



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Client VPN Tunnels from Avaya Phone Manager Pro to the WatchGuard Firebox X Edge X50W Wireless Security Appliance – Issue 1.0

Abstract

These Application Notes cover the configuration of a client VPN (Virtual Private Network) tunnel from Avaya Phone Manager Pro to the WatchGuard Firebox X Edge X50W Wireless security appliance. The WatchGuard SafeNet Mobile User VPN (MUVPN) software is used on the Avaya Phone Manager Pro PC to establish the VPN tunnel. 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 a client VPN (Virtual Private Network) tunnel from a PC running Avaya Phone Manager Pro to the WatchGuard Firebox X Edge X50W Wireless security appliance. The WatchGuard SafeNet Mobile User VPN (MUVPN) software is used on the Avaya Phone Manager Pro PC to establish the VPN tunnel. This configuration does not cover QoS (Quality of Service) implementation to prioritize voice traffic.

The Firebox X Edge X50W 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**, a Client VPN tunnel is established between the Firebox X Edge X50W Wireless security appliance and the WatchGuard MUVPN client running on the Avaya Phone Manager Pro PC. The Avaya Phone Manager Pro is registered to the Avaya IP Office Small Office Edition. For the purposes of the configuration demonstrated in these Application Notes, the wireless capability of the Firebox Edge X50W is not used.

For configuration of the network infrastructure shown in **Figure 1**, refer to the appropriate documentation listed in Section 9.

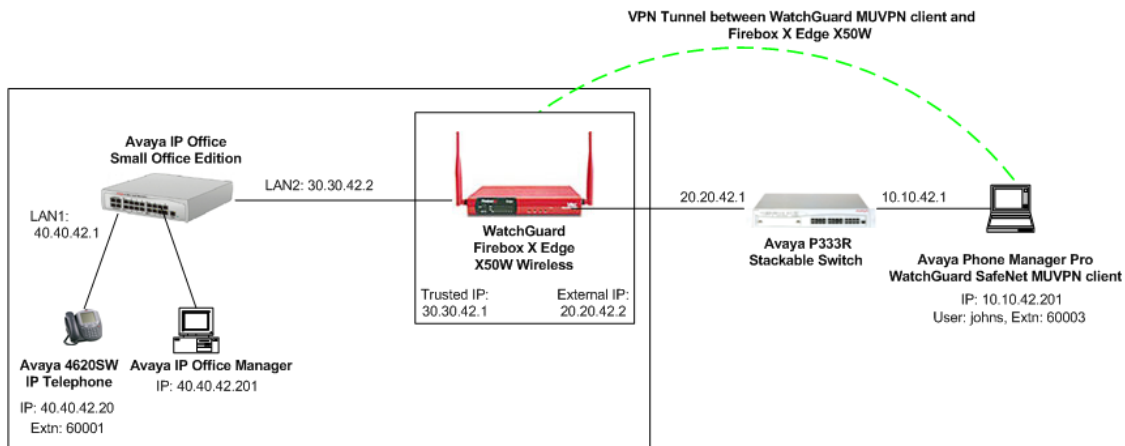


Figure 1 – Network Configuration Diagram

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	3.0(40)
Avaya IP Office Manager	5.0(40)
Avaya Phone Manager Pro	3.0(12)
Avaya P333R Stackable Switch	4.0.9
Avaya 4620SW IP Telephone	2.1.3
WatchGuard Firebox X Edge X50W Wireless	Boot ROM 7.1 Firewall 7.1.1 (Jan. 20, 2005 build 4)
WatchGuard SafeNet MUVPN client	MuVPN 7.3

