



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring VPN Tunnels between Avaya IP Office and WatchGuard Firebox X and SOHO Products – Issue 1.0

Abstract

These Application Notes cover the configuration of site-to-site VPN tunnels between Avaya IP Office and WatchGuard Firebox X and SOHO products. Client VPN tunnels to IP Office are also covered. Information in these Application Notes has been obtained through compliance testing and additional technical discussions. Testing was conducted via the *DeveloperConnection* Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes cover the configuration of site-to-site VPN (Virtual Private Network) tunnels between Avaya IP Office and WatchGuard Firebox X and SOHO products. Client VPN tunnels to IP Office are also covered.

Configuration 1 in **Figure 1** will be used to refer to the site-to-site VPN tunnels established between the Avaya Small Office Edition and the Firebox X or SOHO products. Configuration 2 in **Figure 1** will be used to refer to the client VPN tunnels established between the Avaya Small Office Edition and the Mobile User VPN (MUVPN) client running on the Phone Manager Pro PC.

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.

The WatchGuard Firebox 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 data network infrastructure shown in **Figure 1**; refer to the appropriate documentation listed in Section 9.

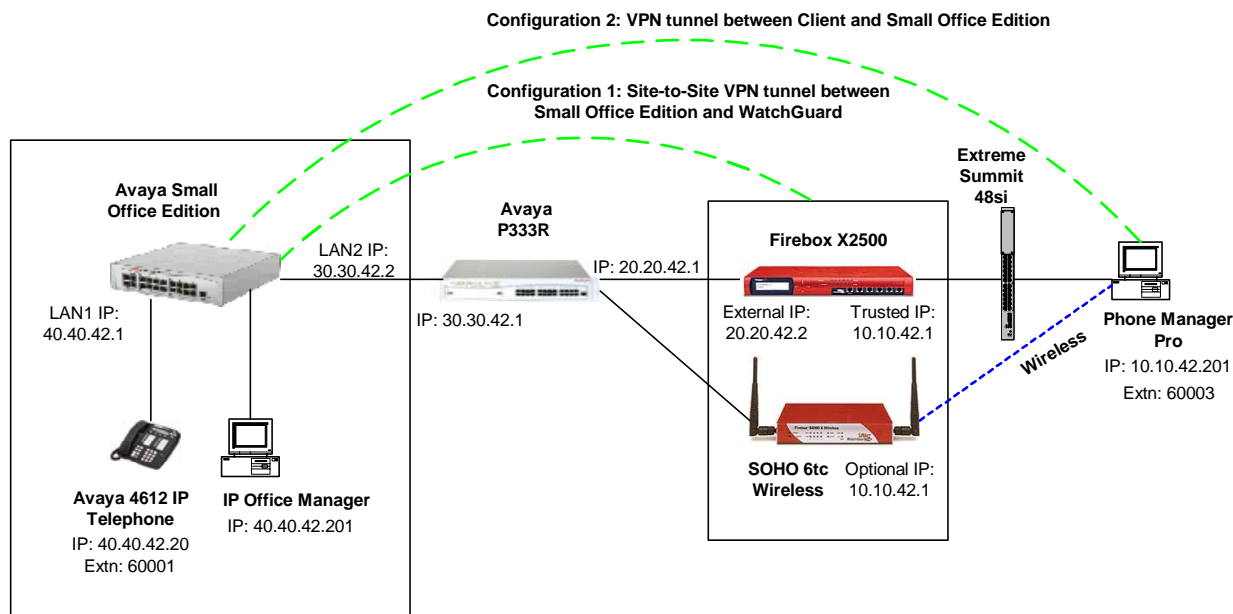


Figure 1 – Network Configuration Diagram

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 configurations will be 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

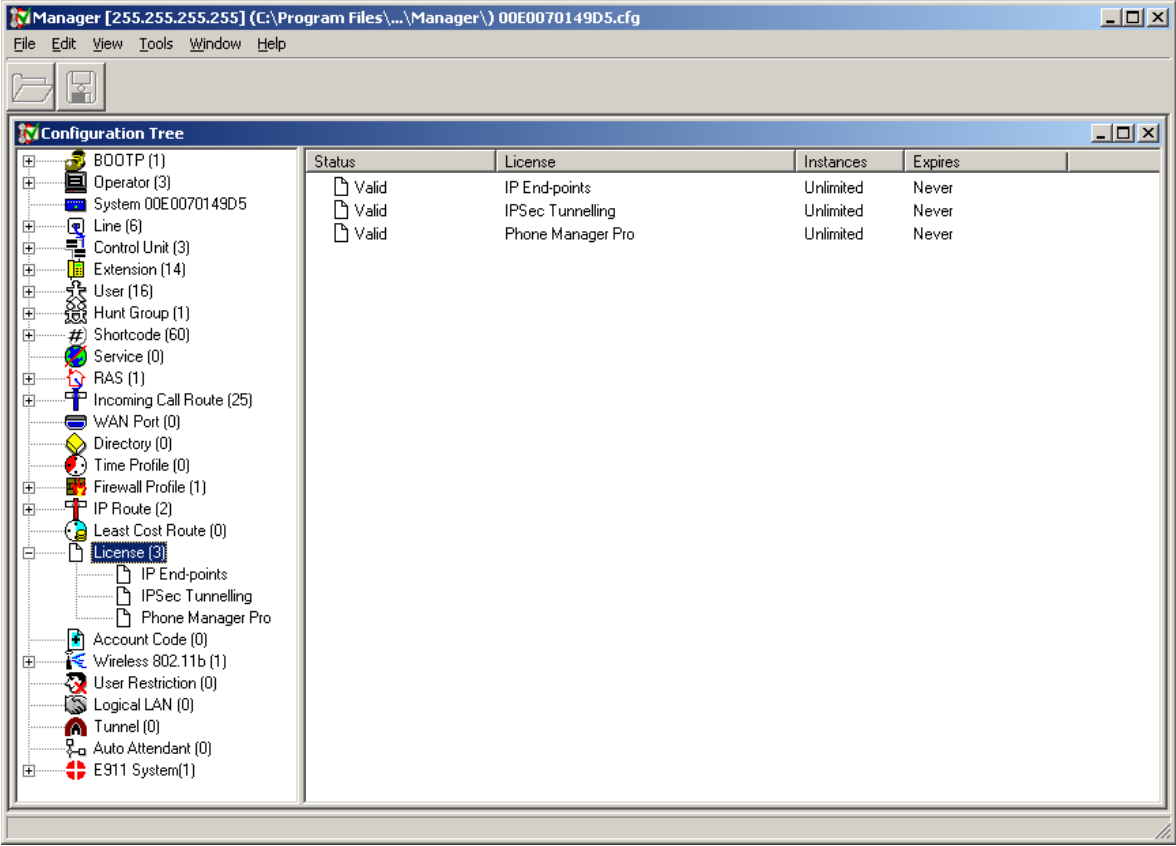
The following products and software were used for the configuration in **Figure 1**:

Product	Software/Version
Avaya IP Office Small Office Edition	2.1 (15)
Avaya P333R Stackable Switch	4.0.9
Avaya 4612 IP Telephone	1.8.2
Avaya Phone Manager Pro	2.1.7
Extreme Summit 48si	6.2.2 (Build 68)
WatchGuard Firebox X2500	7.21.B1596
WatchGuard SOHO 6tc Wireless	6.3 Build 19

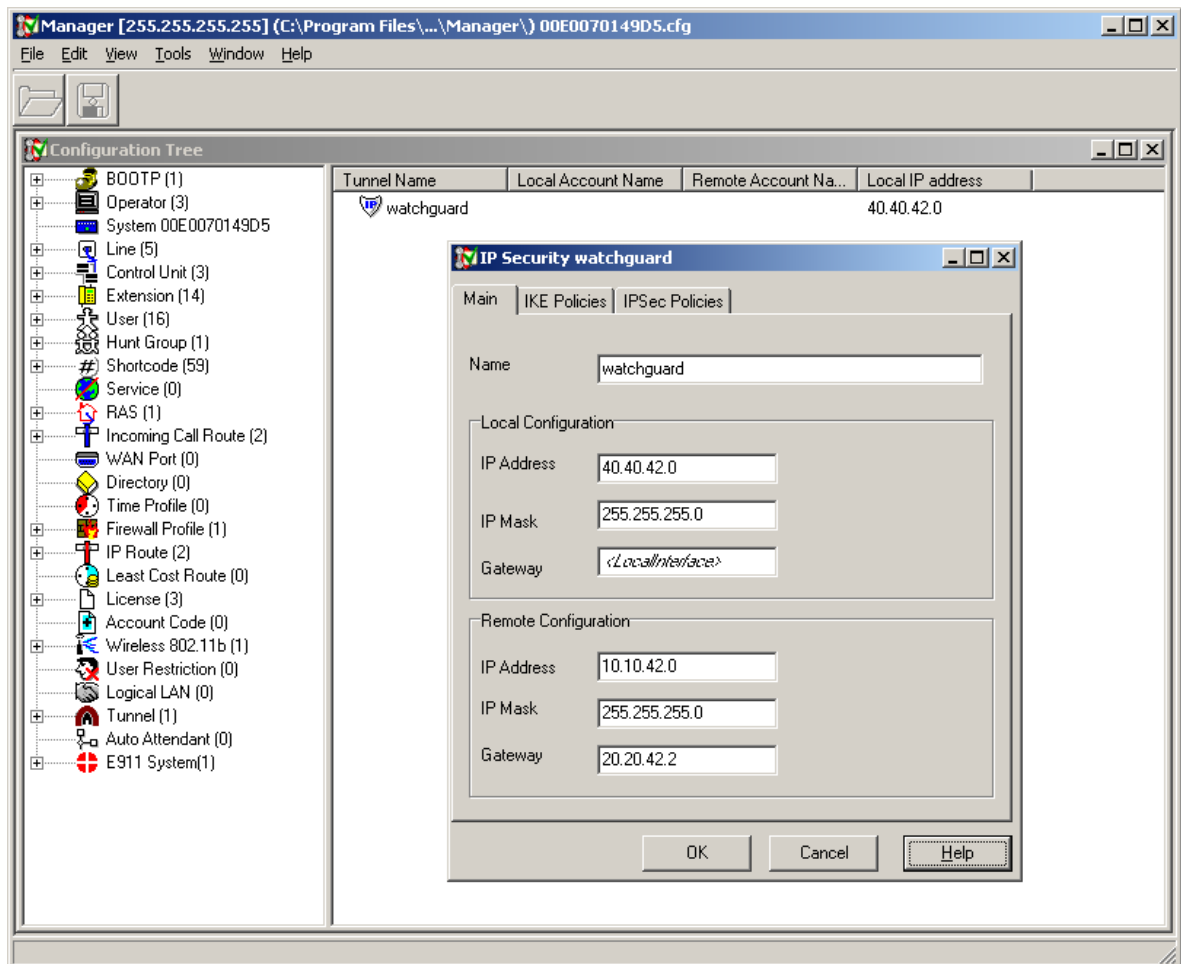
Table 2 – Product and Software Version

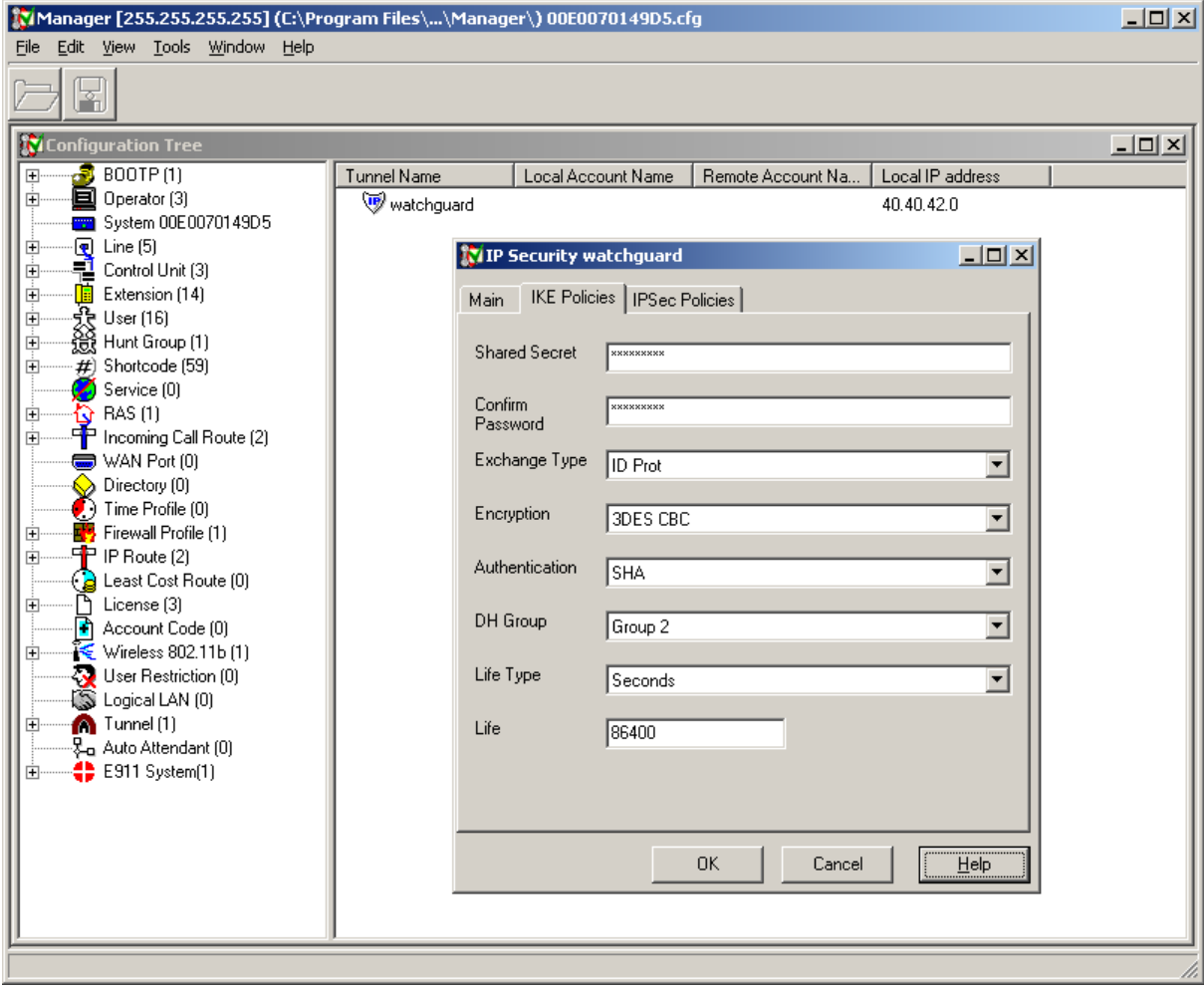
3. Configuration 1 (Site-to-Site VPN Tunnel between IP Office and WatchGuard)

