



## Avaya Solution & Interoperability Test Lab

---

# Application Notes for Configuring Client VPN Tunnels from Avaya Phone Manager Pro to the WatchGuard Firebox X and SOHO Products – Issue 1.0

### Abstract

These Application Notes cover the configuration of client VPN (Virtual Private Network) tunnels from Avaya Phone Manager Pro to the WatchGuard Firebox X and SOHO products. Avaya Phone Manager Pro clients use the WatchGuard Mobile User VPN (MUVPN) software to establish the VPN tunnels. This configuration does not cover QoS (Quality of Service) implementation to prioritize voice traffic. Information in these Application Notes has been obtained through compliance testing and additional technical discussions. Testing was conducted via the Developer*Connection* Program at the Avaya Solution and Interoperability Test Lab.

# 1. Introduction

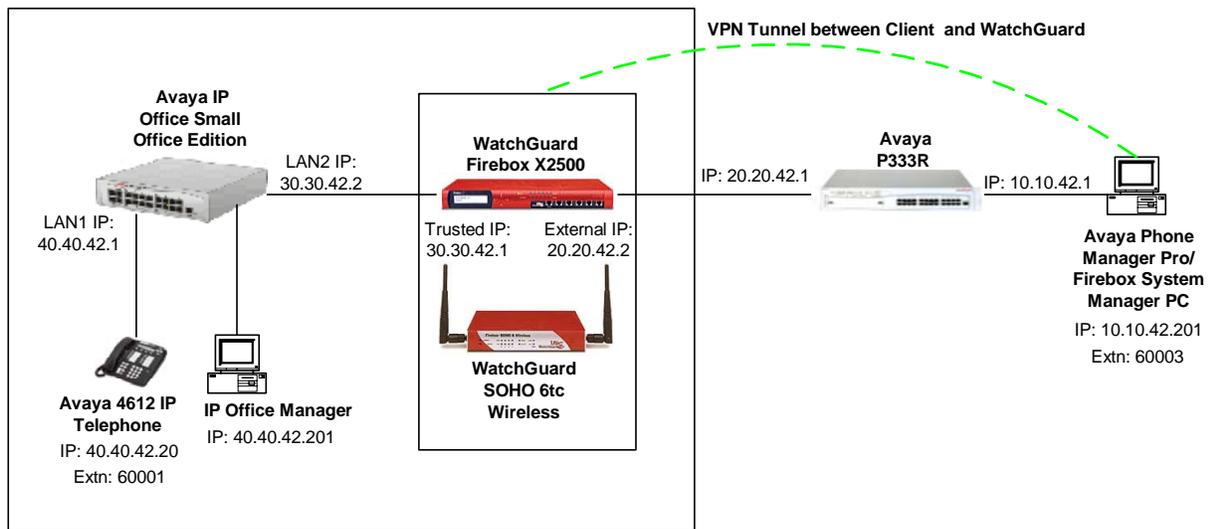
These Application Notes cover the configuration of client VPN (Virtual Private Network) tunnels from Avaya Phone Manager Pro to the WatchGuard Firebox X and SOHO products. Avaya Phone Manager Pro clients use the WatchGuard Mobile User VPN (MUVPN) software to establish the VPN tunnels. This configuration does not cover QoS (Quality of Service) implementation to prioritize voice traffic.

The Firebox X2500 is an integrated security appliance for small and medium enterprises that combines firewall, VPN, application proxies (HTTP, SMTP, FTP, etc.) web content filtering, anti-virus, anti-spam, and secure remote management.

The SOHO 6tc Wireless is an integrated security appliance for the small office/home office/teleworker that combines firewall, VPN, web content filtering, anti-virus, and secure remote management.

In **Figure 1**, Client VPN tunnels will be established between the FireBox X or SOHO product and the MUVPN client running on the Phone Manager Pro PC. The WatchGuard X2500 and SOHO 6tc Wireless were tested separately. The same IP addresses were assigned to the external and trusted interfaces of both devices.

For configuration of the network infrastructure shown in **Figure 1**, refer to the appropriate documentation listed in Section 8.



**Figure 1 – Network Configuration Diagram**

In order to establish an IPsec (IP Security) VPN tunnel, two phases have to be negotiated successfully. Phase 1 or IKE (Internet Key Exchange) is used for authentication and Phase 2 or (IPsec) is used for encryption. The following tunnel configuration will be used in these Application Notes:

<b>Tunnel Type</b>	<b>IKE Exchange Type</b>	<b>Encryption Method</b>	<b>Password Authentication</b>	<b>Diffie-Hellman Group</b>	<b>Encryption Protocol</b>
Client	Aggressive	3DES	SHA	2	ESP

**Table 1 – IPsec Tunnel Configuration**

## 2. Equipment and Software Validated

The following products and software were used for the configuration in **Figure 1**:

<b>Equipment</b>	<b>Version</b>
Avaya IP Office Small Office Edition/IP Office Manager	2.1 (15)
Avaya P333R Stackable Switch	4.0.9
Avaya 4612 IP Telephone	1.8.2
Avaya Phone Manager Pro	2.1.7
WatchGuard Firebox X2500/Firebox System Manager	7.21.B1596
WatchGuard SOHO 6tc Wireless	6.3 Build 19

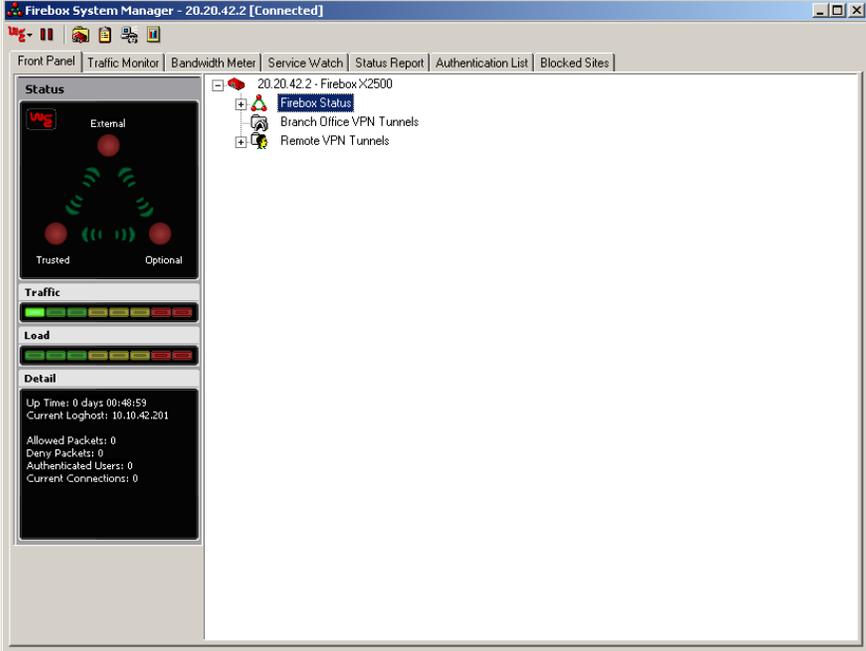
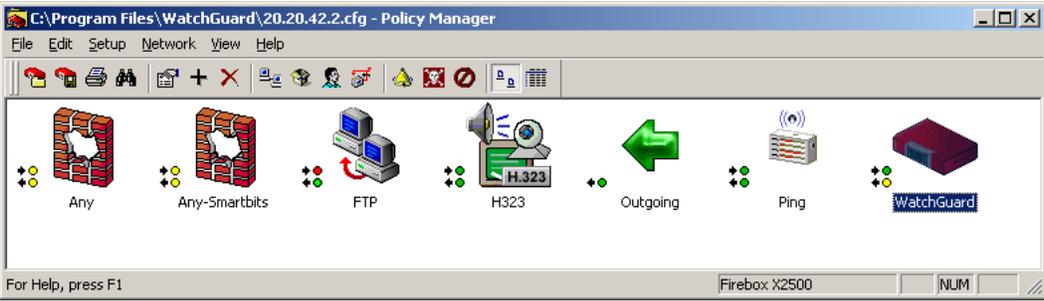
**Table 2 – Product and Software/Version**

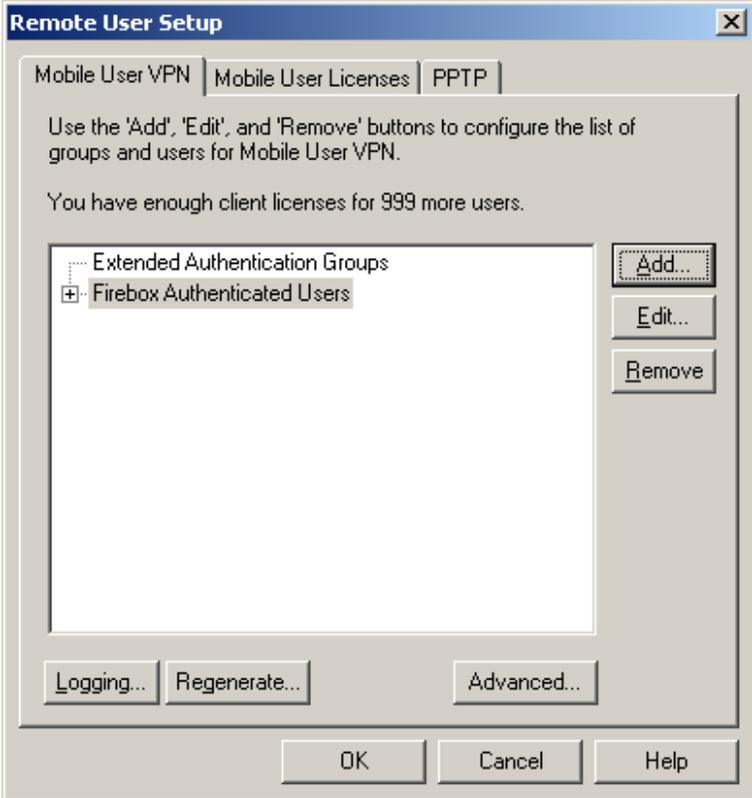
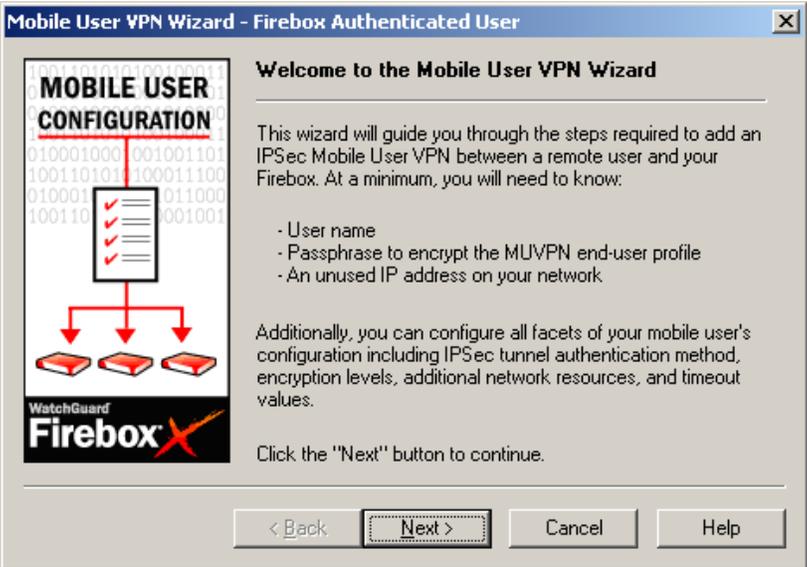
### 3. Configuring Phone Manager Pro

