

INDEX

Note to the reader: Throughout this index **boldfaced** page numbers indicate primary discussions of a topic. *Italicized* page numbers indicate illustrations.

Symbols & Numbers

(pound sign), for privileged mode in PIX, 557
\$ (dollar sign), in share names, 163
\$PATH variable in Linux, 263
> (greater than) symbol, for unprivileged mode in PIX, 557
3DES (Data Encryption Standard), 625
10Base2 Ethernet, 876
10BaseFL, 876
10BaseT, 876
10VGAnyLAN, 876
100BaseVG, 876
100VG (Voice Grade), 876
802 specifications. *See* IEEE specifications

A

AC circuit, 48
access control, **808-817**
 to Samba, **318-328**
 authentication by username and password, **322-328**
 restricting access by computer, **319-322**
 security groups, **811-817**
Access Control List (ACL), **229**, 760, 808, **809-811**, 876
 for blocking in PIX, **589-592**
 impact of moving security principals, 783
 implementation, 810-811
 integration with Samba, **344-349**
Access Control rights in NetWare 6
 for directories, 215
 for users and groups, 217
access mask, 138
access points in WiFi, 60
access token in Windows NT, 771
Access Tokens in Windows 2000, 135-136
 inheriting, **136-137**
Access VPN, 614
account domains, upgrading to Windows 2000, **765-767**
account lockout policy, 854
Account Operators group on domain controller, permissions, 814
account policies, 791, **853-854**
accountability, 115
accreditation, **40-41**
ACE/Server, 109
acknowledgment (ACK), 876
ACL (Access Control List). *See* Access Control List (ACL)
 across-domain referral, 805
 action, for state transition, 22
 Active Directory, 117, **146**, 760, 876
 auditing, 840, **841**
 authentication, 796
 Active Directory Users and Computers snap-in, 796, 797
 for group policy management, 158, 159
active hub, 876
active monitor, 876
active security, 484
Active Server Pages (ASP), 832
Ad-Hoc mode for WiFi, 60
ad hoc RF network, 877
adapter, 877
Adaptive Security Algorithm (ASA), and security levels, **554-556**
adaptivity, 5, 9
Add or Delete Self rights in NetWare 6, for properties, 229
Add Sensor Wizard (Cisco), **688-691**
 to add IDSM object, 720, 720-721, 721
 Default Gateway Address page, 690, 690

- Sensor Configuration page, 690–691, 691
- Sensor Configuration Verification page, 691
- Sensor Identification page, 689
- add user script in Samba, 325–326
- address, 877
- address record, 877
- Address Resolution Protocol (ARP), 428
 - routers and, 432–433
 - Windows NT and, 441–442
- address spoofing, protection against, **523–524**
- Adleman, Leonard, 107
- Admin password, VPN Hardware Client changes, 654–655
- ADMIN\$ share, 163
- Admin user in NetWare 6, 212, 226
- administrative accounts in Windows 2000, minimizing use, 141
- administrative shares, 163
- Administrators group
 - default permissions, 814
 - on domain controller, permissions, 814
 - in Windows XP, 183–184
- ADSL (asymmetrical digital subscriber line), 877
- Advanced Encryption Standard (AES), **102**, 625
- Advanced Security Settings dialog box (Windows XP), 196
 - Permissions tab, 196
- advertised applications, by IntelliMirror, 789
- AES (Advanced Encryption Standard), **102**, 625
- aggressive mode communication in IKE, **636**
- AH (Authentication Header) protocol, 103
- algorithm, 118
- alias record, 877
- aliases for IP addresses, 568
- All attribute in NetWare
 - for directories, 221
 - for files, 223
- all-networks broadcast, 79
- alternating current, 48
- alternatives, 14
 - defining, 14–15
 - documentation of, 36
- Altiga client, 617, 656
- American National Standards Institute (ANSI), 101
- analog circuits, vs. digital communication, 47
- anonymous users, 115
 - Samba restrictions, 328
- ANSI (American National Standards Institute), 101
- anti-replay in IPSec, 618
- antivirus software, **245–247**, 877
- AnyLAN, 877
- Apollo Command Module, risks, 31–32
- Append Data event, auditing, 842
- Application layer, 877
- application-level gateways, 209
- application-level proxies, 384–385
- application partition in IDSM filesystem, 722
- application proxies, 534
- Application Specification for Windows 2000, 827
- applications. *See also* software
 - compatibility with Windows 2000 upgrade, **778–780**
 - secure, **833–834**
- Archive Needed attribute for NetWare files, 223
- ARCnet, 877
- arity of set, 18
- ARP (Address Resolution Protocol), 428
 - routers and, 432–433
 - Windows NT and, 441–442
- ARP table, 877
- ASA (Adaptive Security Algorithm), and security levels, **554–556**
- ASP (Active Server Pages), 832
- Associated Network Service, for Cisco sensors, 689
- asymmetric algorithm, 118, 119
- asymmetric key encryption, 626, 770
- asymmetrical digital subscriber line (ADSL), 877
- Asynchronous Transfer Mode (ATM), **67–68**, 877–878
- Atkins, Todd, 291
- atomic signature for Cisco sensors, 743
- Attachment Unit Interface (AUI) port, 878
- audit logs in Windows 2000, **773–774**
- Audit Object Access Properties dialogbox, 202
- audit policies, **838–844**

- auditing auditors, **844–845**
 - best practices, **843–844**
 - establishing, **838**
 - implementation, **839–843**
 - for Active Directory, **841**
 - for filesystem, **842–843**
 - auditing
 - files and folders, in Windows XP, **199–203**
 - passwords, in Linux, **311–315**
 - AUI (Attachment Unit Interface) port, 878
 - authentication, 83, 116, **795–807**. *See also* passwords
 - in Bluetooth, 63
 - cryptographic, 169
 - of data origin with IPsec, 618
 - encryption for, **387–388**
 - in Windows 2000, **128–129**
 - ISA Server and, 463
 - Kerberos, **801–805**. *See also* Kerberos
 - need for improved, **87–90**
 - pass-through, 763
 - in SafeNet client, **661**
 - in Samba, **322–328**
 - smart card, 772, **805–807**
 - support in Symantec Enterprise Firewall, 457
 - tracking failures, 286
 - administrator notification, 294–295
 - user and machine, 171
 - in Windows 2000, **770–771**
 - Authentication Headers in IPsec, 170, 619, **619–620**
 - authenticator in Kerberos, 147
 - Authenticode (Microsoft), **828–830**
- ## B
- B channel (bearer channel), 878
 - back channels, NAT problems, 434
 - backbone, 878
 - backbone segments, accessibility to attack, 56
 - Backup Domain Controller (BDC), 878
 - upgrades, 763
 - Backup Operators group in Windows XP, 184
 - backup plan, 878
 - backup server, security case study, 30
 - backup window, 878
 - backups, Windows XP rights to run, 186
 - bandwidth, 878
 - groups for conserving, 816–817
 - for T1 line, 64
 - baseband, 878
 - baseline, 878
 - of tripwire, 310
 - baud, 5
 - BDC (Backup Domain Controller), 878
 - Bertalanffy, Ludwig von, 6
 - binding Samba to specific network interfaces, **318–319**
 - biometric identification, 772
 - BIOS for PIX Firewall, **547**
 - black box view, 7, 8
 - blackout, 904
 - blank, 878–879
 - block cipher, 92–94, 93, 118
 - Blowfish, 123
 - Bluetooth, 60, 61–62
 - BNC connector, 879
 - bonding, 879
 - bootp, 500
 - bootstrap mount point, 278
 - border security, 374. *See also* firewalls
 - hidden crossings, 392
 - options, **394–402**
 - disconnection, **400–402**, 401
 - dual firewalls and demilitarized zones, 398, **398–399**
 - enterprise firewalls, **399–400**, 400
 - filtered packet services, 395, **395–396**
 - single-firewall approach, **396–398**, 397
 - reinforcing, **394**
 - BorderManager (Novell), 210
 - bound transmissions, **52–54**
 - boundaries of system, 7
 - bounded media, 879
 - breakable cipher, 118
 - breaking codes, 120

Bridge mode, 60
 bridges, **69–73**, 70, 879
 vs. routing, **80**
 broadband, 879
 broadband fixed wireless, 68
 broadcast address, 879
 broadcast frame, 72
 brouter, 879
 brownout, 904
 Browse rights in NetWare 6, for objects, 228
 brute force attacks, **97–99**
 buffer overflows, 37
 buffer zone. *See* demilitarized zones
 bugs in firewall software, 390–391
 BugTraq mailing list, 258
 Bureau of Export Administration, 99–100
 bus, 879
 bus topology, 879

C

C2 Red Book certification, 247, **248**
 cable, 879
 cable map, 879
 cable-modem routers, risks, 582
 cable tester, 879
 cache poisoning, **89–90**
 caching by ISA Server, 465
 Caesar ciphers, 91
 Caldera OpenLinux, **253–254**
 security advisories, 254
 capture keyword in VLAN access control list entry, 713
 carrier, 880
 Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA), 880
 Carrier Sense Multiple Access/Collision Detection (CSMA/CD), 880
 Carrier Sense Multiple Access with Collision Detection (CSMA/CD), 57
 carrier wave, 53
 case
 of Samba passwords, 327–328
 of Unix username and password, 680
 Catalyst 6000 IDS. *See* Cisco Secure IDS sensors
 catchall rule in iptables, 508–509
 categories, 880
 cattach command (Linux), 279
 CD circuit, 48
 cdetach command (Linux), 279
 cells, 880
 for ATM, 67
 central office, 880
 central processing unit (CPU), for PIX Firewall, **544**
 certificate authorities, 103, 353, **632–633**
 certificates for SSL
 creating, **353–356**
 directory for, 352
 certification, **38**
 Certified For Microsoft Windows logo, 827
 CET (Cisco Encryption Technology), 615
 CGI (Common Gateway Interface), 832
 chains in Linux, 501–502, 508
 packet filters, 509
 change, 28
 change permission in Windows XP, share-level, 164, 194
 Change Permissions event, auditing, 842
 Change Permissions permission in Windows XP, 198
 Channel Service Unit (CSU), 880
 Checkpoint Firewall-1, 437–438, 440–442, **447–454**
 cost and support, **454**
 documentation, **453**
 interface, **451–452**, 452
 major feature set, **448–449**
 VPN features, 449
 minor feature set, **449–451**
 centralized client/server management, 450–451
 policy-based configuration and management, 450
 SecurID for client authentication, 109
 security, **453**
 checkpoints, 880
 checksum, 880
 child domains in Windows 2000, 764
 CIDR (Classless Internetwork Domain Routing), 881

- cipher key. *See* crypto key
- ciphers, 119
 - for Samba, 359
- ciphertext, 91
- CIR (Committed Information Rate), 66
- circuit layer proxy, ISA Server as, 462
- circuit-level gateways, 209, 386
- circuit switching, 880
- Cisco. *See also* PIX Firewall
- Cisco Encryption Technology (CET), 615
- Cisco IOS Firewall, **540–541**
- Cisco routers, **615–616**
- Cisco Secure, 615
- Cisco Secure IDS sensors, **694–696**
 - 4200 series deployment, **667–672**
 - basic installation, **668–669**, 669
 - device management installation, **669–670**, **670–671**
 - firewall sandwich installation, 671
 - remote installation, **672**, 673
 - 4200 series installation, **675–679**
 - 4210 physical layout, 675–676, 676, 677
 - 4230 physical layout, 677–679, 678
 - management access, **679**
 - 4200 series logon, **679–681**
 - 4200 series management
 - CSPM configuration for, **688–695**
 - IDS software version, 733
 - saving and uploading configuration, **694–695**
- advanced configuration, **743–755**
 - multiple directors, **753–755**
 - packet reassembly, **743–751**
 - PostOffice settings, **751–753**
- basic configuration, **732–743**
 - internal networks, **734–738**, 735, 737
 - log files, **740–743**, 742
 - monitor interface, **738–740**, 740
 - sensor identification, 732, **732–733**
- Catalyst 6000 IDSM, **696–703**
 - architecture, **697–703**
 - configuration verification, **718–719**
 - CSPM configuration for, **719–721**
 - deployment, **673–674**, 674
 - features, **696–697**
 - filesystem, **722–723**
 - initial configuration, **705–709**
 - installation, **703–704**
 - management access, **704–705**
 - troubleshooting, **728–729**
 - updating files and partitions, **723–727**
- Catalyst 6000 IDSM traffic-capture parameters, **709–718**
 - command-and-control port VLAN, **709–710**
 - monitoring port to control trunk traffic, **716–718**
 - using SPAN, **710–712**
 - using VACLs, **712–716**
- first time configuration, **681–687**
 - completion, 687
 - IP configuration parameters, 682–683
 - PostOffice communication parameters, 683–684, 684
 - System Management parameters, 685–687
- Cisco Secure Policy Manager (CSPM)
 - adding object to database, **692–693**
 - Advanced tab for sensor object
 - Additional Destinations, 754, 754–755
 - Postoffice settings, 752
 - configuration for Cisco 4200 series sensor, **688–695**
 - configuring for IDSM management, **719–721**
 - database, 731
 - Logging tab for sensor object, 742, 742–743
 - Properties tab for sensor object
 - Identification, 732, 732–733
 - Internal Networks, 737, 737, 738
 - saving and updating configuration, **694–696**
 - Sensing tab for sensor object, 738–740, 740
 - Advanced Sensor Settings, 747
- Cisco VPN Concentrator, **616**
- Cisco VPN devices, **643–661**
 - VPN 3005 Concentrator, **644–646**, 646