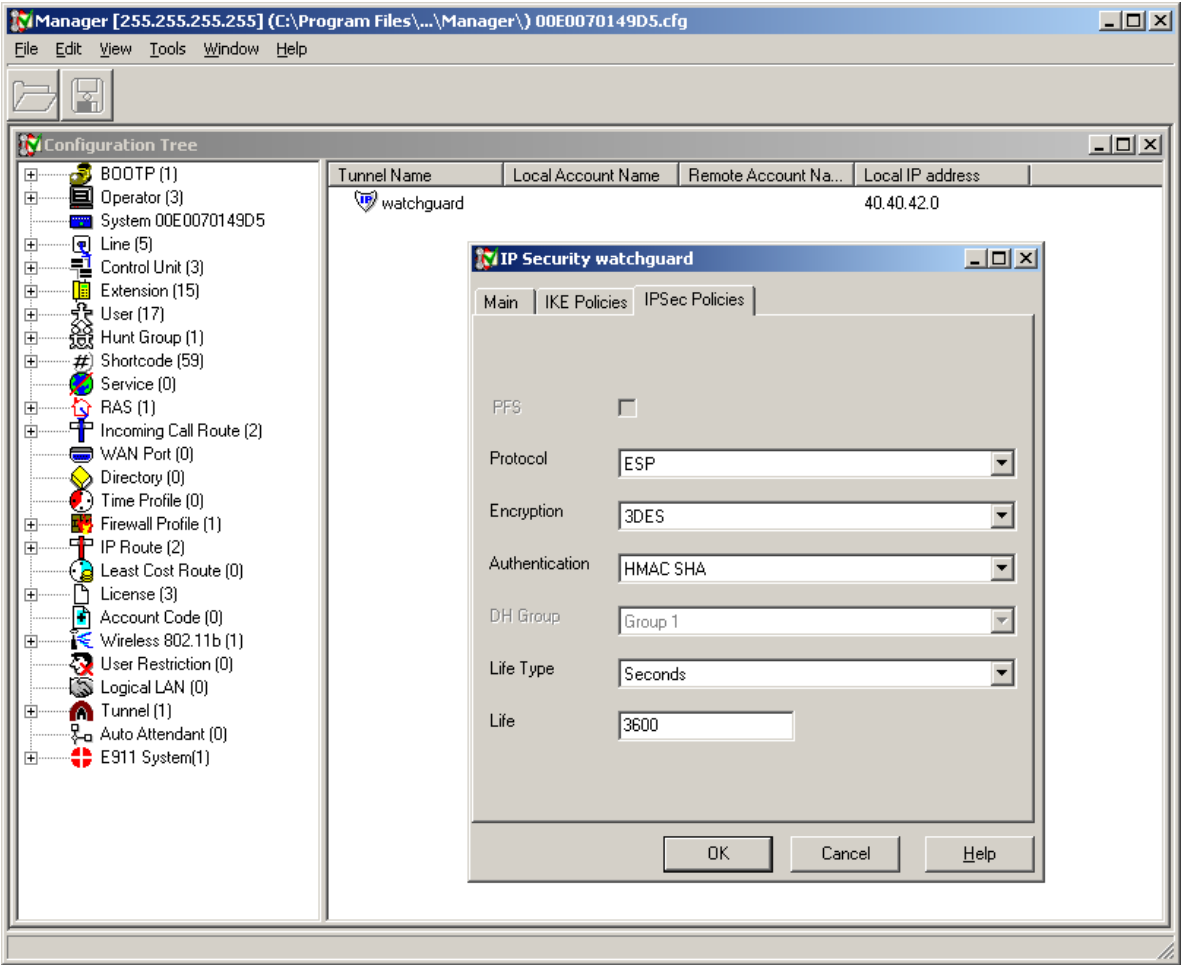
3.1. Configure Avaya IP Office

Step	Description																
1.	<p>Navigate to Start → Programs → IP Office → Manager. Log in with the appropriate credentials. In the Manager window, double-click License under the Configuration Tree panel. Ensure that the licenses shown below are listed as Valid under the <i>Status</i> column.</p>  <p>The screenshot shows the Avaya Manager application window. The Configuration Tree on the left lists various system components, with 'License (3)' selected. The main pane displays a table of licenses:</p> <table border="1" data-bbox="625 783 1479 1434"> <thead> <tr> <th>Status</th> <th>License</th> <th>Instances</th> <th>Expires</th> </tr> </thead> <tbody> <tr> <td>Valid</td> <td>IP End-points</td> <td>Unlimited</td> <td>Never</td> </tr> <tr> <td>Valid</td> <td>IPSec Tunnelling</td> <td>Unlimited</td> <td>Never</td> </tr> <tr> <td>Valid</td> <td>Phone Manager Pro</td> <td>Unlimited</td> <td>Never</td> </tr> </tbody> </table>	Status	License	Instances	Expires	Valid	IP End-points	Unlimited	Never	Valid	IPSec Tunnelling	Unlimited	Never	Valid	Phone Manager Pro	Unlimited	Never
Status	License	Instances	Expires														
Valid	IP End-points	Unlimited	Never														
Valid	IPSec Tunnelling	Unlimited	Never														
Valid	Phone Manager Pro	Unlimited	Never														

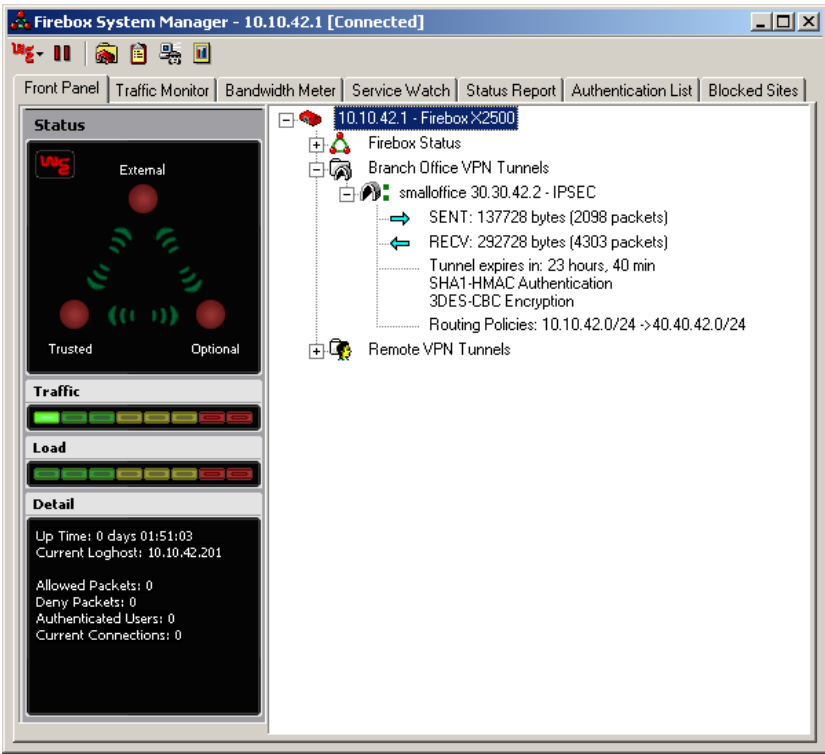

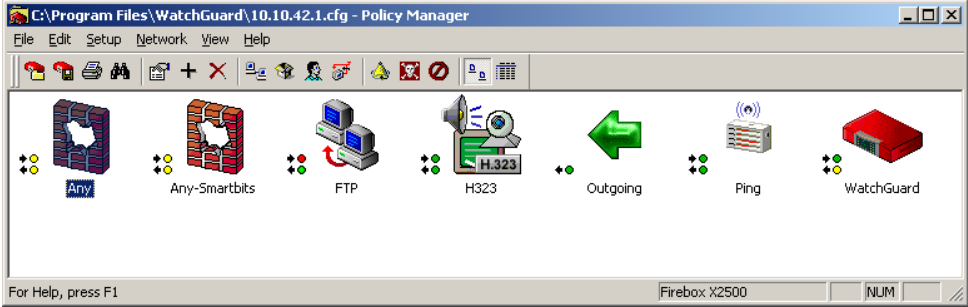
Step	Description
2.	<p>Click on the Tunnel item under the Configuration Tree panel. Right-click over the tunnel view and select New to create an IPsec tunnel. Enter the values shown below to assign a name for the tunnel, the local and remote subnets for the tunnel, and the external IP address of the WatchGuard device in the <i>Gateway</i> field.</p>

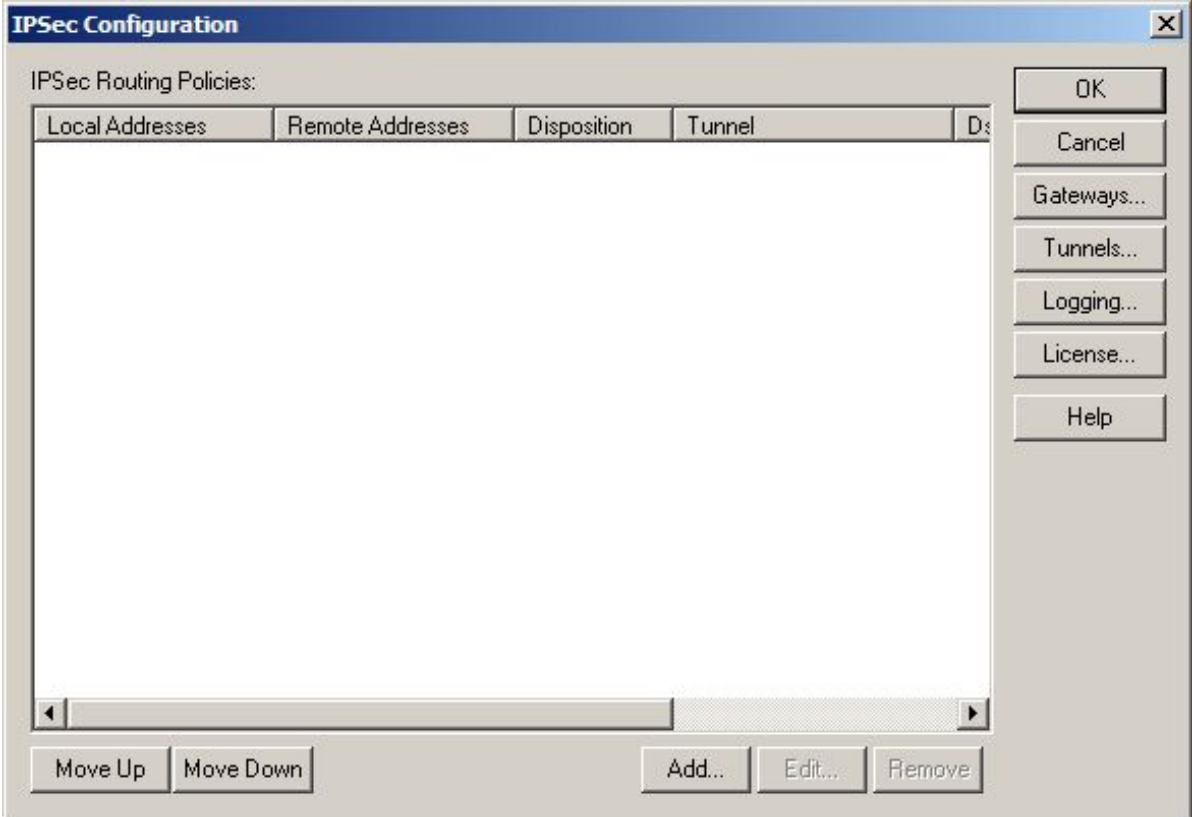


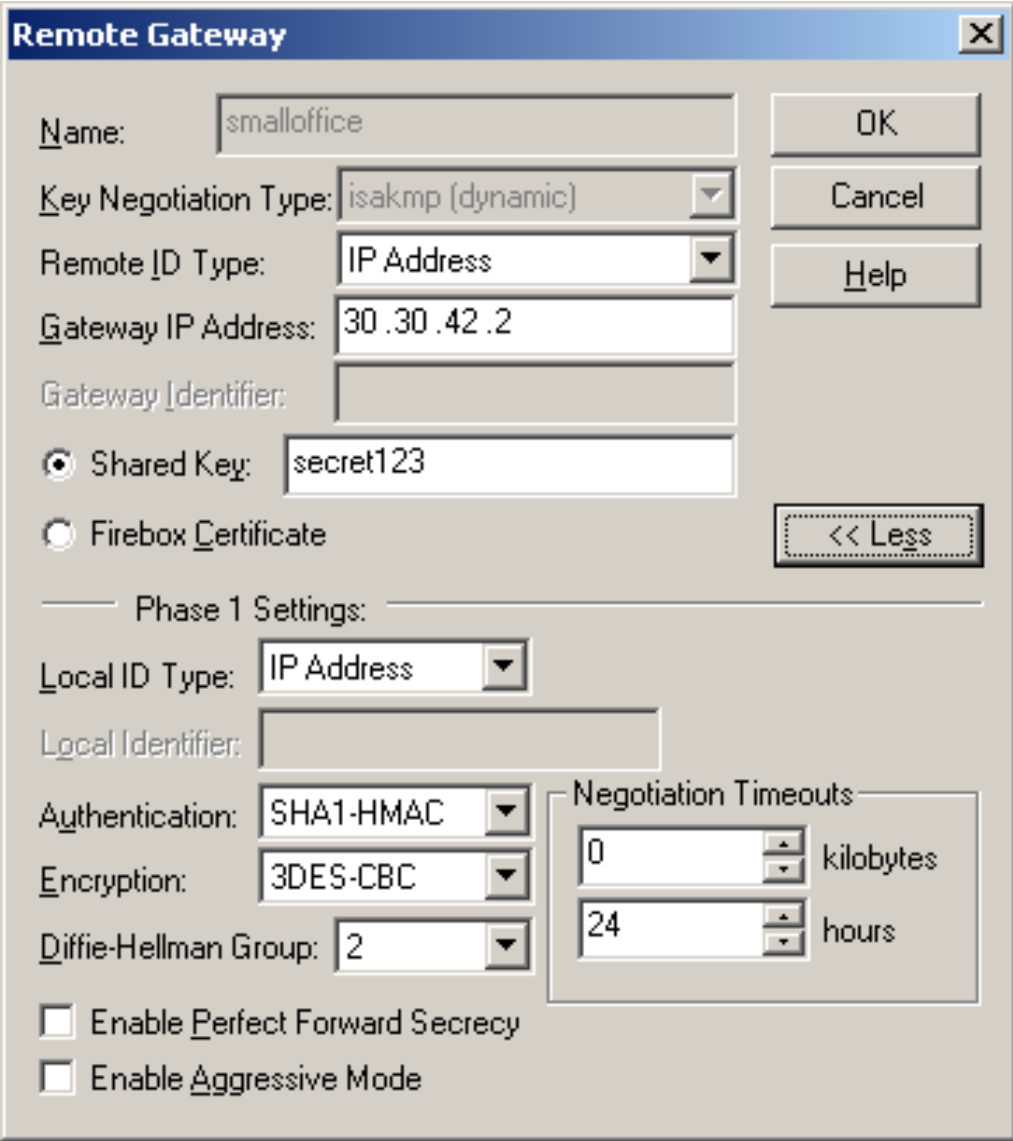
Step	Description
3.	<p>Click the IKE Policies tab. Enter the values shown below for Phase 1 from Table 1 for a site-to-site tunnel:</p> <ul style="list-style-type: none"> • Shared secret – The password used for authentication and must match on the device at the other end of the tunnel. • Confirm Password – Re-enter the shared secret again. • Exchange Type – ID Prot is equivalent to Main Mode on the WatchGuard SOHO (see step 2 of Section 3.3) 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 Hellman Group. • Life Type – Sets whether the Life value is measured in seconds or kilobytes. • Life – The duration before Phase 1 re-authentication is required. 

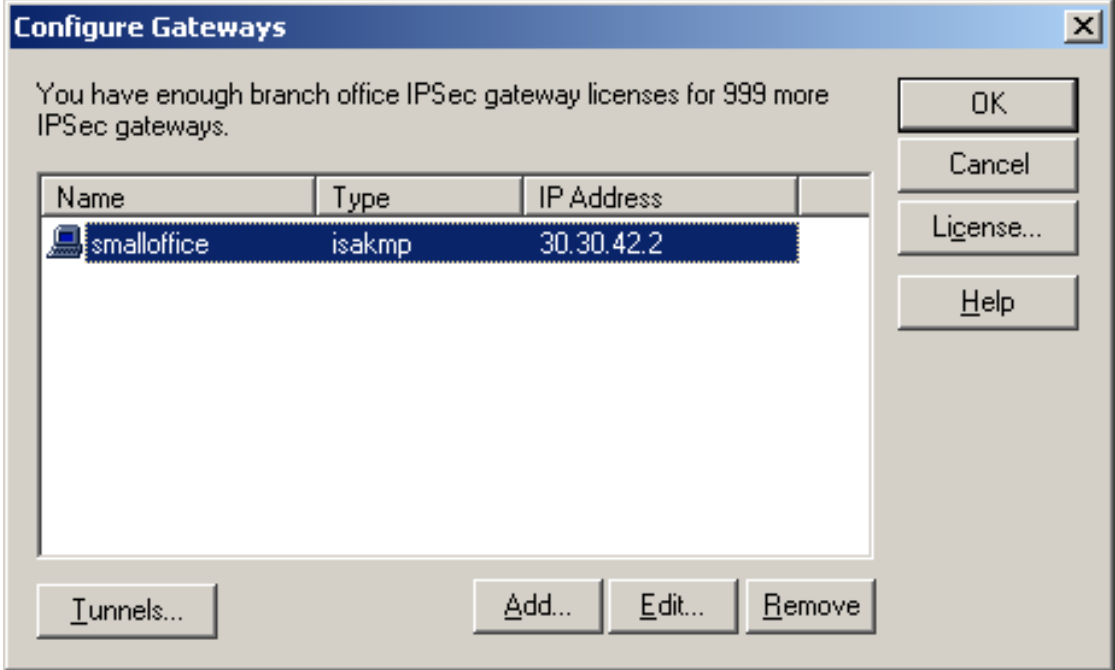
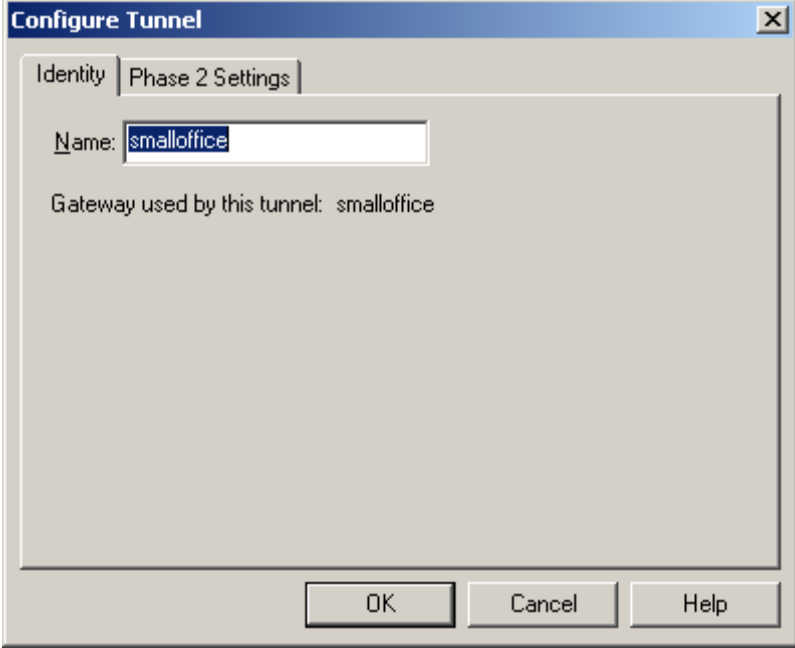
Step	Description
4.	<p>Click the IPSec Policies tab. Enter the values shown below for Phase 2 from Table 1 for a site-to-site tunnel:</p> <ul style="list-style-type: none"> • Protocol – The encryption protocol used by the tunnel. • Encryption – The encryption method used by the tunnel. • Authentication – 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.  <p>Click OK.</p>

