INDEX

A

AAA, implementing, 27–28
access
  to ASA/PIX Security Appliance
    monitoring, 150–151
    securing, 147–150
  to websites, blocking, 153–155
access control, 30
access policies, creating for web and mail servers, 139–142
access rules, 167
  HTTPS, adding, 167–168
accounting, 146
ACLs
  enabling/disabling, 240
  Ethernet types, filtering, 239
  time-based enabled, 238–239
advanced ASA/PIX version 7 features
  authentication enhancements, 237
    accounting records, 238
    simultaneous RADIUS accounting servers, 237–238
  general security appliance enhancements, 247–249
  IPS enhancements, 240–241
    configurable security appliance inspections, 242
    ESMTP command filtering, 242
    FTP command filtering, 242
    HTTP deep packet inspection, 242
    ICMP inspection, 241
  perimeter protection enhancements, 238
    ACLs, enabling/disabling, 240
    ACLs, enforcing Ethernet types, 239
    granular outbound access rules, 239
    time-based enabled ACLs, 238–239
  security management, 243–245
  VPN enhancements, 245–246
Anti-Spoofing configuration, 170
application firewall features, 31
application inspection, 42–43, 160–162
  customizing, 162–164, 166
ASA 5510 Security Appliance, 45
ASA 5520 Security Appliance, 45
ASA 5540 Security Appliance, 45
ASA/PIX Security Appliance
  AAA features, 151
  Anti-Spoofing configuration, 170
  application inspection, 161–162
    customizing, 162–166
  authentication for inbound and outbound services, 151–153
  booting, 48
  configuring, 117–123
    with ASDM, 135–141
  connecting web and mail servers, 134–135
  connecting with ASDM, 110–116
  console ports, 47
  Ethernet ports, 46
  failover ports, 47
  hardening, 26
  inspected protocols, 160
  inspections, 159
  installing, 46
  intrusion prevention, 176
    deploying, 179–180
  IP Audit, signatures, 177–179
  licenses, 55–56
    license key, installing, 56
  monitoring access to, 150–151
  PIX 515E, 44
  PIX 525, 44–45
  PIX 535, 45
  power, installing, 47
  securing access to, 147–150
  security management, 36–37
    syslog reporting system, 38
  troubleshooting, 48
  version 7. *See also* ASA/PIX version 7 advanced features
    accounting records, 238
    authentication enhancements, 237–238
    general security appliance enhancements, 247–249
    IPS enhancements, 240–242
    operating system, reinstalling, 251

perimeter protection, 238–240
security management, 243–245
VPN
enabling, 210–216
enhancements to, 245–246
NAT connectivity, configuring, 219
verifying connectivity, 217–218
ASA/SSM, supported IPS features, 176
ASDM (Adaptive Security Device Manager), 59
ASA/PIX Security Appliance configuration, 135–141
ASA/PIX Security Appliance, configuring, 117–123
connecting to ASA/PIX Security Appliance, 110–116
GUI, 59
launching, 113–116
monitoring VPN client connections, 220–221
navigation bar, 69–71
Configuration icon, 72–93
Home navigation icon, 71–72
Monitor Navigation icon, 94–97
pull-down menus, 61–62
ASDM Wizards menu, 68
File menu, 62–64
Help menu, 68–69
Options menu, 65–66
Rules menu, 64
Search menu, 64–65
Tools menu, 66–68
starting, 60
Startup Wizard, 105
version 5.0, 244
installing, 256–257
Wizards menu, 68
ASDM Launcher, 114
authentication
best practices, 228
customer access service policies, deploying, 230
enhancements for ASA/PIX version 7
accounting records, 238
simultaneous RADIUS accounting servers, 237–238
for inbound and outbound services, 151–153
passwords
best practices, 229
creating, best practices, 37
purpose of, 146
authentication layer, deploying defense in depth, 21–22
authorization, 145
auto-update feature (ASA/PIX version 7), 244
AYT (“are you there”) functionality, 232

B

Back arrow navigation button (ASDM navigation bar), 97
behavior rules engine, 33
best practices
for authentication, 228
passwords, 229
for defense in depth deployment, 24–25
for event logging, 233–234
for host intrusion prevention, 231
for intrusion prevention, 231
for Layer 2 security, 227–228
for perimeter security, 229–230
for VPNs, 231–233
blocking access to websites, 153–155
booting ASA/PIX Security Appliance, 48
buttons (ASDM navigation bar)
Back arrow navigation button, 97
Forward arrow navigation button, 97
Help navigation button, 99
Refresh navigation button, 98
Save navigation button, 98
Search navigation button, 97–98

