
Contents

Check Point Security Administration NGX III	1
Course Layout	2
Prerequisites	2
Recommended Setup for labs	3
Recommended Lab Topology	4
IP Addresses	5
Lab Terms	7
Lab Stations	8
Default Rule Base	9
VMware Setup	10
Course Objectives	13
Chapter 1: General Troubleshooting	19
Troubleshooting Guidelines	21
Identifying the Problem	21
Collecting Related Information	22
Listing Possible Causes	22
Testing Causes Individually and Logically	22
Consulting Various Reference Sources	23
Before Installing VPN-1 NGX	24
IP Forwarding	24
Routing	25
Connectivity	26
IP forwarding and Boot Security	28
SIC and ICA Issues	31
SIC Port Use	31
Root Causes	32
Verifying the Certificate	33
Maintaining SIC	35
Resetting SIC	38

Using fw m sic_reset	39
Network Address Translation	41
Hide NAT	41
Static NAT	43
Debugging NAT	45
Lab 1: Initial installation	49
Install the Security Gateway	50
Install the City Site Web server	53
Install Primary SmartCenter Server	55
Lab 2: Enable SCP on Secureplatform (optional)	59
Implement SCP on Secureplatform	60
Enable the SCP Server	60
Testing SCP	61
Review	63
Review Questions	63
Review Answers	64

Chapter 2: Network Monitoring 65

State Tables and Kernel Memory	67
fw tab Command	67
fw ctl pstat	77
CPU and Memory Stats	81
SmartView Monitor	84
SNMP - (Simple Network Management Protocol)	87
Configuring SNMP	90
Using snmptrap	91
Lab 3: Configure SNMP	93
Configure SNMP on Secureplatform	94
Testing snmp locally	96
snmpwalk	96
snmpget	98
snmpgetnext	98
Installing SNMP Manager	100
Test snmp queries from SNMP Manager	103
SNMP Trap	107

Lab 4: Configure SNMP Manager (optional)	109
Installing SNMP Manager	110
Test snmp queries from SNMP Manager	113
SNMP Trap	117
Review	119
Review Questions	119
Review Answers	120
Chapter 3: Disaster Recovery	121
Filing Structure	123
\$CPDIR	123
\$FWDIR/conf	124
\$FWDIR/lib/*.def Files	126
\$FWDIR/log	127
Files on the Security Gateway	129
Recovery Methods	130
Backup and Restore	130
Restoring with Snapshot	131
Restoring with Upgrade_export and Upgrade_import	132
Restore from a cpinfo	133
Restore from database revision control	135
Manual Restore	136
Lab 5: Recovering SmartCenter Server	139
Recovering a SmartCenter Server	140
Review	143
Review Questions	143
Review Answers	144
Chapter 4: Troubleshooting Utilities	145
cpinfo	147
Overview	147
cpinfo File	149
InfoView	150
Opening SmartDashboard in InfoView	157
DbEdit	159
objects_5_0.C Editing	161

GuiDBedit	163
cp_merge	168
Freeware tools	171
Lab 6: Using cpinfo	175
Run cpinfo on the Security Gateway	176
Examine cpinfo Output File	178
Run cpinfo on the SmartCenter Server	180
Lab 7: Analyzing cpinfo in InfoView	181
Open Gateway cpinfo in Infoview	182
Review Installed Products, System, License, and Other Information	183
Launch SmartDashboard in InfoView	185
Lab 8: Object Filler (optional)	187
Converting Cisco to Check Point	188
Importing the objects	188
Importing the rules	189
Review	191
Review Questions	191
Review Answers	192

Chapter 5: Protocol Analyzers	193
tcpdump	195
snoop	203
fw monitor	208
Wireshark	224
Lab 9: Comparing Client-Side NAT vs. Server-Side NAT with fw monitor ...	233
Configure Automatic Static NAT for www.yourcity.cp.	234
Run fw monitor while webdallas Browses the NAT Address of www.yourcity.cp	235
Disable Client-Side NAT	237
Add Host Route on fwyourcity Gateway	238
Run fw monitor while Browsing NAT IP Address	239
Run fw monitor to Capture Clients Browsing NAT IP of www.yourcity.cp. ...	240