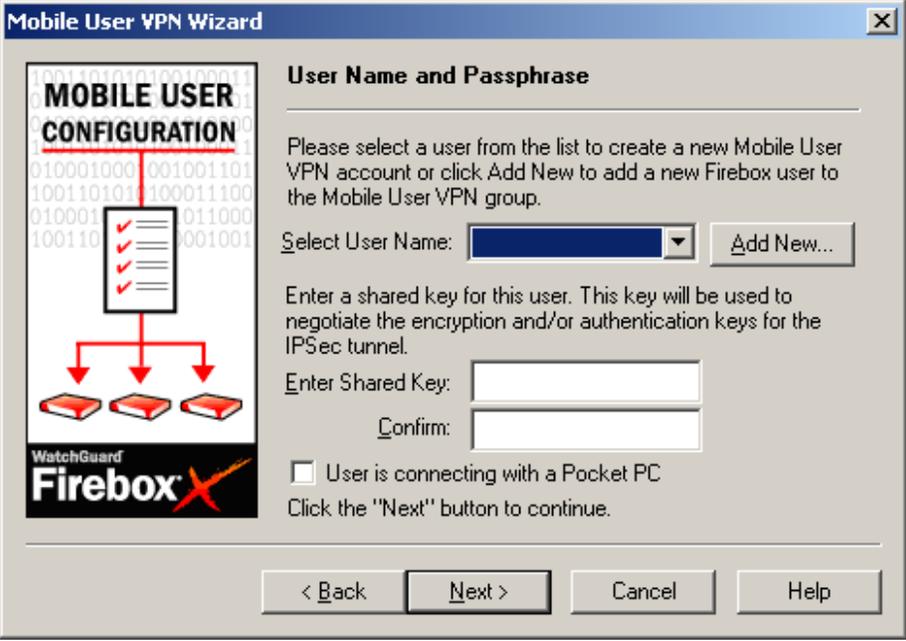
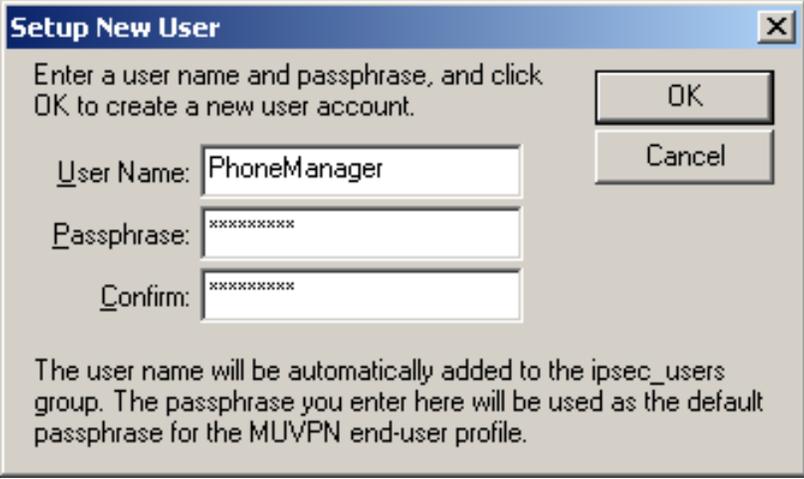
Step	Description
1.	<p>Click <b>Start</b> → <b>Programs</b> → <b>IP Office</b> → <b>PhoneManager</b> to start the PhoneManager Pro application. Click <b>Configure</b> → <b>PBX</b> and specify the LAN2 interface address for IP Office (e.g., <b>30.30.42.2</b>) in the <i>PBX Address</i> field. Select the name defined on the <b>User</b> form in IP Office Manager (e.g., <b>Extn60003</b>) in the <i>UserName</i> field. Click the <b>Login</b> button and check the <i>Login/Logout</i> checkbox. Select the extension (e.g., <b>60003</b>) to be used by Phone Manager in the <i>Base Extension</i> field.</p> 

## 4. Configuring VPN Tunnel between Client and WatchGuard

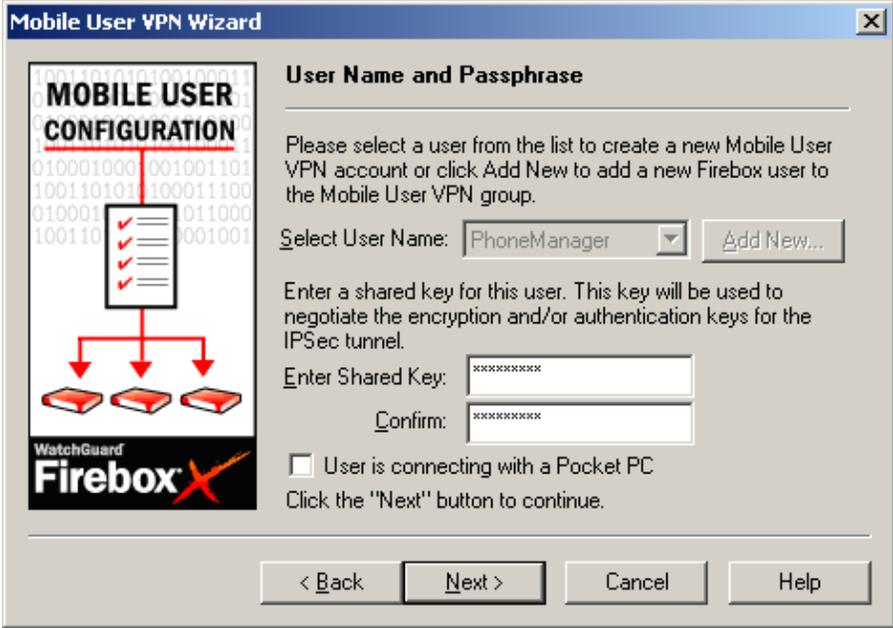
### 4.1. Configure the WatchGuard Firebox X

Step	Description
1.	<p>Log into the Firebox X by navigating to <b>Start</b> → <b>Programs</b> → <b>WatchGuard</b> → <b>Firebox System Manager</b> from the Firebox System Manager PC.</p>  <p>Select <b>Tools</b> → <b>Policy Manager</b> or click on the  taskbar icon.</p>
2.	<p>Click on <b>Network</b> → <b>Remote User...</b> to add a new MUVPN client for Phone Manager Pro.</p> 

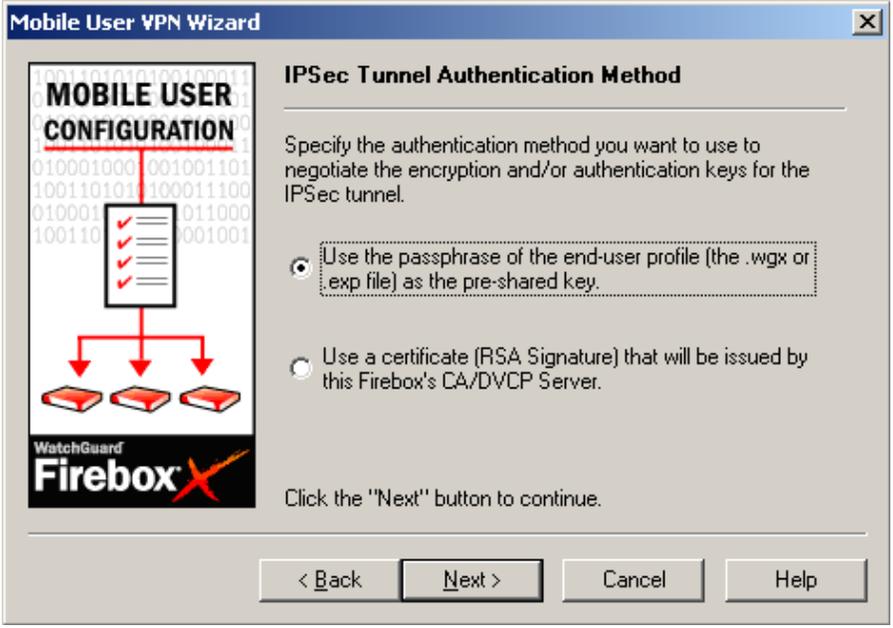
Step	Description
3.	<p>Select <b>Firebox Authenticated Users</b> and click <b>Add</b>.</p>  <p>The screenshot shows the 'Remote User Setup' dialog box with the 'Mobile User VPN' tab active. It includes instructions on using 'Add', 'Edit', and 'Remove' buttons. A message states 'You have enough client licenses for 999 more users.' The 'Extended Authentication Groups' list has 'Firebox Authenticated Users' selected. The 'Add...' button is highlighted with a dashed border.</p>
4.	<p>Click <b>Next</b> to use the Mobile User VPN Wizard to configure the VPN tunnel for the MUVPN client.</p>  <p>The screenshot shows the 'Mobile User VPN Wizard - Firebox Authenticated User' dialog box. It features a 'MOBILE USER CONFIGURATION' graphic on the left and a 'Welcome to the Mobile User VPN Wizard' message on the right. The 'Next &gt;' button is highlighted with a dashed border.</p>

