Avaya Solution & Interoperability Test Lab

Application Notes for Configuring VPN Tunnels between Avaya IP Office and WatchGuard Firebox X Edge X50W Wireless – Issue 1.0

Abstract

These Application Notes describe the configuration of site-to-site VPN tunnels between Avaya IP Office and WatchGuard Firebox X Edge X50W Wireless. WatchGuard SafeNet Mobile User VPN (MUVPN) client tunnels to Avaya IP Office are also described. The Firebox X Edge X50W Wireless is an integrated security appliance for the small office/home office/teleworker that combines wireless access point, NAT, firewall, VPN, web content filtering, anti-virus, and secure remote management. Information in these Application Notes was 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 describe the configuration of a site-to-site VPN (Virtual Private Network) tunnel between an Avaya IP Office and WatchGuard Firebox X Edge X50W Wireless. Configuration of a client VPN tunnel to Avaya IP Office using WatchGuard SafeNet Mobile User VPN (MUVPN) client is also described. The Firebox X Edge X50W Wireless is an integrated security appliance for the small office/home office/teleworker that combines wireless access point, NAT, firewall, VPN, web content filtering, anti-virus, and secure remote management.

The site-to-site VPN tunnel depicted in **Figure 1** is between the Avaya IP Office Small Office Edition and the Firebox X Edge X50W Wireless. The client VPN tunnel in **Figure 1** is between the Avaya IP Office Small Office Edition and the WatchGuard MUVPN client running on the Avaya Phone Manager Pro PC. During compliance testing, the site-to-site VPN configuration and the client VPN tunnel configuration were mutually exclusive. That is, the two configurations did not exist at once.

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

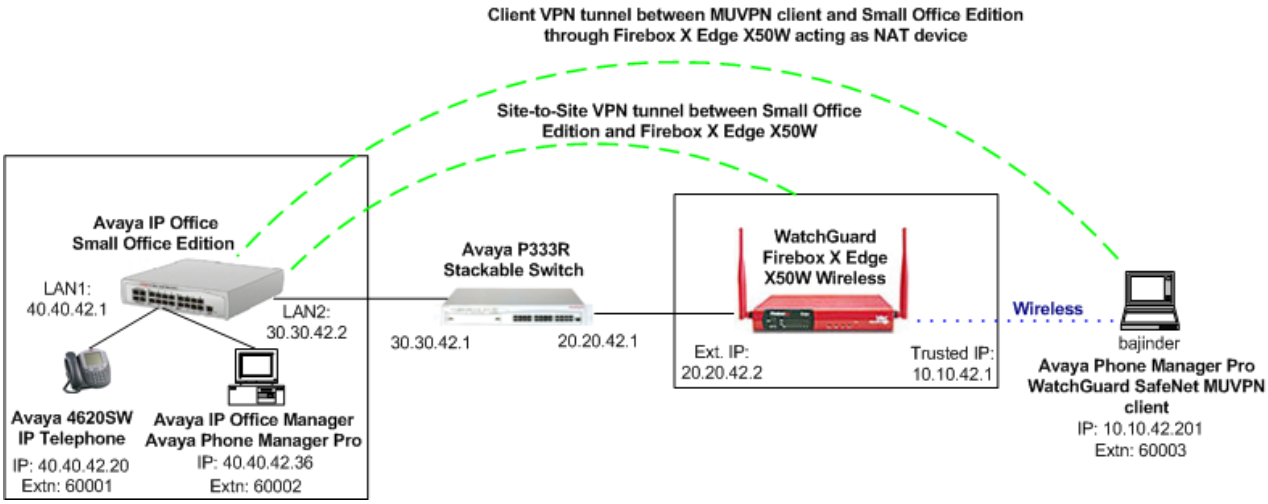


Figure 1 – Network Configuration Diagram

The following tunnel configurations were used in these Application Notes:

Tunnel Type	IKE Exchange Type	Encryption Method	Password Authentication	Diffie-Hellman Group	Encryption Protocol
Site-to-site	ID Prot	3DES	SHA	2	ESP
Client	Aggressive	3DES	SHA	2	ESP

Table 1 – IPSec Tunnel Configurations

2. Equipment and Software Validated

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

Product	Software/Version
Avaya IP Office Small Office Edition	3.0(40)
Avaya Phone Manager Pro	3.0(12)
Avaya 4620SW and 4610SW IP Telephones	2.1.3
Avaya P333R Stackable Switch	4.0.9
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

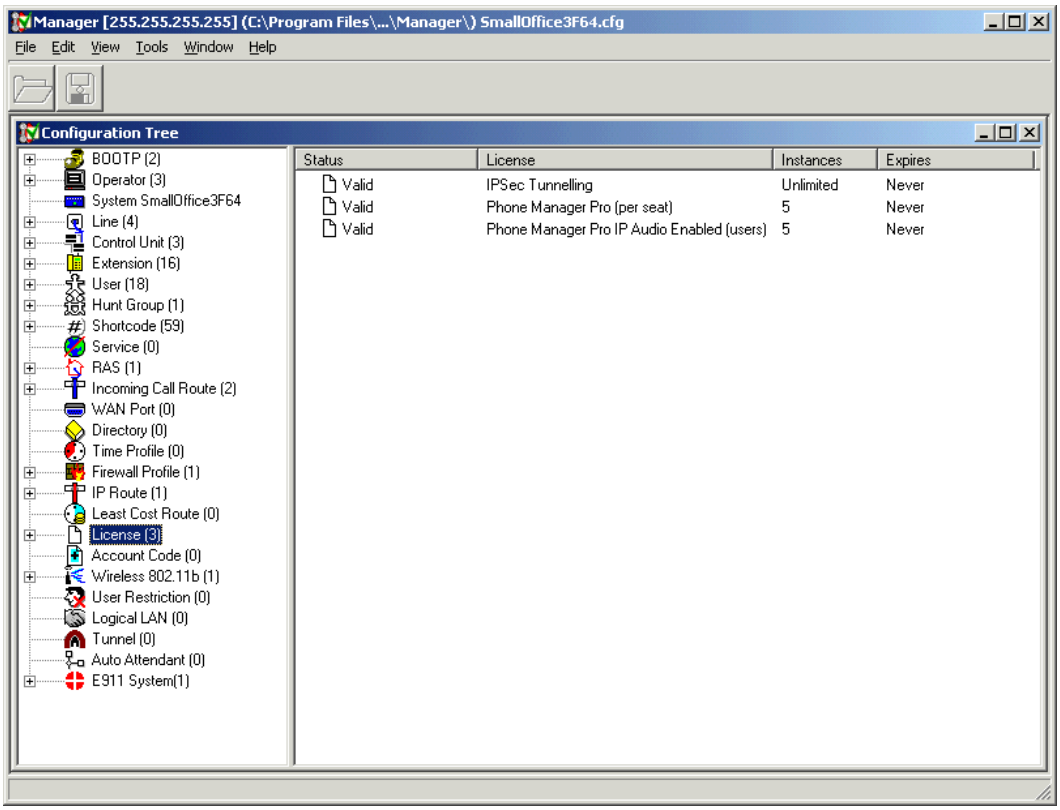
Table 2 – Product and Software Version

3. Configuring a Site-to-Site VPN Tunnel

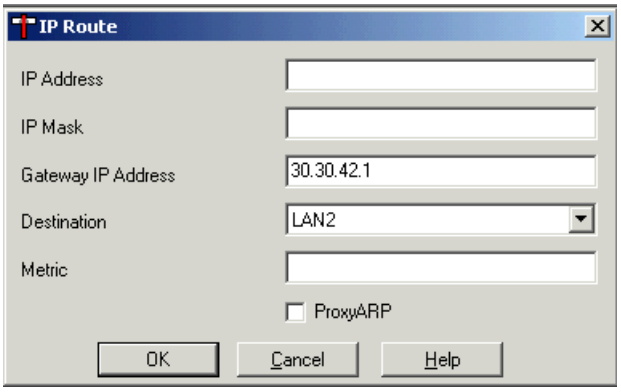
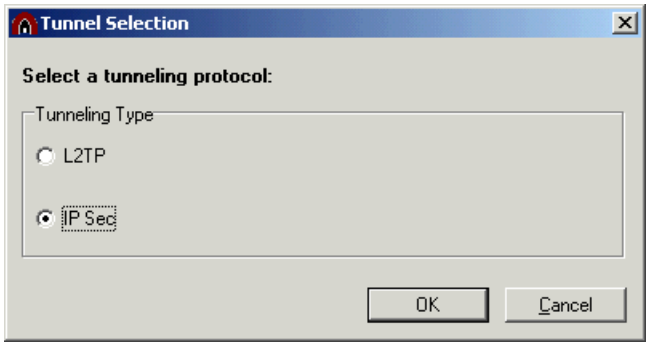
3.1. Configure Avaya IP Office

