplog command, 691****IPS (Intrusion Prevention System)**

- AnalysisEngine, 678
- best practices, 781–785
- capturing traffic
  - with MPLS IP IDS, 776–777*
  - with RSPAN, 773–775*
  - with SPAN, 763–770*
  - with VACL, 775–776*
- CLI, 678
- combined sensor mode, 683
- communication protocols, 678–681
- deployment architecture, 676–677
- FAQs, 777–781
- Inline Bypass sensor mode, 682
- Inline sensor mode, 681–682
- MainApp, 677–678
- monitoring device, troubleshooting event reception issues, 726–733
- NM-CIDS, 831
  - ACL checks, case study, 852*
  - application partition, re-imaging, 854–857*
  - available images, 849*
  - CEF forwarding path, case study, 850*
  - Command and Control port, configuring, 844–845*
  - connecting to, 840–842*
  - console access, 839, 843–844*
  - disconnecting from, 842–843*
  - dropped packets, case study, 853*

*encryption, case study, 852*

*front-panel indicator lights, 833*

*GRE tunnels, case study, 853*

*hardware issues, troubleshooting, 836–838*

*hardware/software requirements, 832*

*installing, 833*

*IPS insertion points, case study, 851*

*managing from IOS router, 848–849*

*NAT, case study, 851*

*network setup, 831*

*packet capturing, configuring, 846–848*

*removing from router, 833*

*slot assignment, 833*

*supported ports, 834–835*

*time stamp configuration, 857–858*

Promiscuous sensor mode, 682–683

sensors

*blocking function, verifying, 744–745*

*blocking issues, troubleshooting, 733–743, 753*

*configuration, backing up, 782–783*

*connecting to network, 784*

*connectivity issues, resolving, 720–725, 746–752*

*initial setup issues, 693–696*

*Inline mode, 757–763*

*MBS, 754*

*NAC function, verifying, 745–746*

*software installation/upgrade issues, 699–717*

*TCP reset, 754–757*

*upgrading to IPS 5.0, 715–717*

*user management issues, 696–698*

Sensor Appliances, installing, 703–707

show commands, 686–690

supported hardware and interfaces, 683–685

traffic, capturing, 763

**IPS 5.0, licensing, 717–720****IPsec**

aggressive mode negotiation, 231–232

AH, 226

backup servers, redundancy on VPN 3000

Concentrator series, 415

debug commands, 300

ESP, 226

firewall issues, troubleshooting, 284–285, 340

- GRE over IPsec
  - configuring*, 256–257
  - troubleshooting*, 257–258
- IKE, 229
  - phase 1*, 229–232
  - phase 2*, 232–233
- interaction with CBAC, 193
- IOS routers, VPN troubleshooting
  - debug commands*, 238
  - PKI*, 258–265
  - Remote Access client VPN connections*, 265–270
- LAN-to-LAN tunnels, 239
  - establishing*, 240–246
  - phase 1 establishment failures*, 247–251
  - phase 2 establishment failures*, 252–254
  - traffic flow, troubleshooting*, 254–255
- LAN-to-LAN VPN tunnels between PIX firewalls
  - configuring*, 302, 305–308
  - crypto maps, creating*, 305–306
  - data not passing through, troubleshooting*, 322–323
  - MTU issues*, 340–342
  - Phase I failures*, 309–319
  - Phase II failures*, 319–321
  - transform sets, creating*, 304
  - tunnel groups, creating*, 305
- main mode negotiation, 229–231
- MTU issues, troubleshooting, 285–286
- NAT-related problems, troubleshooting, 282–284
  - exemptions*, 338
- over NAT-T, configuring, 338–339
- over TCP, configuring, 339
- Phase 1 tunnel negotiations, show commands, 233–235
- Phase 2 tunnel negotiations, show commands, 235–236
- PKI
  - configuring*, 258–261
  - troubleshooting*, 261–265
- Remote Access VPNs on PIX firewall
  - configuring*, 323, 325–327
  - debug output for successful tunnel build-up*, 328–331
  - split tunneling*, 342–344
  - stateful failover, obtaining resiliency through*, 287–288
  - stateless failover, obtaining resiliency through*, 288–295
  - tunnel not passing through traffic*, 333–334
  - unestablished tunnels, troubleshooting*, 332–333
- SAs, 228
- split tunneling issues, troubleshooting, 286
- transparent tunneling options, 340
- transport mode, 226
- tunnel mode, 227–228
- tunnels,
  - tearing down*, 238
  - verifying configuration of*, 237

## J-K

- Java blocking, configuring on CBAC, 184**
- jobs (Firewall MC), rolling back, 942**
- Jonas logs, 963**

- keyed message digest, 225**
- Knoppix security CD, 21**

## L

- LAC routers, troubleshooting, 464–467**
- LAN-to-LAN IPsec VPN tunnels, 239**
  - configuring*, 302, 305–308
  - crypto maps, creating*, 305–306
  - data not passing through, troubleshooting*, 322–323
  - establishing*, 240–246
  - MTU issues*, 340–342
  - on VPN 3000 Concentrator series, troubleshooting*, 356–363
  - Phase 1 establishment failures, troubleshooting*, 247–251, 309–319
  - Phase 2 establishment failures, troubleshooting*, 252–254, 319–321
  - traffic flow, troubleshooting*, 254–255
  - transform sets, creating*, 304
  - tunnel groups, defining*, 305
- Large ICMP events, generating, 1057**
- launching**
  - CiscoWorks Common Services on web browser, 861

