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.

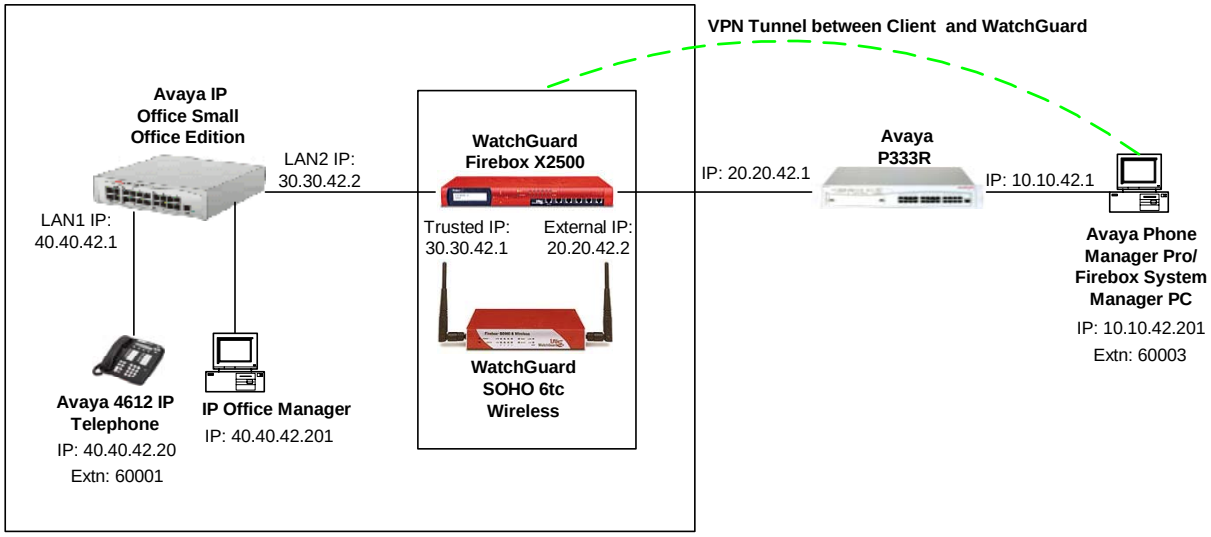


Figure 1 – Network Configuration Diagram

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:

Tunnel Type	IKE Exchange Type	Encryption Method	Password Authentication	Diffie-Hellman Group	Encryption Protocol
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**:

Equipment	Version
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

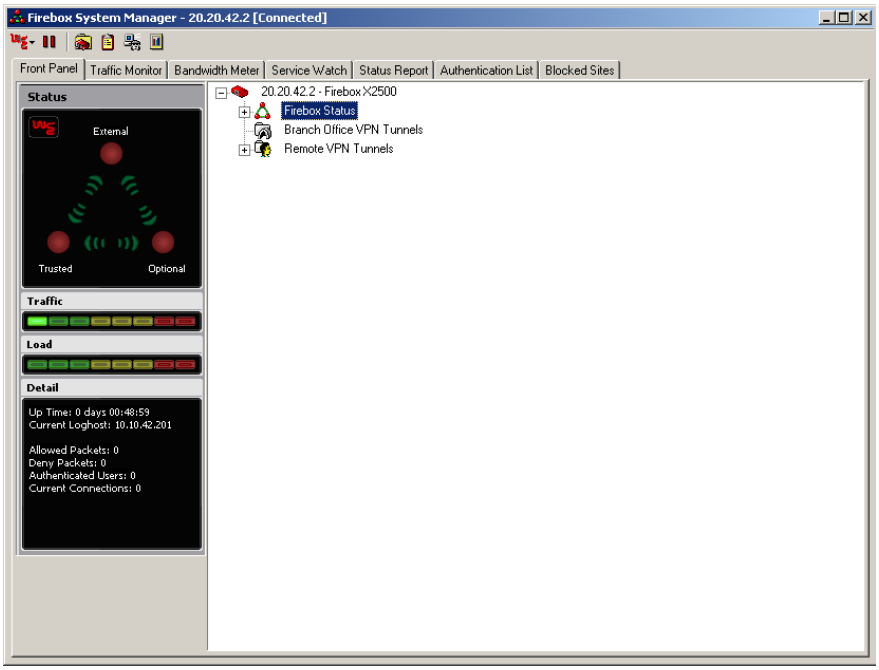
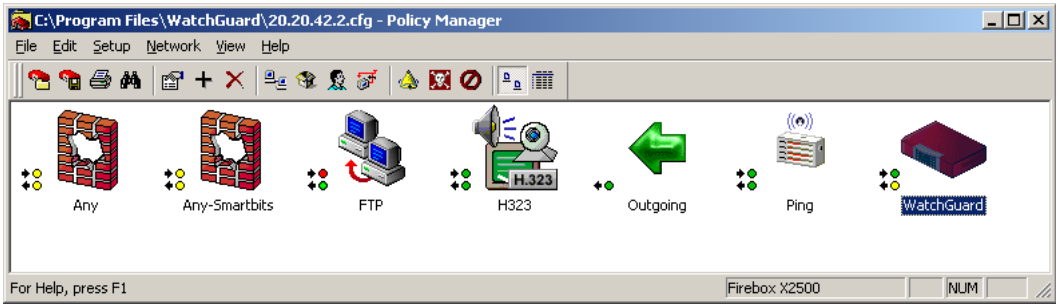
Table 2 – Product and Software/Version

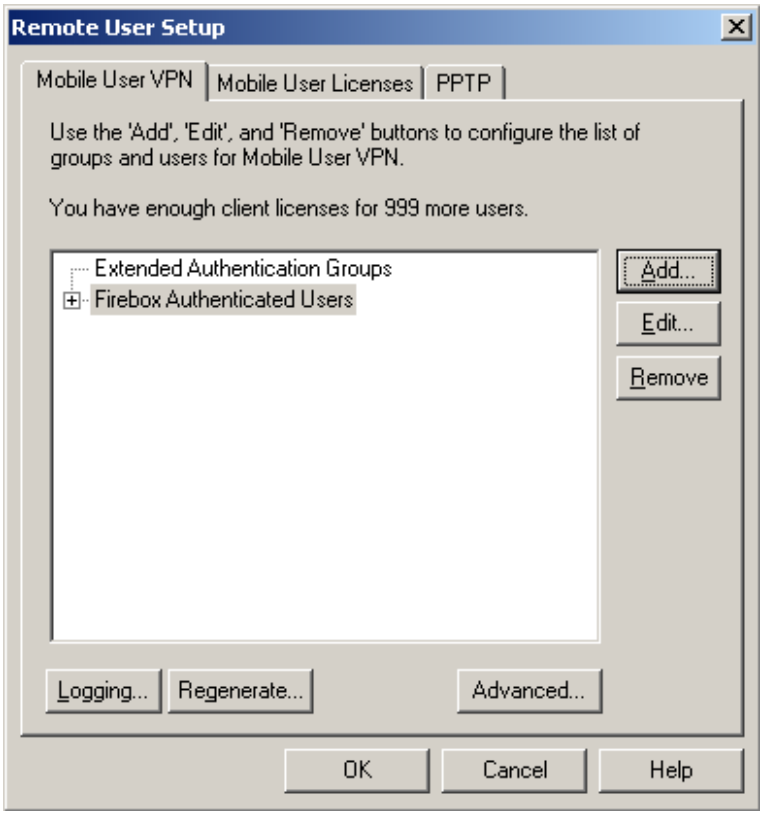
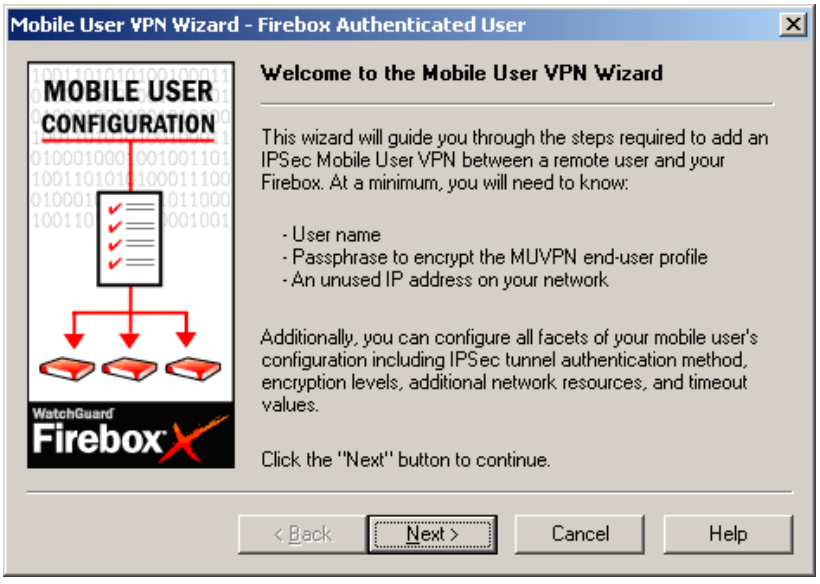
3. Configuring Phone Manager Pro