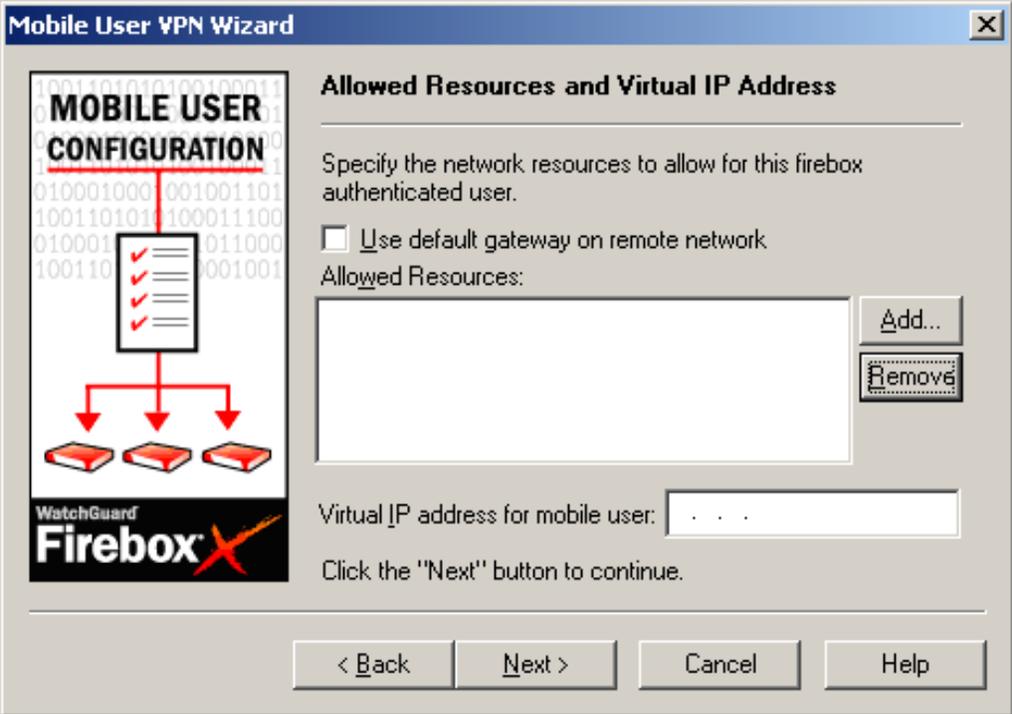
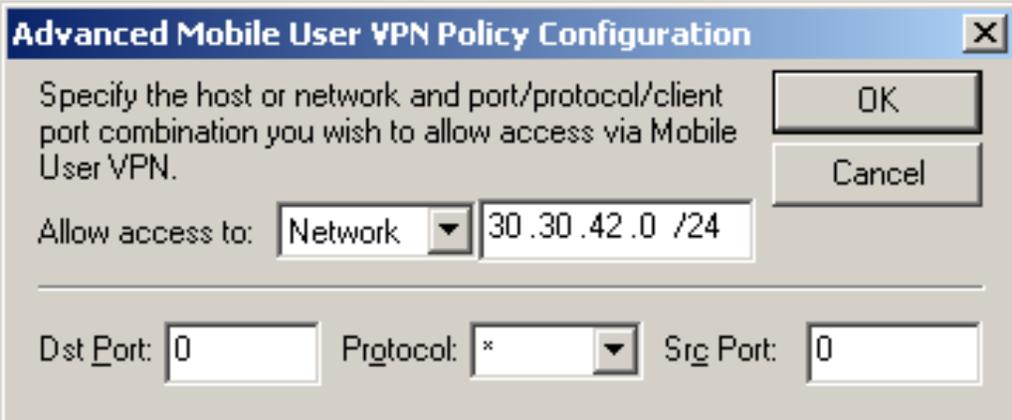
Step	Description
5.	<p>Click <b>Add New...</b> to add a new mobile user VPN account.</p> 
6.	<p>Enter the <i>User Name</i> and <i>Passphrase</i> to be used by the MUVPN client as the shared key for Phase 1 authentication. This user will be automatically added to the ipsec_users group. Click <b>OK</b>.</p> 

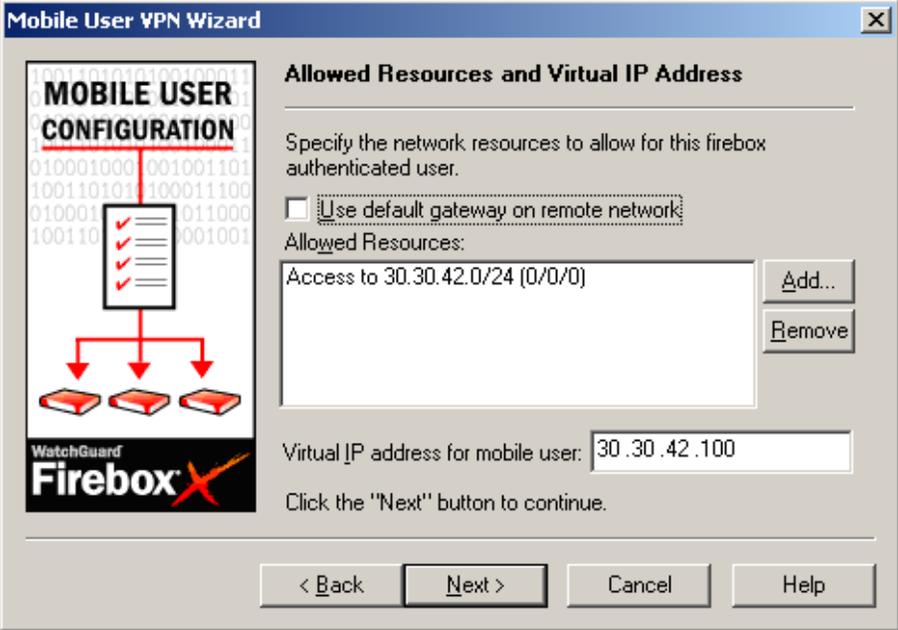
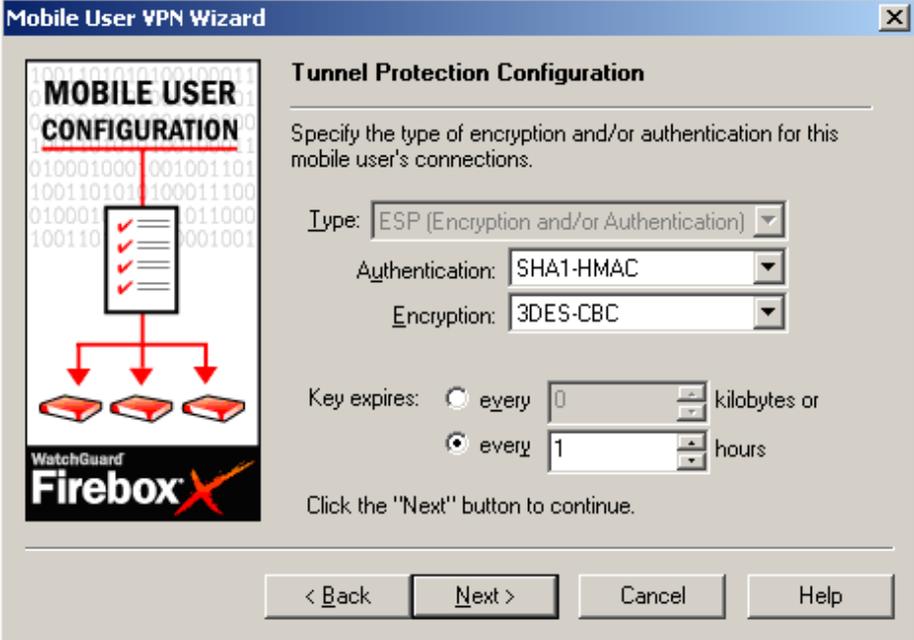
Step	Description
7.	Click <b>Next</b> to continue. The <i>Enter Shared Key</i> and <i>Confirm</i> fields have been populated with the passphrase entered in the previous step.

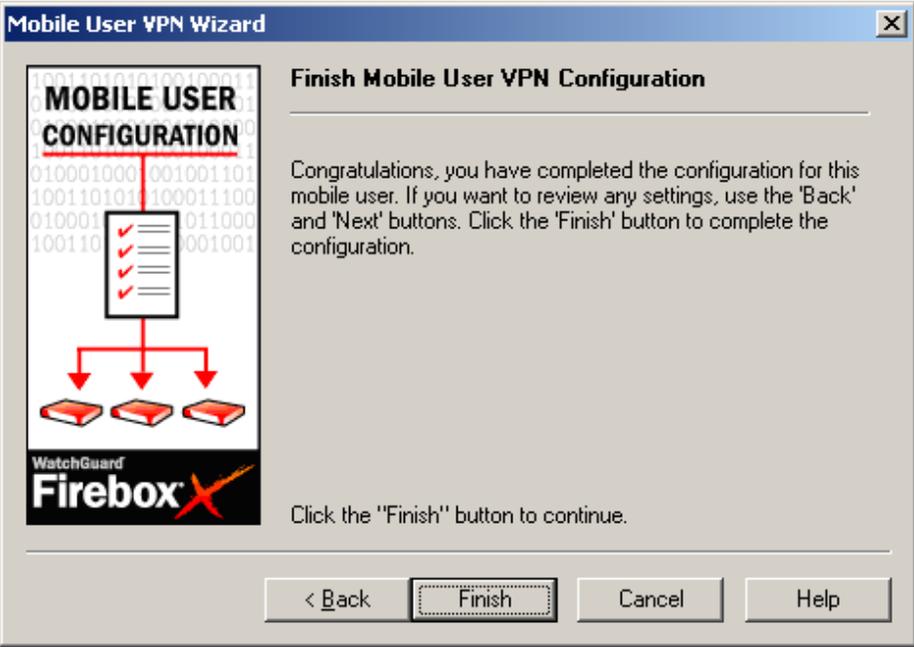


8.	Select the option to <b>Use the passphrase of the end-user profile (the .wgx or .exp file) as the pre-shared key</b> . Click <b>Next</b> .
----	--

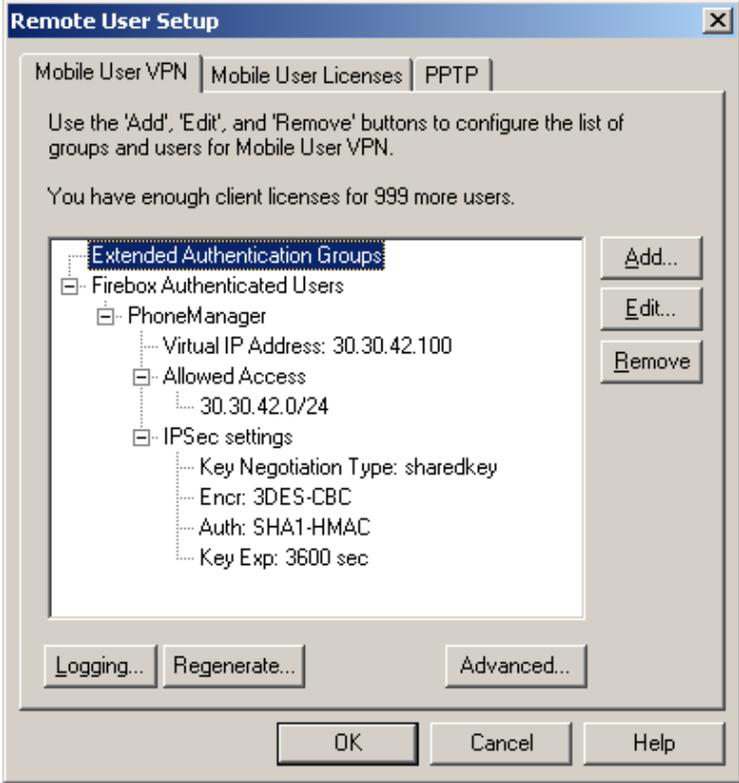


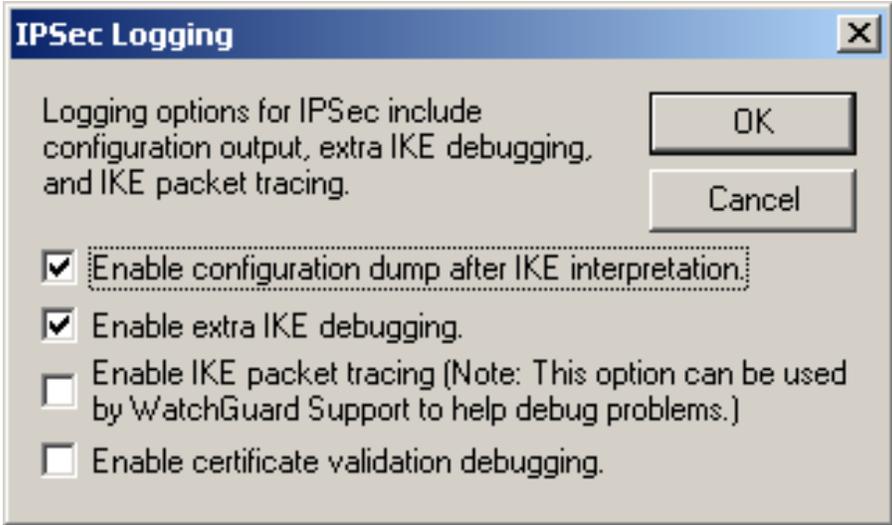
Step	Description
9.	<p>Click <b>Add</b> to specify the network that the MUVPN client will be allowed to access.</p> 
10.	<p>Select <b>Network</b> in the <b>Allow access to</b> drop down list and specify the network for the LAN2 interface of the Small Office Edition. Click <b>OK</b>.</p> 