- CSA MC
  - problems, troubleshooting, 1010–1013*
  - slow launches, troubleshooting, 1013–1014*
- Event Viewer, 1055
- Security Monitor, 1050
- LED indicator lights,**
  - on Catalyst 6500 IDSM-2 blade, 789
  - on VPN 3000 Concentrator series, 354
  - on NM-CIDS, 833
- libpcap format files, 691**
- license keys (CSA MC), installing, 869**
- licensing**
  - for CiscoWorks Common Services, troubleshooting, 869
  - for CSA MC, 1005–1007
    - importing, 1007–1008*
    - troubleshooting, 1009–1010*
  - for FWSM, troubleshooting, 126–127
  - for IDS MC
    - corrupt licenses, troubleshooting, 904*
    - expired licenses, troubleshooting, 905*
  - for IPS software, 717–718
    - procuring license from Cisco.com, 718*
    - sensors, 719–720*
  - for PIX Firewall, 54–56
  - for VMS, 865–868
- limitations**
  - of ACLs, 177
  - of Virtual Firewall, 86
- LLQ (Low-Latency Queuing), configuring on PIX Firewall, 93–94**
- LNS (L2TP Network Server) routers, troubleshooting, 468–471**
- load balancing on VPN 3000 Concentrator series, 413**
- loading Event Viewer, 1057**
- local database installation (CSA MC), troubleshooting, 994**
- local group authentication, configuring on VPN 3K, 596**
- Local mode (CiscoWorks Common Services), 862**
- local user authentication, configuring on VPN 3K, 597–599**
- locking VPN 3K users to specific groups, 601**

- log directory**
  - CSA Agent files, 988
  - CSA MC, 986
- log events, viewing on VPN 3K, 589**
- log files**
  - CSA MC Log, 987
  - for CSA Agent, 988–992
  - securitylog.txt, writing events to, 991
  - size of, monitoring, 1065–1066
- “Logged in Users” report, 668**
- logging**
  - Event Limiting, 991
  - syslog configuration on PIX Firewall, 50–53
- logical PIX firewalls**
  - See Security Contexts*
- login authentication**
  - configuring, 559–560
  - troubleshooting, 561–562
- lost GUI passwords, recovering, 663**
- low memory issues, troubleshooting on PIX Firewall, 98–101**

---

## M

- machine authentication**
  - activating on Cisco switches, 566–567
  - PEAP, configuring, 567–570
- Main mode negotiation (IPsec), 229–231**
- MainApp, 677–678**
- Maintenance Partition (FWSM), 130–132**
- major/minor software, upgrading, 710**
  - to IPS 5.0, 716–717
- managed devices, troubleshooting connectivity with sensor, 746–752**
- Management Center, 985**
- management model for CSA, 983–985**
- managing NM-CIDS from IOS router, 848–849**
- man-in-the-middle attacks, 80**
- manipulating half-open connection threshold values on CBAC routers, 208**
- manual operations**
  - adding trusted hosts to IDM sensors, 892
  - performing backups on CSA MC database, 1023–1024
  - uninstalling CS ACS, 661

**MAPI Proxy (VPN 3000 Concentrator)**  
 configuring, 399–400  
 troubleshooting, 400–401

**mapping**  
 CS ACS group names to VPN 3K  
 group names, 598  
 NHRP issues, resolving, 278–279

**maximum event limit (database), changing, 1066**

**MBS (Master Blocking Sensor), 737**  
 configuring, 741–743  
 troubleshooting, 754

**MDCSUPPORT**

**MDCSupport, 863**  
 collecting on Windows platform, 886  
 contents, analyzing, 886–887  
 files collected by, 864

**MDCSupportInformation.zip file**  
 contents of, 933  
 file summary, 864  
 installation log files, 864

**memory utilization, troubleshooting on PIX Firewall, 98–101**

**memory.dmp file, 990**

**message digest, 225**

**messages, RADIUS, 427**

**mGRE interface, 271**

**minimum installation requirements**  
 CiscoWorks Common Services , 870  
 CSA MC, 995  
 CSAgent, 998–999

**misconfigured ACLs, troubleshooting on CBAC, 202**

**misconfigured IP inspection, troubleshooting on CBAC routers, 203**

**misconfigured URL filtering, troubleshooting, 205**

**mitigating**  
 IP fragmentation with CBAC, 191  
 TCP SYN flood attacks with CBAC, 189, 191

**mls ip ids command, 813**  
 configuring on switch running Native IOS, 809

**modifying**  
 application-to-port mappings, 188–189  
 IP addressing on VMS Server, 898

**monitoring**  
 database, disk utilization, 1066  
 devices, flow rates, 1064–1065

disk usage, 992  
 log files, size of, 1065–1066

**monitoring interface (NM-CIDS), 834**

**MPF (Modular Policy Framework), 37–38**

**MPLS IP IDS, configuring IPS traffic capture, 776–777**

**MSDE database**  
 compacting, 1030  
 repairing, 1031–1032

**MTU problems with IPsec, troubleshooting, 285–286, 340–342**

**multi-channel protocols**  
 inspecting, 187, 205  
 securing with CBAC, 180

**multi-homed machines, running CiscoWorks Common Services on, 879**

**multiple context mode (PIX Firewall), 84–90**

**multiple mode (FWSM), access list memory utilization, 164–166**

**multiple SVI interfaces, configuring on FWSM, 157–162**

## N

**NAC (Network Access Controller) function, verifying, 745–746**

**naming conventions**  
 after CSA MC upgrade, 1004  
 of IDS Sensor Software, 700  
*platform-dependent images, 700–701*  
*platform-independent images, 701–702*

