

CONTENTS

.....

1	Managing Connectra NGX	1
	Course Objectives	1
	Course Layout	2
	Prerequisites	2
	Recommended Setup for labs	3
	Recommended Lab Topology	4
	IP Addresses	5
	Lab Terms	7
	Lab Stations	8
2	Connectra Endpoint-Security Features and Deployment	9
	Objectives	9
	Key Terms	10
	Connectra Security Features	11
	Server-Side Security	11
	Client-Side Security	12
	Deploying Connectra	14
	Deploying Connectra in the DMZ	14
	Deploying Connectra in the LAN	16
	DMZ vs. LAN Deployment	17
	Configuring Gateway Access Rules	17
	Lab 1: Deploying Connectra in the DMZ	19
3	Connectra Settings and Device Options	39
	Objectives	39
	Key Terms	40



The Connectra Administration Portal	41
Admin-Portal Menu Options	41
Admin-Portal Settings	44
Device Options	46
Status	46
Network	46
Control	50
Licenses	51
Date and Time	52
Backup and Restore	52
Upgrade	54
Servers	55
Administrators	55
Authenticating Administrators	57
Configuring Administrator Settings	59
SSL Network Extender	60
SSL Network Extender Application Mode	60
SSL Network Extender Requirements	60
SSL Network Extender Settings	61
Web Data compression	67
Configuring Data Compression	67

4 Managing Users and Groups	71
Objectives	71
Key Terms	72
Authentication and Authorization	73
Authentication and Authorization Process	73
Protection Levels	75
Configuring Protection Levels	75
Managing access	77
Group Types	77
Defining Users and Groups	77



Defining Generic Users	78
Configuring Users and Groups	79
Internal User Groups	79
External User Groups	79
RADIUS Servers	82
SecurID	83
Lab 2: Configuring Internal Users and Groups	85
Lab 3: Configuring the LDAP Server and LDAP User Group	95

5 Connectra Applications 107

Objectives	107
Key Terms	108
Web Applications	109
Understanding Web Applications	109
Connectra and Web Applications	110
Link Translation	111
HTTP Authentication	113
Connectra Web Applications	114
Domino Web Access	115
Outlook Web Access	115
Lab 4: Configuring a Web Application Using OWA	117
File Shares	127
Understanding File Shares	127
Lab 5: Configuring a File Share	129
Mail Services	135
Understanding Mail Services	135
Lab 6: Configuring Web Mail	139
Network Applications	147
Understanding Network Applications	147
SSL Network Extender Application Mode	147
Embedded Network Applications	150
Automatic Commands or Scripts	158
Network Applications Settings	160
Lab 7: Configuring a Network Client in Network Mode with SSL Network Extender	163



Citrix Services	175
Understanding Citrix Services	175
Configuring Citrix Services	180
Single Sign On	182
Understanding Single Sign On	182

6 Configuring Certificates 183

Objectives	183
Key Terms	184
Server Certificates	185
Automatically Generating Server Certificates	185
Obtaining a Connectra Server Certificate	185
Server-Certificate Details	186
Creating a New Server Certificate	187
Changing a Server Certificate	187
Generating a CSR	189
Configuring Client Certificates	192
End-User Login with Client Certificate	192
Configuring CRL Settings	193
Lab 8: Authenticating a User with a Client Certificate	195

7 Security 205

Objectives	205
Key Terms	206
Securing Remote Access	207
Server-Side Security	207
Client-Side (Endpoint) Security	207
SmartDefense	208
Web Intelligence	210
Integrity Clientless Security for Connectra	212
Integrity Secure Workspace	213



Configuring SmartDefense Network Security	217
Configuring DoS Protection	218
Configuring IP and ICMP Protection	219
Configuring TCP Protection	221
Configuring Dynamic Ports Protection	222
Configuring SmartDefense Application Intelligence	223
Configuring FTP Protection	223
Configuring Microsoft Networks Protection	225
Configuring DNS Protection	226
Configuring Web Intelligence	227
Malicious Code Protection	228
General HTTP Worm Catcher	229
Cross Site Scripting	229
LDAP Injection	230
SQL Injection	231
Command Injection	232
Directory Traversal	233
HTTP Format	233
Header Rejection	234
Block Unsafe HTTP Methods	234
Block WebDAV HTTP Methods	235
Configuring Client-Side Security	236
Configuring ICS	236
Configuring the Integrity Firewall-Client Scan	237
Configuring Malware Handling	238
Configuring Antivirus Settings	239
Configuring session Time-Outs	241
Lab 9: Enabling and configuring Client Verification	243

8 Status and Logging	249
Objectives	249
Key Terms	250
Connectra Logging	251



Audit Log	252
Fields	252
Audit-Log Options	253
Traffic Log	255
Fields	255
Traffic-Log Options	256
SmartCenter Management	257
Configuring SmartCenter Management for a Stand-alone Connectra Gateway	257
Configuring Remote Logging for a Connectra Cluster	258
Configuring Log Settings	261
Log-Level Settings	261
Log Capacity	262
SNMP in Connectra	263
The SNMP MIB	263
Handling SNMP Requests for UNIX	264
SNMP Traps	265
Lab 10: Configuring and Verifying Integrity Secure Workspace	267
Lab 11: Configuring a Remote Log Server	275

9 Connectra Cluster XL and High Availability	283
Objectives	283
Key Terms	284
Connectra Gateway Clustering	285
Load Sharing	286
High Availability	287
Administration HA and ClusterXL	288
Active and Standby Members	289
ClusterXL Requirements	291
State Synchronization in ClusterXL	291
ClusterXL Failover	293



Connectra ClusterXL Topology	298
ClusterXL Cluster VIPs	298
Cluster XL Cluster — Member IPs	299
Configuring Cluster Addresses on Different Subnets	299
Connectra ClusterXL Hardware Compatibility	300
Switch Settings for Connectra Clustering	301
Router Settings for Connectra Clustering	301
Lab 12: Deploying HA mode behind the DMZ	303

10 Troubleshooting and Maintenance 319

Objectives	319
Key Terms	320
Configuration Files	321
\$CVPNDIR	321
\$WEBISDIR	321
Connectra Error Messages	322
Citrix Troubleshooting	323
Troubleshooting Checklist	323
ClusterXL Troubleshooting	326
Symptom and Environment	326
Solution	326
Lab 13: LDAP Debug Exercise	327
SecurePlatform Overview	333
SecurePlatform Shell Commands	334
More Commands for Specific Applications	336
Snapshot-Image Management	337
Secure Shell	338
Copying Files Using SCP	338
Lab 14: Creating a Snapshot Image	339
Alternate Steps	342
Lab 15: Backup and restore	343

▪
▪
▪
▪
▪