

Index

Symbols

3-leg perimeter template, 72

A

**AAM (Alternate Access Mapping),
configuring, 403-404**

access control, role-based, 435-437

access groups, 435

access rules

enterprise access rules, creating,
167-168

server publishing rules versus, 418-419

accessing log files, 494-495

**Action tab options (configuring web
publishing rules), 388**

Active Directory

autoenrollment of certificates, 258-259

domains. See domain membership

GPOs, installing firewall clients, 307-308

groups

creating for administrative access,
437-438

role-based access control with, 435

ActiveSync. See EAS (Exchange ActiveSync)

Add-ins node (Management Console), 100

application filters, 101-102

web filters, 102

addresses. See **IP addresses**

administration

- administrative access, 437-441
- delegating, 103-105, 164
- documentation, 532-533
- ISA administrators, roles of, 433-434
- lockdown mode, 446-447
- of multiple servers, 448-450
- remote administration, 441
 - enabling RDP access, 444-446
 - installing ISA Server Management Console, 441-444
- renaming servers in Management Console, 448
- role-based access control, 435-437

administrative access

- Active Directory groups, creating for, 437-438
- delegating, 439, 441
- local user accounts, creating for, 438-439

administrator passwords, when to change, 465

advanced logging service, installing, 491

alerts

- customizing, 496-498
- viewing, 87-88

Alternate Access Mapping (AAM), configuring, 403-404

appliances. See **dedicated hardware devices**

application filters, 101-102

Application layer, 137

application security

- for Exchange Outlook Web Access (OWA), 27, 29
- for HTTP traffic, 29
- for RPC traffic, 29-30

Application Settings tab options (configuring web publishing rules), 396

Application Usage Reports, 500

application-layer firewalls, 10-11

- deployment as, 20, 135-138
 - creating firewall policy rules, 151-152
 - creating network rules, 147-148
 - default network templates, 143-144
 - with edge firewall template, 144-146
 - firewall policy rules, 148-150
 - modifying firewall policy rules, 150-151
 - modifying network rules, 147
 - multi-networking support, 139-140
 - network rules, 143
 - networks, ISA concept of, 141-143
 - publishing servers, 152
 - system policy rules, 153-155
- packet-filtering firewalls versus, 137

archiving event logs, 461

arrays, 169

- configuring, 171
- creating, 170-171
- defining policies, 174
- inter-array communication IP address, configuring, 178
- NLB array network, creating, 173

as-built documentation, 519-521

ASIC-based firewalls, 9

ASR (Automated System Recovery) sets, updating, 463-464

assigning

- IP addresses
 - for site-to-site VPN connections, 281
 - for VPN clients network, 229-230
- routing configurations for VPN clients, 232-233

- attachments (HTTP), restricting, 392
- attacks. *See* threats
- audit trail, logging as, 488
- audits, security, 465-466
- Authentication Delegations tab options (configuring web publishing rules), 396
- authentication methods
 - forms-based authentication, Exchange mobile services, 353-354
 - RADIUS environment, integrating ISA Server 2006 with, 24
 - site-to-site VPN deployment scenario, 279, 285
 - IPSec Tunnel Mode configuration, 292-294
 - L2TP configuration, 288-292
 - PPTP configuration, 286-288
 - for VPN clients, 233-234
 - RADIUS, 236-243
 - VPN protocols, 224
- authorization. *See* permissions
- auto-discovery
 - configuring
 - with DHCP, 302-303
 - with DNS, 303-304
 - enabling, 304
 - of proxy settings, 216-218
- autoenrollment of certificates, 258-259
- automated group policy installation of firewall clients, 307-308
- Automated System Recovery (ASR) sets, updating, 463-464
- Automatic Updates client, 453
- automatically configuring client proxy settings, 214-215
- automating export features with custom scripts, 478-483

B

- back firewall template, 72
- back-end servers
 - RPC over HTTP configuration, 363
 - supporting OMA and ActiveSync on, 349-351, 353
- backup and recovery documentation, 534-535
- backup and recovery tools, 469-470
 - components to backup, 470
 - export and import features, 470
 - automating with custom scripts, 478-483
 - exporting ISA settings
 - individual rule sets, 471-472
 - server configuration, 472
 - system policy, 472-473
 - URLsets, 473-475
 - importing ISA settings
 - individual ISA components, 475-476
 - server configuration, 476-477
 - URL sets, 477-478
 - third-party tools, 483-484
- backups, 26
 - validating, 463
 - verifying, 457-458
- bandwidth
 - constraints with VPNs, 224-225
 - content download jobs and, 100
- baseline performance documentation, 517, 536
 - management-level reporting, 536
 - with MOM (Microsoft Operations Manager), 536
 - technical reporting, 537

bi-directional affinity with NLB, 179

Blaster worm, 414-415

blocking. *See* restricting

branch office deployment. *See* site-to-site VPN deployment scenario

Bridging tab options (configuring web publishing rules), 398

C

Cache Array Routing Protocol (CARP), 179, 204

defining cache drives, 180-181

enabling, 182

cache drives, defining, 180-181

Cache node (Management Console), 97

cache rules, 99

content download jobs, enabling and configuring, 100

enabling caching, 98

cache rules, 99

configuring, 207-209

caching. *See also* content caching deployment scenario

enabling, 98

web caching, 21-22

CARP (Cache Array Routing Protocol), 179, 204

defining cache drives, 180-181

enabling, 182

CAs (certificate authorities)

configuring, 251-253

downloading certificates, 255

installing, 250-251

internal CAs, installing, 322-325

local CAs, 401

third-party CAs, 401

advantages, 317-319

installing, 319-321

certificates

Active Directory autoenrollment, 258-259

downloading, 255

exporting to ISA Server, 331-333

importing/exporting, 255-258

requesting

for ISA servers, 253-254

for VPN clients, 254-255

revocation, 107

SSL certificates

importing/exporting to ISA servers, 405-407

installing on SharePoint servers, 404-405

certificates-based encryption, 288

configuring, 289

requesting certificates, 289-290

change management documentation, 535

Change Password feature (OWA), enabling, 338, 340-342

checklists

for administration and maintenance documentation, 533

for migration documentation, 531-532

CHKDSK utility, 462

choosing. *See* selecting

client roles, assigning to ISA server, 53-54

clients, 297

firewall clients

capabilities of, 298

configuring, 308

- editing per-user rules, 309-310
 - installing, 305-308
 - ISA Server 2006 deployment strategy, 23
 - preparation for, 300-304
- IAS clients, configuring ISA servers as, 238-239
- proxy clients, configuring, 212-218
- quarantined VPN clients networks, 71
- redirecting to Exchange virtual directory, 326, 328
- SecureNAT clients, capabilities of, 298-299
- VPN clients, 300
 - authentication methods, 233-234, 236-243
 - automated deployment with CMAK, 259-267
 - certificates, requesting, 254-255
 - defined, 70
 - enabling access, 93-95, 231-232, 281-283
 - firewall rules, creating, 234-236
 - IP addresses, assigning, 229-230
 - network rules, creating, 227-229
 - routing configurations, assigning, 232-233
- Web Proxy clients, capabilities of, 299-300. *See also* content caching
- Windows XP Professional clients, configuring
 - for L2TP VPN connections, 248-249
 - for PPTP VPN connections, 244-245
- CMAK (Connection Manager Administration Kit), 259-260**
 - installing, 260-261
 - packages, customizing for VPN Quarantine, 273-274
 - profiles
 - creating, 261-266
 - installing, 267
- Code Red virus, 382**
- compression**
 - of HTTP traffic, 211-212
 - for VPN protocols, 223
- computer sets, adding Enterprise version servers to, 174-175**
- configuration. *See also* configuring**
 - as-built documentation of, 519-521
 - custom scripts for documenting, 521-530
 - server configuration
 - exporting for backup, 472
 - importing for restores, 476-477
- Configuration Storage Server (CSS)**
 - deployment, 159-163
 - installing, 161-163
- configuring. *See also* configuration**
 - AAM (Alternate Access Mapping), 403-404
 - arrays, 171
 - auto-discovery
 - with DHCP, 302-303
 - with DNS, 303-304
 - cache rules, 207-209
 - certificate authority (CA), 251-253
 - content download jobs, 100, 210-211
 - dashboard, 87
 - dial-up preferences, 106
 - DiffServ settings, 110
 - enterprise networks and policies, 163-168
 - firewall chaining, 105
 - firewall clients, 105, 308