**NARs (Network Access Restrictions)**  
 configuring, 648–651  
 troubleshooting, 651–652

**NAS (Network Access Server), 421, 639**  
 bulk importing, 667

**NAT (Network Address Translation)**  
 interoperability with CBAC, 188  
 troubleshooting on CBAC router, 202  
 with IPsec, 282–284

**NAT exemptions, 338**

**nat-control, implementing on PIX Firewall, 36**

**Native IOS**  
 IDSM-2, troubleshooting hardware issues, 793–797  
 show commands, 792

**NAT-T (NAT Traversal), configuring, 338–339**

**NBMA (Non-Broadcast Multiple Access), 271****network analyzers, 20****network failures**

- proactive troubleshooting methods, 5–7
- types of, 7

**network resources, protecting on PIX****Firewall, 111****NHRP (Next Hop Resolution Protocol), 271****NMBA addresses, 272****NM-CIDS (Cisco IDS Network Module), 831**

- application partition, re-imaging, 854–857
- case studies
  - ACL checks, 852*
  - CEF forwarding path, 850*
  - dropped packets, 853*
  - encryption, 852*
  - GRE tunnels, 853*
  - IP insertion points, 851*
  - NAT, 851*

Command and Control port, configuring, 844–845

console access, 839

console access, troubleshooting, 843–844

front-panel indicator lights, 833

hardware issues, troubleshooting, 836–838

hardware/software requirements, 832

images, 849

installing, 833

managing from Cisco IOS router, 848–849

network setup, 831

packet capture, configuring, 846–848

removing from router, 833

slot assignment, 833

supported ports, 834–835

time stamping configuration, 857–858

upgrading to version 5.0, 849

**Notifier daemon, 1055****Novell IDS, troubleshooting CS ACS****integration, 630–636****NPs (network processors)**

FWSM architecture, 114–116

NP3, access-list utilization on FWSM, 164–166

**NSDB (Network Security Database), 785**

viewing from Security Monitor, 1073

**nslookup command, 19****NT/RADIUS password authentication feature, testing, 610–611****O****obtaining**

Common Services software production license, 867

IPsec resiliency

*with stateful failover, 287–288*

*with stateless failover, 288–295*

**options for csutil.exe, 655–656****outbound connections, 69**

configuring on PIX Firewall, 69–72

**Output Interpreter, 54****P****Package.cab file, contents of, 622–624****packet capturing**

configuring on NM-CIDS, 846–848

on FWSM, 123–124

**packet command, 692****packet drops. troubleshooting**

on CBAC routers, 210

on FWSM, 144

**packet flows**

through CS ACS, 619–620

through FWSM, 116

*Fast Path packet flow, 116–118*

*FTP session packet flow, 118*

*Session Management packet flow, 118*

**packets, troubleshooting IPsec MTU issues, 285–286****Page Cannot Be Found Error messages (Security Monitor), 1050****PAM (Port Application Mapping), 188–189****Passed Authentication log, turning on, 621****Password Expiry, testing, 610–611****passwords**

encryption (CS ACS), 668

recovering

*from FWSM, 132*

*from IDSM-2, 827, 829*

*from PIX Firewall, 56–60*

**PEAP (Protected EAP)**

configuring, case study, 574–580

machine authentication, configuring, 567–570

**performance issues on CBAC, troubleshooting, 205–210**

**Perl directory (CSA MC), 986****Phase 1 tunnel negotiations**

- IPsec LAN-to-LAN VPN failures, 309–319
- show commands, 233–235

**Phase 2 tunnel negotiation**

- IPsec LAN-to-LAN VPN failures, 319–321
- show commands, 235–236
- tearing down tunnels, 238

**ping command, 17****pinging CBAC router incoming interface, 201****PIX firewalls**

- access lists
  - enabling/disabling, 35*
  - implementing, 34*
  - outbound, 35–36*
  - time-range keyword, 34–35*
- activation keys, 56
- ASA, characteristics of, 29–30
- commands
  - capture, 47–49*
  - debug application-protocol, 47*
  - debug fixup tcpudp, 47*
  - debug icmp trace, 46–47*
  - debug pix process, 47*
  - show asp drop command, 41–42*
  - show blocks, 43*
  - show connection command, 40*
  - show cpu usage command, 42*
  - show local-host command, 40–41*
  - show output filters, 44–45*
  - show service-policy command, 41*
  - show tech-support, 45*
  - show traffic, 42*
  - show xlate command, 39–40*
- connections
  - configuring, 69–72*
  - troubleshooting, 72–76*
- CPU utilization, troubleshooting, 95–98
- Downloadable PIX ACL, 653
- failover
  - active/active failover, configuring, 105–106*
  - active/standby failover, 102*
  - asymmetrical routing support, 106*
  - failover groups, 104*
  - hardware and licensing requirements, 104*
- FAQs, 109–110
- file system commands, 33

