INDEX

Numerics

- 3DES (Triple DES) encryption algorithm 272, 283
- 802.1x standards
  - 802.11 standards 327, 331–333
    - protocol stacks 331, 332
    - scanning functions 334
  - authentication framework 339–342
    - EAP protocol and 802.11i 340–342
- 802.x standards, IEEE 332

A

- AAA (authentication, authorization, and accounting) 131, 165
- AAA model 235
  - accounting 239–241
  - authentication 237–238
  - authorization 238
  - configuration of CiscoSecure ACS 256–265
  - securing network with AAA server 236
  - security servers 241–252
    - Kerberos 250–252
    - RADIUS 245–249
    - TACACS+ versus RADIUS 250
- aaa new-model command 237
- acceptable use policy 82
- access control
  - based on IP addresses 116
  - DAC model, attributes of 112
  - restricting access to a website 114
  - of routers 131
- Access Control Entries (ACE) 138
- access lists, router 138–148
  - applied to an interface, configuring direction of the data flow 143
  - assigning to router interface 154
  - dynamic 252
  - enhanced 144–148
    - dynamic access lists 144
    - time-based access lists 146
    - reflexive access lists 147
  - extended numbered access list 141–144
  - identification numbers and types 138
  - named access list commands 140
  - numbered access list commands 139
  - permissions, example of 154
  - permitting IPSec traffic on VPNs 288
  - PIX Firewall 167–170
  - SNMP managers using community string 359
  - standard numbered IP access lists, additional keywords 140
- access points (APs) 333
  - beacon messages, SSID in 336
  - placement and configuration of 344–349
  - SAFE design recommendations 343
  - wireless clients communicating without 328
  - zone coverage area and 329
- **access-enable** command 255
  - issued for user in a dynamic access list 145
- access-list filters on routers, vulnerability of 162
- accounting 235, 236, 239–241
  - important function records 241
  - TACACS+ 245
- accounts, renaming critical accounts 109
- ACK (Acknowledgment field), TCP headers 23
- Acknowledgment number, TCP 20
- ACS (Access Control Server) 242
  - configuration of 256–265
  - download site, trial copies 250
  - RADIUS authentication setup 249
- active responses to attacks, network IDS 215
- active scanning for wireless stations or access points 334
- adaptive protocols, checking 96
- Adaptive Security Algorithm (ASA) 166
- Address Resolution Protocol (ARP), spoofing 29–30
- address space of program code, making nonexecutable 29
- administrative personnel, access to routers 131
- administration, VPN manager functions 288
- Advanced Services for Network Security (ASNS) 86
- AES (Advanced Encryption Standard) 64, 66, 283
- agents, SNMP 356
  - defining relationship with manager 359

AH (authentication header) protocol 277
  establishing use of in IPSec policy 284
  identified in IPSec transform sets 283
  identifying for IKE Phase 2 283
  transport mode 280
  tunnel mode 281
Airsnort program 338
Aladdin eToken 256
alarms and events (RMON), monitoring traffic with 361
alarms, IDS 194
  analyzing for IDS tuning 227
  monitoring and tuning 225
  network IDS 217
  routers configured for network IDS 212
alerts and audit trails, generated by CBAC 148
algorithms
  asymmetric key algorithms 66–69
    Diffie-Hellman 68
    PGP 69
    RSA 68–69
  definition of 63
  encryption 282–284
  hashing 69
  SSL and TLS 71
  symmetric key algorithms 64–66
    AES 64, 66, 283
    DES 64, 272, 283
    Triple DES (3DES) 65–66, 272, 283
allow all model (security plan) 83
allowed and disallowed behavior, defining 81
analysis tools (network traffic analysis) 95
annualized rate of occurrence (ARO) 9
annual loss expectancy (ALE) 9
anomaly-based IDSs 200
anonymous access 116
antireplay protection 277
antivirus software 51, 181
application layer, OSI model
  data-driven attacks 160
  Kerberos authentication service 250
  SNMP on 356
application-layer protocols, CBAC inspection of 148–152
  APs. *See* access points
ARO (annualized rate of occurrence) 9
ARP (Address Resolution Protocol)
  spoofing 29–30
ASA (Adaptive Security Algorithm) 166
  PIX Firewall data flow 167
ASNS (Advanced Services for Network Security) 86
asymmetric key algorithms 66–69
  Diffie-Hellman 68
  PGP 69
  RSA 68–69
asymmetric key encryption 272, 301
attacks
  broadcast, configuring router to prevent 154
  buffer overflow 28
  connection hijacking (TCP) 26
  connection-killing (TCP/IP) 25
  in cryptoanalysis 61
  data-driven 160
  denial-of-service (DoS)
    distributed 161
    stopping with stateful firewall 163
    using IP spoofing 20
  deriving WEP key stream with protocol analyzer 339
  e-mail 161
  ICMP packets, using to export confidential information 22
  IP fragment attacks 23
  network IDS responses to 213
  prevented by policy-based IDS 199
  rebuffed by network IDS (example) 208
  SYN-flooding, prevention by CBAC 148
  types of attacks 161–162
auditing 109
  audit trails generated by CBAC 148
  case study 366–372
  education on. *See* SANS Institute
  monitoring traffic with RMON and SNMP 361
  network auditing in design process 95
  SAA (Service Assurance Agent), using 362
  SNMP. *See* SNMP
authenticated users, potential threats posed by 6

authentication 85, 235, 237–238
  802.1x framework and EAP protocol 340–342
  alternatives to reusable passwords 50
  configuring for website access 114–117
  encapsulating security payload. *See* ESP protocol 279
  hardware keys, using 43
  HMAC, used with IPSec 274
  IPSec, identifying method for IKE Phase 1 282
  Kerberos 48, 250–252
  open, for wireless networks 337
  peer authentication methods on VPNs 274, 284
  PKI users 307
  RADIUS 246–249
    ACS setup for 249
    attribute pairs (AV pairs) 247
    summary of 248
  shared key authentication, wireless networks 337
  TACACS+ 257–265
  token-based systems 42
  user authentication method, selecting for VPN 294
  WEP protocol 339
  wireless station, using WEP 333, 337
  WLANs, stations and clients 334–335
authentication header protocol. *See* AH protocol
authentication policy 82
authentication, authorization, and accounting. *See* AAA
authority and scope, statement of (security policy) 82
authorization 235, 236, 238
  TACACS+ 243
autocommand 145
automating signature updates for IDSs 221
AV pairs, RADIUS authentication 247
availability of data and resources 8

B

backplane capacity constraints, network design 93
banner for router to warn off intruders 135
baseline of your current security posture 81
basic authentication 116
basic service set (BSS) 333
beacon frames 334
beacon messages, SSID in 336
Belt and Braces Firewall architecture 168
biometrics 53–55
  face recognition 55
  fingerprint scanning 54
  signature recognition 55
  typing 54
  voice recognition 54
block ciphers 64
  AES 64, 66, 283
  DES 64, 272, 283
  Triple DES 65–66, 272, 283
BOOTP server 137
broadcast attacks, prevention of 154
browsers 118–123
Brussels router, 134
BSS (basic service set) 333
buffer capacity constraints, network design 93
buffer overflows 28
bugs, risk of 9
building-to-building wireless networks 330
bytes 15