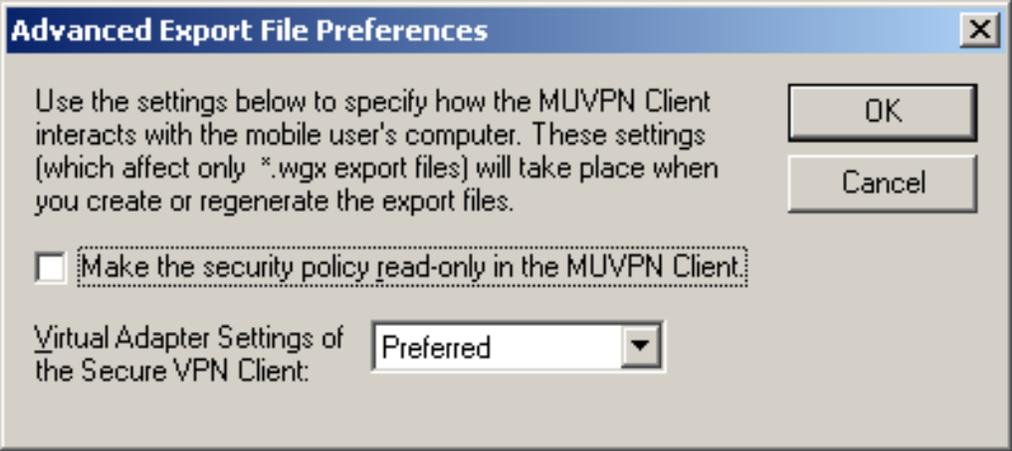
Step	Description
11.	<p>Enter a virtual IP address (e.g., <b>30.30.42.100</b>) for the MUVPN client. Click <b>Next</b>.</p> 
12.	<p>Enter the values shown below for Phase 2 from <b>Table 1</b>. Phase 2 re-authentication is set to occur every hour. Click <b>Next</b>.</p> <ul style="list-style-type: none"> <li>• Authentication – The password authentication used by the tunnel.</li> <li>• Encryption – The encryption method used by the tunnel.</li> </ul> 

Step	Description
13.	<p>Click <b>Finish</b> to complete the mobile user VPN configuration and return to the “Remote User Setup” window. This will result in the creation of a file with a .wgx extension which can be used to update the security policy of the MUVPN client. The WatchGuard Policy Import utility is covered in more detail in Section 4.3.</p> 

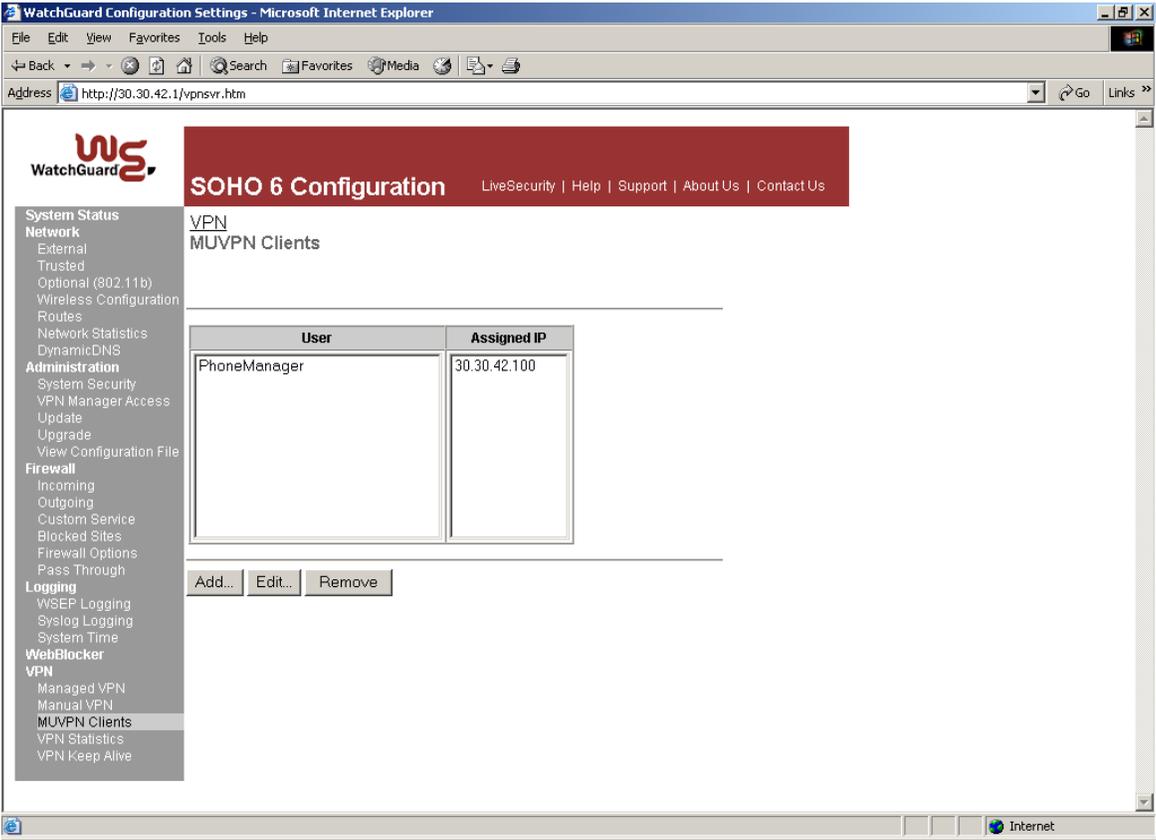
Step	Description
------	-------------

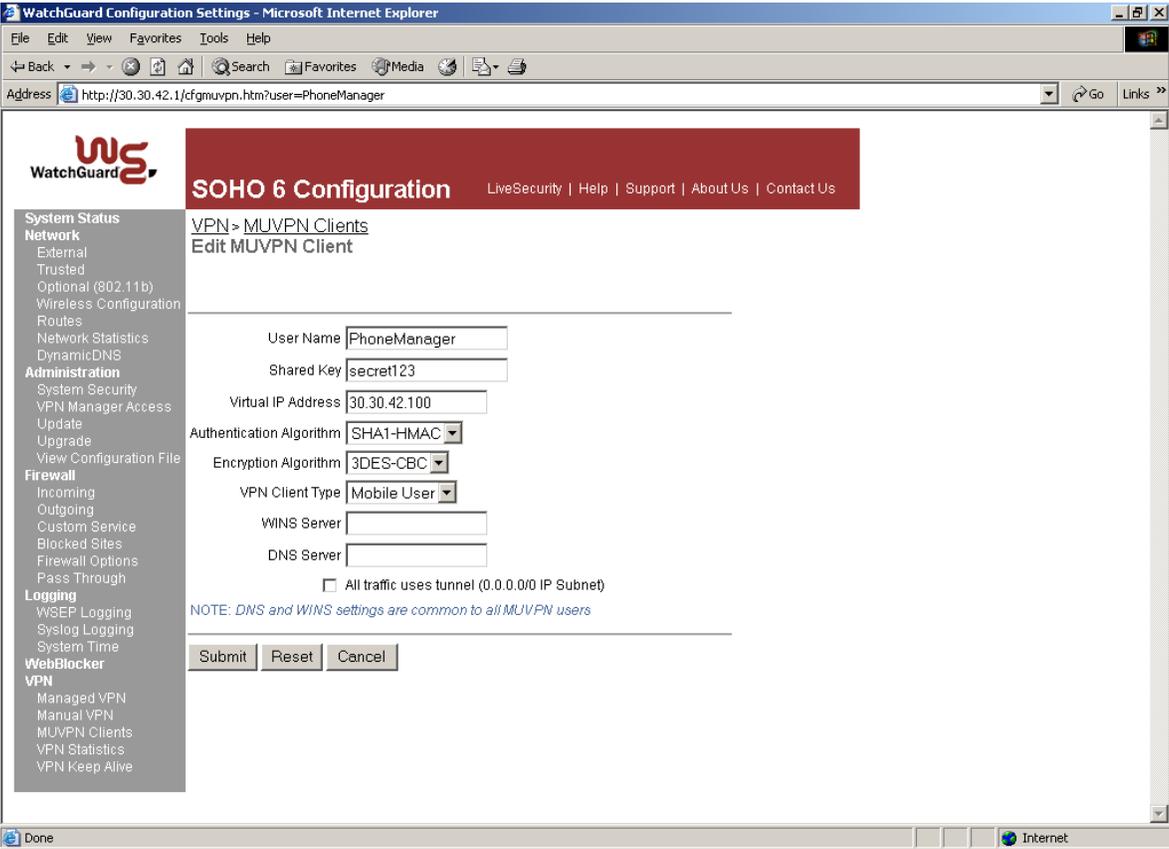
<p><b>14.</b></p>	<p>If desired, click <b>Logging...</b> from the “Remote User Setup” window to enable IPSec logging for debugging purposes.</p>  <p>The screenshot shows the 'Remote User Setup' dialog box with tabs for 'Mobile User VPN', 'Mobile User Licenses', and 'PPTP'. The 'Mobile User VPN' tab is active. It contains instructions to use 'Add', 'Edit', and 'Remove' buttons to configure groups and users. Below this, it states 'You have enough client licenses for 999 more users.' A tree view shows 'Extended Authentication Groups' expanded to show 'Firebox Authenticated Users', which includes 'PhoneManager' with a 'Virtual IP Address: 30.30.42.100'. Under 'PhoneManager', there are 'Allowed Access' (30.30.42.0/24) and 'IPSec settings' (Key Negotiation Type: sharedkey, Encr: 3DES-CBC, Auth: SHA1-HMAC, Key Exp: 3600 sec). To the right of the tree are 'Add...', 'Edit...', and 'Remove' buttons. At the bottom of the dialog are 'Logging...', 'Regenerate...', and 'Advanced...' buttons, and at the very bottom are 'OK', 'Cancel', and 'Help' buttons.</p>
-------------------	--