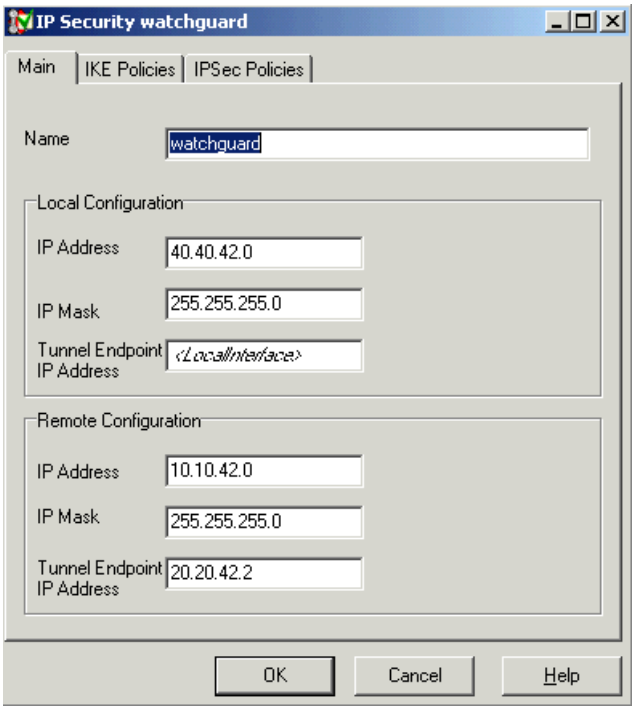
Step	Description
1.	From the PC running IP Office Manager, navigate to **Start → Programs → IP Office → Manager**. Log in with the appropriate credentials.

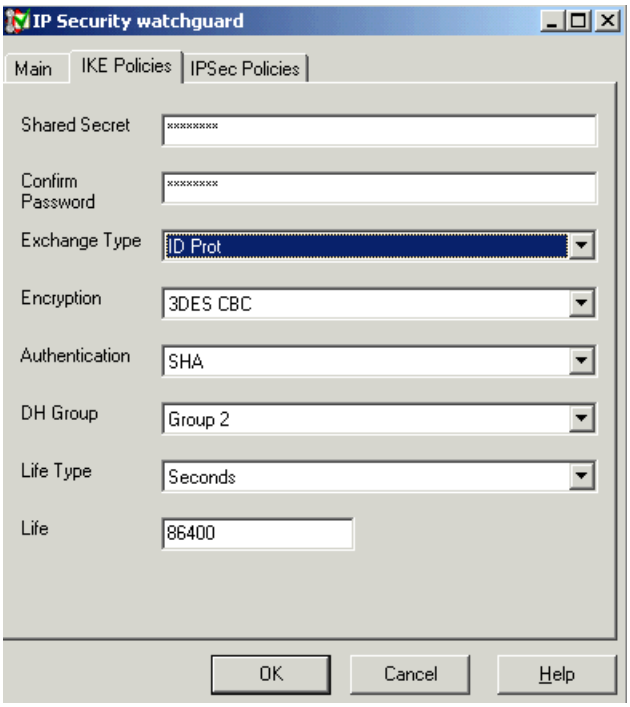
Step	Description
2.	In the **Manager** window, double-click **License** under the Configuration Tree panel. Ensure that the licenses shown below are listed as **Valid** under the *Status* column.

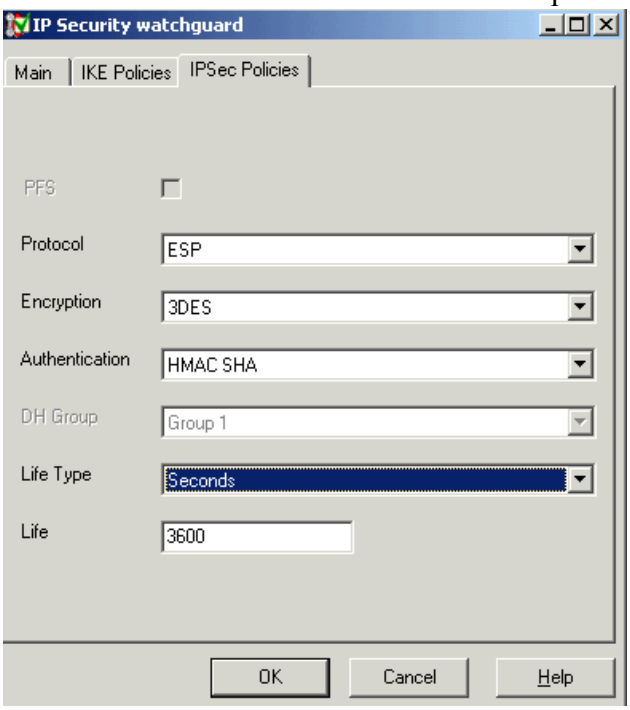


Step	Description
3.	Double-click the **System** item under the Configuration Tree panel. Click the **LAN1** tab. Verify **Enable NAT** is not checked.
4.	Click the **LAN2** tab, check **Enable NAT,** set *DHCP Mode* to **Disabled** and click **OK**.

Step	Description
5.	Click on the **IP Route** item under the Configuration Tree panel. Right click over the IP Route view and select **New**.
6.	In the IP Route window that appears, set *Gateway IP address* to **30.30.42.1**, *Destination* to **LAN2**, and click **OK**. 
7.	Click on the **Tunnel** item under the Configuration Tree panel. Right-click over the tunnel view and select **New** to create an IPSec tunnel.
8.	In the Tunnel Selection window that appears, select **IP Sec** and click **OK**. 

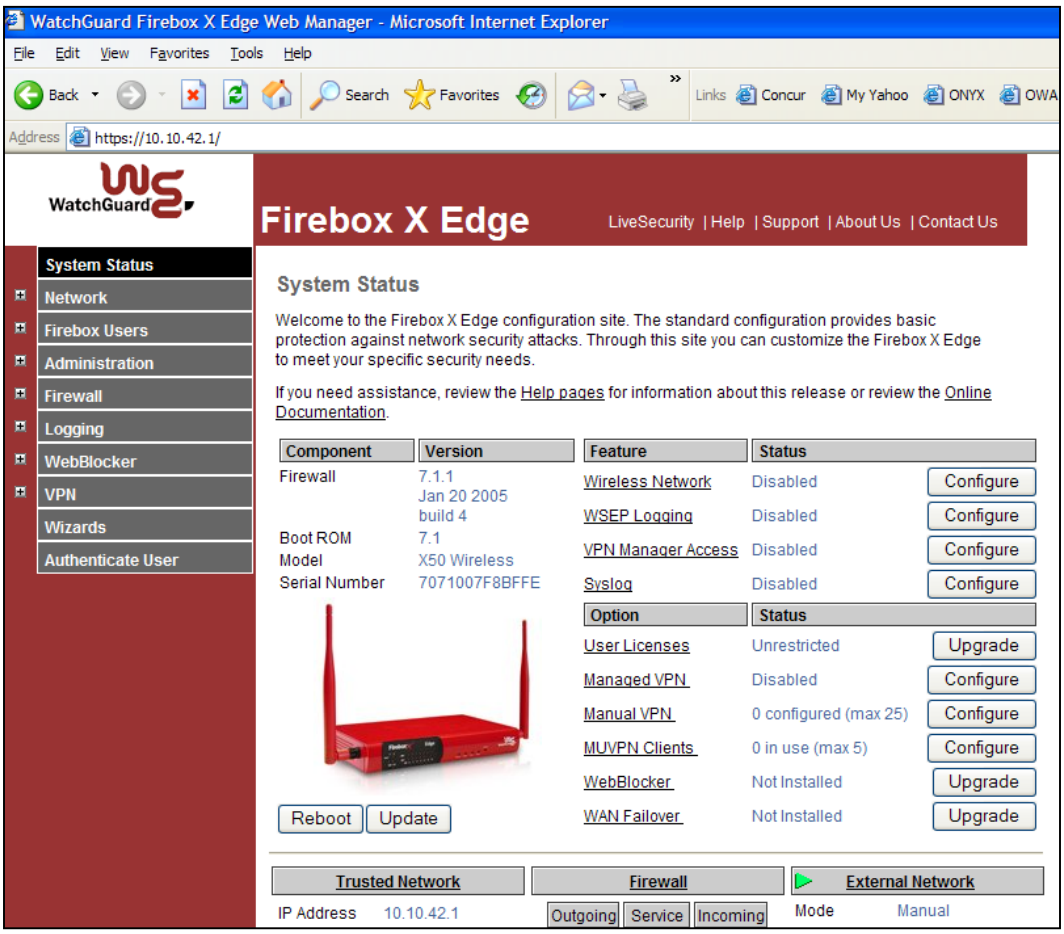
Step	Description
9.	In the IP Security window that appears, enter the values shown below to assign a name for the tunnel, the local and remote subnets for the tunnel, and the external IP address of the WatchGuard device in the *Tunnel Endpoint IP Address* field in the Remote Configuration area. 