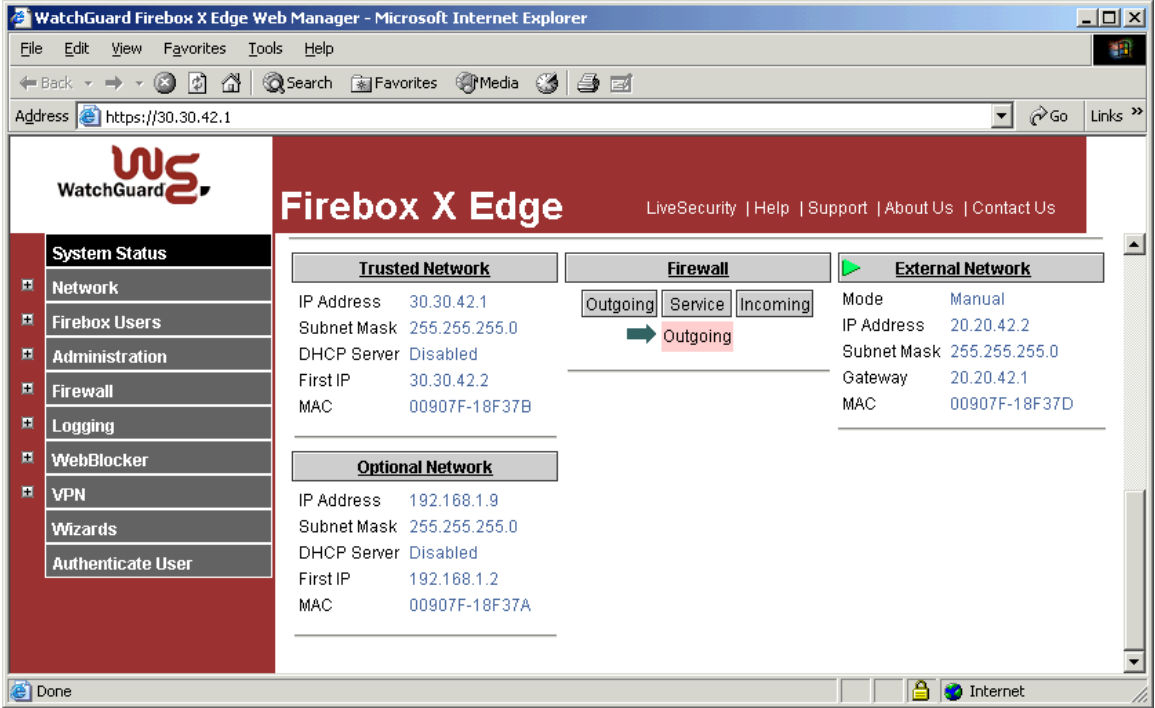
Table 2 – Product and Software/Version

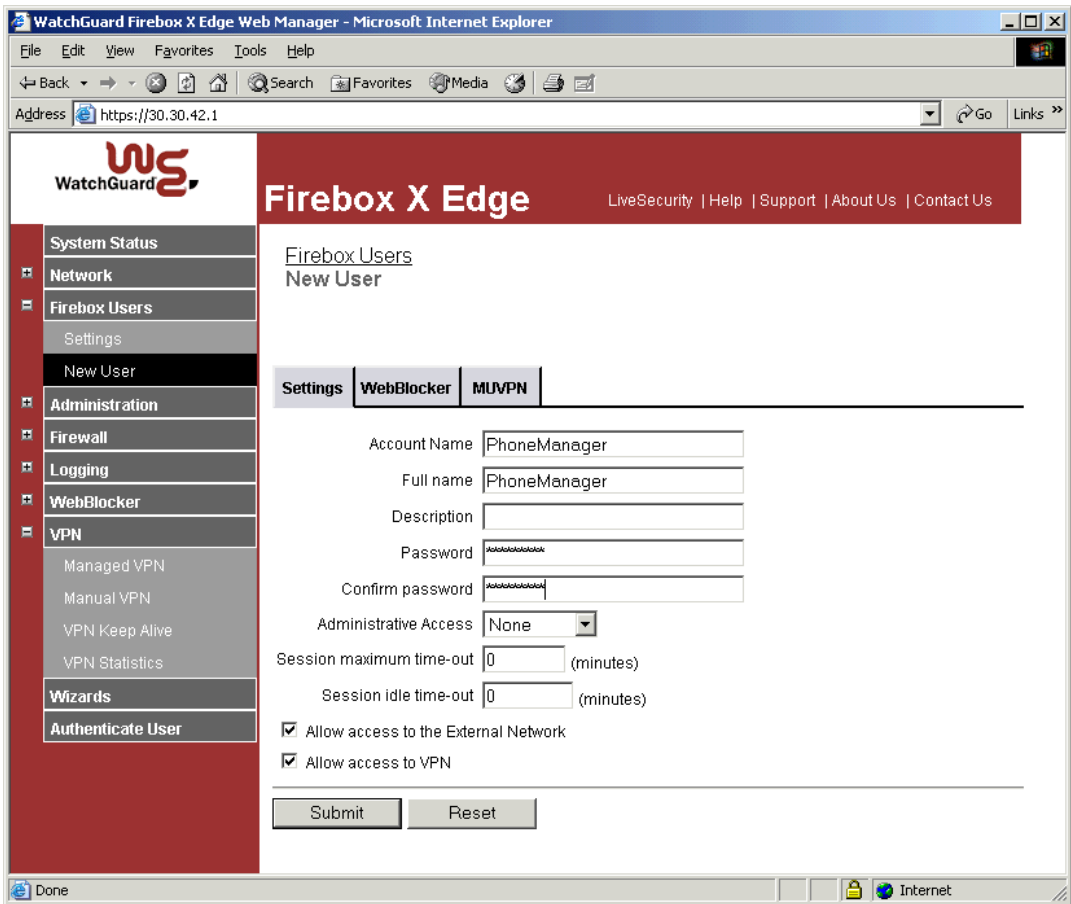
3. Configure the Avaya Phone Manager Pro