C

camera systems, internal physical security 45
campus access policy 82
card bus (wireless NIC) 328
CAs (Certificate Authorities) 37, 72, 302
  creating your own CA 312–323
  enrolling in 73
  hierarchical CAs 305
  single root CA 305
  validating signature of 73
CBAC (Context Based Access Control), 148–152, 154
CDP (Cisco Discovery Protocol) 137
certificate authorities. *See* CAs
certificate revocation lists. *See* CRLs
certificates 72, 274, 275, 284. *See also* digital IDs
  placement on a CRL 308
  types of 38
chalk marks (war-chalking) 342
Challenge Handshake Authentication Protocol (CHAP) 243
change control (business processes) 98
Chargen attack 161

Check Point, software firewalls 173
checksums 15
CIA (confidentiality, integrity, and availability) 8
ciphers 63
  block and stream ciphers 64–65
Cisco
  Advanced Services for Network Security (ASNS) 86
  Internet Operating System. *See* IOS
  Intrusion Detection Host sensor 204
  Intrusion Detection System (IDS) 164
  IOS 165
  IOS-based IDSs, deployment on a router or PIX-based IDS 212
  Light Extensible Authentication Protocol (LEAP) 339
  Linksys product line 331
  PIX Firewall 164, 165–170
  Router Security Configuration Guide 394
  SAFE Blueprint 377–383
  Secure Agent Manager 204, 206
  Secure Integrated Software 212
  Wireless Security Suite 339, 342
Cisco Discovery Protocol (CDP) 137
Cisco IOS Firewall CBAC engine. *See* CBAC
Cisco Press website, certificates 308
Cisco Secure Encyclopedia (CSEC) 162, 195
CiscoSecure Access Control Server. *See* ACS
CiscoSecure Private Internet Exchange Firewall. *See* PIX Firewall 165
CiscoSecure products 162
CiscoView application 367
CiscoWorks VMS Suite 204
client-based firewalls 174
clients, setting up VPN client 297
ClipBook Viewer 111
closed network 79
coded messages. *See* ciphers
cold site (disaster recovery plan) 46
command and control network 218
command and control port, network IDS 208
command line interface (CLI), PIX Firewall and 165
commands
  IOS privileged executive commands 236
  monitoring and troubleshooting SNMP 360
  SAA operations, specifying 363
comments, adding in named access lists 143
Common Criteria EAL 4 ratings (NetScreen and PIX) 170
community networks, wireless 330
community strings, SNMP 359, 371
  assigning a view to 359
compression algorithm (LZS) 295
compromised keys 308
computer resources, in security policies 81
computers, cryptography and 63
conduits. *See* access lists, PIX Firewall
confidentiality, integrity, and availability (CIA) 8
Connect accounting function 241
Connection Establishment timer 25
connection hijacking (TCP) 26
connection-based security policy 166, 183
connection-killing attacks 25
connectivity and associated policies 81
consensus, communicating 81
console access to devices, avoiding 45
consoles, accessing routers from 131
constraints, network design 93
content filtering 178–181
Context-Based Access Control (CBAC) 138, 148–152, 154
cookies 123
costs and benefits of security 9
countermeasures against vulnerabilities, information about 162
covert channels 21
CPU, tie-ups in attacks 161
CPU processing speed 93
crackers 40, 193, 342
  hackers versus 5–6
  script kiddies 6
cracking codes (cryptoanalysis) 61
credentials, Kerberos 252
CRLs (certificate revocation lists) 308
cross certifying 305
cryptography 61–76. *See also* encryption
  asymmetric key algorithms 66–69
    Diffie-Hellman 68
    PGP 69
    RSA 68
  cryptoanalysis versus 61
  digital certificates 72
  hashing algorithms 69

MD5 70
SHA-1 71
history of 61–63
NSA research and education on 393
PKCS (Public Key Cryptography Standard) 307
secret key, Kerberos 48
SSL and TLS 71
symmetric key algorithms
AES 64, 66, 283
DES 64, 272, 283
Triple DES (3DES) 65–66, 272–283
wireless equivalent privacy keys. *See* WEP protocol
CSEC (Cisco Secure Encyclopedia) 162

D

DAC (Discretionary Access Control) 107, 112
DAD (disclosure, alteration, and denial) 8
Data Encryption Standard. *See* DES
data flow
NetScreen firewalls 171
PIX Firewall 167
data integrity 8
on VPNs 273
data packets, inspection up to Layer 4 162
data streams 15
data-driven, application-layer attacks 160
datagrams, IP 16
DDoS (distributed denial-of-service) attacks 165
debug commands (SNMP), documentation of 361
deep packet firewalls 162
Cisco PIX and NetScreen firewalls 164
NetScreen 171
defense in depth strategy 96–97
defenses 35–56
antivirus software 51
biometrics 53–55
in depth 96–97
digital IDs 35–40
encrypted files 52
firewalls 49
intrusion detection systems (IDSs) 40
PC card-based solutions 41
physical security 44–46
residing in multiple locations 96
reusable passwords 50
defining roles 81
definitions section (example VPN security policy) 87
demilitarized zones. *See* DMZs
denial-of-service attacks. *See* DoS attacks
deny all model (security plan) 83
deny all statement
ending extended numbered or named access lists 142
ending standard or named access lists 140
DES (Data Encryption Standard) 64
encryption algorithms 272, 283
design phase, network life cycle 98
designing a secure network 91–101
network design methodology 97–99
network design principles 92–97
defense in depth 96
design activities, tools, and techniques 94–96
requirements and constraints 93
top-down design practices 92
physical security 99–101
return on investment 99
switches and hubs 101
Destination Unreachable message 22
developers' digital ID 38
device management, network IDS 217
IDM (IDS Device Manager) 226
in-band 220
out-of-band 219
device port density constraints, network design 93
devices, physical access to 45
DHCP (Dynamic Host Configuration Protocol) 289
Diffie-Hellman algorithm 68
Diffie-Hellman key exchange 272–273
identifying method for IKE Phase 1 282
digest 40

digital certificates. *See* certificates
digital IDs 35–40
    HTTPS, use of 48
    parameters of 37
    types of 38
digital signatures 73, 274
    combined with passwords 256
    RSA signatures 275
digital signing of public keys 302
director, network-based IDS 208
disaster recovery planning 45, 97, 101
disclosure, alteration, and denial (DAD) 8
Discretionary Access Control (DAC) 107, 112
distributed denial-of-service (DDoS) attacks 161
DMZs (demilitarized zones) 49, 165, 183
    configuring security levels 168
    outside connections and 170
    web server connected on, attacks against 210
DNS (Domain Name Service)
    lookup service 137
    NetScreen Deep Inspection firewall and 171
    passing address to VPN client 295
    spoofing 30
DNS poisoning 161
DoS (denial-of-service) attacks
    launching with TCP flags 24
    Smurf attack 198
    starting with IP address spoofing 20
    stateful firewalls and 163
    TCP SYN flood attacks 161
dropping packets, router configured for network IDS 212
dynamic access lists 252
dynamic access lists, routers 144
dynamic and static translation slots, ASA and 167
Dynamic Host Configuration Protocol (DHCP) 289