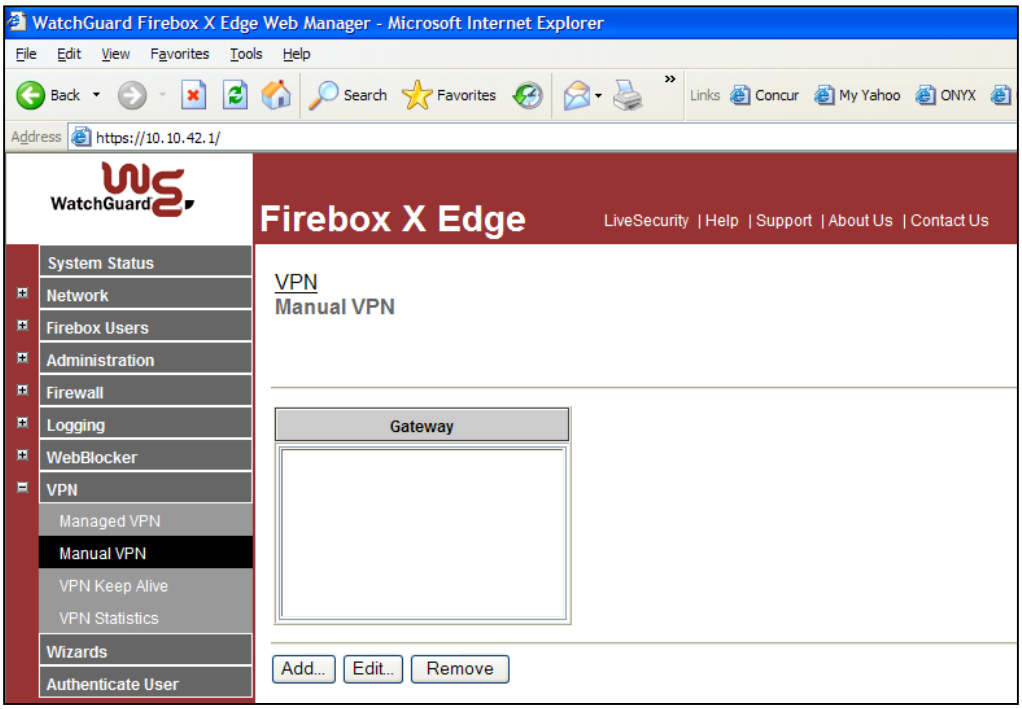
Step	Description
10.	Click the **IKE Policies** tab. Enter the values shown in the screen below. These correspond to Phase 1 parameters from **Table 1** for a site-to-site tunnel: • Shared secret – The password used for authentication must match on the device at the other end of the tunnel. • Confirm Password – Re-enter the shared secret. • Exchange Type – **ID Prot** is equivalent to **Main Mode** on the Firebox X Edge X50W (see step 3 of Section 3.2) and will hide the ID's of the communicating devices. • Encryption – The encryption method used by the tunnel. • Authentication – The password authentication used by the tunnel. • DH Group – Diffie Hellmann Group. • Life Type – Sets whether the Life value is measured in seconds or kilobytes. • Life – The duration before Phase 1 re-authentication is required.  Parameters configured in this form must match those used during configuration of the WatchGuard X50W Wireless in Step 3 of Section 3.2.

Step	Description
11.	Click the **IPSec Policies** tab. Enter the values shown in the screen below. These correspond to Phase 2 parameters from **Table 1** for a site-to-site tunnel. Click **OK**. • Protocol – The encryption protocol used by the tunnel. • Encryption – The encryption method used by the tunnel. • Authentication – The password authentication used by the tunnel. • Life Type – Sets whether the Life value is measured in seconds or kilobytes. • Life – The duration before Phase 2 re-authentication is required.  Parameters configured in this form must match those used during configuration of the WatchGuard X50W Wireless in Step 4 of Section 3.2
12.	In the Manager window, select **File** → **Save** to save the configuration to the IP Office system and wait for the system to update.

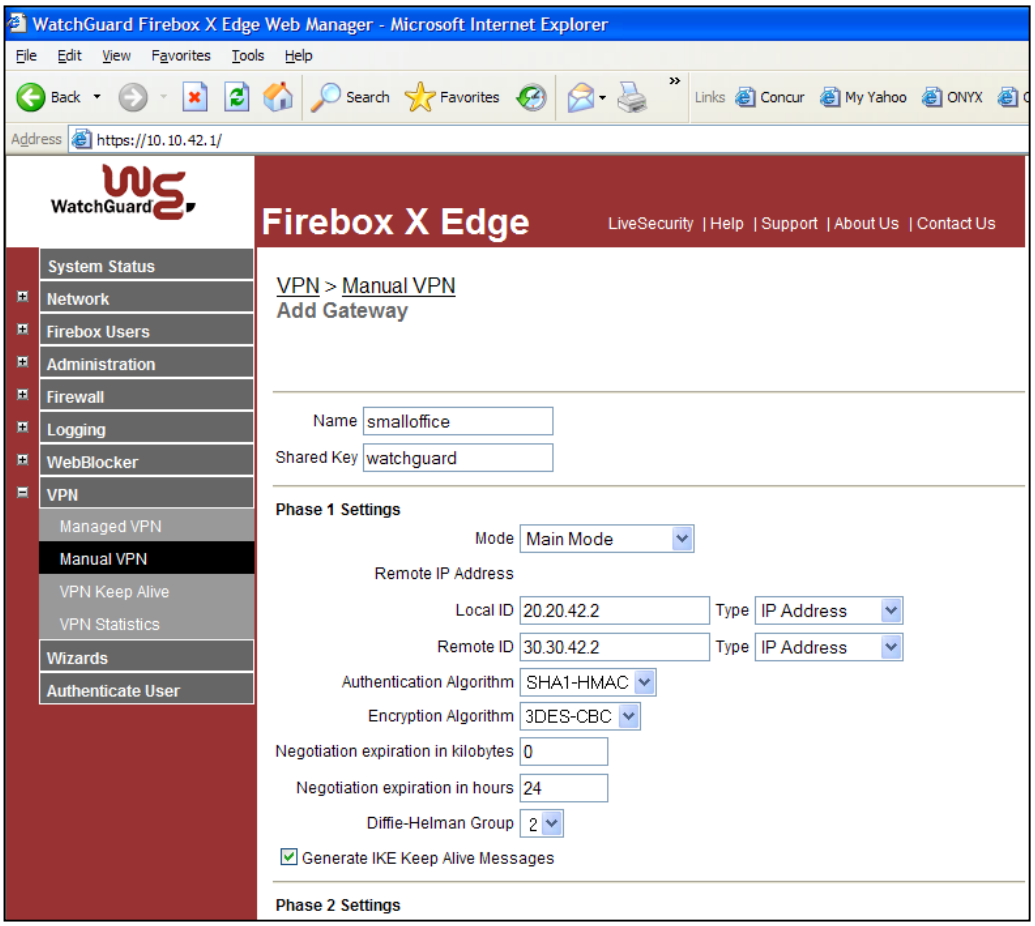
3.2. Configure the Firebox X Edge X50W Wireless

Step	Description
1.	Open the Firebox X Edge X50W configuration screen by specifying its private interface IP address in a browser window. Log into the WatchGuard Firebox X Edge Web Manager using the appropriate administrative privileges. Click the **VPN** option on the left pane.

