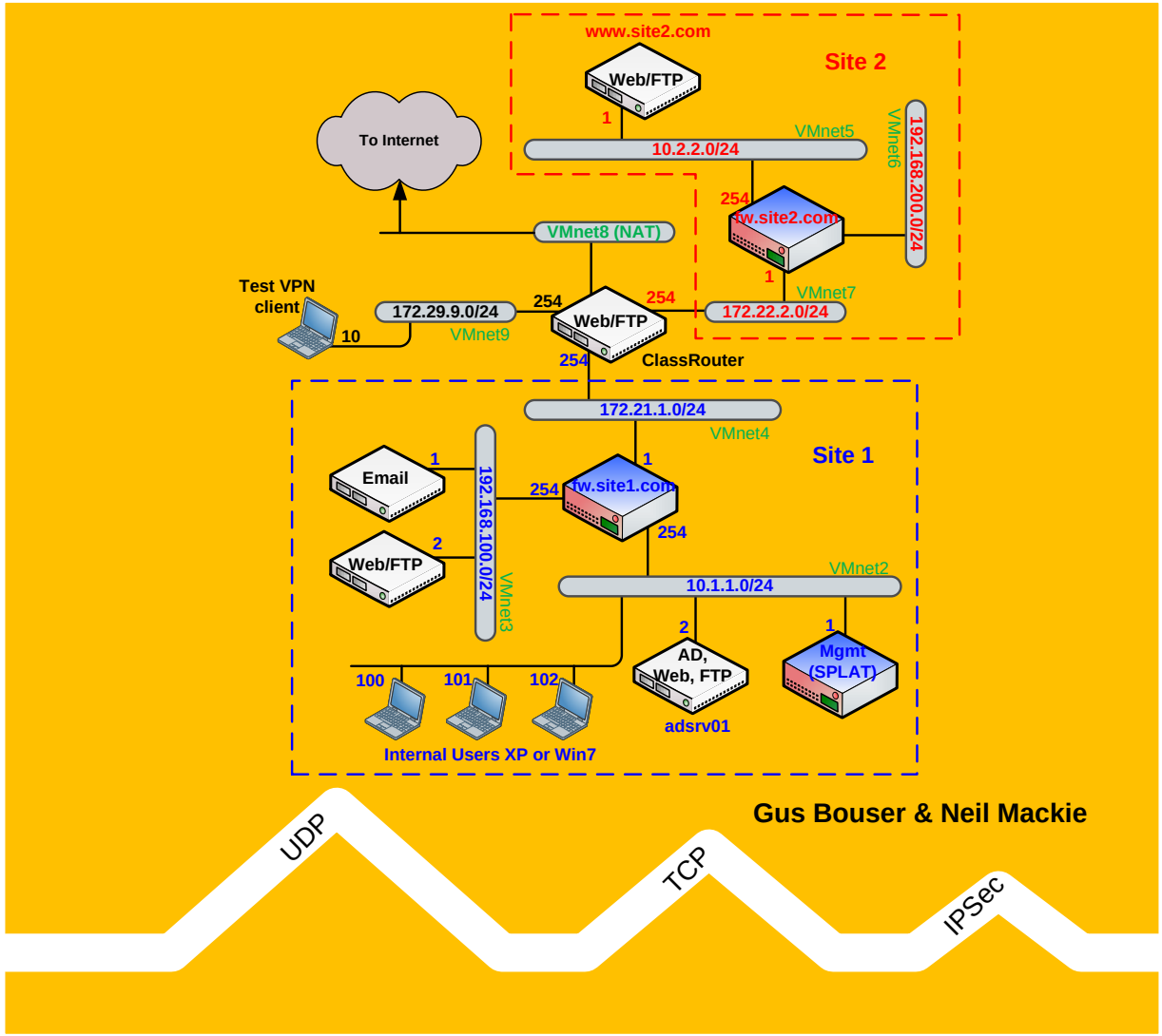
Check Point R75
Management Essentials - Part 2

Training course materials
Preparation for CCSE Certification



Printed and distributed under license from Lezha Publications by ITSec Solutions Ltd.