- VPN 3015 through 3080 Concentrators, **646-648**, 647, 648
- VPN Concentrator client support, **648**, 649
- VPN Hardware Client, **649-656**, 650
 - managing, 655, **655-656**
 - Quick Configuration Utility, **650-655**, 651
- VPN software clients, **656-661**
 - SafeNet client, 660, **660-661**
 - Unified Client, **656-660**, 657
- class of computer, 817
- Classless Internetwork Domain Routing (CIDR), 881
- clear command (PIX), 559
- cleartext, 84
 - in e-mail, 830
 - passive monitoring, **86**
 - for passwords, **329-341**
 - in Windows operating systems, **340-341**
 - protocols using, **87**
- client certificates for SSL, creating, **354-356**
- client/server network, 881
- clients, 881
 - of Samba, configuration to use SSL, **360-363**
 - system upgrades in Windows 2000, **776-777**
- clipper chip, 881
- clock command (PIX), **567**
- clock set command (PIX), 559
- clustering, 881
- mkdir command (Linux), 279
- CNAME record, 881
- Co-concurrence constraint, 20-21, 21
- coaxial cable, 881
- code, 119
- code authentication, 773
- collision, 881
- collision detection, 57
- collision domains, 71, 72
- collision light, 881
- .COM files, Read Only attribute, 244
- command-and-control interface, for sensors, 667
 - command-and-control port
 - assigning to VLAN, 709-710
 - on IDSM, 699
 - command-line interface for PIX Firewall, **556-564**
 - access methods, **556-557**
 - commands, **558-564**
 - editing in, **558**
 - modes, **557-558**
 - commit security acl command, 714
 - Committed Information Rate (CIR), 66
 - Common Gateway Interface (CGI), 832
 - communication between PIX Firewall interfaces, security levels and, 572
 - Compare rights in NetWare 6, for properties, 229
 - Complementarity in Systems Theory, 5
 - complexity in Systems Theory, 5
 - composite signature for Cisco sensors, 743-744
 - computationally secure cipher, 118
 - Computer Administrator account (Windows XP), 183
 - Computer Associates eTrust, **472-475**
 - Computer Management snap-in, Shared Folders extension, 162
 - computer policies, group policies to control, 152, 153-154
 - computers
 - authentication, in Windows 2000, **128-129**
 - restricting Samba access by, **319-322**
 - Windows XP rights to change time, 186
 - concentrator client (Cisco), 617
 - conceptual definition, 34
 - conditional trigger, 22
 - confidentiality of data, 773
 - with IPSec, 618
 - in Windows 2000, **772-773**
 - configuration mode, for PIX Firewall command-line interface, 558
 - configure terminal command (PIX), 558
 - configuring computers. *See* group policies
 - conflict resolution, 12
 - conflicting objectives, 11

- connection-oriented, 882
- connection-oriented transport protocol, 882
- connection slots in PIX Firewall, 550
- connectionless, 881
- connectionless transport protocol, 881
- console, to access PIX Firewall, 556
- ConsoleOne (NetWare 6), 225, **233–243**
 - to change directory and file rights, **236–240**
 - to change object and property rights, **241–243**
 - directory rights in, 215
 - file attributes display, 225
 - revoking property right, **235–236**
- constraints, 12
 - types, 20
- Constructivity in Systems Theory, 6
- containers in NetWare, granting rights to, 240
- content filtering, firewalls for, 376
- Content Vectoring Protocol (CVP), 451
- contingency, multilayered plans, 32
- Control Panel, 882
- controller, 882
- copy command (PIX), 559
- Copy Inhibit attribute for NetWare files, 223
- copying files, EFS and, 861
- core dump size in Linux, limiting, **275–276**
- core OS, 882
- cost, 882
 - Checkpoint Firewall-1, **454**
 - of Linux firewall, 499
 - Microsoft Internet Security and Acceleration Server, **468–469**
 - Symantec Enterprise Firewall, **460**
 - TCO (Total Cost of Ownership) study, 15
- country codes, 882
- courses of action, 14
- Cox, Alan, 501
- cracker
 - access to Administrator account, 163
 - access to ATM data, 67
 - attack on packet filters, **416–418**
 - IP address forging, 408
 - network access through switch, 75
 - network analyzer use by, 86
 - password access, 129
 - restricting with IP address filtering, **407–408**
 - source routing, 410, **439–440**
- CRC (cyclical redundancy check), 882–883
 - of executable files, 246
- Create All Child Objects event, auditing in Active Directory, 841
- Create Files event, auditing, 842
- Create Files/Write Data permission, in Windows XP, 197
- Create Folders/Append Data permission, in Windows XP, 197
- Create Folders event, auditing, 842
- Create rights in NetWare 6
 - for directories, 215
 - for objects, 228
 - for users and groups, 217
- credibility, 40–41
- critical resources, and sensor placement, 664
- crossover cable, 882
- crosstalk, 882
- cryptanalysis, 120
- cryptanalysts, 120
- crypto algorithm, 91
- crypto key, 91
 - generating, **126–127**
 - management, **96**
 - size of, 98
- cryptographic authentication, 169
- Cryptographic File System, **277–280**
 - configuring, **278–279**
 - installing, **277–278**
- cryptography, **117–133**. *See also* encryption
- CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance), 880
- CSMA/CD (Carrier Sense Multiple Access with Collision Detection), 57
- CSMA/CD (Carrier Sense Multiple Access/Collision Detection), 880
- CSPM (Cisco Secure Policy Manager). *See* Cisco Secure Policy Manager (CSPM)
- CSU (Channel Service Unit), 880
- Ctrl+Alt+Del keyboard interrupt, to start WinLogon process, 135, 136

CUSeeMe, NAT problems, 434
 CVP (Content Vectoring Protocol), 451
 cyclical redundancy check (CRC), 882–883
 of executable files, 246

D

D channel (delta channel), 883
 D-type connector, 885
 DACL (Discretionary Access Control List), in
 Windows 2000 security descriptor, 138
 DAS (dual-attached stations), 885
 data
 integrity, 772–773
 with IPSec, 618
 nature of, **16**
 value, and transmission selection, 54–55
 data center management, in technical support,
 786–787
 Data Encryption Standard (DES), 97, **101**,
 119, 123
 Data Link Connection Identifier (DLCI), 66
 Data Link Layer, 883
 data packet, 883. *See also* packets
 data payload encryption, 169
 data recovery, in Encrypting File System,
 864–867
 Data Service Unit (DSU), 883
 datagrams, 883
 settings for fragment reassembly, 747
 daylight savings time, PIX Firewall clock
 and, 567
 Debian Linux, **256**, 257
 debug command (PIX), 559–560
 decision analysis, 9. *See also* systems analysis
 decision-making process, in IPSec, 638,
 638–639
 Default Domain Controllers Policy, 768
 default file permissions in Linux, **275**
 default gateway, 883
 in Add Sensor Wizard, 690, 690
 address for PIX, 575
 defense in depth, 13, 32, 539
 delegation of administrative tasks, **835**
 authority and security groups, **845–850**
 Group Policy objects control, 850,
 858–859
 delegation of authentication, in Kerberos, 150
 Delegation of Control Wizard, 848, 849
 Delete All Child Objects event, auditing in
 Active Directory, 841
 Delete event, auditing, 842
 Delete Inhibit attribute in NetWare
 for directories, 221
 for files, 223
 Delete permission, in Windows XP, 198
 Delete rights, in NetWare 6, for objects, 228
 Delete Subfolders and Files event, auditing, 842
 Delete Subfolders and Files permission, in
 Windows XP, 198
 demarcation point, 883
 demilitarized zones, 399, 399, 734
 PIX Firewall with, **597–602**, 598
 outbound connections, 600
 and sensor placement, 665
 trihomed firewall with, **520–523**, 521
 demodulator, 53
 denial of service (DoS) attack, 883
 deploying secure applications, **827–833**
 DES (Data Encryption Standard), 97, **101**, 119,
 123, 625
 exhaustive key search on, 99
 vulnerability, 279
 Desktop shortcuts in Windows 2000, for
 shares, 162
 desktop support management, **785–786**
 destination port number, 883
 Development and Acquisition in SDLC, **36–38**
 certification, 38
 component and code review, 36–37
 system test review, 37–38
 device-based firewalls, 469
 device drivers, Windows XP rights to
 manage, 187
 DHCP (Dynamic Host Configuration Protocol),
 500, 885
 and PIX Firewall, 570, 575
 diag bootresults command (IDSM), 729
 diag resetcount command (IDSM), 719
 diagnostics configuration mode for IDSM, 719

- dial-up connection to ISP, modems for, 393, 394
- dial-up server, single-homed, sample firewall scenario, **515–517**, 516
- dialogs, 883
- differential cryptanalysis, 121
- Diffie, Whitfield, 94, 125
- Diffie-Hellman key exchange in IPsec, **625–627**
- digest, 124
- digital certificate servers, **102–103**
- digital certificates, 90
- digital communication, 46, **46–47**
 - on noisy circuit, 47
- digital signature, 95, **129–130**
 - in Windows 2000, **772–773**
- digital subscriber line (DSL), 884
- direct current, 48
- Director, alarms to multiple, **753–755**
- Director PostOffice parameters for IDSM, 708
- directories, 884
 - attributes in NetWare 6, **221–222**
 - auditing access, 840, 841
 - for Cryptographic File System, 278–279
 - permissions in Linux, **271–276**
 - limiting core dump size, **275–276**
 - suid and sgid, **271–274**
 - umask setting, **275**
 - rights in NetWare, **214–216**
 - ConsoleOne to change, **236–240**, 237
 - IRF and, **217–220**
 - sharing in Windows 2000, **160–164**
 - for SSL certificates, 352
- directory service, 884
- disable command (PIX), 557
- disabled user account in Windows XP, enabling, 190
- disaster recovery, 884
- disconnection from Internet, **400–402**, 401
- Discretionary Access Control List (DACL), 138
- disk striping, 884
- disposal in SDLC, **41–42**
- distance vector routing protocol, 884
- distributed security strategies, **794–835**
 - access control, **808–817**
 - access control list (ACL), **809–811**
 - security groups, **811–817**
 - authentication of user access, **795–807**
 - Kerberos, **801–805**
 - passwords, **798–800**
 - smart card, **805–807**
 - deploying secure applications, **827–833**
 - managing administration, **834–835**
 - protection for sensitive data, **819–827**
 - Encrypting File System (EFS), **820–822**
 - IPsec (IP Security), **823–827**
 - uniform security policies, **817–819**
 - Distribution Host for Cisco sensors, 690
 - DIX, 884
 - DLCI (Data Link Connection Identifier), 66
 - .DLL files, downloading, 361
 - DMZ. *See* demilitarized zones
 - DNS (Domain Name Service), 884
 - configuration for VPN HardwareClient, 654
 - port for, 380
 - DNS poisoning, **89–90**
 - DNS server, 884
 - DNS zone, 884
 - documentation, 35
 - model symbols, 17–23
 - DoD Networking Model, 884
 - dollar sign (\$) in share names, 163
 - domain-level security, for Samba, **326–327**
 - domain local groups, 812
 - domain model in Windows 2000, **760–762**
 - migrating, 761, **761–762**
 - upgrades, 763
 - domain-name command (PIX), 568
 - Domain Name Service (DNS), 884
 - port for, 380
 - domain policies, 155
 - Domain Security Policy administrative tool, 853
 - domains in Windows 2000, 884
 - consolidation, 763
 - planning migration, **767**
 - policies, 860
 - reasons to restructure, **780–781**
 - restructure, 763
 - implications, **783–785**

- vs. upgrade, **782–783**
- when to restructure, **781–783**
- trust relationships between, **149–152**
- upgrading account domains, **764–765**
- upgrading resource domains, **765–767**
- Don't Compress attribute in NetWare
 - for directories, 221
 - for files, 223
- Don't Migrate attribute in NetWare
 - for directories, 221
 - for files, 223
- DoS (denial of service) attack, 883
- dotted decimal, 885
- downloading
 - .DLL files, 361
 - IDS update files, 723–724
 - and virus risk, 244
- dpkg tool, 369
- drag and drop for file copying, 143
- DSL (digital subscriber line), 884
- DSL adapter, and firewalls, 440–442
- DSU (Data Service Unit), 883
- dual-attached stations (DAS), 885
- dual-homed firewall, sample scenario, 517, **517–520**
- dual-homed gateways, **534–535**
- dumb terminal, 885
- duplexed hard drives, 885
- duplicate server, 885
- Dynamic Host Configuration Protocol (DHCP), 885
 - PIX Firewall support for, 575
- dynamic nature of systems, 32
- dynamic packet filtering, 886
- dynamic routing, 886
- dynamic translation, 425, **426–428**
 - for PIX Firewall, 578–579
- dynamically allocated port, 885
- e-mail (electronic mail), 886
 - forgery, **427–428**
 - secure, **830–831**
 - from swatch, 293
- e-mail systems
 - security, 130
 - sensitivity of data, 55
- e-ppliance, Gauntlet as, 484
- EAP (Extensible Authentication Protocol), **106**
- eavesdropping, 59
- echo command (Linux), 507
- editing in PIX Firewall command-line interface, 558
- education in security, 27
- EEPROM (electrically erasable programmable read-only memory), 886
- EFF (Electronic Frontier Foundation), 99
- Effective Rights dialog box (NetWare), 215–216, 216
- effective rights in NetWare 6, 219
- EFS (Encrypting File System). *See* Encrypting File System (EFS)
- egress SPAN, 700
- EIGRP (Enhanced Interior Gateway Routing Protocol), 606
- electrically erasable programmable read-only memory (EEPROM), 885, 886
- electromagnetic interference (EMI), **48–50**, 49, 886
- Electronic Frontier Foundation (EFF), 99
- electronic mail. *See* e-mail (electronic mail)
- electrostatic discharge (ESD), 886
- embryonic timeout for TCP session, 750
- emergency boot disk for Linux kernel, 258
- EMI (electromagnetic interference), **48–50**, 49, 886
- empty recovery policy, 866
- enable command (PIX), 557
- enable password command (PIX), 560
- Encapsulating Security Payload (ESP), 104, 170, 621, **621–622**
 - in IPSec, 621, **621–622**
 - NAT problems, 435
- encoding, 886
- encrypted tunnels, 386. *See also* virtual private networks (VPN)
- Encrypting File System (EFS), 128, **142–145**, **820–822**
 - best practices, **867–868**
 - data recovery in, **864–867**
 - and end user, **862–864**