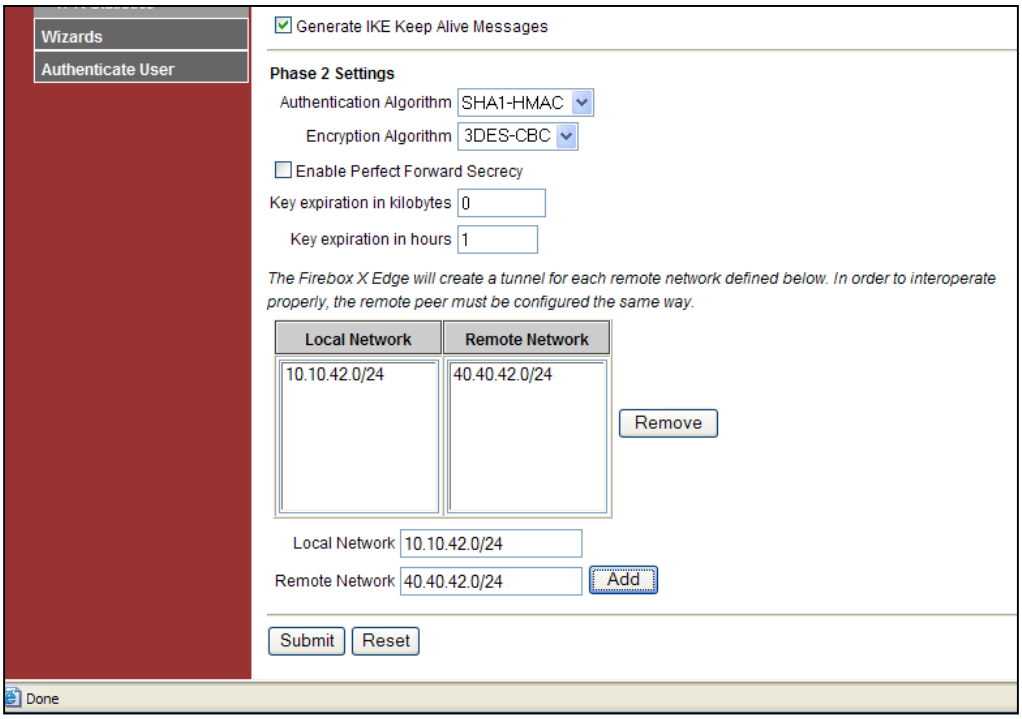


Step	Description
2.	Click the **Manual VPN** option on the left pane and click the **Add…** button to create a VPN tunnel to the IP Office. 

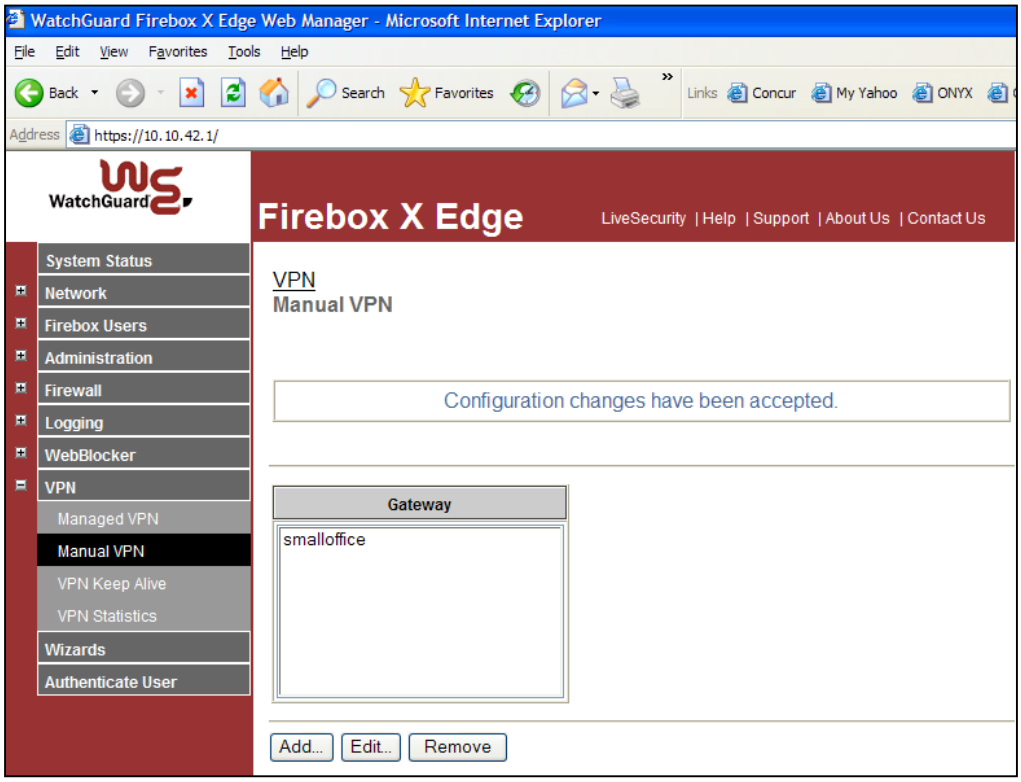
Step	Description
3.	Enter the values shown below to match the IP Office tunnel configuration for **Phase 1** and the shared key.



Step	Description
4.	Scroll down the page to **Phase 2 Settings** and enter the values shown below to match the IP Office tunnel configuration for Phase 2. Enter the subnet of the trusted network in the *Local Network* field and the subnet of the remote IP telephone and IP Office in the *Remote Network* field, click on **Add** to specify the local and remote networks for the tunnel. Click **Submit**.

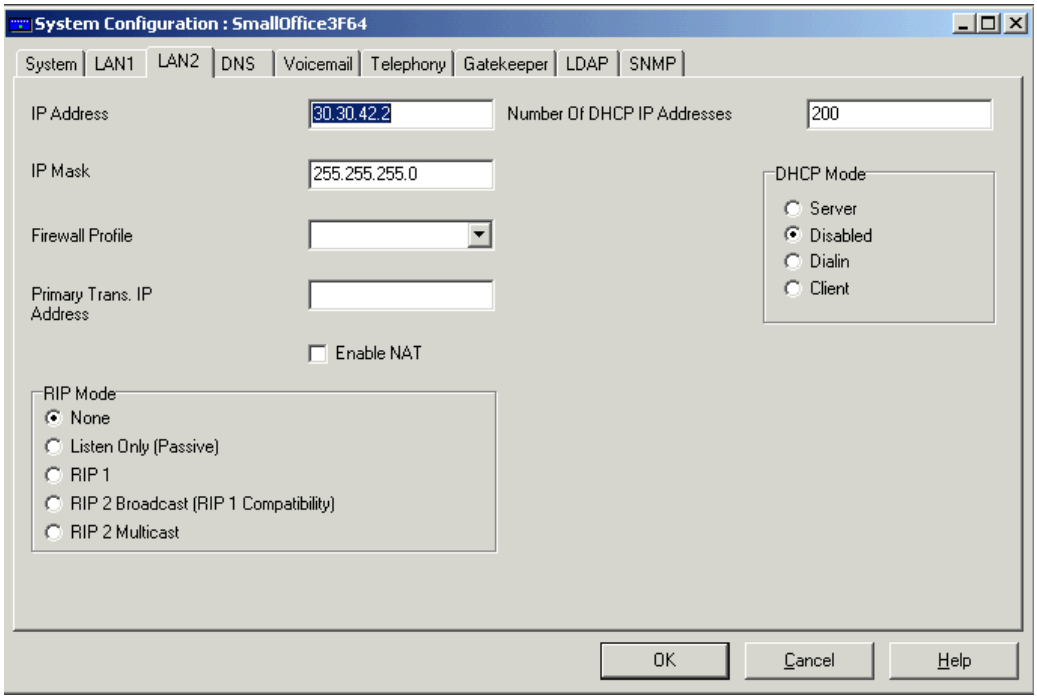


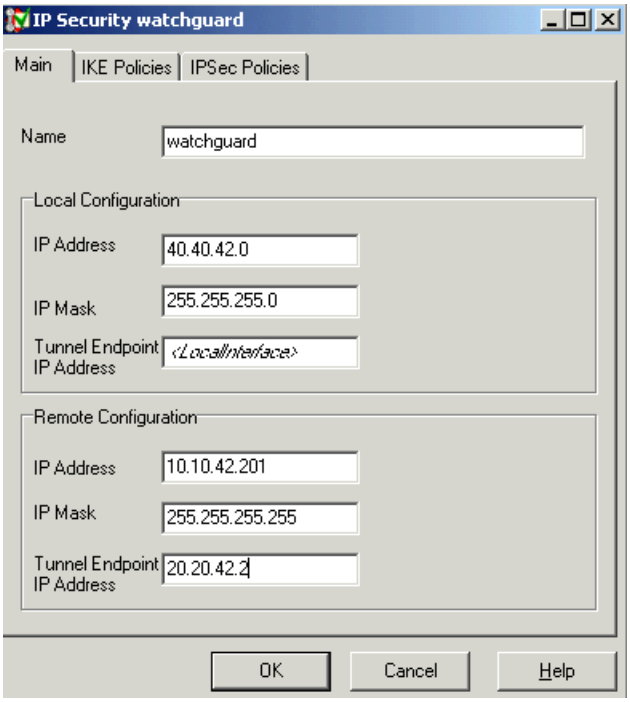
Step	Description
5.	This completes configuration of the site-to-site VPN on the Firebox Edge X50W Wireless.

