

Avaya Solution & Interoperability Test Lab

# Configuring the NETGEAR FVX538 ProSafe VPN Firewall as an IPSec VPN Head-end to Support the Avaya VPNremote Phone and Avaya Phone Manager Pro with Avaya IP Office – Issue 1.0

## Abstract

These Application Notes describe the steps for configuring the NETGEAR FVX538 ProSafe VPN Firewall for Avaya IP Office to support Avaya VPNremote Phone and Phone Manager Pro. This solution can be used for a remote worker who wants to use a multi-button telephone and have the same functionality as a local telephone co-located with the IP Office. The sample configuration presented in these Application Notes utilizes a policy-based IPSec VPN and XAuth enhanced authentication. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab and at the request of the Solutions Marketing Team.

### **Table of Contents**

1. In	troduction	. 3
1.1.	Avaya VPNremote Phone for remote IP Office users	. 3
1.2.	Avaya Phone Manager Pro (in Telecommuter mode)	. 3
1.3.	NETGEAR FVX538 ProSafe VPN Firewall	. 4
2. N	etwork Topology	. 5
3. E	quipment and Software Validated	. 7
4. IF	P Office Configuration	. 7
5. N	ETGEAR FVX538 Configuration	18
5.1.	VPN	18
5.2.	Access NETGEAR FVX538	19
5.3.	Configure NETGEAR FVX538 Ethernet Interfaces	19
5.4.	Mode Config Record	20
5.5.	IKE Policy	22
5.6.	Xauth User	24
5.7.	VPN Policy	24
6. A	vaya VPNremote Phone Configuration	28
6.1.	Avaya VPNremote Phone Firmware	28
6.2.	Configuring Avaya VPNremote Phone	28
7. N	ETGEAR ProSafe VPN Client Configuration	32
8. P	hone Manager Pro Configuration	36
9. V	erification	38
9.1.	VPNremote Phone VPN Status	38
9.2.	NETGEAR FVX538 Debug and Logging	39
9.3.	NETGEAR ProSafe VPN Client Debug and Logging	42
10.	Testing	43
11.	Troubleshooting	44
11.1	. Incorrect User Name or Password	44
11.2	. Mismatched Phase 1 Proposal	45
11.3	. Mismatched Phase 2 Proposal	46
12.	Conclusion	<b>48</b>
13.	Definitions and Abbreviations	<b>49</b>
14.	References	49

## 1. Introduction

These Application Notes describe the steps for configuring the NETGEAR FVX538 ProSafe VPN Firewall for Avaya IP Office to support Avaya VPNremote Phone and Phone Manager Pro. Steps for configuring the NETGEAR FVX538 ProSafe VPN Firewall with a policy-based IPSec VPN and XAuth enhanced authentication to support the Avaya VPNremote Phone and Phone Manager Pro are described in this document.

The solution described in these Application Notes is an integral part of the Unified Communications – Small Business Edition, which provides a remote worker the same functionality as a local worker telephone co-located with the IP Office. The solution specific components are:

- Avaya VPNremote Phone for remote IP Office user
- Avaya Phone Manager Pro (in telecommuter mode)
- NETGEAR FVX538 ProSafe VPN Firewall
- NETGEAR ProSafe VPN Client

### **1.1. Avaya VPNremote Phone for remote IP Office users**

The Avaya VPNremote Phone is a software based IPSec Virtual Private Network (VPN) client integrated into the firmware of an Avaya 4600 or 5600 Series IP Telephone. This capability allows the Avaya IP Telephone to be plugged in and used over a secure IPSec VPN from any broadband Internet connection. End users experience the same IP telephony features as if they were using the telephone in the office.

Avaya IP Office 500 supports Avaya IP Telephone models 4610SW, 5610SW, 4620SW, 5620SW, 4621SW and 5621SW with Avaya VPNremote Phone firmware. Any of the above mentioned Avaya IP Telephones can be converted to an Avaya VPNremote Phone, as described in [1], and [2]. For a VPN solution, the IP Office VPN Phone license is required along with the Avaya VPNremote Phone firmware.

### **1.2.** Avaya Phone Manager Pro (in Telecommuter mode)

In this mode, a user running Phone Manager Pro on a PC with a data connection to the IP Office, (via VPN), is able to have calls routed to a telephone number specified when starting Phone Manager. When the user makes a call using Phone Manager, IP Office will call the user's specified telephone number and, when answered, make the outgoing call for the user. Similarly, incoming calls to the user's extension on IP Office are routed to the remote number. The Hot Desk feature of IP Office will be used with Phone Manager Pro. The Phone Manager Pro user will have an internal IP Office extension with a hard phone. While the user is logged in to Phone Manager as a telecommuter, the physical phone is logged off.

The NETGEAR ProSafe VPN client is used by the remote user to securely connect to the corporate IP network for telephony and data access.

## 1.3. NETGEAR FVX538 ProSafe VPN Firewall

The sample network provided in these Application Notes implements the following features of the NETGEAR FVX538:

• Policy-Based IPSec VPN

The policy-based VPN feature of the NETGEAR FVX538 allows a VPN Tunnel to be directly associated with a security policy as opposed to a route-based VPN being bound to a logical VPN Tunnel interface. Since no network exists beyond a VPN client endpoint, policy-based VPN tunnels are a good choice for VPN end-point configurations, such as the Avaya VPN remote Phone and NETGEAR ProSafe VPN Client.

### • XAuth User Authentication

The XAuth protocol enables the NETGEAR FVX538 to authenticate the individual users of the VPNremote Phone. The NETGEAR ProSafe VPN Client was configured to use pre-shared key and not XAuth user authentication. The XAuth user authentication is in addition to the IKE IPSec VPN authentication. The IKE and XAuth authentication steps are as follows:

- **Step 1. Phase 1 negotiations:** the NETGEAR FVX538 authenticates the Avaya VPNremote Phone by matching the IKE ID and pre-shared key sent by the Avaya VPNremote Phone. If there is a match, the NETGEAR FVX538 XAuth process begins.
- **Step 2.** XAuth: the NETGEAR FVX538 XAuth server prompts the Avaya VPNremote Phone for user credentials (username and password).
- **Step 3. Phase 2 negotiations:** Once the XAuth user authentication is successful, Phase 2 negotiations begin.

### • XAuth Dynamic IP Address Assignment

The XAuth protocol enables the NETGEAR FVX538 appliance to dynamically assign IP addresses from a configured IP Address pool range.

# 2. Network Topology

The sample network implemented for these Application Notes is shown in **Figure 1**. The corporate IP network location contains the NETGEAR FVX538 functioning as a perimeter security device and VPN head-end. The corporate IP network also has the Avaya IP Office 500 and the Avaya IP Office VoiceMail Pro server.

The Avaya VPNremote Phones are located in the public network and configured to establish an IPSec tunnel to the Public IP address of the NETGEAR FVX538. The NETGEAR FVX538 will assign IP addresses to Avaya VPNremote Phones. The assigned IP addresses, also known as the inner addresses, will be used by Avaya VPNremote Phones when communicating inside the IPSec tunnel and in the private corporate network to Avaya IP Office 500.

The Phone Manager Pro PC is located in the public network and configured to establish an IPSec tunnel to the Public IP address of the NETGEAR FVX538. The NETGEAR ProSafe VPN client is used to securely connect to the corporate IP network for telephony and data access.



# 3. Equipment and Software Validated

The following equipment and software/firmware were used for the sample configuration provided:

Device Description	Versions Tested
Avaya IP Office 500	4.1.9
Avaya IP Office Manager	6.1.9
Avaya IP Office Voicemail Pro	4.1.27
Avaya Phone Manager Pro	4.1.14
Avaya 5410 Digital Telephones	
Avaya 5610 IP Telephones	i10d01a2824.bin
Avaya VPNremote Phone (4610SW)	a10bVPN23252.bin
Avaya VPNremote Phone (5610SW)	i10bVPN23252.bin
NETGEAR FVX538 ProSafe VPN Firewall	2.1.3-17
NETGEAR ProSafe VPN Client	10.8.0 Build 20
Linksys WRV54G VPN Broadband Router	2.39.2
Cisco Catalyst Express 500 Switch	12.2(25)FY

### Table 1 – Equipment and Software Validated

## 4. IP Office Configuration

This section describes the IP Office configuration required to support VPNremote Phones and Phone Manager Pro extensions and users. All the commands discussed in this section are executed using the IP Office Manager program. This section assumes that basic configuration on Avaya IP Office has already been completed. For additional information regarding the administration of Avaya IP Office, refer to [3].

Log in to the IP Office Manager PC. Select Start  $\rightarrow$  Programs  $\rightarrow$  IP Office  $\rightarrow$  Manager to launch the Manager application. Log in to the Manager application using the appropriate credentials.

1. *Verify the licenses.* In IP Office Manager, select **License** in the left panel. Verify that IP Office has the correct licenses for **VPN IP Extensions**, **Phone Manager Pro** and **Mobile Twinning (users)**. If not, contact Avaya or an authorized Avaya business partner.

🖬 Avaya IP Office Manager (	5.1 (9) IPO 500 [4.1(9)] [Administ	rator(Administrator	11	
File Edit View Tools H	elp			
2. 🖻 - 🗐 🖪 🖬 🖬	🚺 🛹 🐸 🕴 IPO 500 📃	License	VPN IP Extensions	
IP Offices	License	¥.	VPN IP Extensions	📸 •   🗙   •   <   >
<ul> <li>BOOTP (1)</li> <li>Operator (3)</li> <li>System (1)</li> <li>Ty Line (12)</li> <li>Control Unit (5)</li> <li>Extension (23)</li> <li>User (23)</li> <li>HuntGroup (2)</li> <li>Short Code (72)</li> <li>Service (0)</li> <li>RAS (1)</li> <li>Incoming Call Route (6)</li> <li>WanPort (0)</li> <li>Directory (0)</li> <li>Time Profile (1)</li> <li>IP Route (2)</li> <li>Account Code (0)</li> <li>License (45)</li> <li>Tunnel (0)</li> <li>Logical LAN (0)</li> <li>User Rights (8)</li> <li>Auto Attendant (0)</li> </ul>	License Type  License Type  DPSec Tunnelling  Doble Twinning (users)  Phone Manager Pro (per seat)  Phone Manager Pro IP Audio Enable  Proactive Reporting  Report Viewer  SIP Trunk Channels  Small Office Edition VCM (channels)  Small Office Edition VVFi  SoftConsole (users)  Unused (1)  VMPro Database Interface VMPro Networked Messaging VMPro Outlook Interface VMPro Recordings Administrators VMPro TS (Scensoft) VMPro TS (Scansoft) VMPro VB Script Voicemail Pro (4 Ports)  VMPI IP Extensions	Licenses License Key License Type License Status Instances Expiry Date	VPN IP Extensions Valid 255 Never	
ARS (5)	Wave User			<u>OK</u> <u>Cancel</u> <u>H</u> elp

2. *Verify the TFTP Server IP Addresses.* In IP Office Manager, select **System** in the left panel. Double-click on **System**. Verify the **TFTP Server IP Address** in the right hand panel **System** tab.