E

EAP (Extensible Authentication Protocol) 339
eavesdropping (sniffing) on publicly accessible networks 72
echo and Echo-Reply messages 22
echo messages to IP broadcast addresses 162
e-commerce, necessity of network security for 79, 80
economic constraints, network design 94
EDE (encrypt–decrypt–encrypt) 65
Electronic Communications Privacy Act (EPCA) 8
e-mail 14
    attacks using 161
    protection during transmission with PC encryption cards 43
    social engineering attacks, use in 31
enable secret command 132, 153
encapsulating security payload. *See* ESP protocol
encrypted logins 46
    Kerberos 48
    SSL (Secure Socket Layer) 48–49
    SSH (Secure Shell) 47–48
encryption 85, 272
    Diffie-Hellman key exchange 272–273
    ESP (encapsulating security payload) protocol 279
    file 52
    PC encryption cards 43
    public/private keys, digital IDs 39
    RSA-encrypted nonces 274, 276
    SEP (Scalable Encryption Processing) 292
    symmetric key algorithms 64–66
        AES 64, 66, 283
        DES 64, 272, 283
        Triple DES (3DES) 65–66, 272, 283
    WEP, improvement with TKIP 340
    wired equivalent privacy (WEP) keys 334, 337
encryption algorithms
    establishing in IPSec policy 284
    identified in IPSec transform sets 283
    identifying for ESP in IKE Phase 2 283
    identifying for IKE Phase 1 282
encryption file system (EFS) 52
end stations, wireless. *See* stations, wireless
enforcement section, security policies 87
enhanced access lists 144–148
Enigma machine 62
enrollment procedure, PKI 306

Enterprise Composite Network Model, out-of-band IDS management 220
environmental monitoring, high-level security areas 45
environmental requirements for network equipment 93, 100
EPCA (Electronic Communications Privacy Act) 8
equipment failure, risk of 9
errors, detection in data streams 15
ESP (encapsulating security payload) protocol 279
  establishing use of in IPSec policy 284
  identified in IPSec transform sets 283
  identifying for IKE Phase 2 283
  transport mode 281
  tunnel mode 281
Ethereal tool 27
Ethernet
  crossover cables 328
  NetScreen firewalls and 171
  speed, possible values for 185
  to wireless bridge 328
  WLANs, 802.3 IEEE standard 332
eToken 256
evaluate command 147
evasion techniques for network IDSs 202
events and alarms (RMON), monitoring traffic with 361
exclusive OR (XOR) function 338
exec-timeout command 134
exec-timeout, setting 153
Explicit Congestion Notification (ECN) 20
extended access lists 141
  numbered 141–144
  reflexive 147
extended Log File Format, W3C 113
extended service set (ESS) 333
Extensible Authentication Protocol (EAP) 340–342
external interface of the firewall 149
external physical security 44, 100
external weaknesses 5

F

face recognition 55
fail-over site 46, 101
false negative IDS alarms 194
false positive IDS alarms 194
  eliminating in IDS tuning 227
FERET (facial recognition technology) 55
file encryption 52
file protection 53
file systems, hardening 107–109
file transfers 14
file-based requests (PKI enrollment) 307
filtering
  content filters, firewall 178–181
  packet filtering and stateless, by firewalls 162
  stateful, by firewalls 162, 163
FIN (finished with connection), TCP flag 23, 25
FIN_WAIT timer 25
financial institutions, privacy policies 8
fingerprint scanning 54
Firewall Service Module (FWSM) 166
firewall-based VPNs 270
firewalls 49, 85, 159–191
  CBAC 148
  configured to filter based on TCP ports 20
  definition of 49
  enhancements for 175–181
    antivirus software 181
    content filtering 178–181
  enhancements for
    antivirus software 181
    content filters 178–181
    NAT (network address translation) 175–177
    proxy services 177–178
  hardware-based 164, 165–173
    NetScreen 170–173
    PIX 164, 165–170
  personal 174
  placing filtering routers and firewalls 181–190
  as proxy servers 178
  software-based (Check Point) 173
  stateful 163
  stateless 162–163
  types of 162
flags, TCP 23
folders (cookie), making read-only 123
four-way handshake mechanism, TCP FIN packets 25
fragmentation offset (IP) 17, 23

fragmentation reassembly code, TCP/IP 161
framework for security implementation 81
FTP, NetScreen Deep Inspection Firewall and 171
functional areas of a network, separation with firewalls 49
FWSM (Firewall Service Module) 166

G

gateways (VPN), tunnel mode used between 281
generator (parameter *g*, Diffie-Hellman) 68
GIAC (Global Information Assurance Certification) 385
GLB (Gramm-Leach-Bliley) Act 8
global command (PIX Firewall) 187
Global Information Assurance Certification (GIAC) 385
globalization of business 14
governments
  security for emerging technologies, role in 8
  specifications for physical security 44, 100
Gramm-Leach-Bliley Act (GLB) 8
graphical user interface (CiscoView) 367
GRE (generic routing encapsulation) tunnels 271
group names, specifying for SNMP server 360
group rights 109
groups, configuring on VPN Concentrator Group Screen 290
guideline, definition of 387

H

hacker 5
hardening operating systems and applications 386
hardening systems 107–123
  browsers 118–123
  case study 124–128
  file systems 107–109
  web servers 109–117
hardware, SOHO 331
hardware firewalls 164, 165–173
  NetScreen 170–173
  PIX 164, 165–170
hardware interfaces 184
hardware keys 42
hash 40
hash algorithms
  establishing use of in IPSec policy 284
  identified in IPSec transform sets 283
  identifying for IKE Phase 1 282
  identifying for IKE Phase 2 283
Hashed Message Authentication Codes (HMAC) protocol 274
hashing algorithms 69
  MD5 (Message Digest 5) 70
  Message Digest 5 (MD5) 70
  SHA-1 71
hashing passwords in the router configuration file 132
headers
  IP 16
    address spoofing in 20
  TCP 18
    flags 23
Health Insurance Portability and Accountability Act (HIPAA) 8
hierarchical CA 305
hijacking TCP connections 26
history of operation, showing 365
HMAC-MD5 274
HMAC-SHA-1 274
hoaxes 5
honey-pots 202
host IDS 41, 194, 204–207
  deploying in network 203–206
  network IDS vs. 200
  sensor components and architecture 204
hostnames, identifying VPN peers with 284
hosts, configuring SNMP server hosts 360
hot site (disaster recovery plan) 46
hotspot WLAN 328, 330
HTTP
  access to routers via 131
  cookies, simulating stateful environment with 123
  NetScreen Deep Inspection firewall and 171
HTTP server 137
HTTPS 37, 48
hubs and switches, network security design 101

