

Index

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

Symbols and Numbers

. (dots), URLScan tool check for, 68
 3DES, 135, 435, 512
 8.3 filename autogeneration, disabling,
 58, 84
 802.1g standard (IEEE), 512
 802.1x standard (IEEE), **197–199**, 512
 authentication for, 198
 combining VPNs with, **206**
 802.11a standard (IEEE), 215, 512
 vs. 802.11b, 183, *184*
 802.11b standard (IEEE), 215, 512

A

Access Control Entries (ACEs), 512
 in Discretionary Access Control
 List, 9
 Access Control List (ACL), 512
 configuration, **470–471**
 Access Control Settings dialog box, 19
 Auditing tab, 19, *459*
 access control settings, for system
 services, 23–24
 “Access Is Denied” error message, 438
 access point, 512. *See also* wireless access
 point (WAP)
 access token, 277, 512
 account lockout policy, in security
 templates, 11
 account logon events, tracking, 17, 465
 account management events, tracking,
 17, 465
 Account Policies in security templates, 11
 configuration, *14*, **14–16**

accounts
 Administrator account, renaming,
 59, *60*
 Anonymous user account, 84
 disabling, 67
 real world scenario, 70
 restrictions in Windows 2000
 domain controller, **55–57**, 56
 built-in accounts, securing, **58–59**
 IUSR_computername account, 292
 disabling, 67
 password, 318
 user accounts
 configuring for delegation, 48
 manual reset after lockout, 73
 ACEs (Access Control Entries), 512
 in Discretionary Access Control List, 9
 Active Directory (AD), 5, 512
 for certificate store, 424
 Configuration container, 379
 enabling auditing for object, 20
 GPO assignment to container in, 30
 to provide single-sign-on, 279
 publishing certificates through,
 425–429
 in child domain, **427–429**
 from standalone online CA,
 425–427
 trust relationship between
 Windows NT 4 and, 290
 Active Directory domain
 logon process, 278–279
 NT LAN Manager (NTLM), 273
 Active Directory domain controller,
 client security to traffic, **243–246**
 Active Directory–integrated DNS
 zones, 62
 secure updates to DNS records, 55

534 Active Directory Properties dialog box – auditing

- Active Directory Properties dialog box
 - Advanced tab, 246
 - General tab, 245
- Active Directory Sites and Services (ADSS), 7, 378, 513
 - configuration, 428
- Active Directory Users and Computers (ADUC), 7, 274, 513
 - to apply Group Policy, 54
- Active Server Pages (ASP), adding support for, 71
- AD. *See* Active Directory (AD)
- Add IP Filter dialog box, 330, 330–331
- Add Object dialog box, 25
- Add or Remove Software applet (Control Panel), for RIS service, 102
- Add/Remove Snap-In dialog box, 9, 10
- Administrative Templates settings in GPOs, 4
- Administrator account, renaming, 58–59
- Administrator certificate template, 379
- administrator groups, nesting, 451
- Administrator Properties dialog box, 343
 - Configure Membership tab, 27
 - in mixed mode, 343
 - in native mode, 344
- ADSS (Active Directory Sites and Services), 7, 378, 513
 - configuration, 428
- ADUC (Active Directory Users and Computers), 7, 513
 - to apply Group Policy, 54
- AH (Authentication Header), 149, 173
- AIA (authority information access), 362, 514
- AirSnort, 203
- anonymous account for IIS, 67
- anonymous authentication, 292–294, 513
 - password, 318
- Anonymous user account, 84
 - disabling, 67
 - real world scenario, 70
- anonymous users, access restriction, 55–57
 - with Lockdown tool, 64
- anti-spam filters on gateway, 52
- antireplay, 135, 172
- antivirus software, 503
 - and encrypted files, 438
- application log, 452
 - IPSec entries, 158
- archive keys, in EFS troubleshooting, 438
- archived certificates, 423, 447
- archiving files, during service pack installation, 91, 128
- association in wireless networks, 190
- asymmetric, 513
- asymmetric keys, 219, 513
- asynchronous processing, of Group Policy Objects, 7
- attacks
 - auditing attempts, 457
 - countermeasures, 508–509
 - Denial of Service (DoS) attacks, 134, 504–505, 517
 - hackers, 501–502
 - ping use by, 477
 - indicators of, 496–497
 - isolating and containing, 506
 - preserving chain of evidence, 507–508
 - restoring services after, 510
 - spyware, 504
 - Trojan Horse, 505
 - viruses, 502–504
 - worms, 505–506
 - written policies for, 498
- attribute, 513
 - for Encrypting File System, 417
- Audit Policies
 - blocking inheritance, 461–462
 - security templates, 11
 - configuration, 16–21
- auditing, 42, 450, 452, 457–463, 493, 513
 - enabling, 458–463
 - for resources, 459

Auditing Entry dialog box, 19, 20

auditing logs

- importance of reading, 494
- managing distributed, 481–486
- for RRAS, 332–333

Authenticated Session certificate template, 379

Authenticated users entries, in discretionary access control list, 9

authentication, 272–291, 513

- exam essentials, 311–312
- in extranet scenarios, 286–288
- Kerberos, 276–277
- interoperability with Unix, 284–286
- key for wireless communication, 72
- LAN protocols, 273–277
 - NT LAN Manager (NTLM), 273–275
- logon process, 277–279
- models for SQL Server, 47
- multifactor, with smart cards and EAP, 310–311
- with nontrusted domain members, 286–288
- protocol configuration for mixed Windows client-computer environments, 281–284
 - Windows 95/98 clients, 282–283
 - Windows NT 4, 283–284
- protocol configuration for RRAS, 327
- protocol mismatches RRAS server and clients, 328–329
- for secure remote access, 306–310
 - RRAS protocols, 307
- by Secure Sockets Layer, 219
- troubleshooting, 280
- trust relationships, 288–291, 289
- for web users, 291–306
 - anonymous, 292–294
 - basic authentication, 294–295
 - with client certificate mapping, 303–306
 - digest authentication, 296–298, 518

- integrated Windows authentication, 298–300, 521
- passport authentication, 300–303

Authentication Header (AH), 149, 149, 173, 513

authentication method, 513

- in IPSec rule, 142, 143
- troubleshooting, 157

Authentication Methods dialog box (IIS), 293, 297, 300

authenticator, 276, 513

authenticity in business communications, 358

authority information access (AIA), 362, 514

auto-enrollment, 389–390, 514

- of user certificates, 433

autogeneration of 8.3 filenames, disabling, 58, 84

Automatic Certificate Request Group Policy, 381–383

Automatic Certificate Request Setup Wizard, 151–153

Automatic Updates, 106

B

backup

- of certificate, 223
- of certificate authority, 395–398
- of EFS certificate, 418
- IIS metabase, 113, 395–396

base key in WEP, 193

Base64 Encoded X.509 (.cer), 419, 514

Base64 Encoding, 294, 295

Basic authentication, 294–295, 318

Basic EFS certificate template, 379

beacon, 514

bindery emulation, 74

biometric devices, multifactor authentication with, 310

blocking inheritance, 8, 461–462

boot process. *See* rebooting

536 branch offices – certificates in SSL

branch offices, VPNs for connecting,
324
built-in accounts, and security, 58–59
BulkAdmin role, in SQL Server 2000, 50

C

CA Server Properties dialog box,
Extensions tab, 365
canonicalization, 68, 514
CAs. *See* certificate authorities (CAs)
CDP (CRL distribution point), 516
creating for stand-alone offline root
CA, 364–365
certificate authorities (CAs), 514. *See*
also client certificates
certificate enrollment and renewal,
386–390
auto-enrollment, 389–390
Certificates MMC Snap-in,
388–389
manual enrollment, 386–389
certificate templates for enterprise
CAs, 379–380
exam essentials, 399–400
Group Policies for certificate
distribution, prerequisites,
381–386
hierarchy of, 359, 360
intermediate CAs, 359
installing and configuring,
366–372
issuing CAs, 360
installing and configuring, 372–379
viewing published certificates and
CRLs, 378–379
managing, 390–398
backup, 395–398
editing certificates, 393
managing CRLs, 394
restoring backup, 397–398
revoking certificates, 392–393
viewing certificates, 391–392
and public key infrastructure (PKI),
358–390
for remote clients, 154
root CA, 359
configuring publication of CRLs,
364–366
installing and configuring,
361–363
threats to, 359
Certificate Authority MMC console, to
revoke certificate, 392, 392–393
Certificate dialog box, 391, 391–392
Certificate Export Wizard, 421
Certificate Import Wizard, 422
Certificate Properties dialog box, 394
Certificate Purpose view, 423
certificate revocation list (CRL),
361, 514
configuring publication of, 364–366
managing, 394
viewing in Active Directory, 378–379
Certificate Signing Request (CSR), 222,
223, 269, 514
certificate store, 423–424, 515
certificate templates for enterprise CAs,
379–380, 515
certificate trust list (CTL), 515
friendly name, 386
certificates, 514
exporting, 446
importing, 446
in IPsec, 151–153
configuration, 156–157
renewing, 153
viewing in Active Directory, 378–379
Certificates Enrollment web pages, 386
certificates in SSL
backup of, 223
private, 230–235
renewing, 235–236
public
installation, 227–228
obtaining, 221–230
renewing, 228–230