Review	243
Review Questions	243
Review Answers	244
Chapter 6: NGX kernel debugging	245
fw ctl debug	247
fw ctl kdebug	249
fw ctl debug Flags	250
Examples of fw ctl debug	251
zdebug	254
fw Commands	255
fw ctl Commands	256
fw ctl install	256
fw ctl uninstall	256
fw ctl iflist	256
fw ctl arp	257
fw ctl pstat	257
fw ctl conn	259
Other fw Commands	261
fw sam	261
fw lichosts	263
fw log	264
fw repairlog	265
fw mergefiles	265
fw fetchlogs	266
fw Advanced Commands	268
fw fwd	269
fw fwm	269
fw fetchlocal	270
fw unloadlocal	271
fw dbloadlocal	271
fw defaultgen	272
fw getifs	273
fw stat	273
fwm Commands	276
Use	276
Lab 10: fw ctl debug	283
Run fw ctl debug	284

Review	285
Review Questions	285
Review Answers	286
Chapter 7: User-level process debugging	287
NGX User Processes	289
Debugging fwd	290
Debug options	290
Debugging fwm	295
Debug Options	295
Debugging by Restarting fwm	296
Debugging Licensing	297
Debugging SmartUpdate	299
Debugging cpd	301
cpd_admin usage	302
Debugging SIC	303
Watchdog process - cpwd	306
Lab 11: Using cpd and fwm Debugging	309
Run debugs	310
Debug the Security Gateway	310
Debug the SmartCenter Server	310
Replicate the Problem	311
Turn off debugs	312
View the Output	313
Review	315
Review Questions	315
Review Answers	316
Chapter 8: Security Servers	317
The Folding Process	319
Overview	319
Example of packet flow	319
Transparent Connections	321
Rule Order	322
Security Server Default Messages	322

Troubleshooting Security Server Issues	324
Reviewing CPU and Memory	325
Editing fwauthd.conf	325
Listing Possible Causes	327
Identifying Issue Sources	329
Analyzing Results	330
Debugging Security Servers	331
TDERROR_ALL_ALL Flag	331
SMTP Security Servers	334
Multiple Security Server Troubleshooting	334
Messaging Security	336
Architecture	337
Debugging Messaging Security	338
Review	341
Review Questions	341
Review Answers	342

Chapter 9: VPN Debugging Tools

IKE Basics	345
Phase 1	345
Phase 2	350
Encryption Issues	355
Troubleshooting Overview	357
VPN Debugging Tools	358
VPN Log Files	358
vpn debug Command	358
vpn Command	360
Comparing SAs	362
Troubleshooting Tables	363
Encryption-Troubleshooting Table	364
Common Error Messages	366
Lab 12: Troubleshooting Site to Site VPN	369
Configure the local Gateway	370
Configure the peer	372
Lab 13: Debug Site to Site #1	377
Replicate the failure	378

Lab 14: Debug Site to Site #2	381
Troubleshooting Site to Site failure	382
Review	385
Review Questions	385
Review Answers	386

Chapter 10: Debugging Remote Access

Remote Access Overview	391
SecureClient Ports	392
Ports Used Through the Tunnel	393
SecureClient Packet Flow	394
Creating a Site	394
Connecting to the Site	395
Encrypting Data	396
Connectivity Enhancements	398
IKE over TCP	398
UDP Encapsulation	399
NAT-T	400
Visitor Mode	400
Link Selection for Remote Access	402
Overview	402
Link-Selection Methods in VPN-I NGX	404
SecuRemote/SecureClient Debugging Tools	409
srfw monitor	409
cpinfo	410
IKE Debug and SR_Service Debug	410
srfw ctl Debug	412
Troubleshooting Table	414
SSL Network Extender	419
What does a SNX connection look like?	419
Troubleshooting SNX	423
Troubleshooting the client	424
SecureClient Mobile	427
Client Deployment	428
Debugging SecureClient Mobile	428
Lab 15: UDP encapsulation, NAT-T and Visitor Mode	431
Configuration for this lab	432