🐮 Avaya IP Office Manager 6	🛛 Avaya IP Office Manager 6.1 (9) IPO 500 [4.1(9)] [Administrator(Administrator)]								
File Edit View Tools He	elp								
: 2 🖻 - 🔙 🔺 🖳 🖬 🚺	🚺 🛹 🚢 🔋 IPO 500	<ul> <li>System</li> </ul>	IPO 500	•					
IP Offices	System	×××	IPO 500		$   \overrightarrow{\bullet}   \times   \times   \times   \times   \times  $				
BOOTP (1)     Operator (3)     IPO 500     System (1)     -↑↑ Line (12)     Control Unit (5)     Extension (23)     User (23)     HuntGroup (2)     Short Code (72)	Name	System LAN1 LAN2 DN5 V Name Contact Information Set contact information to place System	oicemail Telephony LDAP 5 IPO 500	ystem Events CDR Twin Locale	ning VCM				
<ul> <li>Service (0)</li> <li>RAS (1)</li> <li>Incoming Call Route (6)</li> <li>WanPort (0)</li> <li>Directory (0)</li> <li>Time Profile (0)</li> <li>Firewall Profile (1)</li> <li>IP Route (2)</li> <li>Account Code (0)</li> <li>Unence (45)</li> </ul>		Time Offset (hours:minutes) TFTP Server IP Address Time Server IP Address File Writer IP Address Dongle Serial Number AVPP IP Address	-08:00 44 · 1 · 1 · 84 30 · 1 · 1 · 254 0 · 0 · 0 · 0 Local 5100396 0 · 0 · 0 · 0	Branch Prefix [ Local Number Length [					
	<	Conferencing Center URL			Cancel Help				

3. *Verify the IP Addresses*. In IP Office Manager, select **System** in the left panel. Doubleclick on **System**. Verify the **IP Address** in the right hand panel **LAN1** → **LAN Settings** tab.

M Avaya IP Office Manager 6.1 (9) IPO 500 [4.1(9)] [Administrator(Administrator)]								
File Edit View Tools He	elp							
	🚺 🛹 🚢 🧵 IPO 500	System	<b>I</b> PO 500	•				
IP Offices	System	×	IPO 500		🚔 -   X	✔   <   >		
<ul> <li>₭ BOOTP (1)</li> <li>✓ Operator (3)</li> <li>✓ IPO 500</li> <li>✓ System (1)</li> <li>– <sup>4</sup> Line (12)</li> <li>✓ Control Unit (5)</li> <li>✓ Extension (23)</li> <li>✓ User (23)</li> <li>✓ HuntGroup (2)</li> <li>✓ Short Code (72)</li> <li>✓ Friewall Profile (0)</li> <li>✓ Firewall Profile (0)</li> <li>✓ Firewall Profile (1)</li> <li>✓ Incense (45)</li> <li>✓ Tunnel (0)</li> <li>✓ Logical LAN (0)</li> <li>✓ Leer Bioths (8)</li> </ul>	Name	System LANI LANZ DNS LAN Settings Gatekeeper Net IP Address IP Mask Primary Trans. IP Address RIP Mode Number Of DHCP IP Addresses DHCP Mode Server Client	Voicemail Telephony LDAP twork Topology 44 1 1 1 1 255 255 255 0 0 0 0 0 None Enable NAT 20 Dialin Disabled	System Events CDR	Twinning VCM			
Auto Attendant (0) Auto Attendant (0) ARS (5)	< >				Cancel			

4. *Configure the system level twinning feature*. In IP Office Manager, select **System** in the left panel. Double-click on **System**.

Select the **Twinning** tab. Enable **Send original calling party information for Mobile Twinning**. Press the **OK** button (not shown).

Avaya IP Office Manager 6.1 (9) IPO 500 [4.1(9)] [Administrator(Administrator)]										
File Edit View Tools H	lelp									
2. 🗁 - 🔜 🔄 💽 🔜 🚺 🛹 🛎 🕴 IPO 500 🔹 System 🔹 IPO 500 🔹										
IP Offices	System	XXX	IPO 500		📸 •   X   •   <   >					
BOOTP (1)     Operator (3)     IPO 500     System (1)     -     (↑ Line (12)     Control Unit (5)     Extension (23)     User (23)     User (23)     Short Code (72)     Service (0)	Name	System LAN1 LAN2 Send original calling pa Calling party information f Mobile Twinning	DNS Voicemail Telephony LDAP arty information for Mobile Twinning for	System Events CDR	Twinning					

5. *Configure an extension for the VPNremote Phone*. An Avaya VPNremote Phone is administered the same as other Avaya IP telephones within Avaya IP Office. Even though the Avaya VPNremote Phone is physically located outside of the corporate network, the Avaya VPNremote Phone will behave the same as other Avaya IP telephones located on the corporate LAN, once the VPN tunnel has been established.

In IP Office Manager, select Extension in the left panel. In the right panel, click on

Create a New Record icon

From the pull down menu, select VoIP Extension.

The VoIP Extension screen will appear in the right panel.

• Enter a unique **Base Extension** number in the **Extn** tab as shown below.

📶 Avaya IP Office Manager 6.1 (	9) IPO 500 [4	l.1(9)] [Administr	ator(Administrator)]		
File Edit View Tools Help					
1 2 🗁 - 🖬 🖪 🔜 🖬 🗸	/ 🛎 🕴 IPO 50	00 💌 E	×tension 🔹	8004 220 🔹	
IP Offices	Ex	tension	<b>1</b>	VoIP Extension: 8005 *	▲ •   ×   •   >
	Id         Ext           ●         49         254           ●         50         210           ●         51         253           ●         55         207           ●         55         207           ●         56         208           ●         73         256           ●         74         250           ●         76         212           ●         77         213           ●         78         214           ●         79         215           ●         800         200           ●         8000         201           ●         8000         202           ●         8000         202           ●         8004         220	Module         Po           BD3         1           BD3         2           BD3         2           BD3         2           BD3         4           BD3         4           BD3         4           BD3         5           BD3         6           BD3         7           BD3         8           BP4         1           BP4         1           BP4         3           BP4         5           BP4         6           BP4         7           BP4         7           BP4         8           0         0           1         0         0           0         0         0           0         0         0	t Extn VoIP Extension Id Base Extension Caller Display Type Reset Volume After Calls Device type Module Port Disable Speakerphone	8005 240 0n Unknown IP handset 0 0	
	1				QK <u>C</u> ancel <u>H</u> elp
				ErrorList	
	Conf	I Record	Description	Enor Elat	
Ready	Comm		Costrictor		

In the **VoIP** tab:

- Enable the VPN Phone Allowed option.
- Un-check the Allow Direct Media Path option.
- Accept default values for all other fields.

M Avava IP Office Manager 6.1 (9) IPO !	500 [4.1	(9)] [Admi	nistrato	r <i>(</i> Administ	rator)]			
File Edit View Tools Help					1			<u>ما</u> لكانك
: 2 🖻 - 🖬 🖪 🔜 🔝 🗸 🎺 🛎 !	IPO 500		▼ Exte	nsion	• 8005 2	240	•	
IP Offices		Exter	nsion		<b>1</b>	VolF	PExtension: 8005 240*	<b>☆</b> •   X   •   <   >
▲ BOOTP (1)         ♥ Operator (3)         ♥ JO 500         ♥ System (1)         - ¶ (be (12)         Control Unit (5)         ● Extension (26)         ● User (23)         ● Warf (20)         ● System (1)         ● To the (12)         ● Control Unit (5)         ● Extension (26)         ● User (23)         ● HuntGroup (2)         ● Swarper (0)         ● Incoming Cal Route (6)         ● Directory (0)         ● Timewall Profile (1)         ● IP Route (2)         ▲ Account Code (0)         ● License (45)         ● Auto Attendant (0)         ● Auto Attendant (0)         ● Septin System (1)	Id ♣ 49 ♣ 50 ♣ 50 ♣ 51 ♣ 52 ♣ 53 ♣ 54 ♣ 55 ♣ 56 ♣ 73 ♣ 74 ♣ 75 ♣ 77 ♣ 77 ♣ 77 ♣ 77 ♣ 77 ♣ 78 ♣ 8000 ♣ 80000 ♣ 80000 ♣ 8000000 ♣ 8000000000000000000000000000000000000	Extension 254 253 210 253 205 206 207 208 252 252 252 212 213 214 213 214 215 7008 201 215 7008 201 215 7008 221 215 7011 7007 202 220 220 221 7011 7017 7011 7012 6568725	Module 603 603 603 603 603 603 803 803 803 803 803 803 804 804 804 804 804 804 804 804	Port  1  2  3  4  5  6  7  8  1  2  3  4  5  6  7  8  0  0  0  0  0  0  0  0  0  0  0  0	Extn VoIP IP Address MAC Address Voice Payload Siz Compression Mod Gain H450 Support	ze (ms) de	0         0	VoIP Silence Suppression Enable Faststart for non-Avaya IP phones Fax Transport Support Out Of Band DTMF Local Tones Enable RSVP Allow Direct Media Path VPN Phone Allowed

Press the **OK** button.

6. *Configure a user for the VPNremote Phone*. In IP Office Manager, select **User** in the left panel.

In the right panel, click on the **Create a New Record** icon

From the pull down menu, select User.

In the User tab, enter a unique Name and the Extension Number created in Step 5.

🖬 Avaya IP Office Manager 6.1 (9) IPO	500 [4.1(9)] [Ad	ministrator(Adminis	trator)]				- 🗆 🔀
File Edit View Tools Help							
	IPO 500	<ul> <li>User</li> </ul>	<ul> <li>240 Extn240</li> </ul>	•			
IP Offices		User		Extn240: 2	240*	🖆 -   🗙   🗸	<   >
♣ BOOTP (1)         ♀ IPO 500         ♀ IPO 500         ♀ IPO 500         ♀ System (1)         ↓ Extension (26)         ↓ User (23)         ♥ HuntGroup (2)         ♥ Short Code (72)         ♥ WarPort (0)         ♥ Time Profile (1)         ● Firewal Profile (1)         ● Firewal Profile (1)         ● Firewal Profile (1)         ● License (45)         ● Tunnel (0)         ▲ Loc Attendant (0)         ▲ Attendant (0)         ▲ Attendant (0)         ▲ F5 (5)         ▶ E911 System (1)	Name           Extn201           Extn201           Extn205           Extn206           Extn206           Extn207           Extn208           Extn208           Extn208           Extn210           Extn211           Extn213           Extn214           Extn215           Extn220           Extn221           Extn231           Extn240           Extn253           Extn254           Extn7007           Extn7008           Extn7011           RemoteManage	Extension 201 202 205 206 207 208 210 211 212 213 214 215 220 221 240 253 254 254 255 254 255 254 255 7007 7008 7011	Button Programming Menu Announcements SIP User Voicemail DND Name Password Confirm Password Full Name Extension Locale Priority Device Type User Rights User Rights User Rights view Working hours time profile Working hours User Rights	Programming Twinning ShortCodes Source N VPNUser240 240 240 240 Ex Directory Unknown User data C C C C C C C C C C C C C C C C C C	T3 Options Pho     Telephony	ne Manager Options Hunt Group Member Forwarding Dial In Voice Recording	rship

In the Voicemail tab, check the Voicemail On option and enter the Voicemail Code.