- Certificates MMC snap-in, 156, 390
 - for certificate enrollment, 386
 - to edit certificates, 393
 - to enroll and renew certificates, 388–389
 - to enroll certificates, 430–431
 - for exporting certificate, 420
 - for importing certificate, 422
 - installation, 383
- Certification Authority Backup Wizard, 395
- Certification Authority MMC snap-in, 390, 391
 - to revoke certificate, 392, 392–393
- certreq.exe, 390
- certutil.exe, 361, 390, 515
 - for IIS metabase backup, 395
 - to restore Certificate Services, 397–398
- chalk marks, 202–203
- Challenge Handshake Authentication Protocol (CHAP), 515
 - for RRAS, 308
- challenge phrase, 223
- child domain, certificates in, 427–429
- child objects, auditing configurations for, 19
- child server, 515
 - for Software Update Services, 114
- CIFS (Common Internet File System), 73, 158, 160, 172, 516
- cipher.exe, 437, 447, 515
- client certificate mapping, authentication with, 303–306
- client certificates, 408–424
 - Encrypting File System (EFS), 415–418, 416
 - enrolling, 430–433
 - auto-enrollment, 433
 - with Certificates MMC snap-in, 430–431
 - with Web Enrollment pages, 431–432
 - exam essentials, 439–440
 - exporting, 419–421
 - with Outlook Express, 414
 - importing, 421–423
 - mapping, 515
 - publishing through Active Directory, 425–427
 - in child domain, 427–429
 - from standalone online CA, 425–427
 - Secure MIME, 408–414
 - to sign and seal e-mail, 410–413
 - storage, 423–424
- Client Installation Wizard, Remote Installation Services for, 5
- client operating systems, security, 73–75
- Client (Response Only) policy for IPSec, 138
- Client Services for NetWare, 74
- clients
 - preventing impersonation, 54
 - securing to Active Directory domain controller traffic, 243–246
 - securing with IPSec, 154
 - troubleshooting security templates for mixed environments, 35
 - for virtual private networks (VPNs) configuration, 333–337
 - Connection Manager Administration Kit, 345–349
 - IP addresses, 327
 - Remote Access Policies, 341–344
 - troubleshooting, 338–339
- CMAK. *See* Connection Manager Administration Kit (CMAK)
- Code Signing certificate template, 379
- Common Internet File System (CIFS), 73, 158, 160, 172, 516
- Comodo InstantSSL, public certificate from, 224–225
- compatible template, 13
- compatws template, 13, 24, 42
- compromised-key attack, 134

538 computer certificates – delegation

- computer certificates
 - Group Policy for automatic enrollment, 381
 - requesting, 389, 431
 - templates, 379
 - Computer Management, to enable auditing, 17
 - computer Properties dialog box, General tab, 49, 49–50
 - Computer Security Incident Response Team, 498–500
 - creating, 498–499
 - computer settings of GPO, processing, 7
 - computers
 - configuration settings on, 6
 - startup scripts, 5
 - conditions, 516
 - in Remote Access Policies, 342
 - confidentiality, 172
 - in business communications, 358
 - IPSec and, 135
 - config.pol file, 16
 - Configuration container for certificate templates, 379
 - Configure Automatic Updates Properties dialog box, 111, 111
 - Connect VPN ServerName dialog box, 335
 - Connection Manager Administration Kit (CMAK), 345–349, 516
 - client deployment and testing, 349
 - wizard install, 346
 - wizard run, 346–348
 - containers
 - GPO assignment in Active Directory, 30
 - linking GPOs to, 6
 - Control Panel, Add or Remove Software applet, for RIS service, 102
 - copy command, for EFS files, 438
 - countermeasures for attacks, 516
 - implementing, 508–509
 - Critical Update Notification service, 113, 129
 - CRL (certificate revocation list), 361, 514
 - configuring publication of, 364–366
 - managing, 394
 - viewing in Active Directory, 378–379
 - CRL distribution point (CDP), 516
 - creating for stand-alone offline root CA, 364–365
 - cross-database ownership chain, 48
 - Cryptographic Message Syntax Standard - PKCS #7 Certificates, 419, 516
 - Cryptographic Service Provider (CSP), 410, 516
 - CSR (Certificate Signing Request), 222, 223, 269, 514
-
- D**
- DAACL (discretionary access control list), 8, 518
 - data decryption field (DDF), 516
 - Data Encryption Standard (DES), 135, 516
 - data loss, countermeasure for, 509
 - data modification by attacker, 133
 - data recovery field (DRF), 517
 - database, in Security Configuration and Analysis tool, 32–33
 - DC security template, 14
 - DDF (data decryption field), 516
 - de-militarized zone (DMZ), 53, 517
 - front-end Exchange servers in, 52
 - dead gateway detection, 57
 - decryption, 517
 - dedicated SMTP virtual servers, 249–250
 - default security templates, 12–13
 - default store for certificates, 424
 - Default Web Site Properties dialog box
 - Directory Security tab, 293
 - Web Site tab, 476
 - delegation
 - trusting computer for, 49
 - user account configuration for, 48

- Delegation Authentication, 83, 84, 517
 - SQL and, 47–48
- Delegation of Control Wizard, 429
- denial of service (DoS) attacks, 84, 134, 504–505, 517
 - countermeasure for, 509
 - DNS susceptibility, 61
 - preventing, 57
- deployment of security templates
 - with Group Policies, 29–30
 - with scripts, 31–33
- DER Encoded Binary X.509 (.cer), 419, 517
- DES (Data Encryption Standard), 135, 516
- desktop.ini file, 437–438, 517
- DHCP (Dynamic Host Configuration Protocol), 60–61
 - for VPN client IP addresses, 327
 - for wireless networks, 185–186
- Diffie-Hellman (DH) algorithm, 135, 172, 517
- Digest authentication, 296–298, 318, 518
- digital certificates. *See* certificates
- digital signatures, 54–55, 135, 358, 409, 518. *See also* SMB signing
- directory permissions in NTFS, 470–471
- Directory Services, 518
 - access events tracking, 17, 466
 - installing client, 282–283
 - log, 452, 493
- disabling autogeneration of 8.3 filenames, 58
- disabling LM hash creation, 58
- disaster recovery, Software Update Services and, 113
- discretionary access control list (DACL), 8, 518
- Distinguished Encoding Rules (DER), 419
- distributed audit logs, 481–486
- distributed denial of service attack, 504
- distribution group, 450
- DMZ (de-militarized zone), 53, 517
 - front-end Exchange servers in, 52
- DNS (Domain Name System), 61–62
 - names allowed access to web server, 66
 - security policies to configure dynamic update settings, 27
 - updates, and security, 55
 - using multiple names, 227
 - for VPN client IP addresses, 327
- DNS Server log, 452
- domain container, Group Policy Objects linked to, 4
- domain controllers
 - DHCP and, 61
 - Group Policies for, 30, 43
 - NETLOGON share point, 16
 - refreshing policies, 8
 - security, 53–59
 - anonymous access restriction, 55–57
 - for built-in accounts, 58–59
 - digital signatures, 54–55
 - disabling autogeneration of 8.3 filenames, 58
 - disabling LM hash creation, 58
 - DNS updates, 55
 - hardening TCP/IP stack, 57–58
 - NTLM for legacy clients, 57
 - SMB signing and, 158–163
 - sysvol folder on, 6
- domain local group, 450
- domain member servers, EFS encryption for, 435–436
- domain name ownership, proof of, 222
- Domain Name System (DNS). *See* DNS (Domain Name System)
- domains
 - enterprise CA placement in, 373
 - logon process, 278–279
- DoS (denial of service) attacks, 84, 134, 504–505, 517
 - countermeasure for, 509
 - DNS susceptibility, 61
 - preventing, 57

