

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	IKE Exchange	Encryption	Password	Diffie-Hellman	Encryption
Type	Type	Method	Authentication	Group	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 $\rightarrow$ P	Click Start $\rightarrow$ Programs $\rightarrow$ IP Office $\rightarrow$ PhoneManager to start the PhoneManager Pro				
	application. Click Configure $\rightarrow$ PBX and specify the LAN2 interface address for IP Office					
	(e.g., <b>30.30.42.2</b>	) in the <i>PBX Addr</i>	ess field. Select the nam	e defined on the <b>User</b> form in IP		
	Office Manager	(e.g., Extn60003)	in the UserName field.	Click the <b>Login</b> button and check		
	the Login/Logou	t checkbox. Selec	ct the extension (e.g., 600	<b>03</b> ) to be used by Phone Manager		
	in the Base Extern	nsion field.				
	PE	3X Configuration Info	rmation	×		
		Us	ser Details	ок		
		LiserName	Exto60003			
				Cancel		
		Password		Help		
	100	PBX Address	30.30.42.2	Login <<		
		1	_ogin/Logout			
		Dess Estantian	60003			
		Base Extension				

## 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 $\rightarrow$ Programs $\rightarrow$ WatchGuard $\rightarrow$ Firebox
	System Manager from the Firebox System Manager PC.
	👗 Firebox System Manager - 20.20.42.2 [Connected]
	Wg- II   画 当 時 通 Front Panel Tradio Monitor   Raveluidh Mater   Service Watch   Status Report   Artheorication   int   Rhoked Sites
	Status     Status
	Extensi Friedox Status
	Trusted Optional
	Detail Uo Time: 0 days 00:49:59
	Current Loghost 10.10.42.201 Allowed Packets: 0
	Deny Packets: 0 Authenticated Users: 0 Current Commontoring: 0
	Salast Tools -> Policy Managar or slick on the 🛐 taskhar ison
	Select <b>1001s -7 Foncy</b> Wanager of click of the was taskbar fcon.
2	Click on <b>Network -&gt; Remote User</b> to add a new MUVPN client for Phone Manager Pro
2.	ener on recourte ' remote eser to add a new trie virt enent for rhone manager rio.
	👼 C:\Program Files\WatchGuard\20.20.42.2.cfg - Policy Manager
	Eile Edit Setup Network Yiew Help
	Any Any-Smartbits FTP H323 Outgoing Ping WatchGuard
	For Help, press E1

Step	Description
3.	Select Firebox Authenticated Users and click Add.
3.	Select Firebox Authenticated Users and click Add.          Remote User Setup         Mobile User VPN         Mobile User VPN         Mobile User VPN         Use the 'Add', 'Edit', and 'Remove' buttons to configure the list of groups and users for Mobile User VPN.         You have enough client licenses for 999 more users.          Extended Authentication Groups
4.	Logging Regenerate       Advanced         OK       Cancel         Help         Click Next to use the Mobile User VPN Wizard to configure the VPN tunnel for the MUVPN client.
	Mobile User VPN Wizard - Firebox Authenticated User
	MOBILE USER CONFIGURATION INTERCENT OF CONFIGURATION INTERCENT OF CONFIGURATION INTERCENT INTERCENT OF CONFIGURATION INTERCENT INTERC

Step	Description
5.	Click Add New to add a new mobile user VPN account.
	Mobile User VPN Wizard
	MOBILE USER
	CONFIGURATION       Please select a user from the list to create a new Mobile User VPN account or click Add New to add a new Firebox user to the Mobile User VPN group.         Select User Name:       Add New         Select User Name:       Add New         Enter a shared key for this user. This key will be used to negotiate the encryption and/or authentication keys for the IPSec tunnel.         Enter Shared Key:       Confirm:         User is connecting with a Pocket PC Click the "Next" button to continue.
	< <u>B</u> ack <u>N</u> ext > Cancel Help
6.	Enter the <i>User Name</i> and <i>Passphrase</i> to be used by the MUVPN client as the shared key for Phase 1 authentication. This user will be automatically added to the ipsec_users group. Click <b>OK</b> .
	Setup New User
	Enter a user name and passphrase, and click   OK to create a new user account.   User Name:   PhoneManager   Cancel     Passphrase:   ************************************