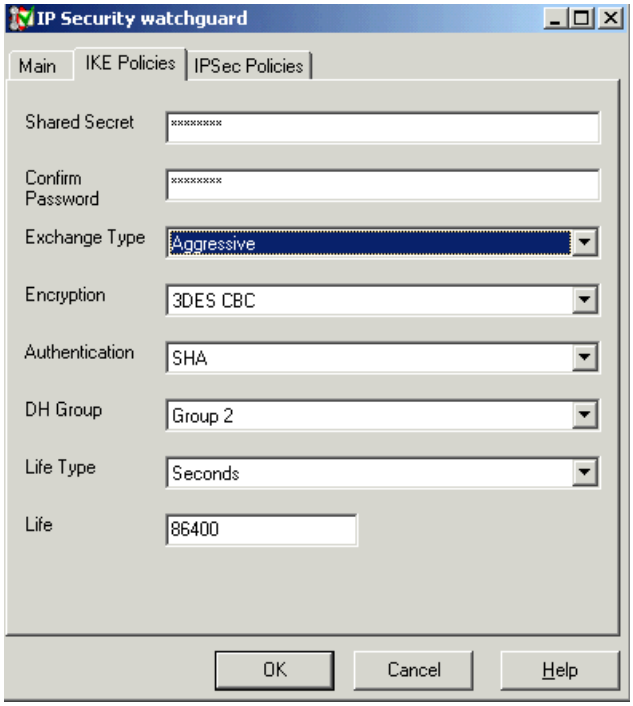


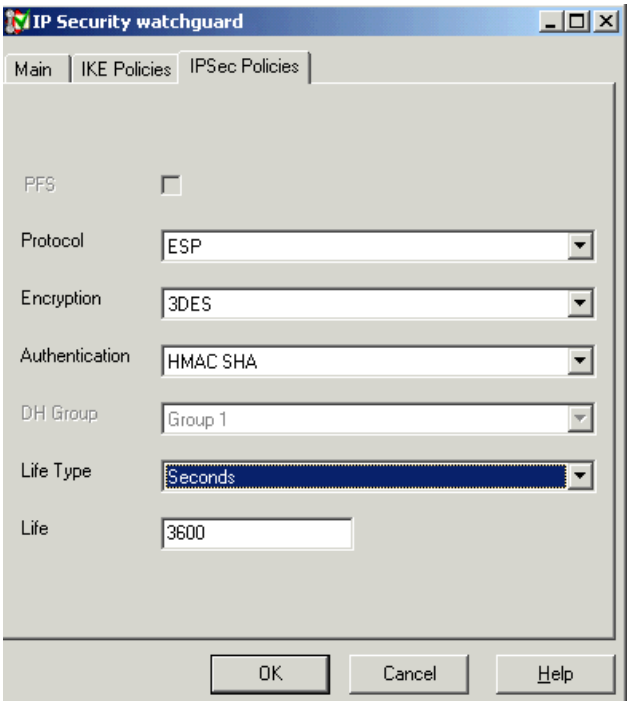
4. Configuring a Client VPN tunnel

4.1. Configure Avaya IP Office

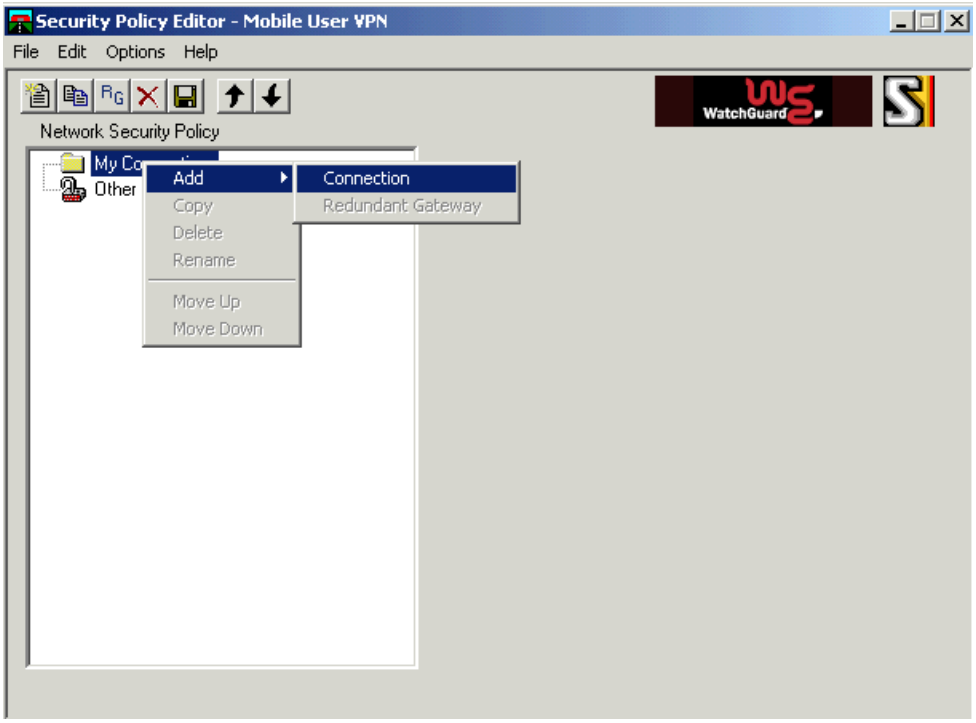
Step	Description
1.	Perform steps 1 – 3 from Section 3.1.
2.	Click the **LAN2** tab, verify **Enable NAT** is not checked and set *DHCP Mode* to **Disabled**. Click **OK**. 
3.	Perform steps 5 – 8 from Section 3.1.

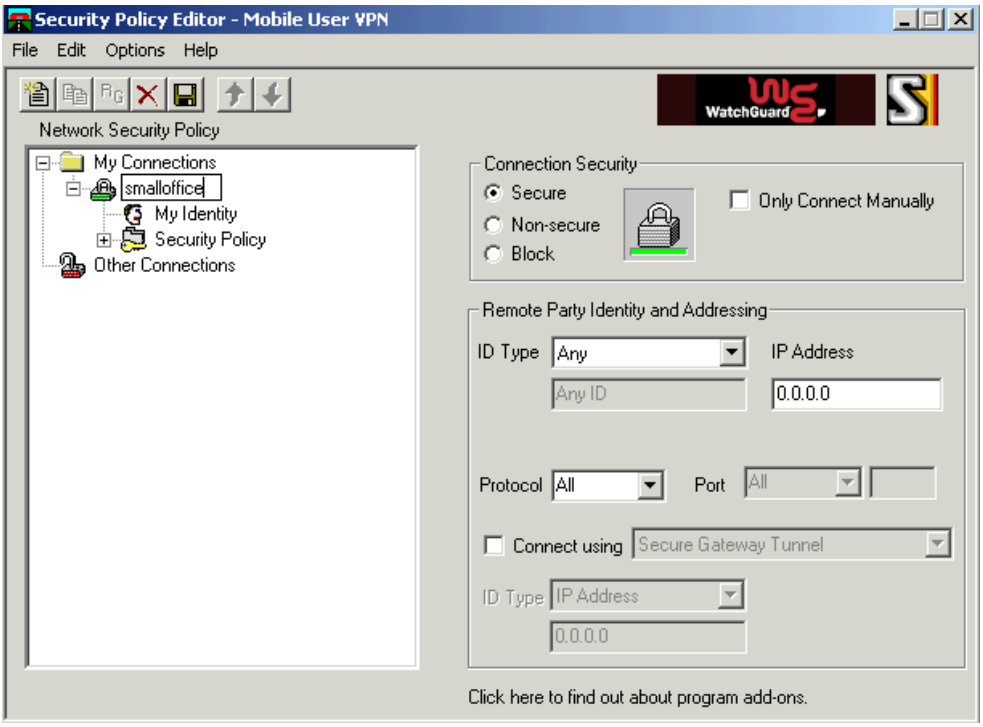
Step	Description
4.	Enter the values shown below for the client VPN tunnel to the remote Phone Manager Pro PC.  **NOTE**: The external IP address of the Firebox X Edge X50W (e.g., **20.20.42.2**) must be specified as the remote tunnel endpoint address in the Remote Configuration *Tunnel Endpoint IP Address* field.