- firewall logging, 492
- firewalls for reverse proxy deployment scenario, 191-192
- flood mitigation settings, 108-109
- HTTP compression, 111, 211-212
- IMAP (Internet Message Access Protocol), 374-376
- inter-array communication IP address, 178
- interfaces for VPN communication, 284-285
- intrusion detection settings, 109
- IP protection, 110
- IPSec pre-shared keys, 247-248
- ISA servers
 - for IAS authentication, 242-243
 - as IAS client, 238-239
- ISA Server 2006. *See also* Management Console
 - to allow MOM communications, 508-509
 - for content caching, 205-206
- MAPI (Message Application Programming Interface), 369
 - filtering rules, 369, 371
- MOM settings, 507
 - for non-domain member ISA servers, 508
- network properties, 41
- networks, troubleshooting, 70
- PKI encryption, 289
- POP3 (Post Office Protocol version 3), 372-374
- proxy clients, 212-218
- RADIUS and LDAP servers, 109-110
- remote access, 95
- reverse proxy
 - for Outlook Web Access, 193, 195
 - for web services, 195
- RPC over HTTP
 - on Exchange back-end servers, 363
 - on Exchange front-end servers, 363-364
 - ISA publishing rules, 365-366
 - Outlook 2003 profiles, 366-368
 - Registry settings, 364
 - RPC virtual directory, 365
- RQS protocol definition, 269-270
- RQS rules, 270-271
- SMTP (Simple Mail Transport Protocol), 376-379
 - custom SMTP filters, 379
 - inbound SMTP filtering, 377
 - outbound SMTP filtering, 377-379
- SSL (Secure Sockets Layer) for OWA (Outlook Web Access)
 - forcing SSL encryption for OWA traffic, 325-326
 - internal CAs (certificate authorities), 322, 324-325
 - overview, 316-317
 - third-party CAs (certificate authorities), 317-321
- SSL-to-SSL bridging, 400-401
- VPN client access, 93-95
- web chaining, 209-210
- Web Proxy logging, 493
- web publishing rules
 - Action tab options, 388
 - Application Settings tab options, 396
 - Authentication Delegations tab options, 396

- Bridging tab options, 398
 - From tab options, 388
 - General tab options, 387
 - Link Translation tab options, 400
 - Listener tab options, 393, 395
 - Paths tab options, 396
 - Public Name tab options, 395
 - Schedule tab options, 399
 - To tab options, 389
 - Traffic tab options, 390-393
 - Users tab options, 398
 - Windows XP Professional clients
 - for L2TP VPN connections, 248-249
 - for PPTP VPN connections, 244-245
 - Connection Manager Administration Kit. See CMAK**
 - connectivity, verifying, 90-91**
 - connectivity verifiers, creating, 499-500**
 - Console. See Management Console**
 - content caching deployment scenario, 12, 21-22, 199-201**
 - Cache Array Routing Protocol (CARP), 204
 - changing default settings, 206
 - configuring
 - cache rules, 207-209
 - ISA Server 2006 for, 205-206
 - proxy clients, 212-218
 - content download jobs, 210-211
 - designing deployment models, 201-203
 - hardware requirements, 203-204
 - HTTP compression, 211-212
 - pre-caching content, 201
 - proxy servers, types of, 203
 - security implications of, 201
 - web chaining, 209-210
 - content download jobs**
 - configuring, 210-211
 - enabling and configuring, 100
 - Content Types toolbox, 85**
 - cost of security breaches, 8-9**
 - CSS (Configuration Storage Server)**
 - deployment, 159-163
 - installing, 161-163
 - custom ISA security template, creating, 52-62**
 - custom RPC protocol definitions, creating, 420-422**
 - custom scripts**
 - automating export features, 478-483
 - for design documentation, 521-530
 - customizing**
 - alerts, 496-498
 - CMAK packages for VPN Quarantine, 273-274
 - log filters, 495-496
 - reports, 501
 - server publishing rules, 428, 430
 - SMTP filters, 379
- ## D
- daily maintenance plans, 456-460**
 - dashboard**
 - configuring, 87
 - monitoring, 456, 496
 - Data Link layer, 136**
 - dedicated hardware devices, 13, 36-37**
 - default cache settings, changing, 206**
 - default network templates, 143-144**

default server publishing rules, 426-427

defining

- array policies, 174
- cache drives, 180-181
- enterprise network rules, 166
- enterprise networks, 165-166

delegating

- administration, 103-105, 164
- administrative access, 439, 441
- monitoring roles, 488-489

deployment

- branch office deployment, 125
 - content caching deployment scenario, 21-22, 199-201
 - Cache Array Routing Protocol (CARP), 204
 - changing default settings, 206
 - configuring cache rules, 207-209
 - configuring ISA Server 2006 for, 205-206
 - configuring proxy clients, 212-218
 - content download jobs, 210-211
 - designing deployment models, 201, 203
 - hardware requirements, 203-204
 - HTTP compression, 211-212
 - pre-caching content, 201
 - proxy servers, types of, 203
 - security implications of, 201
 - web chaining, 209-210
- of CSS (Configuration Storage Server), 159-163
- as firewall, 20, 23, 135-138
- creating firewall policy rules, 151-152
 - creating network rules, 147-148

- default network templates, 143-144
- with edge firewall template, 144-146
- firewall policy rules, 148, 150
- modifying firewall policy rules, 150-151
- modifying network rules, 147
- multi-networking support, 139-140
- network rules, 143
- networks, ISA concept of, 141-143
- publishing servers, 152
- system policy rules, 153-155

- for large organizations, 131-132
- MAPI (Message Application Programming Interface) filtering, 370
- for mid-sized organizations, 129-130
- multiple OWA virtual servers, 354-357
- piloting, 126-127
- prototyping, 125-126
- reverse proxy deployment scenario, 20-21, 185
 - applying network template, 189-190
 - capabilities of, 188
 - configuring existing firewalls for, 191-192
 - in enterprise environments, 196-197
 - for Outlook Web Access, 193, 195
 - preconfigured hardware appliances, 190-191
 - web server publishing rules, 188, 193
 - for web services, 195
 - within security infrastructure, 186-187
- RPC filtering options, 416-417
- site-to-site VPNs, 277
 - authentication methods, 279, 285
 - IPSec Tunnel Mode configuration, 292-294

- L2TP configuration, 288-292
- PPTP configuration, 286-288
- preparation for, 280-285
- reasons for using, 278
- tips for consideration, 280
- for small organizations, 128-129
- for VPNs, 22-23, 225-226
 - domain member, VPN server as, 226
 - workgroup member, VPN server as, 226-227
- deployment project management, 115-117**
- deployment sizing, 124-125**
- design documentation, 117, 518-519**
 - as-built documentation, 519-521
 - custom scripts for, 521-530
- designing**
 - deployment models for content caching
 - deployment scenario, 201-203
 - ISA Server Enterprise version implementation, 159
 - ISA Server implementation, 113-114, 128
 - deployment project management, 115-117
 - documentation of design, 117
 - environment settings, documenting, 114-115
 - ISA Server 2000 versus ISA Server 2006, 118-119
 - for large organizations, 131-132
 - for mid-sized organizations, 129-130
 - security goals/objectives, identifying, 114
 - security goals/objectives, mapping to ISA features, 115-116
 - for small organizations, 128-129
 - validation, 128
- Details pane (Management Console), 67**
- DHCP (Dynamic Host Configuration Protocol)**
 - autodiscovery of proxy settings, 216-217
 - configuring auto-discovery, 302-303
- dial-up networking in CMAK profile creation, 264**
- dial-up preferences, configuring, 106**
- DiffServ settings, configuring, 110**
- directories**
 - OWA directories, 328-329
 - RPC virtual directory, 365
- disabling downlevel client support, 301**
- disaster recovery documentation, 533-534**
 - backup and recovery documentation, 534-535
 - change management documentation, 535
 - formal planning for, 534
 - monitoring and performance documentation, 535
- disk space, checking, 460-461**
- DMZ, reverse proxy deployment scenario, 185**
 - applying network template, 189-190
 - capabilities of, 188
 - configuring existing firewalls for, 191-192
 - in enterprise environments, 196-197
 - for Outlook Web Access, 193-195
 - preconfigured hardware appliances, 190-191
 - web server publishing rules, 188, 193
 - for web services, 195
 - within security infrastructure, 186-187
- DNS (Domain Name Service)**
 - autodiscovery of proxy settings, 217-218
 - configuring auto-discovery, 303-304

documentation

- administration and maintenance documentation, 532-533
- baseline performance documentation, 536-537
- benefits of, 515-517
- design documentation, 117, 518-519
 - as-built documentation, 519-521
 - custom scripts for, 521-530
- disaster recovery documentation, 533-535
- of environment settings, 114-115
- migration documentation, 530
 - checklists for, 531-532
 - numbering migration procedures, 531
 - project plans, creating, 530-531
 - test plans, creating, 531
- security of, 516
- training documentation, 537
- types of, 518
- updating, 464-465

domain membership

- converting ISA servers to, 46-47
- for VPN servers, 226
- workgroup membership versus, 44-45