540 dots (.) – Error message type in event log

dots (.), URLScan tool check for, 68
 DRF (data recovery field), 517
 dynamic DNS, 61
 Dynamic Host Configuration Protocol (DHCP), 60–61
 for VPN client IP addresses, 327
 for wireless networks, 185–186
 dynamic rekeying, 135, 518

E

e-mail. *See also specific protocols*
 countermeasure for flood, 509
 methods for, 247–248, 248
 real world scenario, 259
 S/MIME to sign and seal, 410–413
 scanning for viruses, 52
 signed or sealed, 446
 signing, 414
 testing secured, with Outlook Express, 256–259
 virus risk from, 504
 e-mail servers
 client security to traffic, 246–248
 securing with IPsec, 154
 EAP (Extensible Authentication Protocol), 200–201, 356
 EAP-MD5 (Extensible Authentication Protocol Message Digest 5), 519
 for RRAS, 308–309
 for Windows CE, 182
 EAP-TLS (Extensible Authentication Protocol with Transport Layer Security), 197, 200, 519
 for RRAS, 309–310
 for Windows CE, 182
 EAPOL (Extensible Authentication Protocol Over LANs), 197, 519
 ease of use, vs. security, 53
 eavesdropping, 133
 Edit Dial-in Profile dialog box, 345
 Edit Rule Properties dialog box
 Authentication Methods tab, 142
 Connection Type tab, 142
 Filter Action tab, 145
 Tunnel Setting tab, 140
 editing certificates, 393
 EFS. *See* Encrypting File System (EFS)
 EFS Recovery Agent certificates
 and auto-enrollment, 387
 template, 379
 emergency information for servers, 498
 offline storage, 499
 EnableDeadGWDetect Registry key, 57
 EnablePMTUDiscovery Registry key, 58
 Encapsulating Security Payload (ESP), 149, 150, 173, 519
 Network Address Translation (NAT) and, 339
 Encrypting File System (EFS), 416, 434–439, 519
 disabling, 437–438
 encryption for domain members, 435–436
 implementing, 434–435
 for securing files and folders, 415–418
 and SQL Server 2000, 51
 troubleshooting, 438–439
 and workgroup members, 436–437
 Encrypting File System, SQL Server and, 83
 encryption, 519
 by Secure Sockets Layer, 219
 testing connection, 242–243
 for wireless networks, using 802.1x, 197–199, 198
 encrypted e-mail, sending with Outlook Express, 413
 enterprise CAs, 372
 installation, 373–377
 placement in domains, 373
 placement of servers, 373
 Enterprise mode for WPA, 194
 Enterprise Subordinate CA, 368
 enterprise, SUS deployment, 113–114
 Enterprise Trust list, Group Policy to configure, 384–386
 Error message type in event log, 453, 455

- error messages
 - for Encrypting File System, 438–439
 - information on, 279
 - “Network name is no longer valid”, 163
- ESP (Encapsulating Security Payload), 149, 150, 173, 519
 - Network Address Translation (NAT) and, 339
- event, 452, 519. *See also* Windows events
- Event IDs, 454
 - 512 error, 468
 - 513 error, 468
 - 517 error, 468
 - 529 error, 464
 - 530s error, 464–465
 - 534 error, 464
 - 539 error, 465
 - 560 error, 466
 - 562 error, 466
 - 563 error, 466
 - 564 error, 466
 - 565 error, 466
 - 576 error, 467
 - 577 error, 468
 - 578 error, 468
 - 592 error, 468
 - 593 error, 468
 - 594 error, 468
 - 595 error, 468
 - 608 error, 469–470
 - 609 error, 469–470
 - 610 error, 469
 - 611 error, 469
 - 624 error, 465
 - 626 error, 465
 - 627 error, 465
 - 628 error, 465
 - 629 error, 465
 - 630 error, 465
 - 675 error, 465
 - 677 error, 465
- event logs
 - file formats for saving, 494
 - IPSec, common entries, 157–158
 - for RRAS, 332–333
 - security template configuration, 28, 29
- Event Viewer, 453, 455
 - event messages in, 452–456
 - filtering in, 456, 456
- EventComb, 481–486, 483, 519
 - .txt files from, 483, 484
 - downloading, 481
 - opening screen, 482
 - real world scenario, 485
 - to search for domain controller restarts, 485–486
- Everyone security group, 460, 493
- evidence of attack, preserving, 507–508
- Exchange 2000 Server
 - securing IMAP4 on, 252–253
 - securing POP3 on, 254–256
 - securing SMTP on, 250–251
 - store access, 83
- Exchange Installable File System (ExIFS), 51, 519
- Exchange Server, security, 51–53
- expiration of certificate, 228
- explicit deny, 472
- exporting client certificates, 419–421, 446
 - with Outlook Express, 414
- Extensible Authentication Protocol (EAP), 356
 - authentication methods for wireless networks, 200–201
- Extensible Authentication Protocol Message Digest 5 (EAP-MD5), 519
 - for RRAS, 308–309
 - for Windows CE, 182
- Extensible Authentication Protocol Over LANs (EAPOL), 197, 519
- Extensible Authentication Protocol with Transport Layer Security (EAP-TLS), 197, 519

542 extranets – GRE (Generic Routing Encapsulation)

- for RRAS, 309–310
- for Windows CE, 182
- extranets, 288, 519
 - access methods, 287
 - authentication configuration, 286–288
- with virtual private networks (VPNs), 340–341
- for wireless connections, 204, 204–205

- Flexible Single Master Operations (FSMO) role, 7
- Folder Redirection settings in GPOs, 5
- forest-to-forest trusts, 289, 318
- forest-to-NT4 domain trust, 289
- forest-to-realm trust, 289
- fragmentation, largest acceptable packet without, 58
- front-end/back-end (FE/BE) architecture, 53
- front-end Exchange servers, 52
- FSMO (Flexible Single Master Operations) role, 7
- FTP site, recovering infected, 59
- Full Control permission (NTFS), 470

F

- facial recognition, 272
- failed attempts to access resource, tracking, 461
- Failure Audit message type in Security log, 454, 455
- farm of SUS servers, 113
- FAT (file allocation table) partitions, security templates and, 12
- FEK (file encryption key), 519
- File and Print Services for NetWare, 75
- file encryption key (FEK), 519
- file extensions, URLScan tool check for, 68
- file format, for exporting certificate, 419
- file permissions in NTFS, 470–471
- File Replication log, 452, 493
- file server, EFS encryption by, 435
- File Services for Macintosh, 85
- File System object, in security templates, 12
- File System Permissions, security template configuration, 24–26
- filenames, autogeneration of 8.3, disabling, 58, 84
- Filter Properties dialog box
 - Addressing tab, 144
 - Protocol tab, 144, 145
- filtering, in Event Viewer, 456, 456
- fingerprint scanners, 310
- firewalls, 520
 - configuration issues in IPSec, 157
 - log files, 477
 - and Software Update Services, 128

G

- Gateway Services for NetWare, 75
- Gemplus smart card, 424
- Generic Routing Encapsulation (GRE), 341, 520
- Generic Security Service Application Program Interface (GSSAPI), 285, 520
- GINA (Graphical Identification and Authentication dynamic link library), 273, 278
- global groups, 450
- globally unique identifier (GUID), and GPT name, 6
- GPC (Group Policy Container), 5
- GPOs. *See* Group Policy Objects (GPOs)
- gpresult resource kit utility, 33, 33
- GPT (Group Policy template), 5–6
- Graphical Identification and Authentication (GINA) dynamic link library, 273, 278
- GRE (Generic Routing Encapsulation), 341, 520

Group Policies, 3–9

- applying, 7–8
 - to automatically request certificates, 151, 151–152
 - for certificate auto-enrollment, 433
 - for certificate distribution, 381
 - prerequisites, 381–386
 - configuring, 4–7
 - to enable auditing, 17, 458–463
 - Enterprise Trust list configuration
 - with, 384–386
 - inheritance modification, 8–9
 - for IPsec implementation, 136–148, 137
 - order of processing, 29–30, 43
 - to require digital signing, 54
 - Security Options, 56
 - SMB signing, 161
 - security template deployment with, 29–30
 - Trusted Root Certification
 - Authorities list configuration
 - with, 383–384
- Group Policy Container (GPC), 5
- Group Policy Objects (GPOs), 3
- assignment to container in Active Directory, 30
 - for client security settings, 73
 - to configure SUS client, 110
 - configuring for automated certificate distribution, 244
 - determining object assignment, 33
 - linking to containers, 6
 - processing, 7
- Group Policy template (GPT), 5–6
- GSSAPI (Generic Security Service Application Program Interface), 285, 520
- guest account
 - for IIS, 292
 - renaming, 58–59
- GUID (globally unique identifier), and GPT name, 6