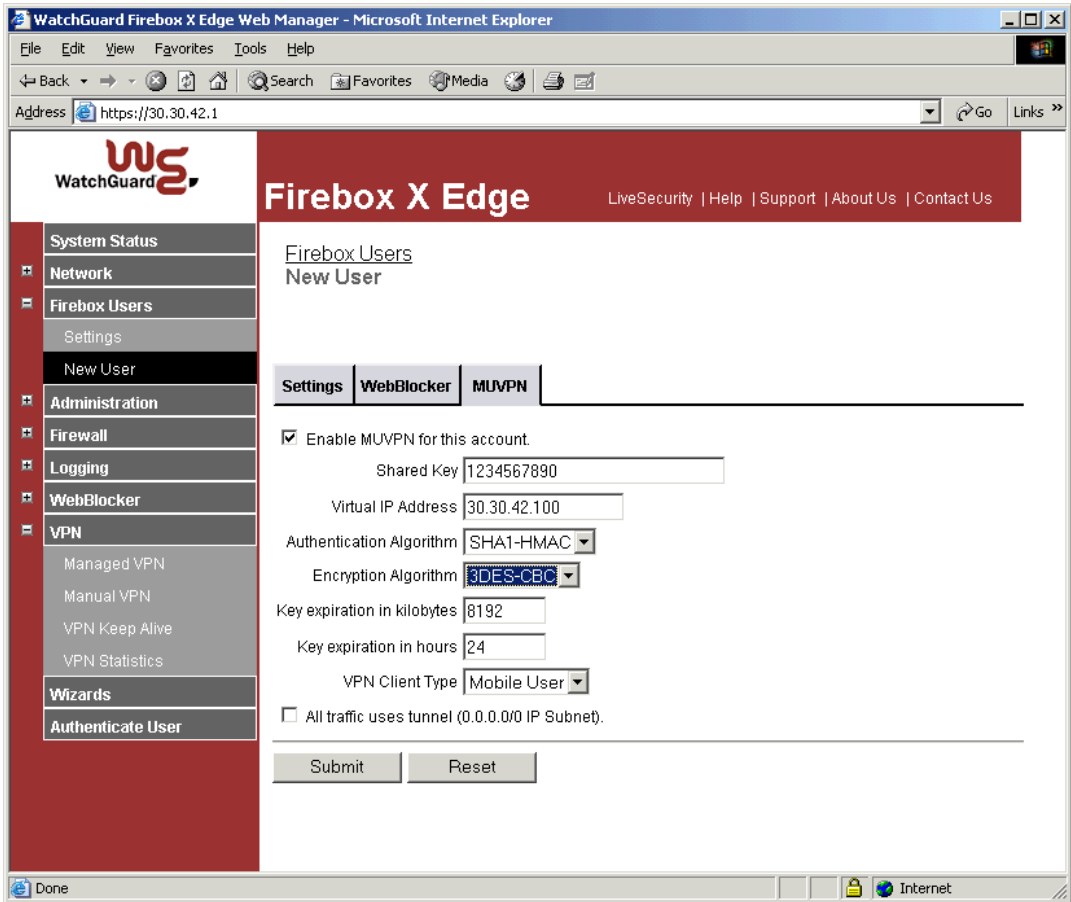
Step	Description
1.	<p>Click Start → Programs → IP Office → PhoneManager to start the PhoneManager Pro application. Click Configure → PBX and specify the LAN2 interface address for Avaya IP Office Small Office Edition (e.g., 30.30.42.2) in the <i>PBX Address</i> field. Select the name defined on the User form in IP Office Manager (e.g., johns) in the <i>UserName</i> field.</p>  <p>The image shows a 'PBX Configuration Information' dialog box with a purple border and a yellow title bar. Inside, there is a 'User Details' section with three fields: 'UserName' (a dropdown menu showing 'johns'), 'Password' (a field with ten black dots), and 'PBX Address' (a text field containing '30.30.42.2'). To the right of these fields are four buttons: 'OK' (yellow), 'Cancel' (gray), 'Help' (gray), and 'Login >>' (gray).</p>