1 - Encryption

Objectives

- Understand how the Firewall uses symmetric encryption
- Understand how the Firewall uses asymmetric encryption
- Understand the requirement for integrity & authenticity
- Understand the function of the Certificate Authority
- Understand the two phases of IKE
- Know the ports & protocol numbers used by IKE and IPSEC
- Understand the process of establishing a VPN tunnel

Prerequisites

- Complete ‘Check Point Management Essentials - Part 1’ Modules
- VMWare Server or Workstation
- Virtual machines configured
- Base firewalls installed and under SmartCenter control

Approximate time for completing each section

Section 1	Securing Communications	30 Minutes
Section 2	IKE and IPSec	40 Minutes
	Total	1Hr 10 Min

Contents

1 Securing Communications 3
1.1 Symmetric Encryption 3
1.1.1 Encryption Key & Algorithms 3
1.1.2 Symmetric Key Problems 3
1.2 Asymmetric Encryption 4
1.2.1 Asymmetric Keys 4
1.2.2 Asymmetric Key Problems 5
1.3 Diffie-Hellman (DH) 5
1.3.1 DH Special Asymmetric Algorithm 5
1.4 Integrity and Authenticity 7
1.4.1 Integrity Using Hashing Algorithms – MD5/SHA-1 7
1.4.2 Sending a Message using MD5 7
1.4.3 Authenticity Using Digital Signatures - RSA 8
1.5 Certificate Authorities 9
1.5.1 Central & Distributed Authorities 9
1.5.2 Check Point Internal Certificate Authority - ICA 9
1.5.3 Certificate Revocation Lists - CRLs 10
2 IKE and IPSEC 12
2.1 ISAKMP/Oakley - IKE 12
2.1.1 IKE Phase 1 12
2.1.2 IKE Phase 2 12
2.1.3 Encryption & Authentication Algorithms 12
2.1.4 Perfect Forward Secrecy - PFS 13
2.1.5 'vpn debug' & IKEView 13
2.2 IPSec 15
2.2.1 Process of Building a VPN Tunnel 15
2.2.2 Encryption Mode -Tunnel or Transport 16
2.2.3 Encryption and Authentication (Packet Integrity) 16
2.2.4 Packet Integrity Problems & NAT 17

2 - Site to Site VPNS

Objectives

- Know the objects that need to be defined to create a VPN
- Understand the different types of VPN Communities
- Create a Mesh type VPN Community using gateways under your control
- Create a Star type VPN Community using gateways under your control
- Create a Partner site VPN using IKE shared secret authentication
- Create a Partner site VPN using certificate authentication
- Know how to reset and clear VPN tunnels
- Know the common faults in configuring VPNs
- Know how to enable debug logging for VPNs

Prerequisites

- Complete Module 1
- Make sure all Virtual Machines are set to the same date and time

Approximate time for completing each section

Section 1	Check Point VPNs	10 Minutes
Section 2	Current Rules Check	10 Minutes
Section 3	Mesh VPN – Gateways Under your Control	20 Minutes
Section 4	Star VPN – Gateways Under your Control	10 Minutes
Section 5	Start Community – Partners, IKE shared Secrets	40 Minutes
Section 6	Star Community – Partners, Certificates	30 Minutes
Section 7	Common Faults & Debugging	30 Minutes
	Total	2 Hrs 30 Min