Step	Description					
7.	Click Next to continue. The Ente	r Shared Key and Confirm fields have been populated with				
	the passphrase entered in the previous step.					
	Mobile User VPN Wizard					
	User Name and Passnbrase					
	MOBILE USER					
	CONFIGURATION 1 0100110101100 100110101100 100110 100110 100110 100110 100110 100110 100110 100110 100110 100110 100100	Please select a user from the list to create a new Mobile User         VPN account or click Add New to add a new Firebox user to the Mobile User VPN group.         Select User Name:       PhoneManager         Enter a shared key for this user. This key will be used to negotiate the encryption and/or authentication keys for the IPSec tunnel.         Enter Shared Key:				
		< <u>B</u> ack <u>N</u> ext > Cancel Help				
8.	Select the option to Use the pass pre-shared key. Click Next.	ohrase of the end-user profile (the .wgx or .exp file) as the				
		IDCas Turnel Authentication Mathed				
	<b>MOBILE USER</b> <b>CONFIGURATION</b> 1 010011000 100011010 100011010 1001100 100110 010001 001001 001001	Specify the authentication method you want to use to negotiate the encryption and/or authentication keys for the IPSec tunnel.  Use the passphrase of the end-user profile (the .wgx or exp file) as the pre-shared key.  Use a certificate (BSA Signature) that will be issued by				
	WatchGuard Firebox	Click the "Next" button to continue.				

Step	Description
9.	Click Add to specify the network that the MUVPN client will be allowed to access.
	Mobile User VPN Wizard
	MOBILE USER       Allowed Resources and Virtual IP Address         CONFIGURATION       Specify the network resources to allow for this firebox authenticated user.
	010001       010001       010001       010001       Add         Allowed Resources:       Add       Removed         WetchGuard       Virtual IP address for mobile user:       • • • •         Click the "Next" button to continue.       Cancel       Help
10.	Select <b>Network</b> in the <b>Allow access to</b> drop down list and specify the network for the LAN2 interface of the Small Office Edition. Click <b>OK</b> .
	Advanced Mobile User VPN Policy Configuration
	Specify the host or network and port/protocol/client OK port combination you wish to allow access via Mobile User VPN. Cancel
	Allow access to: Network 💌 30.30.42.0 /24
	Dst Port: 0 Protocol: *  Src Port: 0

Step	Description			
11.	Enter a virtual IP address (e.g., <b>30.30.42.100</b> ) for the MUVPN client. Click Next.			
	Mobile User VPN Wizard			
	MOBILE USER Allowed Resources and Virtual IP Address			
	CONFIGURATION Specify the network resources to allow for this firebox authenticated user.			
	010001 100110 01001 001000 00000 000000			
	WatchGuard Virtual IP address for mobile user: 30.30.42.100			
	Click the "Next" button to continue.			
	< <u>B</u> ack <u>N</u> ext > Cancel Help			
12.	<ul> <li>Enter the values shown below for Phase 2 from Table 1. Phase 2 re-authentication is set to occur every hour. Click Next.</li> <li>Authentication – The password authentication used by the tunnel</li> </ul>			
	<ul> <li>Encryption – The encryption method used by the tunnel.</li> </ul>			
	Mobile User VPN Wizard			
	Tunnel Protection Configuration			
	<b>CONFIGURATION</b> Specify the type of encryption and/or authentication for this mobile user's connections.			
	100110101 100011100 010001 011000 Ive: ESP (Encryption and/or Authentication)			
	Authentication: SHA1-HMAC			
	Key expires:     every     iobytes or       WatchGuard     Image: every     Image: every			
	Firebox:			
	< <u>B</u> ack <u>N</u> ext > Cancel Help			