I

IANA (Internet Assigned Number Authority) 19

IAR (Internet Accessible Router) 176
IBSS (independent basic service set) 329
ICMP (Internet Control Message Protocol)
  echo (ping) traffic to IP broadcast addresses 162
  used in TCP/IP connection covert channels 22
identification policy 82
identification, two-factor 256
identify theft 72
IDM (IDS Device Manager) 226
IDSs (intrusion detection systems) 40
  anomaly-based 200
  case study 221–232
    active response, blocking host 229–232
    IDS Event Viewer 228
    initializing and configuring network sensors 223–226
    sensor placement on the network 223
    tuning IDS 227
  Cisco, 164
  honey-pots 202
  host-based 204–207
    deploying in the network 206
    host sensor components and architecture 204
  network IDS 207–217
    deploying in the network 210–216
    evasion/antievasion techniques 202
    management communications 217
    notification and reporting 217
    organizational issues and complications 202
  network versus host 200
  policy-based 198
  sensor maintenance 221
  signature-based IDSs 196
IEEE (Institute of Electrical and Electronics Engineers) 327. *See also* 802.1x standards
IETF (Internet Engineering Task Force) 196
IEV (IDS Event Viewer) 227
IIS (Internet Information Services)
  enabling logging 113
  hardening, website information on 117
  log file formats 113
IKE (Internet Key Exchange) protocol 256, 282
  establishing an IKE policy for VPNs 284
  SA (security association) lifetime 282
implementation phase, network life cycle 98
in-band management, network IDS 217, 220
inbound and outbound traffic 168
inbound packets, filtering 143, 154
independent basic service set. *See* IBSS
inform requests, SNMP 357
  configuring router to send to a host 361
information sent to SYSLOG server 355
inside global address (NAT) 177
inside interfaces 183
inside intruders 40, 193
inside local address (NAT) 177
inspect commands, router 150
inspection methodologies, firewalls 162
inspection of packets at application layer by CBAC 148–152
  creating inspection rules (example) 154
Institute of Electrical and Electronics Engineers (IEEE) 327. *See also* 802.1x standards
integrated Windows authentication 116
integrity of data 8
Intercept Correlate Rules Engine (INCORE) (Secure Agent) 204
interface bandwidth constraints, network design 93
interface command (PIX Firewall) 184, 186
interface command to apply an access list to an interface 143
interfaces
  configuring on VPN Concentrator Screen 289
  firewall
    DMZ 183
    internal and external 149
    naming 183
  information about 370
  NetScreen firewalls 171
  network IDS 208
  network, assigning IP addresses to 185
  PIX Firewall
    naming of 165
    security levels 167
  router
    assigning access list to 143
    assigning CBAC inspection rules and access list to 154
    monitoring interfaces 213
internal interface of the firewall 149

internal physical security 45, 100
internal weaknesses and vulnerabilities 6
International Telecommunications Union (ITU-T) 35
Internet
  access policy, coverage in security policy 82
  availability of networks to 80
  communication over 14–15
  mail server attack launched via 208
  restricted employee access to 178
  traffic levels, IDS and 203
Internet Accessible Router (IAR) 176
Internet Assigned Number Authority (IANA) 19
Internet Control Message Protocol. *See* ICMP
Internet Engineering Task Force (IETF) 196
Internet Explorer 118–123
  security levels 119
    predefined, list of 119
  security zones, changing settings for 118–119
  security, website information on 118
Internet Information Services. *See* IIS
Internet Key Exchange. *See* IKE protocol
Internet Operating System. *See* IOS
Internet relay chat, viruses on 51
Internet Security Association and Key Management Protocol (ISAKMP) 282
Internet security zone (Internet Explorer) 118
Internet-enabled business 79
intranet security zone (Internet Explorer) 118
Intrusion Detection System (IDS), Cisco 164
intrusion detection system (IDSs) 40, 193–233
  fundamentals of 194
  IDS sensors 41
    getting past in Ping of Death attack 23
  signature-based IDS 195
IOS (Internet Operating System) 236
  AAA configuration on 236–241
  debug commands for SNMP 361
  IDSs based on, deployment on network 212
  Kerberos support 252
  Service Assurance Agent (SAA) 362–365
  SNMP versions supported 358
  SSH server 48
  TACACS+ support 242
IP router access lists 139
IP address space, NetScreen firewalls and 172
IP addresses
  access control based on (for a PC) 116
  identifying VPN peers by 284
  inside and outside, defining for network interfaces 185
  internal network, translation to global addresses 186
  NAT (network address translation) and 175
  source and destination, TCP/IP connections 19
IP protocol 16–18. *See also* TCP/IP protocol suite
  address spoofing 20
  Explicit Congestion Notification (ECN) 20
  fragment reassembly vulnerability 161
  fragmentation offset 17, 23
  mobile IP 18
  redirect 138
  redirection attacks 339
  sessions, logging of by network IDSs 213
  telephony, network design planning for 97
IPSec (IP Security) 272–283
  antireplay protection 277
  configuring all parameters for VPN 292
  data integrity function 273
  encryption 272
  establishing IPSec policy for VPNs 284
  eToken, storing certificates with 256
  four major functions of 272
  origin authentication 274–277
    preshared keys method 274
    RSA signatures method 275
    RSA-encrypted nonces 276
  preshared keys, peer authentication by 274
  protocol framework 277
    AH (authentication header) 277
    ESP (encapsulating security payload) 279
  selecting Security Association (SA) 293
  transform sets 282
  tunnel or transport mode 279
  VPNs with
    configuring IPSec 285
    preparation for 284
  wireless network security, using for 342
IPSec concentrator 87
iris and retina recognition 55
ISAKMP (Internet Security Association and Key Management Protocol) 282
ISDN networks, NetScreen firewalls and 171

J

Juniper Networks 170

K

KEEP_ALIVE timer 25
Kerberos 241, 250–252
  encrypted login sessions 48
key distribution center (KDC) 250
key distribution methods
  establishing in IKE policy for VPNs 284
  IPSec peer authentication 274
key exchange method, identifying for IKE Phase 1 282
keys, compromised 308
Kismet (WLAN packet analyzer) 336

L

labor requirements, network design and 94
Land.C attacks 161
LANs (local-area networks) 14. *See also* WLANs
  peer-to-peer, limitations of 328
  viruses on 51
  wireless connectivity 330
  WLANs 328
LAN-to-LAN tunnel type 294
latency, testing in network traffic simulation 96
Layer 2 or Layer 3, OSI model, NetScreen firewalls operating at 172
Layer 3, OSI model 163
Layer 4, OSI model (TCP layer) 162
Layer 7, OSI model 250
layered approach to security 91
  defense in depth 96–97
  external physical security 44, 100
  internal physical security 45, 100
least trusted 4
levels of logging 353
  warning levels, information sent to SYSLOG server 354
life cycle (network), stages of 97–99
Light Extensible Authentication Protocol (LEAP) 339
link layer, extensible authentication (802.1x) 340
Linksys, Inc. 331
local Internet security zone (Internet Explorer) 118
local-area networks (LANs) 14
lock-and-key access lists 144
lock-and-key feature 252–256
logging 353–356
  case study 366–372
  default log file directory, changing for security 114
  enabling for web servers 113
    IIS, supported log file formats 113
  IP session, by network IDSs 213
  levels of 353
  SYSLOG 354
logins, encrypted 46
  Kerberos 48
  SSL (Secure Socket Layer) 48–49
  SSH (Secure Shell) 47–48
LZS compression algorithm 295