Domain Name Server (DNS)

- autodiscovery of proxy settings, 217-218
- configuring auto-discovery, 303-304

downlevel client support, enabling/disabling, 301**downloading certificates, 255****Dynamic Host configuration Protocol (DHCP)**

- autodiscovery of proxy settings, 216-217
- configuring auto-discovery, 302-303

E**EAS (Exchange ActiveSync)**

- definition, 347
- enabling, 348
- publishing rules, 358-361
- supporting on back-end mailbox servers, 349-353

edge firewall template, 72

- deployment with, 144-146

email security. See secure mail access**enabling**

- auto-discovery, 304
- caching, 98
- CARP, 182
- Change Password feature (OWA), 338-342
- content download jobs, 100
- downlevel client support, 301
- IMAP (Internet Message Access Protocol), 374
- NLB, 179-180
- POP3 (Post Office Protocol version 3), 372
- PPTP VPN connection support, 243-244
- RDP access, 444-446
- transparent proxies, 213
- VPN client access, 93-95, 231-232, 281-283
- VPN Quarantine, 272-273

Encapsulating Security Payload (ESP), 223**encryption. See also certificates; SSL (Secure Sockets Layer)**

- of HTTP traffic, 383
- PKI, 288
 - configuring, 289
 - requesting certificates, 289-290

- shared key, 288
- of SharePoint sites, 403
- for VPN protocols, 223
- end-to-end SSL bridging. See SSL-to-SSL bridging**
- end-user training documentation, 537**
- enterprise access rules, creating, 167-168**
- enterprise certificate authority. See CAs (certificate authorities)**
- enterprise environments, reverse proxy deployment scenario in, 196-197**
- enterprise network rules, defining, 166**
- enterprise networks, defining, 165-166**
- enterprise policies**
 - changing order of, 168
 - creating, 166-167
- Enterprise version of ISA Server 2006, 19-20**
 - adding to Managed ISA Server computer set, 174-175
 - arrays, 169
 - configuring, 171
 - creating, 170-171
 - defining policies, 174
 - NLB array network, creating, 173
 - bi-directional affinity with NLB, 179
 - configuring inter-array communication IP address, 178
 - CSS deployment, 159-163
 - defining cache drives, 180-181
 - designing implementation of, 159
 - enabling CARP, 182
 - enabling NLB, 179-180
 - installing, 175, 177
 - pre-configuring networks and policies, 163-168
 - prerequisites for, 174
 - Standard version versus, 124-125, 158
- environment settings, documenting, 114-115**
- ESP (Encapsulating Security Payload), 223**
- event logs, archiving, 461**
- Event Viewer, monitoring, 458-460**
- Exadmin directory (OWA), 328**
- Exchange directory (OWA), 328**
- Exchange mobile services. See also EAS (Exchange ActiveSync); OWA (Outlook Web Access)**
 - definition, 353
 - forms-based authentication, 353-354
 - IMAP (Internet Message Access Protocol), 374-376
 - enabling, 374
 - filtering rules, 375-376
 - SSL (Secure Sockets Layer), 375
 - MAPI (Message Application Programming Interface), 369
 - filtering rules, 369-371
 - POP3 (Post Office Protocol version 3), 372-374
 - enabling, 372
 - filtering rules, 374
 - SSL support, 372-374
 - publishing rules, creating, 358-361
- RPC over HTTP**
 - configuring on Exchange back-end servers, 363
 - configuring on Exchange front-end servers, 363-364
 - definition, 347
 - installing, 362
 - ISA publishing rules, 365-366
 - Outlook 2003 profiles, 366-368

Registry settings, 364

RPC virtual directory, 365

SMTP (Simple Mail Transport Protocol),
376-379

custom SMTP filters, 379

inbound SMTP filtering, 377

outbound SMTP filtering, 377-379

supporting on back-end mailbox servers,
349-353

**Exchange System Manager, enabling OMA
(Outlook Web Access) and ActiveSync, 348**

ExchDAV directory (OWA), 329

ExchWeb directory (OWA), 328

**existing security solutions, adapting ISA
Server 2006 to, 14, 23-25**

exploits. See threats

export features, 470

automating with custom scripts, 478-483

components to backup, 470

exporting ISA settings

individual rule sets, 471-472

server configuration, 472

system policy, 472-473

URL sets, 473-475

Export Wizard, 122-124

exporting

certificates, 255-258

OWA certificates to ISA Server, 331-333

prototype configuration settings, 126

server configuration with WinMSD, 519

SSL certificates to ISA servers, 405-407

**extensions of HTTP attachments,
restricting, 392**

external networks, 70

F

file system integrity, checking, 462

filtering RPC traffic, blocking versus, 415

filters

application filters, 101-102

HTTP filters, Properties dialog box
options, 381

Action tab, 388

Application Settings tab, 396

Authentication Delegations tab, 396

Bridging tab, 398

From tab, 388

General tab, 387

Link Translation tab, 400

Listener tab, 393, 395

Paths tab, 396

Public Name tab, 395

Schedule tab, 399

To tab, 389

Traffic tab, 390-393

Users tab, 398

IMAP (Internet Message Access Protocol),
375-376

log filters, customizing, 495-496

MAPI (Message Application Programming
Interface), 369-371

POP3 (Post Office Protocol
version 3), 374

RPC filtering, 415-416

deployment options for, 416-417

SMTP filtering, 377, 379

web filters, 102

financial benefits of documentation, 517

firewall administrators, 434**firewall chaining, configuring, 105****firewall clients**

- capabilities of, 298
- configuring, 105, 308
- editing per-user rules, 309-310
- installing, 305
 - automated group policy installation, 307-308
 - manual installation, 306
 - unattended installation, 306-307
- ISA Server 2006 deployment strategy, 23
- preparation for, 300-304

firewall logging, configuring, 492**Firewall Policy node (Management Console), 79-80**

- firewall access rules, 80-81
- Firewall Policy toolbox, 84-86
- server publishing rules, 82
- system policy rules, 82

firewall policy rules, 80-81, 148-150

- creating, 151-152
 - for VPN clients network, 234-236
- modifying, 150-151

Firewall Policy toolbox, 84-86**firewalls**

- application-layer filtering, 10-11
 - ISA Server 2006 deployment strategy, 20
- configuring for reverse proxy deployment scenario, 191-192
- deployment as, 135-138
 - creating firewall policy rules, 151-152
 - creating network rules, 147-148

- default network templates, 143-144
- with edge firewall template, 144-146

- firewall policy rules, 148-150
- modifying firewall policy rules, 150-151

- modifying network rules, 147
- multi-networking support, 139-140
- network rules, 143

- networks, ISA concept of, 141-143
- publishing servers, 152
- system policy rules, 153-155

explained, 136

- integrating ISA Server 2006 with, 23-24
- need for, 9

flood mitigation settings, 108-109**forcing SSL encryption for OWA traffic, 325-326****forms-based authentication (Exchange mobile services), 353-354****forward proxies**

- automatically configuring client settings, 214-215
- described, 203
- manually configuring client settings, 213-214

From tab options (configuring web publishing rules), 388**front firewall template, 72****front-end servers, RPC over HTTP configuration, 363-364**

G

General node (Management Console), 103

- certificate revocation, 107
- delegating administration, 103-105
- dial-up preferences, configuring, 106
- DiffServ settings, 110
- firewall chaining, 105
- firewall clients, configuring, 105
- flood mitigation settings, 108-109
- HTTP Compression settings, 111
- intrusion detection settings, 109
- IP protection, configuring, 110
- link translation, 106
- RADIUS and LDAP servers, configuring, 109-110
- server details, viewing, 108

General tab options (configuring web publishing rules), 387

generating reports, 501-503

goals. See security goals/objectives

GPMC (Group Policy Management Console) tool, 214, 258, 307

GPOs (Group Policy Objects)

- configuring proxy client settings, 214-215
- installing firewall clients, 307-308

groups (Active Directory)

- creating for administrative access, 437-438
- role-based access control with, 435