C

Cisco ACS (Access Control Server), authentication best practices, 228–229
Cisco ASA 5510 Security Appliance, 45
Cisco ASA 5520 Security Appliance, 45
Cisco ASA 5540 Security Appliance, 45

Class A addresses, 108
Class B addresses, 108
Class C addresses, 108
classes of websites, blocking, 153–155
configurable security appliance inspections, 242
Configuration icon (ASDM navigation bar), 72–73
Building Blocks panel, 84
Device Administration panel, 85–88
Interfaces panel, 74
NAT panel, 77–79
Properties panel, 89–93
Routing panel, 82–83
Security Policy panel, 74–77
VPN panel, 79–82
configuring
ASA/PIX Security Appliance, 117–123
with ASDM, 135–141
NATed VPN connectivity, 219
network topology, 132–133
VPNs
PC client, 216–218
on ASA/PIX Security Appliance, 210–216
connecting
to ASA/PIX Security Appliance with ASDM, 110–116
web and mail servers to ASA/PIX Security Appliance, 134–135
connectivity of VPNs, verifying on ASA/PIX Security Appliance, 217–218
console ports, ASA/PIX Security Appliance, 47
creating
access policy for web and mail servers, 139–142
HTTPS access rule, 167–168
passwords, best practices, 37, 229
CSA (Cisco Security Agent), 24
customer access service policies, deploying, 230
customizing protocol inspections, 162–166

D

day-zero attacks, 24, 142
default gateway address, 108
defense-in-depth, 21
AAA, implementing, 27–28
deploying
at authentication layer, 21–22
at host intrusion prevention layer, 23–24
at perimeter layer, 22
NIPSs, 23
security best practices, 24–25
perimeter security, implementing, 28–31
defining
private network addresses
for DMZ interface, 131–132
for web servers, 132
public addresses for web servers, 132
deploying
defense in depth, 21
at authentication layer, 21–22
at host intrusion prevention layer, 23–24
at perimeter layer, 22
NIPSs, 23
security best practices, 24–25
intrusion prevention on ASA/PIX Security Appliance, 179–180
devices
ASA/PIX Security Appliance, hardening, 26
hosts, hardening, 26–27
limiting access to, 30–31
network device hardening, 25
routers, hardening, 25–26
switches
hardening, 26
security best practices, 227–228
DHCP (Dynamic Host Configuration Protocol), 109
DMZ (demilitarized zone) interfaces, 31, 42
private network address, defining, 131–132
DNS (Domain Name Service), 109
command filtering, 243
DNSGuard, 169
DoS attacks
mitigating, 29, 169
protecting against, 168–169
Anti-Spoofing configuration (ASA/PIX Security Appliance), 170
resource-intensive, protecting against, 170–172
downloading ASA/PIX version 7 OS from TFTP, 252–256

E

enabling IP Audit on an interface, 181–184
ESMTP command filtering, 242
establishing connectivity to ASA/PIX Security Appliance with ASDM, 112–113
Ethernet ports, ASA/PIX Security Appliance, 46
event logging best practices, 233–234
Event Monitor, 233

F

failover, 44
failover ports, ASA/PIX Security Appliance, 47
false positives, 32
File menu (ASDM), 62–64
firewalls, perimeter best practices, 229–230
flat networks, 109
FloodGuard, 30, 169
Forward Arrow navigation button (ASDM navigation bar), 97
FragGuard, 30, 169
FTP command filtering, 242

G

general security appliance enhancements, 247–249
global event correlation engine, 34
granular outbound access rules, 239
graphing VPN tunnel statistics, 221
GUI (ASDM), 59

H

hacker sites, 154
hardening Cisco network devices
- ASA/PIX Security Appliance, 26
- hosts, 26–27
- routers, 25–26
- switches, 26

Help menu (ASDM), 68–69
Home navigation icon (ASDM navigation bar), 71–72, 99
host intrusion prevention, 32–35
- best practices, 231

host intrusion prevention layer, deploying defense-in-depth, , 23–24
hosting web and mail servers on ISP, 130
hosts, hardening, 26–27
HTTP deep packet inspection, 242
HTTPS, creating access rules, 167–168