4. Configure the VPN Tunnel between the MUVPN Client and the Firebox X Edge X50W

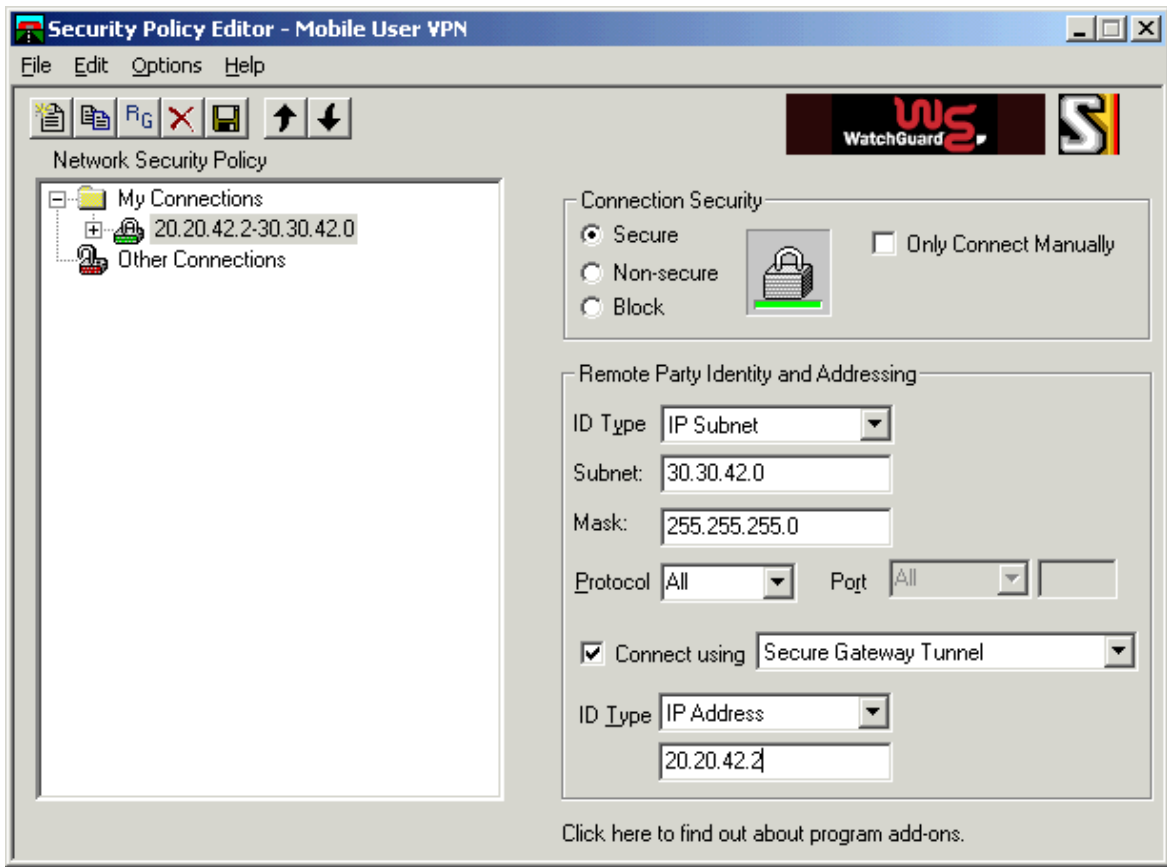
4.1. Configure the WatchGuard Firebox X Edge X50W Wireless