H

- hackers, 501–502
- decryption of WEP base key, 193
 - DNS susceptibility, 61
 - information needed for DHCP, 60
 - ping use by, 477
- hard Security Association, 136
- hardening TCP/IP stack, 57–58
- hash algorithms, 172
- Hash Message Authentication Codes (HMAC), 145, 149
- HFNetChk tool, 92, 128
 - and Microsoft Baseline Security Analyzer, 98–101
 - newsgroup for, 100
- high bit characters, URLScan tool check for, 68
- high security templates, 13
- hisecdc template, 13, 24
- hisecws template, 13, 42
- HKEY_. *See* Registry
- HKEY_LOCAL_MACHINE entries in Registry, 9
- \Software\Microsoft
 - \MSSQLServer\MSSQLServer, 47
 - \Windows\CurrentVersion,
 - \Explorer, 434
 - \Windows\CurrentVersion\WindowsUpdate\CriticalUpdate, 113
 - \WindowsNT\CurrentVersion,
 - \EFS, 438
 - \WindowsNT\CurrentVersion\Hotfix, 93
 - \System\CurrentControlSet
 - \Control\FileSystem, 58
 - \Control\LSA, 282–283, 284
 - \Services\IPSEC\DiagnosticMode, 155
 - \Services\LanManServer\Parameters, 162
 - \Services\PolicyAgent\Oakley\EnableLogging, 155

544 HMAC (Hash Message Authentication Codes) – Internet Information Server (IIS)

- \Services\Rdr\Parameters, 162–163
 - \Services\RemoteAccess\Parameters
 - \Account Lockout, 72, 73
 - \Services\Tcpip\Parameters, 57–58
 - \Services\Tcpip\Parameters\Disable
 - DynamicUpdate, 27
 - \Services\VxD\VNetsup, 163
 - HMAC (Hash Message Authentication Codes), 145, 149
 - honeypot, 509, 520
 - hotfixes, 88, 521. *See also* service packs
 - determining current status, 88–89
 - management, 105–119
 - QChain to install, 118–119
 - troubleshooting, 119–121
 - hotfix.exe, command-line switches, 103
 - HTTP 403.4 error page, 239
-
- I**
- I386 distribution folder, 118
 - identity spoofing, 134
 - IEEE (Institute of Electrical and Electronics Engineers), 197
 - IIS. *See* Internet Information Server (IIS)
 - IIS Lockdown tool, 53, 108
 - IIS metabase, 521
 - backup, 113, 395–396
 - IKE (Internet Key Exchange), 136
 - negotiation failure, 156–157
 - IMAP4 (Internet Messaging Access Protocol), 247–248, 251–254
 - testing secured, with Outlook Express, 256–259
 - impersonation, 134, 172, 521
 - SMB signing to deter, 160–161
 - Import Template dialog box, 32
 - importing, 521
 - client certificates, 421–423, 446
 - Incident Response Plan, of Computer Security Incident Response Team, 499–500
 - incremental security templates, 13–14
 - .inf files, 3, 10
 - Information message type in event log, 453
 - infrastructure security, 59–62
 - DHCP (Dynamic Host Configuration Protocol), 60–61
 - DNS (Domain Name System), 61–62
 - inheritance
 - of auditing settings, 20
 - blocking, 461–462
 - of Group Policy, modifying, 8–9
 - for Group Policy Objects, 7
 - initialization vector (IV), 191, 521
 - installation
 - of intermediate CAs, 366–372
 - of issuing CAs, 372–379
 - of root CA, 361–363
 - of service packs, 89–92
 - of SSL certificate, 227–228
 - Integrated Windows authentication, 298–300, 521
 - integrity
 - in business communications, 172, 358, 361
 - of packet, IPsec and, 135
 - intermediate CAs, 359, 521
 - installing and configuring, 366–372
 - prerequisites, 366
 - Internet Authentication Service (IAS) server, 71–73, 197
 - Internet Explorer Maintenance settings in GPOs, 5
 - Internet Information Server (IIS) authentication configuration
 - anonymous authentication, 293–294
 - Basic authentication, 294–295
 - digest authentication, 296–298
 - Integrated Windows authentication, 299–300
 - changes from SUS install, 120
 - enforcing SSL on, 237, 238
 - Lockdown tool, 53, 62–66
 - Additional Security screen, 64, 64
 - Applying Security Settings screen, 65, 66
 - Internet Services screen, 63, 64

- Ready To Apply Settings screen, 65
 - Script Map screen, 64, 64
 - Select Server Template screen, 63, 63
 - URLScan screen, 65
 - logs, 474–475, 475
 - version 5 security, 62–70
 - anonymous account, 67, 70
 - IP address and DNS restrictions, 66
 - manual checklist, 62
 - URLScan tool, 67–70
 - version 6 security, 70–71, 71
 - Internet Information Services Manager,
 - for metabase backup, 396
 - Internet Key Exchange (IKE), 136
 - Internet Messaging Access Protocol (IMAP4), 247–248, 251–254
 - testing secured, with Outlook Express, 256–259
 - Internet Protocol Security (IPSec). *See* IPSec (Internet Protocol Security)
 - Internet Security & Acceleration Server
 - logs for packet filters, 477
 - URLScan tool on, 69
 - Internet service providers, 322, 521
 - intraforest trusts, 289
 - IP addresses
 - access to web server, 66
 - for VPN clients, 327
 - IP filter list in IPSec rule, 143–144
 - IP Security Monitor, 147–148, 148
 - IPConfig/all command, 195, 215
 - IPSec (Internet Protocol Security), 52, 133–165, 521
 - authentication configuration and administration, 136–148
 - command-line tools and scripts, 147
 - custom MMC for management, 137–138
 - policy inheritance, 148
 - rule configuration, 141–146, 142
 - testing policy assignments, 147–148
 - tunnel mode vs. transport mode, 139–141
 - benefits, 135
 - certificate deployment and management, 151–153
 - certificate renewal, 153
 - certificate template, 379
 - default policies, restoring, 146
 - for DNS, 62
 - exam essentials, 166
 - L2TP tunnels for, 328
 - phases of process, 135–136
 - protocol configuration and encryption levels, 149–151
 - secure communication between server types, 153–154
 - troubleshooting, 154–158
 - authentication issues, 157
 - certificate configuration, 156–157
 - firewalls and routers, 157
 - logging, 155, 157–158
 - rule configuration, 155
 - for VPN client, 336–337
 - IPSecCMD utility, 147
 - Ipsecmon command, 148
 - IPSecPol tool, 147
 - isolated networks, slipstreaming on, 103
 - ISP. *See* Internet service providers
 - issuing CAs, 360, 522
 - installing and configuring, 372–379
 - prerequisites, 372–373
 - viewing published certificates and CRLs, 378–379
 - IUSR_computername account, 292
 - disabling, 67
 - password, 318
 - IV (initialization vector), 191, 521
-
- K**
- KDC (Key Distribution Center), 276, 522
 - Windows use of, 278
 - KeepAliveTime Registry key, 58
 - Kerberos, 42, 276–277
 - and CIFS, 160
 - interoperability with Unix, 284–286

546 Kerberos delegation – logs

Key Distribution Center (KDC),
73, 318
policy in security templates, 11
for trust relationship authentication,
289
Windows NT authentication mode
and, 47
Kerberos delegation, 435, 522
Kerberos V5, 522
Key Distribution Center (KDC), 276,
318, 522
Windows use of, 278
Key Lifetimes, 150–151
key management server (KMS), 522
KMS (key management server), 522
Ksetup.exe, 285–286