<p><b>15.</b></p>	<p>If logging was selected, check the options shown below to include the configuration output and extra IKE debugging in the log and click <b>OK</b> to return to the “Remote User Setup” window.</p>  <p>The screenshot shows the 'IPSec Logging' dialog box. It contains the text: 'Logging options for IPSec include configuration output, extra IKE debugging, and IKE packet tracing.' Below this text are two buttons: 'OK' and 'Cancel'. There are four checkboxes:         <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Enable configuration dump after IKE interpretation. (This checkbox is highlighted with a dashed border.)</li> <li><input checked="" type="checkbox"/> Enable extra IKE debugging.</li> <li><input type="checkbox"/> Enable IKE packet tracing (Note: This option can be used by WatchGuard Support to help debug problems.)</li> <li><input type="checkbox"/> Enable certificate validation debugging.</li> </ul> </p>
-------------------	--

Step	Description
16.	<p>Click <b>Advanced...</b> from the “Remote User Setup” window and select <b>Preferred</b> for the <i>Virtual Adapter Settings of the Secure VPN Client</i>. Click <b>OK</b> to return to Remote User Setup. Click <b>OK</b> to return to Policy Manager.</p> 

## 4.2. Configure the WatchGuard SOHO 6c Wireless

Step	Description				
1.	<p>Open the SOHO 6 Configuration screen by specifying the IP address of the private interface of the SOHO 6c Wireless in a browser window. Click the <b>MUVPN Clients</b> option on the left pane and click <b>Add</b> to add a MUVPN tunnel to the SOHO.</p>  <table border="1" data-bbox="509 758 891 978"><thead><tr><th>User</th><th>Assigned IP</th></tr></thead><tbody><tr><td>PhoneManager</td><td>30.30.42.100</td></tr></tbody></table>	User	Assigned IP	PhoneManager	30.30.42.100
User	Assigned IP				
PhoneManager	30.30.42.100				

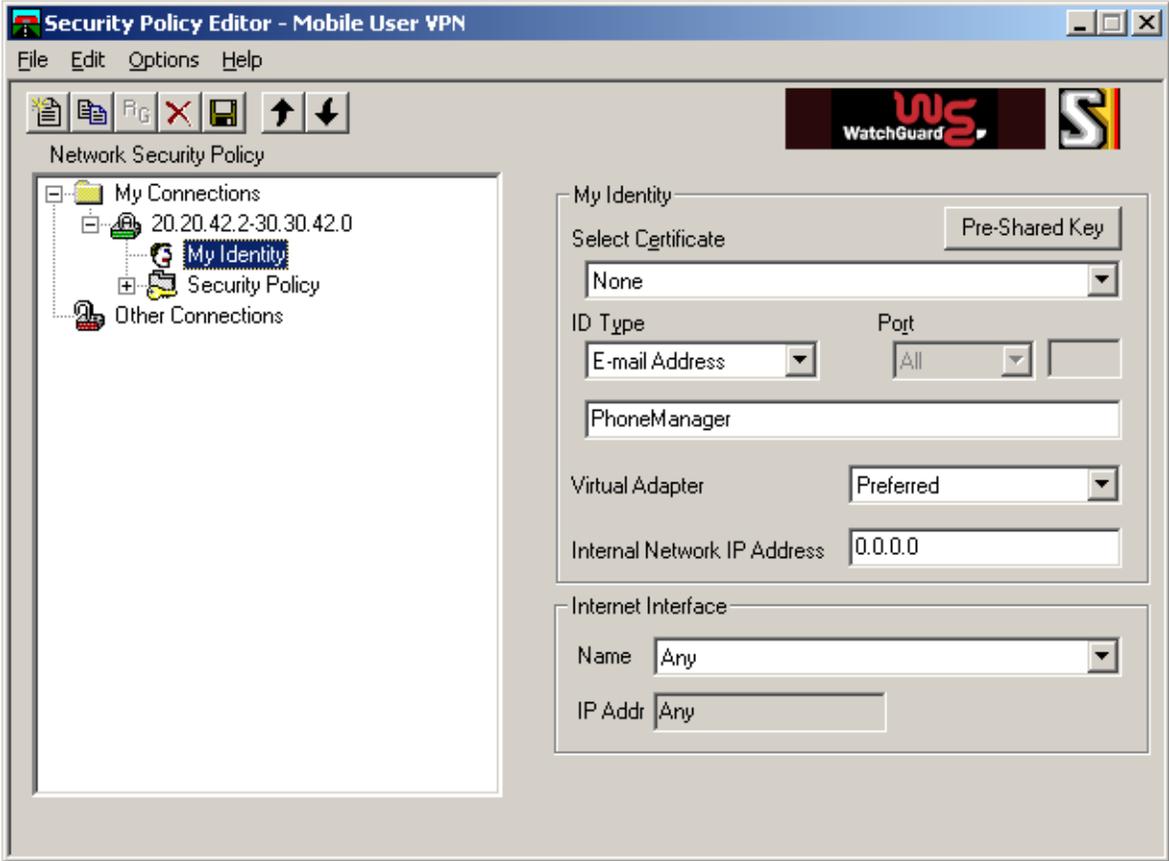
Step	Description
2.	<p>Enter the values shown below for Phase 2 from <b>Table 1</b>.</p> <ul style="list-style-type: none"> <li>• User Name – The name of the MUVPN client</li> <li>• Shared Key – The password used for authentication and must match on the device at the other end of the tunnel.</li> <li>• Virtual IP Address – The virtual IP address assigned to the MUVPN client.</li> <li>• Authentication Algorithm – The password authentication used by the tunnel.</li> <li>• Encryption Algorithm – The encryption method used by the tunnel.</li> <li>• VPN Client Type – <b>Mobile User</b> (MUVPN client)</li> </ul>  <p>Click <b>Submit</b>.</p>

### 4.3. Configure the MUVPN Client

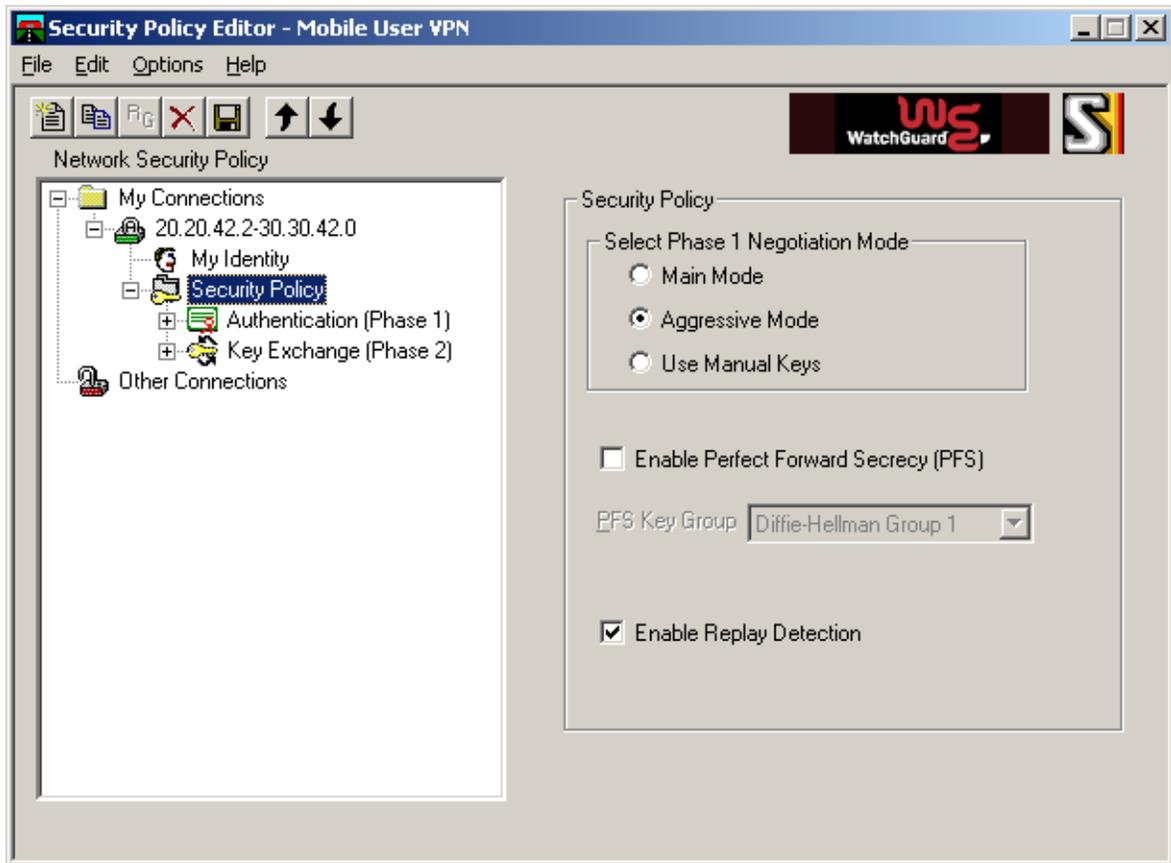
**Note:** The next two steps apply only if the PhoneManager MUVPN client was created using the Firebox System Manager.

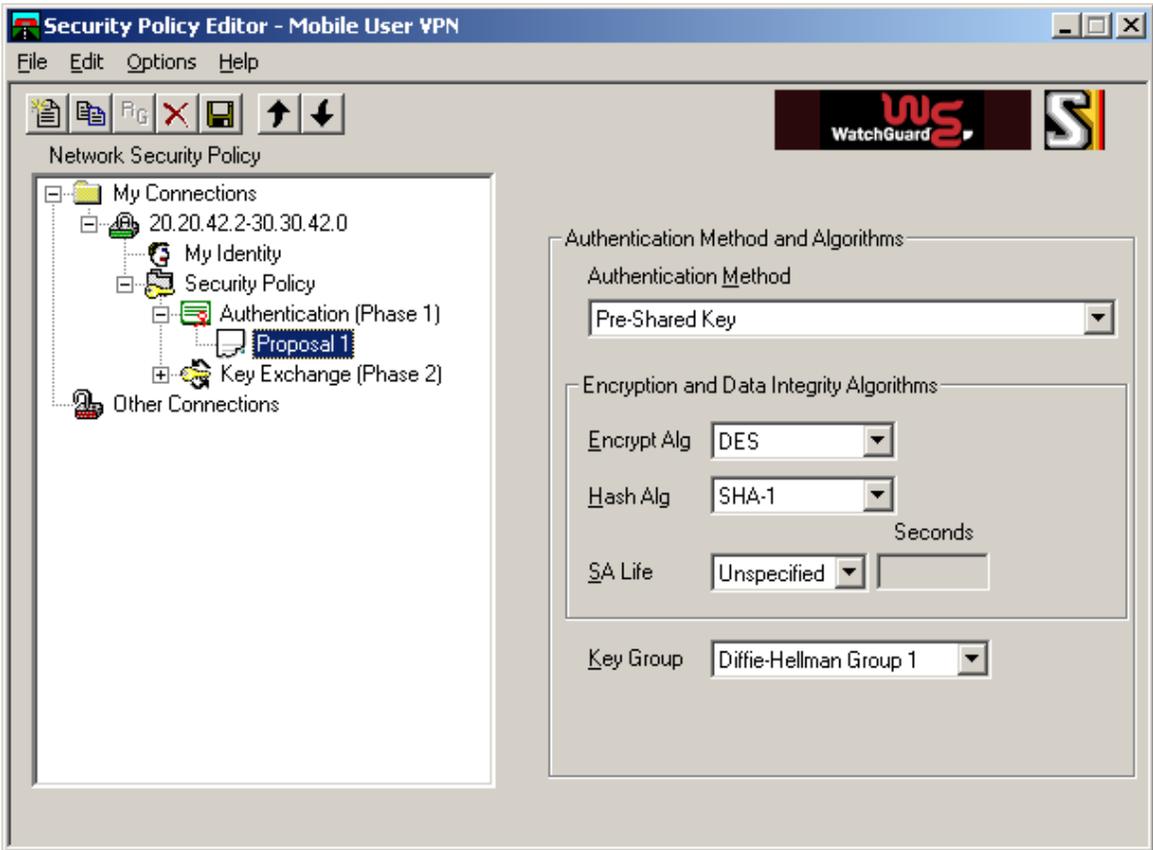
Step	Description
1.	<p>Copy the PhoneManager.wgx file from the Firebox System Manager PC (e.g., c:\Program Files\WatchGuard\Ruvpn\20.20.42.2\wgx\PhoneManager directory) to the MUVPN client and double-click on it after installing the MUVPN software. Enter the same <i>Shared Key</i> that was used in step 7 of Section 4.1. Click <b>OK</b> to import the security policy.</p> 
2.	<p>The following pop-up window appears after importing the security policy. Click <b>OK</b> to exit the import utility.</p> 