Mavaya IP Office Manager 6.1 (9) IPO	500 [4.1(9)] [Adn	ninistrator (Adminis	trator)]			
File Edit View Tools Help						
🛃 🗁 - 🔙 🖪 🔜 🔝 🚺 🛹 🛎	IPO 500	<ul> <li>User</li> </ul>	<ul> <li>240 Extn240</li> </ul>	·		
IP Offices	U	ser	<b>1</b>	Extn240: 240*	<b>- 1</b>	🗙   ✓   <   >
<ul> <li>BOOTP (1)</li> <li>Operator (3)</li> <li>System (1)</li> <li>Control Unit (5)</li> <li>Extension (26)</li> <li>User (23)</li> <li>HuntGroup (2)</li> <li>Short Code (72)</li> <li>Short Code (72)</li> <li>First Short Code (0)</li> <li>Directory (0)</li> <li>User (23)</li> <li>RAS (1)</li> <li>IP Route (2)</li> <li>Account Code (0)</li> <li>Logical LAN (0)</li> <li>Ser Rights (8)</li> <li>Auto Attendant (0)</li> <li>X E911 System (1)</li> </ul>	Name Extn201 Extn202 Extn205 Extn206 Extn206 Extn206 Extn208 Extn210 Extn214 Extn212 Extn214 Extn214 Extn214 Extn214 Extn214 Extn215 FExtn220 Extn221 Extn224 Extn253 Extn254 Extn254 Extn254 Extn254 Extn254 Extn256 Extn7007 Extn207 Extn208 Extn208 Extn208 Extn208 Extn208 Extn208 Extn29 Extn	Extension 201 201 202 205 206 207 208 210 211 212 213 214 215 220 221 240 253 254 256 7007 7008 7011	Announcements SIP Button Programming Men User Voicemail DND Voicemail Code Confirm Voicemail Code Voicemail Email Voicemail Email Off C Co Reception / Breakout (DTMF 2) Breakout (DTMF 3)	u Programming Twinning T3 Option ShortCodes Source Numbers Tel ****** ****** ppy Porward Af ff 0)	Ins Phone Manager Options Hunt G Iephony Forwarding Dial In Voice Voicemail On Voicemail Help Voicemail Ringback Voicemail Email Reading Iert	iroup Membership P Recording ( ( Cel Help

In the **Telephony** tab, enter a password if desired in the **Login Code** field. This is the same password that will be used to log in a VPNremote phone in **Step 4** of **Section 6.2** or the Phone Manager Pro user in **Step 2** of **Section 8**.

👫 Avaya 🕫 Office Manager 6.	.1 (9) IPO 500 [4,1(9)] [Admi	nistrator(Administrator)]		
Elle Edit Yew Tools He	þ			
	🗸 🚈 🕴 IPO 500	🔹 User 📃 2	40 VPN46XX	E (1) (1)
IP Offices	User	E	VPN46XX: 240	<u> </u>
<ul> <li>B DOOTP (1)</li> <li>Operator (3)</li> <li>Operator (3)</li> <li>System (1)</li> <li>17 Une (12)</li> <li>Control Unit (5)</li> <li>Extension (27)</li> <li>User (28)</li> <li>Hurkforup (3)</li> <li>RAS (1)</li> <li>Incoming Call Route (6)</li> <li>Wanhar (0)</li> <li>Fine Pontie (0)</li> <li>Time Pontie (1)</li> <li>Prove (2)</li> <li>Account Code (0)</li> <li>Users (10)</li> <li>Users (10)</li> <li>Users (10)</li> <li>Users (10)</li> <li>Users (10)</li> <li>Users (10)</li> <li>User Rights (0)</li> <li>User Rights (0)</li> <li>W Ans (10)</li> <li>User Rights (0)</li> <li>W E11 System (1)</li> </ul>	Name         Extension           Extra201         201           Extra202         202           Extra205         205           Extra205         206           Extra206         206           Extra208         208           Extra208         208           Extra208         208           Extra208         208           Extra208         208           Extra210         210           Extra213         213           Extra214         214           Extra215         215           PExtra214         214           Extra215         215           PExtra214         221           Extra215         225           PExtra214         254           Extra253         253           Extra206         206           Extra207         207           Extra208         253           Extra208         253           Extra208         256           Extra208         200           Extra208         240           VPMESOX         240           VPMESOX         241	Nerru Programming         Twinning         T3           User         Valcenal         DNO         ShortCO           Outside Call Sequence         Inside Call Sequence         Inside Call Sequence           Ringback Sequence         No Answer Time (secs)         Wrap-up Time (secs)           Wrap-up Time (secs)         Transfer Return Time (secs)         Individual Coverage Time (secs)           Login Code         Login Code         Call Cost Merk-Up           Ring Delay (secs)         Call Cost Merk-Up         Sectus on No-Answer           - Mubi Line Options         I Singing Line Preference         Delayed Ring Preference           Delayed Ring Preference         Answer Pre-Select         Inswer Pre-Select	Options       Phone Manager Options       Hunt Group Men         odes       Source Nambers       Telephony       Innovariang         Default Ring       W         Default Ring       W         Default Ring       W         2       10         10       10         100       Used on the second seco	Indersifip Announcements SIP Dial In Voice Recording Dutton Programming Call Wating On Answer Call Wating On Hold (Analogue) Busy On Held Outgoing Call Bar Offhook Station Can Intrude Cannot be Intruded Proce Login Proce Account Code System Phone System Phone System Phone Can Trace Calls Abbreviated Ring
2016 100 W OI 1FO 500				

In the **Button Programming** tab, program the buttons as needed. An example is shown below.

🜃 Avaya IP Office Manager 6.1 (9) IPO 5	500 [4.1(9)] [Adn	ninistrator(Admini	strator)]						
File Edit View Tools Help									
i 🚨 🕞 - 🔚 🖪 💽 🔜 🚺 🗸 🍏 i	IPO 500	<ul> <li>User</li> </ul>		240 VPN46XX		•			
IP Offices	Us	er	III I		VP	V46XX: 240		ď	•   X   •   <   >
<ul> <li>BOOTP (1)</li> <li>Operator (3)</li> <li>IPO 500</li> <li>System (1)</li> <li>If Line (12)</li> <li>Control Unit (5)</li> <li>Extension (27)</li> <li>User (24)</li> <li>HuntGroup (3)</li> <li>Short Code (72)</li> <li>Service (0)</li> <li>RAS (1)</li> <li>Incoming Call Route (6)</li> <li>WanPort (0)</li> <li>Directory (0)</li> <li>Time Profile (0)</li> <li>Firewall Profile (1)</li> <li>IP Route (2)</li> <li>Account Code (0)</li> <li>License (45)</li> <li>Tunnel (0)</li> <li>Logical LAN (0)</li> <li>War Rights (8)</li> <li>Auto Attendant (0)</li> <li>K E911 System (1)</li> </ul>	Name           Extn201           Extn202           Extn205           Extn206           Extn207           Extn208           Extn201           Extn206           Extn207           Extn208           Extn210           Extn211           Extn212           Extn213           Extn214           Extn255           Extn251           Extn253           Extn254           Extn256           Extn7007           Extn7008           Extn7011           TRemoteManager           VPN46XX           VPN56XX	Extension 201 202 205 206 207 208 210 211 212 213 214 215 220 221 253 254 256 7007 7008 7011 240 241	Announceme User Voice Button Progra Button 1 2 3 4 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 22 22	nts SIP email DND SI mming Menu Pr Label Ext 241 Ext 201 Twinning Voice Mail	Action Action Appearan Bridged A Bridged A Bridged A Twinning Dial	Source Numbers	Telephony Forwarding Dial I ions Phone Manager Options Action Data a= b= VPN56XX;1 Extn201;1:99 *17	Voice Hunt Gr	Recording oup Membership Edit Copy Paste

In the **Twinning** tab,

- Select Mobile for Twinning Type.
- Enter the telephone number for **Twinned Mobile Number**.
- Enable the **Hunt group calls eligible for mobile twinning** option.
- Enable the Forwarded calls eligible for mobile twinning option.

Maya IP Office Manager 6.1 (9) IPO	500 [4.1(9)] [Adr	ninistrator(Administ	trator)]		
File Edit View Tools Help					
i 2 🖻 - 🔲 🖪 🔜 🔜 🚺 🗸 🎽 j	IPO 500	<ul> <li>User</li> </ul>	<ul> <li>240 Extn240</li> </ul>	•	
IP Offices	L	Jser	12	Extn240: 240*	<b>☆</b> •   ×   •   <   >
BOOTP (1)     Operator (3)     System (1)     (7)     (1)     (7)     (1)     (12)     (3)     (2)     (	Name           Extn201           Extn202           Extn205           Extn206           Extn207           Extn208           Extn208           Extn208           Extn208           Extn210           Extn211           Extn212           Extn214           Extn215           FExtn216           Extn217           Extn218           Extn219           Extn214           Extn215           FExtn220           Extn214           Extn230           Extn244           Extn253           Extn254           Extn7007           Extn7007           Extn7011           TmNolser           TmNolser	Extension 201 201 202 205 206 207 208 210 211 212 213 214 215 220 221 221 223 253 254 256 254 256 7007 7008 7011	Announcements SIP User Voicemail DND Sh Button Programming Menu Pro Twinning Type Twinned Handset Maximum Number of Calls Twinned Mobile Number (including dial access code) Twinning Time Profile Mobile Dial Delay (secs) I Hunt group calls eligible for Forwarded calls eligible for Twin Bridge Appearances Twin Coverage Appearances	srtCodes Source Numbers 1 gramming Twinning T3 Opt Mobile CNone > 2 CNone > 2 CNone > 3 S	Telephony Forwarding Dial In Voice Recording ons Phone Manager Options Hunt Group Membership
I I	1				

Press the **OK** button.

7. Configure an extension that will be used by the IP Office telephone at the Main Office and Phone Manager Pro. A Phone Manager Pro extension is administered the same as other Avaya IP telephones within Avaya IP Office.

In IP Office Manager, select **Extension** in the left panel. In the right panel, click on

# Create a New Record icon

From the pull down menu, select **VoIP Extension**. The **VoIP Extension** screen will appear in the right panel, as shown in **Step 5**.