M

MAC (medium access control) layer, WLANs 332
  security enhancements, IEEE 802,11i standard 340
mail server, attack on rebuffed by network IDS 208
malware, definition and categories of 5
man in the middle attacks 162
Management Information Base (MIB) 356
management station
  communication with sensors 217
  network IDS 208
management, IDS 193
manager functions, VPN 288
managers, SNMP
  defining relationship with agent 359
  limiting access to objects 359
man-in-the-middle attacks 72
  WEP protocol, vulnerability to 338
manpower and labor costs for IDSs 203
masks, router access lists 140
McAfee Antivirus software applications 51
MD5 encryption algorithm, secret password hashes 132

MD5 or SHA-1 hash algorithms
  establishing use of in IPSec policy 284
  identifying for IKE Phase 2 283
  IKE Phase 1, using with 282
medium access control. *See* MAC layer, WLANs 332
memory, tied up in TCP SYN flood attacks 161
Message Digest 5 (MD5) algorithm 40, 70
message injection attacks 339
message modification attacks 339
MIB (Management Information Base) 356
Microsoft. *See also* Internet Explorer
  hardening IIS, website information on 117
  security information on the website 110
  operating systems
    security patches and updates 6
misuse, risk of 9
mobile IP 18
modular approach to network security 91
monitoring network 218
monitoring port, network IDS 208
multicasting, testing in network traffic simulation 96
multiple locations for network defenses 96

N

named access lists 139
  commands 140
nameif command (PIX Firewall) 183
NAT (network address translation) 168, 175
  disadvantages of 177
  enabling PIX for 183–189
  router NAT translation table, viewing 176
nat command (PIX Firewall) 186
National Security Agency. *See* NSA
NetScreen firewalls 164, 170–173
  data flow 171
  deep packet layer inspection 171
  functions not convered in detail 173
  session table 171
NetStumbler (WLAN packet analyzer) 336
network accounting function 241
network address translation. *See* NAT
network addresses 140
network architecture 92
network audits 95
network design 91
  fundamental principles 92–97
    defense in depth 96
    design activities, tools, and techniques 94–96
    requirements and constraints 93
    top-down design practices 92
  methodology 97–99
  physical security 99–101
  return on investment 99
  switches and hubs 101
network IDS 41, 194, 207–217
  case study 221–232
    active response, blocking host 229–232
    IDS Event Viewer 228
    sensor initialization and configuration 223–226
    sensor placement 223
    tuning IDS 227
  deploying in the network 210–216
    PIX Firewall as sensor 213
    router IDS features and network modules 212
  evasion and antievasion techniques 202
  host IDS versus 200
  management communications 217
    in-band management 220
    out-of-band management 219
  notification and reporting 217
  organizational issues and complications 202
    political constraints 203
    social constraints 203
    technological constraints 203
  responses to attacks
    IP session logging 213
    TCP resets 215
  sensor components and architecture 208
network infrastructure, requirements of 92
network interface cards (NICs), wireless 328
network layer (Layer 3, OSI model) 163
  correspondence of IP protocol to 16
  mobile IP connections 18
Network Management Server (NMS) 164
Network Management System (NMS) 356
network performance, monitoring with SAA 362

network resources, use and protection of (security policy) 81
network security
  books 427
  responsibilities for 7–8
  websites 428
network security database (NSDB) 197
  updates for IDS signatures 221
network traffic
  analysis of 95
  inbound and outbound 168
  simulating 96
networks, availability to Internet and public networks 80
NMS (Network Management Server) 164
NMS (Network Management System) 356
nonces 274, 276
nonstatistical anomaly detection 200
notification alarms, IDS 194
notification features, network IDS 217
notifications, SNMP 357
  configuring 361
NSA (National Security Agency) 393–395
  security guides 394
NSDB (network security database) 197
  updates for IDS signatures 221
NTFS file encryption 52
number used once. *See* nonces
numbered access list commands 139
numbered access lists, extended 141–144

O

open authentication, wireless networks with 337
operating systems
  hardening security of 107–123
    browsers 118–123
    case study 124–128
    file systems 107–109
    SANS step-by-step guides for 386
    web servers 109–117
  overlapping IP fragment bug 161
  software-based firewalls and 174
operation phase, network life cycle 98
optimization phase, network life cycle 99
origin authentication, IPSec 274–277
OSI model
  Layer 2 or Layer 3 mode, NetScreen firewalls operating at 172
  Layer 3 (network) 163
    IP, corresponding to 16
  Layer 4 (TCP) 162
  Layer 7 (application layer) 250
    SNMP on 356
  TCP/IP mapped to 16
  transport layer (TCP) 18
outbound network traffic 168
outbound packets, filtering 143
out-of-band management, network IDS 217, 219
outside global address (NAT) 177
outside hosts, connections to internal resources 169
outside interfaces 183
outside intruders 40, 193
outside local address (NAT) 177
overlapping IP fragment implementation bug 161

P

packet filtering 162
packet filters for routers. *See* access lists, router 138
parameter *g* (Diffie-Hellman) 68
parameter *p* (Diffie-Hellman) 68
passive response to attacks, network IDS 213
passive scanning for wireless stations or access points 334
Password Authentication Protocol (PAP) 243
passwords
  capture by Trojan horses 161
  combined with digital signatures 256
  configuring secure passwords for routers 131
  encryption, **service password-encryption** command 135, 153
  file protection with 53
  reusable 50
  router
    assigned to the console, VTY, AUX lines, and enable 134
    configuration for Telnet 133
    enable and user-level passwords 133
    recovery procedure for 132
PAT (Port Address Translation) 175, 176
  disadvantages of 177
patching, vulnerabilities 86