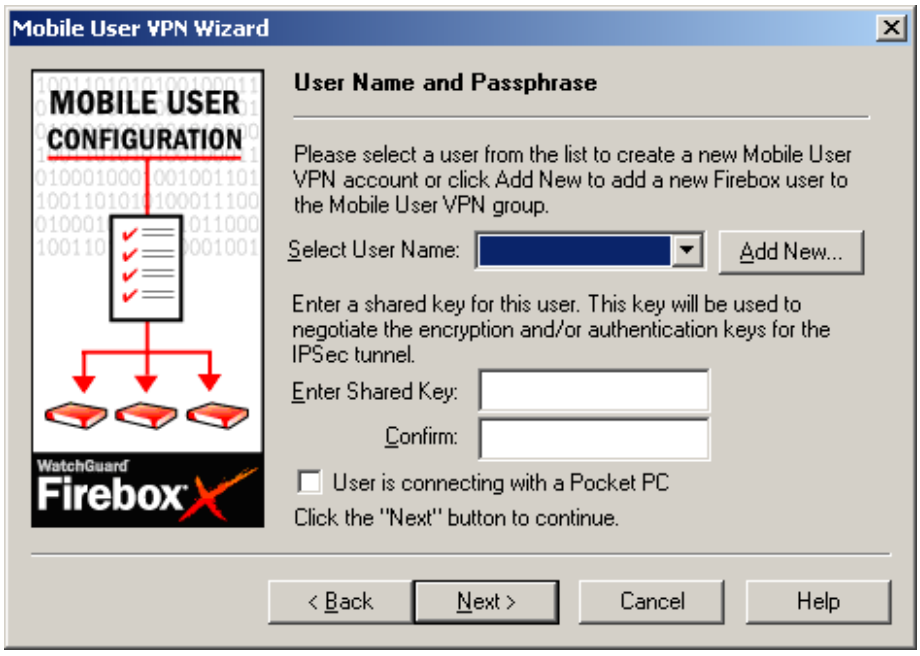
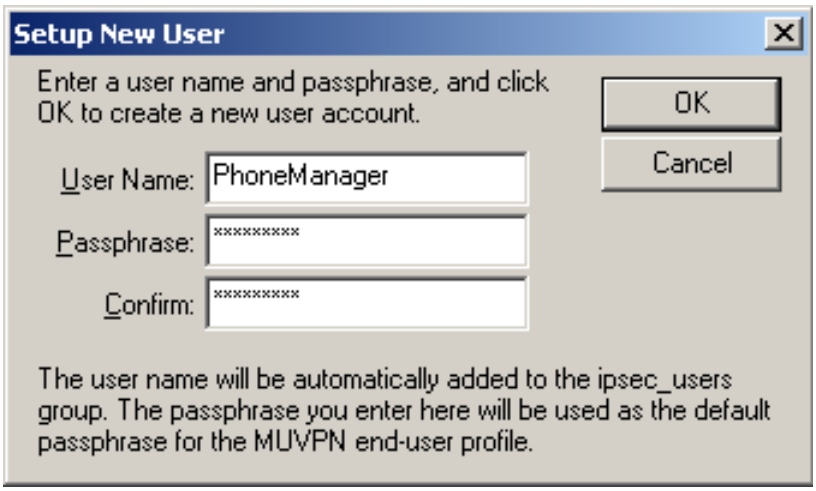
Step	Description
1.	Click **Start → Programs → IP Office → PhoneManager** to start the PhoneManager Pro application. Click **Configure → PBX** and specify the LAN2 interface address for IP Office (e.g., **30.30.42.2**) in the *PBX Address* field. Select the name defined on the **User** form in IP Office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

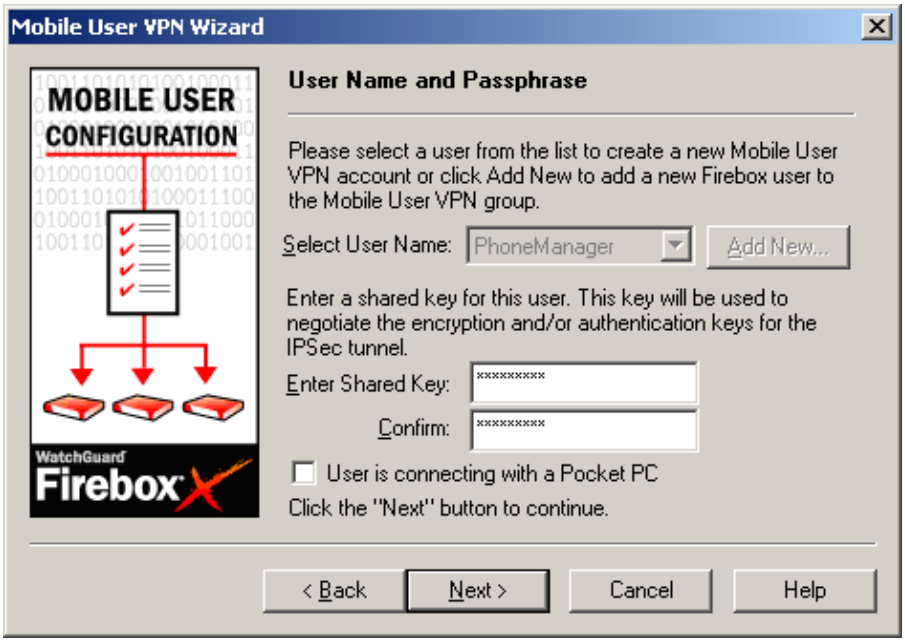
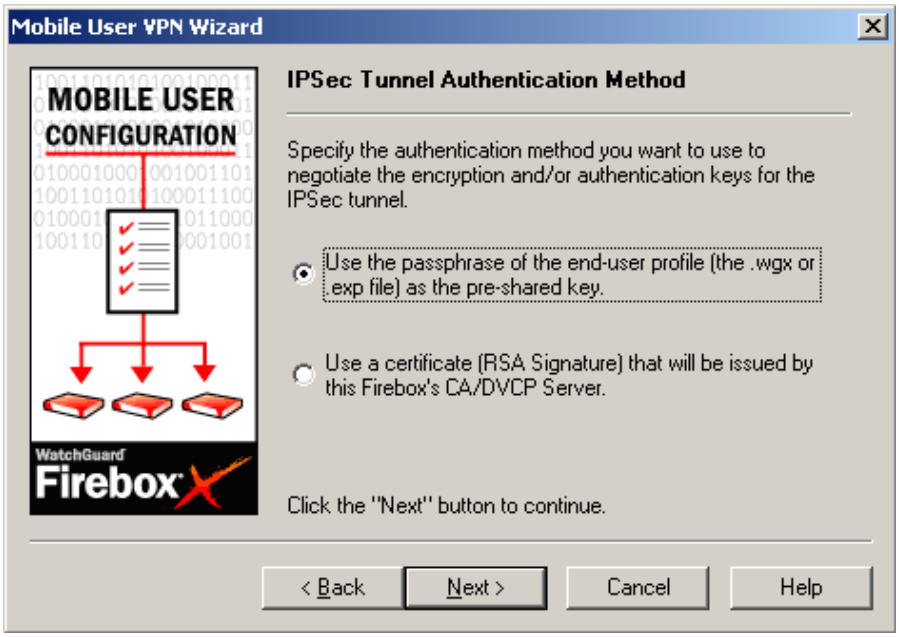
4. Configuring VPN Tunnel between Client and WatchGuard

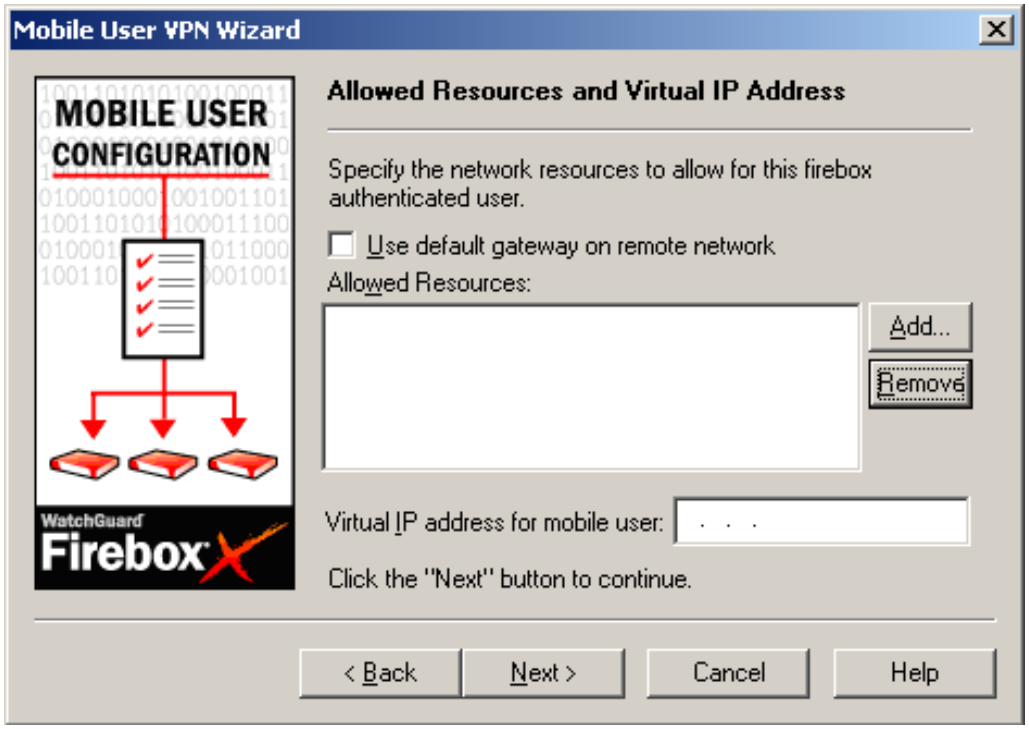
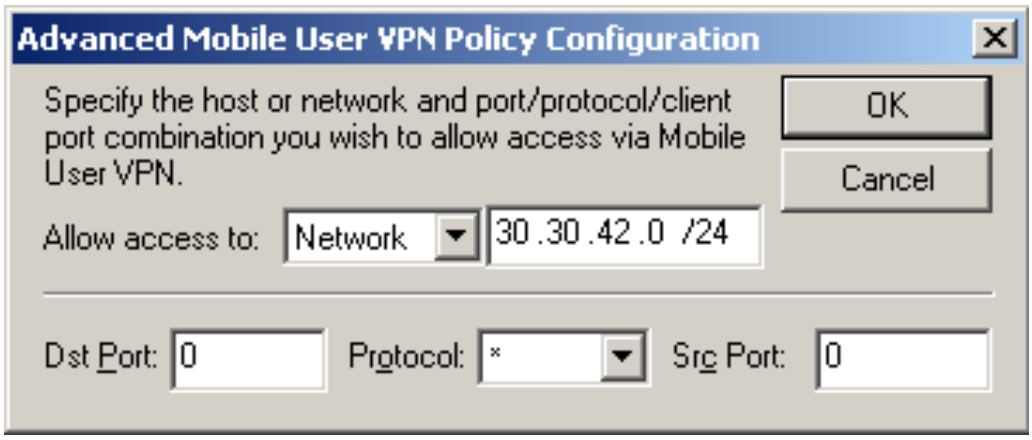
4.1. Configure the WatchGuard Firebox X