	Description	Bich
Click <b>Finish</b> to complete the mobile user VPN configuration and return to the "Remote User Setup" window. This will result in the creation of a file with a .wgx extension which can be used to update the security policy of the MUVPN client. The WatchGuard Policy Import utility is covered in more detail in Section 4.3.		
1	Mobile User VPN Wizard	
	Finish Mobile User VPN Configuration	
	Congratulations, you have completed the configuration for this mobile user. If you want to review any settings, use the 'Back' and 'Next' buttons. Click the 'Finish' button to complete the configuration.	
	Click the "Finish" button to continue.	
	< <u>B</u> ack Finish Cancel Help	
	Mobile User VPN Wizard       Image: Configuration of this mobile user. If you want to review any settings, use the 'Back' and 'Next' buttons. Click the 'Finish' button to complete the configuration.         Image: Configuration of this mobile user. If you want to review any settings, use the 'Back' and 'Next' buttons. Click the 'Finish' button to complete the configuration.         Image: Configuration of this mobile user. If you want to review any settings, use the 'Back' and 'Next' buttons. Click the 'Finish' button to complete the configuration.         Image: Configuration of this mobile user. If you want to review any settings, use the 'Back' and 'Next' buttons. Click the 'Finish' button to complete the configuration.         Image: Configuration of this mobile user. If you want to review any settings, use the 'Back' and 'Next' buttons. Click the 'Finish' button to complete the configuration.         Image: Configuration of this mobile user. If you want to review any settings, use the 'Back' and 'Next' buttons. Click the 'Finish' button to complete the configuration.         Image: Configuration of this mobile user. If you want to review any settings, use the 'Back' and 'Next' buttons.         Image: Configuration of this mobile user. If you want to review any settings, use the 'Back' and 'Next' button' button to complete the configuration.         Image: Configuration of this mobile user. If you want to review any settings, use the 'Back' and 'Next' button' button to continue.         Image: Configuration of this mobile user. If you want to review any settings, use the 'Back' and 'Next' button'	

Step	Description
14.	If desired, click Logging from the "Remote User Setup" window to enable IPSec logging
	for debugging purposes.
	Remote User Setup
	Mobile User VPN Mobile User Licenses PPTP
	Use the 'Add', 'Edit', and 'Remove' buttons to configure the list of groups and users for Mobile User VPN.
	You have enough client licenses for 999 more users.
	Extended Authentication Groups
	Breson Authenticated Users     Edit Edit Edit Edit
	⊡- IPSec settings
	Key Negotiation Type: sharedkey
	- Auth: SHA1-HMAC
	Key Exp: 3600 sec
	Logging Regenerate Advanced
15.	If logging was selected, check the options shown below to include the configuration output and extra IKE debugging in the log and click <b>OK</b> to return to the "Permote User Setup" window
	extra IKE debugging in the log and enex <b>OK</b> to return to the "Remote Oser Setup" window.
	IPSec Logging
	Logging options for IPSec include
	configuration output, extra IKE debugging.
	and IKE packet tracing.
	Enable configuration dump after IKE interpretation.
	Enable extra IKE debugging.
	Enable IKE packet tracing (Note: This option can be used by WatchGuard Support to help debug problems.)
	Enable certificate validation debugging

Step	Description				
16.	Click <b>Advanced</b> from the "Remote User Setup" window and select <b>Preferred</b> for the <i>Virtual Adapter Settings of the Secure VPN Client</i> . Click <b>OK</b> to return to Remote User Setuc Click <b>OK</b> to return to Policy Manager.				
	Advanced Export File Preferences				
	Use the settings below to specify how the MUVPN Client interacts with the mobile user's computer. These settings (which affect only *.wgx export files) will take place when you create or regenerate the export files. Make the security policy read-only in the MUVPN Client. Virtual Adapter Settings of the Secure VPN Client: Preferred				