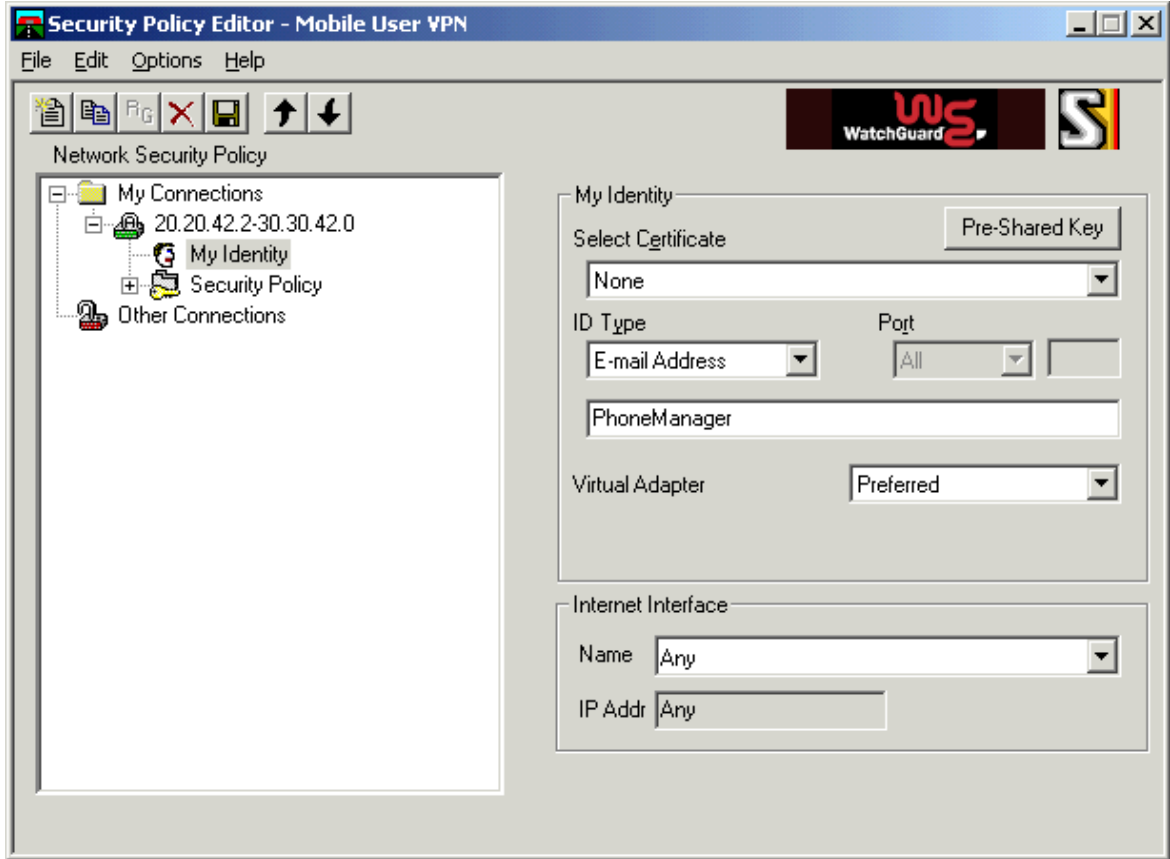
Step	Description
1.	<p>Open the Firebox X Edge X50W Wireless Configuration screen by specifying the IP address of the private interface of the Firebox X Edge X50W in a browser window.</p> 

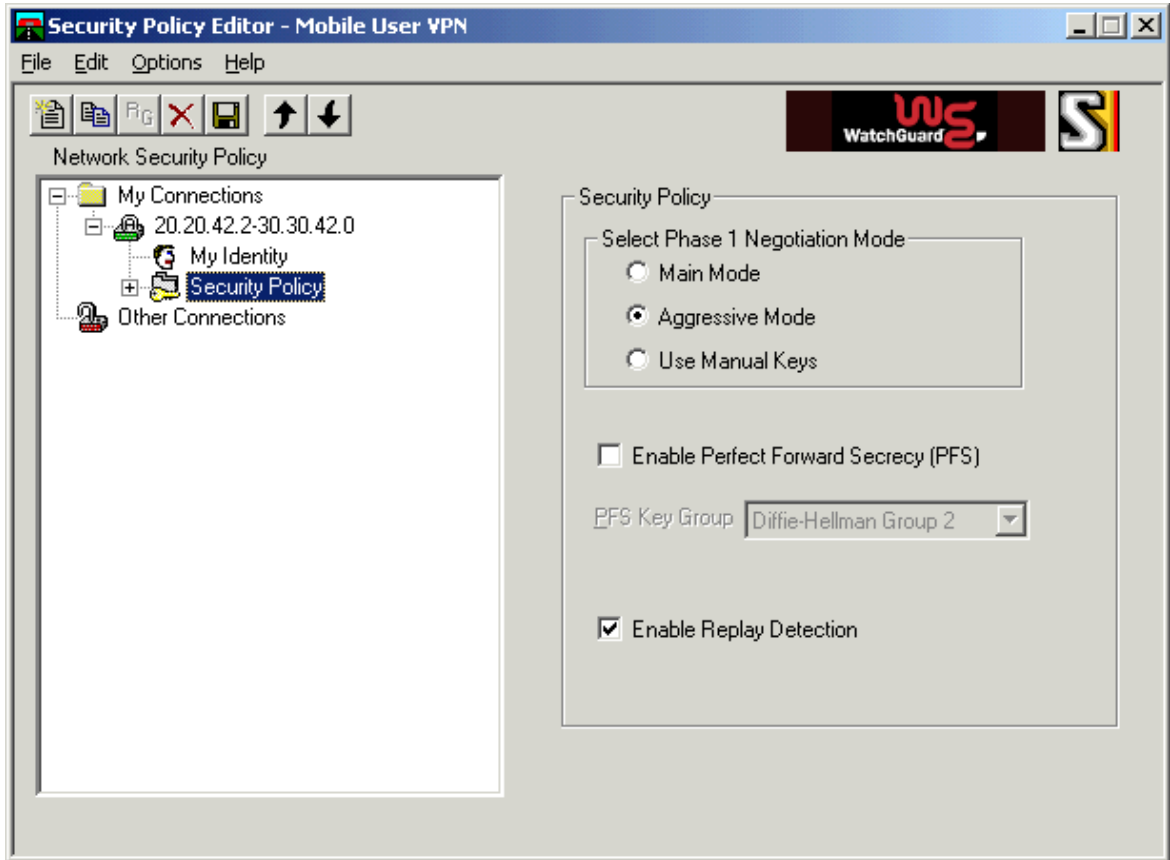
Step	Description
2.	<p>Click the Firebox Users → New User on the left pane. In the Settings tab that appears, enter the Account Name and Password for the new MUVPN client.</p> 