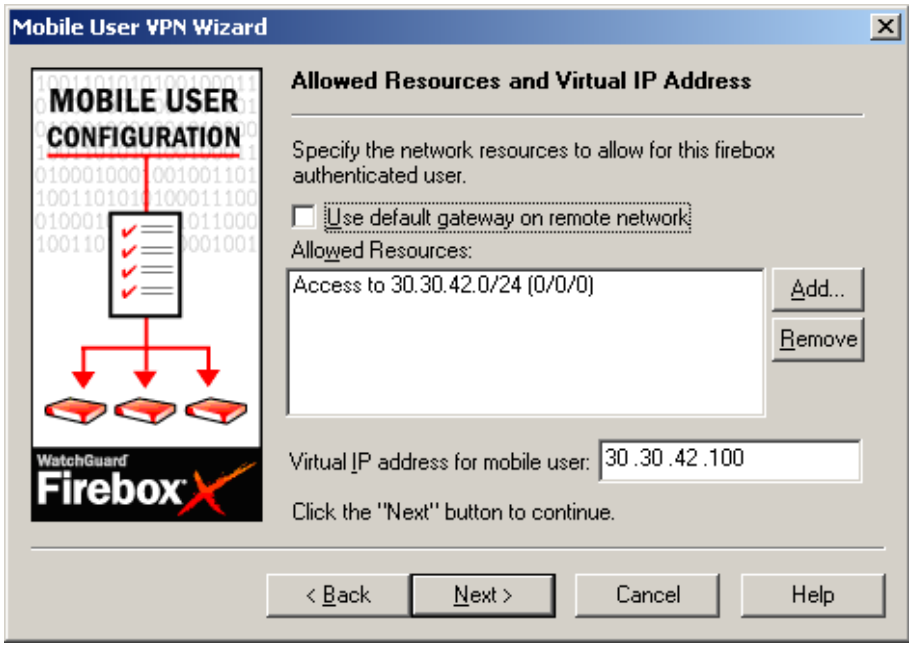
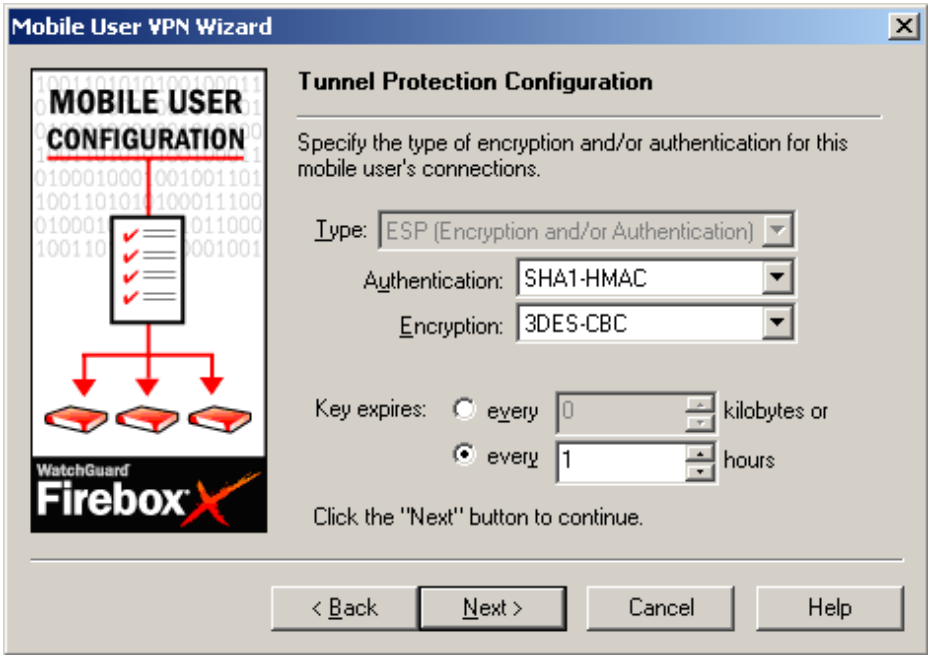
Step	Description
1.	Log into the Firebox X by navigating to **Start → Programs → WatchGuard → Firebox System Manager** from the Firebox System Manager PC.  Select **Tools → Policy Manager** or click on the taskbar icon.
2.	Click on **Network → Remote User…** to add a new MUVPN client for Phone Manager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

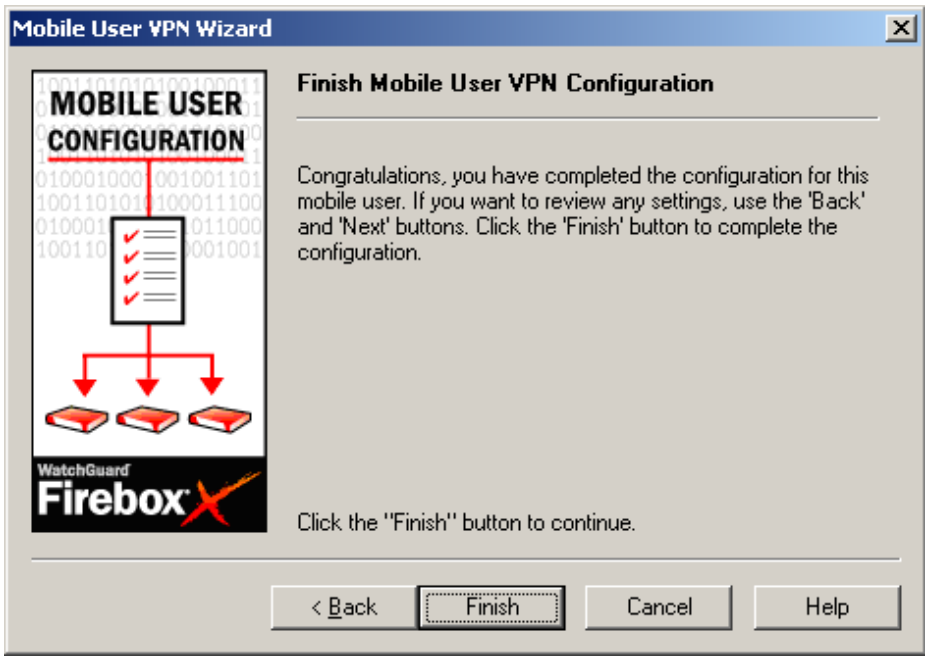
Step	Description
3.	Select **Firebox Authenticated Users** and click **Add**. 
4.	Click **Next** to use the Mobile User VPN Wizard to configure the VPN tunnel for the MUVPN client. 