• Enter a unique **Base Extension** number in the **Extn** tab.

In the **VoIP** tab:

• Accept the default values.

Press the **OK** button.

8. Configure a user that will be used by the IP Office telephone at the Main Office and Phone Manager Pro. In IP Office Manager, select User in the left panel. In the right

panel, click on the **Create a New Record** icon

In the User tab, enter a unique Name and the Extension Number created in Step 7.

In the Phone Manager Options tab, select the Phone Manager Type as Telecommuter.

🗹 Avaya IP Office Manager 6.1 (9) IPO	500 [4.1(9)] [Adr	ninistrator(Admii	nistrator)]			
File Edit View Tools Help						
2 🖻 - 🔲 🖪 🔛 🔝 🗸 🎺	IPO 500	<ul> <li>User</li> </ul>	▼ 220 E)	(tn220 🔹		
IP Offices	Us	er	***	Extn220:	220	📸 •   🗙   🗸   <   >
<ul> <li>BOOTP (1)</li> <li>Operator (3)</li> <li>System (1)</li> <li>Une (12)</li> <li>Control Unit (5)</li> <li>Extension (27)</li> <li>User (24)</li> <li>HuntGroup (3)</li> <li>Short Code (72)</li> <li>Service (0)</li> <li>RAS (1)</li> <li>Incoming Call Route (6)</li> <li>WanPort (0)</li> <li>Directory (0)</li> <li>Time Profile (1)</li> <li>IP Route (2)</li> <li>Account Code (0)</li> <li>License (45)</li> <li>Tunnel (0)</li> <li>Logical LAN (0)</li> <li>User Rights (8)</li> <li>Auto Attendant (0)</li> <li>Y E911 System (1)</li> </ul>	Name           Extn201           Extn202           Extn205           Extn206           Extn207           Extn208           Extn210           Extn210           Extn211           Extn212           Extn213           Extn214           Extn215           FExtn214           Extn215           FExtn214           Extn253           Extn256           Extn7007           Extn7008           Extn7011           FarmoleManager           VPN46XX           VPN56XX	Extension           201           202           205           206           207           208           2101           212           213           214           215           220           221           253           256           7007           7008           7011           240           241	Announcements SIP User Voicemail DI Button Programming Allow user to mod Agent Mode Book with Conferent Phone Manager Type Configuration option Configuration option Configuratio	ND ShortCodes Source Nu Menu Programming Twinning lify Phone Manager settings ence Centre in Phone Manager ence Centre in Phone Mana	mbers Telephony Forward T3 Options Phone Manage TeleCommuter Ringing Internal External Hide options	ing Dial In Voice Recording pr Options Hunt Group Membership  Answering Outlook

Follow the same steps as described in **Step 6** for the **Voicemail** and **Twinning** tabs.

In the **Button Programming** tab, program the buttons as needed. An example is shown below.

File Edit View Tools Help         IPO 500       User       Extn220         IPO Offices       User       220 Extn220         IPO operator (3)       Extn201       201         IPO 500       Extn201       201         IPO 500       Extn202       202         IPO 500       Extn202       202         IPO 500       Extn202       202         IPO 500       Extn205       205         IPO 500       IPO 500       IPO 500       IPO 500         IPO 500       IPO 500       IPO 500       IPO 500       IPO 500         IPO 500       IPO 500       IPO 500       IPO 500       IPO 500       IPO 500         IPO 500       IPO 500       IPO 500       IPO 500       IPO 500       IPO 500       IPO	
Image: Second	
IP Offices     User     Extn220: 220 <sup>®</sup> BOOTP (1) <sup>®</sup> Operator (3) <sup>®</sup> IPO 500 <sup>®</sup> System (1) <sup>®</sup> System (1)	
BOOTP (1)     Name     Extension       Image: Po Source Numbers (3)     Image: Extension (1)     Extra201     201       Image: Po Source Numbers (3)     Image: Extra202     202       Image: Po Source Numbers (3)     Image: Po Source Numbers (3)     Image: Po Source Numbers (3)       Image: Po Source Number (3)     Image: Po Source Number (3)     Image: Po Source Number (3)       Image: Po Source Number (3)     Image: Po Source Number (3)     Image: Po Source Number (3)       Image: Po Source Number (3)     Image: Po Source Number (3)     Image: Po Source Number (3)       Image: Po Source Number (3)     Image: Po Source Number (3)     Image: Po Source Number (3)       Image: Po Source Number (3)     Image: Po Source Number (3)     Image: Po Source Number (3)       Image: Po Source Number (3)     Image: Po Source Number (3)     Image: Po Source Number (3)       Image: Po Source Number (3)     Image: Po Source Number (3)     Image: Po Source Number (3)       Image: Po Source Number (3)     Image: Po Source Number (3)     Image: Po Source Number (3)       Image: Po Source Number (3)     Image: Po Source Number (3)     Image: Po Source Number (3)       Image: Po Source Number (	/   <   >
Control Unit (5)         Extraction         Control Unit (5)         Extraction         Action         Action Data         Remover <ul> <li>Extraction (27)</li> <li>Extractin (28)</li> <li>Extractin (28)</li></ul>	hip

*Note:* The Users configured with Phone Manager Telecommuter option will have in the left panel next to the User Name. This denotes a Hot Desk user. The Phone Manager User has an internal IP Office extension. While logged in to Phone Manager as a telecommuter, the internal IP Office extension is logged off. The internal IP Office extension is logged off.

9. *Save the configuration*. In IP Office Manager, use the licon to save the configuration and load the saved configuration on the IP Office.

# 5. NETGEAR FVX538 Configuration

## 5.1. VPN

Setting up the VPN tunnel encryption and authentication is a two-phase process.

- Phase 1 covers how the Avaya VPNremote Phone and NETGEAR ProSafe VPN Client will securely negotiate and handle the building of the tunnel with the NETGEAR FVX538.
- Phase 2 sets up how the data passing through the tunnel will be encrypted at one end and decrypted at the other. This process is carried out on both sides of the tunnel.

**Table 1** provides the IKE Proposals used in the sample configuration for the Avaya VPNremote Phones.

Phase	Encryption/ Authentication Method	Diffie- Hellman Group	Encryption Algorithm	Hash Algorithm	Life Time (sec)
P1	Pre-Shared Key	2	3DES	SHA-1	432000
P2	ESP	2	3DES	SHA-1	432000

Table 2 – Avaya VPNremote Phones IKE P1/P2 Proposals

**Table 2** provides the IKE Proposals used in the sample configuration for the NETGEAR ProSafe VPN Client.

Phase	Encryption/ Authentication Method	Diffie- Hellman Group	Encryption Algorithm	Hash Algorithm	Life Time (sec)
P1	Pre-Shared Key	2	3DES	SHA-1	28800
P2	ESP	2	3DES	SHA-1	3600

Table 3 – NETGEAR ProSafe VPN Client IKE P1/P2 Proposals

## 5.2. Access NETGEAR FVX538

1. From a web browser, enter http://<IP address of the NETGEAR FVX538>, the IP address of the local interface of the NETGEAR FVX538. Log in using the appropriate credentials.

## 5.3. Configure NETGEAR FVX538 Ethernet Interfaces

The steps below configure the IP addresses of the local and WAN Ethernet interfaces for the configuration shown in **Figure 1**. The Avaya VPNremote Phone and the NETGEAR ProSafe VPN Client will use the IP address of the WAN Ethernet interface to establish an IPSec Tunnel.

 Configure IP address of the LAN interface. Select Network Configuration → LAN Settings → LAN Setup from the top menu bar. Assign IP address 44.1.1.254 with a subnet mask of 255.255.255.0 for the LAN interface of the NETGEAR FVX538. Disable the DHCP Server.



 Configure the IP address of the WAN interface. Select Network Configuration → WAN1 ISP Settings from the top menu bar. Assign IP address 44.2.2.2 with a subnet mask of 255.255.255.252 for the WAN interface of the NETGEAR FVX538.

NETGEAR ProSafe™ - WAN1 ISP Settings - Microsoft Internet Explor	rer IIX
Eile Edit View Favorites Tools Help	
Back - 💭 - 🗶 🛃 🏠 🔎 Search 🎌 Favorites 📢	
Address Address http://44.1.1.254/wan1_setup.htm	🔽 🔁 Go 🛛 Links 🎽 👘 SnagIt 🛅
NETGEAR'	
PROSAFE	NETCEAR DroSafe VDN Firewall FVY538
Network Configuration   Security   VPN   Admini	Istration Monitoring Web Support Logout
WAN Settings Protocol Binding # Dynamic L WAN1 TSP Settings WAN2 TSP Settings WAN Mode	Advanced WAN Status
The for beings that is beings that Hode	
# ISP Login	help
Does Your Internet Connection Require a Login?	Login:
C Yes € No ∫	Password:
// TCD Turs	
ж ISP Туре	Account Name:
	Domain Name:
Which type of ISP connection do you use?	Login Server:
Austria (PPTP)     Other (PPDeE)	Idle Timeout: O Keep Connected
Guiler (PFPDE)	Idle Time: 5 Minutes
)	My IP Address:
	Server IP Address:
Internet (IP) Address (Current IP Address)	Domain Name Server (DNS) Servers
O Get Dynamically from ISP	Get Automatically from ISP
<ul> <li>Use Static IP Address</li> </ul>	Use These DNS Servers
IP Address: 44 •2 •2 •2	Primary DNS Server : 0 0 0 0
IP Subnet Mask: 255 -255 -255 -252	Secondary DNS Server: 0 0 0 0
Gateway IP Address: 44 •2 •2 •1	
Apply Reset	Test Auto Detect
	hr NETGEAD®
Done	Internet

## 5.4. Mode Config Record

The Mode Config record is used to define the pool of IP addresses that will be used by the Avaya VPNremote Phone as well as the authentication and encryption method to use for tunnel traffic by the NETGEAR FVX538. Select **VPN**  $\rightarrow$  **Mode Config** from the top menu bar to create a Mode Config record.

Enter the following information:

- **Record Name**: Enter a name (e.g., **Avayaphn**) for the Mode Config record.
- **First Pool**: Enter the range of IP addresses for the pool.
- **PFS Key Group**: Select the hashing algorithm.
- **SA Lifetime**: Enter the time in seconds for Phase 2 renegotiation. Avaya recommends setting this value to **432000** seconds or 5 days.
- Encryption Algorithm: Select the encryption algorithm for the tunnel.
- Integrity Algorithm: Select the integrity algorithm for the tunnel.
- Local IP Address: Enter the subnet of the IP Office located in the private or trusted side.
- Local Subnet Mask: Enter the subnet mask of the IP Office located in the private or trusted side.