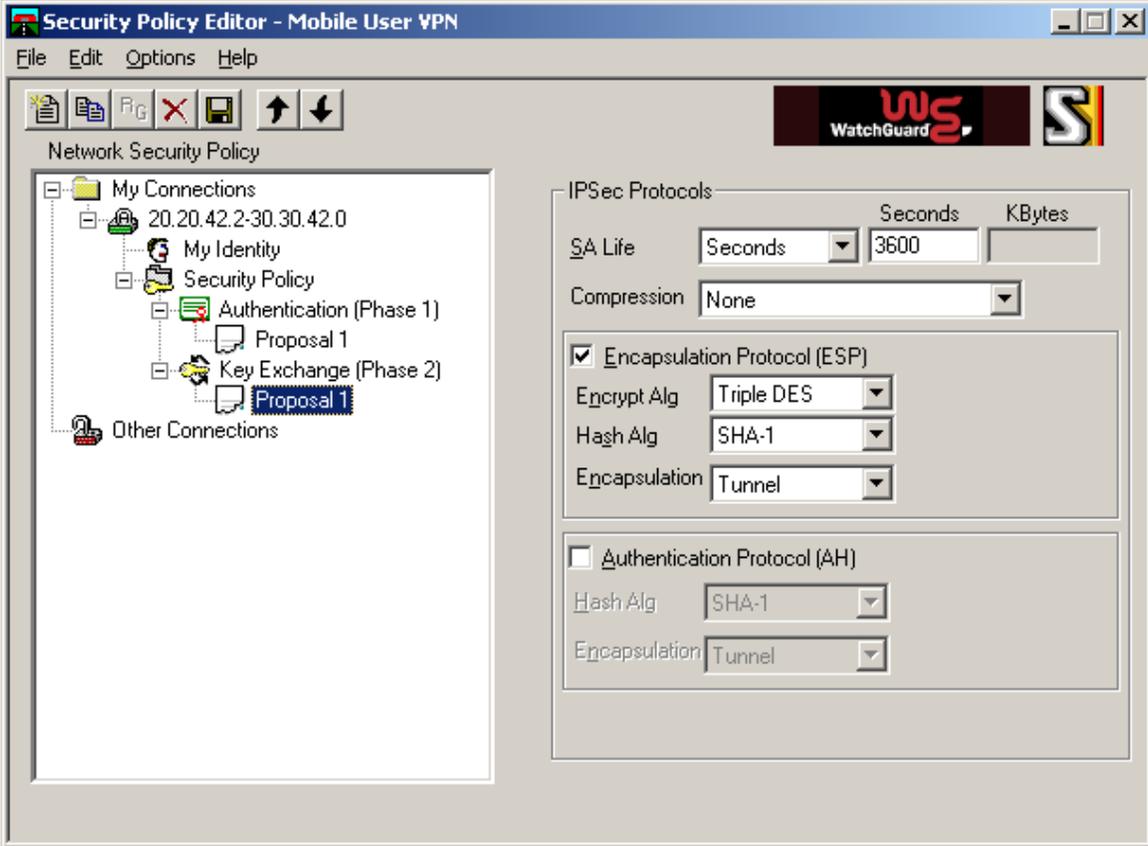
Step	Description
3.	<p><b>Note:</b> If the PhoneManager.wgx file was not used to import the security policy (e.g., in the case where only the SOHO was configured), the configuration shown in the following steps (3-8) must be performed. If the PhoneManager.wgx file was used to import the security policy (e.g., in the case where the Firebox X was configured), the configuration shown in the following steps (3-8) does not need to be performed.</p> <p>Open the Security Policy Editor by navigating to <b>Start → Programs → Mobile User VPN → Security Policy Editor</b>. Right-click <b>My Connections</b> and select <b>Add → Connection</b>. Specify the name of the new connection (e.g., <b>20.20.42.2-30.30.42.0</b>) and enter the values shown below, matching the Firebox X or SOHO tunnel configuration. The remote subnet is that of the Small Office Edition's LAN2 interface. The IP address of the external interface of the Firebox X or SOHO (e.g., <b>20.20.42.2</b>) is specified as the remote tunnel endpoint address.</p>

Step	Description
4.	<p>Expand the new connection by clicking on the “+” next to the connection name and click <b>My Identity</b>. Select <b>None</b> in the <i>Select Certificate</i> drop-down list. Click <b>Pre-Shared Key</b> and <b>Enter Key</b> to supply the same password specified in the Firebox X or SOHO tunnel configuration. Select <b>E-mail Address</b> for the <i>ID Type</i> and enter the Name of the MUVPN client (e.g., <b>PhoneManager</b>) in the subsequent field. Select <b>Preferred</b> in the Virtual Adapter drop-down list and leave the other fields as default.</p> 

Step	Description
5.	<p>Click <b>Security Policy</b>. <b>Aggressive Mode</b> was selected for the <i>Select Phase 1 Negotiation Mode</i> and leave the other fields as defaults.</p>



Step	Description
6.	<p>Expand <b>Security Policy</b> and <b>Authentication (Phase1)</b>. Click <b>Proposal 1</b>. The values shown below are the defaults used for Phase 1 negotiation.</p>  <p>The screenshot shows the 'Security Policy Editor - Mobile User VPN' window. On the left, a tree view under 'Network Security Policy' shows 'My Connections' expanded to '20.20.42.2-30.30.42.0', which contains 'My Identity', 'Security Policy', 'Authentication (Phase 1)', and 'Key Exchange (Phase 2)'. 'Authentication (Phase 1)' is expanded to show 'Proposal 1' selected. On the right, the configuration panel for 'Authentication Method and Algorithms' shows 'Pre-Shared Key' selected in the 'Authentication Method' dropdown. Below, the 'Encryption and Data Integrity Algorithms' section shows 'DES' for 'Encrypt Alg', 'SHA-1' for 'Hash Alg', and 'Unspecified' for 'SA Life' (with a 'Seconds' input field). At the bottom, 'Diffie-Hellman Group 1' is selected in the 'Key Group' dropdown.</p>

Step	Description
7.	<p>Expand <b>Key Exchange (Phase2)</b>. Click <b>Proposal 1</b> and enter the values shown below to match the Firebox X and the SOHO tunnel configuration for Phase 2.</p> 
8.	<p>Click <b>File</b> → <b>Save</b> or the floppy disk icon  on the tool bar to save the configuration.</p>

#### **4.4. Interoperability Compliance Testing**

The features of the Firebox X and SOHO products were tested to determine if VPN tunnels could be established with the MUVPN client used by Phone Manager Pro.

#### **4.5. General Test Approach**

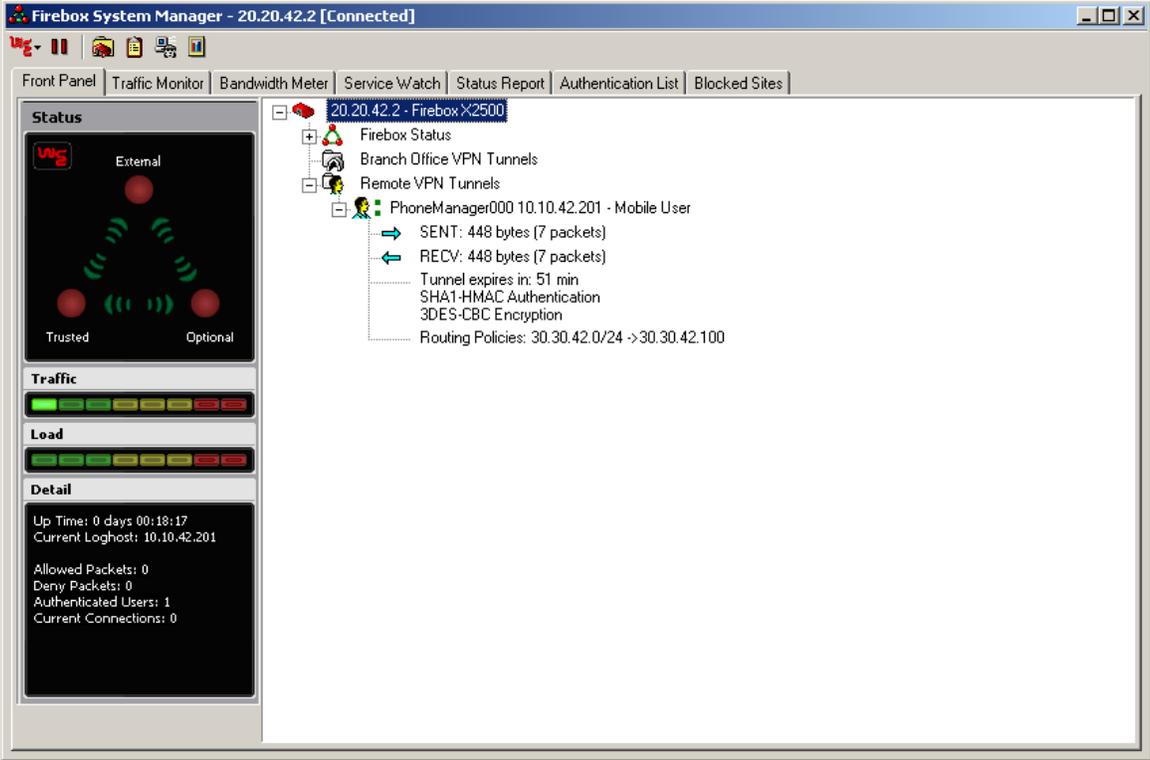
The following scenarios were tested using the network configuration diagrams shown in **Figure 1**:

- Ability to establish a client VPN tunnel between the Firebox X or SOHO and the MUVPN client used for Phone Manager Pro.
- RAS (Registration Admission Status) over the VPN tunnel.
- Voice calls were placed manually and subjective quality noted for both G.711 mu-law and G.729 codecs. Direct Media Path was not supported in this configuration between the Phone Manager Pro and the IP telephone because only one remote subnet can be supported.