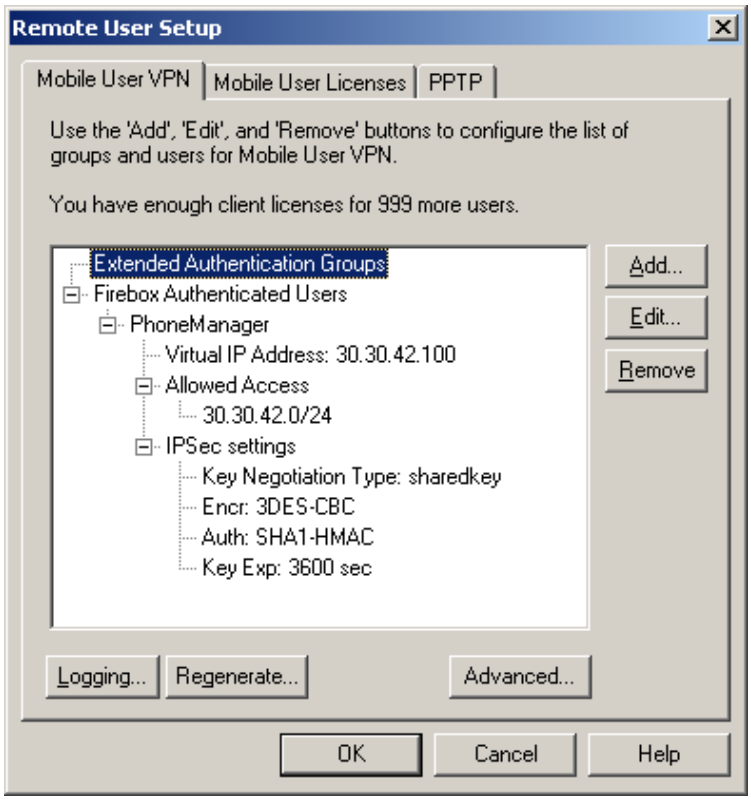
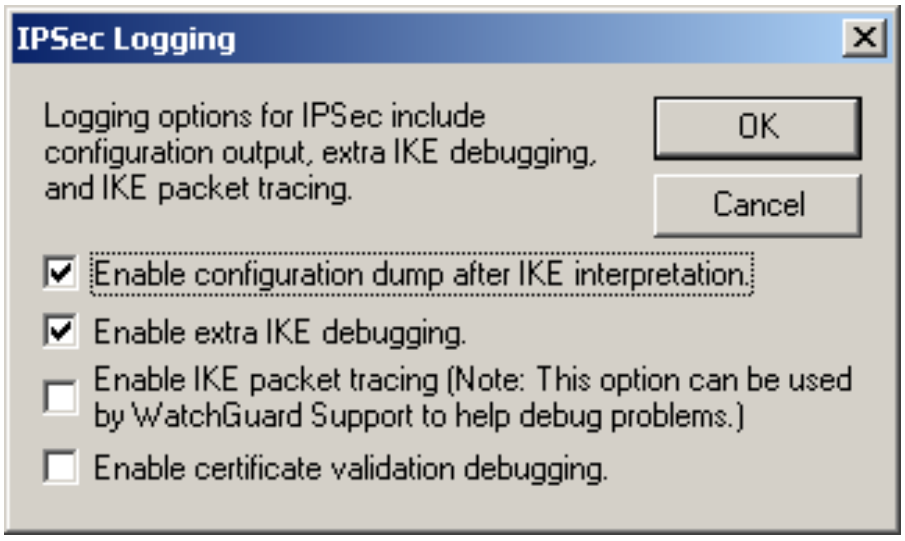
Step	Description
5.	Click **Add New…** to add a new mobile user VPN account. 
6.	Enter the *User Name* and *Passphrase* to be used by the MUVPN client as the shared key for Phase 1 authentication. This user will be automatically added to the ipsec_users group. Click **OK**. 

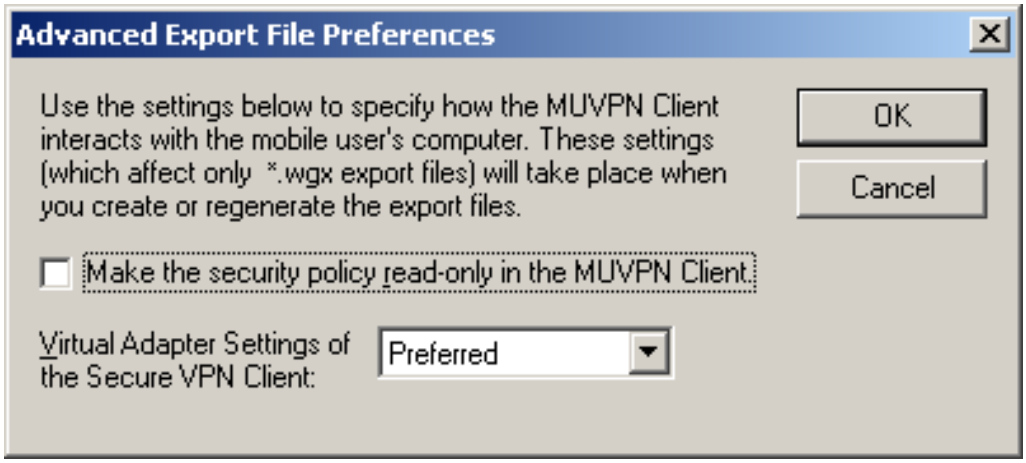
Step	Description
7.	Click **Next** to continue. The *Enter Shared Key* and *Confirm* fields have been populated with the passphrase entered in the previous step. 
8.	Select the option to **Use the passphrase of the end-user profile (the .wgx or .exp file) as the pre-shared key**. Click **Next**. 

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

Step	Description
11.	Enter a virtual IP address (e.g., **30.30.42.100**) for the MUVPN client. Click **Next**. 
12.	Enter the values shown below for Phase 2 from **Table 1**. Phase 2 re-authentication is set to occur every hour. Click **Next**. • Authentication – The password authentication used by the tunnel. • Encryption – The encryption method used by the tunnel. 

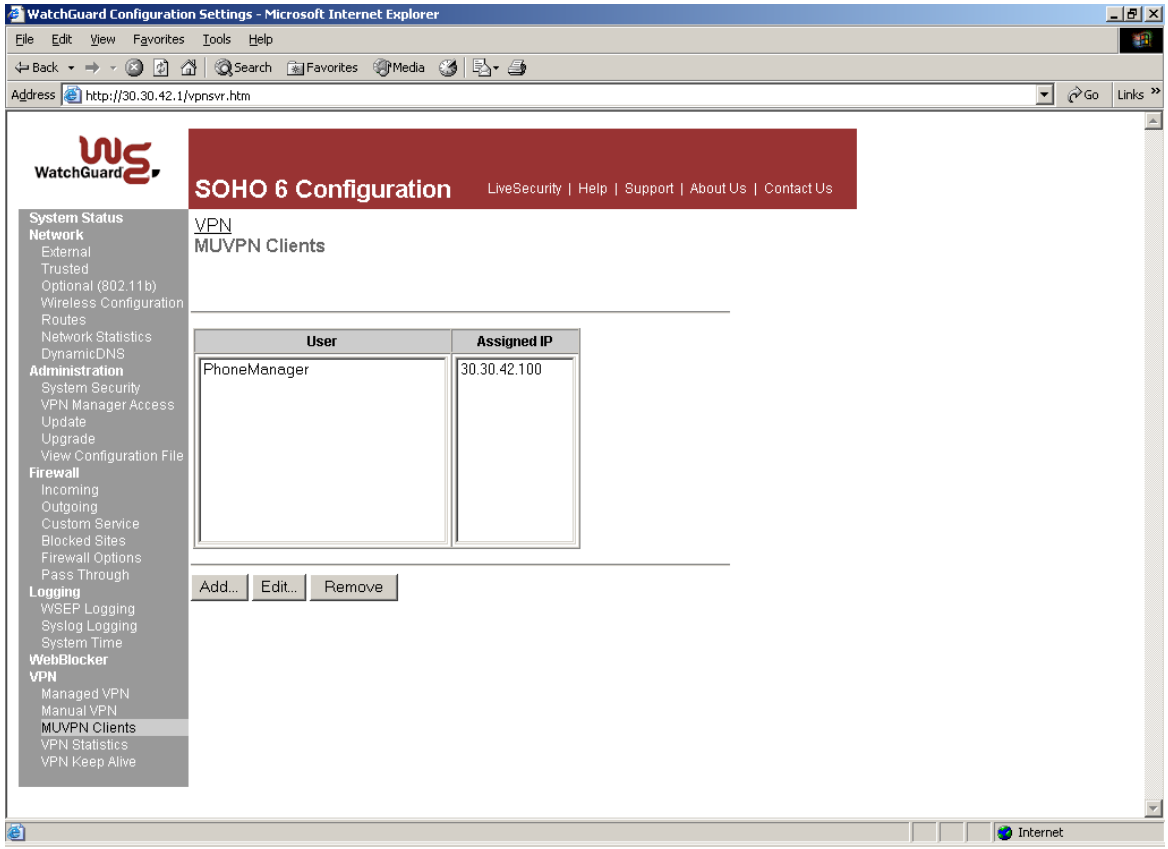
Step	Description
13.	Click **Finish** to complete the mobile user VPN configuration and return to the "Remote User Setup" window. This will result in the creation of a file with a .wgx extension which can be used to update the security policy of the MUVPN client. The WatchGuard Policy Import utility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