L

L2TP (Layer 2 Tunneling Protocol)
for RRAS, 326
tunnels for IPSec, 328
for VPN client, 336–337, 356
L2TP/IPSec, 522
LAN Manager (LM), 522
disabling, 274–275
in Windows NT 4, 284
hash creation, disabling, 58
LAN protocols for authentication,
273–277
Kerberos, 276–277
NT LAN Manager (NTLM),
273–275
laptop computers, Encrypting File
System (EFS) for, 435
LDAP (Lightweight Directory Access
Protocol), 243, 522
testing secured, 245–246
legacy applications, templates for
workstations running, 42
legacy clients
NTLM (NT LAN Manager) for, 57
software updates, 129
Lightweight Directory Access Protocol
(LDAP), 243, 522
testing secured, 245–246
List Folder Contents permission
(NTFS), 471
LM. *See* LAN Manager (LM)
Local Area Connection Properties dialog
box, General tab, 330
Local Policies, in security templates, 11
Local Security Authority (LSA), 273, 522
Lockdown tool for IIS, 53, 62–66, 108
Additional Security screen, 64, 64
Applying Security Settings screen, 66
Internet Services screen, 63, 64
Ready To Apply Settings screen, 65
Script Map screen, 64, 64
Select Server Template screen, 63, 63
URLScan screen, 65
Log On To Windows dialog box, 277, 277
Logical Certificate Stores view, 423–424
logoff scripts, 5
Logon dialog box, security options,
22–23
Logon Events audit policy, 493
logon events, auditing, 17, 18
logon events, tracking, 464–465
logon process, 277–279. *See also*
authentication
logon scripts, 5
logs, 450, 474–480, 493, 522
auditing
managing distributed, 481–486
for RRAS, 332–333
Event Viewer to display message in,
452–456, 453, 455
firewall log files, 477
IIS logs, 474–475, 475
importance of reading, 494
for IPSec, 155
Network Monitor logs, 477–478
RAS logs, 479–480
retention management, 480–481
for Software Update Services, 114, 115

SQL Server for storing events,
475–476
by URLScan tool, 69
loopback processing mode, 9
LSA (Local Security Authority), 273, 522

M

MAC. *See* Media Access Control (MAC)
address
MAC (message authentication code), 160
MAC filtering, 215, 523
machine certificates, 408, 523. *See also*
client certificates; computer
certificates
Macintosh clients, 75
man-in-the-middle attacks, 54
SMB signing to deter, 160–161
MAPI (Messaging Application
Programming Interface), 247
MBSA tool. *See* Microsoft Baseline
Security Analyzer
mbsacl.exe command-line utility,
98–100
mbsasetup.msi file, 93
MD5 (Message Digest 5), 145, 149, 523
Media Access Control (MAC)
address, 523
filtering for wireless networks,
195–196, 196
message authentication code
(MAC), 160
message digest, 296
Message Digest 5 (MD5), 145, 149, 523
message integrity code (MIC), 145
message types in event logs, 453–454
Messaging Application Programming
Interface (MAPI), 247
metabase, 523. *See also* IIS metabase
MIC (message integrity code), 145
Microsoft
security bulletins, 88
security website, 63
Microsoft Baseline Security Analyzer,
92–101, 128
configuration to scan domain, 96
downloading, 92
and HFNetChk tool, 98–101
individual server report, 97
installation, 93–95
opening screen, 95
results, 97
running, 95–97
for service pack level of multiple
workstations, 88
Microsoft Certificate Services screen, 375
Microsoft Challenge-Handshake
Authentication Protocol
(MS-CHAP), 523
for RRAS, 308
Microsoft Challenge-Handshake
Authentication Protocol version 2
(MS-CHAP v2), 200, 318, 523
for RRAS, 308
Microsoft Directory Synchronization
Services, 74, 75
Microsoft File Migration Utility, 75
Microsoft Graphical Identification and
Authentication (MSGINA), 523
Microsoft Management Console
(MMC)
Certificates snap-in, 156, 235
to enroll and renew certificates,
388–389
to enroll certificates, 430–431
for exporting certificate, 420
for importing certificate, 422
installation, 383
Certification Authority MMC
snap-in, 390, 391
to revoke certificate, 392–393
for IP Security Policy Management
node, 137, 137–138
Security Template snap-in, 9
audit log selections, 18, 19
minimum password setting, 15
Registry node, 25

Microsoft Network Security Hotfix Checker (HFNetChk), 92
 and Microsoft Baseline Security Analyzer, 98–101
 newsgroup for, 100
 Microsoft Operations Manager (MOM), 481, 497
 Microsoft Passport Server, 301
 Microsoft Personal Security Advisor, 92
 Microsoft Software Update Services Setup Wizard, 107, 107
 Microsoft User Authentication Module, 75
 microwave ovens, 215
 MIME (Multipart Internet Mail Extension), Secure, 408–414
 Base64 Encoded X.509 (.cer) format for, 419
 to sign and seal e-mail, 410–413
 mirror image for chain of evidence preservation, 507
 missing event, 452, 523
 Mixed Mode authentication model (SQL Server 2000), 47
 mobile communications, 71–73. *See also* wireless communications
 Modify permission (NTFS), 470
 MOM (Microsoft Operations Manager), 481, 497
 MS-CHAP (Microsoft Challenge-Handshake Authentication Protocol), 523
 for RRAS, 308
 MS-CHAPv2 (Microsoft Challenge-Handshake Authentication Protocol version 2), 200, 318, 523
 for RRAS, 308
 MSGINA (Microsoft Graphical Identification and Authentication), 523
 multifactor authentication, with smart cards and EAP, 310–311
 mutual authentication, 276

N

NAT (Network Address Translation), 524
 natural disasters, 501
 “Negotiating IP Security” message, 173
 nesting security groups, 451
 .NET Passport authentication, 301
 net start policyagent command, 157
 net stop policyagent command, 157
 NETLOGON share point, 16
 Netsh utility, 147
 NetStumbler, 203
 NetWare clients, 74–75
 Network Address Translation (NAT), 340, 524
 virtual private networks (VPNs) and, 339–340
 network analyzers, 164–165
 Network Connection Wizard, 336
 Network File System (NFS), for Unix clients, 74
 network interface cards (NICs), wireless, 182–183
 Network Load Balancing, 114
 Network Monitor, 164, 164, 494
 logs, 477–478, 478
 “Network name is no longer valid” error message, 163
 network type in IPsec rule, 142
 newsgroups, for HFNetChk tool, 100
 NFS (Network File System), for Unix clients, 74
 No Override setting, for Group Policy Objects, 8
 nonrepudiation, 135, 172, 405
 in business communications, 358
 nontrusted domains, authentication configuration, 286–288
 normalization, 68
 NT LAN Manager (NTLM), 273–275, 524
 disabling, 274–275
 in Windows NT 4, 284

- for legacy clients, 57
- troubleshooting, 279
- for trust relationship authentication, 289
- ntconfig.pol file, 16
- NTFS (New Technology File System)
 - partitions, security templates and, 12
 - permissions, 470–471
- NTLM (NT LAN Manager), 524
 - for legacy clients, 57

O

- Oakley log, 155
- object access events
 - auditing, 18
 - tracking, 465–466
- oblt-log.log file, 66
- ODBC (Open Database Connectivity)
 - application, to test SQL server encryption, 242–243
- offline CAs, 405
- offline files, 524
 - encryption, 435
- one-way trust creation, 290
- online CAs, 405
- Open Database dialog box, 32
- operating systems, troubleshooting
 - security templates after upgrade, 35
- outbound filters, for PPTP, 332
- Outlook Express
 - and certificates, 412, 413
 - to send signed e-mail, 413
 - for testing secured e-mail, 256–259
- Outlook Web Access (OWA), 51, 83, 247, 269, 524
 - lockdown, 66
 - securing, 52–53, 259–261
- overlap of wireless zones, 188
- ownership chaining, 48

P

- packet size, largest acceptable without fragmentation, 58
- packet traces, 477, 478
 - between dial-up connection and RAS server, 480
 - running, 478
- PAP (Password Authentication Protocol), 524
 - for RRAS, 307
- parent server, 524
 - for Software Update Services, 114
- partitioned subnet, 53. *See also* DMZ (de-militarized zone)
- partitions, file system for, and security templates, 12
- passport authentication, 300–303, 524
- Password Authentication Protocol (PAP), 524
 - for RRAS, 307
- password policy, in security templates, 11
- passwords, 84
 - attacks on, 134
 - for Certificate Signing Request, 223
 - for Macintosh clients, 85
 - for SA account, 47
 - security for Unix, 73
 - setting minimum, 15
 - for Windows 9x clients, 318
- patches. *See* hotfixes
- PDAs (personal digital assistants),
 - Windows CE configuration as wireless client, 182
- PEAP (Protected Extensible Authentication Protocol), 197, 200, 525
 - with MS-CHAP v2, 524
- perfect forward secrecy (PFS), 146, 151, 173, 525
- performance, SMB signing and, 55, 161
- permissions
 - default security templates and, 42
 - file system, 25