H

hardware

- dedicated hardware devices, 13, 36-37
- optimization of, 37-38
- preconfigured appliances, deploying, 190-191

hardware requirements

- for content caching servers, 203-204
- for ISA Server 2006, 34-35

hardware verification, 461

headers (HTTP), restricting, 392

hiding Task pane (Management Console), 67

history of ISA Server 2006, 15-17

hosts file, 195

HTTP (Hypertext Transfer Protocol), 316, 381

- attachments, restricting, 392
- compression, configuring, 111, 211-212
- filter settings for OWA publishing rules, 338
- filters, configuring (Properties dialog box), 381
 - Action tab options, 388
 - Application Settings tab options, 396
 - Authentication Delegations tab options, 396
 - Bridging tab options, 398
 - From tab options, 388
 - General tab options, 387
 - Link Translation tab options, 400
 - Listener tab options, 393-395
 - Paths tab options, 396
 - Public Name tab options, 395

- Schedule tab options, 399
- To tab options, 389
- Traffic tab options, 390-393
- Users tab options, 398
- headers, restricting, 392
- methods, restricting, 391-392
- signatures, restricting, 392-393
- traffic
 - application security for, 29
 - Code Red virus, 382
 - encrypting, 383
 - inherent threat in, 382
 - SSL-to-SSL bridging, configuring, 400-401
 - web publishing rules, 383-387

Hypertext Transport Protocol. See HTTP

I

IAS (Internet Authentication Service)

- configuring ISA server for, 242-243
 - as client, 238-239
- creating Remote Access Policies, 239-241
- installing, 236-237
- permissions for, 237-238

IIS (Internet Information Services), installing, 250-251

IMAP (Internet Message Access Protocol), 374-376

- enabling, 374
- filtering rules, 375-376
- SSL (Secure Sockets Layer), 375

implementation of VPN

- preparation for, 225
- protocols for, 224

import features, 470

- importing ISA settings
 - individual ISA components, 475-476
 - server configuration, 476-477
 - URL sets, 477-478

importing

- certificates, 255-258
- ISA Server 2006 management pack, 506-507
- OWA certificates to ISA Server, 331-333
- SSL certificates to ISA servers, 405-407

in-place upgrades, 122

inbound SMTP filtering, 377

individual access (ISA Server 2006 deployment strategy), 23

infrastructure design. See deployment

installing

- advanced logging service, 491
- CAs (certificate authorities), 250-251
 - internal CAs, 322-325
 - third-party CAs, 319-321
- CMAK (Connection Manager Administration Kit), 260-261
- CMAK profiles, 267
- CSS (Configuration Storage Server), 161-163
- firewall clients, 305
 - automated group policy installation, 307-308
 - manual installation, 306
 - unattended installation, 306-307
- IAS (Internet Authentication Service), 236-237

- IIS (Internet Information Services), 250-251
- ISA Server 2006, 47
 - Enterprise version, 175-177
 - management pack, 505
 - software component prerequisites, 47
 - Standard edition install, 47-50
- ISA Server Management Console, 441-444
- MOM agent, 509-510
- Network Monitor, 423-424
- RPC over HTTP, 362
- RQS (Remote Access Quarantine Service), 268-269
- Security Configuration Wizard, 51
- SSL certificates on SharePoint servers, 404-405
- third-party add-ons, 50
- Windows Server 2003 Service Pack 1, 41-42
- Windows Server 2003 Standard edition, 38-40
- inter-array communication IP address, configuring, 178**
- interfaces, configuring for VPN communication, 284-285**
- internal CAs (certificate authorities), installing**
 - on domain controllers, 322-324
 - on OWA Server, 324-325
- internal networks, 70**
- Internet, goals of, 382**
- Internet Authentication Service (IAS)**
 - configuring ISA server for, 242-243
 - as client, 238-239
 - creating Remote Access Policies, 239-241
 - installing, 236-237
 - permissions for, 237-238
- Internet Information Services (IIS), installing, 250-251**
- Internet Message Access Protocol. See IMAP**
- Internet Protocol Security. See IPsec**
- Internet Security and Acceleration Server. See ISA Server**
- intrusion attempts, monitoring, 488**
- intrusion detection**
 - in DMZ, 197
 - settings, 109
- IP addresses**
 - adding
 - to ISA Server, 357
 - to OWA servers, 355
 - assigning
 - for site-to-site VPN connections, 281
 - for VPN clients network, 229-230
- IP protection, configuring, 110**
- IPsec, 223**
 - pre-shared keys, configuring, 247-248
- IPsec Tunnel Mode, 279**
 - configuring for site-to-site VPN, 292-294
- ISA administrators, roles of, 433-434**
- ISA clients. See clients**
- ISA Management Console. See Management Console**
- ISA Server (Internet Security and Acceleration Server), 7. See also ISA Server 2000; ISA Server 2004; ISA Server 2006**
 - dedicated hardware devices, 36-37
 - hardware optimization, 37-38

ISA Server 2000

- history of ISA Server 2006, 16
- ISA Server 2006 versus, 118-119
- migrating to ISA Server 2006, 119-122

ISA Server 2004

- history of ISA Server 2006, 16
- ISA Server 2000 versus, 118-119
- migrating to ISA Server 2006, 122-124

ISA Server 2006

- administration
 - delegating, 164
 - of multiple servers, 448-450
- administrative access
 - creating Active Directory groups for, 437-438
 - creating local user accounts for, 438-439
 - delegating, 439-441
- application security. *See* application security
- backup and recovery tools. *See* backup and recovery tools
- branch office deployment, 125
- configuring for content caching, 205-206
- deployment. *See* deployment
- designing implementation of, 113-114, 128
 - deployment project management, 115-117
 - documentation of design, 117
 - environment settings, documenting, 114-115
 - ISA Server 2000 versus ISA Server 2006, 118-119
 - for large organizations, 131-132
 - for mid-sized organizations, 129-130

- security goals/objectives, identifying, 114
- security goals/objectives, mapping to ISA features, 115-116
- for small organizations, 128-129
- validation, 128

Enterprise version

- adding to Managed ISA Server computer set, 174-175
- arrays, usage of, 169-174
- bi-directional affinity with NLB, 179
- configuring inter-array communication IP address, 178
- CSS deployment, 159-163
- defining cache drives, 180-181
- designing implementation of, 159
- enabling CARP, 182
- enabling NLB, 179-180
- installing, 175-177
- pre-configuring networks and policies, 163-168
- prerequisites for, 174
- Standard version versus, 19-20, 124-125, 158
- firewall deployment, 135-138
 - creating firewall policy rules, 151-152
 - creating network rules, 147-148
 - default network templates, 143-144
 - with edge firewall template, 144-146
 - firewall policy rules, 148-150
 - modifying firewall policy rules, 150-151
 - modifying network rules, 147
 - multi-networking support, 139-140
 - networks, ISA concept of, 141-143
 - network rules, 143

- publishing servers, 152
- system policy rules, 153-155
- history of, 15-17
- installing, 47
 - software component prerequisites, 47
 - Standard edition install, 47-50
- ISA Server 2000 versus, 118-119
- licensing, 34, 204
- lockdown mode, 446-447
- maintenance plans
 - daily maintenance, 456-460
 - importance of, 451-452
 - monthly maintenance, 462-465
 - operating system patches, 453-456
 - quarterly maintenance, 465-467
 - weekly maintenance, 460-461
- management tools. *See* management tools
- migrating ISA Server 2000 to, 119-122
- migrating ISA Server 2004 to, 122-124
- misperceptions about, 137-138
- new features, 17-18
- operating system for, selecting, 19
- prerequisites, 33-36
- reasons for usage, 8
 - adapting to existing security solutions, 14, 23-25
 - application-layer filtering, 10-11
 - dedicated hardware devices, 13
 - firewalls, need for, 9
 - reduced management overhead, 13-14
 - security breaches, high cost of, 8-9
 - as VPN (Virtual Private Network), 11
 - web caching, 12

- remote administration, 441
 - enabling RDP access, 444-446
 - installing ISA Server Management Console, 441-444
- renaming in Management Console, 448
- role-based access control, 435
 - with Active Directory groups, 435
 - example of, 436-437
- third-party add-ons, installing, 50
- updating, 50

ISA Server 2006 management pack

- importing, 506-507
- installing, 505

ISA Server Auditor role, 434, 488**ISA Server dashboard. *See* dashboard****ISA Server Full Administrator role, 434****ISA Server Management Console. *See* Management Console****ISA Server Monitoring Auditor role, 434, 488****ISA servers**

- certificates, requesting, 253-254
- configuring
 - for IAS authentication, 242-243
 - as IAS client, 238-239
- importing/exporting SSL certificates, 405-407
- manual patches, 453-454

J—K—L**knowledge management, documentation for, 516-517****L2TP (Layer 2 Tunneling Protocol), 222-223, 279**

