

Check Point R75 Management Essentials – Part 2

Check Point Training Course

Section Heading Index

Module 1 - Encryption	3
Module 2 – Site to Site VPNs	20
Module 3 – Remote Access VPNs – SecureClient	68
Module 4 – Clientless VPNs – Secure Network Extender	112
Module 5 – High Availability – Firewall Clusters	127
Module 6 – High Availability - SmartCenters	162

Module 1 – Encryption	3
1 Securing Communications	5
1.1 Symmetric Encryption	5
1.1.1 Encryption Key & Algorithms	5
1.1.2 Symmetric Key Problems.....	5
1.2 Asymmetric Encryption	6
1.2.1 Asymmetric Keys	6
1.2.2 Asymmetric Key Problems.....	7
1.3 Diffie-Hellman (DH).....	7
1.3.1 DH Special Asymmetric Algorithm	7
1.4 Integrity and Authenticity.....	9
1.4.1 Integrity Using Hashing Algorithms – MD5/SHA-1	9
1.4.2 Sending a Message using MD5.....	9
1.4.3 Authenticity Using Digital Signatures – RSA.....	10
1.5 Certificate Authorities.....	11
1.5.1 Central & Distributed Authorities.....	11
1.5.2 Check Point Internal Certificate Authority – ICA	11
1.5.3 Certificate Revocation Lists – CRLs	12
2 IKE and IPSEC	14
2.1 ISAKMP/Oakley – IKE.....	14
2.1.1 IKE Phase 1.....	14
2.1.2 IKE Phase 2.....	14
2.1.3 Encryption & Authentication Algorithms.....	14
2.1.4 Perfect Forward Secrecy – PFS	15
2.1.5 ‘vpn debug’ & IKEView.....	15
2.2 IPsec	17
2.2.1 Process of Building a VPN Tunnel.....	17
2.2.2 Encryption Mode -Tunnel or Transport	18
2.2.3 Encryption and Authentication (Packet Integrity)	18
2.2.4 Packet Integrity Problems & NAT	19