E

- problems, 142–143
- strategy design, **860–869**
- things to know, **861**
- tips for using, **868–869**
- encryption, 83, 90, **90–100**, **117–133**
 - algorithms, **119–125**
 - one-time pad, **121–122**
 - one-way functions, **123–124**
 - public key encryption, **124–125**
 - symmetric functions, **122–123**
 - for authentication, **387–388**
 - file storage on remote servers, **863–864**
 - government intervention, **99–100**
 - in IPSec, **624–625**
 - key generation, **126–127**
 - in Linux, **277–282**
 - methods, **92–95**
 - block cipher, 92–94, 93
 - public/private crypto keys, **94–95**
 - stream cipher, **92**
 - need for, **100–101**
 - one-time pad, **121–122**
 - of passwords, **329–341**
 - in Samba, **333–336**
 - solutions, **101–110**
 - AES (Advanced Encryption Standard), **102**, 625
 - DES (Data Encryption Standard), **101**.
See also DES (Data Encryption Standard)
 - digital certificate servers, **102–103**
 - EAP (Extensible Authentication Protocol), **106**
 - IPSec (IP Security), **103–104**. *See also* IPSec (IP Security)
 - Kerberos, **104–105**. *See also* Kerberos
 - PPTP/L2TP, **105–106**. *See also* PPTP (Point-to-Point Tunneling Protocol)
 - RADIUS (Remote Access Dial-In User Service), **106–107**
 - RSA encryption, **107**, 119
 - security tokens, **108–110**, 109
 - SKIP (Simple Key Management for Internet Protocols), **110**
 - SSH (Secure Shell), **107–108**, 350
 - SSL (Secure Sockets), **108**. *See also* SSL (Secure Sockets)
 - terminology, 118
 - uses, **127–133**
 - authentication, **128–129**
 - digital signature, **129–130**
 - secure file storage, **127–128**
 - secure password exchange, **130**
 - steganography, **131**
 - weaknesses, **95–99**
 - brute force attacks, 97–99
 - cipher deficiencies, 97
 - human error, 95–96
 - in Windows 2000, **769–770**
 - network layer, **164–178**
 - purposes, 119
 - in Windows operating systems, **340–341**
- encryption key, 886
- end-system packet filtering, 412
- endpoint, 886
- Enhanced Interior Gateway Routing Protocol (EIGRP), 606
- enterprise firewalls, **399–400**, 400
- entropy of system, 4
- environment, 6–7, 14
 - change, 28
 - influence on system, 23–24
- environment variables
 - in tripwire install.cfg file, 304
 - for tripwire twcfg.txt, 306
- Erase rights in NetWare 6, 217
- ESD (electrostatic discharge), 886
- ESP (Encapsulating Security Protocol).
See Encapsulating Security Payload (ESP)
 - /etc/exports file, 262
 - /etc/fstab file, 273
 - /etc/inetd.conf file, 368
 - /etc/logcheck directory, 297
 - /etc/passwd file, 266
 - security audit and, 265
 - /etc/shadow file, 266
- Ethernet, **56–59**, 887
 - data frames, 69
 - flow chart of communication rules, 58
 - in PIX Firewall, 572

eTrust firewall (Computer Associates), **472-475**
 event-based trigger, 22
 event log, 791
 policies, **855**
 Event Viewer application, Cisco sensor alarm display, 737
 Everyone security group, 141, 809
 permissions, 813-814
 Evolvability in Systems Theory, 6
 .EXE files, Read Only attribute, 244
 executable downloads, opening, 427
 Execute File event, auditing, 842
 executive summary, 35
 exhaustive key search, 97
 expansion slot, 887
 extended AppleTalk network, 887
 extended packet-matching modules, for iptables tool, 513-514
 Extensible Authentication Protocol (EAP), **106**
 external networks for Cisco sensors, 734
 external reviews in objectives development, 34
 extranet, and sensor placement, 665
 extranet VPN, 614

F

failover device, 887
 failover server, 887
 Fast Ethernet, 887
 in PIX Firewall, 547, 572
 FAT file system, 139, 164
 fault-resistant network, 887
 fault-tolerant network, 887
 FDDI (Fiber Distributed Data Interface), 887
 FDM (frequency division multiplexing), 888
 FEAL, 120
 fee-for-support, 442
 Fiber Channel, 887
 Fiber Distributed Data Interface (FDDI), 887
 fiber-optic, 888
 fiber-optic cable, 50, **50-52**
 file attributes in NetWare 6, **220-225**
 file Properties dialog box (Windows)
 to encrypt file, 862
 Security tab, 345-346, 346
 file rights in NetWare 6
 ConsoleOne to change, **236-240**, 237
 IRF and, **217-220**
 for users and groups, **217**
 File Scan rights in NetWare 6
 for directories, 215
 for users and groups, 217
 file server, 888
 file storage, encryption for, 127-128
 File Transfer Protocol (FTP). *See* FTP (File Transfer Protocol)
 files
 in Linux, integrity auditing, **302-311**
 ownership and permissions, in Samba, **341-349**
 permissions in Linux, **271-276**
 limiting core dump size, **275-276**
 suid and sgid, **271-274**
 umask setting, **275**
 in Windows XP
 auditing, **199-203**
 permissions, **198-199**
 filesystems, 840, 841
 auditing, **842-843**
 and encrypted files, 144
 encryption in Linux, **277-282**
 Cryptographic File System, **277-280**
 PPDD (Practical Privacy Disk Driver), **280-282**
 for IDSM, **722-723**
 partition update, **726-727**
 for PIX Firewall, 545-546
 policies, 791, **857-858**
 security in NetWare 6, **213-225**
 file and directory rights, **214-220**
 file attributes as security enhancement, **220-225**
 filters. *See* packet filters
 fingerprint, 124
 firesandwich installation deployment method, for Cisco sensors, **670-671**, 671
 Firewall-1, 437-438. *See also* Checkpoint Firewall-1
 firewalls, **208-209**, 373-374, 735, 888.
 See also Cisco IOS Firewall; PIX Firewall
 to block Samba access, **364-367**, 365

- border security creation, **388–402**
 - limitations, **392–394**
 - disconnected security model, **400–402**
 - elements, **374–378**
 - encrypted authentication, **387–388**
 - Network Address Translation, **382–383**
 - packet filters, **376–382**. *See also* packet filters
 - proxies, **383–386**, 384
 - virtual private networks (VPN), **386–387**
 - examples, 402–403
 - functionality comparison, **390–392**
 - Linux as platform, **498–500**. *See also* Netfilter
 - disadvantages, 499
 - ipchains tool, **501–506**
 - ipfwadm tool, 501
 - network address translation, **526–529**
 - packet filters, **500–501**
 - sample scenarios, **515–525**
 - options, **394–402**
 - dual, and demilitarized zones, 398, **398–399**, 399
 - enterprise firewalls, 399–400, 400
 - filtered packet services, 395, **395–396**
 - single-firewall approach, **396–398**, 397
 - patches and upgrades, 210
 - technology combinations, **538–539**
 - for Unix, **471–496**
 - Computer Associates eTrust, **472–475**
 - NetWall, **480–483**
 - Network Associates Gauntlet, **483–490**
 - purchasing, **495–496**
 - SecurIT firewall, **476–480**
 - SunScreen Secure Net 3.1, **490–494**, 493
 - for Windows, **445–469**
 - Checkpoint Firewall-1, **447–454**
 - Microsoft Internet Security and Acceleration Server, **461–469**
 - Symantec Enterprise Firewall, **455–460**
 - fixed frequency signals, 53
 - FLAG command (NetWare), 224, 224–225
 - flags in NetWare 6, 220
 - flash memory for PIX Firewall, **545–546**
 - flashfs command (PIX), 545
 - floppy disks, and virus risk, 244
 - folders. *See* directories
 - forging e-mail, **427–428**
 - forward chain in Linux kernel, 502
 - rules for, 505
 - FQDN (Fully Qualified Domain Name), 888
 - fragmentation, **410–411**
 - hackers and, **416–417**
 - reassembly, **744–747**, 745
 - frame relay, **64–67**, 65, 888
 - frames in Ethernet, 748
 - frequency division multiplexing (FDM), 888
 - frequentcheck.sh package, 296
 - FrontPage Server Extensions, 114
 - FTP (File Transfer Protocol), 888
 - cleartext use by, 87
 - NAT problems, 435
 - port for, 380
 - and virus risk, 245
 - FTP proxy, 888
 - full backup, 888
 - Full Control event, auditing in Active Directory, 841
 - Full control permission in Windows, 197
 - for files and folders, 195–196
 - share-level, 194
 - for shares, 164
 - Fully Qualified Domain Name (FQDN), 888
- ## G
- gap analysis, in objectives development, 35
 - gateway-to-gateway VPN, 171
 - gateways, 888
 - circuit-level, 209, 386
 - dual-homed, **534–535**
 - Gauntlet (Network Associates), **483–490**
 - General constraint, 20, 21
 - Generic Routing Encapsulation (GRE), Cisco routers for, 615

global addresses in NAT
 inside, 577
 outside, 578

global command (PIX), 583–586

global groups, 812, 888
 impact of moving security principals, 784–785

GMT (Greenwich mean time), for IPSec, 567

goals, 11

Gopher, port for, 380

GOST, 120

government intervention, in encryption, **99–100**

graphics, hiding information in, 131

GRE (Generic Routing Encapsulation), Cisco routers for, 615

greater than(>) symbol, for unprivileged mode in PIX, 557

Greenwich mean time (GMT), for IPSec, 567

ground loop, 888

group accounts
 auditing, 840
 SIDs (security identifiers), 135
 in Windows 2000, 133–134
 in Windows XP, creating, **190–192**

Group Bull, 480

group memberships, in Linux, 263

group policies in Windows 2000, **152–160**, 803–804, **818–819**
 combining, 158
 considerations for using, 819
 creating, **156–158**
 delegating control, 850
 design, **869–872**
 hierarchy, 154–155, **859–860**
 implementation, 818, **851–858**
 managing, **158–160**
 mechanics, **153–156**
 restricted, **855–856**

Group Policy snap-in in Windows 2000, 787
 to control Internet Explorer security settings, 828, 829
 Kerberos parameters, 802–804, 803
 Security Configuration Manager, **791**

Group Policy Wizard, 201

group rights in NetWare

guidelines, 233

IRF and, 219

groups
 in NetWare 6
 directory rights, **236–240**, 237
 file rights, **217**
 in Windows 2000 security descriptor, 138

Guest account, in Windows XP, 183

Guests group, in Windows XP, 184

H

H.323, NAT problems, 434

hacker. *See* cracker

hacking tests, of Windows firewalls, 446–447

half-duplex, 60

half-open TCP session, 750

hardening the OS, 117, 464

hardware, **68–82**
 bridges, **69–73**, 70
 bridging/switching vs. routing, **80**
 hubs, **69**
 layer-3 switching, **80–82**
 for Linux firewall, 498
 routers, **76–80**
 switches, **73–76**, 74

hardware address, 889

hardware loopback, 889

hash, 124

hashing in IPSec, 618, **624**

heartbeat, 889

Hellman, Martin, 94, 125

help desk, impact of security policies on, 853

HelpServicesGroup group in Windows XP, 184

Hidden attribute in NetWare
 for directories, 221
 for files, 223

hidden protection in NetWare filesystem security, 213

hiding information, 120
 NAT to hide internal IP addresses, 421

hierarchies in systems, 9

HMAC (Hashed Message Authentication Code), 624

hop, 889
 hop count, 889
 host, 889
 Host ID, for Cisco sensors, 689, 733
 Host object, CSPM, 692, 692
 Host-to-Host layer, 889
 hostname command (PIX), 568
 HTML (Hypertext Markup Language), 889
 HTTP (Hypertext Transfer Protocol), 889
 cleartext use by, 87
 port for, 380
 and security, 832
 HTTPS (Hypertext Transfer Protocol Secure), 108
 port for, 380
 hubs, **69**, 889
 human error, in encryption, **95–96**
 hybrid cryptosystem, 125
 Hypertext Markup Language (HTML), 889

I

IAB (Internet Architecture Board), 891
 IANA (Internet Assigned Numbers Authority),
 private use network numbers, 434
 IBM data connector, 890
 ICMP (Internet Control Message Protocol), 891
 NAT problems, 435
 ICMP flood, 88
 IDEA, 120, 123
 identity NAT, **587–589**
 IDSM sensors. *See* Cisco Secure IDS sensors
 IEEE (Institute of Electrical and Electronics
 Engineers, Inc.), 891
 IEEE specifications
 802.01 LAN/MAN Management, 890
 802.02 Logical Link Control, 890
 802.03 CSMA/CD Networking, 57, 890
 802.04 Token Bus, 890
 802.05 Token Ring, 890
 802.06 Distributed Queue Dual Bus
 Metropolitan Area Network, 890
 802.07 Broadband Local Area
 Networks, 890
 802.08 Fiber-Optic LANs and MANs, 890
 802.09 Integrated Services LAN
 Interface, 890
 802.10 LAN/MAN Security, 891
 802.11 Wireless LAN, 60, 61, 68, 891
 802.12 Demand Priority Access
 Method, 891
 IETF (Internet Engineering Task Force), 101, 892
 IIS_WPG (Internet Information Services Worker
 Process Group), in Windows XP, 184
 IKE (Internet Key Exchange), 104, **630–633**
 IPSec with, 617, 824
 NAT problems, 435
 negotiated settings, 635
 Illegal Network Address Translation
 (INAT), 487
 IMAP (Internet Message Access Protocol)
 cleartext use by, 87
 port for, 381
 Immediate Compress attribute in NetWare
 for directories, 221
 for files, 223
 implementation in SDLC, **58–41**
 accreditation, 40–41
 in-place upgrade in Windows 2000, 763
 inactive accounts in Linux, disabling, 261–262
 INAT (Illegal Network Address Translation), 487
 individuals, system use by, **16**
 information, 4
 information technology
 project success rate, 38
 systems analysis applied to, **15–24**
 Information Theory, 4–5
 Infrastructure mode for WiFi, 60
 ingress SPAN, 700
 inheritance
 in NetWare 6, 214, **230–231**
 in Windows 2000, 142
 security policies, **859–860**
 initialization vector, 93
 Initiation in SDLC, **33–36**
 conceptual definition, 34
 functional requirement determination,
 34–35
 protection specifications development,
 35–36
 input, 7

