

### 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 SecureClient
- Know how to create VPN client sites
- Know how to use certificate authentication for users
- Know how to use SecureClient without Desktop rules
- Know the main configuration file for SecureClient, userc.C
- 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, MgmtSite1, fwsite1, classrouter & vpnclient

#### Approximate time for completing each section

<b>Section 1</b>	Rules Check	10 minutes
<b>Section 2</b>	Remote Access VPNs	10 minutes
<b>Section 3</b>	Configuring Remote Access VPNs	25 Minutes
<b>Section 4</b>	Installing SecureClient	10 Minutes
<b>Section 5</b>	Using SecureClient – No Desktop Policy	25 Minutes
<b>Section 6</b>	Using SecureClient – With a Desktop Policy	25 Minutes
<b>Section 7</b>	SecureClient Packaging Tool	35 Minutes
	Total	2 Hr 10 mins

## Contents

<b>1 Rules Check</b> .....	<b>4</b>
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
<b>2 Remote Access VPNs</b> .....	<b>5</b>
2.1 RemoteAccess Community.....	5
2.1.1 Gateway Encryption Domain.....	5
2.1.2 User Groups.....	5
2.2 SecuRemote or SecureClient.....	6
2.2.1 SecureClient License.....	6
2.2.2 Desktop Protection.....	6
2.3 Office Mode.....	6
2.3.1 Why Use Office Mode.....	6
2.3.2 How Office Mode Works.....	7
2.3.3 Office Mode IP address, Config file, Network Pool, DHCP.....	7
2.3.4 Alternative to Office Mode – Gateway IP Pools.....	8
2.4 UDP Encapsulation & Visitor Mode.....	9
2.4.1 VPN1_IPSEC_encapsulation, Port 2746.....	9
2.4.2 NAT-T, Port 4500.....	9
2.4.3 Visitor Mode, Port 443.....	9
<b>3 Configuring RemoteAccess VPN</b> .....	<b>10</b>
3.1 User, Groups and Authentication.....	10
3.1.1 Create the VPN User Groups.....	10
3.1.2 User Authentication.....	10
3.1.3 Create VPN Users.....	11
3.1.4 Set the Gateway RemoteAccess Encryption Domain.....	13
3.1.5 Configure the RemoteAccess Community.....	13
3.1.6 Policy, Global Properties - RemoteAccess.....	13
3.1.7 Check Point Gateway – RemoteAccess Properties.....	15
3.1.8 Configure Office Mode.....	15
3.1.9 Wireless Hotspot/Hotel Registration.....	16
3.1.10 Add Remote Access Rules to the Security Policy.....	16
<b>4 Installing SecureClient</b> .....	<b>17</b>
4.1 SecureClient Installation.....	17

4.1.1 With or Without Desktop Protection – Always with.....	17
4.2 Post Installation Checks.....	18
4.2.1 Device Driver Enabled.....	18
4.2.2 Automatic Start.....	18
4.2.3 SecureClient Diagnostic Tools.....	18
4.2.4 Configuration File – userc.C.....	19
<b>5 Using SecureClient – No Desktop Policy</b> .....	<b>21</b>
5.1 Creating a Site.....	21
5.1.1 Site IP Address and Name.....	21
5.1.2 Authentication Method.....	21
5.1.3 Exchange of Site Certificate.....	22
5.2 Post Site Creation Checks.....	23
5.2.1 Checking Site Properties.....	23
5.2.2 Checking the userc.C.....	24
5.3 Testing Remote Access.....	28
5.3.1 Connecting to the Gateway.....	28
5.3.2 Office Mode IP Address Assigned.....	29
5.3.3 Testing the Rules.....	30
5.4 Basic Problems and Debugging.....	30
5.4.1 Global Properties – Accept Remote Access Control Connections.....	31
5.4.2 Is the Site Correctly Defined – ‘userc.C’.....	31
5.4.3 Do not Clone SecureClient Laptops.....	31
5.4.4 Multiple VPN Clients and Local Firewall.....	31
5.4.5 Overlapping Sites.....	31
5.4.6 Built in Packet Sniffer - ‘srfw monitor’.....	31
5.4.7 Turning on Debugging for SecureClient.....	32
5.4.8 Debugging SecureClient IKE Phase 1 & 2.....	33
<b>6 Using SecureClient – With a Desktop Policy</b> .....	<b>35</b>
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.....	35
6.2.1 Inbound Rules.....	35
6.2.2 Outbound Rules.....	36
6.2.3 Installing Desktop Rules.....	36
6.3 Updating the Remote Access Site - SecureClient.....	36
6.3.1 Site Update.....	36

6.3.2	<i>Checking the Installed Rules</i> .....	37
6.3.3	<i>Testing the Desktop Rules</i> .....	37
6.3.4	<i>Different Users, Different Rules</i> .....	37
6.3.5	<i>Outbound Desktop Rule for Updates</i> .....	38
6.4	<i>Remote Support for VPN Users</i> .....	38
6.4.1	<i>Enable Back Connections</i> .....	38
6.4.2	<i>Testing Remote Support</i> .....	39
6.5	<i>Using Visitor Mode – Tunnel over HTTPS</i> .....	39
6.5.1	<i>Check the WebGui is not using port 443</i> .....	39
6.5.2	<i>Enable Visitor Mode on the Gateway</i> .....	39
6.5.3	<i>Enable Visitor Mode - Desktop Client</i> .....	39
6.5.4	<i>Test Visitor Mode</i> .....	40
<b>7</b>	<b><i>SecureClient Packaging Tool</i></b> .....	<b>42</b>
7.1	<i>Building Pre-packaged Configuration for Easy Deployment</i> .....	42
7.1.1	<i>Overview</i> .....	42
7.1.2	<i>Creating a Package Profile</i> .....	42
7.1.3	<i>Creating a Package</i> .....	46