Contents

1 Check Point VPNs 4
- 1.1 Types of VPN 4
  - 1.1.1 Intranet – All Gateways Controlled by a Single smartCenter 4
  - 1.1.2 Partner – Different Vendor Devices, Partner Cooperation 4
  - 1.1.3 Gateway Authentication – Shared Secret or Certificate 5
  - 1.1.4 Remote Access VPN 5
- 1.2 Components of a VPN Configuration 6
  - 1.2.1 Gateway Endpoints 6
  - 1.2.2 Encryption Domain – Networks, Hosts 7
  - 1.2.3 Encryption Parameters 8
  - 1.2.4 Remote/Partner - Check Point Gateway or Interoperable Device 9
- 1.3 VPN Communities 9
  - 1.3.1 Mesh Communities 10
  - 1.3.2 Star Communities 10
  - 1.3.3 Remote Access Community 11
- 1.4 VPN Rules 11
  - 1.4.1 Rules with Accept and VPN set to 'Any' still Encrypt 11
  - 1.4.2 Limiting the Rule by Community 12
  - 1.4.3 Limiting the Rule by Source and Destination 12
- 1.5 Directional VPNs 12
  - 1.5.1 Enabling Directional VPNs 12
  - 1.5.2 Directional Rule Match Conditions 12
- 1.6 Resetting VPN Tunnels – 'vpn tunnelutil' 13
  - 1.6.1 Resetting tunnels 13
- 1.7 Tunnel Monitoring – Alerts 13

2 Current Rules Check 14
- 2.1 Network Diagram 14
- 2.2 Firewall Control and Rules Check 14
  - 2.2.1 Create a New Policy – 'Site1_P2_Module2' 14
  - 2.2.2 Base Rules 15

3 Creating a Mesh VPN – Gateways Under Your Control 17
- 3.1 Setting Up the Local Endpoint Details 17
  - 3.1.1 Define the Local Gateway Encryption Domain 17
  - 3.1.2 Set the Local Gateway Properties 17
- 3.2 Setting Up the Remote Endpoint Details 18
  - 3.2.1 Define the Remote Gateway Encryption Domain 18
  - 3.2.2 Set the Remote Gateway Properties 18
- 3.3 Create the Mesh Community 18
  - 3.3.1 Create the Mesh Community & Add the Gateways 18
  - 3.3.2 Set the Mesh Community Properties 19
- 3.4 Create the Security & NAT rules for the VPN 21
  - 3.4.1 Network Address Translation and VPNs 21
  - 3.4.2 Single Rule – Testing the Any Rule 21
  - 3.4.3 Single Rule – VPN Community restricted 22
  - 3.4.4 Multiple Rules – Network to Network Restricted 23
  - 3.4.5 Multiple Rules – Source & Destination Restricted 23
  - 3.4.6 Add the firewall Admin rule 23

4 Star Community VPN – Gateways Under your Control 25
- 4.1 Create the Star Community 25
- 4.2 Testing the Star Community VPN 27

5 Star Community VPN – Partners, IKE Shared Secrets 28
- 5.1 Changing fw.site2.com – Independently Managed 28
  - 5.1.1 Remove fw.site2.com from the SmartCenter Objects for Site1 28
  - 5.1.2 Install the new SmartCenter for fw-site2 on Server 10.2.2.1 29
  - 5.1.3 Reset the SIC Communications on fw.site2.com 30
  - 5.1.4 Complete Installation of SmartCenter for Site2 31
  - 5.1.5 Possible Connection Errors to New SmartCenter 31
  - 5.1.6 Create the Basic Objects for Site2 in the new SmartCenter 32
  - 5.1.7 Create a Basic Policy and install on fw.site2.com 33
- 5.2 SmartCenter for Site1 - Local Endpoint Setup 33
- 5.3 SmartCenter for Site1 - Remote Endpoint Setup 33
  - 5.3.1 Create an Interoperable Device Object called fw.site2.com 33
  - 5.3.2 Set the Encryption Domain in the Topology Tab 33
- 5.4 SmartCenter for Site1 – Create the Star VPN Community 34
  - 5.4.1 Create the Star Community – VPN-PartnerSite2 34
  - 5.4.2 Set the Encryption Parameters 35
  - 5.4.3 Set the IKE shared Secret 35
- 5.5 SmartCenter for Site1 – Create the VPN Rules 36
  - 5.5.1 Add the VPN rules for Site1 36
- 5.6 SmartCenter for Site2 - Local Endpoint Setup 37
- 5.7 SmartCenter for Site2 - Remote Endpoint Setup 37