3.2. Configure WatchGuard Firebox X

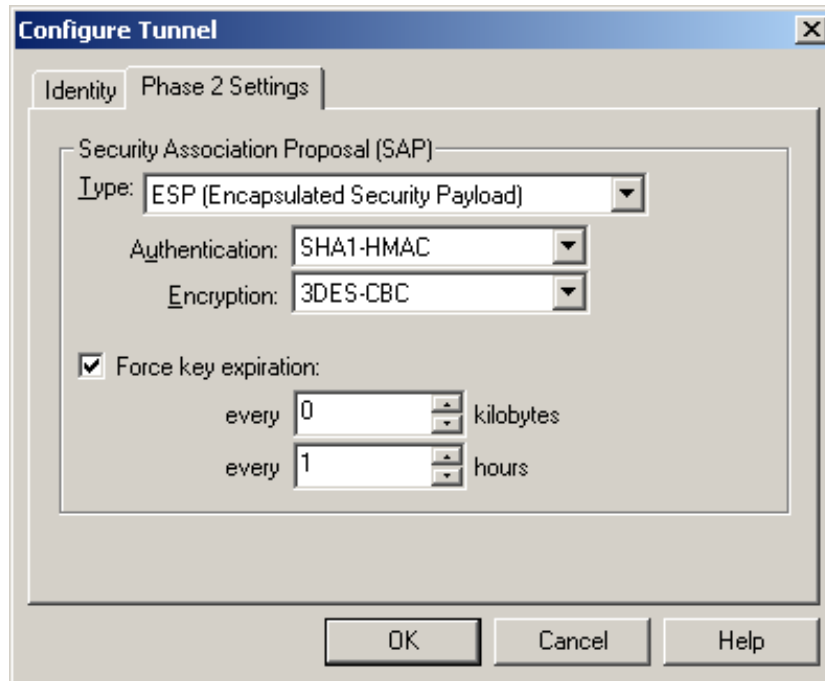
Step	Description
1.	<p>Log into the Firebox X by navigating to Start → Programs → WatchGuard → Firebox System Manager.</p>  <p>Select Tools → Policy Manager or click on the  taskbar icon.</p>
2.	 <p>Click on Network → Branch Office VPN → Manual IPsec... to add a new branch office tunnel with manual security.</p>

Step	Description
3.	<p>Click Gateways and then click Add to add a remote gateway.</p> 

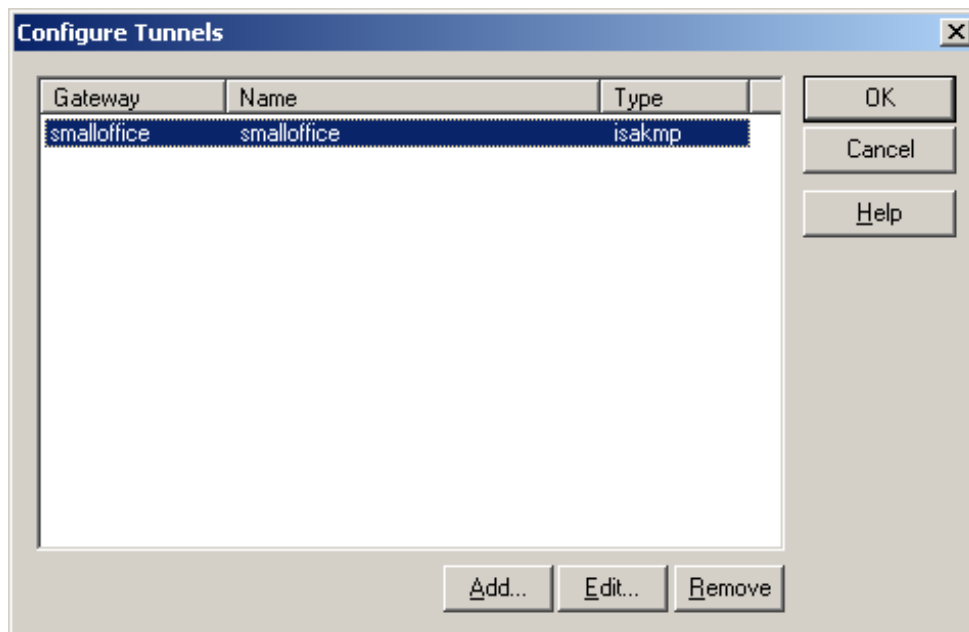
Step	Description
4.	<p>Click More to display the Phase 1 Settings. Enter the values shown below to match the IP Office tunnel configuration for Phase 1. Click OK.</p> 

Step	Description
5.	<p>Click Tunnels... and then click Add to add a new tunnel.</p> 
6.	<p>Select a remote gateway to associate with this tunnel in the Select Gateway dialog window and click OK. Enter a name for the tunnel in the <i>Name</i> field and click the Phase 2 Settings tab.</p> 

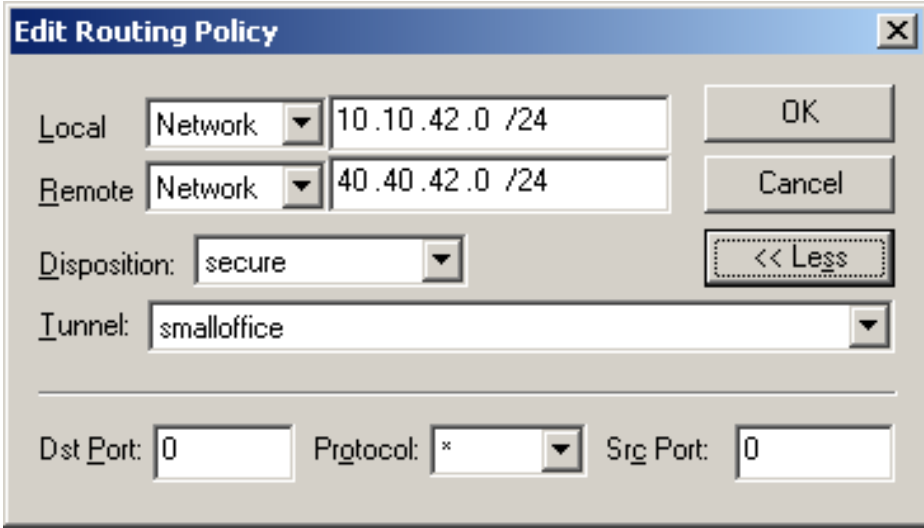
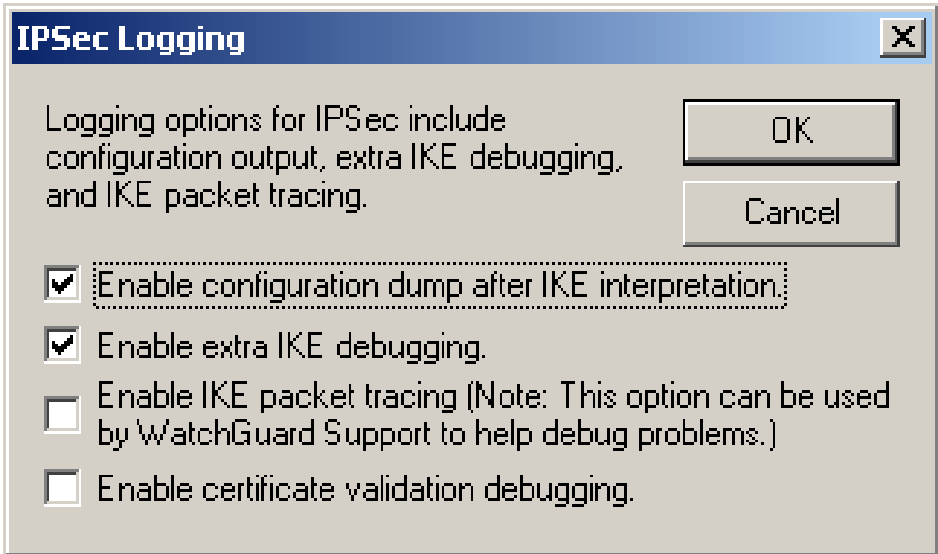
Step	Description
7.	Enter the Phase 2 values shown below to match the IP Office tunnel configuration for Phase 2.

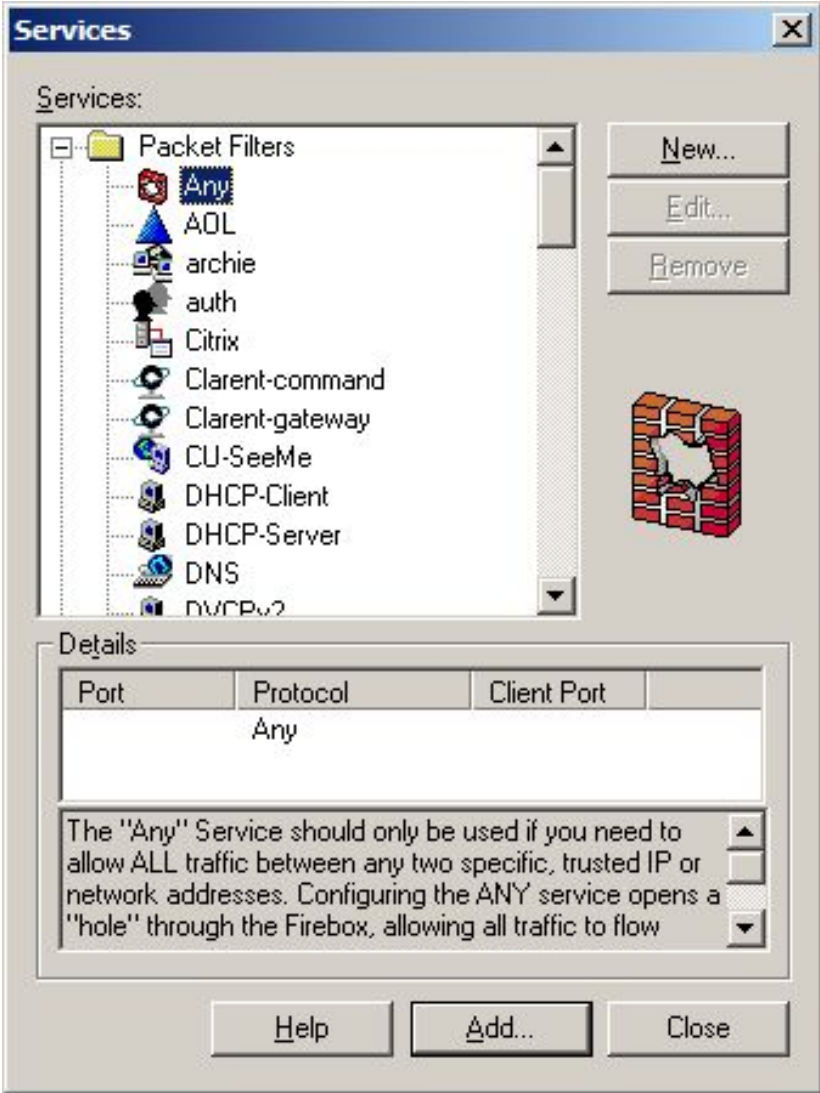


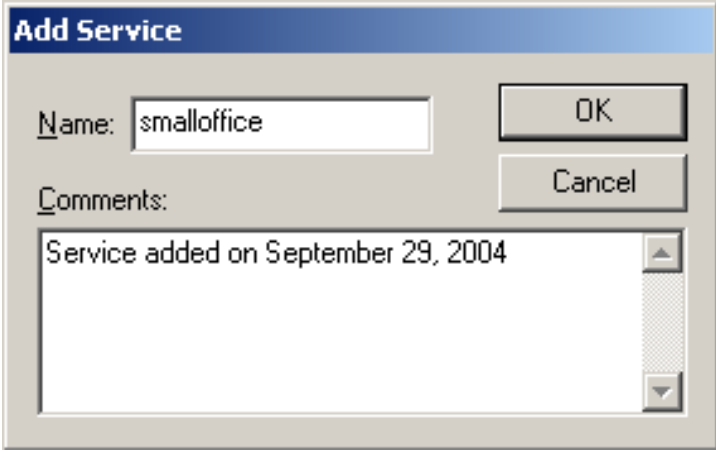
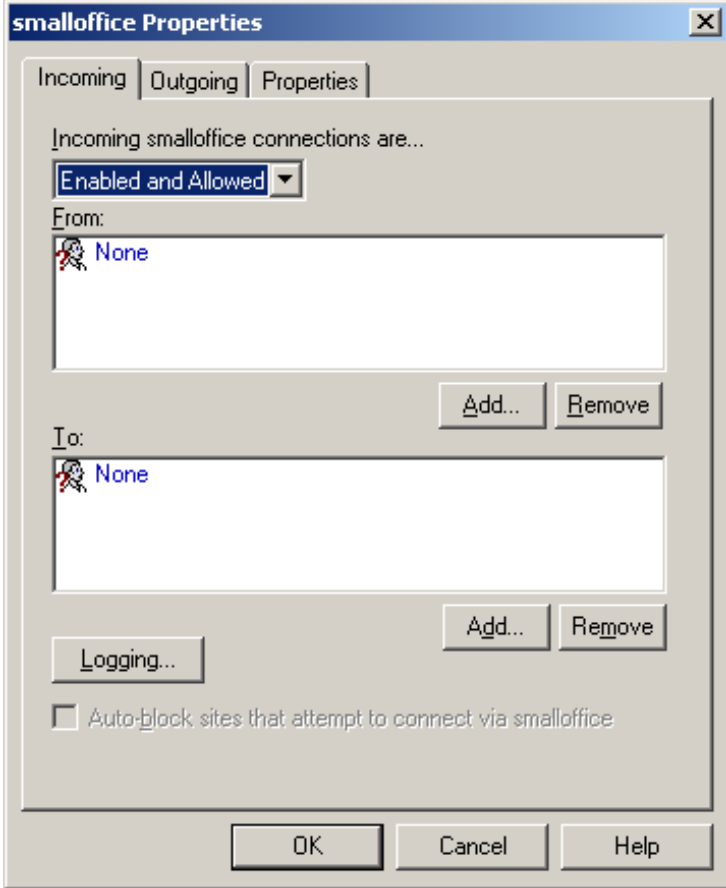
8.	Click OK to return to the Configure Tunnels window.
----	---


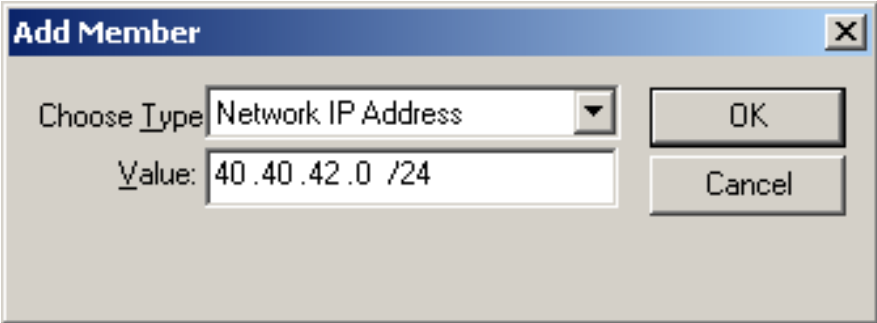



Click **OK** to return to the **IPSec Configuration** window.