550 personal certificate – properties

- NTFS, 470–471
 - in Remote Access Policies, 343
 - in service pack management, 120
 - user rights, 472–474
 - for Users group, in Windows 2003 vs. NT, 13
- personal certificate, 413, 525
- Personal Information Exchange - PKCS #12 (.pfx), 419, 446, 525
- PFS (perfect forward secrecy), 146, 151, 173, 525
- physical certificate stores, 423, 525
- ping command
 - “Negotiating IP Security” message, 173
 - to test IPsec policy assignments, 137, 147
- PKCS file, 432
- PKI (private key infrastructure), for 802.1x standard, 197
- PKI (public key infrastructure), 358–390, 526. *See also* certificate authorities (CAs)
- Pocket PCs, 182
- Point-to-Point Tunneling Protocol (PPTP), 525
 - for RRAS, 326
 - for VPN client, 336
- .pol files, security template configuration, 16
- policy change events, 18, 468–469
- polymorphic virus, 503
- POP3. *See* Post Office Protocol (POP3)
- pornographic spam, 52
- ports
 - for IPsec, 155, 173
 - port 25, 51, 83
 - port 80, 62
 - for SLL, 220
 - for SSL, 269
 - for VPNs, 328
 - creating and deleting, 326
 - with firewalls, 340
 - for web servers, 269
- Post Office Protocol (POP3), 247–248, 254–256
 - testing secured, with Outlook Express, 256–259
- Potential Scripting Violation message, 411, 411
- Power Users group, 42
- PPTP (Point-to-Point Tunneling Protocol), 525
 - for RRAS, 326
 - for VPN client, 336
- PPTP filtering, 328, 329–332, 356, 525
 - manual configuration, 330–332
- Pre-Shared Key (PSK) mode for WPA, 194
- primary domain controller, NETLOGON share point, 16
- private certificate authorities, 221, 525
- private certificates, 269
- private certificates in SSL, 230–235
 - obtaining
 - using online certificate authority, 234
 - using web interface, 231–233
 - renewing, 235–236
- private key, 219, 525
 - exporting, 446
- private key infrastructure (PKI), for 802.1x standard, 197
- private wireless LAN configuration, 179–181
 - with Windows 2000 Professional client, 181
 - with Windows XP Professional client, 180
- privilege use events, 18, 466–468
- process tracking events, auditing, 18
- process tracking events, tracking, 468
- profile, 525
 - in Remote Access Policies, 343
- properties. *See* computer Properties dialog box; service account Properties dialog box; user Properties dialog box

Protected Extensible Authentication Protocol (PEAP), 197, 200, 525
 public certificate authorities, 221, 409, 525
 public certificates in SSL
 installation, 227–228
 obtaining, 221–230
 renewing, 228–230
 public folders, securing, 53
 public key, 417, 446, 526
 public key cryptography, 219, 526
 public key infrastructure (PKI), 221, 358–390, 526. *See also* certificate authorities (CAs)
 and certificate authorities, 358–390
 public-private key pairs, 358, 409, 417, 526
 public wireless LAN configuration
 for Windows 2000 Professional client, 178
 for Windows XP Professional client, 177–178

Q

QChain, 103, 118–119, 121, 129
 Query Analyzer tool, to test SQL server encryption, 242–243

R

radio interference, 203
 RADIUS (Remote Authentication Dial-In User Service), 526
 for wireless technology, 72
 Read & Execute permission (NTFS), 471
 Read permission (NTFS), 471
 real world scenario
 EventComb, 485
 multiple DNS names, 227
 rebooting
 after service pack installation, 91
 QChain to minimize, 118
 receiving e-mail, 247
 recovery agent, 526
 account for, 418
 in workgroup environment, 436
 refreshing policies, secedit.exe to force, 34
 Registry. *See also*
 HKEY_LOCAL_MACHINE entries in Registry
 displaying, 43
 HKEY_CURRENT_USER entries, 9
 security template configuration, 24–26
 Registry object, in security templates, 12
 Remote Access Account Lockout, 72
 remote access, authentication for, 306–310
 RRAS protocols, 307
 remote access policies, 341–344, 526
 Remote Access server, logs, 479–480
 Remote Authentication Dial-In User Service (RADIUS), 526
 for wireless technology, 72
 remote clients, IPsec and, 154
 Remote Installation Services (RIS)
 settings in GPOs, 5
 slipstreaming with, 101–102
 renewing certificates, 389
 replay, 269, 526
 SSL and, 220
 Request for Comments (RFC), RFC 1510, 284
 Request Security (Optional) Properties dialog box, 146
 resident viruses, 503
 resources, auditing, 459
 restoring backup
 of certificate authority, 397–398
 testing, 498
 Restricted Groups, security template configuration, 12, 26–28
 retention of logs, managing, 480–481
 retinal scanners, 310
 reverse polarity threaded naval connectors (RP-TNCs), 183
 revoking certificates, 392–393

552 RFC 1510 – Secure Sockets Layer (SSL)

- RFC 1510, 526
- RIPrep, 102
- roaming profile, 526
 - and certificates, 424
- rogue APs, 201–202
- root CA, 359, 526
 - CDP (CRL distribution point)
 - creation for, 364–365
 - certificate for intermediate CA from, 369–371
 - configuring publication of CRLs, 364–366
 - installing and configuring, 361–363
 - prerequisites, 361–362
- rootsec template, 14
- routers, configuration issues in IPSec, 157
- Routing and Remote Access Server (RRAS), 324–333, 527
 - authentication, 306–310
 - protocol configuration, 307
 - configuration, 324–327
 - network user connection to, 344
 - troubleshooting, 327–333
 - auditing and event logs, 332–333
 - PPTP filtering, 329–332
- Routing and Remote Access Server Setup Wizard, 325
 - Configuration screen, 325
- RP-TNCs (reverse polarity threaded naval connectors), 183, 527
- RRAS. *See* Routing and Remote Access Server (RRAS)
- RRAS Properties dialog box, Logging tab, 333
- RRAS (Routing and Remote Access Server), 527
- rules for IPSec, 141–146
 - components, 142
- SA (security association), 527
 - account password, 47
- SACL (system access control list), 527
- SAD (Security Account Delegation), 527
- SAM (System Account Manager), 273, 529
- Schlumberger smart card, 424
- screened subnet, 53. *See also* DMZ (de-militarized zone)
- script maps, disabling support on web server, 64
- scripts
 - security template deployment with, 31–33
 - for slipstreaming, 102–103
- Scripts settings in GPOs, 5
- seal, 527
- sealed e-mail, 446
- SeAssignPrimaryTokenPrivilege assigned right name, 469
- SeBackupPrivilege assigned right name, 469
- secdit.exe. *See* Security Configuration and Analysis tool (secdit.exe)
- SeChangeNotifyPrivilege assigned right name, 469
- SeCreatePermanentPrivilege assigned right name, 469
- Secure Communications dialog box, 238, 238
- Secure Hash Algorithm (SHA), 145, 149
- Secure MIME, 408–414, 527
 - Base64 Encoded X.509 (.cer) format for, 419
 - to sign and seal e-mail, 410–413
- Secure Server (Require Security) policy for IPSec, 139
- Secure Sockets Layer (SSL), 218, 219, 527
 - for Basic authentication, 295
 - basics, 219, 219–221
 - for client machine to Active Directory domain controller traffic, 243–246
 - for client machine to e-mail server traffic, 246–248

S

S/MIME (Secure Multipurpose Internet Mail Extension), 527. *See also* Secure MIME