5.7.1 Create an Interoperable Device Object called fw.site1.com 37
5.7.2 Set the Encryption Domain for the Partner Site 37
5.8 SmartCenter for Site2 – Create the Star VPN Community 37
5.8.1 Create the Star Community – VPN-PartnerSite1 37
5.8.2 Set the Encryption Parameters 38
5.8.3 Set the IKE shared Secret 38
5.9 SmartCenter for Site2 – Create the VPN Rules 38
5.9.1 Add the VPN rules 38
5.10 Testing the Partner VPN Using Shared Secret Authentication 39
5.10.1 Test Access using FTP 39
6 Star Community VPN – Partners, Certificates 40
6.1 Certificate Relationship ICA and Gateway 40
6.1.1 The ICA Server 40
6.1.2 The Gateway Certificate 40
6.1.3 Certificate Revocation Lists (CRLs) 41
6.2 Changing from Shared Secret to Certificate Authentication 41
6.2.1 Export the Site1 CA Certificate 41
6.2.2 Install the Site1 CA Certificate on SmartCenter Site2 42
6.2.3 Export the Site2 CA Certificate 43
6.2.4 Install the Site2 CA Certificate on SmartCenter Site1 43
6.2.5 Change the Community to use Certificates for Site1 44
6.2.6 Change the Community to use Certificates for Site2 44
6.2.7 Install the Policy for Site1 and Site2 44
6.2.8 Reset all VPN tunnels 44
6.2.9 Test the VPN Community using Certificate Authentication 45
6.2.10 Fetching the Internal CA using port 18264 45
7 Common Faults and Debugging 46
7.1 VPNs Common Faults 46
7.1.1 Common Faults 46
7.2 VPN Log Files & IKEView 47
7.2.1 Using IKEView 47

3 - Remote Access VPNs - SecureClient

Objectives

- Understand the importance of Office Mode
- Use Office Mode and the options for allocating an IP Address
- Know how to define a RemoteAccess VPN
- Know how to install Endpoint Security VPN Client
- Know how to create VPN client sites
- Know how to use certificate authentication for users
- Know how to use Endpoint Security (SecureClient) without Desktop rules
- Know the main configuration file for Endpoint Security, Track.default, Track.config,
- Understand the importance of encrypting the Track.config file
- Know how to write Desktop Security rules
- Understand the need for UDP encapsulation and Visitor Mode
- Know how to use the SecureClient packaging tool

Prerequisites

- Complete Module 2
- The following Virtual machines should be running, mgmt-Site1, fw-Site1, ClassRouter, Host1, ADSRV01 & vpnclient

Approximate time for completing each section

Section 1	Rules Check	10 Minutes
Section 2	Remote Access VPNs	10 Minutes
Section 3	Configuring Remote Access VPNs	25 Minutes
Section 4	Installing Endpoint Security VPN client	10 Minutes
Section 5	Using Endpoint Security VPN – No Desktop Policy	25 Minutes
Section 6	Using Endpoint Security VPN – With a Desktop Policy	25 Minutes
Section 7	SecureClient Packaging Tool	35 Minutes
	Total	2 Hr 10 Mins

E75.10 Endpoint Security VPN replaces SecureClient

Contents

1 Rules Check 4
- 1.1 New Policy and Rules 4
  - 1.1.1 Create a new Policy Package 4
  - 1.1.2 Create and Install the Base Rules 4