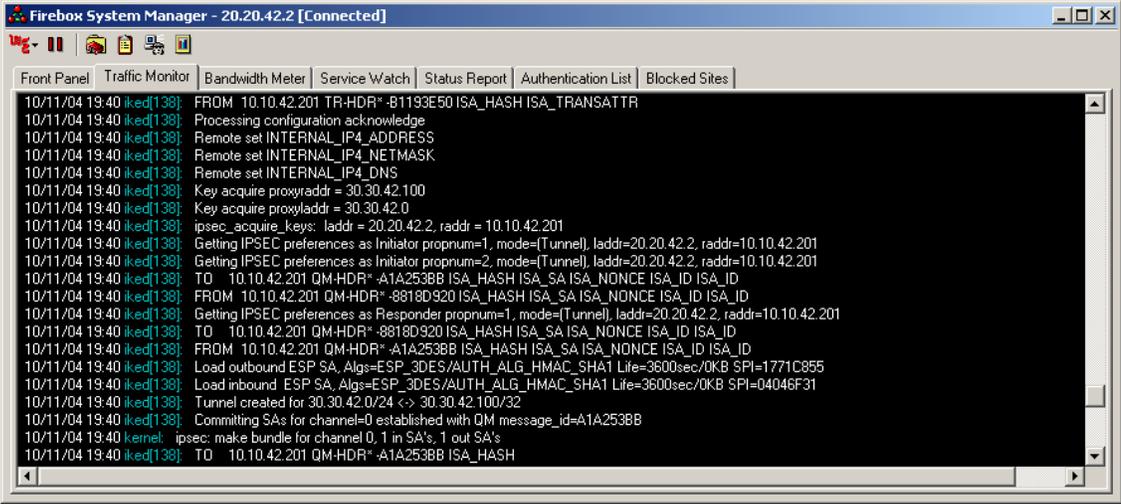
#### **4.6. Test Results**

Testing was successful. Client VPN tunnels could be established between the Firebox X or SOHO with the MUVPN client used by Phone Manager Pro.

## 5. Verification Steps

Step	Description
1.	<p>From the Firebox System Manager window, expand the tunnel name listed under the Remote VPN Tunnels item to view statistics for the remote tunnel between the Firebox X and MUVPN client.</p>  <p>The screenshot displays the Firebox System Manager interface. The main window title is 'Firebox System Manager - 20.20.42.2 [Connected]'. The interface includes a menu bar with options: Front Panel, Traffic Monitor, Bandwidth Meter, Service Watch, Status Report, Authentication List, and Blocked Sites. On the left, there is a 'Status' panel with a diagram showing 'External', 'Trusted', and 'Optional' components. Below this are 'Traffic', 'Load', and 'Detail' sections. The 'Detail' section shows: Up Time: 0 days 00:18:17, Current Loghost: 10.10.42.201, Allowed Packets: 0, Deny Packets: 0, Authenticated Users: 1, Current Connections: 0. The main content area shows a tree view of VPN tunnels. Under 'Remote VPN Tunnels', the tunnel 'PhoneManager000 10.10.42.201 - Mobile User' is expanded, showing: SENT: 448 bytes (7 packets), RECV: 448 bytes (7 packets), Tunnel expires in: 51 min, SHA1-HMAC Authentication, 3DES-CBC Encryption, and Routing Policies: 30.30.42.0/24 -&gt; 30.30.42.100.</p>

**Step 2.** Click on the **Traffic Monitor** tab to view Phase 1 negotiation messages.



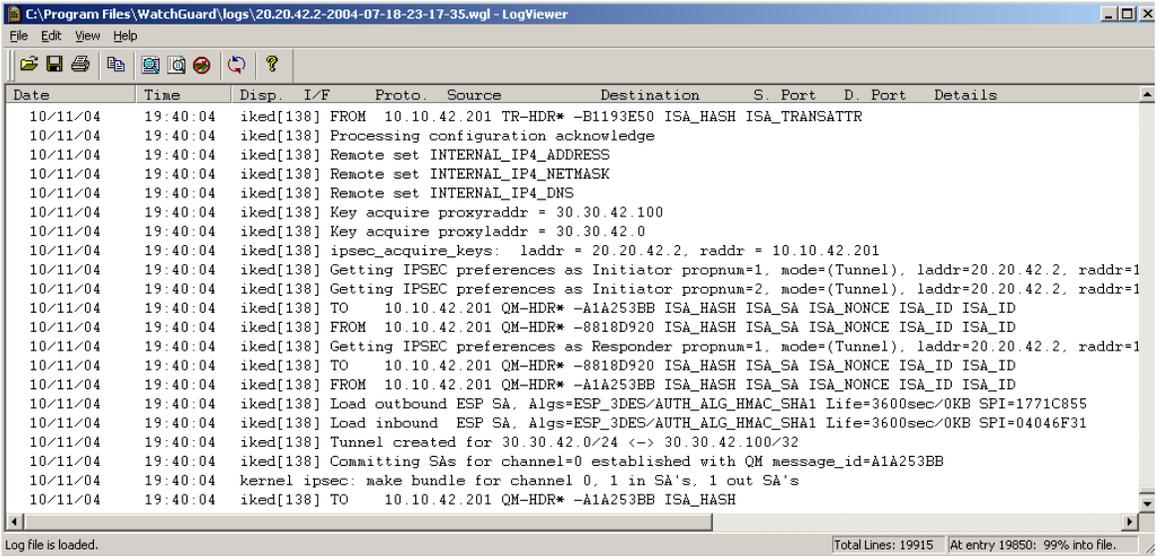
The screenshot shows the 'Traffic Monitor' tab in the Firebox System Manager. The log displays the following messages:

```

10/11/04 19:40 iked[138]: FROM 10.10.42.201 TR-HDR* -B1193E50 ISA_HASH ISA_TRANSATTR
10/11/04 19:40 iked[138]: Processing configuration acknowledge
10/11/04 19:40 iked[138]: Remote set INTERNAL_IP4_ADDRESS
10/11/04 19:40 iked[138]: Remote set INTERNAL_IP4_NETMASK
10/11/04 19:40 iked[138]: Remote set INTERNAL_IP4_DNS
10/11/04 19:40 iked[138]: Key acquire proxyraddr = 30.30.42.100
10/11/04 19:40 iked[138]: Key acquire proxyladdr = 30.30.42.0
10/11/04 19:40 iked[138]: ipsec_acquire_keys: laddr = 20.20.42.2, raddr = 10.10.42.201
10/11/04 19:40 iked[138]: Getting IPSEC preferences as Initiator propnum=1, mode=(Tunnel), laddr=20.20.42.2, raddr=10.10.42.201
10/11/04 19:40 iked[138]: Getting IPSEC preferences as Initiator propnum=2, mode=(Tunnel), laddr=20.20.42.2, raddr=10.10.42.201
10/11/04 19:40 iked[138]: TO 10.10.42.201 QM-HDR* -A1A253BB ISA_HASH ISA_SA ISA_NONCE ISA_ID ISA_ID
10/11/04 19:40 iked[138]: FROM 10.10.42.201 QM-HDR* -8818D920 ISA_HASH ISA_SA ISA_NONCE ISA_ID ISA_ID
10/11/04 19:40 iked[138]: Getting IPSEC preferences as Responder propnum=1, mode=(Tunnel), laddr=20.20.42.2, raddr=10.10.42.201
10/11/04 19:40 iked[138]: TO 10.10.42.201 QM-HDR* -8818D920 ISA_HASH ISA_SA ISA_NONCE ISA_ID ISA_ID
10/11/04 19:40 iked[138]: FROM 10.10.42.201 QM-HDR* -A1A253BB ISA_HASH ISA_SA ISA_NONCE ISA_ID ISA_ID
10/11/04 19:40 iked[138]: Load outbound ESP SA, Algs=ESP_3DES/AUTH_ALG_HMAC_SHA1 Life=3600sec/0KB SPI=1771C855
10/11/04 19:40 iked[138]: Load inbound ESP SA, Algs=ESP_3DES/AUTH_ALG_HMAC_SHA1 Life=3600sec/0KB SPI=04046F31
10/11/04 19:40 iked[138]: Tunnel created for 30.30.42.0/24 <-> 30.30.42.100/32
10/11/04 19:40 iked[138]: Committing SAs for channel=0 established with QM message_id=A1A253BB
10/11/04 19:40 kernel ipsec: make bundle for channel 0, 1 in SA's, 1 out SA's
10/11/04 19:40 iked[138]: TO 10.10.42.201 QM-HDR* -A1A253BB ISA_HASH

```

**Step 3.** From the Firebox System Manager, select **Tools** → **Log Viewer** or click on the  taskbar icon to view the Phase 1 negotiation message history.

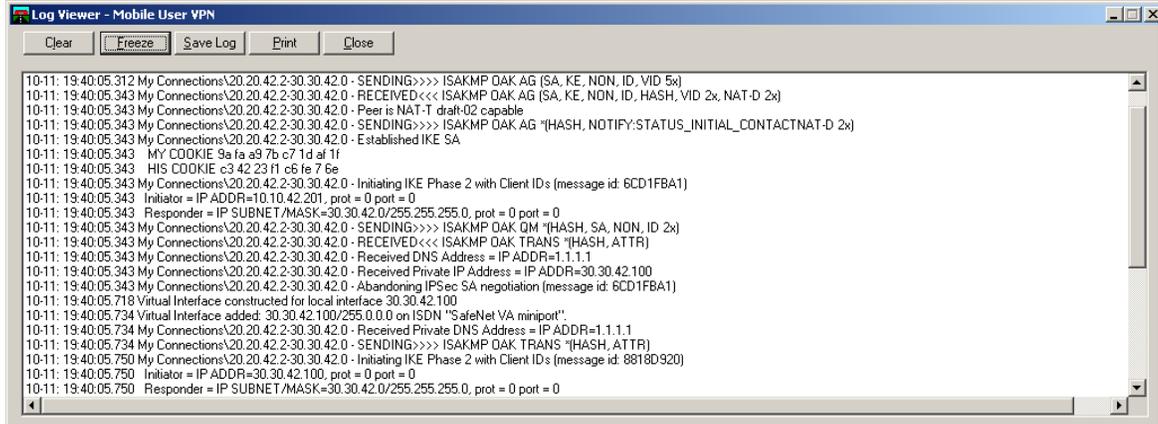


The screenshot shows the Log Viewer window displaying the same Phase 1 negotiation messages as the Traffic Monitor. The log is presented in a table format with the following columns: Date, Time, Disp., I/F, Proto., Source, Destination, S. Port, D. Port, and Details.