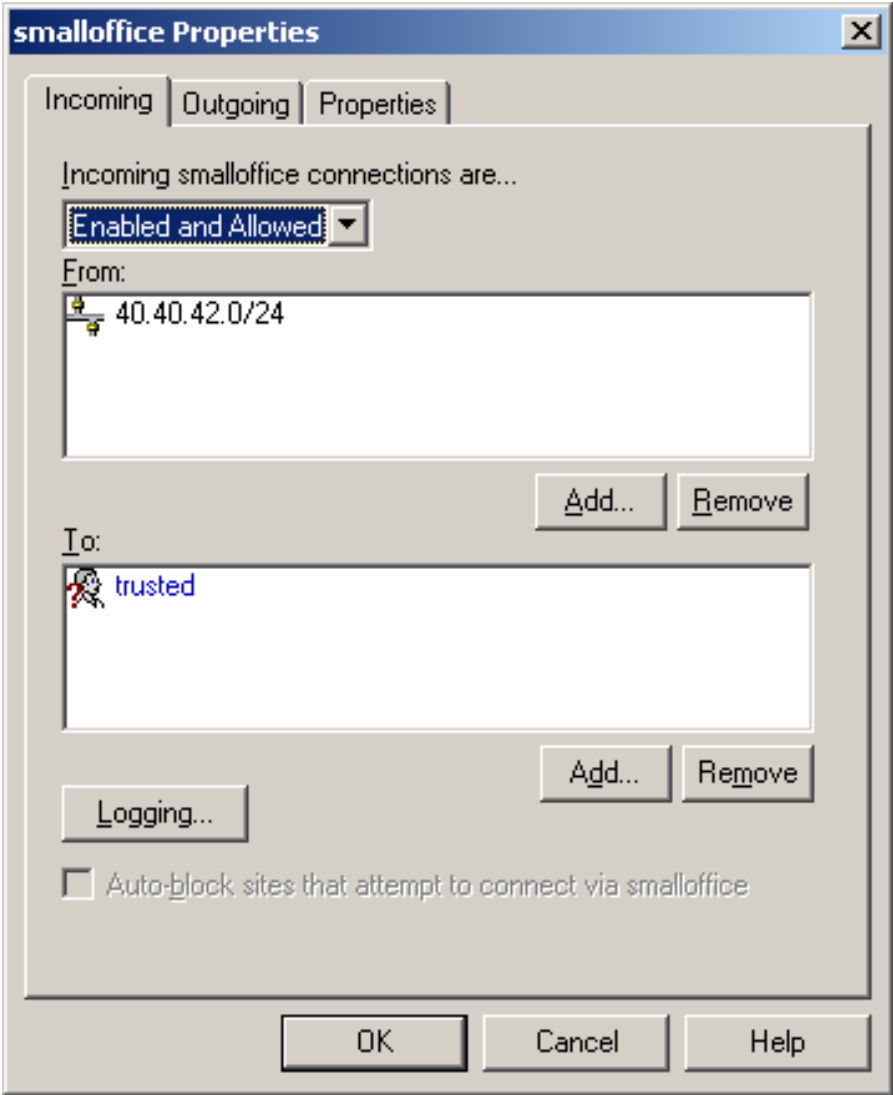
Step	Description
9.	<p>Click Add to add a routing policy. Click More to display the port and protocol fields. Enter the values shown below to specify the local and remote subnets of the tunnel to match the IP Office tunnel configuration and select the tunnel name in the drop-down list to be associated with this routing policy. Click OK.</p> 
10.	<p>If desired, click Logging... to enable IPsec logging for debugging by checking the options shown below. Click OK.</p> 

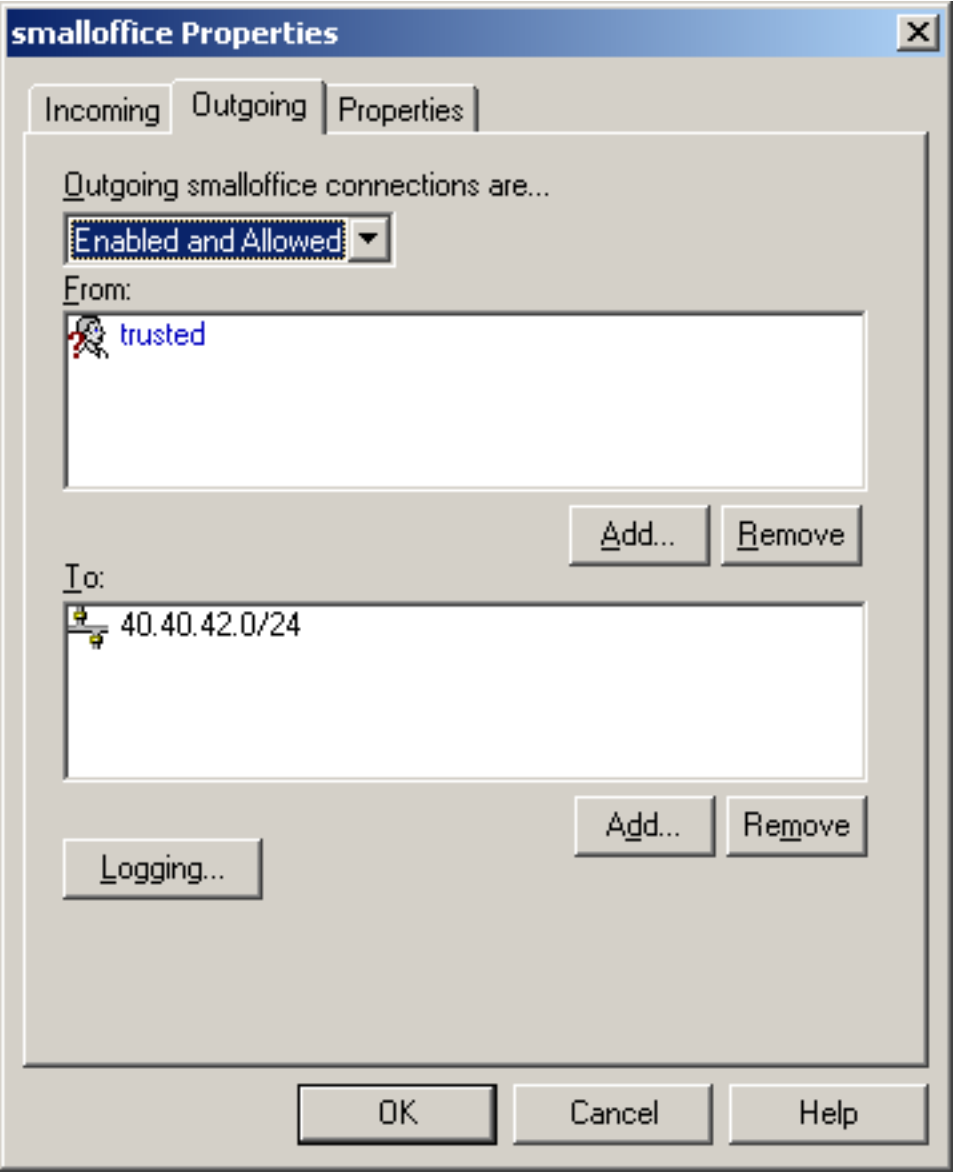
Step	Description
11.	<p>Add a service to allow any access between the network behind Small Office Edition and the trusted network of the Firebox X. In the Policy Manager, select Edit → Add Service, expand the Packet Filters and select the Any service and click Add.</p> 

Step	Description
12.	<p>In the Add Service window, enter a name (e.g., smalloffice) that identifies what this service is being used for and click OK.</p> 
13.	<p>In the Incoming tab, select Enabled and Allowed from the drop-down list. Click Add under the From frame.</p> 

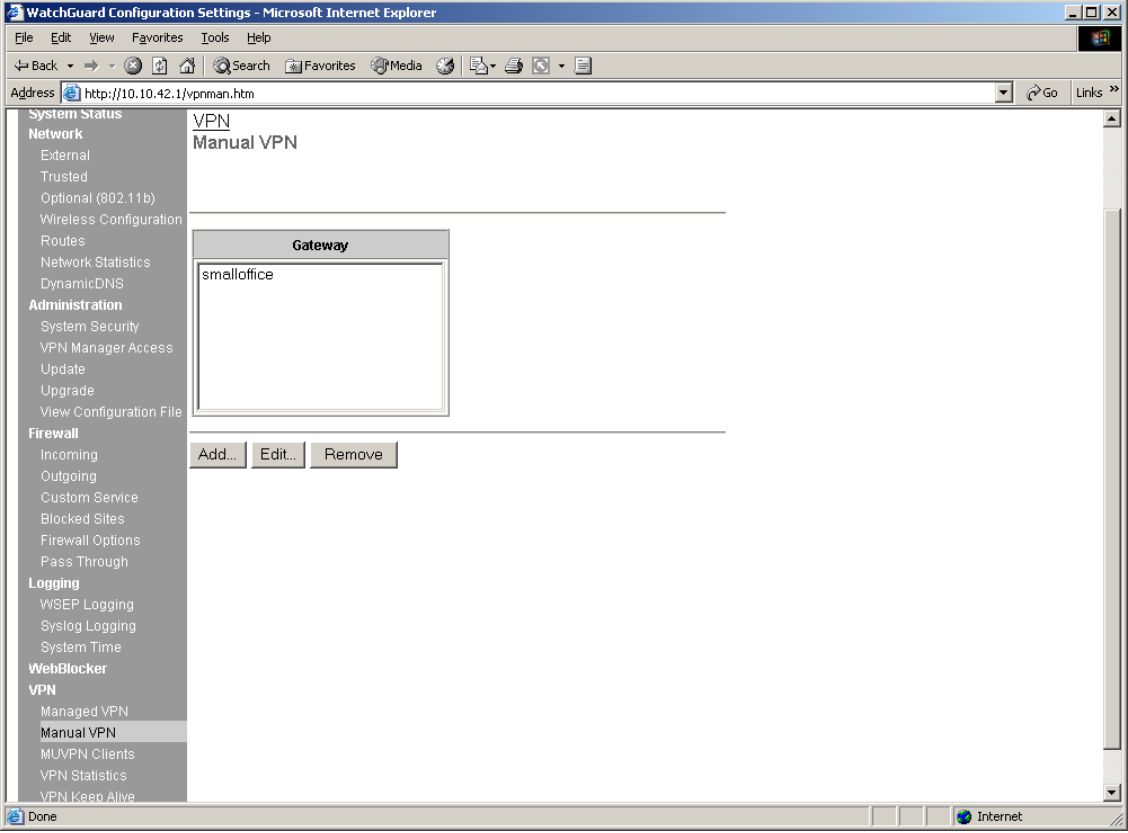
Step	Description
14.	<p>Click Add Other in order to specify the network behind Small Office Edition.</p>  <p>The screenshot shows a dialog box titled "Add Address". It has a "Members:" list with the following items: firebox, optional, trusted, eth3, eth4, eth5, ipsec_users, and pptp_users. The "firebox" item is selected. Below the list are buttons for "Add", "Show Users", "NAT...", and "Add Other...". To the right of the list are buttons for "OK", "Cancel", and "Help". Below the list is a section labeled "Selected Members and Addresses:" with an empty box.</p>
15.	<p>Select Network IP Address from the drop-down list in the <i>Choose Type</i> field and enter the network behind IP Office in the <i>Value</i> field. Click OK twice to return to the smalloffice properties window. Click Add under the To frame.</p>  <p>The screenshot shows a dialog box titled "Add Member". It has a "Choose Type" dropdown menu set to "Network IP Address" and a "Value:" text field containing "40.40.42.0 /24". There are "OK" and "Cancel" buttons on the right.</p>

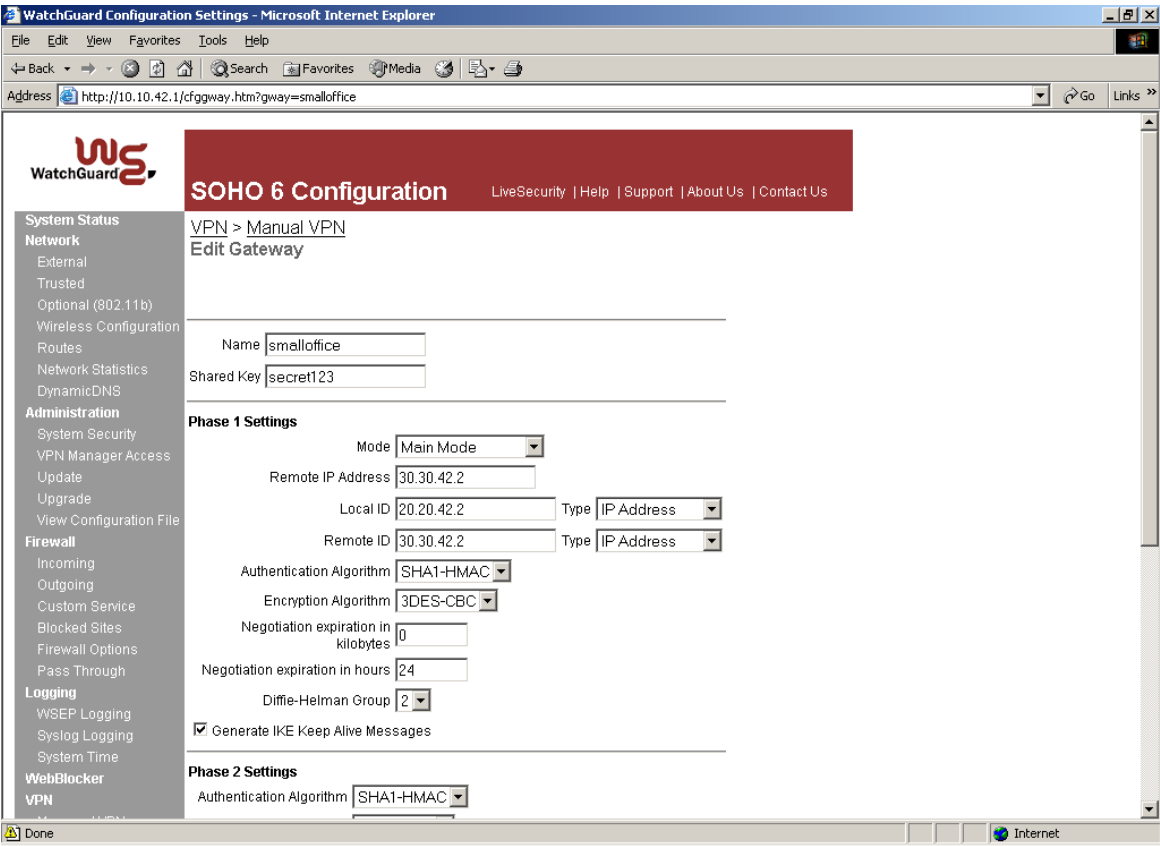
Step	Description
16.	<p>Select trusted and click Add to specify the trusted network behind the Firebox X. Click OK to return to the smalloffice properties window.</p> 

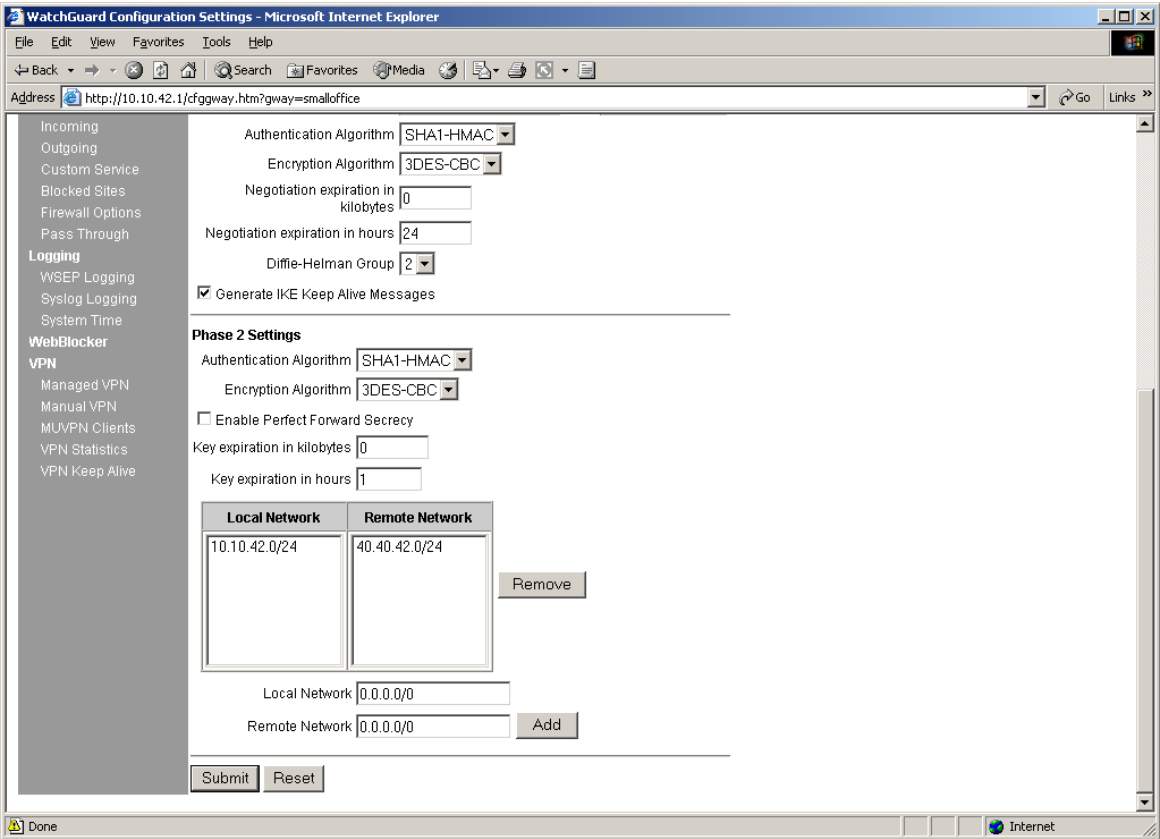
Step	Description
17.	<p>Click the Outgoing tab and repeat steps 13-16 to enable and allow outgoing connections from the trusted network to the network behind Small Office Edition.</p> 