2 Remote Access VPNs 5
- 2.1 RemoteAccess Community 5
- 2.2 Virtual Desktop Infrastructure 5
  - 2.2.1 Gateway Encryption Domain 5
  - 2.2.2 User Groups 6
- 2.3 SecuRemote Client or SecureClient 6
  - 2.3.1 SecureClient License, EndPoint Security Blade 6
  - 2.3.2 Desktop Protection 7
- 2.4 Office Mode 7
  - 2.4.1 Why Use Office Mode 7
  - 2.4.2 How Office Mode Works 8
  - 2.4.3 Office Mode IP address, Config file, Network Pool, DHCP 8
  - 2.4.4 Alternative to Office Mode – Gateway IP Pools 9
- 2.5 UDP Encapsulation & Visitor Mode 10
  - 2.5.1 VPN1_IPSEC_encapsulation, Port 2746 10
  - 2.5.2 NAT-T, Port 4500 10
  - 2.5.3 Visitor Mode, Port 443 10

3 Configuring RemoteAccess VPNs 12
- 3.1 User, Groups and Authentication 12
  - 3.1.1 Create the VPN User Groups 12
  - 3.1.2 User Authentication 13
  - 3.1.3 Create VPN Users 14
  - 3.1.4 Set the Gateway RemoteAccess Encryption Domain 15
  - 3.1.5 Configure the RemoteAccess Community 15
  - 3.1.6 Policy, Global Properties - RemoteAccess 15
  - 3.1.7 Check Point Gateway – RemoteAccess Properties 18
  - 3.1.8 Configure Office Mode 18
  - 3.1.9 Wireless Hotspot/Hotel Registration 19
  - 3.1.10 Add Remote Access Rules to the Security Policy 19

4 Installing Endpoint Security VPN Client 21
- 4.1 Endpoint Security Client Installation 21
  - 4.1.1 With or Without Desktop Protection 21
  - 4.1.2 Endpoint Security Secure Access 21
- 4.2 Post Installation Checks 22
  - 4.2.1 Device Driver Check Point SecuRemote 22
  - 4.2.2 Endpoint Security – Show Client 23
  - 4.2.3 EndPoint Security Configuration Files – Trac.defaults, Trac.config 23

5 Using Endpoint Security VPN – No Desktop Policy 24
- 5.1 Creating a Site 24
  - 5.1.1 Site IP Address and Name 24
  - 5.1.2 Authentication Method 26
- 5.2 Testing Remote Access 27
  - 5.2.1 Connecting to the Gateway 27
  - 5.2.2 Office Mode IP Address Assigned 28
  - 5.2.3 Testing the Rules 29
  - 5.2.4 Trac.config file unencrypted 30
- 5.3 Basic Problems and Debugging 31
  - 5.3.1 Global Properties – Accept Remote Access Control Connections 31
  - 5.3.2 Is the Site Correctly Defined – 'Trac.config' 32
  - 5.3.3 Do not Clone Endpoint Security Laptops 32
  - 5.3.4 Multiple VPN Clients and Local Firewall 32
  - 5.3.5 Overlapping Sites 32
  - 5.3.6 Built in Packet Sniffer SecureClient only - 'srfw monitor' 32
  - 5.3.7 Turning on Debugging for Endpoint Security 33
  - 5.3.8 Debugging SecureClient IKE Phase 1 & 2 33

6 Using Endpoint Security VPN – With a Desktop Policy 35
- 6.1 Enabling the Policy Server 35
  - 6.1.1 Enable Policy Server on the Firewall Module 35
  - 6.1.2 Set the Policy Server User Group 35
- 6.2 Writing Desktop Rules 36
  - 6.2.1 Inbound Rules 36
  - 6.2.2 Outbound Rules 36
  - 6.2.3 Installing Desktop Rules 37
- 6.3 Updating the Remote Access Site – Endpoint Security 37
  - 6.3.1 Site Update 37
  - 6.3.2 The Installed Rules 37
  - 6.3.3 Testing the Desktop Rules 37