pattern-matching IDS signatures 195
PC card-based solutions (security) 41–43
  hardware keys 42
  PC encryption cards 43
  security cards 41
PC encryption cards 43
PCI (Peripheral Component Interconnect) 328
PCMCIA (wireless NIC) 328
PDIOO (planning, design, implementation, operation, and optimization) 97
peer authentication methods on VPNs 274
peer-to-peer WLANs 328, 329
performance, monitoring with SAA 362
Peripheral Component Interconnect. *See* PCI
permissions
  changing in DACs 112
  router access list, example of 154
  web content directory, changing for Internet Explorer 126
  Windows file systems, hardening security settings 107–109
permit entry 147
persistent cookies 123
Personal Computer Memory Card International Association. (PCMCIA) 328
personal digital ID or certificate 38
personal firewalls 174
personnel awareness of security policy 46
personnel training in physical security 101
PGP (Pretty Good Privacy) 69, 302
PHY (physical) layer, WLANs 332
physical security 44–46
  disaster recovery plans 45
  governmental specifications 100
  internal 45, 100
  intrusion by tailgating 101
  network design 99–101
  outside and external security 44
  personnel training 101
  securing the perimeter 100
  survivability and recovery 101
ping, use in Smurf attacks 162
Ping of Death attack 23
PIX Firewall 164, 165–170
  commands for managing and troubleshooting 190
  configuration as cut-through proxy 168
  data flow for 167
  features and functions not covered in detail 170
  full working configuration (case study) 189
  IDS 213
  NAT (network address translation) 183–189
  placement of 169, 181
PKCS (Public Key Cryptography Standard) 307
PKI (Public Key Infrastructure) 72, 301–323
  creating your own CA 312–323
  enrolling in a CA 73
  enrollment procedure 306
  public key distribution 301
  revocation of certificates 307
  topologies of trust 304
  trusted third party 302
    key exchange 304
    public key signing 304
planning stage (network life cycle) 98
plug-ins, browser 118
point-to-multipoint bridge (WLANs) 328
point-to-point bridge (WLANs) 328
point-to-point WLANs 330
policy section (example security policy for a VPN) 87
policy, definition of 387
policy-based IDS 198
  attacks prevented by 199
political constraints
  on network design 94
  on network IDS 203
pool of global addresses 187
Port Address Translation (PAT) 175
port numbers 19
ports
  colors for 369
  risks of open wireless ports 336
power blackouts, countering 45, 101
preshared keys (peer authentication method) 274
Pretty Good Privacy (PGP) 69, 302
prime numbers
  parameter *p*, Diffie-Hellman algorithm 68
  RSA algorithm 69
privacy policies, financial institutions 8
private data traversing public networks 80

Private Internet Exchange. *See* PIX Firewall 165
private key (digital IDs) 39
Private Ports 19
privilege levels 239
processor speed 93
protocol decode-based IDS signatures 195
protocol stacks (802.11 standard) 331
protocols
    adaptive, checking in network traffic simulation 96
    CBAC inspection of 151
    CBAC intelligent filtering for 148
    Internet Key Exchange (IKE) 282
    IPSec 277
        establishing use of in IPSec policy 284
        identification of in transform sets 283
        tunnel or transport mode 279
    tunneling, selecting for VPN 292
proxies
    configuring PIX Firewall as cut-through proxy 168
    limiting attacks with 162
    network use of proxy services 177
PSH (Push function), TCP field 23
public key (digital IDs) 39
public key cryptography 272, 307
Public Key Infrastructure. *See* PKI
public networks, sending private data over 80
Public Service Segment (PSS) 49. *See also* DMZs
purpose of a security policy 82
    example for a VPN 86
PuTTY (SSH client) 48

Q

quality of service (QoS)
    guaranteeing, costs of 94
    validating and testing adequately 96

R

radio frequency (RF) technology, use by WLANs 331
radio, cryptography and 62
RADIUS 241, 245–249
    with 802.11i authentication framework 340
    ACS setup for RADIUS authentication 249
    authentication 246
        attribute pairs 247
    summary of 248
    TACACS+ versus 250
RDEP (Remote Data Exchange Protocol)
    communication between network IDS sensor and director 217
    IP session logging, network IDSs 213
realm 292
recovery from disasters 101
Redirect messages 22
redirection (IP redirect service) 138
redundancy in network designs 97
reflect option 147
reflexive access lists 147
Registered Ports 19
remarks, adding in named access lists 143
remote access 79, 235–266
    AAA model 235
        accounting 239–241
        authentication 237–238
        authorization 238
        servers 241–252
    configuration of AAA server (CiscoSecure ACS) 256–265
    lock-and-key feature 252–256
    security policy coverage of 82
    two-factor identification 256
Remote Access tunnel type 294
remote access VPNs 269
    case study 285–298
Remote Authentication Dial-In User Service. *See* RADIUS
Remote Data Exchange Protocol. *See* RDEP
Remote Monitoring (RMON) 372
remote Telnet sessions and logins, securing 47
reporting features, network IDS 217
requirements and constraints, network design 93
resetting TCP connections
    network IDS response to attacks 215
    router configured for network IDS 212
Response Time Reporter (RTR). *See* SAA
responses to alerts, network IDS 213
restricted security zone (Internet Explorer) 118

retina and iris recognition 55
return on investment (ROI), network design and 99
reusable passwords 50
reverse lookup, countering DNS spoofing with 31
reverse social engineering attacks 31
RFCs (Request for Comments), protocol analysis for violations of 195
rights, permissions versus 107
risk assessment
  annualized rate of occurrence (ARO) 9
  single loss expectancy (SLE) 9
  types of risks 9
risks
  reducing with tools to support design process 95
  vulnerabilities and 13–14
Rivest, Shamir, and Adelman (RSA) algorithm 68, 273
RMON (Remote Monitoring) 361
robust defenses 96
roles, defining 81
route command (PIX Firewall) 188
routers 17
  AAA configurations on Cisco IOS router 236–241
  AAA model, enabling 237
  Brussels 134
  Cisco Router Security Configuration Guide 394
  configuring GRE tunnels on 271
  configuring IPSec on 282
  configuring to send only warnings to SYSLOG server 355
  content filtering 178
  extended access lists 20
  filtering, placement of 181
  IDS features and network modules 212
  NAT translation table, viewing 176
  PIX Firewall and 166
  security
    administrative access, configuring 131
    banner to warn intruders 135
    case study of telecommuter connecting to branch office 152–156
    CBAC (Cisco IOS Firewall) 148–152
    commands to configure a new router 153
    console port, timeout 135
    enable and user-level passwords configured 133
    online information, Cisco web site 138
    passwords assigned to console, VTY, AUX lines and enable 134
    services, turning off or restricting access 137
  security for network protection 138–148
    access lists 138
RSA (Rivest, Shamir, and Adelman) algorithm 273
RSA Laboratories, PKCS standards 307
RSA signatures (peer authentication method) 274, 275
RSA-encrypted nonces (peer authentication method) 274, 276
RST (Reset the connection), TCP header flag 23
RTR (Response Time Reporter). *See* SAA
rtr operation-number command 363

S

SA (security association)
  establishing for IPSec 284
  IKE SA lifetime 282
  ISAKMP protocol 282
  mode configuration option for VPNs 295
  reauthentication after IKE SA expires 295
  selection for IPSec on remote access VPN 293
SAA (Service Assurance Agent) 362–365
SAFE (Security Architecture for Enterprises) 91, 377–383
  Blueprint for Enterprise Networks, web site 97
  out-of-band management, network IDS 220
  overview of architecture 379
  references for further information 382
  summary of 382
  WLAN design 342
SANS Institute 385–390
  policy, standard, and guideline, definitions of 387
  programs and initiatives 385
  references for further information 389
  Security Policy Project 386
  templates for security policies 387–389
scalability
  for cryptographic applications 302
  key exchange with PKI 307
  network configuration, stateless firewalls and 163
  nonscalable methods of public key distribution 301
scanning functions, WLANs 333