- input chain in Linux kernel, 501
- inside global address in NAT, 577
- inside interface for PIX Firewall, 571
- inside local address in NAT, 577
- install.cfg file, for tripwire, 303–304
- installing
 - applications, file attributes after, 222
 - Cryptographic File System, **277–278**
 - John the Ripper, **312–313**
 - logcheck, 296
 - PPDD (Practical Privacy Disk Driver), **280–282**
 - SSL on Linux, **350–351**
 - sudo utility (Linux), **268**
 - swatch (Simple WATCHer), 292
 - tripwire, **303–304**
- Institute of Electrical and Electronics Engineers, Inc. (IEEE), 891. *See also* IEEE ...
- insurance, for critical systems, 40
- Integrated Services Digital Network (ISDN), 891
- integrity of data, 772–773
 - auditing in Linux, **302–311**
 - with IPSec, 618
- intelligent hub, 891
- IntelliMirror, **788–790**
- interface command (PIX), **572–574**
- interfaces for sensors, **666–667**
- internal bridge, 891
- internal modem, 891
- internal networks, configuring in CSPM, **734–738**
- International Organization for Standardization (ISO), 891
- International Traffic in Arms Regulations (ITAR), 99
- Internet, 891
 - disconnection from, **400–402**, 401
 - security issues, 114
- Internet Architecture Board (IAB), 891
- Internet Assigned Numbers Authority (IANA), private use network numbers, 434
- Internet connection, firewall for, **208–209**
- Internet Control Message Protocol (ICMP), 891
 - NAT problems, 435
- Internet Engineering Task Force (IETF), 101, 892
- Internet Explorer
 - Authenticode-based screening of downloaded software, 828
 - downloading .DLL files, 361
 - security flaws, 114
- Internet Information Server (IIS), 114, 832
- Internet Key Exchange (IKE), 104, 172, 173, 174, **630–633**
 - certificate authorities, **632–633**
 - IPSec with, 617, 824
 - NAT problems, 435
 - negotiated settings, 635
 - pre-shared keys, **630**
 - RSA encrypted nonces, **631–632**
 - RSA signatures, **631**
- Internet Message Access Protocol (IMAP)
 - cleartext use by, 87
 - port for, 381
- Internet Protocol (IP), 892
- Internet Research Task Force (IRTF), 892
- Internet Security and Acceleration Server. *See* Microsoft Internet Security and Acceleration Server
- Internet Security Association Key Management Protocol (ISAKMP), 630
- Internet servers, ports for, 380
- Internet service provider (ISP), 892
- internetwork, 892
- Internetwork Packet eXchange (IPX), 892
- interviews, in objectives development, 34
- intranet connection, and sensor placement, 665
- intranet VPN, 614
- intrusion, detection of, 55–56
- inverse multiplexing, 892
- IP (Internet Protocol), 892
- ip address command (PIX), **574–575**
- IP addresses, 892
 - aliases for, 568
 - assigning to PIX Firewall network interface, **574–575**
 - for Cisco sensors, 682, 689, 733
 - declaring those allowed out through PIX Firewall, 587
 - incorrect to divert traffic, 89–90
 - internal vs. external networks, 735–736
 - packet filters for, **407–408**

- private, 576–577
- restricting Samba access by, **319–322**
- translating, **382–383**
- IP blocking, by Cisco sensors, 674
- IP encapsulation, 166
- IP fragmentation. *See also* fragmentation
 - reassemble, **744–747**, 745
- IP load balancing, **429–430**, 430
- IP masquerading, 375, 425, **426–428**. *See also* Network Address Translation (NAT)
- IP packets. *See* packets
- IP proxy, 892
- IP spoofing, 892
 - protection against, **523–524**
- IP (Internet Protocol) version 4, security needs, 84
- IP (Internet Protocol) version 6, NAT and, 421
- IPC\$ share, 163
- ipchains tool, **364–367**, **501–506**
 - examples, **504–506**
 - vs. iptables, 508
- IPCOMP (IP Compression), 104
- ipconfig, 892
- ip_forward switch for Linux kernel, 507
- ipfwadm tool, 367, 501
- IPSec (IP Security), **103–104**, 617, **617–630**, **823–827**
 - building blocks, **618–623**
 - Authentication Headers, 619, **619–620**
 - Encapsulating Security Payload (ESP), 621, **621–622**
 - considerations for using, 825–826
 - for data protection, 820
 - Diffie-Hellman key exchange, **625–627**
 - encryption, **624–625**
 - hashing, **624**
 - Header Authentication, NAT and, 425
 - how it works, 633, **633–639**, 824–825
 - IKE phase 1, **634–636**
 - IKE phase 2, **636–637**
 - interesting traffic definition, 633–634, 634
 - IPSec decision-making process, **638–639**
 - implementation, 825
 - NAT problems, 435, **580–581**
 - policies on Active Directory, **858**
 - Security Associations (SA), **628–630**, 629
 - services, **618**
 - system clock for, 567
 - transform sets, 627, **627–628**
 - troubleshooting, **639–641**
 - access control list (ACL) problems, **640–641**
 - filtering, **640**
 - NAT problems, **640**
 - traffic delay, **639–640**
 - tunnel mode and transport mode, 622, **622–623**
 - for VPN Hardware Client, 653
 - in Windows 2000, 116, **170–176**, 387
 - automatic disabling, 176
- iptables tool, 367, **508–515**
 - to configure NAT, **527–529**
 - extended packet-matching modules, 513–514
 - to prevent address spoofing, **523–524**
 - to prevent ping-of-death attack, **525**
 - to prevent port-scanner attack, **525**
 - to prevent smurf attack, **523–524**
 - to prevent syn-flood attack, **524–525**
 - rules specifications, **511–515**
 - using, **510–511**
- IPX (Internetwork Packet eXchange), 892
- IPX network address, 893
- IRC, NAT problems, 434
- IRF (Inherited Rights Filter), 214
 - and file and directory rights, **217–220**
 - and object and property rights, **231**
- IRTF (Internet Research Task Force), 892
- ISA Server. *See* Microsoft Internet Security and Acceleration Server
- ISAKMP (Internet Security Association Key Management Protocol), 630
- ISDN (Integrated Services Digital Network), 891
- ISDN terminal adapter, 893
- ISO (International Organization for Standardization), 891
- ISP (Internet service provider), 892
- ITAR (International Traffic in Arms Regulations), 99

J

Java, 893
 Java Virtual Machine (JVM), 893
 JavaScript, 427–428
 John the Ripper, **311–315**
 configuring, **314**
 installing, **312–313**
 running, **314–315**
 jumper, 893
 JVM (Java Virtual Machine), 893

K

Kashpureff, Eugene, 89–90
 KDC (Kerberos Key Distribution Center), 146
 Kerberos, **104–105**, 778, **801–805**
 authentication and domain security, **146–152**, 151
 trust between domains, **149–152**
 considerations for using, 804–805
 how it works, 802
 implementation, 802–804
 passwords, 131
 policies, 854
 Kerberos Key Distribution Center (KDC), 146
 kernel, 893
 kernel in Linux
 building secure, **258–261**
 recommended options, 259
 chains built-in, 501–502
 firewall filtering based on, 498
 keyring, 174
 keys, 119, 893. *See also* crypto key
 keyspace, 118
 keyspace attack, 120
 kiosk station, and data protection, 819
 known plain text, and cryptanalysis, 120–121

L

L2F (Layer 2 Forwarding), Cisco routers for, 615

L2TP (Layer 2 Tunneling Protocol), **105–106**, **176–177**
 Cisco routers for, 615
 in Windows 2000, 116, 387
 LAN (local area network), 895
 LAN driver, 893–894
 LAN extension mode for VPN Hardware Client, 653–654
 LAN Manager, passwords, 129
 LAN topologies, **56–63**
 Ethernet, **56–59**
 wireless, **60–63**
 laptop computers
 and data loss, 819
 loss of, **823**
 Large InternetPacket (LIP), 894
 laser printer, 894
 Layer 2 Switch, 894
 Layer 2 Tunneling Protocol (L2TP), **105–106**, **176–177**
 Cisco routers for, 615
 in Windows 2000, 387
 Layer 3 Switch, **80–82**, 894
 LCP (Link Control Protocol), 894
 leased lines, 63–64, 387
 LED (light-emitting diode), 49
 licensed features for PIX Firewall, **548–549**
 light dispersion, 50
 light-emitting diode (LED), 49
 light transmissions, **52**
 lilo, 260
 lilo.conf file, 260
 Limited account in Windows XP, 183
 line conditioner, 894
 line noise, 894
 line voltage, 894
 linear cryptanalysis, 121
 Link Control Protocol (LCP), 894
 link light, 894
 Link Manager Protocol (LMP), 62
 link state route discovery, 894
 link state routing, 895
 link state routing protocol, 895
 Link Support Layer (LSL), 895
 Linux, 895

- building secure kernel, **258–261**
 - recommended options, 259
- command escape to shell, 269
- distribution selection, **252–258**
 - Caldera, **253–254**, 254
 - Debian, **256**, 257
 - Red Hat, **253**
 - SuSE, **254–255**
 - Turbolinux, 255, **255**
- emergency boot disk, 258
- file and directory permissions, **271–276**
 - limiting core dump size, **275–276**
 - suid and sgid, **271–274**
 - umask setting, **275**
- file integrity auditing, **302–311**
- filesystem encryption, **277–282**
 - Cryptographic File System, **277–280**
 - PPDD (Practical Privacy Disk Driver), **280–282**
- as firewall platform, **498–500**. *See also* Netfilter
 - disadvantages, 499
 - ipchains tool, **501–506**
 - ipfwadm tool, 501
 - network address translation, **526–529**
 - packet filters, **500–501**
 - sample scenarios, **515–525**
- log file monitoring, **281–302**
 - logcheck, **296–301**
 - swatch, **291–296**
- logging with syslog, **286–291**
- passwords, auditing, **311–315**
- and Samba, passwords, 331
- syslog security, **276**
- system monitoring, 285
- user account security, **261–271**
 - good passwords, **264–265**
 - shadow passwords, **266–267**
 - sudo utility, **267–271**
 - sudoers file, **268–269**
 - sudo.log file, **270–271**
- linuxconf
 - to set nosuid option, 274
 - to set password length parameters, 265
- LIP (Large InternetPacket), 894
- List Contents event, auditing in Active Directory, 841
- List Folder Contents permission in Windows XP, 196
- List Folder event, auditing, 842
- List Folder/Read Data permission in Windows XP, 197
- List Object event, auditing in Active Directory, 841
- LLC (logical link control), 895
- lmhosts file, 362–363
- LMP (Link Manager Protocol), 62
- load balancing
 - NAT for, 426, **429–430**
 - and PIX Firewall, 612
- local addresses in NAT
 - inside, 577
 - outside, 578
- local area network. *See* LAN topologies
- local computer policies, **854–855**
- local group policy, 154, 157
- local groups, 813, 895
- local loop, 895
- local policies, 791
- local security in Windows 2000, **133–145**
 - resource access, **135–140**
 - rights vs. permissions, **140**
 - security identifiers, **134–135**
- Local Security Settings window (Windows XP), 185, 185–187, 186
- Local Users and Groups snap-in (Windows 2000), account creation, 134
- localhost address, binding proxy server to, 362–363
- Locally Unique Identifier (LUID), 137, 140
- log file, 895
- logcheck, **296–301**
 - configuring, 297–300
 - installing, 296
 - running, 300–301
 - vs. swatch (Simple WATCHer), **301–302**
- logcheck.violations file, 299–300
- logging command (PIX), 568–569
- logging on, 115
 - auditing, 840
 - to Cisco 4200 series sensor, **679–681**

mandatory, in Windows 2000, 136
in NetWare 6, **211–212**

logical bus topology, 895

logical link control (LLC), 895

logical network addressing, 895

logical parallel port, 895–896

logical port address, 896

logical ring topology, 896

logical topology, 896

login scripts, preventing changes to, 235–236

logs

- audit, in Windows 2000, **773–774**
 - disk space requirements, 843
- for Cisco 4200 series sensors, **740–743**, 741
- in Linux, with syslog, **286–291**
- monitoring in Linux, **281–302**
 - logcheck, **296–301**
 - swatch, **291–296**
 - swatch vs. logcheck, **301–302**
- preserving, **276**
- of web servers, 30
- Windows XP rights to manage, 187

LOKI, 120

loose reassembly for TCP session, 749, 750

loose source routing, 410

Love Bug worm, 39

LPR, port for, 381

LSL (Link Support Layer), 895

LSNAT (Load-Sharing Network Address Translation), 527

LUID (Locally Unique Identifier), 137, 140

M

MAC (media access control), 896

MAC address, 896

MAC address poisoning, 75

Macintosh, Encrypting File System and, 864

mail exchange record, 896

mail servers, port for, 381

mailing lists

- BugTraq, 258
- security groups as, 816

maintenance of system, **41**

maintenance partition in IDSM filesystem, 722

make config command (Linux), 259

make dep command (Linux), 260

make zImage command (Linux), 260

man-in-the-middle attack, 88, 88–89, 100–101

management

- access to Cisco Secure IDS sensor, 682–683, 683
- of security administration, **834–835**
- security policy development, 249

mandatory logon in Windows 2000, 136

MANPATH environment variable for tripwire, 304

mapping, 20

- network drive to share, 162

mask field in nat command, 586

MAU (Multistation Access Unit), 897

maximum transmission unit (MTU), 744

- for PIX Firewall network interface, 576

McAfee, 483

media access, 896

media access control (MAC), 896

media converter, 896

member server, 896

mesh topology, 896

Microsoft

- attitudes on security, 114
- Knowledge Base, on IPSec tunnel-mode between gateways, 176
- Resource Kit, 114

Microsoft Authenticode, **828–830**

Microsoft Certificate Services, 822

Microsoft Internet Security and Acceleration Server, **461–469**

- cost and support, **468–469**
- future availability, 469
- interface, **467–468**, 468
- major feature set, **461–463**
- minor feature set, **463–466**
- security, **466–467**

Microsoft Management Console

- Active Directory Sites and Services
 - snap-in, 848, 849
- Active Directory Users and Computers
 - snap-in, 796, 797, 847–848