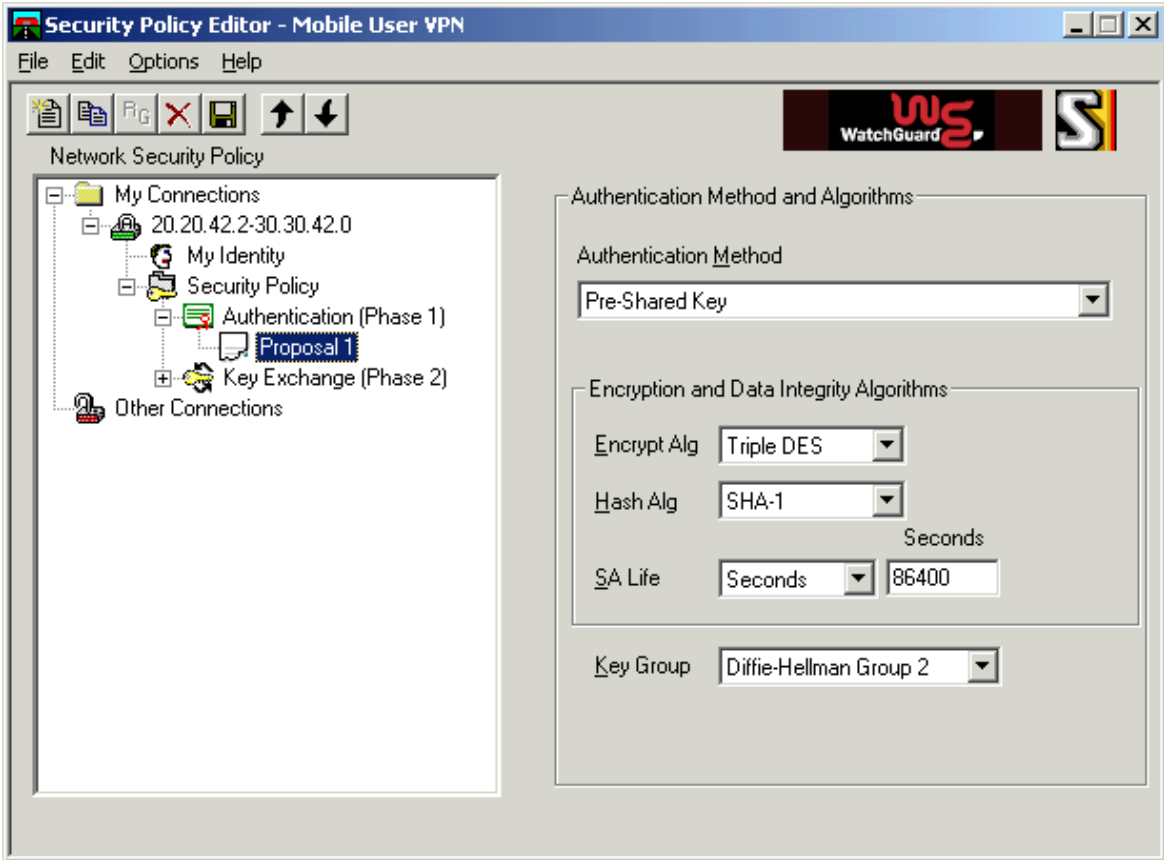
Step	Description
3.	<p>Click the MUVPN tab. Enter the values shown below for Phase 2 from Table 1.</p> <ul style="list-style-type: none"> • Shared Key – The password used for authentication and must match the password used on the MUVPN client at the other end of the tunnel in Section 4.2 Step 2. • Virtual IP Address – The virtual IP address to be assigned to the MUVPN client. • Authentication Algorithm – The password authentication used by the tunnel. • Encryption Algorithm – The encryption method used by the tunnel. • Key expiration in hours – The key expiration time must match the MUVPN client at the other end of the tunnel in Section 4.2 Step 4. • VPN Client Type – Mobile User (MUVPN client). <p>Click Submit.</p> 

