



Debugging SIC	26
Maintaining SIC	27
Using fwm sic_reset	31
Network Address Translation	32
Client-Side Destination NAT	32
Debugging NAT	33
Collecting Data	36
Rule Base Issues	36
NAT Issues	36
Anti-Spoofing Issues	36
SmartDashboard Issues	37
Logging Issues	37
Cluster Issues	38
Security Server Issues	38
OPSEC Server Issues	39
LDAP Issues	39
Core Dump and Dr. Watson Issues	40
Review	43
Review Questions	44
Review Answers	45
3 File Management	47
Objectives	47
Key Terms	48
cpinfo	49
Overview	49
cpinfo File	50
InfoView	52
Opening SmartDashboard in InfoView	59
objects_5_0.C and objects.C	61
objects_5_0.C	61
objects.C	61
Object Properties in objects_5_0.C	62
DbEdit	63



objects_5_0.C Editing	65
GuiDBedit	67
fwauth.NDB	72
\$FWDIR/lib/*.def Files	73
Example	73
Modifying *.def Files	74
Log Files	75
Active Log Files	75
Audit Log Files	76
Log Mechanism	76
Troubleshooting Logging Issues	77
Maintaining Logs and Log-Buffer Queue	78
Configuring Object Properties	78
Debugging Logging	81
Analysis Tools	81
Debugging Log	81
Lab 1: Using cpinfo	83
Lab 2: Analyzing cpinfo in InfoView	89
Lab 3: Using GuiDBedit	93
Lab 4: Using fw logswitch and fwm logexport	101
Review	107
Review Questions	108
Review Answers	109

4 Protocol Analyzers	111
Objectives	111
Key Terms	112
tcpdump	113
tcpdump Syntax	113
tcpdump and Expressions	115
Using tcpdump	116
Viewing tcpdump Output	117
snoop	119
Using snoop	119
Reading snoop Output	120



snoop and Security	122
snoop Limitations	122
fw monitor	124
Overview	124
fw monitor Syntax	124
INSPECT Virtual Machine	126
Filter Expressions	127
fw ctl chain	127
Buffering Issues	138
Ethereal	140
Using Ethereal	140
Viewing Connection Beginnings	143
Viewing Connections Dropped by Kernel	143
Using Filters with Ethereal	143
Lab 5: Comparing Client-Side NAT vs. Server-Side NAT with fw monitor	149
Review	155
Review Questions	156
Review Answers	157

5 NGX Debugging Tools 159

Objectives	159
Key Terms	160
fw ctl debug	161
fw ctl kdebug	161
Kernel Modules	162
fw ctl debug Flags	164
Debugging fwd/fwm	169
fwd Daemon	169
fwm Process	169
Debugging	169
fwd/fwm Debug Switches	170
Debugging without Restarting fwd/fwm	170
Debugging by Restarting fwd/fwm	172
Stopping fwd debug	173



Debugging cpd	174
Use	175
Lab 6: Using cpd and fwm Debugging	177
Review	181
Review Questions	181
Review Answers	183

6 fw advanced Commands 185

Objectives	185
Key Terms	186
fw Commands	187
fw tab Command	188
fw tab Options	188
Table Attributes	189
fw tab Examples	194
fw ctl Commands	197
fw ctl install	197
fw ctl uninstall	197
fw ctl iflist	197
fw ctl arp	198
fw ctl pstat	198
fw ctl conn	205
Other fw Commands	207
fw sam	207
fw lichosts	210
fw log	210
fw repairlog	211
fw mergefiles	211
fw fetchlogs	212
fw Advanced Commands	214
fw fwd	215
fw fwm	215
fw fetchlocal	216
fw unloadlocal	217
fw dbloadlocal	217

fw defaultgen	218
fw getifs	219
fw stat	219
fwm Commands	222
Use	222
fwm load	223
fwm dbload	224
fwm logexport	225
fwm dbexport/fwm dbimport	227
fwm lock_admin	228
Lab 7: Using fw ctl pstat	229
Lab 8: Using fw stat, fwm load, and fw unloadlocal	231
Review	233
Review Questions	233
Review Answers	235