- for group policy management, 158, 159, 852
 - for audit policies, 839
 - Computer Management snap-in, Shared Folders extension, 162
 - Group Policy snap-in, 787
 - to control Internet Explorer security settings, 828, 829
 - Kerberos parameters, 802–804, 803
 - Security Configuration Manager, **791**
 - for ISA Server interface, **467–468**, 468
 - Local Users and Groups snap-in, account creation, 134
 - for Symantec Enterprise Firewall, 459
 - Microsoft Proxy Server, 461
 - weaknesses, 466–467
 - microwave signals, 53
 - mixed mode for Windows 2000 server, 817
 - mkbootdisk command (Linux), 258
 - mk smbpasswd command, 338–339
 - models
 - object-based, 17
 - Object-Interaction Model (OIM), 22–24
 - Object-Relationship Model (ORM), **17–22**
 - modem, 897
 - for dial-up connection to ISP, 393, 394
 - internal, 891
 - Modify Owner event, auditing in Active Directory, 841
 - Modify permission in Windows XP, 195
 - Modify Permissions event, auditing in Active Directory, 841
 - Modify rights in NetWare 6
 - for directories, 215
 - for users and groups, 217
 - monitoring interface for sensors, 666–667, 738
 - monitoring port
 - on IDS, 699
 - configuring to control trunk traffic, **716–718**, 717
 - on switches, 74
 - Moore's Law, **41**
 - moving files, EFS and, 861
 - MTU (maximum transmission unit), 744
 - for PIX Firewall network interface, 576
 - mtu command (PIX), 576
 - multimode fiber-optic cable, 51
 - multinetting, 570
 - multiple collision, 58
 - multiple-server clustering, 897
 - multiplexing, 897
 - multipoint RF network, 897
 - Multistation Access Unit (MAU), 897
 - multitier applications, delegation of authentication for, 150, 152
 - mutuality in Systems Theory, 5
 - My Network Places icon (Windows 2000), 162
- ## N
- N-series connector, 901
 - NAI Gauntlet, 469
 - name resolution, 897
 - nameif command (PIX), **570–572**
 - names command (PIX), 568
 - names for domains in Windows 2000, 764
 - NAPT (Network Address and Port Translation), 426, 526–527
 - NASA, 31–32
 - NAT. *See* Network Address Translation (NAT)
 - nat 0 command (PIX), 588, 592
 - NAT + Bridge mode, 60–61
 - nat command (PIX), 583–586
 - NAT mode, 60
 - National Computing Security Center (NCSC), 897
 - National Security Agency (NSA), 46, 99, 897
 - native mode for Windows 2000 domains, 762, 817
 - nbtstat (NetBIOS over TCP/IP statistics), 897
 - NCP (NetWare Core Protocol), 899
 - NCSC (National Computing Security Center), 897, 898
 - NDPS (Novell Distributed Print Services), 900
 - NDS (Novell Directory Services), 900
 - NDS security, **226–233**
 - ACL (Access Control List), **229**
 - guidelines, **232–233**
 - IRF and object and property rights, **231**
 - management layers, 226

- object rights vs. property rights, **227–229**
- rights inheritance, **230–231**
- NDS tree, 898
- nearline site, 898
- nested groups in Windows 2000, 816
- Net News, port for, 380
- NetBEUI (NetBIOS Extended User Interface), 898
- NetBIOS (network basic input/output system), 899
- NetBIOS Extended User Interface (NetBEUI), 898
- NetBIOS name, 898
- NetBIOS Name Service, port for, 381
- NetBIOS over TCP/IP statistics (nbtstat), 897
- NetBIOS Session Service
 - blocking, 409
 - port for, 381
- Netfilter, **506–515**
 - configuring, **506–507**
 - iptables tool, **508–515**, 509
 - rule specifications, 511–515
 - using, 510–511
- netrangr account, for Cisco 4200 series sensor, 680
- Netscape
 - downloading .DLL files, 361
 - SSL (Secure Sockets), 108, 126
- Netscape Certificate Server, 103
- netstat, 898
- NetWall, **480–483**
- NetWare, 898
- NetWare 6
 - ConsoleOne, **233–243**
 - to change directory and file rights, **236–240**
 - to change object and property rights, **241–243**
 - revoking property right, **235–236**
 - filesystem security, **213–225**
 - file and directory rights, **214–220**
 - file attributes as security enhancement, **220–225**
 - NDS security, **226–233**
 - ACL (Access Control List), **229**
 - guidelines, **232–233**
 - IRF and object and property rights, **231**
 - object rights vs. property rights, **227–229**
 - rights inheritance, **230–231**
 - passwords and login restrictions, **211–212**
 - protection from viruses, **244–247**
 - security
 - improvements, **247–249**
 - management responsibility, **249–250**
 - NetWare Administrator, 899
 - vs. ConsoleOne, 215
 - NetWare Core Protocol (NCP), 899
 - NetWare Link State Protocol (NLSF), 899
 - NetWare Loadable Module (NLM), 899
 - network, 899
 - Network Address and Port Translation (NAPT), 426
 - Network Address Translation (NAT), 375, **382–383**, **421–442**
 - and authentication headers, 620
 - and filtering, **417–418**
 - hacking through, **437–440**
 - IANA private use network numbers, **434**
 - in Linux, **526–529**
 - iptables to configure, **527–529**
 - original purpose, 405
 - in PIX Firewall, **576–581**
 - configuring, **582–592**
 - configuring on multiple interfaces, **596–606**
 - consequences, **580–581**
 - global and local addresses, **577–578**
 - mechanisms, **549–550**
 - and security, **581–582**
 - static and dynamic, **578–579**
 - problems, **434–437**
 - procedure for, **422–425**, 424
 - router configuration, **431–434**
 - by Symantec Enterprise Firewall, 456
 - translation modes, **425–431**
 - dynamic translation, **426–428**
 - load balancing, **429–430**, 430

- network redundancy, *431*, **431**
 - static translation, **429**
 - network analyzer, 59
 - to capture POP3 authentication session, 86
 - Network Associates Gauntlet, **483–490**
 - network attached storage, 899
 - network basic input/output system (NetBIOS), 899
 - network-centric, 899
 - Network Configuration Operators group, in Windows XP, 184
 - Network File System (NFS), 899
 - Network General, 483–484
 - network interface card (NIC), 899
 - network interfaces
 - binding Samba to, **318–319**
 - for PIX Firewall, **547–548**, **569–576**
 - IP address assignment, **574–575**
 - maximum transfer unit, **576**
 - name and security level, **570–572**
 - properties and shutdown, **572–574**
 - security levels, **554–556**
 - Network layer, 899
 - network management in technical support, **786**
 - network media, 900
 - network operating system (NOS), 900
 - network protocols, **76–77**
 - cleartext use by, **87**, 131
 - filtering, **406–407**
 - and firewalls, 385–386
 - specificity of routers, **79–80**
 - network redundancy, NAT for, 426, *431*, **431**
 - network security in Windows 2000, **145–178**
 - Active Directory, **146**
 - group policies, **152–160**
 - Kerberos authentication and domain security, **146–152**, 151
 - network layer encryption, **164–178**
 - share security, **160–164**
 - network security matrix, 794
 - network security plan, 794
 - network software diagnostics, 900
 - Network Time Protocol (NTP), 685
 - network transmissions, **46–56**
 - bound and unbound transmissions, **52–54**
 - choosing medium, **54–56**
 - cleartext, 84
 - digital communication, 46, **46–47**
 - on noisy circuit, 47
 - EMI (electromagnetic interference), **48–50**, 49
 - fiber-optic cable, 50, **50–52**
 - Neuling, Michael, 501
 - New Group dialog box (Windows XP), 190–191, 191
 - New User dialog box (Windows XP), 189, 189–190
 - NFS (Network File System), 899
 - blocking port, 409
 - NIC (network interface card), 899
 - NIC diagnostics, 900
 - NIMDA virus, 600
 - NLM (NetWare Loadable Module), 899
 - NLSP (NetWare Link State Protocol), 899
 - NNTP, port for, 380
 - no-recovery policy at domain level, 865, 866
 - noisy circuit, digital communication on, 47
 - non-unicast packet, 900
 - nonrepudiation in Windows 2000, **773**
 - Normal attribute in NetWare
 - for directories, 222
 - for files, 223
 - NOS (network operating system), 900
 - Novell BorderManager, 210
 - Novell Directory Services (NDS), 900
 - Novell Distributed Print Services (NDPS), 900
 - Novell Support Connection, 900
 - nrconns command (IDSM), 729
 - nrvrs command, 733
 - NSA (National Security Agency), 897
 - nslookup, 901
 - NT Directory Services (NTDS), 901
 - NTFS file system permissions, **140–142**
 - NTP (Network Time Protocol), 685
- ## O
- Object-Behavior Model (OBM), 17
 - object classes, 17, 18
 - Object-Interaction Model (OIM), 17, 22–24

object-oriented programming languages, black box view and, 8

Object-Relationship Model (ORM), **17-24**

object rights in NetWare 6, vs. property rights, **227-229**

objectives, 11

- development, 34-35
- proxy, 12

objects, 17, 17, 901

- adding to CSPM database, **692-693**
- auditing access, 840
- in NetWare 6
 - IRF and rights, **231**
 - rights, **241-243**
- as object class member, 18
- relationship sets as, 19
- in Windows 2000, **137-139**

OBM (Object-Behavior Model), 17

octet, 901

ODI (Open Datalink Interface), 901

OE (operator error), 901

OFDM (Orthogonal Frequency-Division Multiplexing), 61

Office (Microsoft), security flaws, 114

offline, 901

OIM (Object-Interaction Model), 17

one-time pad, 92, 96, **121-122**

one-way functions, **123-124**

Open Datalink Interface (ODI), 901

open establish timeout for TCP session, 750

Open Folder event, auditing, 842

Open Shortest Path First (OSPF), 606

Open Systems Interconnect (OSI), 901

OpenLinux, 901

OpenSSL, 350

operating systems. *See also* specific system names

- filtering, 378
- for firewall, 390
- hardening, 464
- packet filters, **412**
- remote installation, 790
- security, 418

operation and maintenance in SDLC, **41**

operation of system, **41**

organization ID for Cisco sensors, 689, 733

organization, universal principles, 9

organizational units in Windows 2000, 795

- policies, 155, 157, 860
- restructuring resource domains as, 766

ORM (Object-Relationship Model), **17-24**

Orthogonal Frequency-Division Multiplexing (OFDM), 61

OSA (Object-Oriented Systems Analysis), 17

OSI (Open Systems Interconnect), 901

- network layers and security filters, 208-209

OSPF (Open Shortest Path First), 606

out-of-sequence delivery of TCP segments, 748

Outlook, security flaws, 114

Outlook Express, 427

output, 7

- output chain in Linux kernel, 501

outside global address in NAT, 578

outside interface for PIX Firewall, 571

outside local address in NAT, 578

overhead, 47

overloading, 579. *See also* Port Address Translation (PAT)

oversampling, 901

oversight, attacks due to, 31

overvoltage threshold, 902

owner in Windows 2000 security descriptor, 138

ownership

- in Samba, **341-349**
- in Windows XP, **203-206**
 - defining, **204**
 - right to control, 187
 - taking, **205-206**

P

packet capture device, for Cisco 4200 series sensors, 738-739

packet filters, 209, 375, 376, **376-382**, **405-419**, 902

- advantages and drawbacks, **535-536**
- best practices, **418**
- general rules, **381-382**
- hacking through, **416-418**
- ipchains tool for, 367

- leaky filters, **419**
- in Linux, **500–501**, 509
- security limitations, **378–381**
- stateful, 406, **413–415**, 414
- stateless, **406–412**
 - filtering on other information, **410–411**
 - IP address filtering, **407–408**
 - problems, **411–412**
 - protocol filtering, **406–407**
 - TCP/UDP ports, **408–410**
- packet processing by PIX Firewall, **550–554**
 - inbound packets, **552**
 - outbound packets, **551**
 - routing, **552–554**, 553
- packet-switched technology, **64–67**, 902
- packets, 79, 748, 902
 - fragmentation, **410–411**
 - reassembly, Cisco sensor configuration for, **743–751**
- Participation constraint, 20
- pass-through authentication, 763
- passive detection, 902
- passive hub, 902
- passive mode for PIX Firewall RIP support, 552–553
- passwd command (PIX), 561
- password history, 902
- passwords, **131–133**
 - best practices, **798–800**
 - case sensitivity in Unix, 680
 - changing, 133
 - for Cisco Secure IDS sensor, 686, 686
 - encrypted or cleartext, **329–341**
 - advantages and drawbacks, **329–332**
 - guessing, **775**
 - levels, 132–133
 - in Linux, **264–265**
 - auditing, **311–315**
 - expiration, 261–262
 - shadow passwords, **266–267**
 - in NetWare 6, **211–212**
 - policies, 854
 - implementation, 800–801
 - root, 267–268
 - in Samba, **322–328**
 - encryption, **333–336**
 - setting up, **338–340**
 - smbpasswd command, **336–338**
 - secure exchange, **130**
 - selecting, 131–132
 - in Windows XP, for new user, 190
 - in Windows XP Professional, 188
- PAT. *See* Port Address Translation (PAT)
- patch, 902
- patch cable, 902
- patch panel, 902
- PATH environment variable
 - SSL path inclusion, 352
 - for tripwire, 304
- PDC (Primary Domain Controller), 905
- PDP (policy distribution point), 693, 694
- peer-to-peer network, 902
- per-share ownership, in Samba, **341–342**
- Perfect Forward Secrecy (PFS), 637
- perfmom command (PIX), 561
- performance
 - of Linux for firewall, 499
 - and sensor placement, 664
 - of Windows firewalls, 446
- peripheral, 902
- permanent virtual circuit (PVC), 64, 902
 - vulnerability, 67–68
- Permission Entry dialog box, 197
- permissions, 808
 - accumulating, 194–195
 - default for security groups, 813–814
 - in Samba, **341–349**
 - in Windows 2000, **137–139**
 - vs. rights, **140**
 - for shares, 164
 - in Windows XP, **192–203**
 - auditing files and folders, **199–203**
 - file and folder, **194–199**
 - ownership to change, 205
 - share-level, **192–194**
- PFS (Perfect Forward Secrecy), 637
- PGP (Pretty Good Privacy), 484, 905
- physical bus topology, 903
- Physical layer, 903
- physical mesh topology, 903