- authentication methods, 224
- compression methods, 223

- configuring
 - for site-to-site VPN, 288-292
 - Windows XP Professional clients for, 248-249
- creating VPN connections, 246-247
- encryption methods, 223
- implementation issues, 224
- IPSec pre-shared keys, configuring, 247-248
- PKI (Public Key Infrastructure), creating, 249-259
- large organizations, ISA Server 2006 deployment for, 131-132**
- launching Management Console, 66**
- Layer 2 Tunneling Protocol. See L2TP (Layer 2 Tunneling Protocol)**
- LDAP servers, configuring, 109-110**
- legal issues, high cost of security breaches, 9**
- licensing for ISA Server 2006, 34, 204**
- link translation, 106**
- Link Translation tab options (configuring web publishing rules), 400**
- lisadmpwd directory (OWA), 328**
- Listener tab options (configuring web publishing rules), 393-395**
- listeners, 402**
- load balancing with ISA security appliances, 196. See also arrays; NLB (Network Load Balancing)**
- local certificate authorities (CAs), 401**
- local host networks, 70**
- local user accounts, creating for administrative access, 438-439**
- lockdown mode, 446-447**
- logging. See also monitoring**
 - Event Viewer logs, monitoring, 458-460
 - firewall logging, configuring, 492
 - formats for storage, 490-491
 - importance of, 487-488
 - installing advanced logging service, 491
 - in Monitoring node (Management Console), 91
 - tools for, 26-27
 - troubleshooting with, 493
 - accessing log files, 494-495
 - customizing log filters, 495-496
 - types of, 489
 - Web Proxy logging, configuring, 493

M

- maintenance documentation, 532-533**
- maintenance plans, 26**
 - daily maintenance, 456-460
 - importance of, 451-452
 - monthly maintenance, 462-465
 - operating system patches, 453-456
 - quarterly maintenance, 465, 467
 - weekly maintenance, 460-461
- Managed ISA Server computer set, adding Enterprise version servers to, 174-175**
- Management Console, 25-26, 65-66**
 - Details pane, 67
 - installing, 441-444
 - launching, 66
 - nodes
 - Add-ins, 100-102
 - Cache, 97-100
 - Firewall Policy, 79-86
 - General, 103-111
 - list of, 67

- Monitoring, 86-91
- Network, 68-79
- VPN, 91-97
- renaming servers in, 448
- Scope pane, 67
- Task pane, 67
- management tools. See also Management Console**
 - backups and restores, 26
 - ISA Server 2006 management pack, 505-507
 - logging and monitoring, 26-27
 - maintenance procedures, 26
 - reduced overhead with, 13-14
- management-level reporting, 536**
- manual patches for ISA servers, 453-454**
- manually configuring client proxy settings, 213-214**
- manually installing firewall clients, 306**
- MAPI (Message Application Programming Interface) filtering rules, 369-371**
- mean time between failures (MTBF), 461**
- mean time to repair (MTTR), 461**
- Message Authentication (RADIUS), 241**
- messaging administrators, 434**
- messaging security**
 - EAS (Exchange ActiveSync)
 - definition, 347
 - enabling, 348
 - publishing rules, 358-361
 - supporting on back-end mailbox servers, 349-353
 - IMAP (Internet Message Access Protocol), 374-376
 - enabling, 374
 - filtering rules, 375-376
 - SSL (Secure Sockets Layer), 375
 - importance of, 346
 - ISA Server 2006 messaging security mechanisms, 346-347
 - MAPI (Message Application Programming Interface) filtering rules, 369-371
 - overview, 345
 - OWA (Outlook Web Access). See OWA
 - POP3 (Post Office Protocol version 3), 372-374
 - RPC over HTTP
 - configuring on Exchange back-end servers, 363
 - configuring on Exchange front-end servers, 363-364
 - definition, 347
 - installing, 362
 - ISA publishing rules, 365-366
 - Outlook 2003 profiles, 366-368
 - Registry settings, 364
 - RPC virtual directory, 365
 - SMTP (Simple Mail Transport Protocol), 376-379
- methods (HTTP), restricting, 391-392**
- Microsoft Management Console (MMC) sessions, setting up, 255-256**
- Microsoft Operations Manager (MOM), 503-505, 536**
 - configuring
 - ISA to allow communications, 508-509
 - settings, 507-508
 - importing ISA Server 2006 management pack, 506-507
 - installing
 - ISA Server 2006 management pack, 505
 - MOM agent, 509-510
 - monitoring performance data, 510

Microsoft Point-to-Point Compression (MPPC), 223

Microsoft Point-to-Point Encryption (MPPE), 223

Microsoft Update, 50, 453-455

allowing access to, 454-455

Windows Update versus, 43

mid-sized organizations, ISA Server 2006 deployment for, 129-130

migrating

ISA Server 2000 to ISA Server 2006, 119-122

ISA Server 2004 to ISA Server 2006, 122-124

migration documentation, 530

checklists for, 531-532

numbering migration procedures, 531

project plans, creating, 530-531

test plans, creating, 531

MMC (Microsoft Management Console) sessions, setting up, 255-256

mobile services (Exchange). See Exchange mobile services

modifying

firewall policy rules, 150-151

network rules, 147

web publishing rules for SSL-to-SSL bridging, 401

MOM (Microsoft Operations Manager), 503-505, 536

configuring

ISA to allow communications, 508-509

settings, 507-508

importing ISA Server 2006 management pack, 506-507

installing

ISA Server 2006 management pack, 505

MOM agent, 509-510

monitoring performance data, 510

monitoring. See also logging; reports; troubleshooting

with alerts, 496-498

with connectivity verifiers, 499-500

with dashboard, 496

delegating role of, 488-489

in DMZ, 197

documentation for, 535

Event Viewer, 458-460

importance of, 487-488

ISA Server dashboard, 456

with MOM (Microsoft Operations Manager). See MOM (Microsoft Operations Manager)

performance, 466

sessions and services, 88, 498-499

tools for, 26-27

with Windows Performance Monitor, 511

Monitoring node (Management Console), 86-87

connectivity, verifying, 90-91

dashboard, configuring, 87

logging information, 91

monitoring sessions and services, 88

reports, generating, 88, 90

viewing alerts, 87-88

monthly maintenance plans, 462-465

MPPC (Microsoft Point-to-Point Compression), 223

MPPE (Microsoft Point-to-Point Encryption), 223
MTBF (mean time between failures), 461
MTRR (mean time to repair), 461
multi-networking support, 139-140
multiple servers, administration of, 448-450

N

NAT (Network Address Translation) network relationships, 73, 143
network administrators, 434
network bandwidth constraints with VPNs, 224-225
network configurations. See deployment
Network layer, 137
Network Load Balancing. See NLB
Network Monitor
 identifying RPC UUIDs with, 422-426
 installing, 423-424
Network node (Management Console), 68
 network rules, 73-74
 network sets, 71
 Network Template Wizard, 74-78
 network templates, defining, 72-73
 networks versus subnets, 69-71
 web chaining, 79
Network Objects toolbox, 85
network prerequisites for ISA Server 2006, 36
network properties, configuring, 41

network rules, 73-74, 143
 creating, 147-148
 for VPN clients network, 227-229
 enterprise network rules, defining, 166
 modifying, 147
network segments, securing RPC traffic between, 415
 ISA deployment options, 416-417
 with RPC filtering, 415-416
network sets, 71
Network Template Wizard, 74-78
network templates
 default templates, 143-144
 defining, 72-73
 single network adapter template, applying to unihomed ISA Server, 189-190
networks
 configuring, troubleshooting, 70
 enterprise networks
 defining, 165-166
 pre-configuring, 163-168
 ISA concept of, 141-143
 network rules, 73-74
 network sets, 71
 Network Template Wizard, 74-78
 network templates, defining, 72-73
 perimeter networks, setting up, 139-140
 subnets versus, 69-71
 types of, 70-71
 web chaining, 79
new features of ISA Server 2006, 17-18
NLB (Network Load Balancing), 178
 bi-directional affinity with, 179
 enabling, 179-180
 with ISA security appliances, 196

NLB array network, creating, 173

nodes (Management Console)

- Add-ins, 100
 - application filters, 101-102
 - web filters, 102
- Cache, 97
 - cache rules, 99
 - content download jobs, enabling and configuring, 100
 - enabling caching, 98
- Firewall Policy, 79-80
 - firewall access rules, 80-81
 - Firewall Policy toolbox, 84-86
 - server publishing rules, 82
 - system policy rules, 82