6.3.4 Different Users, Different Rules 37
6.3.5 Outbound Desktop Rule for Updates 38
6.4 Remote Support for VPN Users 38
6.4.1 Enable Back Connections 38
6.4.2 Testing Remote Support 38
6.5 Using Visitor Mode – Tunnel over HTTPS 39
6.5.1 Check the WebGui is not using port 443 39
6.5.2 Enable Visitor Mode on the Gateway 39
7 SecureClient Packaging Tool 40
7.1 Building Pre-packaged Configuration for Easy Deployment 40
7.1.1 Overview 40
7.1.2 Creating a Package Profile 40

4 - Clientless VPNs – Secure Network Extender

Objectives

- Know how to enable SNX support on the Firewall
- Know how to set SNX Global properties
- Know how to configure Clientless VPNs
- Know how to control access for Clientless VPN users
- Know how to use user Certificate Authentication with SNX

Prerequisites

- Complete Module 3 RemoteAccess VPNs

Approximate time for completing each section

Section 1	SSL Network Extender	20 Minutes
Section 2	Configuring Clientless VPNs	45 Minutes
	Total	1 Hr 5 Min

Contents

1 SSL Network Extender - SNX 3
- 1.1 SSL Network Extender 3
  - 1.1.1 Network Extender License Requirements 3
  - 1.1.2 How SSL Network Extender Works 3
- 1.2 Configuration Requirements 3
  - 1.2.1 Enable Gateway for Clientless VPNS 3
  - 1.2.2 Users & Groups for Authentication 4
  - 1.2.3 SSL Authentication and Encryption Options 4
  - 1.2.4 Remote Access VPN rule 5
  - 1.2.5 Supported Platforms and Web Browsers 5

2 Configuring Clientless VPNs 6
- 2.1 SSL Network Extender 6
  - 2.1.1 Check the Clientless Global Properties Settings 6
  - 2.1.2 Gateway Properties 6
  - 2.1.3 Check the Security Rules 7
  - 2.1.4 SNX and SecureClient on the same Desktop 7
  - 2.1.5 Check that the 'vpnd' is running on port 443 7
- 2.2 Testing SSL Network Extender 8
  - 2.2.1 Connecting to the Gateway – Authentication 8
  - 2.2.2 Thin client Download and Install 9
  - 2.2.3 Connecting to Internal Networks 10
  - 2.2.4 User Certificate Authentication with SNX 11

5 - High Availability – Firewall Clusters

Objectives

- Understand the requirement for ClusterXL
- Understand the importance of the synchronization network
- Understand the problems with adding existing firewalls to a cluster object
- Know how to configure ClusterXL for an Active/Passive HA
- Know how to configure ClusterXL for a Load Sharing HA
- Know how to configure Client VPNs with HA

Prerequisites

- Complete Module 4

Approximate time for completing each section

Section 1	Firewall HA	40 Minutes
Section 2	Configuring HA – Active/Passive	85 Minutes
Section 3	Configuring HA – Load Sharing	30 Minutes
Section 4	Clusters and VPNs	60 Minutes
	Total	3 Hrs 35 Min

Contents

1 Firewall High Availability 3
- 1.1 Firewall HA 3
  - 1.1.1 Firewall Licenses 3
  - 1.1.2 ClusterXL 3
  - 1.1.3 Cluster Control Protocol 4
- 1.2 HA and Synchronization 4
  - 1.2.1 HA Interfaces 4
  - 1.2.2 Synchronization Interfaces 5
  - 1.2.3 Synchronization Restrictions 6
- 1.3 HA Design 6
  - 1.3.1 Active/Passive Mode 7
  - 1.3.2 Load Sharing Multicast Mode 7
  - 1.3.3 Load Sharing Unicast Mode 7
- 1.4 CPHA Commands 8
  - 1.4.1 cphaprob 8
  - 1.4.2 cphastart/cphastop 9
  - 1.4.3 Cluster Member States 9
- 1.5 Converting an Existing Gateway to a Cluster Member 9
  - 1.5.1 Cannot add Member to Cluster 9