Step	Description
18.	<p>Click OK and Close on the Services window to return to the Policy Manager window.</p> 

3.3. Configure the WatchGuard SOHO

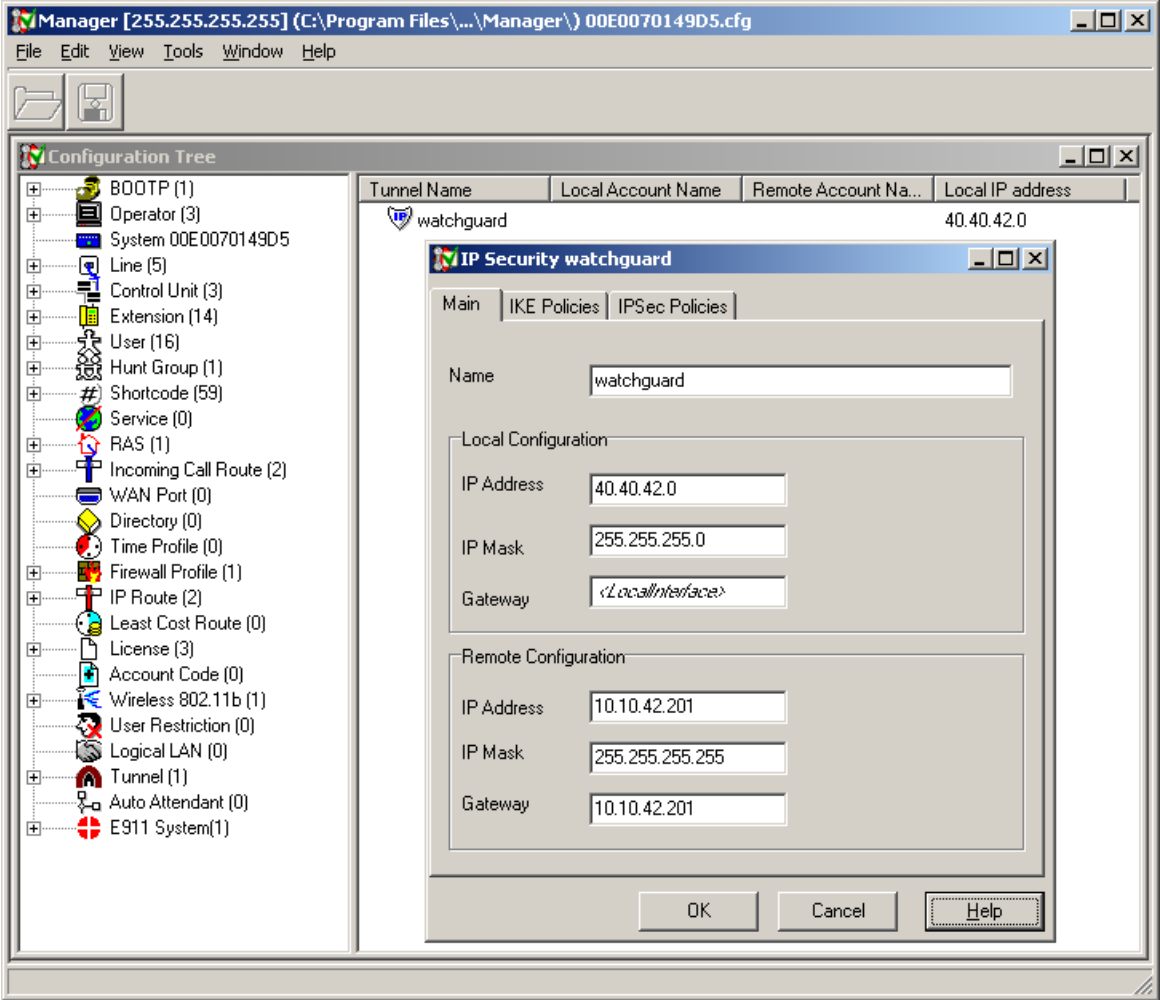
Step	Description
1.	<p>Open the SOHO 6 Configuration screen by specifying the IP address of private interface of the SOHO 6tc Wireless in a browser window. Click the Manual VPN option on the left pane and click Add to create a VPN tunnel to the IP Office.</p>  <p>The screenshot shows a web browser window titled "WatchGuard Configuration Settings - Microsoft Internet Explorer". The address bar shows "http://10.10.42.1/vpnman.htm". The left navigation pane is expanded to "Manual VPN". The main content area shows a "Gateway" field with the text "smalloffice" entered. Below the field are three buttons: "Add...", "Edit...", and "Remove".</p>

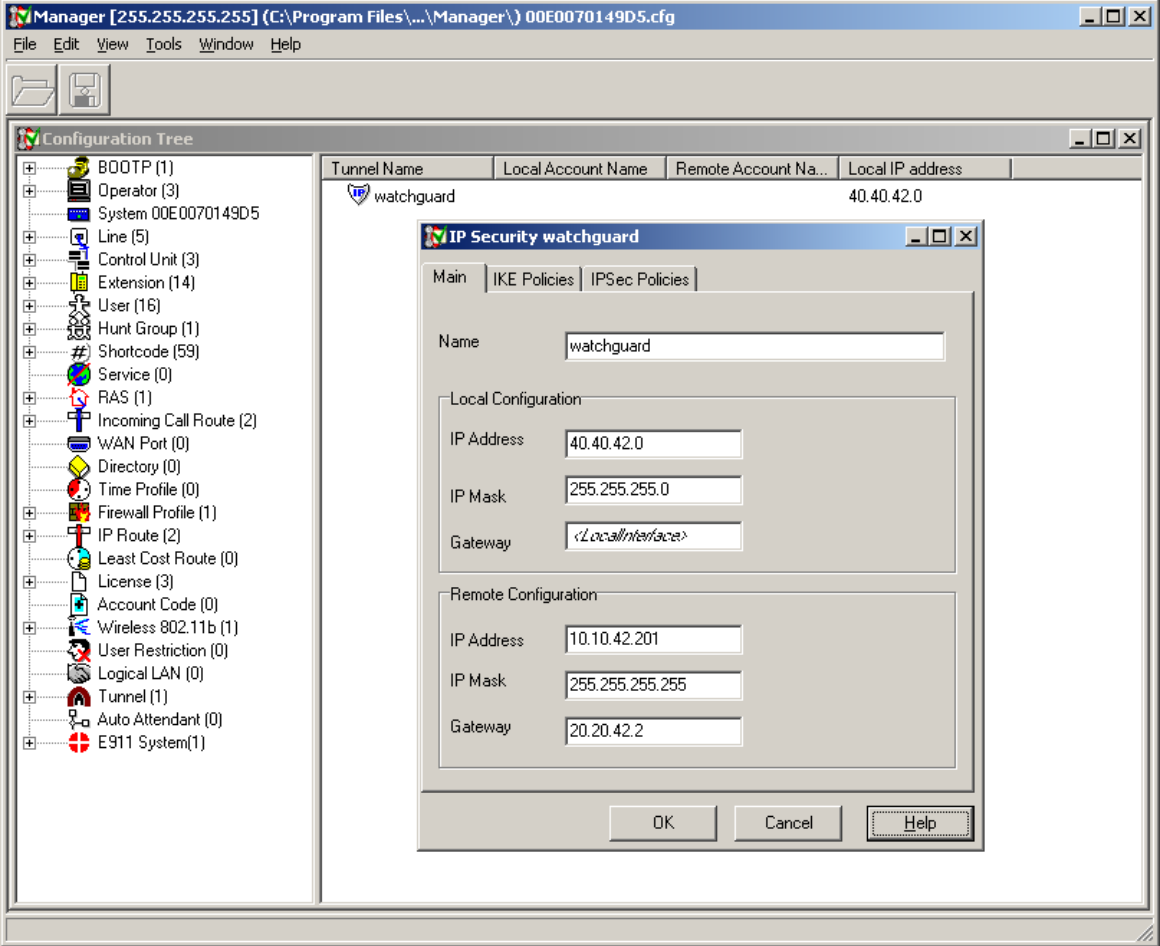
Step	Description
2.	<p>Enter the values shown below to match the IP Office tunnel configuration for Phase 1 and the shared key.</p>  <p>The screenshot shows the WatchGuard Configuration Settings web interface in Microsoft Internet Explorer. The browser address bar shows <code>http://10.10.42.1/cfggway.htm?gway=smalloffice</code>. The page title is "SOHO 6 Configuration" and the sub-page is "VPN > Manual VPN Edit Gateway".</p> <p>System Status</p> <ul style="list-style-type: none"> Network <ul style="list-style-type: none"> External Trusted Optional (802.11b) Wireless Configuration Routes Network Statistics DynamicDNS Administration <ul style="list-style-type: none"> System Security VPN Manager Access Update Upgrade View Configuration File Firewall <ul style="list-style-type: none"> Incoming Outgoing Custom Service Blocked Sites Firewall Options Pass Through Logging <ul style="list-style-type: none"> WSEP Logging Syslog Logging System Time WebBlocker VPN <p>Configuration Fields:</p> <ul style="list-style-type: none"> Name: <input type="text" value="smalloffice"/> Shared Key: <input type="text" value="secret123"/> Phase 1 Settings <ul style="list-style-type: none"> Mode: <input type="text" value="Main Mode"/> Remote IP Address: <input type="text" value="30.30.42.2"/> Local ID: <input type="text" value="20.20.42.2"/> Type: <input type="text" value="IP Address"/> Remote ID: <input type="text" value="30.30.42.2"/> Type: <input type="text" value="IP Address"/> Authentication Algorithm: <input type="text" value="SHA1-HMAC"/> Encryption Algorithm: <input type="text" value="3DES-CBC"/> Negotiation expiration in kilobytes: <input type="text" value="0"/> Negotiation expiration in hours: <input type="text" value="24"/> Diffie-Helman Group: <input type="text" value="2"/> <input checked="" type="checkbox"/> Generate IKE Keep Alive Messages Phase 2 Settings <ul style="list-style-type: none"> Authentication Algorithm: <input type="text" value="SHA1-HMAC"/>

Step	Description				
3.	<p>Enter the values shown below to match the Phase 2 IP Office tunnel configuration. Enter the subnet of the Phone Manager PC in the <i>Local Network</i> field and the subnet of the IP telephone and IP Office in the <i>Remote Network</i> field and click on Add to specify the local and remote networks for the tunnel.</p>  <p>The screenshot shows the WatchGuard Configuration Settings interface in Microsoft Internet Explorer. The browser address bar shows 'http://10.10.42.1/cfggateway.htm?gway=smalloffice'. The left sidebar contains a navigation menu with categories: Incoming, Outgoing, Custom Service, Blocked Sites, Firewall Options, Pass Through, Logging, WebBlocker, and VPN. The main content area is titled 'Phase 2 Settings' and includes the following fields and controls:</p> <ul style="list-style-type: none"> Authentication Algorithm: SHA1-HMAC (dropdown) Encryption Algorithm: 3DES-CBC (dropdown) Negotiation expiration in kilobytes: 0 (text input) Negotiation expiration in hours: 24 (text input) Diffie-Helman Group: 2 (dropdown) <input checked="" type="checkbox"/> Generate IKE Keep Alive Messages Phase 2 Settings section: <ul style="list-style-type: none"> Authentication Algorithm: SHA1-HMAC (dropdown) Encryption Algorithm: 3DES-CBC (dropdown) <input type="checkbox"/> Enable Perfect Forward Security Key expiration in kilobytes: 0 (text input) Key expiration in hours: 1 (text input) Network configuration table: <table border="1" data-bbox="516 913 812 1081"> <thead> <tr> <th>Local Network</th> <th>Remote Network</th> </tr> </thead> <tbody> <tr> <td>10.10.42.0/24</td> <td>40.40.42.0/24</td> </tr> </tbody> </table> Local Network: 0.0.0.0/0 (text input) Remote Network: 0.0.0.0/0 (text input) Buttons: Remove, Add, Submit, Reset 	Local Network	Remote Network	10.10.42.0/24	40.40.42.0/24
Local Network	Remote Network				
10.10.42.0/24	40.40.42.0/24				

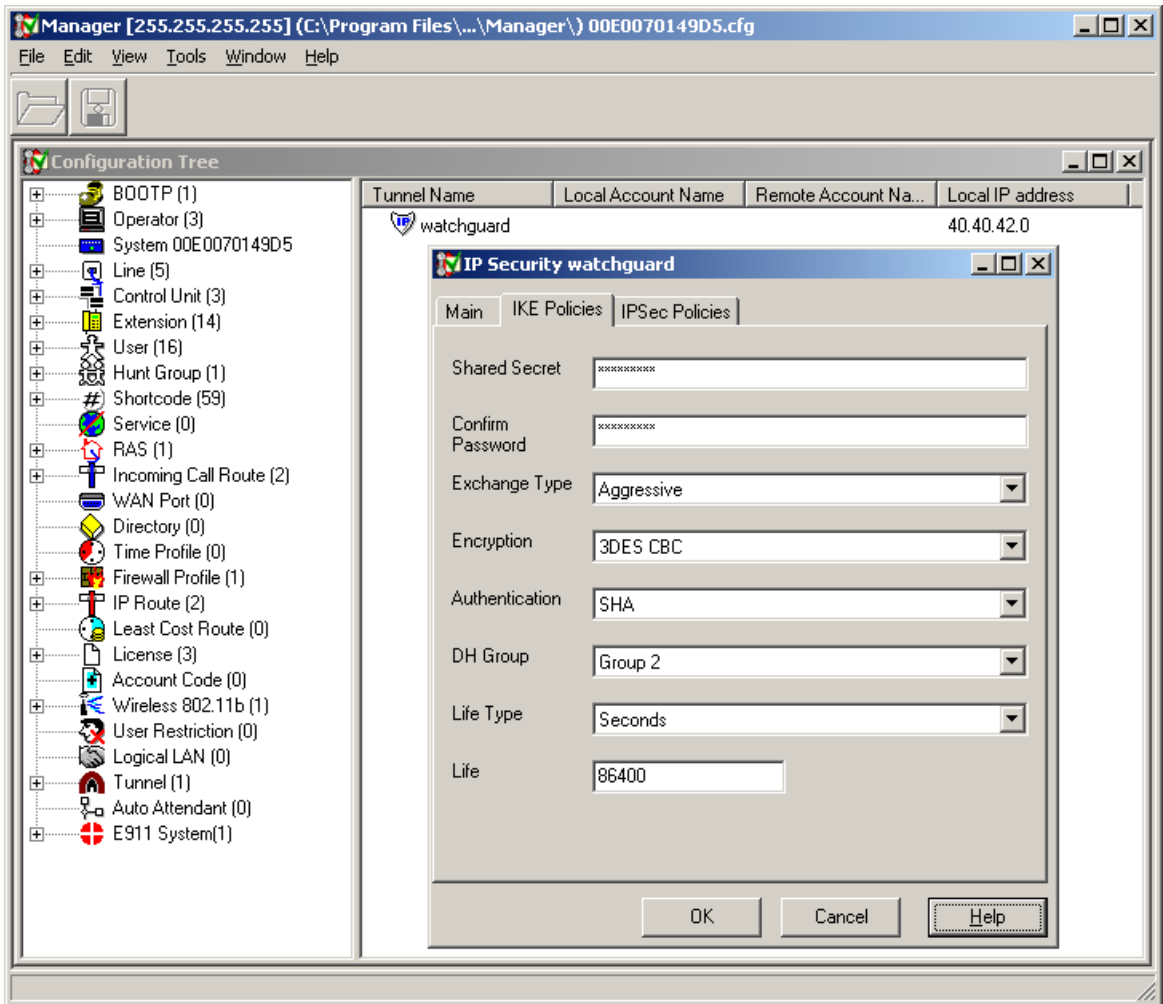
4. Configuration 2 (VPN tunnel between client and IP Office)