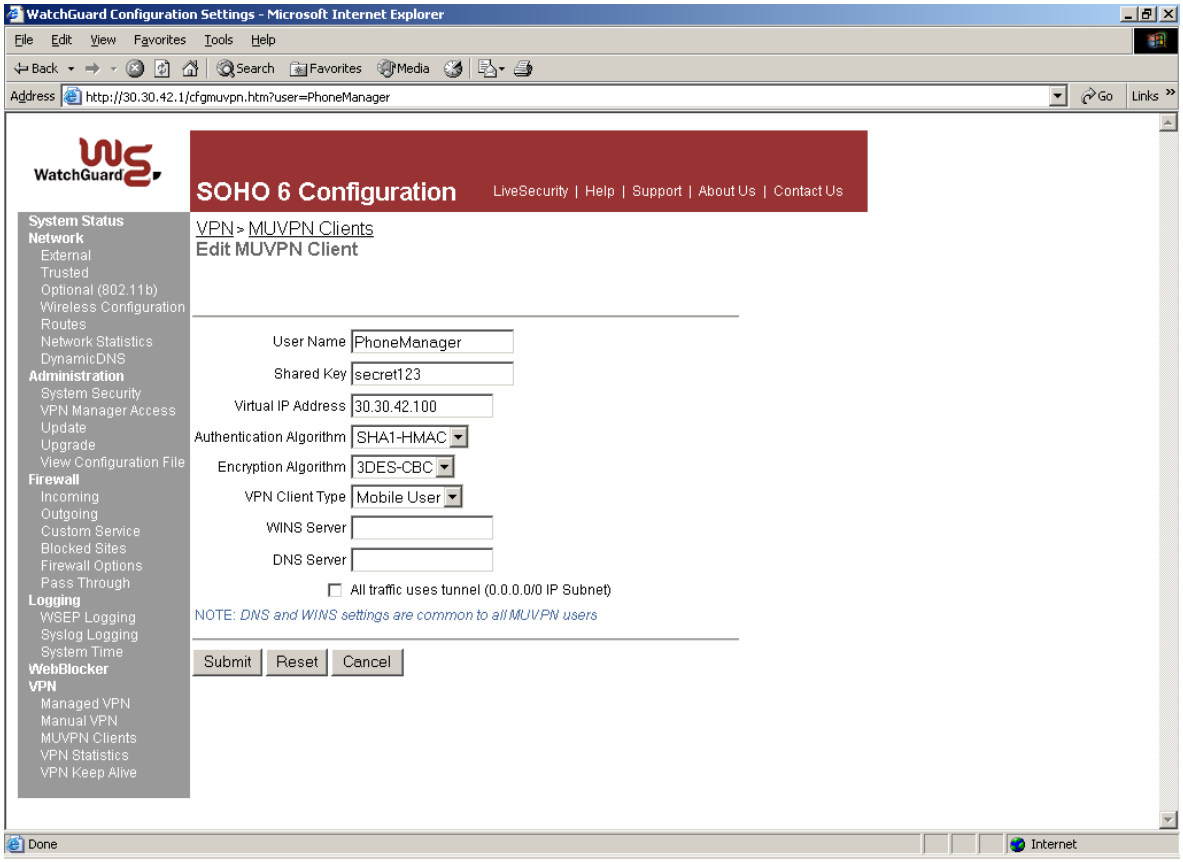
Step	Description
14.	If desired, click **Logging…** from the "Remote User Setup" window to enable IPSec logging for debugging purposes. 
15.	If logging was selected, check the options shown below to include the configuration output and extra IKE debugging in the log and click **OK** to return to the "Remote User Setup" window. 

Step	Description
16.	Click **Advanced…** from the "Remote User Setup" window and select **Preferred** for the *Virtual Adapter Settings of the Secure VPN Client*. Click **OK** to return to Remote User Setup. Click **OK** to return to Policy Manager. 

4.2. Configure the WatchGuard SOHO 6tc Wireless

Step	Description
1.	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 **MUVPN Clients** option on the left pane and click **Add** to add a MUVPN tunnel to the SOHO.

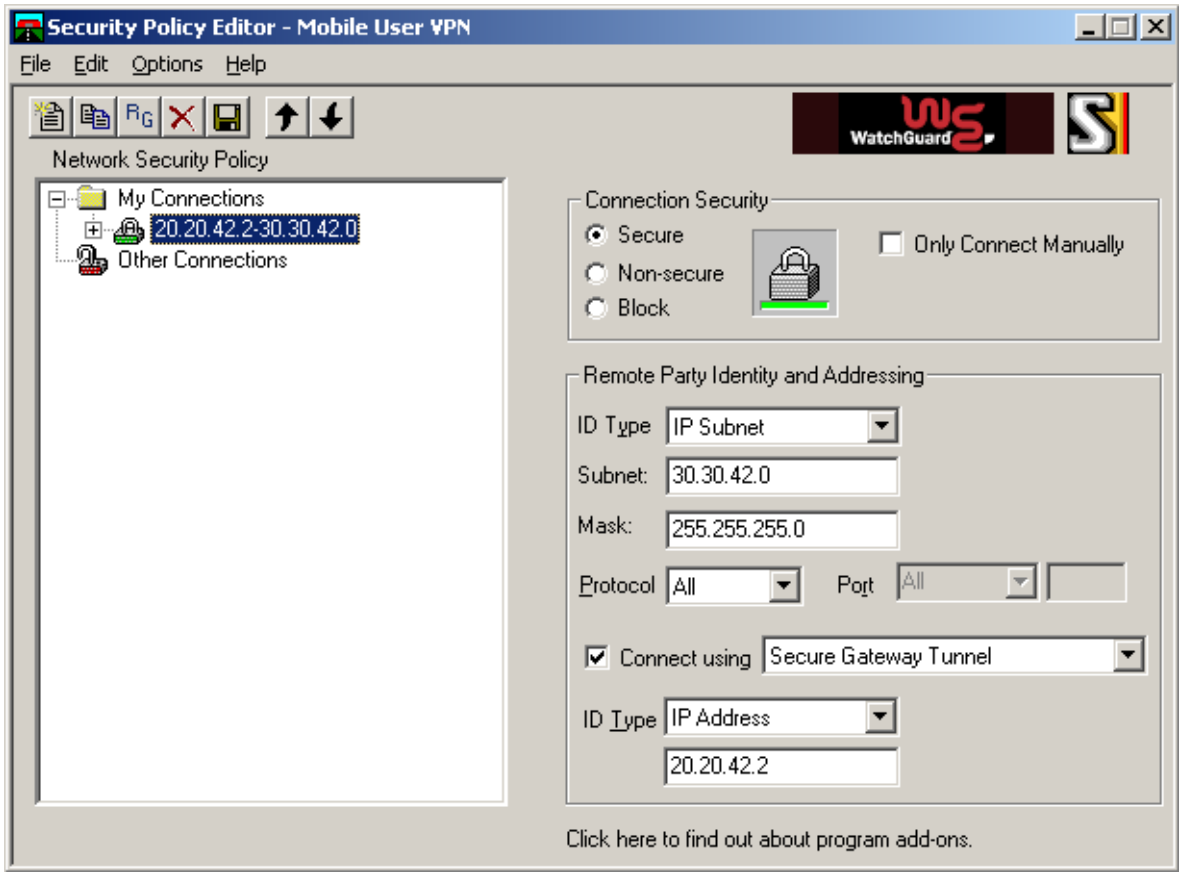


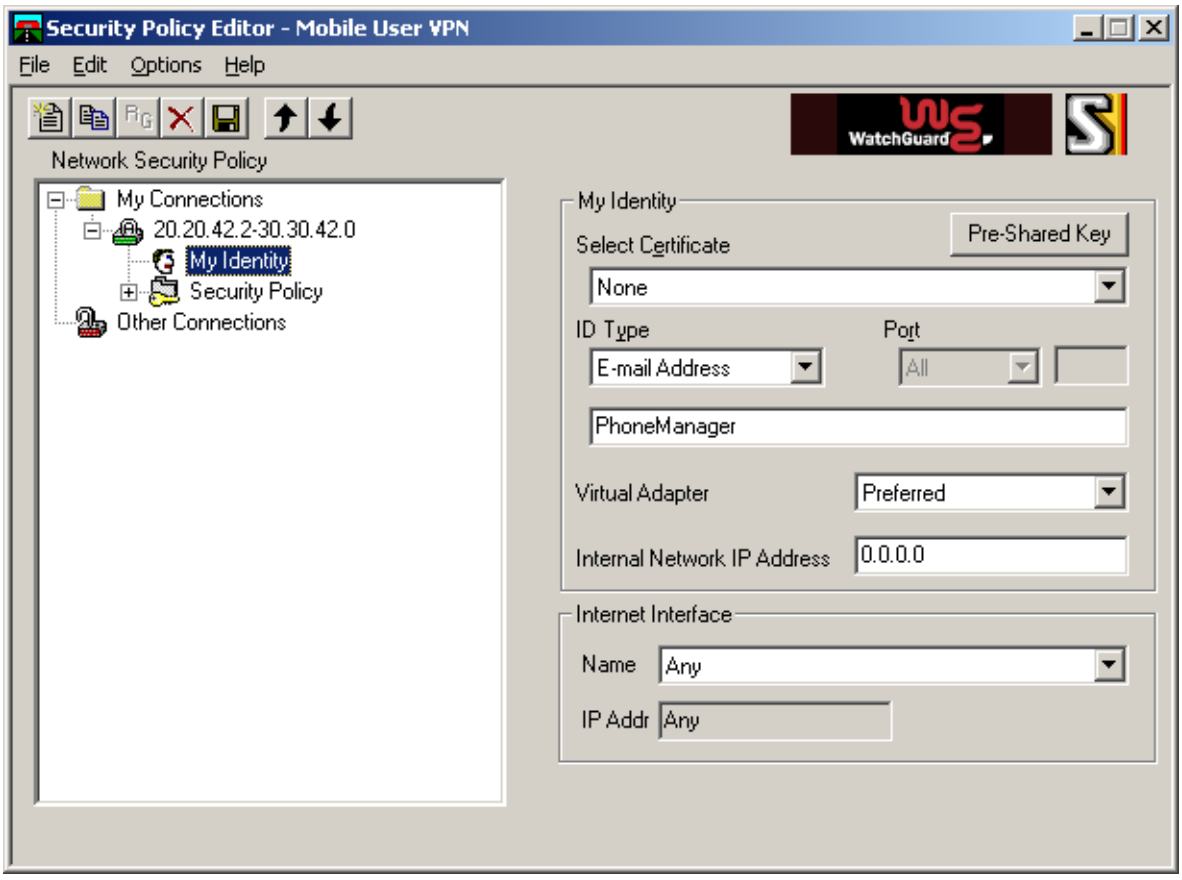
Step	Description
2.	Enter the values shown below for Phase 2 from **Table 1**. • User Name – The name of the MUVPN client • Shared Key – The password used for authentication and must match on the device at the other end of the tunnel. • Virtual IP Address – The virtual IP address assigned to the MUVPN client. • Authentication Algorithm – The password authentication used by the tunnel. • Encryption Algorithm – The encryption method used by the tunnel. • VPN Client Type – **Mobile User** (MUVPN client)  Click **Submit**.