## Hairpinning, 334–337

- high availability on VPN connections, obtaining, 344–345

## IDENT protocol, troubleshooting on PIX Firewall, 102

## licensing issues, troubleshooting, 54–56

## memory utilization, troubleshooting, 98–101

## MPF, 37–38

## multiple context mode, configuring, 87–90

## nat-control, configuring, 36

## packet processing, 30–32

## password recovery issues, troubleshooting, 56–60

## protecting network resources, best practices, 110–111

## QoS issues, troubleshooting, 90, 92–94

## Remote Access VPNs

*configuring, 323, 325–327**debug output for successful tunnel**build-up, 328–331**tunnel not passing through traffic,**333–334**unestablished tunnels, troubleshooting,**332–333*

## Security Contexts, 84

*multiple context mode, 84–86*

## software upgrade/downgrade issues, troubleshooting, 60–68

## syslog, 50–53

## tools, 53

## traceback, 53

## Transparent Firewall, 38–39, 78

*configuring, 79–82**troubleshooting, 82–83*

## Virtual Firewall, 84–86

**PKI**

## configuring, 258–259, 261

## troubleshooting, 261–265

**platform-dependent images, naming conventions, 700–701****platform-independent images, naming conventions, 701–702****policies, 985–987****Policies directory (CSA MC), 986****policing, configuring on PIX Firewall, 90–92****polling issues with CSA MC, troubleshooting, 1014–1015**

- port forwarding, VPN 3000 Concentrator**
  - configuring, 396–397
  - troubleshooting, 397–399
- port-level authentication, 542**
- ports**
  - ISDM-2 switch support, 790
  - mapping information, changing, 188–189
  - NM-CIDS, configuring Command and Control interface, 834–835, 844–845
- Post-Block ACL, 735**
- Pre-Block ACL, 734**
- privilege levels, assigning to VPN 3K users, 592**
- proactive troubleshooting methods, 5–7**
- processes running**
  - on Firewall MC, 931
  - on IDS MC, 884
  - on Router MC, 959
  - on SecMon, 884
- procuring**
  - CSA MC license, 1007
  - CSAgent license, 1007
  - CSAgent software, 997–998
  - IPS 5.0 license from Cisco.com, 718
- production license for Common Services software, obtaining, 867**
- production network failures, 8, 12–13**
  - defining the problem, 9–10
  - gathering the facts, 10–11
- Profiler, 1022**
- Promiscuous mode (IDSM-2), 805**
  - configuring, 805
    - on switch running CatOS, 810–813*
    - on switch running Native IOS, 806–809*
  - troubleshooting, 814–816
- Promiscuous sensor mode (IPS), 682–683**
- protecting**
  - inside network, 178–180
  - PIX Firewall, best practices, 110–111
- protocol analyzers, 20**
- pruning**
  - IDS MC database, 920
  - troubleshooting, 1067–1068
- public key algorithms, 224**
- purge-mc-tasks utility, 942**
- purging CSA MC database, 1028–1029**

## Q–R

---

- QoS, 90**
  - LLQ, configuring on PIX Firewall, 93–94
  - policing, PIX Firewall configuration, 90–92
- RADIUS, 425–426, 609**
  - authentication operation, 426–427
  - authorization operation, 426–427
  - configuring on Cisco IOS routers, case study, 462–463
  - dynamic filters, configuring, 604
  - group authentication, configuring on VPN 3K, 599–600
  - user authentication, configuring on VPN 3K, 596–597
  - versus TACACS+, 428–429
- rcp, generating core dumps, 23**
- RDEP (Remote Data Exchange Protocol), 1041**
- RDEP2, 679**
- real-time alerts, configuring, 192–193**
- reclaiming disk space, 1011**
- records, pruning from IDS MC database, 920**
- recover application-partition command, 709**
- recovering**
  - application partition, 708–709
  - lost GUI passwords, 663
  - user passwords from IDSM-2, 827–829
- recovering lost passwords**
  - from FWSM, 132
  - from GUI, 663
  - from PIX Firewall, 56–60
- recovery packages, 702**
- Recovery Server (Firewall MC)**
  - configuring, 953–954
  - enabling, 954
- redirecting archive/backup files away from Database Disk, 1063**
- redundancy**
  - failover
    - active/active failover, configuring, 105–106*
    - active/standby failover, 102*
    - configuring on FWSM, 149–155*
    - monitoring on FWSM, 147–148*
    - troubleshooting on FWSM, 144, 146–147, 155–157*