P NETGEAR ProSafe™ - Add Mode Config Record - Microsoft Internet Explorer	
<u>File Edit Vi</u> ew F <u>a</u> vorites <u>T</u> ools <u>H</u> elp	
🔾 Back 🝷 📀 🖌 🗾 🛃 🏠 🔎 Search 🥂 Favorites 🤣 😥 🕹 🔜 🦓	
A <u>d</u> dress 🙆 http://44.1.1.254/platform.cgi 💽 Go 🛛 Links 🎽 👘 🗸 🔰 🈏	SnagIt 🛃
	<b>_</b>
<u>NEIGEAR</u>	
NETGEAR ProSafe VPN Firewall F	VX538
Network Configuration   Security   VPN   Administration   Monitoring   Web Support   Log	jout
:: Policies :: VPN Wizard :: Certificates :: Mode Config :: VPN Client :: Connection Status ::	
Edit Mode Config Record	
Operation succeeded.	
# Client Pool	?)help
Record Name: Avayaphn	
First Pool: Starting IP 10 .10 .10 .10 Ending IP 10 .10 .20	
Second Pool: Starting IP 0 .0 .0 .0 Ending IP 0 .0 .0	
Third Pool: Starting IP 0 .0 .0 Ending IP 0 .0 .0	
WINS Server: Primary 0 0 0 0 Secondary 0 0 0	
DNS Server: Primary 0 0 0 0 Secondary 0 0 0	
Traffic Lunnel Security Level	help
SA Lifetime: 432000 Seconds	
Encryption Algorithm: 3DES	
Integrity Algorithm: SHA-1 🔽	
Local IP Address: 44 · 1 · 1 · 0	
Local Subnet Mask: 255 -255 -0	
Apply	
2006 © Copyright NETGEAR®	
🗿 Done	

## 5.5. IKE Policy

Create an IKE policy for phase 1 negotiation by selecting VPN  $\rightarrow$  Policies  $\rightarrow$  IKE Policies from the top menu bar. Enter the following information:

#### Mode Config Record

- Do you want to use Mode Config Record?: Select Yes.
- Select Mode Config Record: Select the Mode Config record (e.g., Avayaphn) created in Step 5.4.

General

- **Policy Name**: Enter a name for the IKE policy.
- Exchange Mode: Select Aggressive.
- Local
  - Select Local Gateway: Select WAN1.
  - Identifier Type: Select Local Wan IP.

Remote

- Identifier Type: Select FQDN.
- Identifier: Enter the "Group Name" that will be used by the Avaya VPNremote phone to establish the VPN tunnel in Step 3 of Section 6.2.

**IKE SA Parameters** 

- Encryption Algorithm: Select the encryption algorithm.
- Authentication Algorithm: Select the authentication algorithm.
- Authentication Method: Select Pre-shared key.
- **Pre-shared key**: Enter the "Group PSK" that will be used by the Avaya VPNremote phone in **Step 3** of **Section 6.2**.
- Diffie-Hellman (DH) Group: Select the DH Group.
- **SA-Lifetime (sec)**: Enter the time in seconds for Phase 2 renegotiation. Avaya recommends setting this value to **432000** seconds or 5 days.
- Enable Dead Peer Detection: Select No.
- XAUTH Configuration: Select Edge Device.
- Authentication Type: Select User Database. The VPN clients stored in the user database of the NETGEAR FVX538 will be used for authentication. The VPN clients will be defined in Step 5.6.

METGEAR ProSafe™ - Edit IKE Policy - Microsoft Internet Explorer	
<u>File Edit View Favorites Tools Help</u>	
🛛 🚱 Back 🔹 🕥 👻 😰 🏠 🔎 Search   https://www.search	😣 🍃 🍃 🦓
Address 🗃 http://44.1.1.254/platform.cgi	🔽 🎅 Go 🛛 Links 🌺 🔹 🌘 SnagIt 📷
<u>NETGEAR</u>	
PROSAFE	NETGEAR ProSafe VPN Firewall FVX538
Network Configuration     Security     VPN     Admin	stration Monitoring Web Support Logout
:: Policies :: VPN Wizard :: Certificates :: M	ode Config :: VPN Client :: Connection Status ::
Edit IKE Policy	Add New VPN Policy
Operation	succeeded.
Mode Config Record     Phelp	III General 📀 help
Do you want to use Mode Config Record?	Policy Name: Avaya
Ves No	Direction / Type: Responder
Select Mode Config Record: Avayaphn	Exchange Mode: Aggressive 💌
# Local	# Remote Delp
Select Local Gateway: • WAN1 • WAN2	
Identifier Type: Local Wan IP 💌	Identifier Type : FQDN
Identifier: 44.2.2.2	Identifier: avaya
IKE SA Parameters	() help
Encryption Algorithm:	3DES •
Authentication Algorithm:	SHA-1 •
Authentication Method:	© Pre-shared key C RSA-Signature
Pre-shared key:	1234567890 (Key Length 8 - 49 Char)
Diffie-Hellman (DH) Group:	Group 2 (1024 bit) 💌
SA-Lifetime (sec):	432000
Enable Dead Peer Detection:	() Yes (• No
Detection Period:	180 (Seconds)
Reconnect after failure count:	
Done	i internet
13 Yeards	

The bottom half of the IKE policy screen is shown below.

METGEAR ProSafe™ - Edit IKE Policy - Microsoft Internet Explorer	
Eile Edit View Favorites Iools Help	2
🛛 😋 Back 🔹 📀 👻 😰 🐔 🔎 Search  Favorites 🤣 🍰 🍓 🔜 🖓	
Address 🙆 http://44.1.1.254/platform.cgi	2
# Extended Authentication	
XAUTH Configuration       Authentication Type: User Database •         O       None         •       Edge Device         •       IPSec Host	
Apply Reset	
2006 © Copyright NETGEAR®	
🖉 🛛 🖉 Internet	

Solution & Interoperability Test Lab Application Notes ©2008 Avaya Inc. All Rights Reserved.

23 of 51 IPO-NTGR-FVX538.doc

### 5.6. Xauth User

Add a user that will be used by the Avaya VPN remote phone for authentication by selecting VPN  $\rightarrow$  VPN Client from the top menu.

- User Name: Enter the name of the user.
- **Password**: Enter the password for the user.
- **Confirm Password**: Enter the password again.

Click add.

NETGEAR ProSafe™ - User Database - Mic	rosoft Internet Explorer		
ile <u>E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> ools <u>H</u> elp			4
🔾 Back 🗸 🕥 🖌 🗾 🖉	Search 🤺 Favorites 🤣 🔗 -	2 2 2	
dress 🗃 http://44.1.1.254/user_db.htm		🔽 🔁 Go 🛛 Links 🎽 🔁 🔹	🌀 SnagIt 😁
NETGEAR PROSAFE		NETGEAR ProSafe VPN Firewa	all FVX538
Network Configuration Secu	rity   VPN   Administration	Monitoring   Web Support	Logout
:: Policies :: VPN Wizard	:: Certificates :: Mode Config ::	VPN Client :: Connection Status ::	
User Database RADIUS Client			
# Configured Users			Phelp
	User Name		Action
	rich		😥 edit
	tom		🧭 edit
	harry		🧭 edit
Add New User:			
User Name	Password	Confirm Password	Add
			🛞 add
	·		
	2006 @ Conversiont NETGEAR®		

### 5.7. VPN Policy

The VPN policy will be used by the NETGEAR ProSafe VPN client to establish a tunnel to the NETGEAR FVX538. Create a new VPN policy by selecting **VPN**  $\rightarrow$  **VPN Wizard**. Enter the following information:

- This VPN tunnel will connect to the following peers: Select VPN Client.
- What is the new Connection Name?: Enter a name for the VPN policy.
- What is the pre-shared key?: Enter the key that will be used by the NETGEAR ProSafe VPN client for authentication.
- This VPN tunnel will use following local WAN Interface: Select WAN 1.
- What is the Remote Identifier Information?: Enter the arbitrary Domain Name which will be used in Step 2 of Section 7.

SH; Reviewed: SPOC 3/4/2008 • What is the Local Identifier Information?: Enter the arbitrary Domain Name which will be used in Step 1 of Section 7.

Click Apply.

🚰 NETGEAR ProSafe™ - VPN Wizard - Microsoft Internet Explorer	
Eile Edit View Favorites Tools Help	
🛛 🚱 Back 🔹 🕥 👻 🙎 🏠 🔎 Search 🤺 Favorites 🚱 🔗 🎍 🔜 🦓	
Address 🕘 http://44.1.1.254/vpn_wizard.htm	) Links 🎽 🔁 🕶 🛛 🈏 SnagIt 📑
NETCEAD'	
NETGEAR I	ProSafe VPN Firewall FVX538
Network Configuration   Security   VPN   Administration   Monitoring	Web Support   Logout
:: Policies :: VPN Wizard :: Certificates :: Mode Config :: VPN Client ::	Connection Status
VPN Wizard	VPN Wizard Default Values
# About VPN Wizard	(?) help
The Wizard sets most parameters to defaults as proposed by the VPN Consortium ( <u>VPNC</u> ) key, which greatly simplifies setup. After creating the policies through the VPN Wizard, you	, and assumes a pre-shared can always update the
parameters through the <u>Policies</u> menu.	
This VPN tunnel will connect to the following peers:	
C Gateway 💿 VPN Client	
# Connection Name and Remote IP Type	?help
What is the new Connection Name? home	
What is the pre-shared key? 1234567890	(Key Length 8 - 49 Char)
This VPN tunnel will use following local WAN Interface: 10 WAN 1 C WAN 2	
# End Point Information	Phelp
What is the Remote Identifier Information? fvx_remote.com	
What is the Local Identifier Information? fvx_local.com	
Secure Connection Remote Accessibility	help
What is the remote LAN IP Address?	
What is the remote LAN Subnet Mask?	
Apply Reset	
2006 © Copyright NETGEAR®	
	🔹 🚺 🔮 Internet

The following VPN policy is created automatically and is shown below.

🗿 NETGEAR ProSafe™ - Edit VPN Policy - Microsoft Internet Explorer	_ 🗆 X
Ele Edit View Favorites Iools Help	-
🕞 Back 🔹 🛞 🖌 😰 🏠 🔎 Search 🤺 Favorites 🤣 🍰 👟 🌺 🥽 🦓	
Address 🙆 http://44.1.1.254/platform.cgi	gIt 😁
N E T G E A R'	
PROSAFE NETGEAR ProSafe VPN Firewall FVX	538
Network Configuration   Security   VPN   Administration   Monitoring   Web Support   Logou	
Dolicies VDN Wizard Certificates Mode Config VDN Client Connection Status	
Edit VPN Policy	
Operation succeeded.	
∰ General @htt	elp
Policy Name: home	
Policy Type: Auto Policy	
Select Local Gateway: © WAN1 © WAN2	
Remote Endpoint: O IP Address:	
FQDN: rvx_remote.com	
Enable Keenalive: O Yes O No	
Ping IP Address: 0 .0 .0 .0	
Detection period: 10 (Seconds)	
Reconnect after failure count: 3	
III Traffic Selection	elp
Local IP: Subnet 💌 Remote IP: Any 💌	
Start IP Address: 44 1 1 0 Start IP Address: 0 0 0 0	
End IP Address: 0 0 0 End IP Address: 0 0 0	
Subnet Mask: 255 .255 .0 Subnet Mask: 0 .0 .0	
🕘	

The bottom half of the VPN policy is shown below.