Gateway Side: Enable Office Mode on the Gateway	433
Gateway Side: Create the SecureClient User	434
Gateway Side: Configure the Remote Access Community	435
Client Side: Installing and Creating the site	437
UDP Encapsulation	439
NAT-T	443
Visitor Mode	445
Lab 16: SNX Network Extender	447
Configure SNX (SSL Network Extender)	448
Connecting with the client	450
Review vpnd	454
Review	455
Review Questions	455
Review Answers	456

Chapter 11: Advanced VPN	459
Route-Based VPN	461
Domain-Based VPN	463
VPN Tunnel Interface	464
VPN Routing Process	464
Best Practices	466
Numbered/Unnumbered VTIs	466
Configuring Numbered VTIs	467
Configuring Unnumbered VTIs	469
Dynamic VPN Routing	471
Configuring Dynamic VPN Routing Using OSPF	471
Wire Mode	476
How Wire Mode Works	476
Wire Mode in Route-Based VPN	480
Directional VPN Rule Match	482
Interface Groups	482
Tunnel Management	485
Permanent Tunnels	485
VPN Tunnel Sharing	487

Tunnel-Management Configuration	487
VPN Tunnel Sharing Configuration	492
Lab 17: Route-Based VPN Using Static Routes.....	493
Configure fwyourcity to Join MyIntranet Community	495
Configure fwpartnercity Gateways to Join MyIntranet Community	496
Add Participating Gateways to MyIntranet	497
Create VTIs on fwyourcity.....	498
Configure VTI Topology in Gateway Object	502
Add Static Routes to Internal Networks	503
Enable VPN Directional Rule Match	505
Configure Wire Mode	510
Lab 18: Dynamic VPN Routing Using OSPF.....	515
Update the Policy for OSPF Routing.....	517
Configure OSPF Interfaces	520
Configure OSPF on fwyourcity	522
Reconfigure Anti-Spoofing on fwyourcity.....	526
Verify Routes and OSPF Configuration	529
Test VPN tunnels	532
Review.....	535
Review Questions.....	535
Review Answers	536

Chapter 12: ClusterXL	537
Configuration Recommendations.....	538
Recommendations for ClusterXL	538
Recommendations for State Synchronization.....	539
Troubleshooting ClusterXL	541
cphaprob	541
cphaprob state	544
cphaprob -a if	547
cphaprob -i list	548
cphaprob -d <device> -s problem -t 0 register	549
cpstat ha -f all	550

fw ctl debug -m cluster	551
Kernel Flags	554
fwaha_enable_if_probing and fwaha_monitor_if_link_state	554
fwaha_restrict_mc_sockets (0 by Default)	555
fwaha_use_arp_packet_queue (0 by Default)	556
fwaha_send_gratuitous_arp_var	556
fw_gratuitous_arp_timeout	557
fw_allow_connection_traffic_drop (1 by Default)	557
fwaha_allow_simultaneous_ping	557
fwconn_merge_all_syncs	558
fwtcpstr_reject_synced (On by Default)	559
New behavior in NGX	559
Lab 19: Running cphastart -d	561
Run cphastop on Cluster Members	562
Run cphastart -d on Cluster Members	563
Lab 20: Manual Failover Using cphaprob -d Device Command	565
Configure ClusterXL new mode HA	566
Generate Failover in New Mode HA Cluster	567
Lab 21: State Sync	569
Run FTP session	570
Review	571
Review Questions	571
Review Answers	572

Appendix A: Collecting Data	573
Rule Base Issues	573
NAT Issues	573
Anti-Spoofing Issues	573
SmartDashboard Issues	574
Logging Issues	574
Cluster Issues	575
Security Server Issues	575
OPSEC Server Issues	575
LDAP Issues	576
Core Dump and Dr. Watson Issues	576

Appendix B: NGX kernel debug	579
fw kernel module options	579