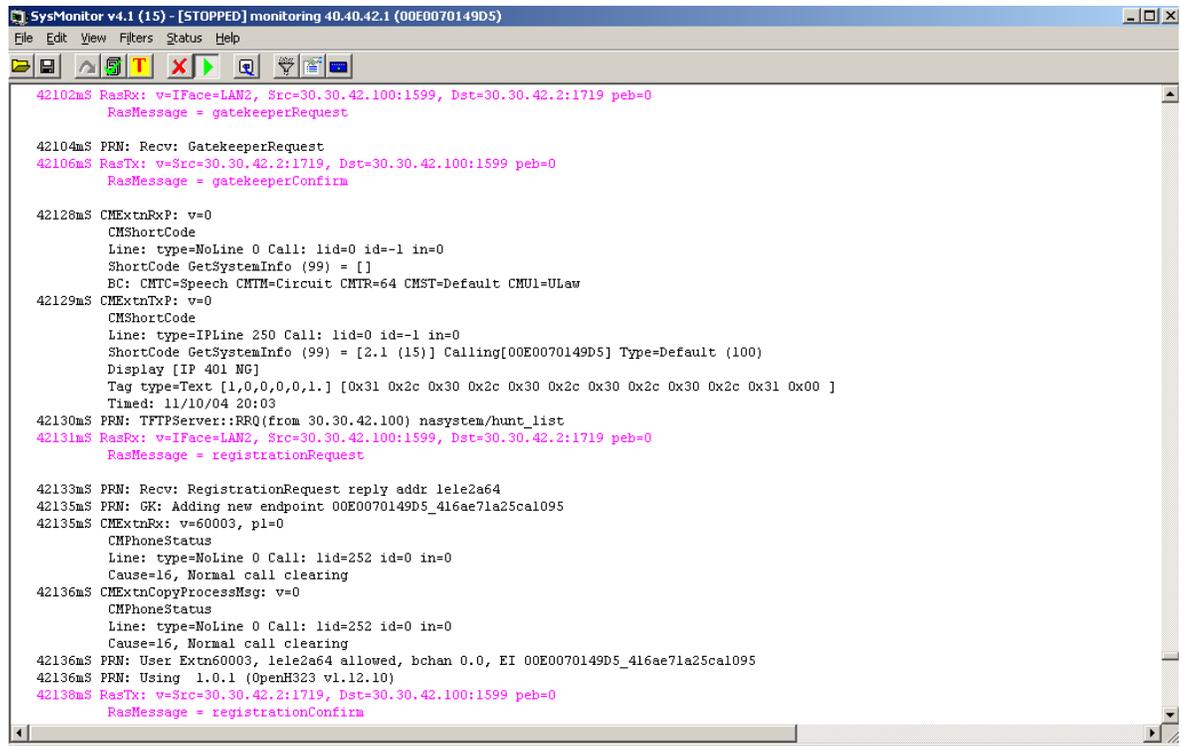
Date	Time	Disp.	I/F	Proto.	Source	Destination	S. Port	D. Port	Details
10/11/04	19:40:04	iked[138]		FROM	10.10.42.201	TR-HDR* -B1193E50	ISA_HASH	ISA_TRANSATTR	
10/11/04	19:40:04	iked[138]				Processing configuration acknowledge			
10/11/04	19:40:04	iked[138]				Remote set INTERNAL_IP4_ADDRESS			
10/11/04	19:40:04	iked[138]				Remote set INTERNAL_IP4_NETMASK			
10/11/04	19:40:04	iked[138]				Remote set INTERNAL_IP4_DNS			
10/11/04	19:40:04	iked[138]				Key acquire proxyraddr = 30.30.42.100			
10/11/04	19:40:04	iked[138]				Key acquire proxyladdr = 30.30.42.0			
10/11/04	19:40:04	iked[138]				ipsec_acquire_keys: laddr = 20.20.42.2, raddr = 10.10.42.201			
10/11/04	19:40:04	iked[138]				Getting IPSEC preferences as Initiator propnum=1, mode=(Tunnel), laddr=20.20.42.2, raddr=10.10.42.201			
10/11/04	19:40:04	iked[138]				Getting IPSEC preferences as Initiator propnum=2, mode=(Tunnel), laddr=20.20.42.2, raddr=10.10.42.201			
10/11/04	19:40:04	iked[138]		TO	10.10.42.201	QM-HDR* -A1A253BB	ISA_HASH	ISA_SA ISA_NONCE ISA_ID ISA_ID	
10/11/04	19:40:04	iked[138]		FROM	10.10.42.201	QM-HDR* -8818D920	ISA_HASH	ISA_SA ISA_NONCE ISA_ID ISA_ID	
10/11/04	19:40:04	iked[138]				Getting IPSEC preferences as Responder propnum=1, mode=(Tunnel), laddr=20.20.42.2, raddr=10.10.42.201			
10/11/04	19:40:04	iked[138]		TO	10.10.42.201	QM-HDR* -8818D920	ISA_HASH	ISA_SA ISA_NONCE ISA_ID ISA_ID	
10/11/04	19:40:04	iked[138]		FROM	10.10.42.201	QM-HDR* -A1A253BB	ISA_HASH	ISA_SA ISA_NONCE ISA_ID ISA_ID	
10/11/04	19:40:04	iked[138]				Load outbound ESP SA, Algs=ESP_3DES/AUTH_ALG_HMAC_SHA1 Life=3600sec/0KB SPI=1771C855			
10/11/04	19:40:04	iked[138]				Load inbound ESP SA, Algs=ESP_3DES/AUTH_ALG_HMAC_SHA1 Life=3600sec/0KB SPI=04046F31			
10/11/04	19:40:04	iked[138]				Tunnel created for 30.30.42.0/24 <-> 30.30.42.100/32			
10/11/04	19:40:04	iked[138]				Committing SAs for channel=0 established with QM message_id=A1A253BB			
10/11/04	19:40:04	kernel				ipsec: make bundle for channel 0, 1 in SA's, 1 out SA's			
10/11/04	19:40:04	iked[138]		TO	10.10.42.201	QM-HDR* -A1A253BB	ISA_HASH		

Step	Description																		
4.	<p>Open the SOHO 6 Configuration screen by specifying the IP address of the private interface of the SOHO 6tc Wireless in a browser window. Click the <b>VPN Statistics</b> option on the left pane to view statistics for the client VPN tunnel between the SOHO and MUVPN client.</p> <p>The screenshot shows the WatchGuard Configuration Settings interface in Microsoft Internet Explorer. The browser address bar shows <code>http://30.30.42.1/vpnstat.htm</code>. The page title is "SOHO 6 Configuration" with navigation links for LiveSecurity, Help, Support, About Us, and Contact Us. A left-hand navigation pane lists various system settings, with "VPN Statistics" selected. The main content area displays "VPN Statistics" and "IPSec Statistics".</p> <pre> IPSec Statistics BUNDLE (0) (Tunnel) refcnt = 2   20.20.42.2(7efb0401) (ESP): (Mature) refcnt(1)SRC:10.10.42.201 PROXY:10.10.42.201   AUTH: SHA1-HMAC Authentication   CRYPT: 3DES-CBC Encryption   Create Time: 0000000000000025b First Use: 00000000000000274   Bytes: 0000000002401a0 Packets: 00008ec4   Soft Timeouts: Bytes: 0007c28f5 Use Time: 0000149d3   Hard Timeouts: Bytes: 0007ffff Use Time: 0000153f3 BUNDLE (0) (Tunnel) refcnt = 1   10.10.42.201(beel7037) (ESP): (Mature) refcnt(1)SRC:20.20.42.2 PROXY:20.20.42.2   AUTH: SHA1-HMAC Authentication   CRYPT: 3DES-CBC Encryption   Create Time: 0000000000000025b First Use: 00000000000000274   Bytes: 000000000069b378 Packets: 0001a0f9   Soft Timeouts: Bytes: 0007ae147 Use Time: 0000138f3   Hard Timeouts: Bytes: 0007ffff Use Time: 0000153f3 </pre>																		
5.	<p>On the Phone Manager Pro PC, navigate to <b>Start → Programs → Mobile User VPN → Connection Monitor</b> to view statistics for the client VPN tunnel to the Firebox X or SOHO device.</p> <p>The screenshot shows the "Connection Monitor - Mobile User VPN" application window. It features a "Global Statistics" section with input fields for "Non-Secured Packets" (299), "Secured Packets" (8), "Dropped Packets" (0), and "Secured Data (KBytes)" (1). There are buttons for "Reset", "Close", and "Details". Below the statistics is a table with the following data:</p> <table border="1"> <thead> <tr> <th>Connection Name</th> <th>Local Address</th> <th>Local Subnet</th> <th>Remote Address</th> <th>Remote Modifier</th> <th>GW Address</th> <th>Protocol</th> <th>Local Port</th> <th>Rem Port</th> </tr> </thead> <tbody> <tr> <td>My Connection...</td> <td>30.30.42.100</td> <td>255.255.255.255</td> <td>30.30.42.0</td> <td>255.255.255.0</td> <td>20.20.42.2</td> <td>ALL</td> <td>ALL</td> <td>ALL</td> </tr> </tbody> </table>	Connection Name	Local Address	Local Subnet	Remote Address	Remote Modifier	GW Address	Protocol	Local Port	Rem Port	My Connection...	30.30.42.100	255.255.255.255	30.30.42.0	255.255.255.0	20.20.42.2	ALL	ALL	ALL
Connection Name	Local Address	Local Subnet	Remote Address	Remote Modifier	GW Address	Protocol	Local Port	Rem Port											
My Connection...	30.30.42.100	255.255.255.255	30.30.42.0	255.255.255.0	20.20.42.2	ALL	ALL	ALL											

Step	Description
6.	<p>On the Phone Manager Pro PC, navigate to <b>Start → Programs → Mobile User VPN → Log Viewer</b> to view Phase 1 and Phase 2 negotiation messages for the client VPN tunnel to Firebox X or SOHO device.</p>



7.	<p>Using the IP Office SysMonitor log, confirm Phone Manager Pro registration.</p>
----	--



## 6. Support

For technical support on WatchGuard, visit <http://www.watchguard.com/support>.

## 7. Conclusion

The configuration of client VPN tunnels between the WatchGuard Firebox X and SOHO products and the MUVPN client used by Phone Manager Pro has been successfully compliance tested.

## 8. References

- [1] *WatchGuard Firebox X Reviewer's Guide*, April 2004
- [2] *WatchGuard System Manager User Guide*, 2004.
- [3] *WatchGuard Firebox SOHO 6 Wireless User Guide*, Firmware Version 6.3, 2003
- [4] *ExtremeWare Software User Guide*, Software Version 6.2.1, April 2002; Document Number: 100049-00 Rev.05
- [5] *Avaya IP Office 2.1 Manager Application*, Issue 15c, 6th May 2004; Document Number: 40DHB0002USAU
- [6] *Avaya P333R Installation and Configuration Guide*, Software Version 4.0, April 2003

---

**©2004 Avaya Inc. All Rights Reserved.**

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya Developer*Connection* Program at [devconnect@avaya.com](mailto:devconnect@avaya.com).