### 4.2. Configure the WatchGuard SOHO 6tc Wireless

Step	Description	
1.	Open the SOHO 6 Configuration screen by specifying the IP address of the priv	ate interface of
	the SOHO 6tc Wireless in a browser window. Click the MUVPN Clients optic	on on the left
	pane and click Add to add a MUVPN tunnel to the SOHO.	
	- A Mathematics Cathless - Miness (Markess & Frederic	
	Elle Edit View Favorites Iools Help	
	↓ Back + → - ③ ② ঐ 🖄 ◎ Search 🔊 Favorites ᢀ Media 🔇 🖏 - 🎒	
	Address 🕘 http://30.30.42.1/vpnsvr.htm	▼ 🖉 Go Links ≫
		<u> </u>
	WatchGuard SOHO 6 Configuration LiveSecurity   Help   Support   About Us   Contact Us	
	System Status VPN	
	External MUVPN Clients	
	Provided (202.11b)	
	Routes	
	DynamicDNS Dependenager 30.30.42.100	
	System Security	
	View Configuration File	
	Incoming	
	Custom Service	
	Firewall Options	
	Logging Add Edit Remove	
	Systog Logging	
	System Time WebBlocker	
	VPN Managed VPN	
	Manual VPN MUVPN Clients	
	VPN Statistics VPN Keep Alive	
		-
		🥶 Internet

Step	Description
2.	Enter the values shown below for Phase 2 from <b>Table 1</b> .
	<ul> <li>User Name – The name of the MUVPN client</li> <li>Shared Key – The password used for authentication and must match on the device at the other end of the tunnel.</li> <li>Virtual IP Address – The virtual IP address assigned to the MUVPN client.</li> <li>Authentication Algorithm – The password authentication used by the tunnel.</li> <li>Encryption Algorithm – The encryption method used by the tunnel.</li> <li>VPN Client Type – Mobile User (MUVPN client)</li> </ul>
	🖉 WatchGuard Configuration Settings - Microsoft Internet Explorer
	Elle Edit View Favorites Iools Help
	Address Chttp://30.30.42.1/cfgnuvpn.htm?user=PhoneManager
	System Status       VPN > MUVPN Clients         External       Configuration         Unstand (802.11b)       VPN > MUVPN Clients
	Routes       User Name       PhoneManager         Network Statistics       User Name       PhoneManager         DynamicDNS       Shared Key       secret123         System Security       Virtual IP Address       30.30.42.100         Vpgrade       Authentication Algorithm       SHA1-HMAC V         View Configuration File       Encryption Algorithm       3DES-CBC V         Firewall       VPN Client Type       Mobile User V
	Ougoing     WINS Server       Blocked Sites     DNS Server       Pass Through     All traffic uses tunnel (0.0.0.0/0 IP Subnet)       Logging     NOTE: DNS and WINS settings are common to all MUVPN users       Syslog Logging     NOTE: DNS and WINS settings are common to all MUVPN users       System Time     Submit       WebBlocker     Submit       VPN     Managed VPN       Managed VPN     MUVPN Clients       VPN Keep Allve     VPN Keep Allve
	Done
	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 <b>OK</b> to import the security policy.
	used in step 7 of section 4.1. Click <b>OK</b> to import the security policy.
	WatchGuard Policy Import
	Welcome to the WatchGuard Policy Import utility. This will assist you in configuring your Mobile User client.
	File To Import: ager\PhoneManager.wgx Browse
	Shared Key: ******
2.	The following pop-up window appears after importing the security policy. Click <b>OK</b> to exit
	the import utility.
	WatchGuard Policy Import
	Concertedetional
	You have successfully configured your Mobile User client. You can begin safely compunicating through your typpel immediately.
	sarely commanicating through your tarine immediately.
	<u>[UK</u>



Step	Description
4.	Expand the new connection by clicking on the "+" next to the connection name and click <b>My</b>
	<b>Enter Key</b> to supply the same password specified in the Firebox X or SOHO tunnel configuration. Select <b>E-mail Address</b> for the <i>ID Type</i> , and enter the Name of the MUVPN
	client (e.g., <b>PhoneManager</b> ) in the subsequent field. Select <b>Preferred</b> in the Virtual Adapter
	drop-down list and leave the other fields as default.
	E Security Policy Editor - Mobile User VPN
	Elle Edit Options Help
	Network Security Policy     Image: Security Policy </th