- physical parallel port, 903
- physical port, 903
- physical ring topology, 903
- physical security in Windows 2000, **774**
- physical star topology, 903
- physical topology, 903
- piconet, 62
- PIN (personal identification number), with smart card, 806
- Ping, 903
 - port for, 380
- Ping of Death attack, 903
 - protection against, **525**
- PIX Firewall, **541-549, 616**
 - command-line interface, **556-564**
 - access methods, **556-557**
 - commands, **558-564**
 - editing in, **558**
 - modes, **557-558**
 - components, **543-549**
 - BIOS, **547**
 - CPU, **544**
 - flash memory, **545-546**
 - interfaces, **547-548**
 - licensed features, **548-549**
 - RAM, **544**
 - system image, **546**
 - configuration commands, **567-569**
 - clock command, **567**
 - domain-name command, 568
 - hostname command, 568
 - logging command, 568-569
 - names command, 568
 - configuration preparation, **566-567**
 - documentation pages, 583
 - features, **542**
 - interface configuration, **569-576**
 - enabling, 573
 - IP address assignment, **574-575**
 - maximum transfer unit, **576**
 - name and security level, **570-572**
 - properties and shutdown, **572-574**
 - Network Address Translation (NAT), **576-581**
 - configuring, **582-592**
 - configuring on multiple interfaces, **596-606**
 - consequences, **580-581**
 - global and local addresses, **577-578**
 - and security, **581-582**
 - static and dynamic, **578-579**
 - operation, **549-556**
 - ASA (Adaptive Security Algorithm) and security levels, **554-556**
 - NAT mechanisms, **549-550**
 - packet processing, **550-554**
 - order of operation on, 582-583
 - Port Address Translation (PAT), 576, **579-580**
 - configuring, **592-596**
 - routing, configuring, **606-612**
- PKI (Public Key Infrastructure), 770
 - and nonrepudiation, 773
 - for smart card, 806
- plain text. *See* cleartext
- plenum-rated coating, 904
- point-to-point, 63, 904
- Point-to-Point Protocol (PPP), 904
- Point-to-Point Tunneling Protocol (PPTP), **105-106, 387, 904**
 - Cisco routers for, 615
 - communication in, 168
 - NAT problems, 434
 - in Windows 2000, 116, **177-178**
- policies
 - for stateful filters, 414
 - in Windows 2000, 116
 - group, **152-160**
- policy analysis, 9. *See also* systems analysis
- policy-based firewalls, Checkpoint Firewall-1 as, 450-451
- policy distribution point (PDP), for sensor object, 693, 694
- polling, 904
- POP3 (Post Office Protocol version 3), 904
 - authentication session, 84-85, 85, 86
 - blocking, 409
 - port for, 381

- Port Address Translation (PAT), **579–580**
 - in PIX Firewall, 576, **579–580**
 - configuring, **592–596**
 - and security, 581–582
 - for VPN Hardware Client, 653–654
- port filtering, **408–410**
- port forwarding mode, 429
 - NAT in, 423–424
- port redirection, 594
- port-scanner attack, protection against, **525**
- ports, 904
 - disabling, 418
 - on PIX Firewalls, 547
 - for SMB/CIFS, **364**
 - for TCP/IP services, 380–381
- Post Office Protocol (POP3). *See* POP3 (Post Office Protocol version 3)
- PostOffice communication parameters
 - for Cisco sensors, **751–753**
 - for IDSM, 707
- PostOffice heartbeat, 751
 - interval for Cisco sensors, 689
- POTS (plain old telephone service), 904
- pound sign (#) for privileged mode in PIX, 557
- power blackout, 904
- power brownout, 904
- power overage, 904
- power sag, 904
- power spike, 905
- power surge, 905
- power underage, 905
- Power Users group
 - default permissions, 814
 - in Windows XP, 184
- power users, recognizing, 232
- PPDD (Practical Privacy Disk Driver), **280–282**
- PPP (Point-to-Point Protocol), 904
- PPTP (Point-to-Point Tunneling Protocol), **105–106**, 387, 904
 - Cisco routers for, 615
 - communication in, 168
 - NAT problems, 434
 - in Windows 2000, 116, **177–178**
- Practical Privacy Disk Driver (PPDD), **280–282**
- pre-shared keys, **630**
- precomputed hash, 129
- Presentation layer, 905
- Pretty Good Privacy (PGP), 484, 905
- Primary Domain Controller (PDC), 905
 - upgrades, 763
- principle of least privilege, 835, 847
- Print Operators group on domain controller, permissions, 814
- print server, 905
- print services, 905
- PRINT\$ share, 163
- printer Properties dialog box, Security tab, for access control list, 810, 810
- printing in Windows 2000, and file encryption, 144
- private interface, for VPN Hardware Client, 652, 652
- private IP addresses, 576–577
- private key, 905
- private network, 905
- privileged mode for PIX Firewall command-line interface, 557
- problem, defining scope, **10–11**
- process, 4
- programs. *See* software
- promiscuous mode, 59
- prompt, root, in Linux, 262–263
- property rights in NetWare 6
 - IRF and, **231**
 - vs. object rights, **227–229**
 - revoking, **235–236**
 - setting or modifying, **241–243**
- protection for sensitive data, **819–827**. *See also* encryption
 - Encrypting File System (EFS), **820–822**
 - IPSec (IP Security), **823–827**
- protection specifications development, **35–36**
- protocol analyzer, 906
- protocol suite, 906
- protocols, 905. *See also* network protocols
- prototype, 37
- proxy, 906
- proxy cache server, 906
- proxy objectives, 12

proxy server, 906
 and firewall, 375, **383–386**, 384
 original purpose, 405
 SSL (Secure Sockets), 361, **361–362**
 for Windows, 446

Proxy Server (Microsoft), 461. *See also*
 Microsoft Internet Security and Acceleration
 Server
 weaknesses, 466–467

pseudorandom numbers, 126

PSTN (Public Switched Telephone Network), 906

public, 906

public interface, for VPN Hardware Client,
 652–653, 653

public key, 906
 policies, **858**

public key algorithm, 119

public key encryption, **124–125**, 169, **770**

Public Key Infrastructure (PKI), 770
 and nonrepudiation, 773
 for smart card, 806

[Public] object, default object and property
 rights, 234

public passwords, 132–133

public/private crypto keys, **94–95**

[Public] trustee in NetWare 6, 214

punchdown tool, 906

purchasing firewalls, **495–496**

Purge attribute in NetWare
 for directories, 222
 for files, 223

PVC (permanent virtual circuit), 64, 902
 vulnerability, 67–68

Q

QoS (Quality of Service), 907

quad decimal, 906

Quality of Service bandwidth allocation by ISA
 Server, 466

quaternary set, 18

Quick Configuration Utility for VPN Hardware
 Client, **650–655**, 651
 Admin password changes, 654–655
 DNS configuration, 654

enabling users, 654–655

IPSec, 653

PAT or LAN extension mode, 653–654

private interface, 652, 652

public interface, 652–653, 653

static routing configuration, 654

system time, 652

R

radio waves, **53–54**

RADIUS (Remote Access Dial-In User Service),
106–107

RAID (Redundant Array of Independent
 Disks), 907

RAM for PIX Firewall, **544**

random numbers, 126–127

Raptor Management Console, 459

rdate command (Unix), 685

Read & Execute permission in
 Windows XP, 195

Read All Properties event, auditing in Active
 Directory, 841

Read Attributes event, auditing, 842

Read Attributes permission in
 Windows XP, 197

Read Data event, auditing, 842

Read Extended Attributes event, auditing, 842

Read Extended Attributes permission, in
 Windows XP, 197

Read Only attribute
 for .EXE and .COM files, 244
 for NetWare files, 223

read permission for shares, 164

Read permission in Windows XP
 for files and folders, 195
 share-level, 194

Read Permissions event, auditing, 841, 842

Read Permissions permission in
 Windows XP, 198

Read rights in NetWare 6
 for directories, 215
 for properties, 229
 for users and groups, 217

Read Write attribute for NetWare files, 223

README file, 907

- realms. *See also* domains
 - in Kerberos, 149
- rebooting Linux, initializing packet filtering at, 509–510
- recommendations in documentation, 36
- recovery agent for EFS, 822, 864–865
- recovery-agent policy, 866
- recovery keys for EFS
 - archives, 868
 - securing, 867–868
- Red Hat Linux, **253**
 - OpenSSL with, 351
- reduced instruction set computing (RISC), 907
- redundance, 32
 - NAT for, **431**, 431
- Redundant Array of Independent Disks (RAID), 907
- referral ticket in Kerberos, 150
- Reflexivity in Systems Theory, 6
- regeneration process, 907
- Registry
 - policies, 791, **857**
 - in Windows 2000, encryption certificates, 143
- relationship sets, 18, 19
- reload command (PIX), 562
- Remote Access Dial-In User Service (RADIUS), **106–107**
- remote access protocol, 907
- remote access server, 176, 907
 - and sensor placement, 665
- remote control, Trojan horse to establish, 419
- Remote Desktop Users group in Windows XP, 184
- remote installation deployment method, for Cisco sensors, **672**, 673
- Remote Procedure Call, port for, 381
- remote servers, encrypted files on, **863–864**
- remote shutdown, Windows XP rights to force, 186
- Rename Inhibit attribute in NetWare
 - for directories, 222
 - for files, 223
- Rename rights in NetWare 6, for objects, 228
- repeater, 907
- repetition with recursion, 32
- replication, 907
 - impact on bandwidth, 817
- report systemstatus command (IDSM), 729
- reset module hdd:partition command, 728
- resource conservation, 32
- resource domains, upgrading to Windows 2000, **764–765**
- resource groups, 812
- resources, local administration of, 766
- restricted algorithm, 118
- restricted group policies, **855–856**
- restricted groups, 791
- RFC (Request for comments)
 - 1631, on address translation, 576
 - 1918, on private addresses, 576–577
 - 2402, on authentication headers, 619
 - 2406, on Encapsulating Security Payload, 621
 - 2409, on IKE (Internet Key Exchange), 630
 - 2631, on Diffie-Hellman key exchange, 625
- RFI (radio frequency interference), 907
- RG-58, 908
- RG-62, 908
- .rhosts file to control Samba access, 320–321
- rights
 - in NetWare
 - file and directory, **214–220**
 - guidelines for granting, 232–233
 - IRF to revoke, 218
 - in Windows 2000, vs. permissions, **140**
- Rijndael algorithm, 102, 625
- ring topology, 908
- RIP (Router Information Protocol), 908
 - PIX Firewall support for, 552–553
- rip command, **607–608**
- RISC (reduced instruction set computing), 907
- risk, 13
 - assessment, 13
 - mitigation, case studies, **29–32**
- Rivest, Ron, 107
- RJ (Registered Jack) connector, 908
- roaming profile, 908
- root account
 - for Cisco 4200 series sensor, 680
 - password protection, 686–687

- in Linux
 - disabling, 262
 - restricting to system console, 263–264
 - root domain in Windows 2000, 764
 - [Root] object, default rights, 234
 - routable IP addresses, 577
 - route, 908
 - route cost, 908
 - routed daemon, 432
 - Router Information Protocol (RIP), 908
 - PIX Firewall support for, 552–553
 - router switching, 81
 - routers, **76–80**, 77, 908
 - configuring for NAT, **431–434**
 - Linux kernel configuration for, 507
 - protocol specificity, **79–80**
 - registering with certificate authority, 632
 - vs. switches/bridges, **80**
 - routine, risk from, 42
 - routing, 908
 - by PIX Firewall, **552–554**, 553
 - configuring, **606–612**
 - routing table, 908
 - Rowland, Craig, 296
 - RPC Locator service, port for, 380
 - rpm tool, 369
 - RSA Data Security, Inc., 908
 - RSA encrypted nonces, **631–632**
 - RSA encryption, **107**, 119
 - RSA Laboratories, 99
 - RSA signatures, **631**
 - Rshell, NAT problems, 434
 - rule base in Checkpoint Firewall-1, 452
 - Run As feature of Windows 2000, 141
 - Russell, Paul, 501
- S**
- S-HTTP (Secure Hypertext Transfer Protocol), 909
 - S/MIME (Secure/Multipurpose Internet Mail Extensions), 830
 - SACL (System Access Control List), in Windows 2000 security descriptor, 138
 - sadmind worm, 30
 - SafeNet client, 617, 656, 660
 - authentication configuration, **661**
 - configuring, **660–661**
 - sag, 904
 - SAM (Security Accounts Manager), 134, 182, 909
 - limits on database size, 765
 - Samba, 317
 - ACLs integration with, **344–349**
 - controlling initial access, **318–328**
 - authentication by username and password, **322–328**
 - binding to specific network interfaces, **318–319**
 - restricting access by computer, **319–322**
 - file ownership and permissions, **341–349**
 - per-share, **341–342**
 - per-user controls, **343–344**
 - ipchains or firewall to block access, **364–367**
 - non-Samba servers, **368–369**
 - over SSL, **349–363**
 - certificate creation, **353–356**
 - client configuration to use SSL, **360–363**
 - Samba configuration to use SSL, **356–360**
 - SSL configuration, **350–352**
 - passwords
 - encrypted vs. cleartext, **329–341**
 - parameters, 327–329
 - ports for SMB/CIFS, **364**
 - running through TCP wrappers or xinetd, **367–368**
 - SAR (segmentation and reassembly), of ATM packets, 67
 - SAS (single-attached stations), 911
 - scatternets, 62
 - Schneier, Bruce, 123
 - scope of problem, defining, **10–11**
 - scope of security process, 34
 - screened subnet, 538, 539. *See also* demilitarized zones
 - SDLC. *See* Systems Development Life Cycle
 - secchecksript (SuSE), 254