Module 2 – Site to Site VPNs20

1 Check Point VPNs23

1.1 Types of VPN.....23

1.1.1 Intranet – All Gateways Controlled by a Single SmartCenter.....23

1.1.2 Partner – Different Vendor Devices, Partner Cooperation23

1.1.3 Gateway Authentication – Shared Secret or Certificate24

1.1.4 Remote Access VPN34

1.2 Components of a VPN Configuration25

1.2.1 Gateway Endpoints.....35

1.2.2 Encryption Domain – Networks, Hosts.....26

1.2.3 Encryption Parameters27

1.2.4 Remote/Partner - Check Point Gateway or Interoperable Device..28

1.3 VPN Communities.....38

1.3.1 Mesh Communities29

1.3.2 Star Communities39

1.3.3 Remote Access Community.....30

1.4 VPN Rules.....30

1.4.1 Rules with Accept and VPN set to ‘Any’ still Encrypt30

1.4.2 Limiting the Rule by Community31

1.4.3 Limiting the Rule by Source and Destination31

1.5 Directional VPNs.....31

1.5.1 Enabling Directional VPNs.....31

1.5.2 Directional Rule Match Conditions31

1.6 Resetting VPN Tunnels – ‘vpn tunnelutil’32

1.6.1 Resetting tunnels32

1.7 Tunnel Monitoring – Alerts32

2 Current Rules Check.....33

2.1 Network Diagram33

2.2 Firewall Control and Rules Check.....33

2.2.1 Create a New Policy – ‘Site1_P2_Module2’.....33

2.2.2 Base Rules34

3 Creating a Mesh VPN – Gateways Under Your Control36

3.1 Setting Up the Local Endpoint Details.....36

3.1.1 Define the Local Gateway Encryption Domain.....36

3.1.2 Set the Local Gateway Properties.....36

3.2 Setting Up the Remote Endpoint Details.....37

3.2.1 Define the Remote Gateway Encryption Domain.....37

3.2.2 Set the Remote Gateway Properties.....37

3.3 Create the Mesh Community37

3.3.1 Create the Mesh Community & Add the Gateways.....37

3.3.2 Set the Mesh Community Properties38

3.4 Create the Security & NAT rules for the VPN.....40

3.4.1 Network Address Translation and VPNs.....40

3.4.2 Single Rule – Testing the Any Rule40

3.4.3 Single Rule – VPN Community restricted41

3.4.4 Multiple Rules – Network to Network Restricted42

3.4.5 Multiple Rules – Source & Destination Restricted.....42

3.4.6 Add the firewall Admin rule42

4 Star Community VPN – Gateways Under your Control.....44

4.1 Create the Star Community.....44

4.2 Testing the Star Community VPN46

5 Star Community VPN – Partners, IKE Shared Secrets.....47

5.1 Changing fw.site2.com – Independently Managed.....47

5.1.1 Remove fw.site2.com from the SmartCenter Objects for Site147

5.1.2 Install the new SmartCenter for fw-site2 on Server 10.2.2.1.....48

5.1.3 Reset the SIC Communications on fw.site2.com49

5.1.4 Complete Installation of SmartCenter for Site2.....50

5.1.5 Possible Connection Errors to New SmartCenter50

5.1.6 Create the Basic Objects for Site2 in the new SmartCenter51

5.1.7 Create a Basic Policy and install on fw.site2.com.....52

5.2 SmartCenter for Site1 - Local Endpoint Setup52

5.3 SmartCenter for Site1 - Remote Endpoint Setup52

5.3.1 Create an Interoperable Device Object called fw.site2.com.....52

5.3.2 Set the Encryption Domain in the Topology Tab.....52

5.4 SmartCenter for Site1 – Create the Star VPN Community.....53

5.4.1 Create the Star Community – VPN-PartnerSite253

5.4.2 Set the Encryption Parameters54

5.4.3 Set the IKE shared Secret54

5.5 SmartCenter for Site1 – Create the VPN Rules55

5.5.1 Add the VPN rules for Site155

5.6 SmartCenter for Site2 - Local Endpoint Setup56

5.7 SmartCenter for Site2 - Remote Endpoint Setup56

5.7.1 Create an Interoperable Device Object called fw.site1.com.....56

5.7.2	Set the Encryption Domain for the Partner Site	56
5.8	SmartCenter for Site2 – Create the Star VPN Community	56
5.8.1	Create the Star Community – VPN-PartnerSite1	56
5.8.2	Set the Encryption Parameters	57
5.8.3	Set the IKE shared Secret	57
5.9	SmartCenter for Site2 – Create the VPN Rules	57
5.9.1	Add the VPN rules	57
5.10	Testing the Partner VPN Using Shared Secret Authentication	58
5.10.1	Test Access using FTP	58
6	Star Community VPN – Partners, Certificates	58
6.1	Certificate Relationship ICA and Gateway	58
6.1.1	The ICA Server	58
6.1.2	The Gateway Certificate	58
6.1.3	Certificate Revocation Lists (CRLs)	60
6.2	Changing from Shared Secret to Certificate Authentication	60
6.2.1	Export the Site1 CA Certificate	60
6.2.2	Install the Site1 CA Certificate on SmartCenter Site2	61
6.2.3	Export the Site2 CA Certificate	62
6.2.4	Install the Site2 CA Certificate on SmartCenter Site1	62
6.2.5	Change the Community to use Certificates for Site1	63
6.2.6	Change the Community to use Certificates for Site2	63
6.2.7	Install the Policy for Site1 and Site2	63
6.2.8	Reset all VPN tunnels	63
6.2.9	Test the VPN Community using Certificate Authentication	64
6.2.10	Fetching the Internal CA using port 18264	64
7	Common Faults and Debugging	65
7.1	VPNs Common Faults	65
7.1.1	Common Faults	65
7.2	VPN Log Files & IKEView	66
7.2.1	Using IKEView	66
	Module 3 – RemoteAccess VPNs	68
1	Rules Check	71
1.1	New Policy and Rules	71
1.1.1	Create a new Policy Package	71