- on VPN 3000 Concentrator series
  - clustering, 412–414*
  - using IPsec Backup Servers, 415*
  - using VVRP, 410–411*
- Reflexive ACLs, 180**
- regenerating Apache certificates, 897**
- registered CSA MC agents, identifying, 1008**
- registering CSA MC, 868**
- re-imaging**
  - ISDM-2, 818–823
  - NM-CIDS application partition, 854–857
- Remote Access VPN connections**
  - on PIX firewall, troubleshooting, 323–327
    - debug output for successful tunnel build-up, 328–331*
    - MTU issues, 340–342*
    - tunnel not passing through traffic, 333–334*
    - unestablished tunnels, 332–333*
  - on VPN 3000 Concentrator series,
    - troubleshooting, 364–371
      - client routing, 377–381*
      - Internet inaccessibility, 381–382*
      - local LAN inaccessibility, 382*
      - tunnel establishment, 372–377*
    - split tunneling, configuring, 342–344
- remote database installation (CSA MC), troubleshooting, 994**
- removing**
  - CSA MC components, 995–997
  - CSAgent from Windows systems, 999–1000
  - ISDM-2 blade from switch, 790
  - NM-CIDS from router, 833
  - terminal activities from Firewall MC, 941–942
- repairing CSA MC database, 1031–1032**
- replication, 640**
  - Bidirectional, 647
  - “cascade”, 645
  - CS ACS
    - configuring, 640, 644*
    - troubleshooting, 644–647*
  - of dynamically mapped users, 670
- REPLY packets (TACACS+), 422**
- reports**
  - daily alarm reports, scheduling, 1073
  - generation failures, troubleshooting, 1060
  - pruning reports, 1067
  - Router MC, 963
- resolving**
  - connection problems between IDS MC and sensor, 893
  - CS ACS Crypto Errors, 661
  - DNS errors, 1048
- restoring**
  - CiscoWorks Common Services, 875–876, 950
  - CSA MC database, 1025–1027
    - data, 657
    - Router MC database, 973
- Roles, 862**
- rollback feature (Firewall MC), 942**
- Router MC**
  - ACS, setup procedures, 979–980
  - authentication problems, resolving, 967
  - backup/restore operations, troubleshooting, 973
  - browser issues, troubleshooting, 965, 967
  - checking status of, 960
  - communication architecture, 960
  - dangling connections, 968
  - database
    - backing up, 972*
    - restoring, 973*
  - debug information, collecting/viewing, 961–962
  - device configurations
    - deploying, 970–971*
    - importing, 969–970*
  - features, 960
  - installation failures, troubleshooting, 963
  - logging levels, setting, 961
  - processes, 959
  - reports, 963
  - user permissions, case study, 974–975, 978
- RRI (Reverse Route Injection), 345**
- RSPAN (remote SPAN), configuring IPS traffic capture, 773–775**
- rules**
  - CSA MC, 985
  - database/event, creating, 1064
  - for dynamic filters, syntax, 603
- Rx SPAN, 764**