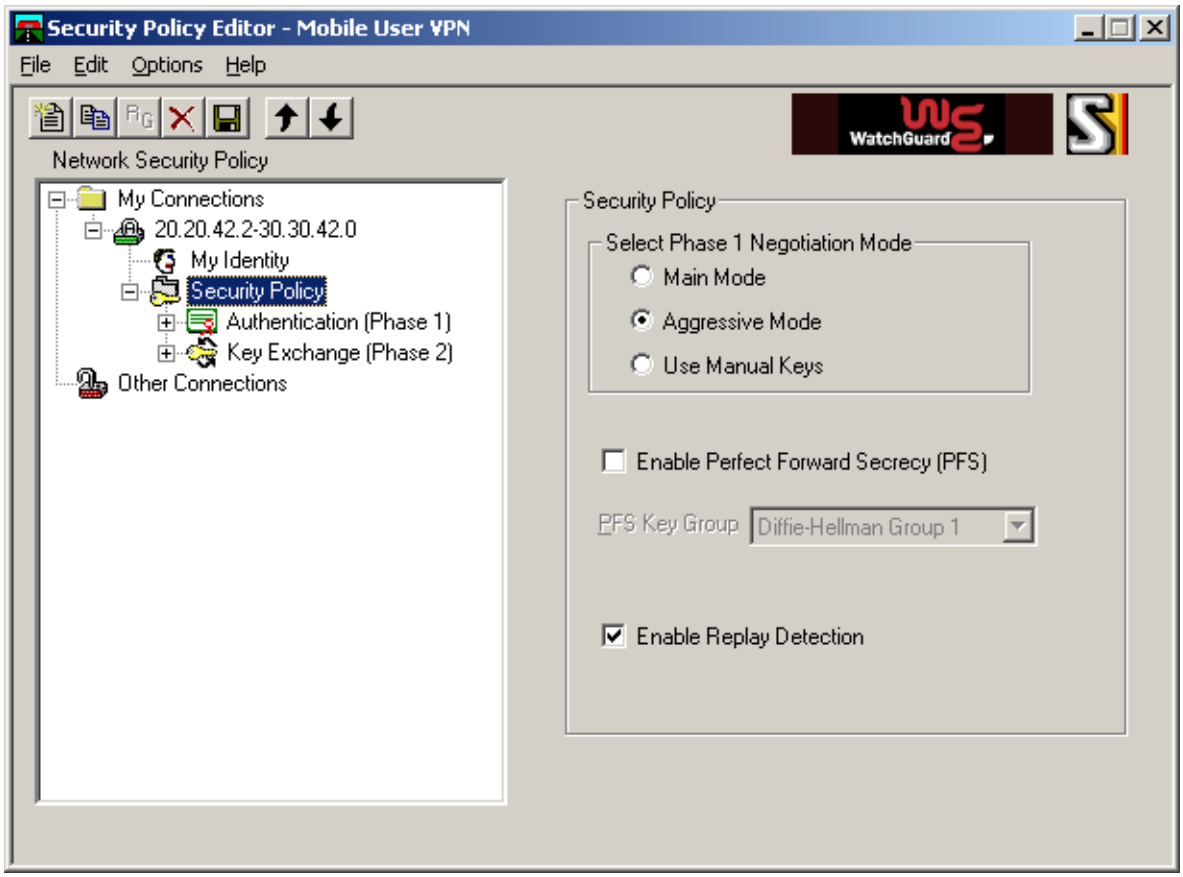
4.3. Configure the MUVPN Client

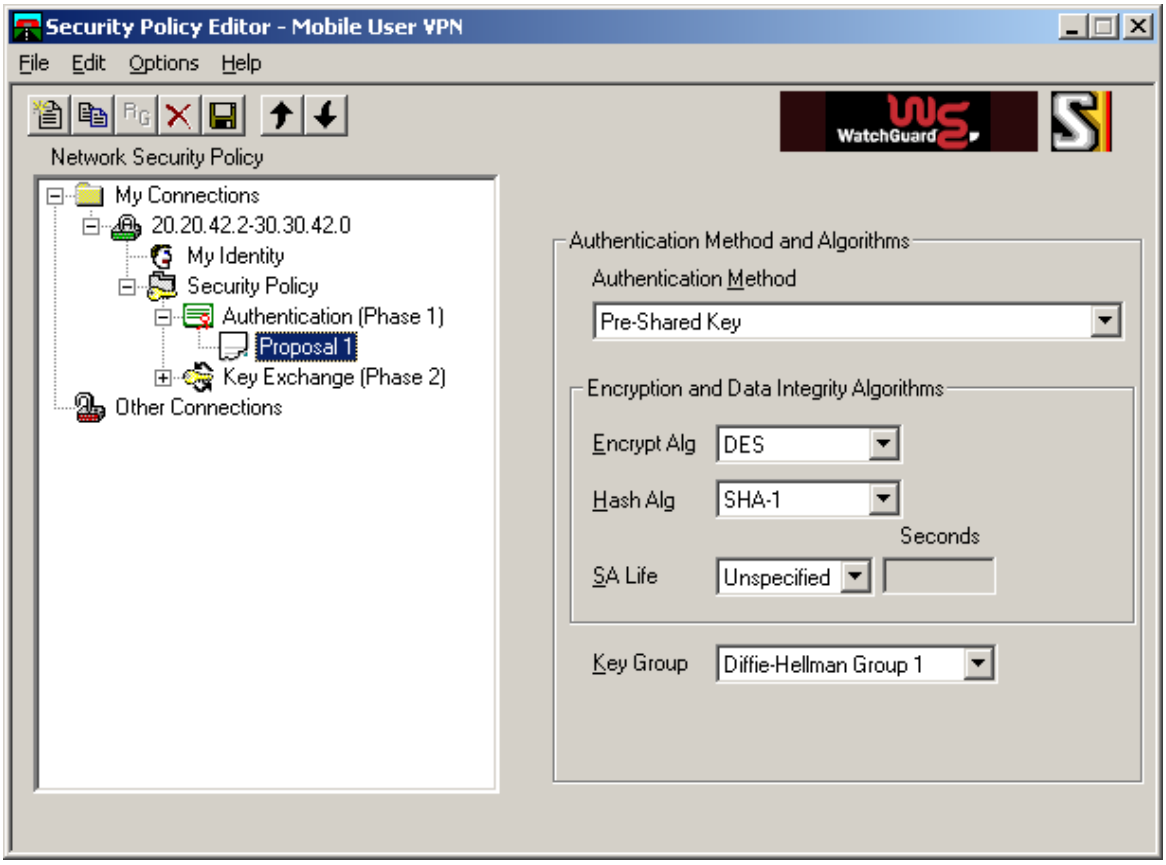
Note: The next two steps apply only if the PhoneManager MUVPN client was created using the Firebox System Manager.

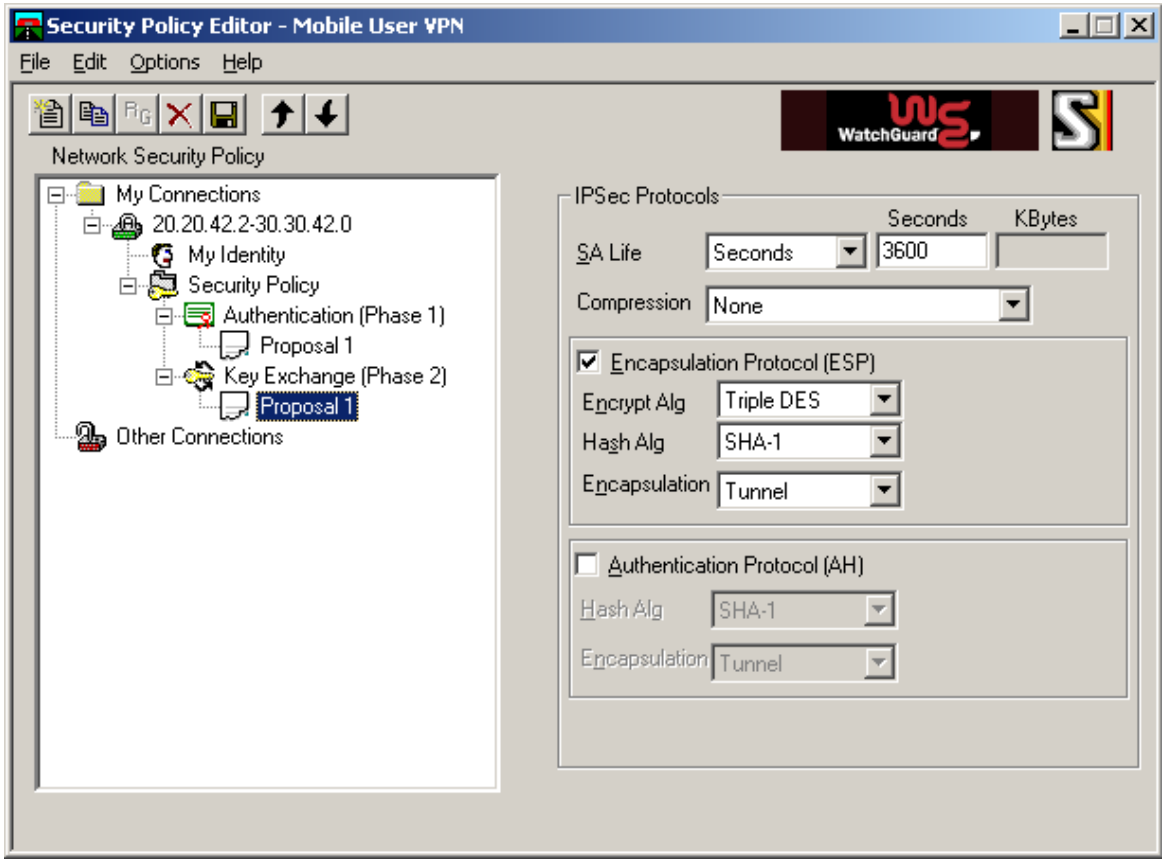
Step	Description
1.	Copy the PhoneManager.wgx file from the Firebox System Manager PC (e.g., c:\Program Files\WatchGuard\Ruvpn\20.20.42.2\wgx\PhoneManager directory) to the MUVPN client and double-click on it after installing the MUVPN software. Enter the same *Shared Key* that was used in step 7 of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

Step	Description
3.	**Note:** 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. Open the Security Policy Editor by navigating to **Start → Programs → Mobile User VPN → Security Policy Editor**. Right-click **My Connections** and select **Add → Connection**. Specify the name of the new connection (e.g., **20.20.42.2-30.30.42.0**) 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., **20.20.42.2**) is specified as the remote tunnel endpoint address. 