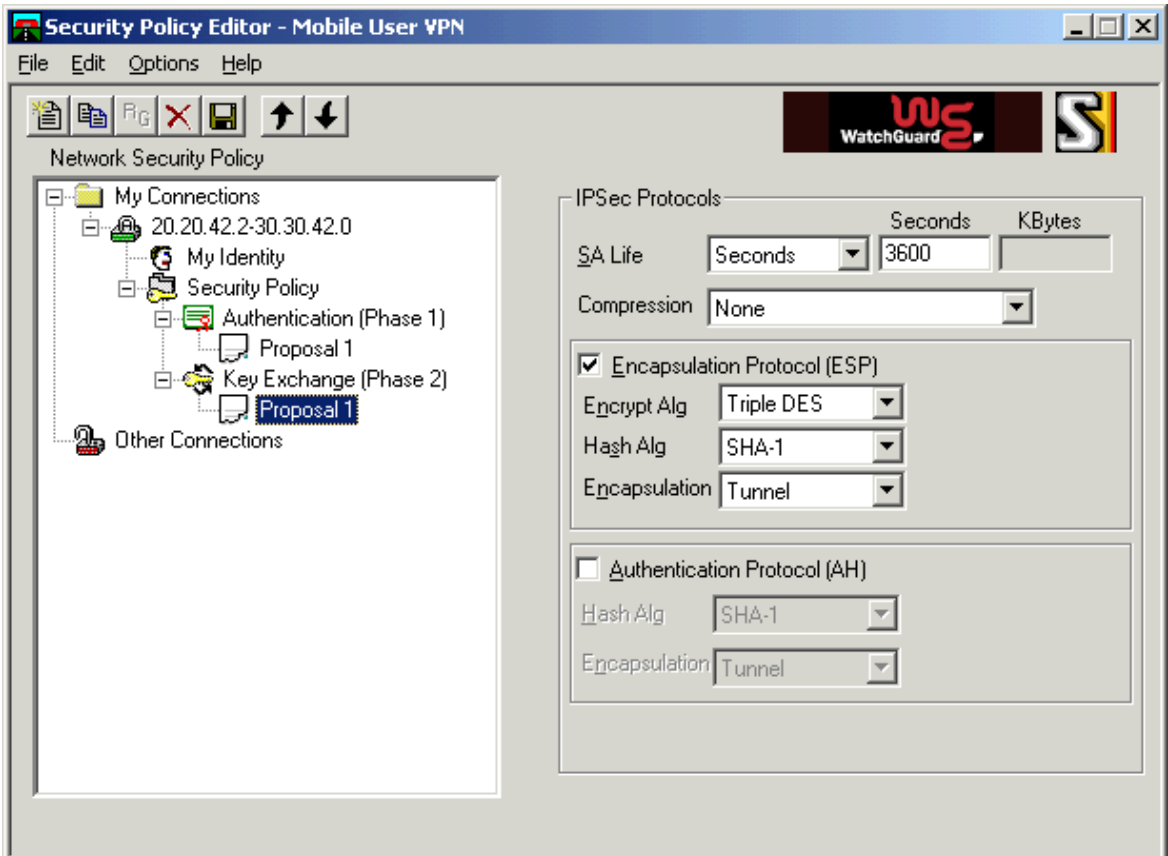

4.2. Configure the WatchGuard MUVPN Client

Step	Description
1.	<p>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 Edge X50W tunnel configuration. The remote subnet is that of the Avaya IP Office Small Office Edition LAN2 interface. The IP address of the external interface of the Firebox X Edge X50W (e.g., 20.20.42.2) is specified as the remote tunnel endpoint address.</p> 

Step	Description
2.	<p>Expand the new connection by clicking on the “+” next to the connection name and click My Identity. Select None in the <i>Select Certificate</i> drop-down list. Click Pre-Shared Key and Enter Key to supply the same password specified in the Firebox X Edge X50W tunnel configuration. Select E-mail Address for the <i>ID Type</i> 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.</p> 