1.1.2	Create and Install the Base Rules	71
2	Remote Access VPNs	72
2.1	RemoteAccess Community	72
2.2	Virtual Desktop Infrastructure	72
2.2.1	Gateway Encryption Domain	72
2.2.2	User Groups	73
2.3	SecuRemote Client or SecureClient	73
2.3.1	SecureClient License, EndPoint Security Blade	73
2.3.2	Desktop Protection	74
2.4	Office Mode	74
2.4.1	Why Use Office Mode	74
2.4.2	How Office Mode Works	75
2.4.3	Office Mode IP address, Config file, Network Pool, DHCP	75
2.4.4	Alternative to Office Mode – Gateway IP Pools	76
2.5	UDP Encapsulation & Visitor Mode	77
2.5.1	VPN1_IPSEC_encapsulation, Port 2746	77
2.5.2	NAT-T, Port 4500	77
2.5.3	Visitor Mode, Port 443	77
3	Configuring RemoteAccess VPNs	79
3.1	User, Groups and Authentication	79
3.1.1	Create the VPN User Groups	79
3.1.2	User Authentication	80
3.1.3	Create VPN Users	81
3.1.4	Set the Gateway RemoteAccess Encryption Domain	82
3.1.5	Configure the RemoteAccess Community	82
3.1.6	Policy, Global Properties – RemoteAccess	82
3.1.7	Check Point Gateway – RemoteAccess Properties	85
3.1.8	Configure Office Mode	85
3.1.9	Wireless Hotspot/Hotel Registration	86
3.1.10	Add Remote Access Rules to the Security Policy	86
4	Installing Endpoint Security VPN Client	88
4.1	Endpoint Security Client Installation	88
4.1.1	With or Without Desktop Protection	88
4.1.2	Endpoint Security Secure Access	88
4.2	Post Installation Checks	89
4.2.1	Device Driver Check Point SecuRemote	89

4.2.2	Endpoint Security – Show Client.....	90
4.2.3	EndPoint Security Configuration Files – Trac.defaults, Trac.config	
5	Using Endpoint Security VPN – No Desktop Policy	91
5.1	Creating a Site	91
5.1.1	Site IP Address and Name.....	91
5.1.2	Authentication Method	93
5.2	Testing Remote Access	94
5.2.1	Connecting to the Gateway.....	94
5.2.2	Office Mode IP Address Assigned	95
5.2.3	Testing the Rules.....	96
5.2.4	Trac.config file unencrypted.....	97
5.3	Basic Problems and Debugging.....	98
5.3.1	Global Properties – Accept Remote Access Control Connections.....	98
5.3.2	Is the Site Correctly Defined – ‘Trac.config’	99
5.3.3	Do not Clone Endpoint Security Laptops	99
5.3.4	Multiple VPN Clients and Local Firewall	99
5.3.5	Overlapping Sites.....	99
5.3.6	Built in Packet Sniffer SecureClient only - ‘srfw monitor’.....	99
5.3.7	Turning on Debugging for Endpoint Security	100
5.3.8	Debugging SecureClient IKE Phase 1 & 2.....	100
6	Using Endpoint Security VPN – With a Desktop Policy	102
6.1	Enabling the Policy Server	102
6.1.1	Enable Policy Server on the Firewall Module.....	102
6.1.2	Set the Policy Server User Group.....	102
6.2	Writing Desktop Rules.....	103
6.2.1	Inbound Rules.....	103
6.2.2	Outbound Rules.....	103
6.2.3	Installing Desktop Rules	104
6.3	Updating the Remote Access Site – Endpoint Security.....	104
6.3.1	Site Update.....	104
6.3.2	The Installed Rules	104
6.3.3	Testing the Desktop Rules.....	104
6.3.4	Different Users, Different Rules	104
6.3.5	Outbound Desktop Rule for Updates	105
6.4	Remote Support for VPN Users	105
6.4.1	Enable Back Connections.....	105

6.4.2	Testing Remote Support.....	105
6.5	Using Visitor Mode – Tunnel over HTTPS	106
6.5.1	Check the WebGui is not using port 443.....	106
6.5.2	Enable Visitor Mode on the Gateway.....	106
7	SecureClient Packaging Tool	107
7.1	Building Pre-packaged Configuration for Easy Deployment.....	107
7.1.1	Overview.....	107
7.1.2	Creating a Package Profile	107

Module 4 – Clientless VPNs 112

1	SSL Network Extender – SNX	114
1.1	SSL Network Extender.....	114
1.1.1	Network Extender License Requirements.....	114
1.1.2	How SSL Network Extender Works	114
1.2	Configuration Requirements	114
1.2.1	Enable Gateway for Clientless VPNS	114
1.2.2	Users & Groups for Authentication	115
1.2.3	SSL Authentication and Encryption Options	115
1.2.4	Remote Access VPN rule	116
1.2.5	Supported Platforms and Web Browsers	116
2	Configuring Clientless VPNs.....	117
2.1	SSL Network Extender.....	117
2.1.1	Check the Clientless Global Properties Settings.....	117
2.1.2	Gateway Properties	117
2.1.3	Check the Security Rules.....	118
2.1.4	SNX and SecureClient on the same Desktop	118
2.1.5	Check that the ‘vpnd’ is running on port 443.....	118
2.2	Testing SSL Network Extender	119
2.2.1	Connecting to the Gateway – Authentication.....	119
2.2.2	Thin client Download and Install	120
2.2.3	Connecting to Internal Networks.....	121
2.2.4	User Certificate Authentication with SNX.....	122