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

Step	Description
5.	Click **Security Policy. Aggressive Mode** was selected for the *Select Phase 1 Negotiation Mode* and leave the other fields as defaults. 

Step	Description
6.	Expand **Security Policy** and **Authentication (Phase1)**. Click **Proposal 1.** The values shown below are the defaults used for Phase 1 negotiation. 

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

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**:

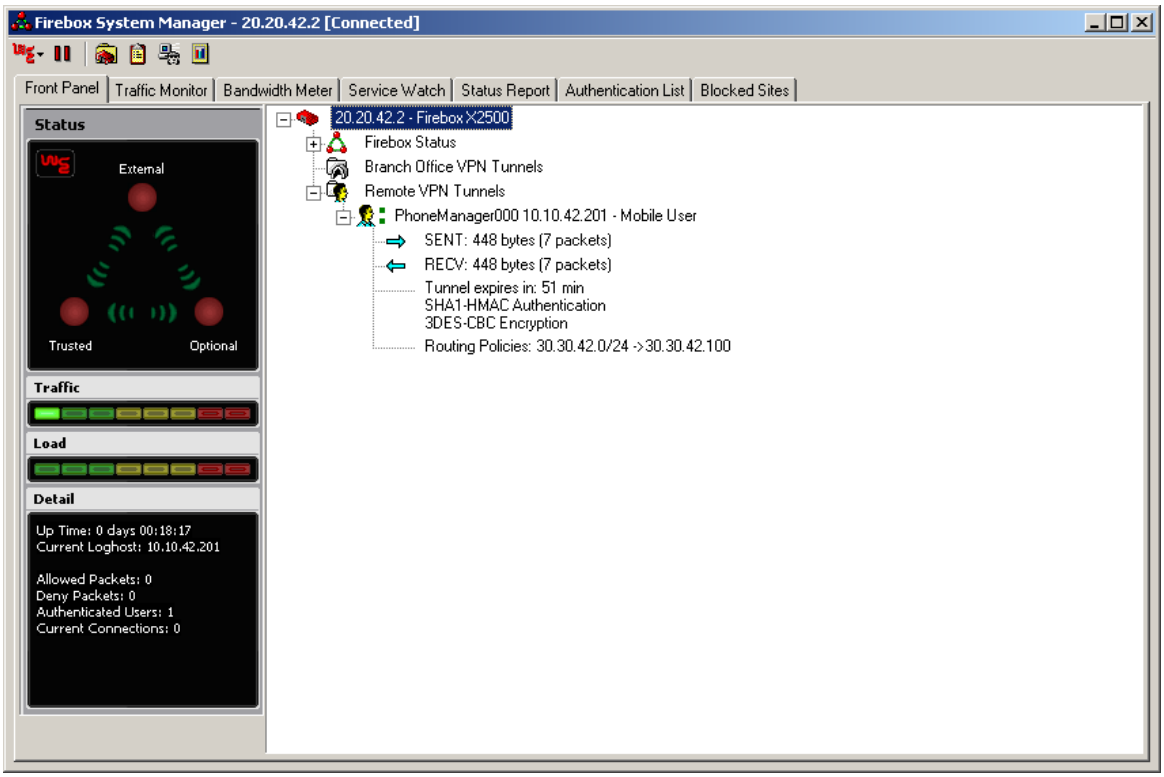
- Ability to establish a client VPN tunnel between the Firebox X or SOHO and the MUVPN client used for Phone Manager Pro.
- RAS (Registration Admission Status) over the VPN tunnel.
- Voice calls were placed manually and subjective quality noted for both G.711 mu-law and G.729 codecs. Direct Media Path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

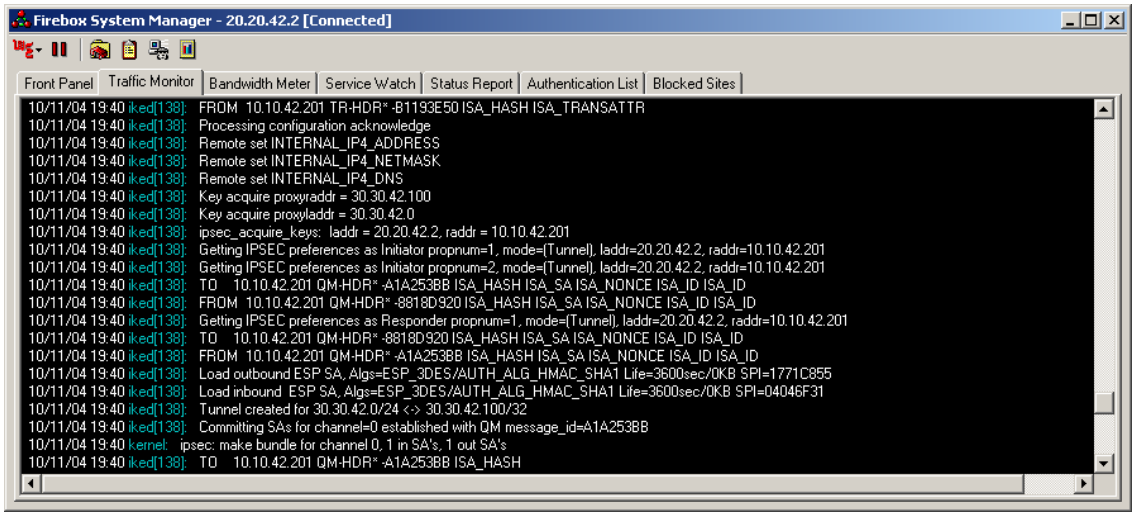
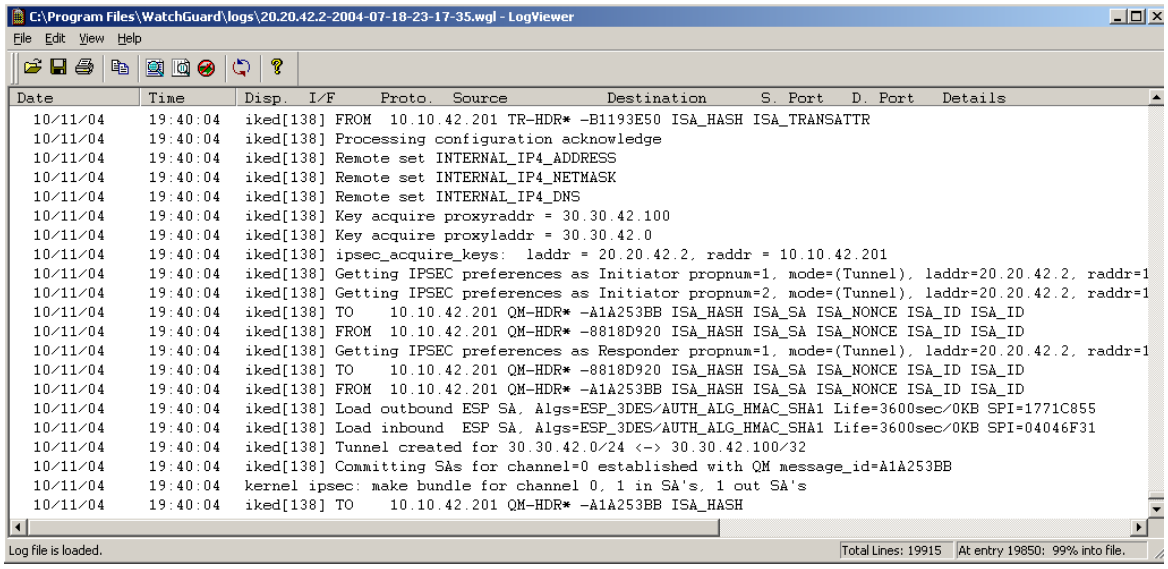
4.6. Test Results