I

ICMP inspection, 241
icons (ASDM navigation bar)
- Configuration icon, 72–73
  - Building Blocks panel, 84
  - Device Administration panel, 85–88
  - Interfaces panel, 74
  - NAT panel, 77–79
  - Properties panel, 89–93
  - Routing panel, 82–83
  - Security Policy panel, 74–77
  - VPN panel, 79–82
- Home Navigation icon, 71–72
- Monitor Navigation icon, 94
  - Administration Monitor panel, 96
  - Connection Graphs Monitor Monitor panel, 96
  - Interfaces panel, 94–95
  - IP Audit Monitor panel, 97
  - Logging Monitor Monitor panel, 96–97
  - Routing Monitor panel, 95
  - VPN Monitor panel, 95

implementing defense-in-depth
- AAA, 27–28
- perimeter security, 28–31

inside addresses, 108
inside network, 109
inspections, 159
installing. *See also* reinstalling
- ASA/PIX Security Appliance, 46
  - power, 47
- ASDM 5.0, 256–257

PIX license key, 56
version 7 operating system on ASA/PIX Security Appliance, 48–55
interfaces
DMZ interfaces, 131
for ASA/PIX Security Appliance
console ports, 47
Ethernet ports, 46
failover ports, 47
Internet terminology, 107–109
interoperability of NAT and VPN client, 218–219
intrusion prevention, 176
best practices, 231
deploying on ASA/PIX Security Appliance, 179–180
IP addresses, 108
IP Audit
alarms, monitoring, 185–186
comparing with IPS, 175–176
enabling on an interface, 181–184
signatures, 177–179
modifying, 180–181
IPSs (intrusion prevention systems)
ASA/PIX version 7 enhancements, 240–241
configurable security appliance inspections, 242
ESMTP command filtering, 242
FTP command filtering, 242
HTTP deep packet inspection, 242
ICMP inspection, 241
ASA/SSM supported features, 176
comparing with IP Audit, 175–176
IPv6, 108
IPVerify, 30, 169
ISPs (Internet service providers), 107
server hosting, 130

K–L

keepalives, VPN best practices, 233

launching ASDM, 113–116
Layer 2 security best practices, 227–228
licenses (ASA/PIX Security Appliance), 55
license key installation, 56
limiting access to network devices, 30–31
low and slow scan, 34
“low-hanging fruit,” 21

M

mail servers
access policy, creating, 139–142
placing in network, 129–130
services, selecting, 132
manually installing ASA/PIX Security Appliance version 7 operating system, 49–55
menus (ASDM), 61–62
ASDM Wizards menu, 68
File menu, 62–64
Help menu, 68–69
Options menu, 65–66
Rules menu, 64
Search menu, 64–65
Tools menu, 66–68
meta events, 179
MGCP command inspection, 243
mitigating
DoS attacks, 29, 168–169
resource-intensive DoS attacks, 170–172
modifying IP Audit signatures, 180–181
modular policy framework, 244
Monitor Navigation icon (ASDM navigation bar), 94
Administration Monitor feature, 96
Connection Graphs Monitor feature, 96
Interfaces feature, 94–95
IP Audit Monitor feature, 97
Logging Monitor feature, 96–97
Routing Monitor feature, 95
VPN Monitor feature, 95
monitoring
access to ASA/PIX Security Appliance, 150–151
triggered IP Audit alarms, 185–186
VPN client connections
from ADSM, 220–221
from Statistics panel, 220

N

NAT (Network Address Translation)
    compatibility with VPN client, 218–219
    configuring for VPN, 219
navigation bar (ASDM), 69–71
    Back arrow navigation icon, 97
    Configuration icon, 72–73
        Building Blocks panel, 84
        Device Administration panel, 85–88
        Interfaces panel, 74
        NAT panel, 77–79
        Properties panel, 89–93
        Routing panel, 82–83
        Security Policy panel, 74–77
        VPN panel, 79–82
    Forward arrow navigation icon, 97
    Help navigation icon, 99
    Home navigation icon, 71–72
    Monitor Navigation icon, 94
        Administration Monitor feature, 96
        Connection Graphs Monitor feature, 96
        Interfaces feature, 94–95
        IP Audit Monitor feature, 97
        Logging Monitor feature, 96–97
        Routing Monitor feature, 95
        VPN Monitor feature, 95
    Refresh navigation icon, 98
    Save navigation icon, 98
    Search navigation icon, 97–98
Net Shield, 33
network address translation, 109
network devices
    ASA/PIX Security Appliance, hardening, 26
    hosts, hardening, 26–27
    limiting access to, 30–31
    routers, hardening, 25–26
    switches, hardening, 26
network perimeter attack protection, 22
network topology, configuring, 132–133
network-based intrusion prevention, 31–32
    deploying defense-in-depth, 23
    host intrusion prevention, 32–35