Step	Description
5.	Click the **IKE Policies** tab. Enter the values shown in the screen below. These values correspond to the parameters for Phase 1 from **Table 1** for a client tunnel: • Shared secret – The password used for authentication must match on the device at the other end of the tunnel. • Confirm Password – Re-enter the shared secret. • Exchange Type – Aggressive provides faster security setup but does not hide the ID's of the communicating devices. • Encryption – The encryption method used by the tunnel. • Authentication – The password authentication used by the tunnel. • DH Group – Diffie Hellmann Group • Life Type – Sets whether the Life value is measured in seconds or kilobytes. • Life – The duration before re-authentication is required. 

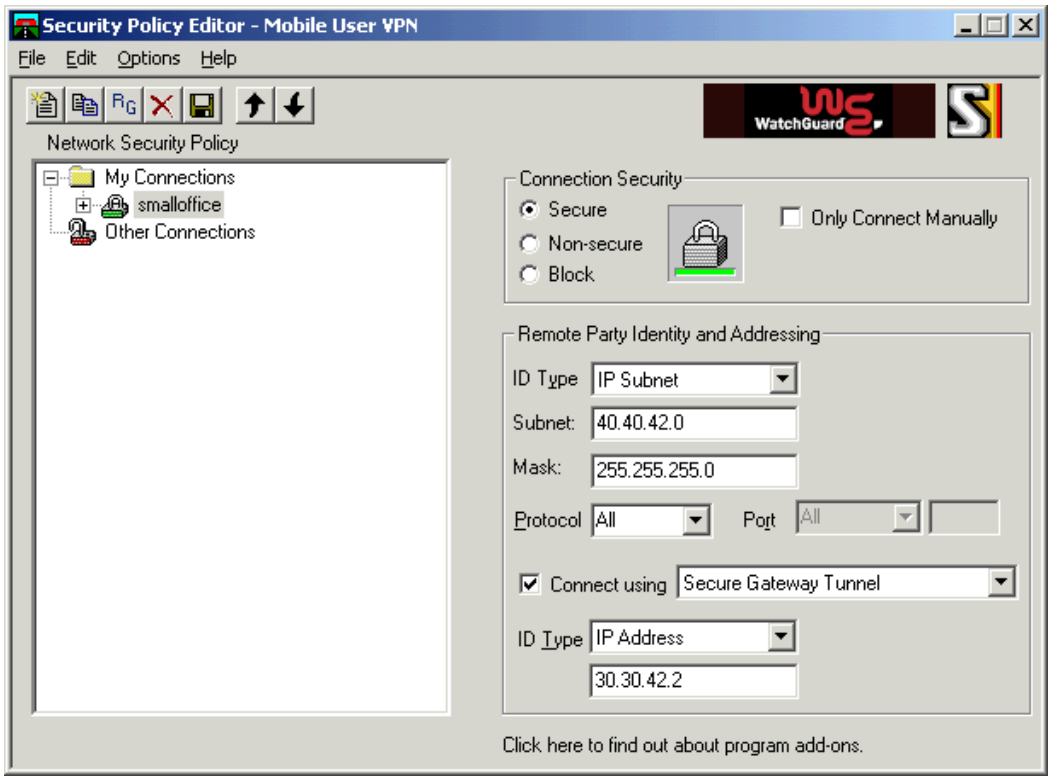
Step	Description
6.	Click the **IPSec Policies** tab. Enter the values shown in the screen below. These values correspond to the Phase 2 parameters from **Table 1** for a client tunnel. Click **OK**. • Protocol – The encryption protocol used by the tunnel. • Encryption – The encryption method used by the tunnel. • Authentication – The password authentication used by the tunnel. • Life Type – Sets whether the Life value is measured in seconds or kilobytes. • Life – The duration before re-authentication is required 
7.	In the Manager window, select **File** → **Save** to save the configuration to the IP Office system and wait for the system to update.

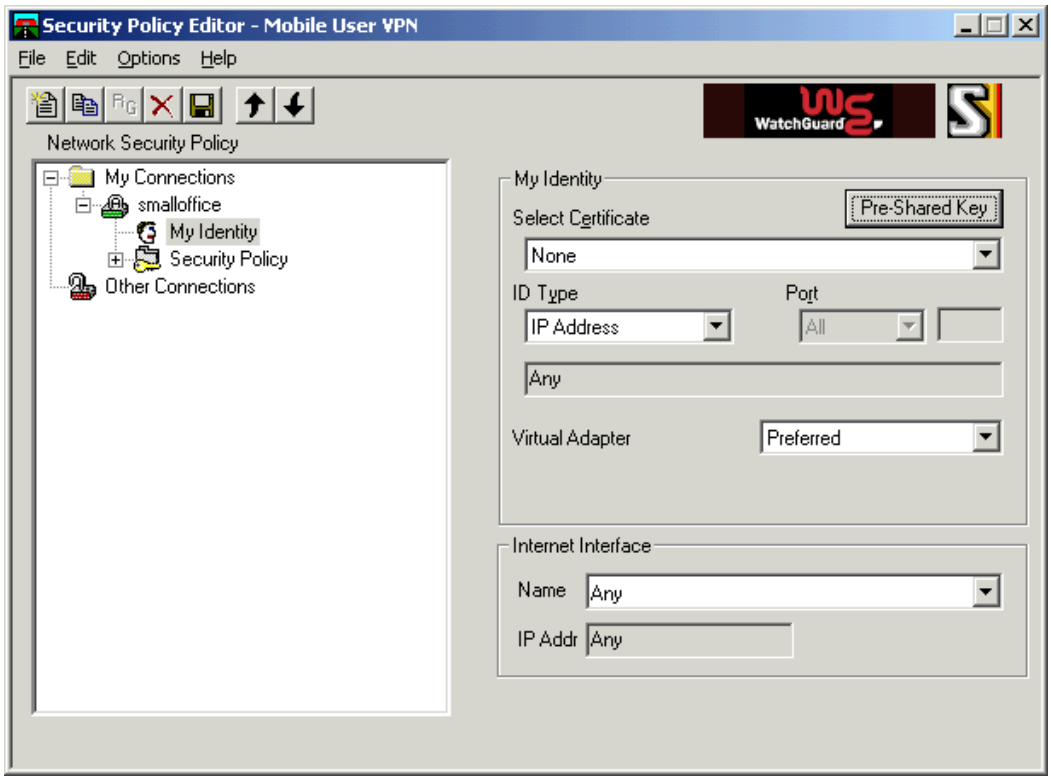
4.2. Configure WatchGuard SafeNet MUVPN Client