## S

**Samples directory (CSA MC), 986**

**SAs, 228**

**saving crash information to Flash on PIX**

**Firewall, 53**

**scheduling daily alarm reports, 1073**

**SDEE (Security Device Event Exchange),  
679–680, 1041**

**SDI (Secure ID), CS ACS integration, 636– 639**

**SecMon**

database Pruning, 920

processes, starting/stopping, 884

**security administrators, 984**

**Security Contexts, 84**

multiple context mode, 84– 90

**Security Monitor**

best practices, 1077

database maintenance issues,  
troubleshooting, 1062

DNS errors, resolving, 1048

email notification

*configuring, 1068–1070*

*troubleshooting, 1071–1072*

Event Viewer

*launching, 1055*

*troubleshooting, 1057*

inability to launch, troubleshooting, 1050

inability to receive events, troubleshooting, 726,  
728–733

installation guidelines, website, 1047

Internal Server Error messages,  
troubleshooting, 1050

licensing issues, troubleshooting, 1051

NSDB, viewing, 1073

Page Cannot Be Found Error messages,  
troubleshooting, 1050

report generation failures, troubleshooting,  
1060

sensor connection status, troubleshooting,  
1053–1055

strange behavior, troubleshooting, 1051

tabs, 1048

user management, 1045

**securitylog.txt file, writing events to, 991**

**selecting**

slot for ISDM-2 placement, 788

traffic capture method on IDSM-2, 827

UDP connection timeout for CBAC, 207–208

**sensor modes**

combined modes, 683

Inline Bypass mode, 682

Inline mode, 681–682

Promiscuous mode, 682–683

**sensors**

active processes, verifying, 893–895

blocking

*for specific signatures,*

*troubleshooting, 753*

*process, verifying, 923–924*

connectivity, 721–725

IDM

*accessing, 888*

*trusted hosts, adding/configuring,  
889–892*

IDS, importing from IDS MC, 1051

IDS MC

*configuring, 906*

*deploying, 917–920*

*import process, troubleshooting, 907–908*

*shunning, case study, 920–925*

*upgrade process, troubleshooting,  
908–917*

inaccessibility, troubleshooting, 901–902

IPS, troubleshooting

*ACLs, 734–735*

*backing up configuration, 782–783*

*blocking, 734–745*

*connecting to network, 784*

*connectivity with managed device,  
746–752*

*initial setup issues, 693–696*

*Inline mode, configuring, 757–762*

*Inline mode, troubleshooting, 762–763*

*MBS, 737, 741–744*

*software installation/upgrade issues,  
699–717*

*supported managed devices and  
versions, 735*

*TCP reset, 754–757*

*user management issues, 696–698*

- licensing, 719–720
  - with CLI*, 719–720
  - with IDM*, 719
- resolving connection problems with
  - IDS MC, 893
- signature level, updating, 899–901
- upgrading to IPS 5.0, 715–717
- verifying secure communication with
  - IDS MC, 893
- serial cable, connecting to IDSM-2 blade, 826**
- server selftest information, displaying, 988**
- service packs, IDS MC**
  - upgrading sensors, 908–910
  - verifying version of, 895–896
- service-module command, connecting to NM-CIDS, 840**
- services, CSAdmin, 615–616**
- Session Management packet flow through FWSM, 118**
- Shared File Components (CS ACS), 653–654**
- Shared Profile (command authorization), configuring, 444**
- shims, disabling, 1016–1017**
- show aaa servers command, 430**
- show aaa user command, 430**
- show access-list command, 655**
- show accounting command, 554**
- show asp drop command, 41–42**
- show authorization command, 554**
- show blocks command, 43**
- show commands**
  - for IPsec Phase 1 tunnel negotiations, 233–235
  - for IPsec Phase 2 tunnel negotiations, 235–236
  - for Native IOS, 792
  - FWSM-related, 120–122
- show configuration command, 687**
- show connection command, 40**
- show cpu usage command, 42**
- show crypto ipsec command, 299–300**
- show crypto map command, 237**
- show dot1x all command, 556**
- show dot1x statistics command, 557**
- show events command, 687**
- show interfaces command, 689**
- show ip inspect command, 194–195**
- show local-host command, 40–41**
- show localusers command, 552**
- show module command, 791**
- show output filters command, 44–45**
- show radius command, 553**
- show radius statistics command, 430**
- show running config command, 15**
- show running logging command, 52**
- show running-config command, 300**
- show security acl command, 792**
- show service-policy command, 41, 94**
- show span command, 792**
- show statistics command, 687–688**
- show tacacs command, 430, 553**
- show tech-support, 45**
- show tech-support command, 689**
- show test command, 792**
- show traffic command, 42**
- show trunk command, 792**
- show users command, 430**
- show version command, 15, 686–687, 689–690, 791**
  - verifying installed IOS Firewall feature set, 200
- show vlan brief command, 558**
- show xlate command, 39–40**
- shunning on IDS MC sensor, case study, 920–925**
- signature levels, updating on IDS MC sensors, 899–901**
- signature updates, installing on IDSM-2, 824–825**
- signatures, IDS MC**
  - upgrading IDS MC sensors, 908–910
  - verifying version of, 895–896
- single channel protocol**
  - inspection
    - application-layer*, 183
    - ICMP*, 182
    - SMTP*, 183
    - UDP*, 182
  - securing on inside network, 179–180
- single-mode (FWSM), access list memory utilization, 164–166**
- size of log files, monitoring, 1065–1066**
- slot assignment of NM-CIDS on router, 833**
- slow CSA MC launches, troubleshooting, 1013–1014**
- SMTP**
  - email notification
    - configuring*, 1068–1070
    - troubleshooting*, 1071–1072
  - traffic inspection, 183–184

**sniffer software, 49**

Ethereal, 199

**sniffer traces, capturing, 199****sniffing ports on IDS/IDSM-2, 791****software**installation/upgrade problems (IPS),  
troubleshooting, 699–717**requirements***for ISDM-2 blade, 788**for NM-CIDS support, 832*upgrade/downgrade issues, troubleshooting on  
PIX Firewall, 60–61,  
63–66, 68**Software Advisor Tool, verifying correct IOS****Firewall version, 200****source port, 764****SPAN (Switched Port Analyzer)****configuring***on Catalyst 2900/3600XL, 765–767**on Catalyst 2950/3550 and 3750, 767–770**on Catalyst 4000/6000 running CatOS,  
770–771**on Catalyst 4000/6000 running Native  
IOS, 771–772**on switch running CatOS, 810**on switch running Native IOS, 806–807***IPS traffic capture, configuring, 763, 765***on Catalyst 2900/3500XL, 765, 767**on Catalyst 2950, 767–770**on Catalyst 3550, 767–770**on Catalyst 3750, 767–770***SPI (security parameter index), 228****split tunneling**

configuring, 342–344

troubleshooting, 286

**spoke-to-spoke tunnels, creating, 275****SQL Server 2000, compacting, 1031****SSH, tasks performed on IDS MC, 885****SSL**

CSA MC communication architecture, 987

enabling, 1049

**SSL VPN**

clientless mode, 390

*configuring, 390**troubleshooting, 391–395***thick client mode***configuring, 402–403**troubleshooting, 403–405***thin client mode, 395–396***E-mail Proxy, configuring, 401**E-mail Proxy, troubleshooting,  
401–402**MAPI Proxy, configuring,  
399–400**MAPI Proxy, troubleshooting,  
400–401**port forwarding, 397–399***START packets (TACACS+), 422****starting IDS MC/SecMon processes, 884****stateful failover**

for VPN connections, 345

obtaining IPsec resiliency, 287–288

**stateless failover, obtaining IPsec resiliency,  
288–295****static ACLs, established keyword, 180****status indicator lights**