- secret key algorithm, 94, 169
- secret key encryption, 770
- secure applications, **827–833**
- secure cipher, 118
- Secure Hypertext Transfer Protocol (S-HTTP), 909
- Secure Shell (SSH), **107–108**, 350
 - port for, 380
- Secure Sockets (SSL), **108**. *See also* SSL (Secure Sockets)
- SecurIT firewall, **476–480**
- security
 - myth of total, **26–29**
 - need for improved, **84–87**
 - plan design, **869–872**
 - deployment planning checklist, **870–872**
 - systems analysis
 - objectives, constraints, risks and cost, **11–15**
 - scope of problem, **10–11**
 - theory, **115–117**
- Security Accounts Manager (SAM), 134, 182, 909
 - limits on database size, 765
- Security Associations (SA), 824
 - in IPSec, 173, **628–630**, 629
- Security Configuration Manager, **791**
- security descriptor, 137–138, 771
- security design
 - effect on existing systems and applications, **776–780**
 - application compatibility, **778–780**
 - client and server interoperability, **777–778**
 - client systems upgrades, **776–777**
 - upgrades and restructuring, **780–785**
- security groups in Windows 2000, **811–817**, 847–848
 - considerations for using, 815–817
 - default permissions, 813–814
 - how they work, 812
 - implementation, 815
 - policies, 155
 - predefined types, 812–813
- security identifiers (SIDs) in Windows 2000, **134–135**, **768–769**
- security levels in PIX Firewall, **554–556**
 - in 6 interface configuration, 603
 - assigning, **570–572**
- security log, 909
- security model
 - disconnected, **400–402**
 - for Samba, **323–327**
 - domain-level, **326–327**
 - server-level, **325–326**
 - share-level, **323–324**
 - user-level, **324–325**
- Security Parameter Index in ESP, 622
- security policies, 909
 - account policies, 791, **853–854**
 - auditing, 840
 - event log policies, **855**
 - filesystem policies, **857–858**
 - group policies. *See also* group policies restricted, **855–856**
 - local computer policies, **854–855**
 - placement and inheritance, **859–860**
 - public key policies, **858**
 - registry policies, **857**
 - restricted group policies, **855–856**
 - system services policies, **856–857**
- Security Policy (Windows 2000), **768–774**
 - audit logs, **773–774**
 - authentication, **770–771**
 - digital signature and data confidentiality, **772–773**
 - encryption, **769–770**
 - nonrepudiation, **773**
 - physical security, **774**
 - security configuration and analysis, **769**
 - security identifiers (SIDs), **768–769**
 - single sign-on, 770, **771–772**
 - two-factor authentication, **772**
 - user education, **774**
- security principals
 - moving in restructure process, **783–785**
 - in Windows NT, 768
- security proxies in Symantec Enterprise Firewall, 456–457
- Security Reference Monitor, **139**
- security requirements, **787**
- security templates in Windows 2000, 799

- security tokens, **108–110**, 109
- seed value, 126–127
- segmentation and reassembly (SAR), of ATM packets, 67
- segments, 909
 - in TCP, 748
- Select Users dialog box (Windows XP), 191
- selection criteria, 35
- selection methodology in documentation, 35
- self-powered, 909
- sensor IP parameters for IDSM, 707
- sensors. *See also* Cisco Secure IDS sensors
 - deployment, **664–674**
 - common locations, **665**, 666
 - interfaces, **666–667**
 - placement considerations, **664–665**
- sequence number, 909
 - in ESP, 622
- Sequenced Packet eXchange (SPX), 909
- Serial Line Internet Protocol (SLIP), 909
- server and client configuration, 909
- server-centric, 909
- Server Gated Cryptography (SGC) protocol, 832
- server-level security for Samba, **325–326**
- Server Operators group on domain controller, permissions, 814
- servers, 909. *See also* proxy server
 - backup, security case study, 30
 - digital certificate, **102–103**
 - disabling, 369
 - DNS, 884
 - duplicate, 885
 - failover, 887
 - file, 888
 - Internet Information Server (IIS), 114, 832
 - Internet, ports for, 380
 - mail, port for, 381
 - member, 896
 - Microsoft Internet Security and Acceleration Server, **461–469**
 - cost and support, **468–469**
 - future availability, 469
 - interface, **467–468**, 468
 - major feature set, **461–463**
 - minor feature set, **463–466**
 - security, **466–467**
 - Microsoft Proxy Server, 461
 - weaknesses, 466–467
 - non-Samba, **368–369**
 - remote access, 176, 907
 - and sensor placement, 665
 - remote servers, encrypted files on, **863–864**
 - single-homed dial-up, sample firewall scenario, **515–517**, 516
 - super server, xinetd as, 367
 - telephony, 913
 - verifying, **89**
 - web, 918
- service accounts, 910
- service pack, installing for IDSM, 725
- services, 910
 - on firewalls, 389
- session hijacking, **88–89**
- Session layer, 910
- session ticket from Kerberos, 147
- sessions in SPAN, 701
- set boot device command, 722–723
- set security acl map command, 715
- set vlan command, 710
- sets, relationship, 18
- SGC (Server Gated Cryptography) protocol, 832
- sgid in Linux, **271–274**
- shadow passwords
 - john and, 315
 - in Linux, **266–267**
- Shamir, Adi, 107
- Shannon, Claude E., 4
- share-level permissions in Windows XP, **192–194**
- share-level security, 910
 - for Samba, **323–324**
- share permissions, 811
- share security in Windows 2000, **160–164**
- Shareable attribute for NetWare files, 223
- shared secret encryption, 169, 625
- shares
 - for Samba ownership, **341–342**
 - in Windows 2000
 - accessing, 162

- creating, 161–162
 - default, 163
 - vs. file security, 163–164
 - permissions, 164
- Sharing Properties dialog box, 161–162
- shell, 910
- shielded, 910
- shielded twisted-pair cable (STP), 910
- show commands (Catalyst switch), **718–719**
- show config command, 725
- show configuration command (IDSM), 719
- show errorfile command (IDSM), 729
- show eventfile command (IDSM), 719
- show interface command (PIX), **562–563**, 574
- show ip command (PIX), 585
- show module command, 704, 728
- show nameif command (PIX), 585
- show port command, 728
- show rip command (PIX), 553
- show route command (PIX), 554, 609–610
- show tech-support command (PIX), 563
- show top pkts command, 728
- show version command (PIX), 543–544
- shun command (PIX), **563–564**
- shutdown
 - of IDSM, 726
 - of PIX network interface, 573
 - Windows XP rights to force remote, 186
- shutdown command (IDSM), 728
- SIDs (security identifiers), **134–135**
 - impact of moving security principals, 783
- signal, 910
- signal encoding, 910
- signaling method, 910
- signature-based detection, by Cisco sensors, 743
- signature of file, 302
- signature template for Cisco sensors, 691
- signing message, 95
- Simple Key Management for Internet Protocols (SKIP), **110**
- Simple Mail Transfer Protocol (SMTP), 830, 910
 - cleartext use by, 87
 - port for, 381
- Simple Network Management Protocol (SNMP), 911
 - logging on PIX Firewall, 568
- Simple WATCHer (swatch). *See* swatch (Simple WATCHer)
- single-attached stations (SAS), 911
- single-homed dial-up server, sample firewall scenario, **515–517**, 516
- single-mode fiber-optic cable, 51
- single sign-on in Windows 2000, 770, **771–772**, 796
- site policies, 154–155, 860
- SKIP (Simple Key Management for Internet Protocols), **110**
- skipjack, 911
- SLIP (Serial Line Internet Protocol), 909
- SLMsoft, 476
- smart cards, 772, 796, 799, **805–807**
 - cost of administering, 807
 - logon, **805–807**
- SMB, 165
- SMB/CIFS, ports for, **364**
- smbclient program, 360
- smb.conf file, for password encryption policies, **333–336**
- smbpasswd file
 - creating, 338
 - vs. smbpasswd program, 336
- smbpasswd program, 326, **336–338**
 - interface for, 318–319
- smid service, 753
- SMn modes for Bluetooth, 62–63
- SMTP (Simple Mail Transfer Protocol), 830, 910
 - cleartext use by, 87
 - port for, 381
- smurf attack, protection against, **524**
- SNMP (Simple Network Management Protocol), 911
 - cleartext use by, 87
 - logging on PIX Firewall, 568
- social engineering attack, user education against, **774**
- software
 - code review, 37
 - compatibility with Windows 2000 upgrade, **778–780**
 - secure, **833–834**
 - secure design, **827–833**
 - for virus protection, **245–247**

- Solaris/sadmind.worm, 30
- SONET (Synchronous Optical Network), 911
- source address, 911
- source port number, 911
- source routing, **410**
 - through NAT, **439–440**
- Soviet Union, 96
- space-based radio transmissions, 54
- Spafford, Gene, 302
- SPAN (Switch Port Analyzer), 668
 - for IDSM traffic capture, 700–701
 - limitations, 702–703
- Special Access dialog box (Windows), 347, 347
- special access, in Windows XP, 196
- splitter, 911
- spooling documents for printing, 144
- spread spectrum signal, 53
- SPS (Standby Power Supply), 911
- SPX (Sequenced Packet eXchange), 909
- Sqlnet2, NAT problems, 435
- SSH (Secure Shell), **107–108**, 350
- SSL (Secure Sockets), **108**
 - Samba over, **349–363**
 - certificate creation, **353–356**
 - client configuration to use SSL, **360–363**
 - Samba configuration to use SSL, **356–360**
 - SSL configuration, **350–352**
- SSL Proxy, 361
- SSLey, 350
- stakeholders, 40
- Standby Power Supply (SPS), 911
- star topology, 911–912
- state, 11
 - in model, 22
 - in risk assessment, 13
- state nets, 22
- state table, 912
- stateful inspection firewalls, 209, 497–498, **537**
 - Checkpoint Firewall-1 as, 447–448
 - ISA Server as, 462
 - with multiple interfaces, **539**
 - PIX Firewall as, 542
 - for Windows, 446
- stateful packet filtering, 406, **413–415**, 414
- stateless packet filtering, **406–412**
 - filtering on other information, **410–411**
 - IP address filtering, **407–408**
 - problems, **411–412**
 - protocol filtering, **406–407**
 - TCP/UDP ports, **408–410**
- static ARP table entries, 912
- static command (PIX), **587**, 605–606
- static NAT, 527
- static Port Address Translation (PAT), 593, **593–596**
- static routing, 912
 - configuration for VPN Hardware Client, 654
- static translation, 425, **429**
 - for PIX Firewall, 578–579
 - problems, **437–438**
- statistics from PIX firewall, 561
- stealth mode in SunScreen, 492
- stealth rule in iptables, 508–509
- steganography, **131**
- sticky bit in Linux permissions mask, 273
- STP (shielded twisted-pair cable), 910
- straight tip, 912
- stream cipher, **92**, 118
- strict reassembly for TCP session, 749, 750
- strict source routing, 410
- strong cipher, 118
- Stunnel, 361
- subgoal, 11
- subnet mask, 912
- subnetting, 912
- subnetwork, 912
- subnetwork address, 912
- subscriber connector, 912
- subsystems, defining, 17
- sudo utility (Linux), **267–271**
 - installing, **268**
 - sudoers file, **268–269**
 - sudo.log file, **270–271**
 - using, **269–270**
- suid in Linux, **271–274**
- SunScreen Secure Net 3.1, **490–494**, 493
- super server, xinetd as, 367

- supernetting, 912
- SUPERVISOR, 212, 226
- Supervisor rights
 - guidelines for granting, 232–233
 - in NetWare 6
 - for directories, 215
 - IRF and, 220, 231
 - for objects, 228
 - for properties, 229
 - for users and groups, 217
- surge protector, 912
- SuSE Linux, **254–255**
- SVC (switched virtual circuit), vulnerability, 67–68
- SWAT (Samba Web Administration Tool), interface for, 318–319
- swatch (Simple WATCHer), **291–296**
 - configuration examples, 294–295
 - configuring, **292–294**
 - installing, 292
 - vs. logcheck, **301–302**
 - running, 295–296
- Switch Port Analyzer (SPAN), 668
 - for IDS traffic capture, 700–701
 - limitations, 702–703
- switch routing, 81
- switched, 912
- switched virtual circuit (SVC), vulnerability, 67–68
- switches, **73–76, 74**
 - layer-3, **80–82**
 - vs. routing, **80**
- Symantec Enterprise Firewall, **455–460**
 - cost and support, **460**
 - as device, 469
 - documentation, **459–460**
 - interface, 459, **459**
 - major feature set, **455–457**
 - minor feature set, **457–458**
 - security, **458**
- symbols, known and unknown, 4
- symmetric algorithm, 118
- symmetric encryption, 169
- symmetric functions, **122–123**
- symmetric key encryption, 626, 770
- symmetrical keys, 913
- SYN flood attack, 913
 - protection against, **524–525**
- Synchronize event, auditing, 842
- Synchronous Optical Network (SONET), 911
- sysconfig-sensor utility, 681, **681–687**
 - IP configuration parameters, **682–683**
 - PostOffice communication parameters, **683–684, 684**
 - System Management parameters, **685–687**
 - date and time, 685
 - passwords, 686, 686
- SysKey, 143
- SYSLOG, logging on PIX Firewall, 568
- syslog utility (Linux), **276, 286**
 - server security, **290–291**
- syslog.conf file (Linux), **287–290**
- system, 3
 - dynamic nature, 32
 - environment influence on, 23–24
 - organization use of, **16**
 - views, 7
- System Access Control List (SACL), in Windows 2000 security descriptor, 138
- system accounts in Linux, 263
- System attribute for NetWare directories, 222
- system clock, clock command (PIX) to set, **567**
- System File attribute for NetWare files, 223
- system image for PIX Firewall, **546**
- system management tools, **788–791**
 - IntelliMirror, **788–790**
 - Security Configuration Manager, **791**
- system services policies, 791, **856–857**
- System SID, 135
- system time
 - for VPN Hardware Client, 652
 - Windows XP rights to change, 186
- systems analysis, **4–15**
 - applying to information technology, **15–24**
 - process steps, 10
 - defining problem scope, **10–11**
 - objectives, constraints, risks and cost, **11–15**

Systems Development Life Cycle, **33–42**
 Development and Acquisition, **36–38**
 certification, 38
 component and code review, 36–37
 system test review, 37–38
 disposal, **41–42**
 implementation, **38–41**
 accreditation, 40–41
 Initiation, **33–36**
 conceptual definition, 34
 functional requirement determination, 34–35
 protection specifications development, 35–36
 operation and maintenance, **41**
 Systems Theory, 5
 SYSVOL\$ share, 163