NETGEAR ProSafe <sup>IN</sup> - Edit VPN Policy - Microsoft Internet Explorer	
Eile Edit View Favorites Tools Help	
🕞 Back 🔹 🌍 🖌 📓 🐔 🔎 Search 🤺 Favorites 🚱 🔗 - 😓 🕞 🦓	
Address 🗑 http://44.1.1.254/platform.cgi 💽 🔂 Go 🗍 Links » 🕅 🐑 🗸	SnagIt 😁
# Manual Policy Parameters	🕐 help
SPI-Incoming: (Hex, 3-8 Chars) SPI-Outgoing: (Hex, 3-8 Chars)	hars)
Encryption Algorithm: 3DES 💌 Integrity Algorithm: SHA-1 💌	
Key-In: Key-In:	
Key-Out: Key-Out:	
(DE5-8 Char & 3DE5-24 Char) (MD5-16 Char & SHA-1-20	0 Char)
# Auto Policy Parameters	Phelp
SA Lifetime 3600 Seconds -	
Encryption Algorithm: 3DES 🔹 Integrity Algorithm: SHA-1 💽	
PFS Key Group: DH Group 2 (1024 bit)	
Salact IVE Balian harro	
Apply Reset	
2006 © Copyright NETGEAR®	
	iternet

Solution & Interoperability Test Lab Application Notes ©2008 Avaya Inc. All Rights Reserved.

26 of 51 IPO-NTGR-FVX538.doc The following IKE policy is created automatically and is shown below.

A NETGEAR ProSafe™ - Edit IKE Policy - Microsoft Internet Explorer	_ [0] ×
	1
🕞 Back 🔹 💮 🖌 😰 🐔 🔎 Search 🦖 Favorites 🚱 🖇	2- 👌 🗔 🦓
Address Addres	▼ Sag Links » 🕀 - SnagIt 🖭
NETGEAR PROSAFE	NETGEAR ProSafe VPN Firewall FVX538
Network Configuration   Security   VPN   Administration	on   Monitoring   Web Support   Logout
:: Policies :: VPN Wizard :: Certificates :: Mode Conf	ig :: VPN Client :: Connection Status ::
Edit IKE Policy	Add New VPN Policy
Operation succeed	led.
Mode Config Record     Ohelp     Ge	eneral 📀 help
Do you want to use Mode Config Record?	Policy Name: home
O Yes O No	Direction / Type: Responder
Select Mode Config Record:	Exchange Mode: Aggressive v
🤎 view selected	
# Local @belo # Re	mote (2) help
Select Local Gateway:   WAN1 OWAN2	C
	Identifier Type : FODN
Identifier: fvx local.com	Identifier: fvx_remote.com
⊯ IKE SA Parameters	() help
Encryption Algorithm: 3DES	
Authentication Algorithm: SHA-1	
Authentication Method: • Pre	-shared key O RSA-Signature
Pre-shared key: 123456	(Key Length 8 - 49 Char)
Diffie-Hellman (DH) Group: Group	2 (1024 bit)
SA-Lifetime (sec): 28800	
Enable Dead Peer Detection: C Yes	(• No
Detection Period: 10	(Seconds)
Reconnect after failure count: 3	
	🚺 🚺 👔 Internet

The bottom half of the IKE policy is shown below.

🦓 NETGEAR ProSafe™ - Edit IKE Policy - Microsoft Internet Explorer	
<u>File Edit View Favorites Iools Help</u>	2
🔀 Back 🔹 🌍 🖌 📓 🐔 🔎 Search 🤺 Favorites  🚱 😓 😓 🖓	
Address 🙆 http://44.1.1.254/platform.cgi	2
III Extended Authentication	
XAUTH Configuration     Authentication Type:     User Database        Image: State Stat	
Apply Reset	
2006 © Copyright NETGEAR®	
Internet	

Solution & Interoperability Test Lab Application Notes ©2008 Avaya Inc. All Rights Reserved.

27 of 51 IPO-NTGR-FVX538.doc

# 6. Avaya VPNremote Phone Configuration

## 6.1. Avaya VPNremote Phone Firmware

The Avaya VPNremote Phone firmware must be installed on the phone prior to the phone being deployed in the remote location. Refer to [1] and [2] for details on installing Avaya VPNremote Phone firmware. The firmware version of Avaya VPNremote Phone can be identified by viewing the version displayed on the phone upon boot up or when the phone is operational by selecting the **Options** hard button  $\rightarrow$  **View IP Settings** soft button  $\rightarrow$  **Miscellaneous** soft button  $\rightarrow$  **h**ard button. The Application file name displayed denotes the installed firmware version.

As displayed in **Table 1**, Avaya VPNremote Phone firmware includes the letters **VPN** in the name. This allows for easy identification of firmware versions incorporating VPN capabilities.

## 6.2. Configuring Avaya VPNremote Phone

The Avaya VPNremote Phone configuration can be administered centrally from an HTTP/TFTP server or locally on the phone. These Application Notes utilize the local phone configuration method. Refer to [1] and [2] for details on a centralized configuration.

1. There are two methods available to access the **VPN Configuration Options** menu from the Avaya VPNremote Phone.

### a. During Telephone Boot:

During Avaya VPNremote Phone boot up, the option to press the \* key to enter the local configuration mode is displayed on the telephone screen as shown below.

DHCP \* to program

When the \* key is pressed, several configuration parameters are presented such as the phones IP Address, the Call Server IP Address, etc. Press # to accept the current settings or set to an appropriate value. The final configuration option displayed is the VPN Start Mode option shown below. Press the \* key to enter the VPN Options menu.

VPN Start Mode: Boot \*=Modify #=OK

#### b. During Telephone Operation:

While Avaya VPNremote Phone is in an operational state, i.e. registered with IP Office, press the following key sequence on the telephone to enter VPN configuration mode:

Mute-V-P-N-M-O-D-# (Mute-8-7-6-6-6-3-#)

The follow is displayed: VPN Start Mode: Boot \*=Modify #=OK

Press the \* key to display the VPN Options menu.

2. The Avaya VPNremote Phone can interoperate with several VPN head-end vendors. The Avaya VPNremote Phone must be told which VPN head-end vendor will be used so the appropriate protocol dialogs can take place. This is done by setting the **VPN Configuration Profile** on the Avaya VPNremote Phone.

Press the **Profile** soft button at the bottom of the Avaya VPNremote Phone display while in the VPN Options mode. The **VPN Configuration Profile** options, shown below, are displayed. If a Profile other than **Juniper Xauth with PSK** is already chosen, press the Modify soft button to display the following list:

- Avaya Security Gateway
- Cisco Xauth with PSK
- Juniper Xauth with PSK
- Nortel Contivity

•

Press the button adjacent to the **Juniper Xauth with PSK** profile option then press the **Done** soft button. **Juniper Xauth with PSK** must be used instead of the **Generic PSK** profile because the sample network is using Xauth authentication.

**3.** The VPN configuration options menu is displayed. For a detailed description of each VPN configuration option, refer to [1] and [2].

The configuration values of one of the Avaya VPNremote Phones used in the sample configuration are shown in **Table 4** below.

Note: The values entered below are case sensitive.

Press the  $\blacktriangleright$  hard button on the telephone to access the next screen of configuration options. Phone models with larger displays (e.g., 4621) will present more configuration options per page.

Configuration Options	Value	Description
Server:	44.2.2.2	IP address of the NETGEAR FVX538 (WAN interface configured in <b>Step 2</b> of <b>Section 5.3</b> ).
User Name:	rich	User created in Section 5.6.
Password:	****	Must match user password entered in <b>Section 5.6</b> .
Group Name:	avaya	Must match the "Remote Identifier" entered in <b>Section</b> <b>5.5</b> .
Group PSK:	1234567890	Must match the "Pre-shared key" entered in <b>Section 5.5</b> .
VPN Start Mode	BOOT	IPSec tunnel dynamically starts on phone power up.
Password Type	Save in Flash	User is not prompted at phone boot up.
Encapsulation	4500-4500	This default value enables NAT Traversal.
Syslog Server	-	
IKE Parameters	DH2-3DES-SHA1	
IKE ID Type:	FQDN	
Diffie-Hellman Grp:	2	Can be set to "Detect" to accept VPN Concentrator settings.
Encryption Alg	3DES	Can be set to "Any" to accept VPN Concentrator settings.
Authentication Alg	SHA1	Can be set to "Any" to accept VPN Concentrator settings.
IKE Xchg Mode	Aggressive	
IKE Config Mode:	Enable	
XAUTH	Enable	
Cert Expiry Check	Disable	
Cert DN Check	Disable	
<b>IPSec Parameters</b>	DH2-3DES-SHA1	
Encryption Alg	3DES	Can be set to "Any" to accept VPN Concentrator settings.
Authentication Alg	SHA1	Can be set to "Any" to accept VPN Concentrator settings.

<b>Configuration Options</b>	Value	Description
Diffie-Hellman	2	Can be set to "Detect" to
Grp:		accept VPN Concentrator
		settings.
Protected Nets		
Remote Net #1:	44.1.1.0/24	Access to IP Office subnet.
Copy TOS:	Yes	Maintain phone TOS setting
		on Corp. Network for QoS.
File Srvr:	44.1.1.84	TFTP File Server.
Connectivity Check:	Always	Always test IPSec
		connectivity.
Qtest	Disable	Can be set to either Enable or
		Disable to allow user access
		to QTest feature.

#### Table 4 – Avaya VPNremote Phone Configuration

When all VPN configuration options have been set, press the **Done** soft button. The following is displayed. Press # to save the configuration and reboot the phone.

Save new values ? \*=no #=yes

4. After the phone reboots, enter the **Base Extension**, administered in **Step 5** of **Section 4**, as the **Extension** when prompted. Enter the **Login Code**, administered in **Step 6** of **Section 4** as the **Password** when prompted.

# 7. NETGEAR ProSafe VPN Client Configuration

This section shows the configuration of the NETGEAR ProSafe VPN Client. This section assumes that the NETGEAR ProSafe VPN Client software is already installed on the client desktop.