Step	Description	
5.	Click Security Policy. Aggressive Mod	le was selected for the Select Phase 1 Negotiation
	Mode and leave the other fields as defaul	ts.
	🚘 Security Policy Editor - Mobile User ¥PN	
	<u>File Edit Options Help</u>	
		1012
		WatchGuard -
	Network Security Policy	
	□ ···· · · · · · · · · · · · · · · · ·	
	G My Identity	Select Phase 1 Negotiation Mode
	🖨 😓 Security Policy	O Main Mode
	🕀 🗐 Authentication (Phase 1)	Aggressive Mode
		🔿 Use Manual Keys
	Other Connections	
		Exclusion Francisco (PEC)
		Enable Perfect Forward Secrecy (PFS)
		PFS Key Group Diffie-Hellman Group 1
		Enable Replay Detection
	,	

Step	Description	
6.	Expand Security Policy and Authentica	tion (Phase1). Click Proposal 1. The values shown
	below are the defaults used for Phase 1 n	egotiation.
	Security Policy Editor - Mobile Liser VPN	
	File Edit Options Help	
		WatchGuard -
	Network Security Policy	
	□ □ ··· □ My Connections	
	G My Identity	Authentication Method and Algorithms
	🖻 👼 Security Policy	Authentication <u>M</u> ethod
	□··= Authentication (Phase 1)	Pre-Shared Key
	🕀 🏀 Key Exchange (Phase 2)	- Execution and Data InterviewAlgorithms
		Encryption and Data Integrity Algorithms
		Encrypt Alg DES
		Hash Alg
		Seconds
		SA Life Unspecified 🔻
		Keu Group Diffie Hellman Group 1