- client security for web server traffic, 236–239
- enforcing on IIS, 237, 238
- exam essentials, 262
- IMAP4 (Internet Messaging Access Protocol), 241–244
- Outlook Web Access (OWA), 259–261
- POP3 (Post Office Protocol), 254–256
- private certificates, 230–235
 - obtaining using online CA, 234–235
 - obtaining using web interface, 231–234
 - renewing, 235–236
- public certificates, 221–230
 - installation, 227–228
 - renewing, 228–230
- SMTP (Simple Mail Transfer Protocol), 249–251
- standard vs. secure web page, 237, 237
- testing secure e-mail with Outlook Express, 256–258
- for Web server to SQL Server traffic, 239–243
 - certificates on SQL Server, 240–241
 - encryption, 241–242
 - testing connection encryption, 242–243
- secure templates, 13
- secured subnet, 53. *See also* DMZ (de-militarized zone)
- securedc template, 13
- securews template, 13
- Security Account Delegation (SAD), 83, 527
 - SQL and, 47–48
- security association (SA), 136, 527
- security breach. *See* attacks
- Security Configuration and Analysis tool (secedit.exe), 527
 - database creation, 32–33
 - security template deployment with, 31–32
- Security dialog box (Exchange), 253
- Security Event Log, 17
- security groups
 - adding new group to, 28
 - nesting, 451
 - in Windows Server 2003, 450–451
- security log, 452, 457
- Security Log Properties dialog box
 - Filter tab, 456, 456
 - General tab, 456, 456
- security options policy, in security templates, 11
- Security Options, security template configuration, 22–23
- Security Parameter Index (SPI)
 - messages, 155
 - receiving bad, 155
- security principal, 528
- Security settings in GPOs, 4
- Security Support Provider Interface (SSPI), 278, 528
- security templates, 3, 9–14, 528
 - configuration, 14–28
 - Account Policies, 14, 14–16
 - audit policies, 16–21
 - event logs, 28, 29
 - .pol files, 16
 - Registry and File System Permissions, 24–26
 - Restricted Groups, 26–28
 - Security Options, 22–23
 - System Services, 23–24
 - User Rights Assignment, 21–22, 22
 - default, 12–13
 - deployment, 29–33, 43
 - with Group Policies, 29–30
 - with scripts, 31–33
 - exam essentials, 36
 - incremental, 13–14
 - objects in, 11–12
 - objects in MMC, 10–12, 11
 - troubleshooting, 33–35
- security, vs. ease of use, 53
- SeDebugPrivilege assigned right name, 469

554 SeIncreaseBasePriorityPrivilege assigned right name – SMB signing

- SeIncreaseBasePriorityPrivilege assigned right name, 469
- Select User, Computer, or Group dialog box, 460
- SeMachineAccountPrivilege assigned right name, 469
- sending e-mail, methods for, 247
- SeRemoteShutdownPrivilege assigned right name, 469
- SeRestorePrivilege assigned right name, 469
- server header, URLScan tool and, 69
- Server Message Blocks (SMBs), 51, 158, 528
- Server (Request Security) policy for IPSec, 138
- servers, preventing impersonation, 54
- service account Properties dialog box, Account tab, 50
- service packs
 - determining current status, 88–89
 - exam essentials, 122
 - installation, 89–92
 - management, 105–119. *See also*
 - Software Update Services (SUS) permissions, 120
 - QChain, 118–119
 - Systems Management Server, 118
 - third-party applications compatibility, 120
 - troubleshooting deployment, 119–121
 - version conflicts, 121
 - slipstreaming, 101–105
 - uninstalling, 128
- service set identifier (SSID), 177, 528
 - for wireless networks, 186–189
 - broadcasting, 215
- Services for NetWare, 75
- SeSecurityPrivilege assigned right name, 469
- SeSystemtimePrivilege assigned right name, 469
- SeTakOwnershipPrivilege assigned right name, 470
- SetShutdownPrivilege assigned right name, 470
- SetTcbPrivilege assigned right name, 469
- setup security template, 13
- Setup Wizard for service pack installation, 90, 90–92
- SHA (Secure Hash Algorithm), 145, 149
- Share level model in SMB, 160
- share point for CDP, 364
- shared folder, redirection as local folder, 5
- shutdown scripts, 5
- sign, 528
- signed e-mail, 414, 446
- Simple Mail Transfer Protocol (SMTP), 154, 247, 249–251, 409
 - dedicated virtual servers, 249–250
 - security, 51–52, 83
 - testing secured, with Outlook Express, 256–259
- single-factor authentication, 310
- single sign-on, 284–285, 528
 - Active Directory for, 279
- site container, Group Policy Objects linked to, 4
- slipstreaming, 101–105, 117, 128, 528
 - with custom scripts, 102–103
 - on isolated networks, 103
 - for new clients and servers, 104–105
 - with Remote Installation Services (RIS), 101–102
- Smart Card Logon certificate template, 379
- Smart Card User certificate template, 379
- smart cards, 309, 405
 - for certificates, 424
 - multifactor authentication with, 310–311
- SMB signing, 54, 84, 158–163, 528
 - architecture, 172
 - CIFS (Common Internet File System), 160
 - commands, 159

- configuration, 160
- enabling, 160–163
- in mixed environment, 172
- SMBs (server message blocks), 51, 158, 528
- SMS (Systems Management Server), 118
- SMTP (Simple Mail Transfer Protocol), 154, 247, 249–251, 409
 - dedicated virtual servers, 249–250
 - security, 51–52, 83
 - testing secured, with Outlook Express, 256–259
- soft Security Association, 136
- Software Installation settings in GPOs, 5
- Software Update Services (SUS), 103, 106–116, 108, 528
 - client installation, 110–113
 - configuration, 109
 - deployment in enterprise, 113–114
 - and disaster recovery, 113
 - exam essentials, 122
 - Monitor Server page, 114, 116
 - server creation, 107–108
 - server requirements, 129
 - Set Options page, 110, 115
 - troubleshooting, 114, 116
 - for update deployment to workstations, 116–117
- spam, pornographic, 52
- Specify Intranet Microsoft Update Service Location Properties dialog box, 111, 112
- SPI (Security Parameter Index) messages, 155
- spoofing MAC addresses, 196
- spyware, 504
- SQL Server
 - and Encrypting File System, 83
 - Secure Sockets Layer (SSL) on, 239–243, 269
 - certificate install, 240–241
 - encryption for specific client, 241–242
 - testing, 242–243
 - for storing log events, 475–476
- SQL Server 2000
 - BulkAdmin role, 50
 - Encrypting File System (EFS), 51
 - security, 47–48
 - Windows security and, 48–50
- SSID (Service Set Identifier), 177, 528
 - for wireless networks, 186–189
 - broadcasting, 215
 - security concerns, 189–190
- SSL. *See* Secure Sockets Layer (SSL)
- SSPI (Security Support Provider Interface), 278, 528
- stand-alone root CA, 405, 446
 - CDP creation for, 364–365
 - installation, 362–363
- Stand-Alone Subordinate CA, 368
- startup settings, for system services, 23–24
- statistics server, 111–112
- stealth virus, 503
- Subordinate Certification Authority
 - certificate template, 379
- Success Audit message type in event log, 453
- SUS. *See* Software Update Services (SUS)
- susetup.msi file, 107
- svcpack.inf file, 104
- symmetric, 529
- symmetric key, for Encrypting File System, 416
- SYN attack, 84
- SynAttackProtect Registry key, 57
- synchronization
 - by Software Update Services, 106
 - of SUS server and Windows Update server, 109
- synchronous processing, of Group Policy Objects, 7
- system access control list (SACL), 527
- System Account Manager (SAM), 273, 529
- system events, 18, 468
- system log, 452
 - IPSec entries, 158
- System Policy Editor, .pol file creation, 16

556 System Properties dialog box – urlscan.ini file

System Properties dialog box, 88–89
 General tab, 88, 89
 System Services, in security templates,
 12, 23–24
 Systems Management Server (SMS), 118
 Network Monitor, 164
 sysvol folder, on domain controllers, 6

T

tarjitting, 508
 TCP/IP stack hardening, 57–58
 TCP/IP troubleshooting
 for RRAS, 329
 for VPN, 338
 TechNet, 279
 templates. *See* certificate templates for
 enterprise CAs; security templates
 Terminal Services Setup window, 374
 TGT (ticket-granting ticket), 276, 529
 third-party applications, compatibility
 with SUS, 120
 thumbprint, 436, 529
 ticket-granting ticket (TGT), 276, 529
 tickets, 42
 TLS (Transport Layer Security) Channel,
 creating, 200
 TLS (Transport Layer Security)
 protocol, 529
 for Exchange 2000, 246
 tokens, multifactor authentication
 with, 310
 transactional file system, 418, 529
 Transport Layer Security (TLS)
 protocol, 529
 for Exchange 2000, 246
 Transport mode, 529
 for IPSec, 139–140
 Trojan Horse, 505, 529
 countermeasure for, 509
 troubleshooting
 authentication, 280
 Encrypting File System (EFS),
 438–439
 IPSec (Internet Protocol Security),
 154–158
 authentication issues, 157
 certificate configuration, 156–157
 firewalls and routers, 157
 rule configuration, 155
 Routing and Remote Access Server
 (RRAS), 327–333
 auditing and event logs, 332–333
 PPTP filtering, 329–332
 security templates, 33–35
 after operating system upgrade, 35
 group policy-applied, 34
 mixed client environments, 35
 service packs deployment,
 119–121
 Software Update Services, 114, 116
 VPN client systems, 338–339
 trust relationships, 288–291, 289, 529
 authentication, 289
 Trusted Root Certification Authorities
 list, Group Policy to configure,
 383–384
 tunnel endpoint, 142
 Tunnel mode, 529
 for IPSec, 140–141, 173
 two-factor authentication, 318