Step	Description
3.	<p>Click Security Policy. Select Aggressive Mode for <i>Select Phase 1 Negotiation Mode</i> and leave the other fields as defaults.</p>  <p>The screenshot shows the 'Security Policy Editor - Mobile User VPN' window. The left pane, titled 'Network Security Policy', contains a tree view with the following items: 'My Connections' (expanded), '20.20.42.2-30.30.42.0', 'My Identity', 'Security Policy' (highlighted), and 'Other Connections'. The right pane, titled 'Security Policy', contains the following settings:</p> <ul style="list-style-type: none"> Select Phase 1 Negotiation Mode: Three radio buttons are present: 'Main Mode' (unselected), 'Aggressive Mode' (selected), and 'Use Manual Keys' (unselected). Enable Perfect Forward Secrecy (PFS): An unchecked checkbox. PFS Key Group: A dropdown menu currently showing 'Diffie-Hellman Group 2'. Enable Replay Detection: A checked checkbox.

Step	Description
4.	<p>Expand Security Policy and Authentication (Phase1). Click Proposal 1 and enter the values shown below to match the Firebox X Edge X50W tunnel configuration for Phase 1.</p> 

Step	Description
5.	<p>Expand Key Exchange (Phase2). Click Proposal 1 and enter the values shown below to match the Firebox X Edge X50W tunnel configuration for Phase 2.</p> 
6.	Click File → Save or the floppy disk icon  on the tool bar to save the configuration.

5. Interoperability Compliance Testing

The features of the Firebox X Edge X50W Wireless security appliance were tested to determine if VPN tunnels could be established with the WatchGuard MUVPN client used on an Avaya Phone Manager Pro PC.

5.1. General Test Approach

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

- Ability to establish a VPN tunnel between the Firebox X Edge X50W Wireless security appliance and the MUVPN client used on Phone Manager Pro PC.
- Avaya Phone Manager Pro registers with Avaya IP Office Small Office Edition 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. That is, the Firebox X Edge X50W Wireless security appliance lists the 30.30.42.0 subnet as the protected network. The Firebox X Edge X50W Wireless cannot add the Avaya IP Office Small Office Edition LAN1 network (40.40.42.0), which is NATed, to the remote subnet list.

5.2. Test Results

Testing was successful. A client VPN tunnel could be established between the Firebox X Edge X50W Wireless security appliance and the Phone Manager Pro PC using the MUVPN client.

6. Verification Steps

The following steps may be used to verify the configuration:

- Open the Firebox X Edge X50W Wireless Configuration screen by specifying the IP address of the private interface of the Firebox X Edge X50W in a browser window. Click **VPN → IPSec Statistics** on the left pane to view statistics for the client VPN tunnel between the Firebox X Edge X50W and MUVPN client. Verify that statistics are listed for the MUVPN client PC and the Firebox X Edge X50W such as the type of authentication and encryptions used by each side to the tunnel and the IP addresses on each side of the tunnel.

- 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 Edge X50W. Verify that the Local and Remote IP Addresses as well as Gateway IP Address are listed for the established connection.
- 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 the Firebox X Edge X50W. Verify messages indicating that the tunnel is coming up such as 'Establishing IKE SA' are listed.
- Use the Avaya IP Office SysMonitor to confirm Phone Manager Pro registration. Verify messages indicating the Phone Manager Pro is registering appear, i.e., 'GK: Adding new endpoint...'

7. Support

Customers should call WatchGuard Technologies, Inc. Customer Support when having problems related to the WatchGuard Firebox X Edge X50W Wireless or WatchGuard SafeNet MUVPN client.

For technical support on the WatchGuard products discussed in these Application Notes, contact WatchGuard Technical Support at (877) 232-3531 or visit <http://www.watchguard.com/support>.

8. Conclusion

The configuration of a client VPN tunnel between the WatchGuard Firebox X Edge X50W Wireless security appliance and the WatchGuard MUVPN client used on the Avaya Phone Manager Pro PC has been successfully compliance tested.

9. References

- [1] *WatchGuard Firebox X Reviewer's Guide*, April 2004
- [2] *WatchGuard System Manager User Guide*, 2004
- [3] *WatchGuard Firebox X Edge User Guide*, Firmware Version 7.1, 2005
- [4] *Avaya IP Office Manager 3.0 Manual*, Issue 16p, 20th July 2005
- [5] *Avaya P333R Installation and Configuration Guide*, Software Version 4.0, April 2003

©2005 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.