Step	Description
7.	Expand Key Exchange (Phase2). Click Proposal 1 and enter the values shown below to
7.	Expand Key Exchange (Phase2). Click Proposal I and enter the values shown below to match the Firebox X and the SOHO tunnel configuration for Phase 2.
	Network Security Policy
δ.	Click File $\rightarrow$ Save or the floppy disk icon $\blacksquare$ 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
2.	Click on the <b>Traffic Monitor</b> tab to view Phase 1 negotiation messages.
	👗 Firebox System Manager - 20.20.42.2 [Connected]
	隆 - 11 🖓 🗎 🐜 🔟
	Front Panel Traffic Monitor Bandwidth Meter Service Watch Status Report Authentication List Blocked Sites
	10/11/04 1940 iked[138]       FRID 10.104.2201       THADR = 81193E50 ISA_HASH ISA_TRANSATTR         10/11/04 1940 iked[138]       Processing configuration acknowledge       10/11/04 1940 iked[138]       Fronce set INTERNAL_IP4_ADDRESS         10/11/04 1940 iked[138]       Remote set INTERNAL_P4_DNS       ISA       ISA       ISA         10/11/04 1940 iked[138]       Remote set INTERNAL_P4_DNS       ISA       ISA       ISA         10/11/04 1940 iked[138]       Remote set INTERNAL_P4_DNS       ISA       ISA       ISA         10/11/04 1940 iked[138]       Key acquire proxyaddr = 30.30.42.0       ISA       ISA       ISA       ISA         10/11/04 1940 iked[138]       Key acquire proxyaddr = 30.30.42.0       ISA       ISA <t< th=""></t<>
3.	From the Firebox System Manager select <b>Tools</b> $\rightarrow$ Log Viewer or click on the $[3]$ taskbar icon
	to view the Phase 1 negotiation message history
	to view the r hase r hegotiation message instory.
	🖹 C:\Program Files\WatchGuard\logs\20.20.42.2-2004-07-18-23-17-35.wgl - LogYiewer
	Ele Edit View Help
	Date     Disp. 1/F     Froto.     Source     Destination     S. Fort     D. Fort     Details       10/11/04     19:40:04     iked[138]     FROM     10.10.42.201     TR-HDR* -B1193E50     ISA_HASH     ISA_TRANSATTR
	10/11/04 19:40:04 iked[138] Processing configuration acknowledge
	10/11/04 19:40:04 iked[138] Remote set INTERNAL_IF4_ADDRESS 10/11/04 19:40:04 iked[138] Remote set INTERNAL_IF4_NETMASK
	10/11/04 19:40:04 iked[138] Remote set INTERNAL_IP4_DNS
	10/11/04 19:40:04 iked[138] Key acquire proxyradar = 30.30.42.100 10/11/04 19:40:04 iked[138] Key acquire proxyladdr = 30.30.42.0
	10/11/04 19:40:04 iked[138] ipsec_acquire_keys: laddr = 20.20.42.2, raddr = 10.10.42.201
	10/11/04 19:40:04 iked[138] Getting IPSEC preferences as Initiator propum=1, mode=(Tunnel), laddr=20.20.42.2, raddr=1
	10/11/04 19:40:04 iked[136] Getting irssc preferences as intractor proprim=2, mode-(lumer), iddr-20.20.42.2, raddr-1 10/11/04 19:40:04 iked[138] TO 10.10.42.201 OM-HDR* -Ala253BE ISA HASH ISA SA ISAS NONCE ISA ID ISA ID
	10/11/04 19:40:04 iked[138] FROM 10.10.42.201 QM-HDR* -8818D920 ISA_HASH ISA_SA ISA_NONCE ISA_ID ISA_ID
	10/11/04 19:40:04 iked[138] Getting IPSEC preferences as Responder propnum=1, mode=(Tunnel), laddr=20.20.42.2, raddr=1
	10/1/04 19:40:04 iked[130] 10 10:10:42:201 (0H=DK# -86160920 ISA_HASH ISA_SA ISA_NONCE ISA_ID ISA_ID 10/11/04 19:40:04 iked[138] FROM 10:10:42:201 (0H=DK# -41425388 ISA HASH ISA SA ISA NONCE ISA ID ISA ID
	10/11/04 19:40:04 iked[138] Load outbound ESP SA, Algs=ESP_3DES/AUTH_ALG_HMAC_SHA1 Life=3600sec/0KB SPI=1771C855
	10/11/04 19:40:04 iked[138] Lad inbound ESP SA, Algs=ESP_3DES/AUTH_ALG_HMAC_SHA1 Life=3600sec/0KB SPI=04046F31
	10/11/04 19:40:04 iked[138] Tunnel created for 30.30.42.0/24 <-> 30.30.42.100/32
	10/11/04 19:40:04 kernel ipsec: make bundle for channel 0.1 in SA's.1 out SA's
	10/11/04 19:40:04 iked[138] TO 10.10.42.201 QM-HDR* -A1A253BB ISA_HASH
	Log file is loaded. Total Lines: 19915 At entry 19850: 99% into file.