2 Configuring HA – Active/Passive 11
- 2.1 Clustering – Active/Passive 11
  - 2.1.1 Diagram of Cluster Configuration 11
  - 2.1.2 Change IP Address of fw.site1.com 11
  - 2.1.3 Create the Virtual Machines for Firewalls – fwa, fwb 12
  - 2.1.4 Install SecurePlatform on Firewalls – fwa, fwb 13
  - 2.1.5 Create the Firewall Objects fwa & fwb 14
  - 2.1.6 Create the Cluster object – Site1-Cluster 15
  - 2.1.7 Create a Base Cluster Security Policy 19
  - 2.1.8 Check Cluster Status and State Table Synchronization 20
  - 2.1.9 Testing Cluster Failover 21

3 Configuring HA – Load Sharing 24
- 3.1 Clustering – Load sharing, Multicast 24
  - 3.1.1 Edit the Cluster Configuration – Load Sharing Multicast 24
  - 3.1.2 Check Load Distribution and Test the Cluster 24
- 3.2 Clustering – Load sharing, Unicast 25
  - 3.2.1 Edit the Cluster Configuration – Load Sharing Unicast 25
  - 3.2.2 Check Load Distribution and Test the Cluster 25

4 Clusters and VPNs 26
- 4.1 Site to Site VPN 26
  - 4.1.1 Site2 Firewall Control 26
  - 4.1.2 Cluster VPN endpoint IP Address 27
  - 4.1.3 VPN Community Setup 28
  - 4.1.4 Test the VPN Link, Check SAs using 'vpn tu' 28
- 4.2 RemoteAccess VPN 31
  - 4.2.1 Office Mode Networks for each Cluster Member 31
  - 4.2.2 Edit the RemoteAccess Community - Add Site1-Cluster 32
  - 4.2.3 Editing Policy with fw.site.com to Site1-Cluster 32
  - 4.2.4 Testing RemoteAccess VPN with a Cluster 33
  - 4.2.5 Cluster Failover and RemoteAccess 34
  - 4.2.6 Office Mode IP – 'fw tab –t om_assigned_ip –f' 35

6 - High Availability - SmartCenters

Objectives

- Know the requirements for management HA
- Understand the role of the Primary and Secondary SmartCenter
- Know how to configure SmartCenter HA
- Understand the different states of Management synchronization
- Understand how logging works in Management HA
- Know how to handle a ‘Collision’ state

Prerequisites

- Complete Module 5

Approximate time for completing each section

Section 1	Management HA	20 Minutes
Section 2	Configuring Management HA	80 Minutes
	Total	1 Hr 40 Min

Contents

1 Management HA 3

1.1 The Management High Availability Solution 3

1.1.1 The Need for Management HA 3

1.1.2 The Secondary SmartCenter 4

1.1.3 What Data is Stored on the Standby SmartCenter 5

1.1.4 Synchronization Methods & Status 5

2 Configuring Management HA 6

2.1 Configuring Management HA – Secondary SmartCenter 6

2.1.1 Virtual Machines and Network Diagram 6

2.1.2 Checking Connectivity for all the Servers & Firewalls 7

2.1.3 Installing the Secondary SmartCenter – 10.2.2.1 8

2.1.4 SmartCenter Object – Gateway or Host 9

2.1.5 Synchronization of Primary and Secondary 11

2.1.6 Changing the Status of the Primary 11

2.1.7 Testing Policy Changes & Installs by the Standby SmartCenter 12

2.1.8 Site1 Cluster Install Problem from the Secondary – FW IP's 13

2.1.9 Recovering the Primary – Checking Synchronization 14

2.1.10 Management HA Collision State 14

2.1.11 Resetting SIC from the Standby SmartCenter – Cluster Member 14