7 Security Servers	237
Objectives	237
Key Terms	238
The Folding Process	239
Overview	239
Folding-Process Example	240
Content-Security Rule Order	242
Security Server Default Messages	242
HTTP 1.0 and 1.1	243
Troubleshooting Security Server Issues	244
Reviewing CPU and Memory	245
Editing fwauthd.conf	245
Listing Possible Causes	246
Identifying Issue Sources	247
Analyzing Results	248
Debugging Security Servers	249
TD_ERROR_ALL_ALL Flag	249
FTP Security Servers	249
HTTP Security Servers	250



SMTP Security Servers	251
Multiple Security Server Troubleshooting	252
Review	253
Review Questions	254
Review Answers	256
8 VPN Debugging Tools	257
Objectives	257
Key Terms	258
IKE Basics	259
Phase 1	259
Phase 2	264
Encryption Issue	268
Troubleshooting Overview	270
VPN Debugging Tools	271
VPN Log Files	271
vpn debug Command	271
vpn Command	272
Comparing SAs	275
Troubleshooting Tables	276
Lab 9: Running IKE Debugging on a Site-to-Site VPN	281
Review	289
Review Questions	289
Review Answers	291
9 Troubleshooting and Debugging SecuRemote/SecureClient	293
Objectives	293
Key Terms	294
Necessary Ports	295
Ports Used Through the Tunnel	296
Packet Flow	297
Packet Flow When Creating a Site	297
Packet Flow When Connecting/Resolving Gateway IP	297



Packet Flow When Connecting/IKE Negotiation	298
Packet Flow When Connecting/Encrypting Data	298
Link Selection for Remote Access	299
Overview	299
Link-Selection Methods in VPN-1 NGX	301
SecuRemote/SecureClient Debugging Tools	306
srfw monitor	306
cpinfo	306
IKE debug	307
sr_service Debug	308
IKE and sr_service Debug	308
sc log Debug	309
srfw ctl Debug	309
Enhanced Debugging Tool	311
Troubleshooting Table	313
Lab 10: Observing IKE Negotiation Between a Gateway and SecureClient	319
Lab 11: Running srfw monitor	325
Review	329
Review Question	330
Review Answer	331
10 Advanced VPN	333
Objectives	333
Key Terms	334
Route-Based VPN	335
Domain-Based VPN	337
VPN Tunnel Interface	338
VPN Routing Process	338
Best Practices	339
Numbered/Unnumbered VTIs	340
Configuring Numbered VTIs	341
Configuring Unnumbered VTIs	344
Dynamic VPN Routing	345
Configuring Dynamic VPN Routing Using OSPF	345



Wire Mode	350
How Wire Mode Works	350
Wire Mode in Route-Based VPN	353
Directional VPN Rule Match	355
Interface Groups	355
Tunnel Management	358
Permanent Tunnels	358
VPN Tunnel Sharing	360
Tunnel-Management Configuration	360
VPN Tunnel Sharing Configuration	365
Lab 12: Route-Based VPN Using Static Routes	367
Lab 13: Dynamic VPN Routing Using OSPF	385
Review	401
Review Questions	403
Review Answers	405

11 ClusterXL	407
Objectives	407
Key Terms	408
Configuration Recommendations	409
Recommendations for ClusterXL	409
Recommendations for State Synchronization	410
Troubleshooting ClusterXL	412
cphaprob	412
cphaprob state	414
cphaprob -a if	417
cphaprob -i list	418
cphaprob -d <device> -s problem -t 0 register	419
cpstat ha -f all	420
fw ctl debug -m cluster	421
Kernel Flags	424
fwha_enable_if_probing and fwha_monitor_if_link_state	424
fwha_restrict_mc_sockets (0 by Default)	425
fwha_use_arp_packet_queue (0 by Default)	426
fwha_send_gratuitous_arp_var	426



fw_gratuitous_arp_timeout	427
fw_allow_connection_traffic_drop (1 by Default)	427
fwha_allow_simultaneous_ping	428
fwconn_merge_all_syncs	429
fwtcpstr_reject_synced (On by Default)	429
Lab 14: Manual Failover Using cphaprob -d device Command	431
Lab 15: Running cphastart -d	437
Review	439
Review Question	440
Review Answer	441

Appendix A: Using DbEdit 443