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.
	🖉 WatchGuard Configuration Settings - Microsoft Internet Explorer
	Elle Edit View Favorites Iools Help
	Address 🙆 http://30.30.42.1/vpnstat.htm
	SOHO 6 Configuration LiveSecurity   Help   Support   About Us   Contact Us
	System Status VPN Network Statistics
	External Oraciations
	Uptional (802:116) Wireless Configuration Poutoc
	Notwork Statistics DynamicDNS BUNDLE (0) (Tunnel) refcnt = 2
	Administration 20.20.42.2(7efb0401)(ESP): (Mature) refcnt(1)SRC:10.10.42.201 PR0XY:10.10.42.201 System Security AUTH: SHA1-HMAC Authentication
	VPN Manager Access CFYPT: 3DES-CEC Encryption Update Create Time: 00000000000025b First Use: 000000000000274
	Upgrade Bytes: 000000002401a0 Packets: 000008ec4 View Configuration File Soft Timeouts: Bytes: 000766ff Use Time: 0000149d3
	Firewall BUNDLE (0) (Tunnel) refort = 1
	Outgoing AUTH: SHAI-HMAC Authentication CUVPT: 3DES_CEC Forewrition
	Blocked Sites Create Time: 00000000000025b First Use: 000000000000274 Firewall Options Bytes: 000000000000081378 Packets: 0001a0f9
	Pass Inrough Soft Timeouts: Bytes: 0007ael47 Use Time: 0000138f3
	System Time
	System mine WebBlocker V/DN
	Managed VPN Manual VPN
	MUVPN Clients
	VPN Keep Alive
	C Internet
_	
5.	On the Phone Manager Pro PC, navigate to Start $\rightarrow$ Programs $\rightarrow$ Mobile User VPN $\rightarrow$
	<b>Connection Monitor</b> to view statistics for the client VPN tunnel to the Firebox X or SOHO
	device.
	Connection Monitor - Mobile User VPN
	Global Statistics
	Non-Secured Packets Secured Packets Education Secured Packets
	Dropped Packets U Secured Data (KBytes) 1
	Connection Name Local Address Local Subnet Remote Address Remote Modifier GW Address Protocol Local Port Rem Port
	Com <sup>®</sup> My Connection 30.30.42.100 233.233.233.233 30.30.42.0 233.233.233.0 20.20.42.2 ALL ALL ALL ALL