IDS/IDSM-2, 789

NM-CIDS, 833

**status of Router MC processes, checking, 960****stopping**

CSAgent service, 991

deployed jobs, 942

**supplicant, 542****supported tokens on VPN 3K, 604****suspending NM-CIDS sessions, 842****switch management, 558****accounting***configuring, 565**troubleshooting, 566***authorization***configuring, 564–565**troubleshooting, 565*

enable password authentication,

*troubleshooting, 562–564*

login authentication, troubleshooting, 559–562

**switching path on CBAC, troubleshooting****performance issues, 209****symmetric cryptographic algorithms, 224****syntax**

for database backups, 656

for downloadable PIX/IP ACLs, 606

for dynamic filter rules, 603

rtrformat utility, 990

syslogs, 21  
 activating on Cisco routers, 193  
 configuring on PIX Firewall, 50–53  
 on FWSM, 125  
**System Image, re-imaging IDSM-2, 818–823**  
**system images, upgrading to IPS 5.0, 716**  
 sysvars.cf file, 991

## T

**tabs, Security Monitor, 1048**  
**TACACS+, 421**  
 AAA packet flows, 422–423  
 accounting operation, 424  
 authentication operation, 422–423  
 authorization operation, 424  
 configuring on VPN 3K, 590–592  
 versus RADIUS, 428–429  
**TCP reset, 754–757**  
 on IDSM-2, 818  
**TCP SYN flood attacks, mitigating with CBAC, 189–191**  
**tcpdump command, 690**  
**tearing down IPsec tunnels, 238**  
**telnet, connecting to NM-CIDS, 841–842**  
**telnet command, 18**  
**terminating CSAgent service, 991**  
**test events, generating on Event Viewer, 1057**  
**testing**  
 authentication, 593–594  
 core dump setup, 24  
 NT/RADIUS password expiration feature, 610–611  
**TFTP, 20**  
 generating core dumps, 22  
**Thick Client SSL VPN mode (VPN 3000 Concentrator series)**  
 configuring, 402–403  
 troubleshooting, 403–405  
**Thin Client SSL VPN mode (VPN 3000 Concentrator series), 395–396**  
**“time exceeded” error messages, 18**  
**time stamping on NM-CIDS, configuring, 857–858**  
**time-range command, 34–35**  
**Tmp directory (CSA MC), 986**  
**tomcat logs, 962**  
**traceback, configuring on PIX Firewall, 53**  
**traceroute command, 18**  
**traffic capture method on IDSM-2, configuring**  
 with mls ip ids command, 813  
*on switch running Native IOS, 809*  
 with SPAN  
*on switch running CatOS, 810*  
*on switch running Native IOS, 806–807*  
 with VACL  
*on switch running CatOS, 811*  
*on switch running Native IOS, 807–809*  
**traffic filtering, ACLs**  
 limitations of, 177  
 wide holes, 181  
**traffic inspection**  
 of multi-channel protocols, 187  
 of single channel protocols, 182  
*application-layer protocols, 183*  
*ICMP, 182*  
*SMTP, 183*  
*UDP, 182*  
**transform sets, 325**  
 creating, 304  
**translation details, displaying for PIX Firewall, 39–40**  
**transparent firewalls, 38–39, 193**  
 configuring, 79–82, 193  
 troubleshooting on PIX Firewall, 78, 82–83  
**transparent tunneling options, 340**  
**transport mode, 226**  
**trusted hosts**  
 adding to IDM sensors, 890–892  
 configuring on IDM sensors, 889–890  
**tunnel groups, VPN 3K, 326**  
 attributes, 589  
 authentication, 588–589  
 defining for LAN-to-LAN tunnels, 305  
**tunnel mode, 227–228**  
**turning off**  
 debugging, 555  
 Passed Authentication log, 621  
**turning on CSA Agent debug mode, 989**  
**Tx SPAN, 765**

## U

### UDP

- connection timeout, selecting, 207–208
- traffic inspection, 182, 203–205

### uninstalling. *See also removing*

- CS ACS, 661
- CSA MC, 995

### Unknown User Policy, configuring, 609–610

### unlocking Firewall MC activities, 941

### updating

- CSAgent, 1004–1005
- signature level on IDS MC sensors, 899–901

### upgrading

- Cisco IOS code base on CBAC routers, 209
- CiscoWorks Common Services license, 868
- CS ACS on Windows platform, 625–626
- CSA MC, 1002
- CSA MCL

*on same system, 1002–1003*

*on separate system, 1003–1004*

### IDS MC sensors, 908–910

*failures, troubleshooting, 910–917*

### IDS-2 to version 5.x, 826

### IPS Sensor Appliances, 703

*with CD-ROM, 703–704*

*with TFTP server, 704–707*

### Maintenance Partition on IDS-2, 823–824

### Major/Minor Software, 710

### NM-CIDS, 849

### PIX Firewall, 61–63

*in failover setup, 68*

*ROM Monitor mode, 63–66*

### Router MC, troubleshooting failures, 963

### to IPS 5.0, 715–717

### URL filtering

- activating, 186
- configuring on CBAC, 185–187
- on CBAC routers, troubleshooting, 211
- troubleshooting, 205

### user attributes (VPN 3K), 589

### user authentication

- on CiscoWorks Common Services, case study, 876–877
- on VPN 3K, 588–589
- with RADIUS, configuring, 596–597

### user management

- on CiscoWorks Common Services, 862, 873
- on IPS, troubleshooting, 696–698
- on Security Monitor, 1045

### user passwords, recovering from IDS-2, 827–829

### user permissions on Router MC, case study, 974–975, 978

### users, deleting

- in multiple groups, 669
- on CS ACS, 659

### utilities

- csutil.exe
  - arguments, 655–656*
  - syntax, 655*
- IdsAlarms.exe, 1076
- IDSdbcompact, 1068
- MDCSUPPORT, 863–864
- purge-mc-tasks, 942