Module 5 – Firewall High Availability127

1 Firewall High Availability	129
1.1 Firewall HA.....	129
1.1.1 Firewall Licenses	129
1.1.2 ClusterXL.....	129
1.1.3 Cluster Control Protocol.....	130
1.2 HA and Synchronization.....	130
1.2.1 HA Interfaces.....	130
1.2.2 Synchronization Interfaces.....	131
1.2.3 Synchronization Restrictions.....	132
1.3 HA Design.....	132
1.3.1 Active/Passive Mode.....	133
1.3.2 Load Sharing Multicast Mode	133
1.3.3 Load Sharing Unicast Mode.....	133
1.4 CPHA Commands.....	134
1.4.1 cphaprob.....	134
1.4.2 cphastart/cphastop.....	135
1.4.3 Cluster Member States	135
1.5 Converting an Existing Gateway to a Cluster Member.....	135
1.5.1 Cannot add Member to Cluster.....	135
2 Configuring HA – Active/Passive.....	137
2.1 Clustering – Active/Passive.....	137
2.1.1 Diagram of Cluster Configuration.....	137
2.1.2 Change IP Address of fw.site1.com.....	137
2.1.3 Create the Virtual Machines for Firewalls – fwa, fwb	138
2.1.4 Install SecurePlatform on Firewalls – fwa, fwb.....	139
2.1.5 Create the Firewall Objects fwa & fwb	140
2.1.6 Create the Cluster object – Site1-Cluster.....	141
2.1.7 Create a Base Cluster Security Policy	145
2.1.8 Check Cluster Status and State Table Synchronization.....	146
2.1.9 Testing Cluster Failover.....	147
3 Configuring HA – Load Sharing.....	150
3.1 Clustering – Load sharing, Multicast	150
3.1.1 Edit the Cluster Configuration – Load Sharing Multicast.....	150
3.1.2 Check Load Distribution and Test the Cluster.....	150
3.2 Clustering – Load sharing, Unicast	151

3.2.1 Edit the Cluster Configuration – Load Sharing Unicast.....	151
3.2.2 Check Load Distribution and Test the Cluster.....	151
4 Clusters and VPNs	152
4.1 Site to Site VPN	152
4.1.1 Site2 Firewall Control.....	152
4.1.2 Cluster VPN endpoint IP Address.....	153
4.1.3 VPN Community Setup.....	154
4.1.4 Test the VPN Link, Check SAs using ‘vpn tu’	154
4.2 RemoteAccess VPN.....	157
4.2.1 Office Mode Networks for each Cluster Member	157
4.2.2 Edit the RemoteAccess Community - Add Site1-Cluster	158
4.2.3 Editing Policy with fw.site.com to Site1-Cluster	158
4.2.4 Testing RemoteAccess VPN with a Cluster	159
4.2.5 Cluster Failover and RemoteAccess.....	160
4.2.6 Office Mode IP – ‘fw tab –t om_assigned_ip –f’	161

Module 6 – SmartCenter High Availability 162

1 Management HA	164
1.1 The Management High Availability Solution	164
1.1.1 The Need for Management HA	164
1.1.2 The Secondary SmartCenter	165
1.1.3 What Data is Stored on the Standby SmartCenter	166
1.1.4 Synchronization Methods & Status	166
2 Configuring Management HA	167
2.1 Configuring Management HA – Secondary SmartCenter.....	167
2.1.1 Virtual Machines and Network Diagram.....	167
2.1.2 Checking Connectivity for all the Servers & Firewalls.....	168
2.1.3 Installing the Secondary SmartCenter – 10.2.2.1	169
2.1.4 SmartCenter Object – Gateway or Host.....	170
2.1.5 Synchronization of Primary and Secondary.....	172
2.1.6 Changing the Status of the Primary	172
2.1.7 Testing Policy Changes & Installs by the Standby SmartCenter..	173
2.1.8 Site1 Cluster Install Problem from the Secondary – FW IP’s	174
2.1.9 Recovering the Primary – Checking Synchronization	175
2.1.10 Management HA Collision State	175
2.1.11 Resetting SIC from the Standby SmartCenter – Cluster Member.....	