General, 103

- certificate revocation, 107
- delegating administration, 103-105
- dial-up preferences, configuring, 106
- DiffServ settings, 110
- firewall chaining, 105
- firewall clients, configuring, 105
- flood mitigation settings, 108-109
- HTTP Compression settings, 111
- intrusion detection settings, 109
- IP protection, configuring, 110
- link translation, 106
- RADIUS and LDAP servers, configuring, 109-110
- server details, viewing, 108

list of, 67

Monitoring, 86-87

- connectivity, verifying, 90-91
- dashboard, configuring, 87

- logging information, 91
- monitoring sessions and services, 88
- reports, generating, 88-90
- viewing alerts, 87-88

Network, 68

- network rules, 73-74
- network sets, 71
- Network Template Wizard, 74-78
- network templates, defining, 72-73
- networks versus subnets, 69-71
- web chaining, 79

VPN, 91

- client access, enabling and configuring, 93-95
- remote access, configuring, 95
- remote site networks, creating, 96
- VPN quarantine, 96-97

NTBackup, 483-484

numbering migration procedures, 531

O

objectives. See security goals/objectives

Open System Interconnection (OSI) Reference model, layers in, 136-137

operating systems

- for ISA Server 2006, selecting, 19
- patching, 42-44, 453-456
- prerequisites for ISA Server 2006, 35
- Windows Server 2003 Standard edition, installing, 38-40

OpsMgr (Operations Manager). See MOM (Microsoft Operations Manager)

optimization of server hardware, 37-38

OSI (Open System Interconnection) Reference model, layers in, 136-137

outbound SMTP filtering, 377-379

Outlook Anywhere. See RPC over HTTP

Outlook profiles, RPC over HTTP support, 366-368

OWA (Outlook Web Access)

- application security for, 27-29
- configuring reverse proxy for, 193-195
- definition, 316, 347
- enabling, 348
- publishing rules
 - creating, 334-338, 358-361
 - enabling change password feature with, 338-342
 - HTTP filter settings, 338
- redirecting clients to Exchange virtual directory, 326-328
- securing with ISA Server 2006
 - exporting/importing OWA certificates, 331-333
 - overview, 329-331
 - OWA publishing rules, 334-342
- SSL (Secure Sockets Layer)
 - forcing SSL encryption for OWA traffic, 325-326
 - HTTP (Hypertext Transfer Protocol), 316
 - internal CAs (certificate authorities), 322-325
 - overview, 316-317
 - third-party CAs (certificate authorities), 317-321
- supporting on back-end mailbox servers, 349-353

virtual servers

- adding IP addresses to, 355
- assigning SSL certificates to, 357
- creating, 355-357
- deploying multiple, 354-357
- settings, 328-329

P

packet-filtering firewalls, 9

- application-filtering firewalls versus, 137

passwords, when to change, 465

patches, checking for, 460

patching

- ISA Server 2006, 50
- operating systems, 42-44, 453-456

Paths tab options (configuring web publishing rules), 396

per-user rules for firewall clients, editing, 309-310

perfmon (Windows Performance Monitor) utility, 511

performance data, monitoring, 466

- with MOM, 510
- with Windows Performance Monitor, 511

performance documentation, 535-536

perimeter networks, setting up, 139-140

permissions for IAS (Internet Authentication Service), 237-238

persistent routes, adding to route tables, 142

Physical layer, 136

piloting ISA Server 2006 deployment, 126-127

PKI (Public Key Infrastructure), 288

- configuring, 289
- creating for L2TP VPN connections, 249-259
- requesting certificates, 289-290
- for SSL-to-SSL bridging, 400-401

Point-to-Point Protocol (PPP), 222**Point-to-Point Tunneling Protocol (PPTP), 222-223, 279**

- authentication methods, 224
- compression methods, 223
- configuring
 - for site-to-site VPN, 286-288
 - Windows XP Professional clients for, 244-245
- enabling VPN support for, 243-244
- encryption methods, 223
- testing VPN connections, 245-246

policies

- array policies, defining, 174
- enterprise policies
 - changing order of, 168
 - creating, 166-167
 - pre-configuring, 163-168

POP3 (Post Office Protocol version 3), 372-374

- enabling, 372
- filtering rules, 374
- SSL support, 372-374

PPP (Point-to-Point Protocol), 222**PPTP (Point-to-Point Tunneling Protocol), 222-223, 279**

- authentication methods, 224
- compression methods, 223

configuring

- for site-to-site VPN, 286-288
- Windows XP Professional clients for, 244-245

- enabling VPN support for, 243-244
- encryption methods, 223
- testing VPN connections, 245-246

pre-caching content, 201**pre-shared keys (IPSec), configuring, 247-248****preconfigured hardware appliances, deploying, 190-191****preparing**

- for firewall clients, 300-304
- for site-to-site VPN deployment scenario, 280-285
- for VPN implementation, 225

prerequisites for ISA Server 2006, 33

- for Enterprise version, 174
- hardware prerequisites, 34-35
 - for content caching servers, 203-204
- network prerequisites, 36
- operating system prerequisites, 35
- service packs, described, 35-36
- software component prerequisites, 47

Presentation layer, 137**proactive maintenance, importance of, 452****procedural documentation, 533****profiles**

- CMAK profiles
 - creating, 261-266
 - installing, 267
- Outlook profiles, RPC over HTTP support, 366-368

project plans, creating, 530-531

Properties dialog box (web publishing rules)

- Action tab options, 388
- Application Settings tab options, 396
- Authentication Delegations tab options, 396
- Bridging tab options, 398
- From tab options, 388
- General tab options, 387
- Link Translation tab options, 400
- Listener tab options, 393-395
- Paths tab options, 396
- Public Name tab options, 395
- Schedule tab options, 399
- To tab options, 389
- Traffic tab options, 390-393
- Users tab options, 398

protocols. *See names of specific protocols (HTTP, IMAP, etc.)*

Protocols toolbox, 84

prototyping

- ISA Server 2006 deployment, 125-126
- ISA server patches, 456

proxy clients, configuring, 212-218

Proxy Server, 15-16

proxy servers. *See also content caching deployment scenario*

- described, 186
- types of, 203

Public directory (OWA), 329

Public Key Infrastructure. *See PKI*

Public Name tab options (configuring web publishing rules), 395

publishing

- RPC services, 419-420
- servers, firewall deployment and, 152

publishing rules, 82

- access rules versus, 418-419
- creating, 358-361, 427-428
- customizing, 428-430
- default server publishing rules, 426-427
- IMAP (Internet Message Access Protocol), 374-376
- OWA (Outlook Web Access)
 - creating, 334-338
 - enabling change password feature with, 338-342
 - HTTP filter settings, 338
- POP3 (Post Office Protocol version 3), 372-374
- RPC over HTTPS servers, 365-366
- for RPC services, 419-420
 - creating custom PRC protocol definitions, 420-422
- SharePoint publishing rules, creating, 407-411
- web publishing rules. *See web publishing rules*

Q

Quarantine feature (VPN), 96-97, 267-268

- configuring
 - RQS protocol definition, 269-270
 - RQS rules, 270-271
- customizing CMAK packages for, 273-274
- enabling, 272-273
- installing RQS (Remote Access Quarantine Service), 268-269

quarantined VPN clients networks, 71

quarterly maintenance plans, 465-467

R

RADIUS (Remote Access Dial-Up Service), 236, 279

- integrating ISA Server 2006 with, 24
- Message Authentication in, 241
- servers, configuring, 109-110
- VPN client authentication, 236-243

RDP access, enabling, 444-446

reassessing security goals/objectives, 466-467

recovery. *See* backup and recovery tools

redirecting clients to Exchange virtual directory, 326-328

redundancy with ISA security appliances, 196

Registry, RPC over HTTP configuration, 364

relationships. *See* network rules

remote access, configuring, 95. *See also* RADIUS; VPN

Remote Access Dial-Up Service. *See* RADIUS

Remote Access Policies, creating in IAS, 239-241

Remote Access Quarantine Service (RQS)

- configuring
 - protocol definition, 269-270
 - rules, 270-271
- installing, 268-269

remote administration, 441

- enabling RDP access, 444-446
- installing ISA Server Management Console, 441-444