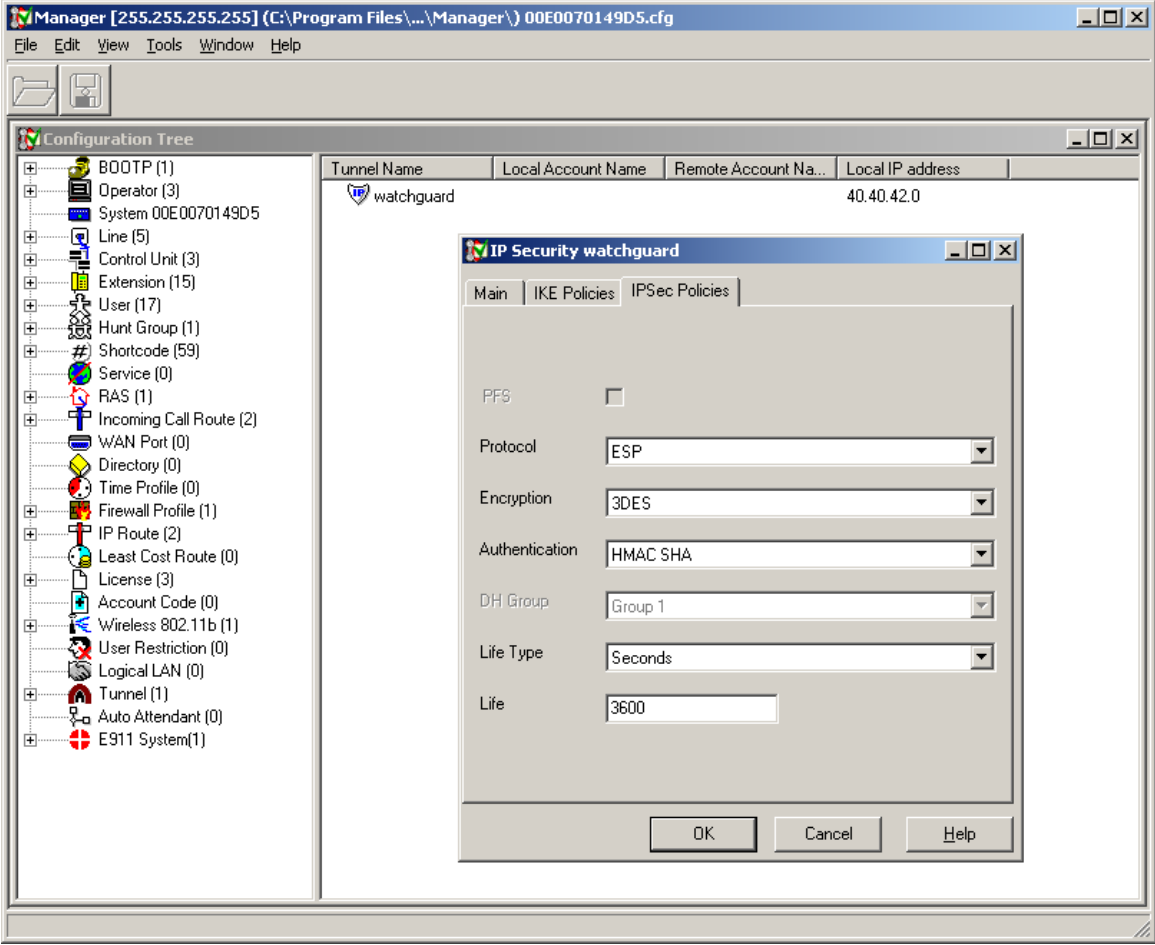
4.1. Configuring Avaya IP Office

Step	Description
1.	<p>The following screen applies when the Firebox X is used in configuration 2. Click on the Tunnel item under the Configuration Tree view. Right-click over the tunnel window Enter the values shown below for the local and remote networks and the remote tunnel endpoint address of the Phone Manager PC in the <i>Gateway</i> field.</p> 

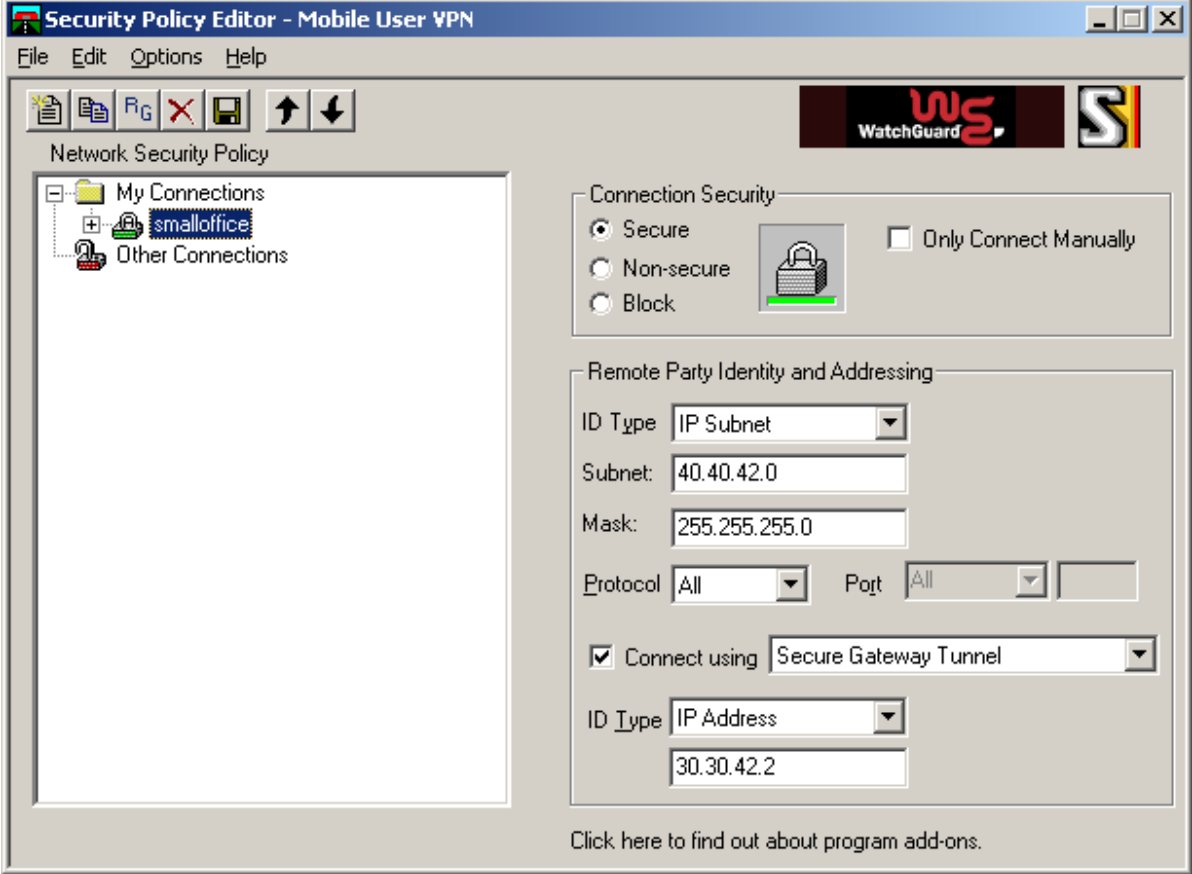
Step	Description
	<p>Note: The following screen applies when the SOHO is used in configuration 2. The external IP address of the SOHO (e.g., 20.20.42.2) must be specified as the remote tunnel endpoint address in <i>the Gateway</i> field because NAT (Network Address Translation) cannot be turned off on the SOHO.</p>  <p>The screenshot displays the Manager software interface. On the left is a Configuration Tree with various system components. The main window shows a table with columns: Tunnel Name, Local Account Name, Remote Account Name, and Local IP address. The 'watchguard' tunnel is selected, showing a Local IP address of 40.40.42.0. An 'IP Security watchguard' dialog box is open, showing configuration details for the tunnel. The 'Local Configuration' section includes fields for IP Address (40.40.42.0), IP Mask (255.255.255.0), and Gateway (<LocalInterface>). The 'Remote Configuration' section includes fields for IP Address (10.10.42.201), IP Mask (255.255.255.255), and Gateway (20.20.42.2). Buttons for OK, Cancel, and Help are visible at the bottom of the dialog.</p>

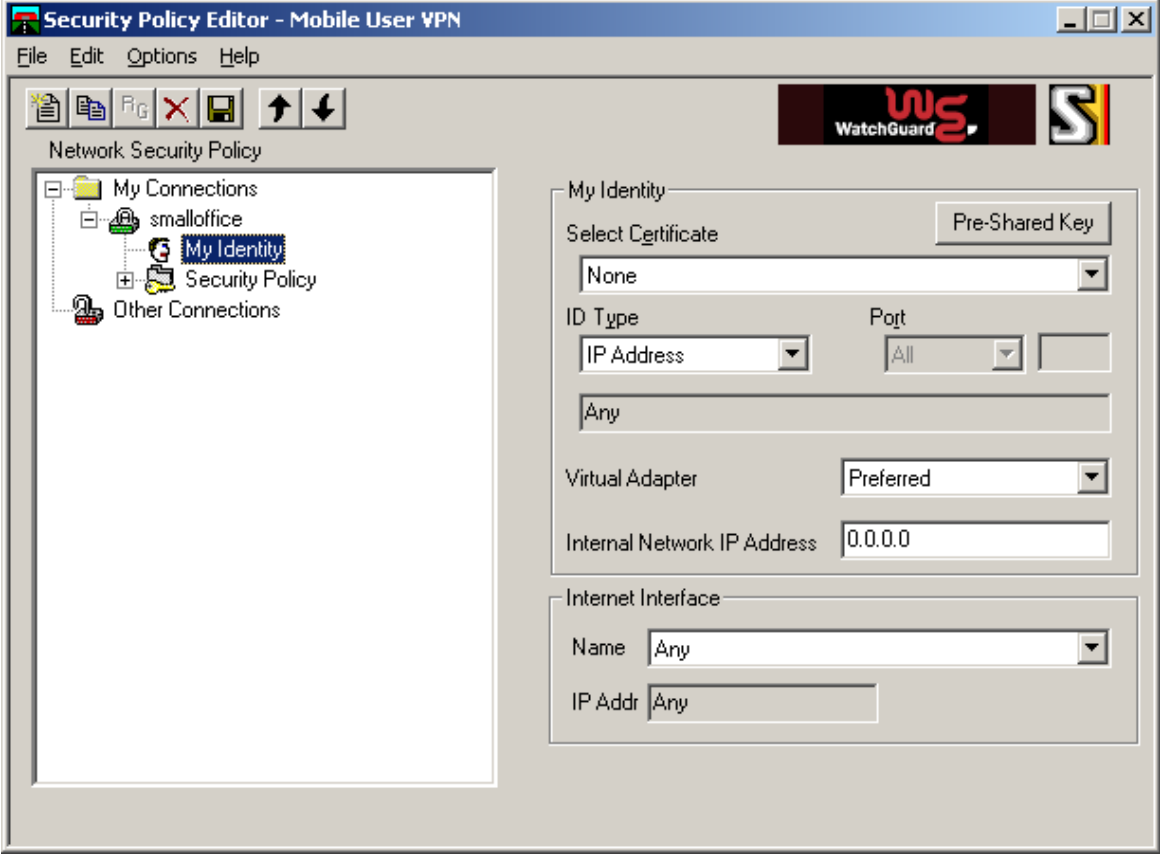
Step	Description
3.	<p>Click the IKE Policies tab. Enter the values shown below for Phase 1 from Table 1 for a client tunnel:</p> <ul style="list-style-type: none"> • Shared secret – The password used for authentication and must match on the device at the other end of the tunnel. • Confirm Password – Re-enter the shared secret again • 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.

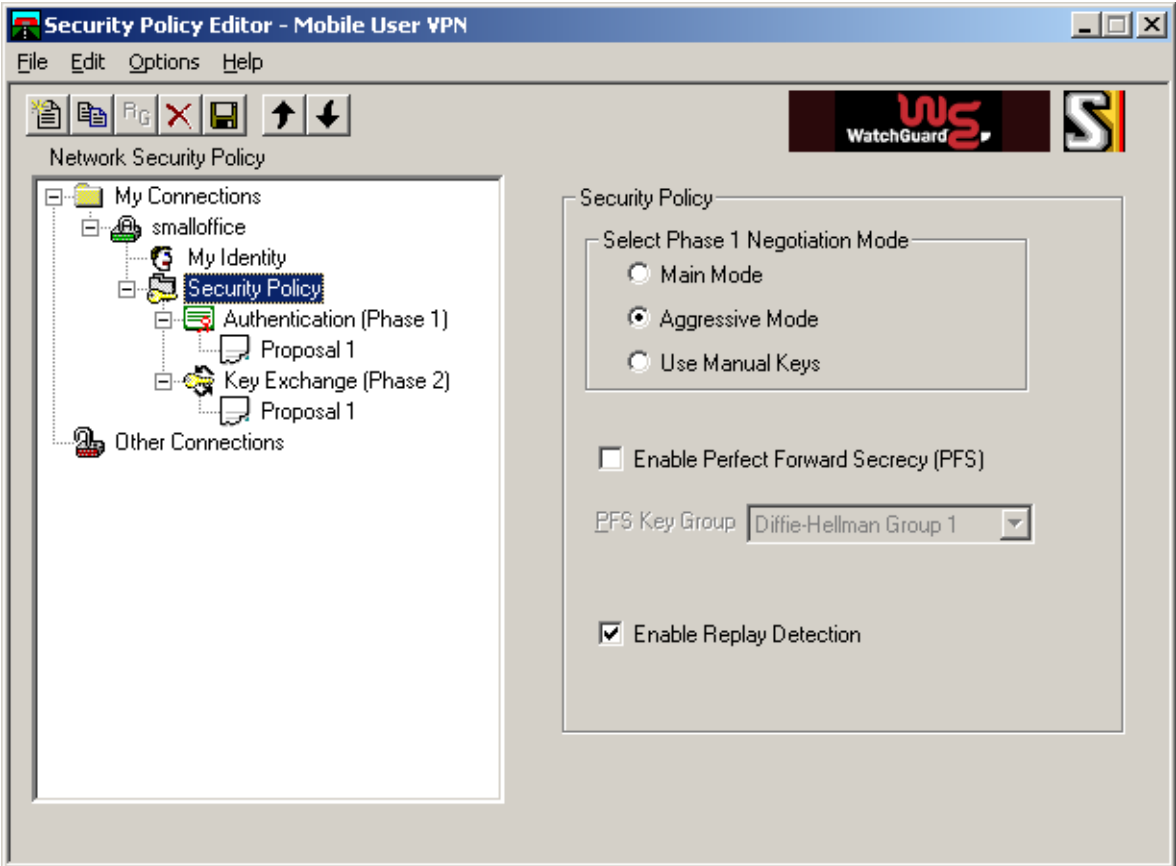


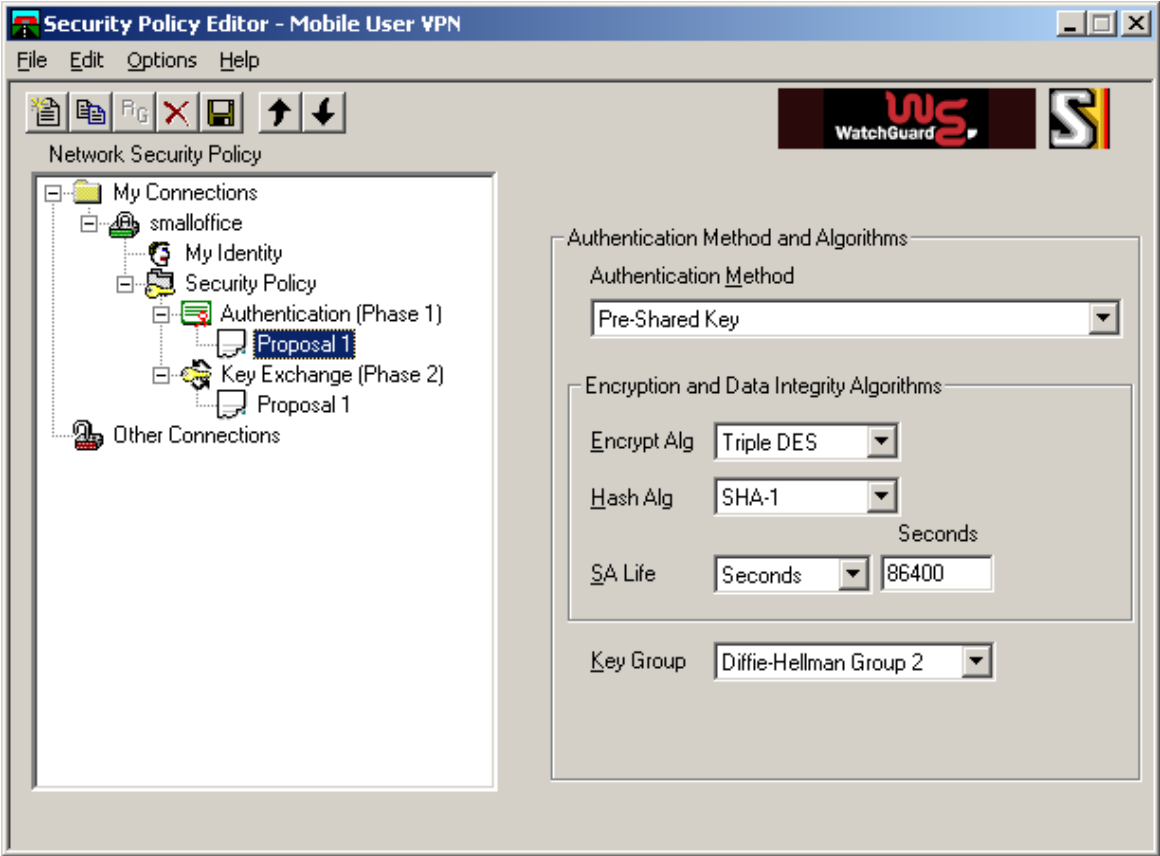
Step	Description
4.	<p>Click the IPSec Policies tab. Enter the values shown below for Phase 2 from Table 1 for a client tunnel:</p> <ul style="list-style-type: none"> • Protocol – The encryption protocol used by the tunnel. • Encryption – The encryption method used by the tunnel. • Authentication – The 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  <p>Click OK.</p>

