

---

# Table of Contents

<b>Course Objectives</b> .....	i
<b>Preface: Endpoint Security Secure Access R70</b> .....	v
Course Layout .....	vi
Prerequisites .....	vi
Recommended Setup for Labs .....	vii
Recommended Lab Topology .....	viii
Training and Certification .....	ix
CCMA .....	x
Learn More .....	x
<b>Chapter 1 Introduction to Endpoint Security</b> .....	1
Endpoint Security Overview .....	3
System Architecture .....	5
Major Security Features .....	9
Communications, Modes and Views .....	13
Ports .....	13
Modes and Views .....	13
Switching Views .....	15
Activating Policies .....	15
Managing Catalogs and Groups .....	16
Authenticating Users .....	16
User Catalogs .....	17
Planning .....	19

---

Prerequisites.....	19
Choosing Client Type.....	19
Choosing Enterprise Policy Types.....	20
Choosing the Security Model.....	21
General Administrative Workflow.....	22
Lab 1: Server Installation.....	25
Review.....	53
<b>Chapter 2   The Security Infrastructure</b> .....	<b>57</b>
Introduction to Security Policies.....	59
Connected Policies.....	59
Disconnected Policies.....	60
Policy Arbitration.....	60
Policy Packages.....	61
Policy Assignment.....	61
Security Policy Component Overview.....	63
Managing Security Policies.....	69
Policy Workflow.....	69
Introduction to Client Installation Packages.....	71
Client Package Workflow.....	72
Planning Client Distribution.....	73
Deployment Options.....	73
Client Types.....	74
New Client Versions.....	75
Policies.....	75
Assigning Policies.....	76
Installation Options.....	76
Client Network Configuration.....	79
Configuring a New Network Connection.....	79
Lab 2: Building Policies and Packages.....	81
Lab 3: Catalogs and Policy Assignment.....	111
Review.....	121
<b>Chapter 3   Advanced Endpoint Security Features</b> .....	<b>125</b>
Program Control.....	127
Program Permissions.....	127

---

---

Program Groups . . . . .	128
Permission Precedence . . . . .	129
Global and Policy Permissions . . . . .	130
Program Evaluation Process . . . . .	130
<b>Program Control Workflow . . . . .</b>	<b>131</b>
Program Control Planning Tips . . . . .	131
<b>Protecting Against Spyware . . . . .</b>	<b>133</b>
Scan Target Drives and Exclusions . . . . .	133
Treatment Options . . . . .	133
Anti-spyware Workflow . . . . .	134
Enforcing Anti-spyware Scans and Treatments . . . . .	135
<b>Protecting Against Viruses . . . . .</b>	<b>136</b>
Scan Methods . . . . .	136
Scan Target Drives and Exclusions . . . . .	137
Treatment Options . . . . .	138
<b>Monitoring Anti-virus and Anti-spyware Activity . . . . .</b>	<b>139</b>
Monitoring Infection Activity on Connected Endpoints . . . . .	139
Monitoring Spyware and Virus Event History . . . . .	140
Monitoring Infection Scan and DAT Update Status . . . . .	140
<b>Enforcing Endpoint Security . . . . .</b>	<b>142</b>
Enforcement Rule Types . . . . .	142
Enforcement Rules Process . . . . .	143
Enforcement Rule Workflow . . . . .	145
Antivirus Provider Rules . . . . .	147
Client Enforcement Rules . . . . .	148
Grouping Enforcement and Antivirus Provider Rules . . . . .	148
Remediation Resources . . . . .	149
Using Rules that Observe or Warn . . . . .	151
<b>Tracking Enforcement Rule Compliance . . . . .</b>	<b>153</b>
Viewing Compliance Status . . . . .	153
Violations by Rule and Policy . . . . .	154
Viewing Antivirus Versions . . . . .	154
<b>High Availability . . . . .</b>	<b>155</b>
Architecture . . . . .	155
Configuring High Availability . . . . .	157
Forcing Replication . . . . .	159
<b>Lab 4: Antivirus and Spyware . . . . .</b>	<b>161</b>
<b>Review . . . . .</b>	<b>171</b>

---

---

<b>Chapter 4</b>	<b>Cooperative Enforcement and VPNs</b>	175
	Gateways and Cooperative Enforcement	177
	Virtual Private Networking Basics	179
	Configuring the Client VPN Connection	179
	Configuring profiles and sites	182
	VPN Options and Workflow	183
	Managing connection profiles	185
	Managing VPN Sites	188
	Managing Certificates	189
	Configuring Connection Options	190
	Lab 5: Configuring the VPN	193
	Review	223

---

---

---