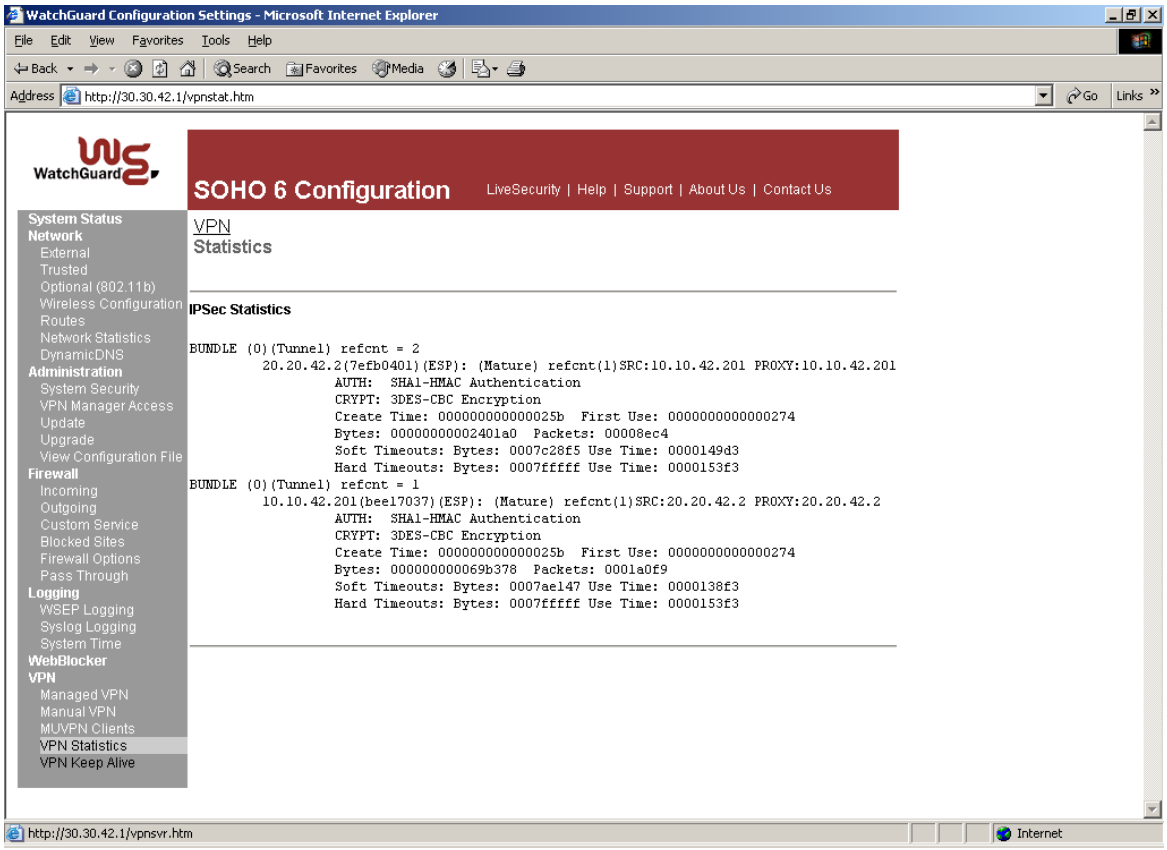
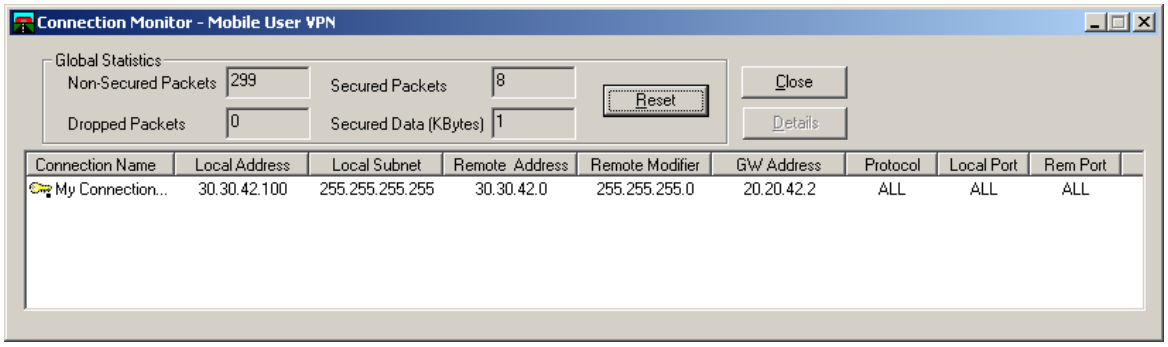
Testing was successful. Client VPN tunnels could be established between the Firebox X or SOHO with the MUVPN client used by Phone Manager Pro.

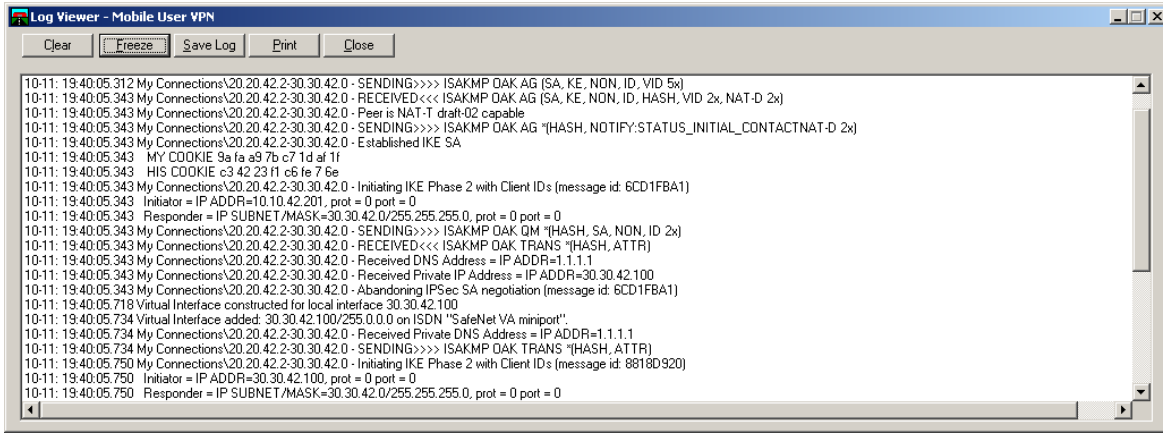
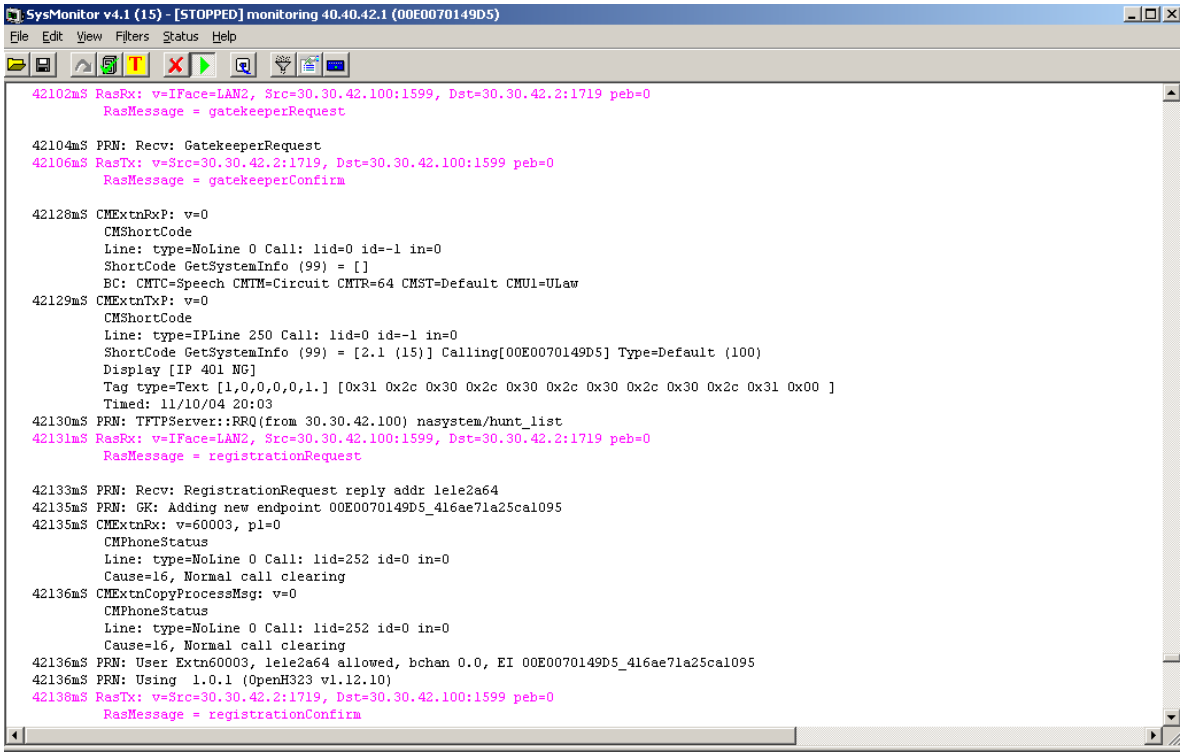
5. Verification Steps

Step	Description
1.	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.



Step	Description
2.	Click on the **Traffic Monitor** tab to view Phase 1 negotiation messages. 
3.	From the Firebox System Manager, select **Tools → Log Viewer** or click on the taskbar icon to view the Phase 1 negotiation message history. 

Step	Description
4.	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 **VPN Statistics** option on the left pane to view statistics for the client VPN tunnel between the SOHO and MUVPN client. 
5.	On the Phone Manager Pro PC, navigate to **Start → Programs → Mobile User VPN → Connection Monitor** to view statistics for the client VPN tunnel to the Firebox X or SOHO device. 

Step	Description
6.	On the Phone Manager Pro PC, navigate to **Start → Programs → Mobile User VPN → Log Viewer** to view Phase 1 and Phase 2 negotiation messages for the client VPN tunnel to Firebox X or SOHO device. 
7.	Using the IP Office SysMonitor log, confirm Phone Manager Pro registration. 

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

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.