Remote Procedure Call traffic. *See* RPC traffic

remote site networks, creating, 96

renaming servers in Management Console, 448

reports. *See also* monitoring

- customizing, 501
- generating, 88-90, 501-502
- management-level reporting, 536
- scheduling generation of, 502-503
- technical reporting, 537
- types of, 500-501

requesting certificates

- for ISA servers, 253-254
- for VPN clients, 254-255

requirements. *See* prerequisites

restores, 26

- from automatic export scripts, 483
- importing ISA settings
 - individual ISA components, 475-476
 - server configuration, 476-477
 - URL sets, 477-478

restricting

- HTTP attachments, 392
- HTTP headers, 392
- HTTP methods, 391-392
- HTTP signatures, 392-393
- RPC traffic, filtering versus, 415

reverse proxy deployment scenario, 20-21, 185

- applying network template, 189-190
- capabilities of, 188
- configuring existing firewalls for, 191-192
- in enterprise environments, 196-197
- preconfigured hardware appliances, 190-191
- web server publishing rules, 188, 193
 - for Outlook Web Access, 193-195
 - for web services, 195
- within security infrastructure, 186-187

reverse proxy servers, described, 82, 186, 203

role groups, 435

role-based access control, 435

with Active Directory groups, 435
example of, 436-437

roles

assigning to ISA server, 52
with monitoring capabilities, 488

Root directory (OWA), 328

route network relationships, 143

Route relationships (network rules), 73

route tables, adding persistent routes to, 142

Routing and Remote Access Service (RRAS), 94, 232

routing configurations, assigning for VPN clients, 232-233

Rpc directory (OWA), 329

RPC filtering, 415-416

deployment options, 416-417

RPC over HTTP

configuring on Exchange servers
back-end servers, 363
front-end servers, 363-364
definition, 347
installing, 362
ISA publishing rules, 365-366
Outlook 2003 profiles, 366-368
Registry settings, 364
RPC virtual directory, 365

RPC services

custom RPC protocol definitions,
creating, 420-422
publishing, 419-420

RPC traffic

application security for, 29-30
blocking versus filtering, 415
dangers of, 413-415
securing between network segments, 415
ISA deployment options, 416-417
with RPC filtering, 415-416

RPC UUIDs, identifying with Network Monitor, 422-426

RQS (Remote Access Quarantine Service)

configuring
protocol definition, 269-270
rules, 270-271
installing, 268-269

RRAS (Routing and Remote Access Service), 94, 232

rule sets

exporting for backup, 471-472
importing for restores, 475-476

rules. See firewall rules; publishing rules; web publishing rules

S

Schedule tab options (configuring web publishing rules), 399

scheduled maintenance. See maintenance plans

Schedules toolbox, 85

scheduling

automatic export scripts, 481-483
report generation, 502-503

Scope pane (Management Console), 67. See also nodes (Management Console)

scripts, custom

- automating export features, 478-483
- for design documentation, 521-530

SCW (Security Configuration Wizard), 50-51

- custom ISA security template, creating, 52-62
- installing, 51

secure mail access

- EAS (Exchange ActiveSync), 347
 - enabling, 348
 - publishing rules, 358-361
 - supporting on back-end mailbox servers, 349-353
- IMAP (Internet Message Access Protocol), 374-376
 - enabling, 374
 - filtering rules, 375-376
 - SSL (Secure Sockets Layer), 375
- importance of, 346
- ISA Server 2006 messaging security mechanisms, 346-347
- MAPI (Message Application Programming Interface) filtering rules, 369-371
- overview, 345
- OWA (Outlook Web Access). *See* OWA
- POP3 (Post Office Protocol version 3), 372-374
- RPC over HTTP, 347
 - configuring on Exchange servers, 363-364
 - installing, 362
 - ISA publishing rules, 365-366
 - Outlook 2003 profiles, 366-368
 - Registry settings, 364
 - RPC virtual directory, 365

SMTP (Simple Mail Transport Protocol), 376-379

- custom SMTP filters, 379
- inbound SMTP filtering, 377
- outbound SMTP filtering, 377, 379

Secure Sockets Layer. *See* SSL**SecureNAT clients, capabilities of, 298-299****securing OWA (Outlook Web Access)**

- definition, 347
- enabling OWA, 348
- with ISA Server 2006
 - exporting/importing OWA certificates, 331-333
 - overview, 329, 331
 - OWA publishing rules, 334-336, 338, 340-342
- overview, 315
- publishing rules, creating, 358-359, 361
- redirecting clients to Exchange virtual directory, 326-328
- SSL (Secure Sockets Layer)
 - forcing SSL encryption for OWA traffic, 325-326
 - internal CAs (certificate authorities), 322-325
 - overview, 316-317
 - third-party CAs (certificate authorities), 317-321
- supporting on back-end mailbox servers, 349-353
- virtual servers
 - adding IP addresses to, 355
 - assigning SSL certificates to, 357
 - creating, 355-357
 - deploying multiple, 354-357
 - settings, 328-329

security. *See also* application security; encryption; secure mail access

- in content caching deployment scenario, 201
- of documentation, 516
- SSL (Secure Sockets Layer)
 - forcing SSL encryption for OWA traffic, 325-326
 - internal CAs (certificate authorities), 322-325
 - overview, 316-317
 - third-party CAs (certificate authorities), 317-321

security appliances. *See* reverse proxy deployment scenario

security audits, 465-466

security breaches, high cost of, 8-9

Security Configuration Wizard (SCW), 50-51

- custom ISA security template, creating, 52-62
- installing, 51

security goals/objectives

- identifying, 114
- mapping to ISA features, 115-116
- reassessing, 466-467

security infrastructure, reverse proxy deployment scenario in, 186-187

Security Reports, 501

selecting

- Enterprise versus Standard version of ISA Server 2006, 19-20, 124-125, 158
- operating system for ISA Server 2006, 19

Server Console. *See* Management Console

server hardware. *See* hardware

server publishing rules. *See* publishing rules

servers

- configuration
 - exporting for backup, 472
 - importing for restores, 476-477
- details, viewing, 108
- functionality, checking, 456
- multiple servers, administration of, 448-450
- OWA (Outlook Web Access). *See* OWA publishing, firewall deployment and, 152
- renaming in Management Console, 448

Service Pack 1, applying to Windows Server 2003, 41-42

service packs, described, 35-36

services, monitoring, 88, 498-499

Session layer, 137

sessions, monitoring, 88, 498-499

shared key encryption, 288

SharePoint sites, 402-403

- Alternate Access Mapping (AAM), configuring, 403-404
- encrypting, 403
- publishing rules, creating, 407-408, 410-411
- SSL certificates
 - importing/exporting, 405-407
 - installing, 404-405

signatures (HTTP), restricting, 392-393

Simple Mail Transport Protocol (SMTP), 376-379

single network adapter templates, 72

- applying to unihomed ISA Server, 189-190

site-to-site VPN deployment scenario, 125, 277

- authentication methods, 279, 285
- IPSec Tunnel Mode configuration, 292-294
- L2TP configuration, 288-292
- PPTP configuration, 286-288
- preparation for, 280-285
- reasons for using, 278
- remote site networks, creating, 96
- tips for consideration, 280

sizing ISA Server 2006 deployment, 124-125

small organizations, ISA Server 2006 deployment for, 128-129

SMTP (Simple Mail Transport Protocol), 376-379

software component prerequisites for ISA Server 2006, 47

software-based firewalls, 9

SSL (Secure Sockets Layer), 383

- certificates
 - importing/exporting to ISA servers, 405-407
 - installing on SharePoint servers, 404-405
- enabling for OWA (Outlook Web Access)
 - forcing SSL encryption for OWA traffic, 325-326
- internal CAs (certificate authorities), 322, 324-325
- overview, 316-317
- third-party CAs (certificate authorities), 317, 319-321

IMAP (Internet Message Access Protocol), 375

POP3 (Post Office Protocol version 3), 372, 374

SharePoint site encryption, 403

SSL-to-SSL bridging, configuring, 400-401

stand alone server, VPN server as, 226-227

Standard version of ISAServer 2006, 19-20

- Enterprise version versus, 124-125, 158
- installing, 47-50

subnets, networks versus, 69-71

Summary Reports, 501

system policies, 82, 153-155

- exporting for backup, 472-473

System Policy Editor, 82

- allowing Windows/Microsoft Update access, 454-455

system usage policy documentation, 537

T

Task pane (Management Console), 67

Task Scheduler, scheduling automatic export scripts, 481-483

technical reporting, 537

technical training documentation, 537

templates. See also network templates

- custom ISA security template, creating, 52-62
- default network templates, 143-144
- edge firewall template, deployment with, 144-146
- Network Template Wizard, 74-78

test plans, creating, 531

testing

- PPTP VPN connections, 245-246
- UPS (uninterruptible power supply), 463

third-party add-ons, installing, 50

third-party backup and restore tools, 483-484

third-party CAs (certificate authorities), 401

advantages, 317-319

installing, 319-321

third-party VPN products, integration with, 292-294

threats, 382

To tab options (configuring web publishing rules), 389

Traffic and Utilization Reports, 501

Traffic tab options (configuring web publishing rules), 390, 392-393

training documentation, 537

transparent proxies

described, 203

enabling, 213

Transport layer, 137

troubleshooting. See also logging; monitoring; Monitoring node (Management Console)

documentation of, 517

with logging, 493

accessing log files, 494-495

customizing log filters, 495-496

network configuration, 70

VPN client access, 94

U

unattended installation of firewall clients, 306-307

unihomed ISA Server 2006. See reverse proxy deployment scenario

uninterruptible power supply (UPS), testing, 463

updates, checking for, 460

updating

ASR (Automated System Recovery) sets, 463-464

documentation, 464-465

ISA Server 2006, 50

operating systems, 42-44 453-456

upgrading. See migrating

UPS (uninterruptible power supply), testing, 463

URL sets

exporting for backup, 473-475

importing for restores, 477-478

user accounts, creating VPN user accounts, 283-284

Users tab options (configuring web publishing rules), 398

Users toolbox, 84

UUIDs, identifying RPC UUIDs with Network Monitor, 422-426

V

validating

backups, 463

of ISA Server design implementation, 128

verifying

backups, 457-458

connectivity, 90-91

hardware, 461

viewing

alerts, 87-88

server details, 108

Virtual Private Network. See VPN

virtual servers (OWA)