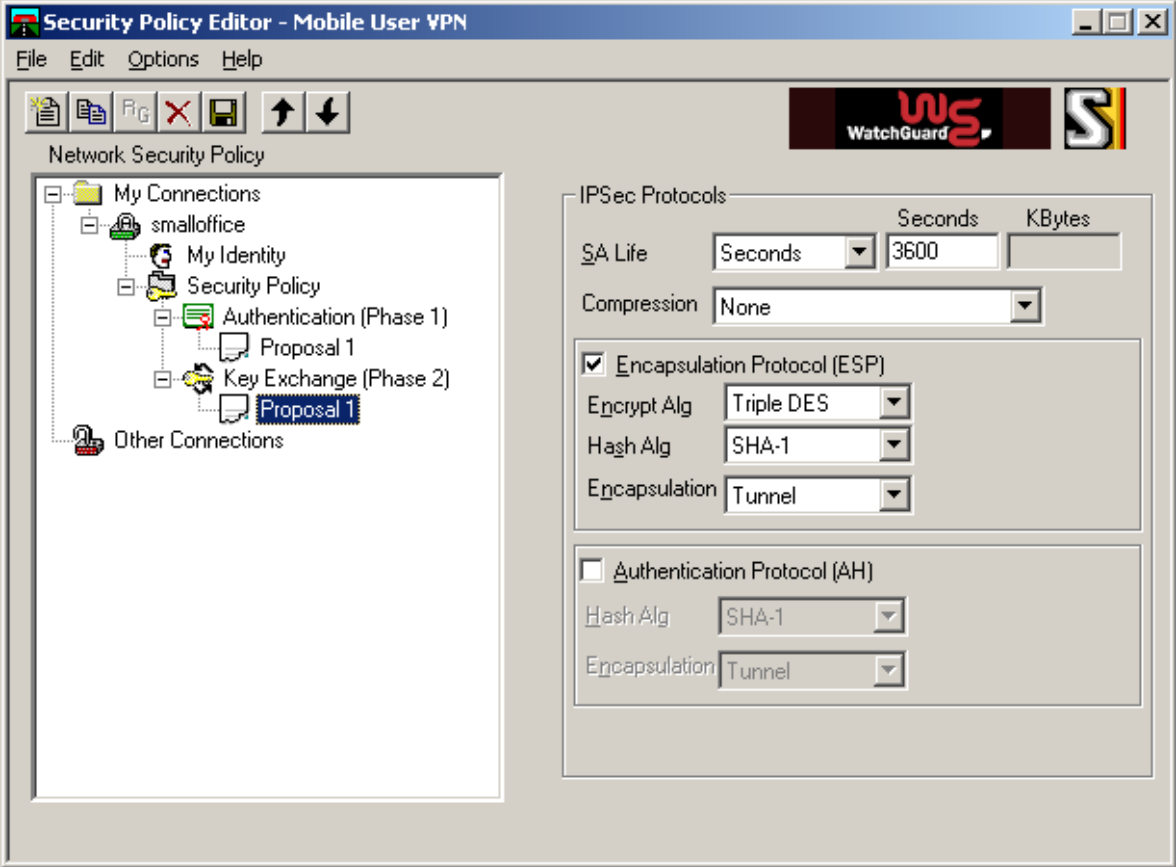

4.2. Configure MUVPN Client

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., smalloffice) and enter the values shown below, matching the IP Office tunnel configuration by specifying the remote subnet and IP address of the Small Office Edition 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 IP Office tunnel configuration. Select Preferred in the Virtual Adapter drop-down list and leave the other fields as default.</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 reveal 'My Identity'. The right pane is titled 'My Identity' and contains the following settings:</p> <ul style="list-style-type: none"> Select Certificate: A dropdown menu set to 'None'. A 'Pre-Shared Key' button is visible to the right. ID Type: A dropdown menu set to 'IP Address'. Port: A dropdown menu set to 'All'. Virtual Adapter: A dropdown menu set to 'Preferred'. Internal Network IP Address: A text box containing '0.0.0.0'. Internet Interface: A section with 'Name' set to 'Any' and 'IP Addr' set to 'Any'.

Step	Description
3.	<p>Click Security Policy and 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 displays a tree structure under 'Network Security Policy' with 'Security Policy' selected. The right pane shows the configuration for the selected policy, including the 'Select Phase 1 Negotiation Mode' section where 'Aggressive Mode' is selected. Other options include 'Enable Perfect Forward Secrecy (PFS)', 'PFS Key Group' (set to 'Diffie-Hellman Group 1'), and 'Enable Replay Detection' (checked).</p>

Step	Description
4.	<p>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.</p> 

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

5. Interoperability Compliance Testing

The features of the WatchGuard Firebox and SOHO products 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 configuration diagram shown in **Figure 1**:

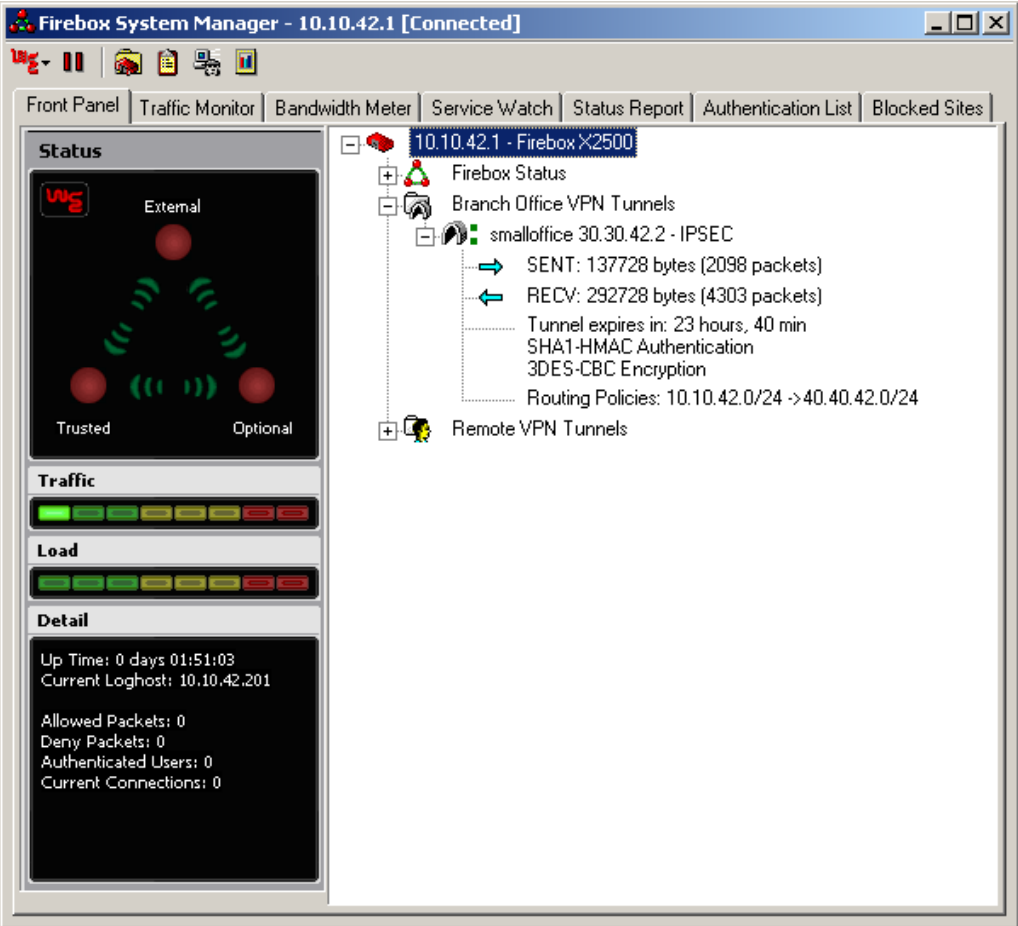
- Ability to establish a site-to-site VPN tunnel (Configuration 1) between the WatchGuard products (Firebox X2500 or SOHO 6tc Wireless) and the Small Office Edition
- Ability to establish a VPN tunnel (Configuration 2) between the Phone Manager Pro client and the Small Office Edition using the MUVPN 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 Small Office Edition
- RAS (Registration Admission Status) over the VPN tunnel

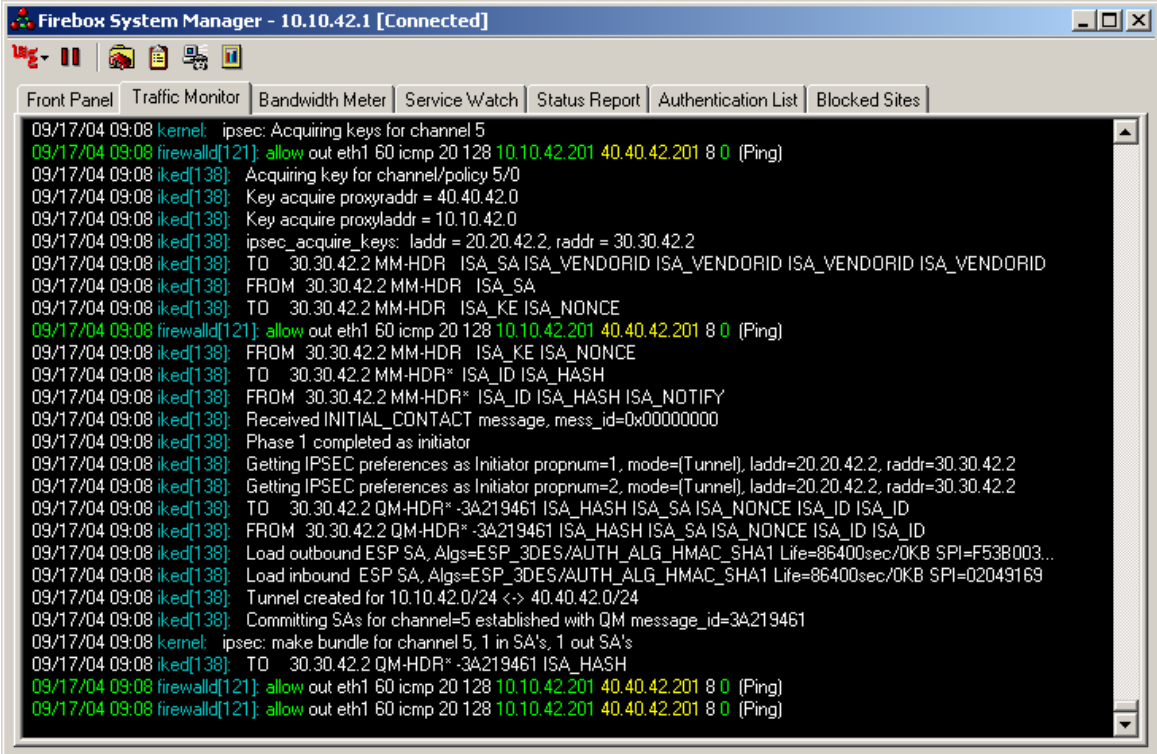
5.2. Test Results


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

6. Verification Steps

Step	Description
1.	<p>Using the IP Office SysMonitor log, verify that Phase 1 and Phase 2 negotiations completed. The negotiation messages will only appear if the trace option IPSec Events is checked under the VPN tab for the SysMonitor log filter. Following is an example of the Phase 1 and Phase 2 negotiation messages.</p> <pre data-bbox="305 499 1497 1360"> 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=ffdeea0 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 </pre>

Step	Description
2.	<p>From the Firebox System Manager window, expand the tunnel name listed under the Branch Office VPN Tunnels item to view statistics for the site-to-site tunnel between the Firebox X and Small Office Edition.</p>  <p>The screenshot displays the Firebox System Manager interface for IP address 10.10.42.1. The interface includes a navigation bar with tabs: Front Panel, Traffic Monitor, Bandwidth Meter, Service Watch, Status Report, Authentication List, and Blocked Sites. The main content area is divided into two sections. On the left, the 'Status' section shows a network diagram with 'External', 'Trusted', and 'Optional' zones. Below it are 'Traffic' and 'Load' indicators, and a 'Detail' section showing system information like 'Up Time: 0 days 01:51:03' and 'Current Loghost: 10.10.42.201'. On the right, a tree view shows the configuration hierarchy: 10.10.42.1 - Firebox X2500, Firebox Status, Branch Office VPN Tunnels, and Remote VPN Tunnels. The 'smalloffice 30.30.42.2 - IPSEC' tunnel is expanded, showing statistics: SENT: 137728 bytes (2098 packets), RECV: 292728 bytes (4303 packets), Tunnel expires in: 23 hours, 40 min, SHA1-HMAC Authentication, 3DES-CBC Encryption, and Routing Policies: 10.10.42.0/24 -> 40.40.42.0/24.</p>

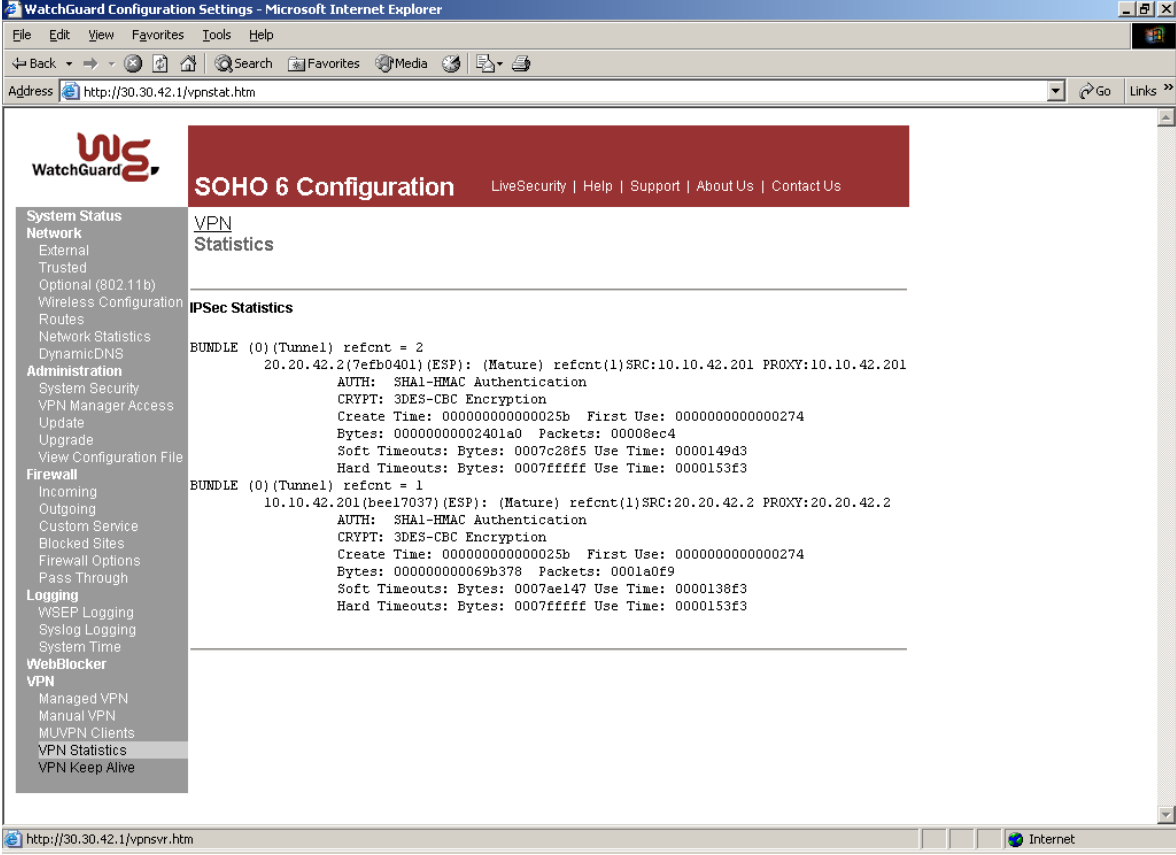
Step	Description
3.	<p>Click on the Traffic Monitor tab to view Phase 1 negotiation messages.</p>  <p>The screenshot shows the Firebox System Manager interface with the Traffic Monitor tab selected. The log output includes the following messages:</p> <pre> 09/17/04 09:08 kernel: ipsec: Acquiring keys for channel 5 09/17/04 09:08 firewall[121]: allow out eth1 60 icmp 20 128 10.10.42.201 40.40.42.201 8 0 (Ping) 09/17/04 09:08iked[138]: Acquiring key for channel/policy 5/0 09/17/04 09:08iked[138]: Key acquire proxyaddr = 40.40.42.0 09/17/04 09:08iked[138]: Key acquire proxyladdr = 10.10.42.0 09/17/04 09:08iked[138]: ipsec_acquire_keys: laddr = 20.20.42.2, raddr = 30.30.42.2 09/17/04 09:08iked[138]: TO 30.30.42.2 MM-HDR ISA_SA ISA_VENDORID ISA_VENDORID ISA_VENDORID ISA_VENDORID 09/17/04 09:08iked[138]: FROM 30.30.42.2 MM-HDR ISA_SA 09/17/04 09:08iked[138]: TO 30.30.42.2 MM-HDR ISA_KE ISA_NONCE 09/17/04 09:08 firewall[121]: allow out eth1 60 icmp 20 128 10.10.42.201 40.40.42.201 8 0 (Ping) 09/17/04 09:08iked[138]: FROM 30.30.42.2 MM-HDR ISA_KE ISA_NONCE 09/17/04 09:08iked[138]: TO 30.30.42.2 MM-HDR* ISA_ID ISA_HASH 09/17/04 09:08iked[138]: FROM 30.30.42.2 MM-HDR* ISA_ID ISA_HASH ISA_NOTIFY 09/17/04 09:08iked[138]: Received INITIAL_CONTACT message, mess_id=0x00000000 09/17/04 09:08iked[138]: Phase 1 completed as initiator 09/17/04 09:08iked[138]: Getting IPSEC preferences as Initiator proppnum=1, mode=(Tunnel), laddr=20.20.42.2, raddr=30.30.42.2 09/17/04 09:08iked[138]: Getting IPSEC preferences as Initiator proppnum=2, mode=(Tunnel), laddr=20.20.42.2, raddr=30.30.42.2 09/17/04 09:08iked[138]: TO 30.30.42.2 QM-HDR* -3A219461 ISA_HASH ISA_SA ISA_NONCE ISA_ID ISA_ID 09/17/04 09:08iked[138]: FROM 30.30.42.2 QM-HDR* -3A219461 ISA_HASH ISA_SA ISA_NONCE ISA_ID ISA_ID 09/17/04 09:08iked[138]: Load outbound ESP SA, Algs=ESP_3DES/AUTH_ALG_HMAC_SHA1 Life=86400sec/0KB SPI=F53B003... 09/17/04 09:08iked[138]: Load inbound ESP SA, Algs=ESP_3DES/AUTH_ALG_HMAC_SHA1 Life=86400sec/0KB SPI=02049169 09/17/04 09:08iked[138]: Tunnel created for 10.10.42.0/24 <-> 40.40.42.0/24 09/17/04 09:08iked[138]: Committing SAs for channel=5 established with QM message_id=3A219461 09/17/04 09:08 kernel: ipsec: make bundle for channel 5, 1 in SA's, 1 out SA's 09/17/04 09:08iked[138]: TO 30.30.42.2 QM-HDR* -3A219461 ISA_HASH 09/17/04 09:08 firewall[121]: allow out eth1 60 icmp 20 128 10.10.42.201 40.40.42.201 8 0 (Ping) 09/17/04 09:08 firewall[121]: allow out eth1 60 icmp 20 128 10.10.42.201 40.40.42.201 8 0 (Ping) </pre>