O–P

obtaining ASA/PIX version 7 operating system, 251–252
online image upgrades, 244
Options menu (ASDM), 65–66

passwords, best practices for creating, 37, 229
perimeter layer, defense in depth, deploying, 22, 28–31
perimeter traffic filtering, 166
PIX 515E, 44
PIX 525, 44–45
PIX 535, 45
placing web and mail servers in network, 129–130
power, installing on ASA/PIX Security Appliance, 47
private addresses, 108
private inside addresses, 109
private network address
    defining for DMZ interface, 131–132
    defining for web servers, 132
protocols, application inspection, 160–162
    customizing, 162–164, 166
public address, defining for web servers, 132
public servers, 109
pull-down menus (ASDM), 61–62
    ASDM Wizards menu, 68
    File menu, 62–64
    Help menu, 68–69
    Options menu, 65–66
    Rules menu, 64
    Search menu, 64–65
    Tools menu, 66–68

R

rate limiting, 169
Refresh navigation button (ASDM navigation bar), 98
reinstalling ASA/PIX version 7 operating system, 251
remote-access defense, 36

resource-intensive DoS attacks, protecting against, 170–172
restricting access to network devices, 30–31
routers, hardening, 25–26
Rules menu (ASDM), 64

S

Save navigation button (ASDM navigation bar), 98
Search menu (ASDM), 64–65
Search navigation button (ASDM navigation bar), 97–98
security management, 243–245
- on ASA/PIX Security Appliance, 36–38

security posture analysis, 230
selecting services for web and mail servers, 132
servers, hardening, 26–27
services, selecting for web and mail servers, 132
severity levels of syslog messages, 234
signature-based intrusion prevention, 31
signatures, 23
- IP Audit, 177–181

SNMP command filtering, 243
SPA (Cisco Security Posture Assessment), 230
SSH (Secure Shell), 148–150
SSH2, 245
SSM (Security Services Module), 175
starting ASDM, 60
stateful firewalling, 29
stateful inspection, 42
static network access translation, 30
subnet mask, 108
SunRPC inspection, 243
switches
- hardening, 26
- security best practices, 227–228

SYN packets, 171
syslog
- ASA/PIX Security Appliance reporting system, 38
- message severity levels, 234

SYSLOG TCP transport, 245

T

TCP Intercept, 30, 169
TCP SYN attacks, 171
TCP SYN flood, 30
time-based enabled ACLs, 238–239
Tools menu (ASDM), 66–68
traffic
- normalization, 176
- rate limiting, 169

traffic filtering, 22, 29
- on perimeter, 166

transparent firewalls, 239
troubleshooting ASA/PIX Security Appliance, 48
tunnel statistics, graphing, 221

U–V

URL blocking, 153–155
URL filtering, 243
uRPF (Unicast Reverse Path Forwarding), 92

verifying VPN connectivity on ASA/PIX Security Appliance, 217–218
viewing IP Audit syslog messages, 185–186
VPN service
- best practices, 231–233
- client connections
  - monitoring from ADSM, 220–221
  - monitoring from Statistics panel, 220
- compatibility with NAT, 218–219
- enabling on ASA/PIX Security Appliance, 210–216
- enhancements to, 245–246
- NAT connectivity, configuring, 219
- PC client configuration, 216–218
- tunnel statistics, graphing, 221

vulnerability scanning, 230

W-X-Y-Z

web servers, 109
- access policy, creating, 139–142
- connecting to ASA/PIX Security Appliance, 134–135
- placing in network, 129–130
- private network address, defining, 132
- public address, defining, 132
- services, selecting, 132

websites, blocking access to, 153–155