T

T-series connections, 916
 T1 line, 63–64
 Take Ownership event, auditing, 842
 Take Ownership permission, in Windows XP, 198
 targets, 11
 TCO (Total Cost of Ownership) study, 15
 TCP (Transmission Control Protocol), 364, 915
 port filtering, **408–410**
 TCP/IP (Transmission Control Protocol/Internet Protocol), 915
 security weaknesses, 329–330, 330
 TCP sessions, reassembly, **748–751**
 TCP Wrappers, running Samba through, **367–368**
 TDMA (Time Division Multiple Access), 914
 TDR (time-domain reflectometer), 914
 technical support structure analysis, **785–787**
 data center management, **786–787**
 desktop support management, **785–786**
 network management, **786**
 security requirements, **787**
 technology, types, **16**
 telephony server, 913

Telnet, 913
 to access PIX Firewall, 556
 blocking, 409
 cleartext use by, 87
 port for, 380
 temp files in Windows 2000, encryption, 144
 templates, 913
 for Windows 2000 security settings, 769
 terminal emulator, 913
 terminator, 913
 ternary set, 18
 terrestrial radio transmissions, 54
 test accounts, 913
 testing SSL on Samba, **360**
 TFTP (Trivial File Transfer Protocol), 915
 and Cisco router access, **546–547**
 TGT (Ticket-Granting Ticket) in Kerberos, 149
 Thicknet (Thick Ethernet), 913
 Thinnet (Thin Ethernet), 914
 threads, Access Token for, 135
 threats, 13
 hierarchy of, 14
 keeping up with, **210–211**
 three-way handshake for TCP session, 749–750
 throughput, 7
 ticket from Kerberos, 147
 Ticket-Granting Ticket (TGT) in Kerberos, 149, 802
 time division, 64
 Time Division Multiple Access (TDMA), 914
 time-domain reflectometer (TDR), 914
 time to live (TTL), 914
 time zones, PIX Firewall clock and, 567
 timeout by firewall, 438–439
 TIS (Trusted Information Systems), 484
 token, 914
 token cards, 108, 109
 token passing, 914
 Token Ring network, 914
 tone generator, 914
 tone locator, 914
 topology, 914
 topology security, **56–68**

- LAN topologies, **56-63**
 - Ethernet, **56-59**
 - wireless, **60-63**
- wide area network, **63-64**
 - ATM (Asynchronous Transfer Mode), **67-68**
 - frame relay, **64-67**
 - wireless, **68**
- Total Cost of Ownership (TCO) study, 15
- total security, myth of, **26-29**
- tracert, 915
- traffic capture by IDS, **698-699**
 - Catalyst switch parameters, **709-718**
 - command-and-control port VLAN, **709-710**
 - SPAN to configure, **710-712**
 - VACLs to configure, **712-716**
- traffic in IPSec tunnel, duration indicator, 637
- traffic isolation by bridges, 71
- trailer, 915
- training, 38
- Transactional attribute for NetWare files, 223
- transceiver, 915
- transform sets in IPSec, 627, **627-628**
- transient, 915
- transition in model, 22
- transitive trust, 763
- translation slot in PIX Firewall, 550, 581, 588
 - and packet processing, **551**
- translation table for PIX Firewall, 550
- transmission, 915
- Transmission Control Protocol (TCP), 364, 915
- Transmission Control Protocol/Internet Protocol (TCP/IP), 915
 - security weaknesses, 329-330, 330
- transmission media, 915
- transparent proxies, 385, 464
- Transport layer, 915
- transport mode in IPSec, 104, 170-171, 622, **622-623**
- trap-door, 124
- Traverse Folder/Execute File permission in Windows XP, 197
- triggers
 - for state transition, 22
 - in system log monitoring, 291
- trihomed firewall, 399, 399
 - with demilitarized zone, **520-523**, 521
- triple-DES, 101
- tripwire, **302-311**
 - configuring, **304-310**
 - environment variables, 306
 - policy file, **306-310**
 - policy file property mask characters, 308
 - Data Files rule, 309
 - installing, **303-304**
 - running, **310-311**
- Trivial File Transfer Protocol (TFTP), 915
- Trojan horses, 419
- troubleshooting
 - IDS, **728-729**
 - IPSec, **639-641**
- trunk lines, 915
- trunking capabilities of IDS monitoring interface, 673
- trust, 734
 - between domains, **763-767**
 - Windows NT vs. 2000, 767
 - in Kerberos, 146
- trusted devices in Bluetooth, 63
- trusted domains in Samba, 320
- Trusted Information Systems (TIS), 484
- trustee in NetWare, 213
 - rights to volume object, 238
- TTL (time to live), 914
- tunnel. *See* virtual private networks (VPN)
- tunnel lifetime, renewing at expiration, **637**
- tunnel mode in IPSec, 104, 170-171, 172, 622, **622-623**
- Turbolinux, 255, **255**
- twadmin utility, 305
- twisted-pair cable, 49, 916
- two-factor authentication
 - with smart card, 806
 - in Windows 2000, **772**
- type command (DOS), 916

U

- U (height measurement unit), 645
- UDP (User Datagram Protocol), 364, 917
 - port filtering, **408-410**
- ulimit command (Linux), 276
- umask setting in Linux, **275**
- unbound transmissions, **52-54**
- unconditionally secure cipher, 118
- Unified Client (Cisco), 617, **656-660**, 657
 - Authentication properties, 658, **658**
 - connection configuration, **657**
 - Connection properties, **659**, 659
 - General properties, **658**
 - preconfiguring clients, 659-660
- Uniform Resource Locator (URL), 916
- uniform security policies, **817-819**
- uninterruptible power supply (UPS), 916
- unit ID for security token, 109
- universal groups, 813
- Unix, 916
 - case sensitivity of username and password, 680
 - filtering by, **378**
 - firewalls, **471-496**
 - Computer Associates eTrust, **472-475**
 - NetWall, **480-483**
 - Network Associates Gauntlet, **483-490**
 - purchasing, **495-496**
 - SecurIT firewall, **476-480**
 - SunScreen Secure Net 3.1, **490-494**, 493
 - versions, 471
- unprivileged mode for PIX Firewall command-line interface, 557
- unshadow script for john, 315
- unshielded, 916
- unshielded twisted-pair cable (UTP), 49, 916
- untrusted networks, sensors for connections to, 664
- upgrade, 916
- UPS (uninterruptible power supply), 916
- uptime, 917
- URL (Uniform Resource Locator), 916
- usability, vs. security, 115
- user accounts, 115
 - auditing, 840
 - in Linux, **261-271**
 - good passwords, **264-265**
 - shadow passwords, **266-267**
 - sudo utility, **267-271**
 - sudoers file, **268-269**
 - sudo.log file, **270-271**
 - in Windows 2000, 133-134
 - in Windows XP, **182-192**
 - built-in groups, 183-184
 - creating, **187-190**
 - disabled, 190
 - rights, **185-187**
 - types, 183
- User Datagram Protocol (UDP), 364, 917
- user-level security, 917
 - for Samba, **324-325**
- user policies, group policies to control, 152-153, 154
- username, case sensitivity in Unix, 680
- users, 917
 - acceptance of system, 39
 - access control, in Samba, **343-344**
 - auditing. *See* audit policies
 - authentication
 - in Samba, **322-328**
 - in Windows 2000, **128-129**
 - education, **774**
 - EFS and, **862-864**
 - enabling for VPN Hardware Client, 654-655
 - encryption errors by, **95-96**
 - hacker seduction of, 438
 - involvement in planning and implementation, 39
 - in NetWare 6
 - default rights, 234
 - directory rights, **236-240**, 237
 - file rights, **217**
 - password protection, 775
 - password selection, 311
 - in Samba, 339
 - as risk, 210
 - role in security, 26-27

Users group in Windows XP, 184
 UTP (unshielded twisted-pair cable), 916

V

VACL (VLAN access control list)
 adding IDSM monitoring port, 715
 creating, 713–714
 for IDSM, 696
 for IDSM traffic capture, 701–703, 702
 vampire tap, 917
 /var/log/boot.log file, 287
 /var/log/maillog file, 287
 /var/log/messages file, 286, 287
 /var/log/secure file, 287
 variable-length subnet masking, 591
 /varlog/spooler file, 287
 VDO Live, NAT problems, 434
 vector, 28
 Vernam cipher, 92
 versions of Cisco Secure IDS software, 733
 video conferencing, NAT problems, 434
 vigilance, constant, **42–43**
 virtual COM, 917
 virtual local area network (VLAN), 75, 917
 mapping VACL to, 714–715
 virtual private networks (VPN), 164–165, **386–387**, 917. *See also* IPSec (IP Security)
 firewalls for, 375
 technologies, **166–169**
 types, **614–617**
 Cisco routers, **615–616**
 Cisco VPN Concentrator, **616**
 PIX Firewall, **616**
 VPN client software, **616–617**
 VPN devices, **615**
 virtual terminal password for IDSM, 707
 virus, 917
 virus engine, 917
 virus hoaxes, 27
 virus protection
 firewalls for, 375
 in NetWare 6, **244–247**
 VLAN (virtual local area network), 75, 917
 mapping VACL to, 714–715

VLAN access control list (VACL)
 adding IDSM monitoring port, 715
 creating, 713–714
 for IDSM, 696
 for IDSM traffic capture, 701–703, 702
 VLAN groups, 75
 VLAN SPAN, 700
 Voice over IP (VoIP), encryption, 640
 volume, 918
 volume objects in NetWare, trustee rights to, 238
 Vos, Jos, 501
 VPN (virtual private networks), 164–165, **386–387**, 917
 IP Security (IPSec) for, 103–104
 technologies, **166–169**
 VPN 3005 Concentrator (Cisco), **644–646**, 646
 characteristics, 645
 VPN 3015 through 3080 Concentrators (Cisco), **646–648**, 647, 648
 VPN Concentrator client support (Cisco), **648**, 649
 VPN Hardware Client (Cisco), **649–656**, 650
 managing, 655, **655–656**
 Quick Configuration Utility, **650–655**, 651
 VPN software clients (Cisco), **656–661**
 SafeNet client, 660, **660–661**
 Unified Client, **656–660**, 657
 vulnerability
 to brute force attack, 98
 from network cables, 49

W

WAN. *See* wide area network (WAN)
 WAP (wireless access point), 919
 Watchdog, 751
 settings, 752–753
 Watchguard Firebox, 499
 Watchguard Technologies, 506
 web browser, for VPN Hardware Client
 configuration, 650, 651
 web proxy, 918
 web server, 918

- web sites
 - for Internet RFCs, 114
 - for john updates, 315
 - secure, **831-833**
- whacking, 68
- white box view, 7, 8
- WhoAmI (Windows 2000), 135
- wide area network (WAN), **63-64**, 918
 - ATM (Asynchronous Transfer Mode), **67-68**
 - frame relay, **64-67**
 - wireless, **68**
- WiFi, 60
- Windows 95, virus spread on, 140-141
- Windows 2000. *See also* Security Policy (Windows 2000)
 - backward compatibility, 779
 - default state, 116
 - delegation of administration, 766-767
 - Encrypting File System (EFS), **142-145**
 - local security, **133-145**
 - resource access, **135-140**
 - rights vs. permissions, **140**
 - security identifiers, **134-135**
 - management tools, **788-791**
 - IntelliMirror, **788-790**
 - Security Configuration Manager, **791**
 - network security, **145-178**
 - Active Directory, **146**
 - group policies, **152-160**
 - Kerberos authentication and domain security, **146-152**, 151
 - network layer encryption, **164-178**
 - share security, **160-164**
 - NTFS file system permissions, **140-142**
 - security concepts, **760-768**
 - authentication and authorization model, 760
 - domain model, 760-762, 761
 - trust management, **763-767**
 - security mechanisms, 115-116
 - security tools, 114
 - upgrades and domain restructuring, **780-785**
 - virus block by, 141
- Windows Internet Name Service (WINS), 777, 918
- Windows NT, 918
 - Address Resolution Protocol (ARP) and, 441-442
 - authentication and access tokens in, 771
 - limits on account database size, 765
 - security issues, 113-114
- Windows NT Service, 918
- Windows operating system
 - default encryption, **332-333**
 - encryption policy setup, **340-341**
 - filtering by, **378**
 - firewalls, **445-469**
 - Checkpoint Firewall-1, **447-454**
 - Microsoft Internet Security and Acceleration Server, **461-469**
 - Symantec Enterprise Firewall, **455-460**
 - hacking attempts against, 391
 - versions, 379
- Windows Terminal Services
 - blocking port, 409
 - port for, 381
- Windows XP, 181-182
 - group accounts, creating, **190-192**
 - ownership, **203-206**
 - defining, **204**
 - taking, **205-206**
 - permissions, **192-203**
 - auditing files and folders, **199-203**
 - file and folder, **194-199**
 - share-level, **192-194**
 - user accounts, **182-192**
 - built-in groups, 183-184
 - creating, **187-190**
 - rights, **185-187**
 - types, 183
- winipcfg, 918
- WinLogon process, 135
 - steps, 137
- WinNuke, 918
- WINS (Windows Internet Name Service), 777, 918
- wire crimper, 919

wireless

- hacking, 68
- hubs, 69
- for LAN, **60–63**
- for WAN, **68**
- wireless access point (WAP), 919
- wireless bridge, 919
- workgroup, 919
- workstation, 919
- World Wide Web (WWW), 919
 - port for, 380
- worms, 919
- Write All Properties event, auditing in Active Directory, 841
- Write Attributes event, auditing, 842
- Write Attributes permission in Windows XP, 198
- write command (PIX), **564**
- Write Data event, auditing, 842
- Write Extended Attributes event, auditing, 842
- Write Extended Attributes permission in Windows XP, 198
- Write permission in Windows XP, for files and folders, 195

- Write rights in NetWare 6
 - for directories, 215
 - for properties, 229
 - for users and groups, 217
- WWW (World Wide Web), 919

X

- x*-ary set, 18
- X Windows, 919
 - blocking port, 409
- X.509 standard, 103
- xinetd program, 368
 - running Samba through, **367–368**
- Xing, NAT problems, 434
- xlate table, for PIX Firewall, 550
- XOR cipher, 122
- Xsentry Internet Firewall, 499

Y

- Ylönen, Tatu, 107