SCIF (Sensitive Compartmented Information Facilities), physical security manual 44
scope of a security policy 82
  example policy for a VPN 86
script kiddies 6
scripting languages, most popular for browser plug-ins 118
secret key cryptography 48
secret passwords, enabling for Cisco routers 132
Secure Agent Managers, Cisco 206
Secure Agent, Cisco 204–205, 206
secure areas 49
Secure Hash Algorithm (SHA) 71
Secure Integrated Software, Cisco 212
Secure Policy Manager (Cisco), alarm-reporting feature 217
Secure Server Certification authority 38, 310
Secure Shell. *See* SSH
Secure Socket Layer. *See* SSL
Security Architecture for Enterprises. *See* SAFE
security cards 41
security guides (NSA) 394
security incidents 81
  handling procedure 82, 84
security levels
  Internet Explorer 119
  PIX Firewall interfaces 167, 183
security plan 82
  deny all and allow all models 83
security policies 79–88, 91
  auditing state of 95
  connection-based 166, 183
  defining 81
  development process 82
  development team 83
  development, best practices 378
  IDSs based on 198
  importance of 81–82
  incident handling process 84
  key components of 82
  main purpose of 82
  mixing models, problems with 83
  personnel awareness of 46
  reusable passwords and 50
  sample security policy for a VPN 86
  SANS templates for 387–389
  security wheel 84
  senior management enforcement of 7
Security Policy Project (SANS) 386
security servers
  Cisco ACS 242
  Kerberos 48, 241, 250–252
  RADIUS 245–249
  TACACS+ versus RADIUS 250
security training and certification. *See* SANS Institute
security wheel 81, 84–85
senior management, responsibilities for network security 7
Sensitive Compartmented Information Facilities (SCIF), online information 100
sensor components and architecture 208
sensors, IDS 41, 193
  host sensor components and architecture 204
  maintenance of 221
  network sensors 209
    communication with director 217
    components and architecture 208
    placement on the network 210
SEP (Scalable Encryption Processing) 292
separate service subnet (SSN) 165, 170
SEQ/ACK (Sequence and Acknowledgment) numbers
  attackers, use by 25
  in connection hijacking 26
sequence numbers, TCP 20
  prediction of in connection-killing attacks 25
  SYN (Synchronize sequence numbers) flag 23
server digital ID or website certificate 38
Service Level Agreements (SLAs), verifying with SAAs 362
service password-encryption command 135, 153
service set identifiers. *See* SSIDs
services
  router, turning off or restricting access to 137
  selectively enabling or turning on all for host system 83
  unnecessary, disabling, or removing 109
    list of services that can be disabled 110
session cookies 123, 124

session table, NetScreen 171
sessions
  TCP and UDP, management by CBAC 148
SHA-1 (Secure Hash Algorithm) 71
show aaa user all command (Cisco IOS) 239
show access-lists command 145, 255
  reflexive access lists 147
show accounting command (Cisco IOS) 239
show ip nat translations command 176
show privilege command 239
show rtr command 364
show rtr history command 365
signature recognition (biometrics) 55
signature-based IDS 194, 195
  pros and cons of 196
  updating signatures 221
Simple Network Management Protocol. *See* SNMP
single logon (Kerberos) 252
Single Loss Expectancy (SLE) 9
single root CA 305
site security architecture 82
Site Security Handbook (RFC 2196) 81
site-to-site VPNs 270
small office/home office (SOHO) hardware 331
smart cards 41, 256
  token-based authentication 42
smoke, temperature, and humidity sensors 45
Smurf attacks 162, 198
Sniffer Pro (WLAN packet analyzer) 336
sniffing on publicly accessible networks 72
SNMP (Simple Network Management Protocol) 356–362
  access to routers via 131
  configuration 359–361
  notifications 357
  RMON, using with 361
  SAA, accessing with 363
  setup (case study) 366
  versions 358
snmp-server command 359
SoBig virus 51
social constraints
  network design 94
  on network IDS 203
social engineering 31
  countermeasures 32
sockets 19
software
  protection with hardware keys 42
  unpatched, security threats from 6
software firewalls (Check Point) 173
source and destination IP addresses, TCP/IP connections 19
source and destination port numbers 19
Source Quench message 22
speech analysis 54
speed, network interface 185
split tunneling 87
spoof attacks 162
spoofing
  antispoofing protection, router configuration 154
  countermeasures 31
  techniques for 29
spyware 5
SSH (Secure Shell) 47–48
  versions 48
  wireless network security, using for 342
SSIDs (service set identifiers) 334
  vulnerabilities of 336
SSL (Secure Socket Layer) 48–49, 71
SSN (separate service subnet) 165, 170
standard IP access lists 139
standard numbered IP access lists, additional keywords supported 140
standard, definition of 387
standards for telecommunication equipment 35
state information for TCP and UDP sessions, CBAC and 148
stateful filtering (firewalls) 162
stateful firewalls 163
stateful pattern-matching IDS systems 195
stateless filtering 162
static and dynamic translation slots, ASA and 167
static routing on a PIX Firewall 188
stations, wireless 333
  SAFE design recommendations for 343
  scanning for other stations or access points 333
statistical anomaly detection 200
stream ciphers 64
subnet masks 140, 182
survivability and recovery, physical security planning 101
switches and hubs, network security design 101
  switch security features, examples of 102

switches, configuring for traffic-capture functions 211
Sygate firewall 174
symmetric key algorithms 64–66
  AES 64, 66, 283
  DES (Data Encryption Standard) 64, 272
  Triple DES (3DES) 65–66, 272, 283
symmetric key encryption 272
SYN (Synchronize sequence numbers), TCP flag 23
SYN-flooding attacks, prevention by CBAC 148
SysAdmin, Audit, Network, and Security. *See* SANS Institute
SYSLOG 354
SYSLOG server
  router configured to send more information to 355
  router configured to send only warnings 355