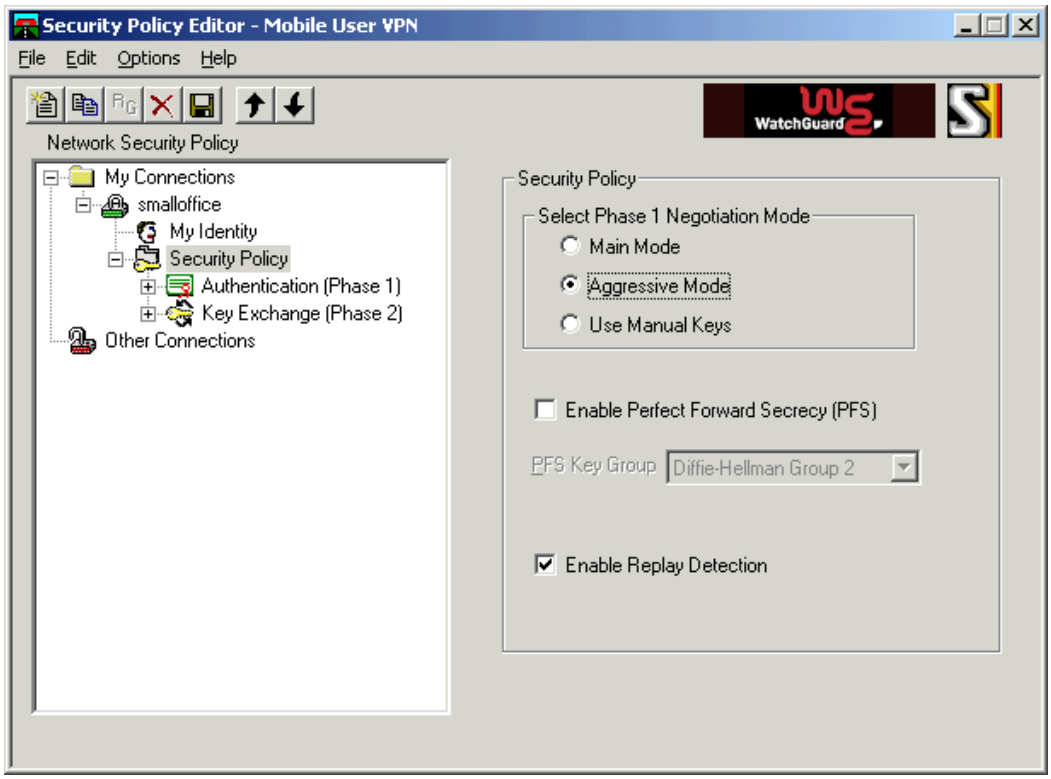
Step	Description
1.	From the PC running the WatchGuard SafeNet MUVPN client, open the Security Policy Editor by navigating to **Start → Programs → Mobile User VPN → Security Policy Editor**. Right-click **My Connections** and select **Add → Connection**. 

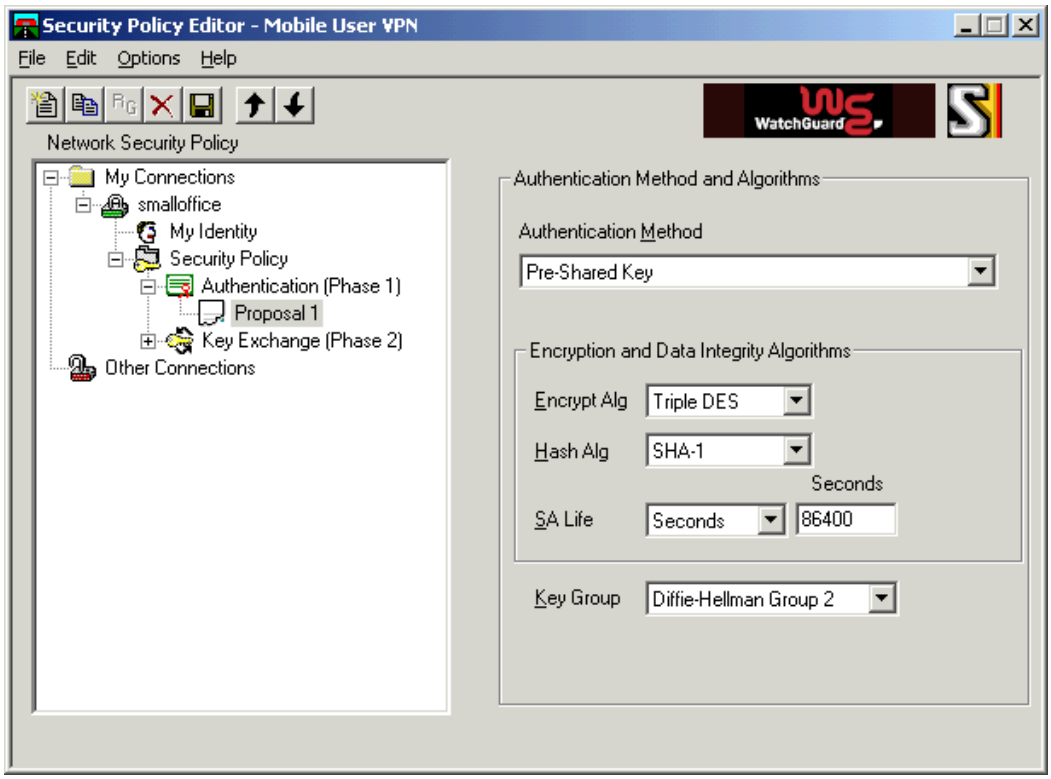
Step	Description
2.	In the **Security Policy Editor** window, specify the name of the new connection (e.g., **smalloffice**). 

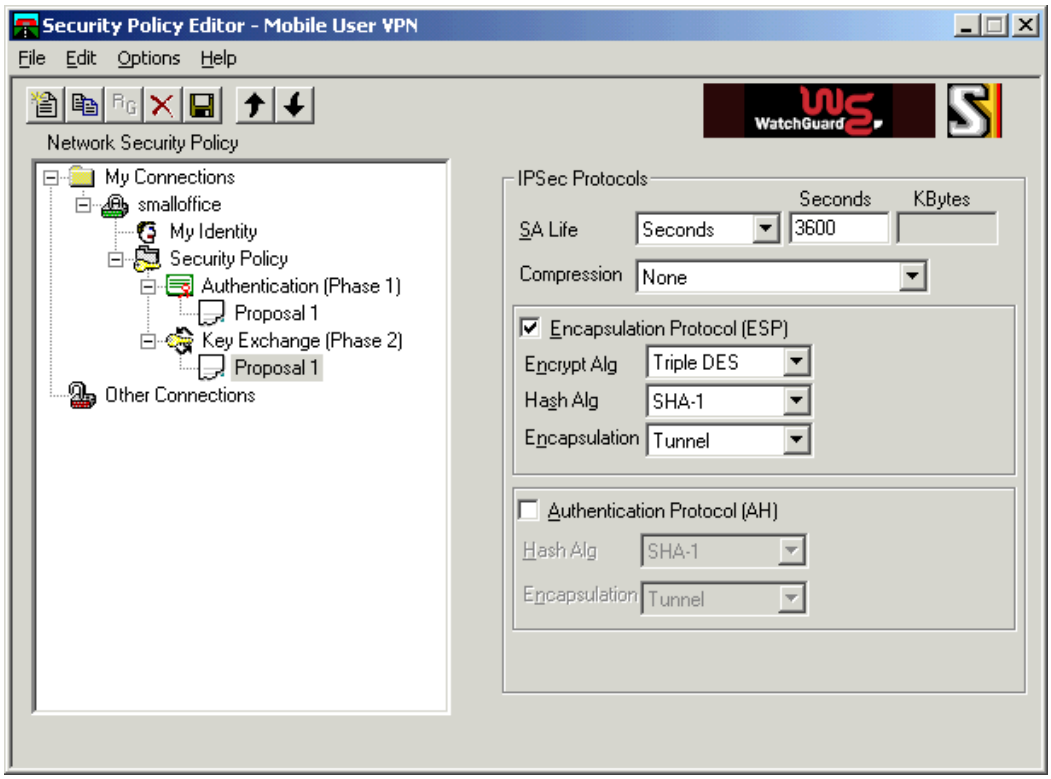
Step	Description
3.	In the **Security Policy Editor** window, enter the values shown in the screen below, matching the IP Office tunnel configuration by specifying the remote subnet and IP address of the Avaya IP Office Small Office Edition as the remote tunnel endpoint address.



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** (not shown) to supply the same password specified in the IP Office tunnel configuration. Select **Preferred** in the *Virtual Adapter* drop-down list and leave the other fields as default. 

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

Step	Description
6.	Expand **Security Policy** and **Authentication (Phase1)**. Click **Proposal 1** and enter the values shown below to match the IP Office tunnel configuration for Phase 1. 

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

5. Interoperability Compliance Testing

Features of the WatchGuard Firebox X Edge X50W Wireless were tested to determine if VPN tunnels could be established with IP Office.

5.1. General Test Approach

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

- Ability to establish a site-to-site VPN tunnel between the WatchGuard Firebox X Edge X50W Wireless and the Small Office Edition,
- Ability to establish a VPN tunnel between the Phone Manager Pro client PC and the Avaya IP Office Small Office Edition using the SafeNet MUVPN client provided by WatchGuard,
- Two-way tunnel creation,
- Support for two IPSec (IP Security) tunnel types, as defined in **Table 1,** for the site-to-site and client VPN tunnels,

- Voice calls were placed manually and subjective quality noted for both G.711 and G.729 codecs. Direct Media Path was enabled for the Avaya IP Office Small Office Edition,
- RAS (Registration Admission Status) over the VPN tunnel.