- Launch the NETGEAR ProSafe VPN Client Security Policy Editor by selecting Start → All Programs → NETGEAR ProSafe VPN Client (Security Policy Editor. Right click the folder My Connections and select Add (Connection (not shown). Provide a descriptive name for the new connection. netgear was used in the sample configuration. Configure the fields shown below.
  - Select Secure for Connection Security.
  - Select **IP Subnet** for **ID Type**.
  - Enter 44.1.1.0 in the Subnet field and 255.255.255.0 in the Mask field.
  - Select All in the Protocol field.
  - Check the Use box and select Secure Gateway Tunnel from the drop down menu.
  - Enter **fvx\_local.com** as the arbitrary **Domain Name** in the **ID Type** field. This must match the **Local Identifier** entered in **Section 5.7**.
  - Enter 44.2.2.2, the IP address of the NETGEAR FVX538 public interface, as the Gateway IP Address.

Security Policy Editor - NETGEAR ProSafe V	PN Client
<u>File E</u> dit <u>O</u> ptions <u>H</u> elp	
Network Security Policy	NETGEAR S
<ul> <li>☐ My Connections</li> <li>☐ An Instance</li> <li>☐ An</li></ul>	Connection Security  Secure Non-secure Block  Conly Connect Manually
	Remote Party Identity and Addressing         ID Type       IP Subnet         Subnet:       44.1.1.0         Mask:       255.255.255.0         Protocol       All
	Use Secure Gateway Tunnel

- 2. Expand the netgear folder and select My Identity. Configure the fields shown below.
  - Select None for the Select Certificate field.
  - Select **Domain Name** for the **ID Type** field and enter arbitrary domain **fvx\_remote.com**. This must match the **Remote Identifier** in **Section 5.7**.
  - Select Preferred for the Virtual Adapter field.
  - Select the network interface in the Internet Interface field.

All remaining fields can be left as the defaults. Click **Pre-Shared Key** to continue.

N Security Policy Editor - NETGEAR ProSafe V	PN Client
<u>File E</u> dit <u>O</u> ptions <u>H</u> elp	
Network Security Policy	NETGEAR 🔀
My Connections netgear My Identity Defensions Security Policy Other Connections	My Identity Select Cgrificate None ID Type Pot Domain Name Fvx_remote.com Secure Interface Configuration Virtual Adapter Internet Interface Name [1] Broadcom NetXtreme 57xx Gigabit Controller IP Addr [192.168.1.105

**3.** Click **Enter Key** and type the Pre-Shared Key. This must match the Pre-shared Key entered in **Section 5.7**. Click **OK**.

Pre-Shared Key		X
Enter Key		
	Enter Pre-Shared Key (at least 8 characters)	1
	This key is used during Authentication Phase if the Authentication Method Proposal is "Pre-Shared key".	
	OK Cancel	

Solution & Interoperability Test Lab Application Notes ©2008 Avaya Inc. All Rights Reserved.

- 4. Select Security Policy. Configure the fields shown below.
  - Select Aggressive Mode for Select Phase 1 Negotiation Mode.
  - Check Enable Perfect Forward Secrecy (PFS).
  - Select PFS Key Group. Refer to Section 5.7.
  - Check the **Enable Replay Detection** box.

N Security Policy Editor - NETGEAR ProSafe VPN Client	
<u>File Edit Options H</u> elp	
Network Security Policy	NETGEAR 😽
Image: Security Policy         Image: Security Poli	cy ase 1 Negotiation Mode in Mode gressive Mode a Manual Keys Perfect Forward Secrecy (PFS) iroup Diffie-Hellman Group 2 Replay Detection

- 5. Expand the folder Security Policy → Authentication (Phase 1) and select Proposal 1. Configure the highlighted fields shown below.
- Select Pre-Shared Key for the Authentication Method field.
- Select **Triple DES** for the **Encrypt Alg** field.
- Select SHA-1 for the Hash Alg field.
- Select **Unspecified** for the **SA Life** field.
- Select Diffie-Hellman Group 2 for the Key Group field.

Edit Options Help     Network Security Policy     My Connections     My Identity   Security Policy     Authentication Method and Algorithms     Authentication Method     Pre-Shared Key     Encryption and Data Integrity Algorithms     Encryption and Data Integrity Algorithms     Encrypt Alg   Triple DES   Hash Alg   SA Life   Unspecified     Key Group	Security Policy Editor - NETGEAR ProSafe VI	PN Client
Network Security Policy My Connections My Identity Security Policy Authentication Method and Algorithms Authentication Method Pre-Shared Key Encryption and Data Integrity Algorithms Encrypt Alg Triple DES My Identity Seconds SA Life Unspecified Key Group Diffie-Hellman Group 2	<u>File Edit Options Help</u>	
Authentication Method and Algorithms          My Connections         My Identity         Security Policy         Authentication (Phase 1)         Pre-Shared Key         Pre-Shared Key         Dther Connections         Encryption and Data Integrity Algorithms         Encrypt Alg         Triple DES         Hash Alg         SHA-1         Seconds         SA Life         Unspecified	Retwork Security Policy	NETGEAR <mark>S</mark>
	My Connections netgear My Identity Security Policy Authentication (Phase 1) Proposal 1 Connections Other Connections	Authentication Method and Algorithms Authentication Method Pre-Shared Key Encryption and Data Integrity Algorithms Encrypt Alg Triple DES Hash Alg SHA-1 Seconds SA Life Unspecified Seconds SA Life Unspecified Seconds Second

- 6. Expand the folder Security Policy → Key Exchange (Phase 2) and select Proposal 1. Configure the fields shown below. All remaining fields can be left as the defaults.
- Check the Encapsulation Protocol (ESP) box.
- Select Triple DES for Encrypt Alg field.
- Select SHA-1 for the Hash Alg field.
- Select **Tunnel** for the **Encapsulation** field.

Ele Edit Options Help         Network Security Policy         My Connections         My Connections         My Identity         Security Policy         Authentication (Phase 1)         Proposal 1         Key Exchange (Phase 2)         Proposal 1         Proposal 2         Proposal 2	Security Policy Editor - NETGEAR ProSafe VPI	N Client
Metwork Security Policy       IPSec Protocols         My Connections       IPSec Protocols         My Identity       Security Policy         Authentication (Phase 1)       Proposal 1         Key Exchange (Phase 2)       Image: Compression None         Image: Compression None       <	<u>File Edit Options H</u> elp	
Image: My Connections       IPSec Protocols         Image: My Identity       Security Policy         Image: Security Policy       Image: Security Policy         Image: Security Policy       I	Network Security Policy	NETGEAR 😽
Bother Connections	My Connections netgear My Identity Security Policy Authentication (Phase 1) Proposal 1 Key Exchange (Phase 2) Proposal Other Connections	IPSec Protocols         SA Life       Unspecified       Seconds       KBytes         Compression       None       ▼         ✓       Encapsulation Protocol (ESP)       ▼         Encrypt Alg       Triple DES       ▼         Hagh Alg       SHA-1       ▼         Encapsulation       Tunnel       ▼         ▲uthentication Protocol (AH)       Hash Alg       SHA-1         Encapsulation       Tunnel       ▼

From the menu, select File  $\rightarrow$  Save to save the configuration.

# 8. Phone Manager Pro Configuration

Log in to the PC and select **Start**  $\rightarrow$  **Programs**  $\rightarrow$  **IP Office**  $\rightarrow$  **Phone Manager** to launch the application.

- 1. In IP Office Phone Manager Where do you want to work? screen:
  - Select Remote (Telecommuter Mode)
  - Enter a descriptive **Remote Profile Name**
  - Enter the telephone number in **Contact Number** field, as it would be dialed from any IP Office extension. In these Application Notes, **2552020** is the number of a PSTN phone used by the telecommuter.
  - Accept the default values for Continuous Mode and Test Call Required.
  - Click on Save Profile.
  - Click on **OK**.

0	Internal (Office)	
Ø	Remote (Telecommuter Mode	.)
		-
	Sav	ved Remote Profile Details
	Remote Profile Name	Home Office
	Contact Number	2552020
		Continuous Mode
		Test Call Required
		Save Profile
		Save Profile

- 2. In the IP Office Phone Manager / Login screen, enter:
  - User Name\Extn
  - **Password**. This password must match the **Login Code** administered in **Step 6** of **Section 4**.
  - Enter the LAN1 IP Address of IP Office, from Step 3 of Section 4, in the Unit Name\IP-Address field.
  - Click on **OK**.

Phone Manage	er Login	the second s	
User Name	e\ Extn		
Extn220		User List	
Password			
	•	O Remember Password	
Unit Name	IP-Address		
44.1.1.1		Browse	

*Note:* The User configured with Phone Manager Telecommuter option is a Hot Desk user, as mentioned in **Section 4**, **Step 8**. When a user logs in using Phone Manager Pro, the internal IP Office extension will be logged off. The internal IP Office extension is logged in automatically after the user exits Phone Manager.

# 9. Verification

### 9.1. VPNremote Phone VPN Status

VPN status is available after the Avaya VPNremote Phone establishes an IPSec tunnel, registers with IP Office and becomes functional. From the telephone keypad, press the **OPTIONS** hard button ( $\sqrt{i}$  icon), then press the  $\blacktriangleright$  hard button to access the next screen. Select the **VPN Status...** option. Two screens of IPSec tunnel statistics are displayed. Use the  $\blacktriangleright$  hard button to access the next screen. Press the **Refresh** soft button to update the displayed statistics.

The statistics from Avaya VPNremote Phone used in the sample configuration are shown below.

VPN	Status
PKT S/R	474/574
FRAG RCVD	0
Comp/Decomp	0/0
Auth Failures	0
<b>Recv Errors</b>	0
Send Errors	0
Gateway	44.2.2.2
Outer IP	192.168.1.101
Inner IP	10.10.10.10
<b>Gateway Version</b>	KAME/raccoon
<b>Inactivity Timeout</b>	0
	DH2-3DES-SHA-120 hrs

## 9.2. NETGEAR FVX538 Debug and Logging

On the NETGEAR FVX538 WebUI, select **VPN**  $\rightarrow$  **Connection Status** from the top menu bar. The following screenshot shows the connection status of the VPN tunnels.