T

TACACS+ 241, 258–265
  accounting 245
  ACS log 265
  authorization 243
  lock-and-key feature 253–256
  RADIUS versus 250
  summary of 244
  user authentication 144
tailgating 101
TCP 18–20
  additional information on, RFC 793 20
  Layer 4 of OSI model 162
  segment format 19
  sequence number prediction 25
  three-way handshake preceding data exchange 20
TCP connections
  resetting capability, network IDSs 215
  resetting with router configured for nework IDS 212
TCP SYN flood attacks 161
TCP SYN packets, in Land.C attacks 161
TCP/IP protocol suite
  fragmentation reassembly code 161
  IP layer 16
  mapped to OSI model 16
  security issues 20–27
  weaknesses of 14–16
    closing a connection by FIN 25
    covert channels 21
    hijacking TCP connections 26
    IP fragment attacks 23
    SYN flood 25
    TCP flags 23
TCP/UDP ports, stateless firewalls and 163
teardrop attacks 161
technological constraints
  on network design 93
  on network IDS 203
telecommunications standards 35
telecommuter connecting to branch office, protecting routers (case study) 152–156
telegraph, cryptography and 62
telephone calls, used in social engineering attacks 31
telephony, IP 97
Telnet
  access to routers 131
  router sessions via, configuring VTY password 132
Temporal Key Integration Protocol (TKIP) 340
Terminal Access Controller Access Control System plus. *See* TACACS+
terminals, logical virtual type (VTY) lines 133
terrorism
  Internet exploitation 14
  physical security and 44
theft, risk of 9
three-way handshake, TCP connections 20
  flags used in 23
  timers and TCP flags, sequences of 25
time-based access lists, routers 146
timeout
  console port of routers 135
  and thresholds in session management by CBAC 150
timers, TCP/IP sessions 25
TKIP (Temporal Key Integration Protocol) 340
TLS (Transport Layer Security) 48, 71
Token Ring networks
  802.5 wireless standard, IEEE 332
  NetScreen firewalls and 171
  speed, values for 185

token-based authentication systems 42
tools used in network design process 81, 94
topologies of trust, PKI 302
traffic filtering, CBAC 148
traffic inspection, CBAC 148
traffic, inbound and outbound 168
traffic, network
    analysis of 95
    monitoring with RMON and SNMP 361
    simulating 96
transform sets 282–283
    establishing use of in IPSec policy 284
translation slots, PIX Firewall 168
translation table (NAT), viewing on Cisco router 176
Transmission Control Protocol. *See* TCP
Transmission Control Protocol/Internet Protocol. *See* TCP/IP protocol suite 14
Transport Layer Security (TLS) 48, 71
transport layer, OSI 18
transport mode (IPSec connections) 280
traps, SNMP 357
    configuring recipient of 360
    configuring router to send 361
Triple DES. *See* 3DES encryption algorithm
Trojan horses 5, 161
troubleshooting SNMP, commands for 360
trust 3–4
trusted sites security zone (Internet Explorer) 118
trusted third-party protocol (PKI) 302
    enrollment procedure for PKI users 306
    topologies of trust, PKI 304
tunnel mode (IPSec) 281
tunneling
    GRE (generic routing encapsulation) tunnels 271
    LAN-to-LAN or Remote Access tunnel type 294
    selecting protocol for VPN 292
    split tunneling 87
two-factor identification 256
typing biometrics 54

U

UDP bomb 161
UDP ports, stateless firewalls and 163
UDZs (user-defined zones) 171
unauthorized programs, potential security holes from 6
uninterruptible power supplies (UPSs) 45, 101
universal serial bus (USB) Smartcard key (eToken) 256
unpatched software, security threats posed by 6
unsafe environments, communicating and doing business safely in 80
untrusted 4
URG (Urgent pointer field), TCP flag 23
URL filtering. *See* content filtering
URLs, secure (https) 37
use policy for the network resources 81
User Datagram Protocol (UDP) service, use in chargen attack 161
user-defined zones (UDZs) 171
usernames, capture by Trojan horses 161
users
    configuring for SNMP 360
    VPN 296

V

ventilation requirements for network equipment 93, 100
view record, creating or modifying 359
Virtual Private Networks. *See* VPNs
virtual type terminal (VTY) lines 132–133
viruses 5
    antivirus software 51, 181
    enabled by Trojan horses 161
    risk of 9
    smart card protection against 42
VMS Management Center for IDS, Cisco 217
voice communication over IP, government role in security 8
voice recognition 54
VPN concentrator 87
VPNs (virtual private networks) 269–299
    case study, remote access VPN 285–298
    enrollment of devices in PKI 307
    GRE (generic routing encapsulation) tunnels 271
    IPSec (IP Security) 272–283
        antireplay protection 277
        data integrity 273
        origin authentication 274–277
        protocol framework 277
        transform sets 282

tunnel or transport mode 279
PKI solution for authentication 301
types of 269
using IPSec with
configuring IPSec 285
preparation for 284
wireless network security, using for 342
VTY (virtual type terminal) lines 132–133
vulnerabilities 13–32
buffer overflows 28
communications over public networks 72
on data port 139, 161
fingerprint scanning 54
information about, in CSEC 162
internal and external 5–6
log file alteration or deletion by intruders 114
patching 86
reusable passwords 50
risk and 13–14
shared key authentication, WLANs 337
social engineering 31
countermeasures 32
software-based firewalls 174
spoofing techniques 29
SSIDs, WLAN 336
TCP/IP security issues 20–27
WEP protocol 338
countermeasures to 339

W

W3C extended Log File Format 113
WAN (wide area network) bandwidth, cost of 94
war-driving and war-chalking 342
warm site (disaster recovery plan) 46
warning level of information sent to SYSLOG server 354
warnings, Syslog 355
weak passwords 50
weaknesses. *See also* vulnerabilities
internal and external 5–6
of TCP/IP protocol suite 14–16
Web applications 14
web of trust 302
web security 107
hardening 107–123
browsers 118–123
case study 124–128
file systems 107–109
web servers 109–117
SSL as standard for 48
web servers
attacks against, prevention with signature-based IDS 196
denial-of-service (DoS) attacks against 20–21, 24, 161, 163, 198
hardening 112–117
logging, enabling 113
restricting access to a website 114–117
securing, tasks involved in 109
web-based requests (PKI enrollment) 307
website certificates 38
websites
information on network security 428
restricting access to 114–117
SSL-enabled 48
Well-Known Ports 19
WEP (wired equivalent privacy) protocol 334, 336
countermeasures to vulnerabilities 339
overview of 337
vulnerabilities of 338
WEPCrack program 338
wheel cipher 62
Windows Internet Naming Service (WINS) 295
Windows systems
file systems, hardening 107–109
integrated authentication 116
software patches for 6, 7
wired equivalent privacy. *See* WEP protocol
wireless
how it works 333
standards for WLAN applications 328
wireless and voice communication over IP, government role in security 8
wireless local-area networks. *See* WLANs
wireless network interface cards (NICs) 328
wireless networks
building-to-building, types of 330
community networks 330

wireless security 327–350
  adding wireless to secure network 344–349
  SAFE WLAN design 342
  war-driving and war-chalking 342
Wireless Security Suite, Cisco 339, 342
WLANs (wireless LANs) 327
  different configurations of 328–331
  EAP protocol and 802.11i standard 340
  hotspot 330
  how wireless works 333
  overview of 331
  peer-to-peer 329
  risks of open wireless ports 336
  SAFE WLAN design 342
  setting up WLAN connection 333
worms 5

X

X.509 standard for digital certificates 35
xlate. *See* translation slots, PIX Firewall
XOR (exclusive OR) function 338

Z

ZoneAlarm firewall 174
zones
  firewall 171
  DMZs. *See* DMZs
  peer-to-peer WLAN 329