5.2. Test Results

Testing was successful. Site-to-site and client VPN tunnels could be established between IP Office and the WatchGuard Firebox X Edge X50W Wireless.

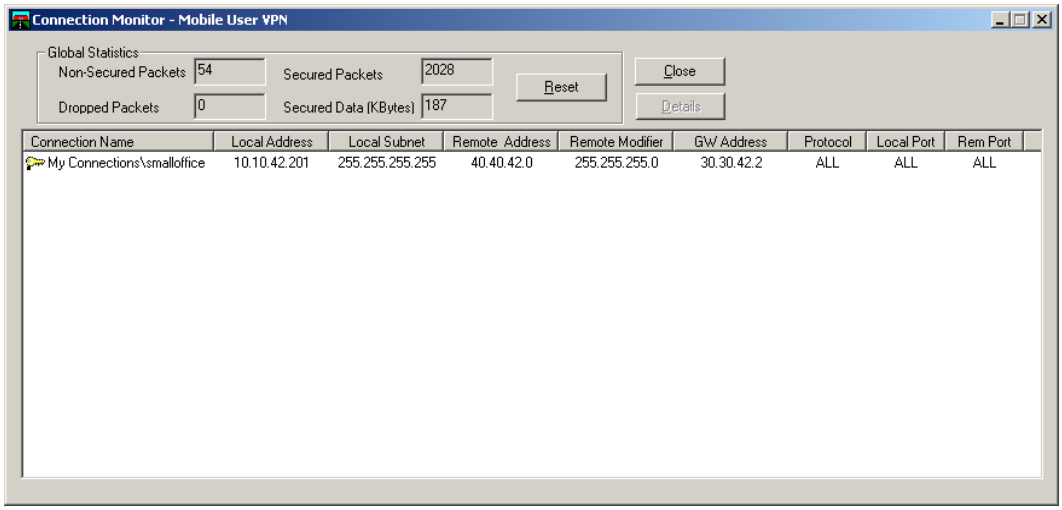
6. Verification Steps

- **To verify Phase 1 and Phase 2 negotiations completed on IP Office:**
  Using the IP Office SysMonitor log, verify that Phase 1 and Phase 2 negotiations complete. The negotiation messages will only appear if the trace option **IPSec Events** is checked under the **VPN** tab for the SysMonitor log filter. The following is an example of Phase 1 and Phase 2 negotiation messages for a site-to-site VPN tunnel.

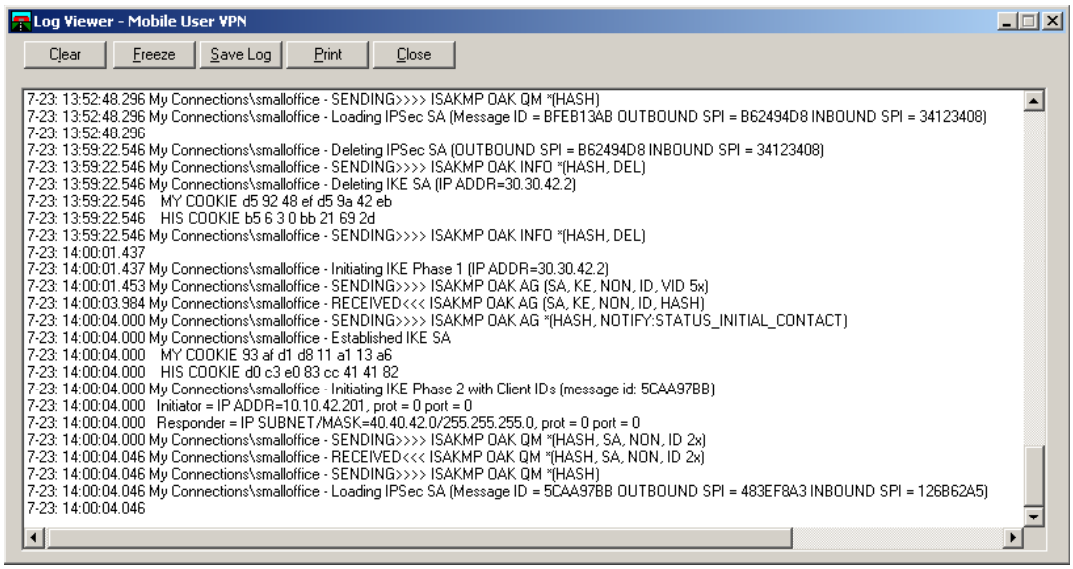
```
297545mS IPSecEvent: transport_add: adding ffe8e6c0
297546mS IPSecEvent: transport_reference: transport ffe8e6c0 now has 1 references
297546mS IPSecEvent: Received request to negotiate ID_PROT Mode Phase 1 security for
policy watchguard
297548mS IPSecEvent: transport_reference: transport ffe8e6c0 now has 2 references
297550mS IPSecEvent: transport_reference: transport ffe8e6c0 now has 3 references
297572mS IPSecEvent: transport_reference: transport ffe8e6c0 now has 4 references
297573mS IPSecEvent: transport_release: transport ffe8e6c0 had 4 references
297573mS IPSecEvent: transport_release: transport ffe8e6c0 had 3 references
297573mS IPSecEvent: transport_reference: transport ffe8e6c0 now has 3 references
300022mS IPSecEvent: transport_reference: transport ffe8e6c0 now has 4 references
300022mS IPSecEvent: transport_release: transport ffe8e6c0 had 4 references
300024mS IPSecEvent: transport_release: transport ffe8e6c0 had 3 references
300025mS IPSecEvent: transport_reference: transport ffe8e6c0 now has 3 references
300028mS IPSecEvent: Phase 1 negotiations completed: src: 30.30.42.2 dst: 20.20.42.2
300028mS IPSecEvent: exchange_free: calling: timer_remove_event(exchange->death)
300029mS IPSecEvent: transport_release: transport ffe8e6c0 had 3 references
300029mS IPSecEvent: transport_release: transport ffe8e6c0 had 2 references
300040mS IPSecEvent: transport_reference: transport ffe8e6c0 now has 2 references
300042mS IPSecEvent: Received request to start Phase 2 security negotiations, src:
30.30.42.2 dst: 20.20.42.2
300042mS IPSecEvent: transport_reference: transport ffe8e6c0 now has 3 references
300044mS IPSecEvent: transport_reference: transport ffe8e6c0 now has 4 references
300068mS IPSecEvent: transport_reference: transport ffe8e6c0 now has 5 references
300068mS IPSecEvent: transport_release: transport ffe8e6c0 had 5 references
300073mS IPSecEvent: transport_release: transport ffe8e6c0 had 4 references
300074mS IPSecEvent: IPSec: Chosen IPSec Auth Algo = 7
300074mS IPSecEvent: IPSec Object=ffdeeae0 created for SA=ffdef10c destination=20.20.42.2
300075mS IPSecEvent: IPSec: Chosen IPSec Auth Algo = 7
300075mS IPSecEvent: IPSec Object=ffdee6f0 created for SA=ffdedb90 destination=30.30.42.2
300076mS IPSecEvent: Completed Phase 2 negotiations between src: 30.30.42.2 dst:
20.20.42.2
300076mS IPSecEvent: exchange_free: calling: timer_remove_event(exchange->death)
300076mS IPSecEvent: transport_release: transport ffe8e6c0 had 3 references
```

- **To view VPN tunnel statistics on the Firebox X Edge X50W Wireless:**
  Open the Firebox X Edge X50W configuration screen by specifying its private interface IP address in a browser window. Click the **VPN** option and then click the **VPN Statistics** option on the left pane to view statistics for the site-to-site tunnel between the Firebox X Edge X50W and Avaya IP Office Small Office Edition.

- **To view statistics on the WatchGuard SafeNet MUVPN client:**
  Navigate to **Start → Programs → Mobile User VPN → Connection Monitor** to view statistics for the client VPN tunnel to Avaya IP Office Small Office Edition. The following is an example of what will appear.



- **To view Phase 1 and Phase 2 negotiations on the WatchGuard SafeNet MUVPN:** Navigate to **Start → Programs → Mobile User VPN → Log Viewer** to view Phase 1 and Phase 2 negotiation messages for the client VPN tunnel to Avaya IP Office Small Office Edition. The following is an example of what will appear.



7. Support

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

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 site-to-site VPN tunnels between the Avaya IP Office and WatchGuard Firebox X Edge X50W Wireless as well as client VPN tunnels to Avaya IP Office using the WatchGuard SafeNet MUVPN client 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

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.