## V

### VACLs (VLAN ACLs)

- blocking, 736
- configuring
  - on switch running CatOS, 811*
  - on switch running Native IOS, 807–809*
- IPS traffic capture, configuring, 775–776

### VACL Capture (IDS-2), 827

### verifying

- active processes on sensors, 893–895
- Apache certificate on IDS MC, 896
- blocking process configuration on sensors, 744–745, 923–924
- CBAC CPU utilization, 205–206
- core dump configuration, 24
- Firewall MC installation, 934
- IPsec tunnel configuration, 237
- NAC function, 745–746
- network connectivity with ping command, 17
- Router MC installation, 963
- secure communication between IDS MC and sensor, 893
- service pack version on IDS MC, 895–896
- version of IDS MC, 895–896

**viewing**

- event log on VPN 3000 Concentrator series, 350–352
- Firewall MC debug information, 932
- log events on VPN 3K, 589
- NSDB from Security Monitor, 1073
- processes on IDS MC/SecMon, 884
- Router MC debug information, 961–962

**Virtual Firewall, 84–86****Virtual Reassembly option (IOS Firewalls), 191****VMS (VPN/Security Management Solution)**

- CiscoWorks Common Services
  - backing up, 874–875*
  - FAQs, 877–881*
  - installing, 870–873*
    - problems, troubleshooting, 871–873
    - user management issues, 873
  - managing, best practices, 881*
  - restoring, 875–876*
  - running on mult-homed machines, 879*
  - user authentication, case study, 876–877*
- licensing issues, 865–866
  - obtaining Common Services production license, 867*
  - upgrading Common Services license, 868*

**VMS Server, modifying IP addressing, 898****VPDNs (Virtual Private Dial-up Networks)**

- LAC router, troubleshooting, 464–467
- LNS router, troubleshooting, 468–471
- on Cisco IOS routers, case study, 458–462
- troubleshooting on Cisco IOS routers, case study, 464–472

**VPN 3000 Concentrator series**

- AAA
  - session timeouts, avoiding, 593*
  - TACACS+, configuring, 590–592*
- Administer Sessions window, 352
- authentication, 590
  - causes of failure, 607–608*
- FAQs, 406–410
- Cisco Secure ACS server, configuring, 590–591
- communicating with CS ACS RADIUS server, 597–599
- concentrator management, 587
- configuration files, 354
- CRSHDUMP.TXT file, 354

## Digital Certificates, 383–384

- on VPN client, 382–383*
- troubleshooting, 384–389*

## dynamic filters, configuring, 602

## E-mail Proxy

- configuring, 401*
- troubleshooting, 401–402*

## event classes, configuring, 348

## event log, viewing, 350–352

## failure, causes of, 607

## group authentication with RADIUS, configuring, 599–600

## group configuration, 608

## group names, mapping to CS ACS group names, 598

## LAN-to-LAN tunnel issues

- configuring, 356*
- troubleshooting, 359–63*

## LED indicators, 354

## local group and user authentication, configuring, 595–596

## local user authentication, configuring, 597–599

## log events, viewing, 589

## MAPI Proxy

- configuring, 399–400*
- troubleshooting, 400–401*

## port forwarding

- configuring, 396–397*
- troubleshooting, 397–399*

## privilege levels, assigning to users, 592

## RADIUS Server, configuring, 609

## redundancy

- using clustering, 412–414*
- using IPsec Backup Servers, 415*
- using VVRP, 410–411*

## Remote Access VPN connections

- configuring, 364–365*
- troubleshooting, 365–382*

## SSL VPN

- clientless mode, 390–395*
- Thick Client mode, 402–405*
- thin client mode, 395–396*

## supported tokens, 604

## tunnel group authentication, 588–589

## user authentication, 588–589

- with RADIUS, configuring, 596–597*

users, locking to specific group, 601  
VPN client log, 354–355  
X-Auth, troubleshooting, 594–596

#### **VPNs**

on Cisco IOS routers, DMVPN, 270–280  
stateful failover, 345  
transparent tunneling options, 340

**VRRP (Virtual Router Redundancy Protocol),  
redundancy on VPN 3000 Concentrator series,  
410–411**

## **W**

---

#### **web browsers**

CiscoWorks Common Services, launching, 861  
on Firewall MC, troubleshooting, 937  
on Router MC, troubleshooting, 965–967

#### **websites**

Ethereal, 20  
Knoppix tool, 2  
Security Monitor installation guidelines, 1047

**well-known ports, changing port-to-application  
mappings, 188–189**

**wide holes, 181**

#### **Windows operating system**

CS ACS  
    *installing, 625–627*  
    *related registries, 663*  
CSAgent, removing, 999–1000  
IDS MC  
    *MDCSupport file, 886–887*  
    *MDCSupport file, collecting, 886*  
system information, displaying, 988

**Windows NT/2000 Domain Authentication,  
configuring Unknown User Policy, 609–610**

**winmsd command, 988**

**worry state, IKE keepalives, 345**

## **X-Y-Z**

---

**X-Auth, troubleshooting, 594–596**

    on Cisco routers, 457

**XML parser, 1044**