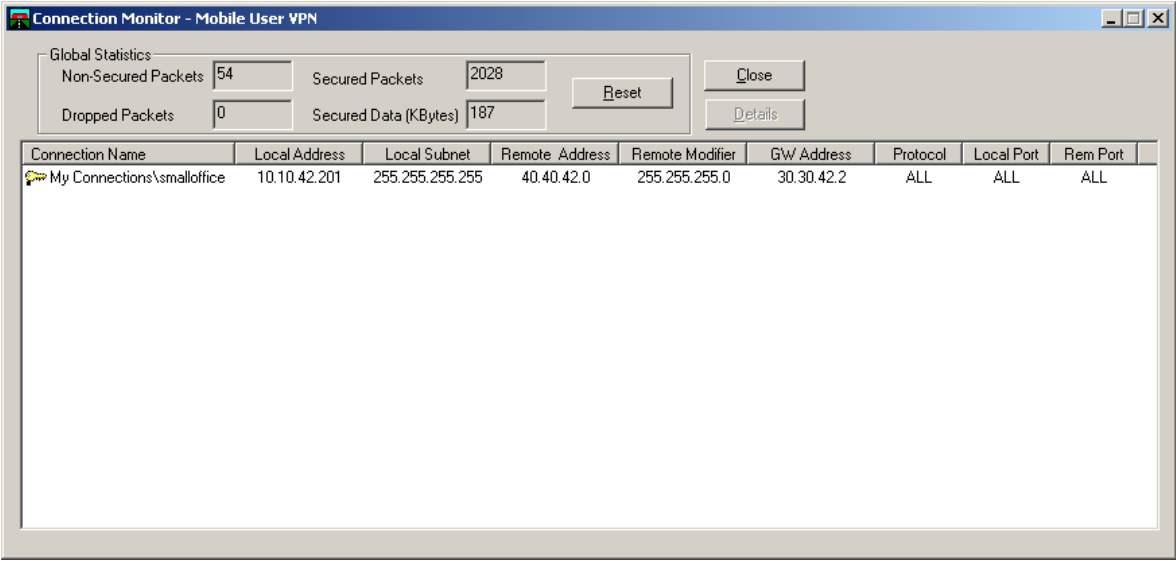
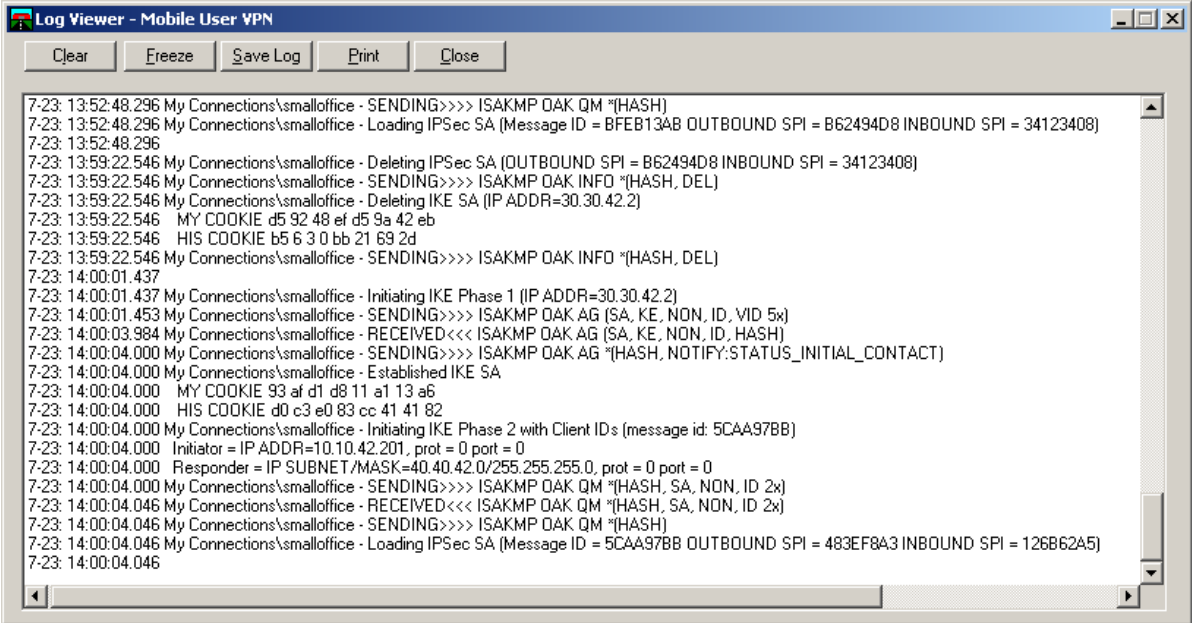
- Step** **Description**
- 4.** From the Firebox System Manager, select **Tools** → **Log Viewer** or click on the  taskbar icon to view the Phase 1 negotiation message history.

```

C:\Program Files\WatchGuard\logs\10.10.42.1-2004-09-15-14-14-33.wgl - LogViewer
File Edit View Help
[Icons]
Date Time Disp. I/F Proto. Source Destination S. Port D. Port Details
09/17/04 09:08:42 kernel ipsec: Acquiring keys for channel 5
09/17/04 09:08:42 allow eth1 icap 10.10.42.201 40.40.42.201 8 0 (Ping)
09/17/04 09:08:42iked[138] Acquiring key for channel/policy 5/0
09/17/04 09:08:42iked[138] Key acquire proxyraddr = 40.40.42.0
09/17/04 09:08:42iked[138] Key acquire proxyladdr = 10.10.42.0
09/17/04 09:08:42iked[138] ipsec_acquire_keys: laddr = 20.20.42.2, raddr = 30.30.42.2
09/17/04 09:08:42iked[138] TO 30.30.42.2 MM-HDR ISA_SA ISA_VENDORID ISA_VENDORID ISA_VENDORID ISA_VENDORID
09/17/04 09:08:42iked[138] FROM 30.30.42.2 MM-HDR ISA_SA
09/17/04 09:08:42iked[138] TO 30.30.42.2 MM-HDR ISA_KEY ISA_NONCE
09/17/04 09:08:43allow eth1 icap 10.10.42.201 40.40.42.201 8 0 (Ping)
09/17/04 09:08:43iked[138] FROM 30.30.42.2 MM-HDR ISA_KEY ISA_NONCE
09/17/04 09:08:43iked[138] TO 30.30.42.2 MM-HDR* ISA_ID ISA_HASH
09/17/04 09:08:45iked[138] FROM 30.30.42.2 MM-HDR* ISA_ID ISA_HASH ISA_NOTIFY
09/17/04 09:08:45iked[138] Received INITIAL_CONTACT message, mess_id=0x00000000
09/17/04 09:08:45iked[138] Phase 1 completed as initiator
09/17/04 09:08:45iked[138] Getting IPSEC preferences as Initiator propnum=1, mode=(Tunnel), laddr=20.20.42.2, raddr=
09/17/04 09:08:45iked[138] Getting IPSEC preferences as Initiator propnum=2, mode=(Tunnel), laddr=20.20.42.2, raddr=
09/17/04 09:08:45iked[138] TO 30.30.42.2 QM-HDR* -3A219461 ISA_HASH ISA_SA ISA_NONCE ISA_ID ISA_ID
09/17/04 09:08:45iked[138] FROM 30.30.42.2 QM-HDR* -3A219461 ISA_HASH ISA_SA ISA_NONCE ISA_ID ISA_ID
09/17/04 09:08:45iked[138] Load outbound ESP SA, Algs=ESP_3DES/AUTH_ALG_HMAC_SHA1 Life=86400sec/0KB SPI=F53B003D
09/17/04 09:08:45iked[138] Load inbound ESP SA, Algs=ESP_3DES/AUTH_ALG_HMAC_SHA1 Life=86400sec/0KB SPI=02049169
09/17/04 09:08:45iked[138] Tunnel created for 10.10.42.0/24 <-> 40.40.42.0/24
09/17/04 09:08:45iked[138] Committing SAs for channel=5 established with QM message_id=3A219461
09/17/04 09:08:45kernel ipsec: make bundle for channel 5, 1 in SA's, 1 out SA's
09/17/04 09:08:45iked[138] TO 30.30.42.2 QM-HDR* -3A219461 ISA_HASH
09/17/04 09:08:45allow eth1 icap 10.10.42.201 40.40.42.201 8 0 (Ping)
09/17/04 09:08:46allow eth1 icap 10.10.42.201 40.40.42.201 8 0 (Ping)
09/17/04 09:18:29firewalld[121] Putting file wg.cfg (from 10.10.42.201)
09/17/04 09:18:29firewalld[121] File synchronization completed
09/17/04 09:18:29firewalld[121] Property not restartable: debug.syslog.facility_log_localn
09/17/04 09:18:38firewalld[121] Rebooted by 10.10.42.201
09/17/04 09:18:41fwcheck[130] fwcheck: reboot request received, rebooting...
09/17/04 09:18:41fwcheck[130] Shutting down eth0
09/17/04 09:18:41fwcheck[130] Shutting down eth1
09/17/04 09:19:32installd[63] Watchguard Installer Daemon 7.21.B1596 (C) 1996-2004 WGTI
09/17/04 09:19:32installd[63] Performing loopback detect...
For Help, press F1 Total Lines: 15807 At entry: 15807 info file: /usr/sbin/...
Fri, 17 September 2004

```

Step	Description
5.	<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 VPN Statistics option on the left pane to view statistics for the site-to-site tunnel between the SOHO 6tc Wireless and Small Office Edition.</p> 

Step	Description																		
6.	<p>Navigate to Start → Programs → Mobile User VPN → Connection Monitor to view statistics for the client VPN tunnel to Small Office Edition.</p>  <table border="1" data-bbox="342 472 1469 520"> <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 Connections\smalloffice</td> <td>10.10.42.201</td> <td>255.255.255.255</td> <td>40.40.42.0</td> <td>255.255.255.0</td> <td>30.30.42.2</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 Connections\smalloffice	10.10.42.201	255.255.255.255	40.40.42.0	255.255.255.0	30.30.42.2	ALL	ALL	ALL
Connection Name	Local Address	Local Subnet	Remote Address	Remote Modifier	GW Address	Protocol	Local Port	Rem Port											
My Connections\smalloffice	10.10.42.201	255.255.255.255	40.40.42.0	255.255.255.0	30.30.42.2	ALL	ALL	ALL											
7.	<p>Navigate to Start → Programs → Mobile User VPN → Log Viewer to view Phase 1 and Phase 2 negotiation messages for the client VPN tunnel to Small Office Edition.</p>  <pre data-bbox="326 1129 1469 1606"> 7-23: 13:52:48.296 My Connections\smalloffice - SENDING>>> ISAKMP OAK QM *(HASH) 7-23: 13:52:48.296 My Connections\smalloffice - Loading IPSec SA (Message ID = BFE13AB OUTBOUND SPI = B62494D8 INBOUND SPI = 34123408) 7-23: 13:52:48.296 7-23: 13:59:22.546 My Connections\smalloffice - Deleting IPSec SA (OUTBOUND SPI = B62494D8 INBOUND SPI = 34123408) 7-23: 13:59:22.546 My Connections\smalloffice - SENDING>>> ISAKMP OAK INFO *(HASH, DEL) 7-23: 13:59:22.546 My Connections\smalloffice - Deleting IKE SA (IP ADDR=30.30.42.2) 7-23: 13:59:22.546 MY COOKIE d5 92 48 ef d5 9a 42 eb 7-23: 13:59:22.546 HIS COOKIE b5 6 3 0 bb 21 69 2d 7-23: 13:59:22.546 My Connections\smalloffice - SENDING>>> ISAKMP OAK INFO *(HASH, DEL) 7-23: 14:00:01.437 7-23: 14:00:01.437 My Connections\smalloffice - Initiating IKE Phase 1 (IP ADDR=30.30.42.2) 7-23: 14:00:01.453 My Connections\smalloffice - SENDING>>> ISAKMP OAK AG (SA, KE, NON, ID, VID 5x) 7-23: 14:00:03.984 My Connections\smalloffice - RECEIVED<<< ISAKMP OAK AG (SA, KE, NON, ID, HASH) 7-23: 14:00:04.000 My Connections\smalloffice - SENDING>>> ISAKMP OAK AG *(HASH, NOTIFY:STATUS_INITIAL_CONTACT) 7-23: 14:00:04.000 My Connections\smalloffice - Established IKE SA 7-23: 14:00:04.000 MY COOKIE 93 af d1 d8 11 a1 13 a6 7-23: 14:00:04.000 HIS COOKIE d0 c3 e0 83 cc 41 41 82 7-23: 14:00:04.000 My Connections\smalloffice - Initiating IKE Phase 2 with Client IDs (message id: 5CAA97BB) 7-23: 14:00:04.000 Initiator = IP ADDR=10.10.42.201, prot = 0 port = 0 7-23: 14:00:04.000 Responder = IP SUBNET/MASK=40.40.42.0/255.255.255.0, prot = 0 port = 0 7-23: 14:00:04.000 My Connections\smalloffice - SENDING>>> ISAKMP OAK QM *(HASH, SA, NON, ID 2x) 7-23: 14:00:04.046 My Connections\smalloffice - RECEIVED<<< ISAKMP OAK QM *(HASH, SA, NON, ID 2x) 7-23: 14:00:04.046 My Connections\smalloffice - SENDING>>> ISAKMP OAK QM *(HASH) 7-23: 14:00:04.046 My Connections\smalloffice - Loading IPSec SA (Message ID = 5CAA97BB OUTBOUND SPI = 483EF8A3 INBOUND SPI = 126B62A5) 7-23: 14:00:04.046 </pre>																		

7. Support

For technical support on WatchGuard, 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 and SOHO products as well as client VPN tunnels to IP Office 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 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.