U

UCE (unsolicited commercial e-mail),
 load from, 52
 unbroken ownership chain, 48
 universal groups, 451
 Unix clients, security, 73–74
 Unix, Kerberos interoperability with,
 284–286
 unsolicited commercial e-mail (UCE),
 load from, 52
 update.exe, command-line switches,
 102–103
 URLScan tool, 53, 65, 67–70, 108
 urlscan.ini file, 67, 67, 69
 Options section, 68

user accounts
 configuring for delegation, 48
 manual reset after lockout, 73

user certificate
 requesting, 388, 431
 templates, 380

user logon, scripts for, 5

user Properties dialog box, Account tab, 49

user rights, 471–476

User Rights Assignment, security
 template configuration, 21–22, 22

user rights policy, in security templates, 11

User security model in SMB, 160

users
 configuration settings on, 6
 Group Policy Objects for, 4
 permissions for EFS encrypted files and folders, 435

Users group, Windows 2000 vs. Windows NT, permissions, 13

V

version conflicts, in service pack management, 121

View Options dialog box, for certificates, 423

viewing certificates, 391–392

virtual directory for CDP, 364

Virtual PC 2004, 362

virtual private networks (VPNs), 356, 530. *See also* Routing and Remote Access Server (RRAS)
 authentication protocol
 configuration, 327
 branch office connections with, 324
 client systems
 configuration, 333–337
 Connection Manager Administration Kit, 345–349
 Remote Access Policies, 341–344
 troubleshooting, 338–339

 creating and deleting ports, 326
 exam essentials, 350
 firewall servers with, 340–341
 and Internet service providers, 322–324
 connections, 323
 Network Address Translation (NAT) and, 339–340, 340
 ports, creating and deleting, 326
 RRAS configuration for, 325–326
 for wireless networks protection, 205, 205–206
 combining with 802.1x, 206

Virtual Server, 362

virtual servers, 530
 dedicated SMTP, 249–250
 on Exchange Server, 248

viruses, 502–504, 530
 countermeasure for, 509
 scanning e-mail for, 52
 software protection against, 503

VPN connection Properties dialog box, General tab, 339

VPNs. *See* virtual private networks (VPNs)

W

W3C Extended Log File Format, 477

WAP. *See* wireless access point (WAP)

war chalking, 202–203

war driving, 202, 530

Warning message type in event log, 453, 455

web enrollment, 530

Web Enrollment pages
 for certificate enrollment, 431–432
 for manual certificate enrollment, 387

web folders, 530
 encrypted files in, 435

web interface, to obtain private certificate, 231–233

558 Web server – Windows events

- Web server. *See also* Internet Information Server (IIS)
changes, Lockdown tool and, 66
securing to SQL Server traffic, 239–243
certificates on SQL Server, 240–241
encryption, 241–242
testing connection encryption, 242–243
securing with IPsec, 153–154
- Web Server certificates
and auto-enrollment, 387
template, 380
- Web Service Extensions, 70, 71
- web users
authentication for, 291–306
anonymous, 292–294
basic authentication, 294–295
with client certificate mapping, 303–306
digest authentication, 296–298
integrated Windows authentication, 298–300
passport authentication, 300–303
- WEP (Wired Equivalent Privacy), 531
attacks on, 203
key definition, 72
for wireless networks encryption level, 190–194
basics, 191–192
enabling, 192–194, 193
flaws, 193–194
- Wi-Fi Protected Access (WPA), 194–195, 530–531
- Windows 9x
authentication protocol configuration for mixed environments, 282–283
Certificates Enrollment web pages, 386–387
manual certificate enrollment, 386–389
Web enrollment, 431–432
- Windows 98 workstation
client software updates, 129
security, 493
- Windows 2000, 104
- Windows 2000 Professional client and 802.1x, 207
private wireless LAN configuration with, 181
public wireless LAN configuration for, 178
VPN configuration, 335–336
- Windows 2000 Professional, Group Policies for certificate distribution, 381
- Windows 2003 Server
recovery policy configuration, 436–437
running packet trace, 478
- Windows Authentication Mode, 83
- Windows CE, configuration as wireless client, 182
- Windows clients, refreshing policies, 8
- Windows Components Wizard, 373–375
- Windows events, 462–481
enabling auditing for, 458–463
Event Viewer, 452–456, 455
EventComb to manage distributed audit logs, 481–486, 483
real world scenario, 485
logs, 474–480
firewall log files, 477
IIS logs, 474–475, 475
Network Monitor logs, 477–478
RAS logs, 479–480
retention management, 480–481
types, 464–470
account logon events, 465
account management events, 465
Directory Service access events, 466
logon events, 464–465
object access events, 465–466
policy change events, 468–469
privilege use events, 466–468

- process tracking events, 468
- system events, 468
- Windows Internet Naming Service (WINS), for VPN client IP addresses, 327
- Windows Management Instrumentation (WMI) filters, 9
- Windows .NET Server, IAS (RADIUS) implementation, 201
- Windows NT
 - manual certificate enrollment, 386–389
 - running applications under Windows Server 2003 User context, 13
 - Web enrollment, 431–432
- Windows NT 4
 - authentication mode, 47
 - authentication protocol configuration for mixed environments, 283–284
 - Certificates Enrollment web pages, 386–387
 - domain logon process, 278–279
- Windows NT Challenge/Response authentication, 298
- Windows Only authentication model (SQL Server 2000), 47
- Windows Server 2003
 - Certification Authority, 390
 - Group Policies for certificate distribution, 381
 - Group Policies to remove standard programs from, 4
 - security groups, 450–451
 - nesting, 451
- Windows Update Synchronization Service, 106, 129, 531
- Windows XP Professional
 - client configuration
 - private wireless LAN, 180
 - public wireless LAN, 177–178
 - VPN, 334–335
 - configuration, for third-party Kerberos version 5, 285–286
 - Encrypting File System (EFS)
 - features, 435
 - Group Policies for certificate distribution, 381
- WINS (Windows Internet Naming Service), for VPN client IP addresses, 327
- Wired Equivalent Privacy (WEP), 531
 - for wireless networks encryption level, 190–194
 - basics, 191–192
 - enabling, 192–194, 193
 - flaws, 193–194
- wireless access point (WAP), 72, 176, 182–183, 531
 - moving to DMZ, 204, 204
 - rogue APs, 201–202
 - sample office layout, 187, 188
 - SSIDs as part, 186–189
- wireless communications components, 182–184
 - extending capabilities, real world scenario, 185
- wireless LANs, 531
- Wireless Network Connection Properties dialog box, Wireless Networks tab, 187
- Wireless Network Properties dialog box, 192, 193
 - Authentication tab, 199
- wireless networks, basics, 179
- wireless networks security, 176
 - configuration, 185–201
 - DHCP (Dynamic Host Configuration Protocol), 185–186
 - EAP authentication methods, 200–201
 - encryption levels using 802.1x, 197–199, 198
 - MAC filtering, 195–196, 196, 215
 - SSID (service set identifier), 186–189
 - SSID security concerns, 189–190

560 WMI – zone transfers

- WEP for encryption levels, 190–194
- Wi-Fi Protected Access (WPA), 194–195
- WMI, 204
- exam essentials, 208
- LAN configuration, 176–185
 - private wireless, 179–181
 - public wireless, 177–179
- levels, 207
- problems and attacks, 201–203
 - radio interference, 203
 - rogue APs, 201–202
 - war chalking, 202–203
 - war driving, 202
 - WEP attacks, 203
- VPNs (virtual private networks) for, 205, 205–206
- Windows CE configuration as client, 182
- WMI. *See* Windows Management Instrumentation (WMI) filters
- workgroup members, and Encrypting File System (EFS), 436–437

- workstations
 - with legacy applications, templates for, 42
 - service pack level for multiple, 88
- worms, 505–506, 531
 - countermeasure for, 509
- WPA (Wi-Fi Protected Access), 194–195, 530–531
- Write permission (NTFS), 471
- wuau22.msi file, 110

X

- xcopy command, for EFS files, 438
- XML file, to verify hotfix updates, 92–93

Z

- zone transfers, 62
 - by unauthorized computers, 61