Step	Description
6.	On the Phone Manager Pro PC, navigate to Start $\rightarrow$ Programs $\rightarrow$ Mobile User VPN $\rightarrow$ Log
	<b>Viewer</b> to view Phase 1 and Phase 2 negotiation messages for the client VPN tunnel to Firebox
	X or SOHO device.
	Tog Viewer - Mobile User VPN
	Liear <u>Freeze Save Log Finnt</u> Liose
	10-11: 19:40:05:312 My Connections/20:20:42:30:30:42:0 - SENDING>>>> ISAKIP DaK AG (SA, KE, NDN, ID, VID 5x) 10-11: 19:40:05:343 My Connections/20:20:42:30:30:42:0 - RECEIVED<<< ISAKIMP DAK AG (SA, KE, NDN, ID, HASH, VID 2x, NAT-D 2x) 10-11: 19:40:05:343 My Connections/20:20:42:30:30:42:0 - RECEIVED<<< ISAKIMP DAK AG (SA, KE, NDN, ID, HASH, VID 2x, NAT-D 2x)
	10-11: 19:40:05:343 My Connections/20:20:42:2:30:30:42:0: SENDING>>>> ISAK MP DAK AG "(HASH, NOTIFY:STATUS_INITIAL_CONTACTNAT-D 2x) 10-11: 19:40:05:343 My Connections/20:20:42:2:30:30:42:0: Established IKE SA
	10-11: 19:40:05:343 MY COOKIE 9a fa a9 7b c7 1d af 1f 10-11: 19:40:05:343 HIS COOKIE c3:42:31f c6 fe 7 6e 10:11: 19:40:05:343 HIS COOKIE c3:42:31f c6 fe 7 6e
	10-11: 13:40:05.343 M/ Commections 20:20:42:2-30:30:42:0-1 initiating intel Phase 2 with Lifent IDs (message to: 6CD (FBA1) 10-11: 13:40:05.343 Initiator = IP ADDR=10.10.42:201, prot = 0 port = 0 10-11: 19:40:05.343 Responder = IP SUBNET /MASK=30:30:42:0/255.255:255:0 prot = 0 port = 0
	10-11: 19:40:05.343 My Connections\20.20.42.2:30.30.42.0 - SENDING>>>> ISAKMP DAK QM "(HASH, SA, NON, ID 2x) 10-11: 19:40:05.343 My Connections\20.20.42.2:30.30.42.0 - RECEIVED<<< ISAKMP DAK TRANS "(HASH, ATTR)
	10-11: 19:40:05:343 My Connections/20:20:42:30:30:42:0 - Received DIS Address = IP ADDR=1.1.1 10-11: 19:40:05:343 My Connections/20:20:42:30:30:42:0 - Received Private IP Address = IP ADDR=30:30:42:100 10:11: 19:40:05:243 My Connections/20:20:42:30:30:42:0 - Received Private IP Address = IP ADDR=30:30:42:100
	10-11: 13:40:05:718 Virtual Interface constructed for local interface 30:30:42:100 10-11: 13:40:05:718 Virtual Interface eaded: 30:30:42:100 10-11: 19:40:05:734 Virtual Interface eaded: 30:30:42:100/25:0.0.0 on ISDN 'SafeNet VA miniport'.
	10-11: 19:40:05.734 My Connections\20.20.42.2-30.30.42.0 - Received Private DNS Address = IP ADDR=1.1.1.1 10-11: 19:40:05.734 My Connections\20.20.42.2-30.30.42.0 - SENDING>>>> ISAKMP DAK TRANS *(HASH, ATTR)
	10-11: 13:40:05.750 My Connections'20.20.42.2-30.30.42.0 - Initiating IKE Phase 2 with Lilent IDs (message id: 88180/920) 10-11: 13:40:05.750 Initiator = IP ADDR=30.30.42:100, prot = 0 port = 0 10-11: 19:40:05.750 Decementary - IDS INITE VMACK-30:30.42.02/65.255:0 prot = 0 port = 0
_	
7.	Using the IP Office SysMonitor log, confirm Phone Manager Pro registration.
	📜 SysMonitor v4.1 (15) - [STOPPED] monitoring 40.40.42.1 (00E0070149D5)
	Ele Edit View Filters Status Help
	→         ▲         ×         ▶         ■         ×         ■           42102mS         Page=14W2         Syn=30         30         42         211719         mah=0         ■
	RasMessage = gatekeeperRequest
	42104mS PRN: Recv: GatekeeperRequest 42106mS RasTx: v=Src=30.30.42.2:1719, Dst=30.30.42.100:1599 peb=0
	RasMessage = gatekeeperConfirm
	42128mS CMExtnRxP: v=0 CHShortCode
	Line: type=NoLine 0 Call: lid=0 id=-1 in=0 ShortCode GetSystemInfo (99) = []
	BC: CMTC=Speech CMTM=Circuit CMTR=64 CMST=Default CMU1=ULaw 42129mS CMExtnTxP: v=0
	CMShortCode Line: type=IPLine 250 Call: lid=0 id=-1 in=0
	ShortCode GetSystemInfo (99) = [2.1 (15)] Calling[00E0070149D5] Type=Default (100) Display [IP 401 NG]
	Tag type=Text [1,0,0,0,0,1.] [0x31 0x2c 0x30 0x2c 0x30 0x2c 0x30 0x2c 0x30 0x2c 0x31 0x00 ] Timed: 11/10/04 20:03
	42130mS PRN: TFTPServer::RRQ(from 30.30.42.100) nasystem/hunt_list 42131mS RasRx: v=IFace=LAN2, Src=30.30.42.100:1599, Dst=30.30.42.2:1719 peb=0
	RasMessage = registrationRequest
	42133mS FRN: Recv: RegistrationRequest reply addr lele2a64 42135mS FRN: GK: Adding new endpoint 00E0070149D5_416ae71a25ca1095
	42135mS CHExtnkx: v=60003, p1=0 CMPhoneStatus
	Line: type=NoLine 0 Call: lid=252 id=0 in=0 Cause=16, Normal call clearing
	42136mS CMExtnCopyProcessMsg: v=0 CMPhoneStatus
	Line: type=NoLine 0 Call: lid=252 id=0 in=0 Cause=16, Normal call clearing
	42136mS FKN: User Extn60003, lele2a64 allowed, bchan 0.0, EI 00E0070149D5_416ae71a25ca1095 42136mS FKN: Using 1.0.1 (OpenH323 v1.12.10)
	42130mS RASIX: V=Src=30.30.42.2:1719, Dst=30.30.42.100:1599 peb=0 RasMessage = registrationConfirm

## 6. Support

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

# 7. Conclusion

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

# 8. References

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

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

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by  $\mathbb{B}$  and  $^{TM}$  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.