- adding IP addresses to, 355
- assigning SSL certificates to, 357
- creating, 355-357
- deploying multiple, 354-357
- settings 328-329

viruses. See threats**VPN (Virtual Private Network), 11, 221-222**

- deployment scenarios, 22-23, 225-226
 - domain member, VPN server as, 226
 - workgroup member, VPN server as, 226-227
- L2TP VPN connections
 - configuring Windows XP Professional clients for, 248-249
 - creating, 246-247
 - IPSec pre-shared keys, configuring, 247-248
 - PKI (Public Key Infrastructure), creating, 249-259
- network bandwidth constraints, 224-225
- PPTP VPN connections
 - configuring Windows XP Professional clients for, 244-245
 - enabling support for, 243-244
 - testing, 245-246
- preparation for implementation, 225
- protocols, 222-224
- Quarantine feature, 267-268
 - configuring RQS protocol definition, 269-270
 - configuring RQS rules, 270-271
 - customizing CMAK packages for, 273-274
 - enabling, 272-273
 - installing RQS (Remote Access Quarantine Service), 268-269

- site-to-site VPN deployment scenario, 277
- authentication methods, 279, 285
- IPSec Tunnel Mode configuration, 292-294
- L2TP configuration, 288-292
- PPTP configuration, 286-288
- preparation for, 280-285
- reasons for using, 278
- tips for consideration, 280
- user accounts, creating, 283-284

VPN clients, 70, 300

- authentication methods, 233-234
 - RADIUS, 236-243
- automated deployment with CMAK, 259-260
 - creating CMAK profiles, 261-266
 - installing CMAK, 260-261
 - installing CMAK profiles, 267
- certificates, requesting, 254-255
- enabling access, 93-95, 231-232, 281-283
- firewall rules, creating, 234-236
- IP addresses, assigning, 229-230
- network rules, creating, 227-229
- routing configurations, assigning, 232-233

VPN node (Management Console), 91

- client access, enabling and configuring, 93-95
- remote access, configuring, 95
- remote site networks, creating, 96
- VPN quarantine, 96-97

W-Z

web caching. See content caching deployment scenario

web chaining, 79

configuring, 209-210

web filters, 102

Web Proxy clients, capabilities of, 299-300.

See also content caching deployment scenario

Web Proxy logging, configuring, 493

web publishing rules, 383

configuring

Action tab options, 388

Application Settings tab options, 396

Authentication Delegations tab options, 396

Bridging tab options, 398

From tab options, 388

General tab options, 387

Link Translation tab options, 400

Listener tab options, 393-395

Paths tab options, 396

Public Name tab options, 395

Schedule tab options, 399

To tab options, 389

Traffic tab options, 390-393

Users tab options, 398

creating, 384-387

defining for reverse proxies, 188, 193

modifying for SSL-to-SSL bridging, 401

for Outlook Web Access, 193-195

for web services, 195

web services, configuring reverse proxy for, 195

web traffic. See HTTP traffic

Web Usage Reports, 500

web-based email. See OWA (Outlook Web Access)

Website Publishing Wizard, creating web publishing rules, 384-387

weekly maintenance plans, 460-461

Windows Performance Monitor, 511

Windows Server 2003

applying Service Pack 1, 41-42

installing, 38-40

Windows Server Update Services (WSUS), 453

Windows Update, 453-455

allowing access to, 454-455

Microsoft Update versus, 43

Windows XP Professional clients, configuring

for L2TP VPN connections, 248-249

for PPTP VPN connections, 244-245

WinMSD utility, 519

workgroup membership

domain membership versus, 44-45

functional limitations of, 45-46

for VPN servers, 226-227

WSUS (Windows Server Update Services), 453



THIS BOOK IS SAFARI ENABLED

INCLUDES FREE 45-DAY ACCESS TO THE ONLINE EDITION

The Safari® Enabled icon on the cover of your favorite technology book means the book is available through Safari Bookshelf. When you buy this book, you get free access to the online edition for 45 days.

Safari Bookshelf is an electronic reference library that lets you easily search thousands of technical books, find code samples, download chapters, and access technical information whenever and wherever you need it.

TO GAIN 45-DAY SAFARI ENABLED ACCESS TO THIS BOOK:

- Go to <http://www.sampublishing.com/safariabled>
- Complete the brief registration form
- Enter the coupon code found in the front of this book on the "Copyright" page

If you have difficulty registering on Safari Bookshelf or accessing the online edition, please e-mail customer-service@safaribooksonline.com.

UNLEASHED

Unleashed takes you beyond the basics, providing an exhaustive, technically sophisticated reference for professionals who need to exploit a technology to its fullest potential. It's the best resource for practical advice from the experts, and the most in-depth coverage of the latest technologies.

OTHER UNLEASHED TITLES

ASP.NET 2.0 Unleashed
ISBN: 0672328232

**Microsoft BizTalk Server
2006 Unleashed**
ISBN: 0672329255

**Microsoft Exchange
Server 2007 Unleashed**
ISBN: 0672329204

**Microsoft Expression
Blend Unleashed**
ISBN: 067232931X

**Microsoft ISA Server
2006 Unleashed**
ISBN: 0672329190

**Windows PowerShell
Unleashed**
ISBN: 0672329530

**Microsoft SharePoint
2007 Development
Unleashed**
ISBN: 0672329034

**Microsoft Small
Business Server 2003
Unleashed**
ISBN: 0672328054

**Microsoft SQL Server
2005 Unleashed**
ISBN: 0672328240

**Microsoft System Center
Operations Manager
2007 Unleashed**
ISBN: 0672329557

**Microsoft Visual C#
2005 Unleashed**
ISBN: 0672327767

**Microsoft Visual Studio
2005 Unleashed**
ISBN: 0672328194

**Microsoft XNA
Unleashed**
ISBN: 0672329646

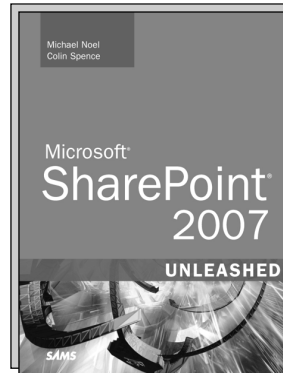
**Silverlight 1.0
Unleashed**
ISBN: 0672330075

**VBScript, WMI and ADSI
Unleashed**
ISBN: 0321501713

**Windows
Communication
Foundation Unleashed**
ISBN: 0672329484

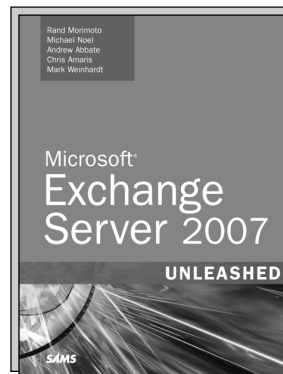
**Windows PowerShell
Unleashed**
ISBN: 0672329530

**Windows Presentation
Foundation Unleashed**
ISBN: 0672328917



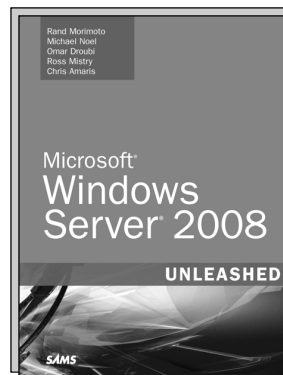
**Microsoft® SharePoint 2007
Unleashed**

ISBN: 0672329476



**Microsoft® Exchange Server 2007
Unleashed**

ISBN: 0672329204



Windows Server 2008 Unleashed

ISBN: 0672329301

SAMS

www.sampublishing.com