NETGEAR ProSafe™ - IPSe	c Connection Stat	tus - Microso	ft Internet Explorer		
<u>File E</u> dit <u>V</u> iew F <u>a</u> vorite	s <u>T</u> ools <u>H</u> elp				
🌏 Back 👻 🕥 👻 🔀	2 🏠 🔎	Search 🤸	Favorites 🧭 🔗	)• 🎍 🖃 🦓	
dress 🗃 http://44.1.1.254	/platform.cgi			💌 🄁 Go	Links 🎇 🌀 SnagIt 🖻
NETGE	A R'			NETGEAR ProSafe V	PN Firewall FVX538
Network Configura	tion Securi	ity   VPN :: Certifica	Administration	Monitoring   Web Su     :: VPN Client :: Connection	<b>upport   Logout  </b> 1 Status ::
IPSec Connection Sta	atus	C	peration succeede	ed.	
# Active IPSec SA(s	;)				?help
Policy Name	Endpoint	Tx (KB)	Tx (Packets)	State	Action
10.10.10.10*	33.1.1.150	158.59	508	IPsec SA Established	🧚 drop
192.168.1.105*	33.1.1.150	330.87	512	IPsec SA Established	🆩 drop
* Client Policy					
	Poll Inte	rval: 5	(Seconds) (Seconds)	interval 🖨 stop	

On the NETGEAR FVX538 WebUI, select **Monitoring**  $\rightarrow$  VPN Logs from the top menu bar. The NETGEAR FVX538 VPN Log shown below contains the IKE Phase1, IKE Phase2 and XAuth events logged as an Avaya VPNremote Phone establishes an IPSec tunnel. The screen below shows the events of a single Avaya VPNremote Phone successfully establishing an IPSec tunnel.

```
1970 Jan 1 00:01:43 [FVX538] [IKE] Remote configuration for identifier "avaya" found_
1970 Jan 1 00:01:43 [FVX538] [IKE] Received request for new phase 1 negotiation:
44.2.2.2[500]<=>33.1.1.150[2070]_
1970 Jan 1 00:01:43 [FVX538] [IKE] Beginning Aggressive mode._
1970 Jan 1 00:01:43 [FVX538] [IKE] Received unknown Vendor ID_
1970 Jan 1 00:01:43 [FVX538] [IKE] Received Vendor ID: draft-ietf-ipsec-nat-t-ike-02_
1970 Jan 1 00:01:43 [FVX538] [IKE] Received unknown Vendor ID
                 - Last output repeated 2 times -
1970 Jan 1 00:01:43 [FVX538] [IKE] Received Vendor ID: draft-ietf-ipsra-isakmp-xauth-06.txt_
1970 Jan 1 00:01:43 [FVX538] [IKE] For 33.1.1.150[2070], Selected NAT-T version: draft-ietf-
ipsec-nat-t-ike-02_
1970 Jan 1 00:01:45 [FVX538] [IKE] Floating ports for NAT-T with peer 33.1.1.150[4500]_
1970 Jan 1 00:01:45 [FVX538] [IKE] NAT-D payload matches for 44.2.2.2[4500]_
1970 Jan 1 00:01:45 [FVX538] [IKE] NAT-D payload does not match for 33.1.1.150[4500]_
1970 Jan 1 00:01:45 [FVX538] [IKE] NAT detected: Peer is behind a NAT device_
1970 Jan 1 00:01:45 [FVX538] [IKE] Sending Xauth request to 33.1.1.150[4500].
1970 Jan 1 00:01:45 [FVX538] [IKE] ISAKMP-SA established for 44.2.2.2[4500]-33.1.1.150[4500]
with spi:1ff20d555c1aea7a:31c367d492a950f0_
1970 Jan 1 00:01:45 [FVX538] [IKE] Received attribute type "ISAKMP_CFG_REPLY" from
33.1.1.150[4500]
1970 Jan 1 00:01:45 [FVX538] [IKE] Login succeeded for user "rich"_
1970 Jan 1 00:01:45 [FVX538] [IKE] Received attribute type "ISAKMP_CFG_REQUEST" from
33.1.1.150[4500]_
1970 Jan 1 00:01:45 [FVX538] [IKE] 10.10.10.10 IP address is assigned to remote peer
33.1.1.150[4500]_
1970 Jan 1 00:01:45 [FVX538] [IKE] Ignored attribute 5_
1970 Jan 1 00:01:45 [FVX538] [IKE] Ignored attribute 6_
1970 Jan 1 00:01:47 [FVX538] [IKE] Responding to new phase 2 negotiation:
44.2.2.2[0]<=>33.1.1.150[0]
1970 Jan 1 00:01:47 [FVX538] [IKE] Ignore INITIAL-CONTACT notification from 33.1.1.150[4500]
because it is only accepted after phase1._
1970 Jan 1 00:01:47 [FVX538] [IKE] Using IPsec SA configuration: 44.1.1.0/24<-
>10.10.10.0/24_
1970 Jan 1 00:01:47 [FVX538] [IKE] Adjusting peer's encmode 61443(61443)->Tunnel(1).
1970 Jan 1 00:01:49 [FVX538] [IKE] IPsec-SA established[UDP encap 4500->4500]: ESP/Tunnel
33.1.1.150->44.2.2.2 with spi=251917329(0xf03f411)
1970 Jan 1 00:01:49 [FVX538] [IKE] IPsec-SA established[UDP encap 4500->4500]: ESP/Tunnel
44.2.2.2->33.1.1.150 with spi=1478768541(0x5824379d)_
```

The NETGEAR FVX538 VPN Log shown below contains the IKE Phase1, IKE Phase2 events logged as a NETGEAR ProSafe VPN Client establishes an IPSec tunnel.

1970 Jan 1 00:26:15 [FVX538] [IKE] Remote configuration for identifier "fvx\_remote.com" found 1970 Jan 1 00:26:15 [FVX538] [IKE] Received request for new phase 1 negotiation: 44.2.2.2[500] <=>33.1.1.150[500] 1970 Jan 1 00:26:15 [FVX538] [IKE] Beginning Aggressive mode.\_ 1970 Jan 1 00:26:15 [FVX538] [IKE] Received unknown Vendor ID\_ - Last output repeated 2 times 1970 Jan 1 00:26:15 [FVX538] [IKE] Received Vendor ID: draft-ietf-ipsra-isakmp-xauth-06.txt 1970 Jan 1 00:26:15 [FVX538] [IKE] Received unknown Vendor ID 1970 Jan 1 00:26:15 [FVX538] [IKE] Received Vendor ID: draft-ietf-ipsec-nat-t-ike-02\_\_\_ 1970 Jan 1 00:26:15 [FVX538] [IKE] For 33.1.1.150[500], Selected NAT-T version: draftietf-ipsec-nat-t-ike-02 1970 Jan 1 00:26:16 [FVX538] [IKE] Floating ports for NAT-T with peer 33.1.1.150[27701]\_ 1970 Jan 1 00:26:16 [FVX538] [IKE] NAT-D payload matches for 44.2.2.2[4500]\_ 1970 Jan 1 00:26:16 [FVX538] [IKE] NAT-D payload does not match for 33.1.1.150[27701]\_ 1970 Jan 1 00:26:16 [FVX538] [IKE] Ignore REPLAY-STATUS notification from 33.1.1.150[27701]. 1970 Jan 1 00:26:16 [FVX538] [IKE] Ignore INITIAL-CONTACT notification from 33.1.1.150[27701] because it is only accepted after phase1.\_ 1970 Jan 1 00:26:16 [FVX538] [IKE] NAT detected: Peer is behind a NAT device 1970 Jan 1 00:26:16 [FVX538] [IKE] ISAKMP-SA established for 44.2.2.2[4500]-33.1.1.150[27701] with spi:0329354c4ce217e2:1bd3e066bf94373c\_ 1970 Jan 1 00:26:16 [FVX538] [IKE] Sending Informational Exchange: notify payload[INITIAL-CONTACT]\_ 1970 Jan 1 00:26:16 [FVX538] [IKE] Responding to new phase 2 negotiation: 44.2.2.2[0]<=>33.1.1.150[0] 1970 Jan 1 00:26:16 [FVX538] [IKE] Using IPsec SA configuration: 44.1.1.0/24<->0.0.0.0/0 from fvx\_remote.com\_ 1970 Jan 1 00:26:16 [FVX538] [IKE] No policy found, generating the policy : 192.168.1.105/32[0] 44.1.1.0/24[0] proto=any dir=in\_ 1970 Jan 1 00:26:16 [FVX538] [IKE] Adjusting peer's encmode 61443(61443)->Tunnel(1) 1970 Jan 1 00:26:16 [FVX538] [IKE] IPsec-SA established[UDP encap 27701->4500]: ESP/Tunnel 33.1.1.150->44.2.2.2 with spi=186021828(0xb1677c4)\_ 1970 Jan 1 00:26:16 [FVX538] [IKE] IPsec-SA established[UDP encap 4500->27701]: ESP/Tunnel 44.2.2.2->33.1.1.150 with spi=3180860194(0xbd981322)\_

### 9.3. NETGEAR ProSafe VPN Client Debug and Logging

Launch the NETGEAR ProSafe Log Viewer by selecting Start  $\rightarrow$  All Programs  $\rightarrow$  NETGEAR **ProSafe VPN Client**  $\rightarrow$  Connection Monitor. The NETGEAR ProSafe VPN Client Connection Monitor can be used to determine the connection status of the IPSec VPN tunnel.

NCo	nnection Monitor - NE	TGEAR ProSafe	/PN Client							
	Global Statistics Non-Secured Packets Dropped Packets	15836 Sed 2 Sed	ured Packets	525 71	<u>R</u> eset		Show Idle Connectio Freeze Display	ons	<u>C</u> lose Details	
Cor	nection Name	Local Address	Local Subnet	Remote Add	ress Remote	Modifier	GW Address	Protocol	Local Port	Rem Port
<b>⇔</b> ,	My Connections\netgear	192.168.001.105	&255.255.255.255	044.001.001.	000 &255.25	5.255.000	044.002.002.002	ALL	ALL	ALL

Launch the NETGEAR ProSafe VPN Client Log Viewer by selecting Start  $\rightarrow$  All Programs  $\rightarrow$  NETGEAR ProSafe VPN Client  $\rightarrow$  Log Viewer. The NETGEAR ProSafe VPN Client Log Viewer shown below contains the IKE Phase1, IKE Phase2 events logged as an IPSec tunnel is established.

```
2-21: 14:22:15.895
 2-21: 14:22:15.895 My Connections\netgear - Initiating IKE Phase 1 (IP
ADDR=44.2.2.2)
2-21: 14:22:16.161 My Connections\netgear - SENDING>>>> ISAKMP OAK AG (SA, KE, NON,
ID, VID 6x)
2-21: 14:22:16.598 My Connections\netgear - RECEIVED<<< ISAKMP OAK AG (SA, KE, NON,
ID, HASH, VID 3x, NAT-D 2x, VID)
2-21: 14:22:16.598 My Connections\netgear - Peer is NAT-T draft-02 capable
2-21: 14:22:16.598 My Connections\netgear - NAT is detected for Client
2-21: 14:22:16.598 My Connections\netgear - Floating to IKE non-500 port
2-21: 14:22:16.739 My Connections\netgear - SENDING>>>> ISAKMP OAK AG *(HASH, NAT-D
2x, NOTIFY:STATUS_REPLAY_STATUS, NOTIFY:STATUS_INITIAL_CONTACT)
2-21: 14:22:16.739 My Connections\netgear - Established IKE SA
2-21: 14:22:16.739 My Connections\netgear - MY COOKIE 3 29 35 4c 4c e2 17 e2
2-21: 14:22:16.739 My Connections\netgear - HIS COOKIE 1b d3 e0 66 bf 94 37 3c
 2-21: 14:22:16.973 My Connections\netgear - Initiating IKE Phase 2 with Client IDs
(message id: 5EE6A314)
 2-21: 14:22:16.973 My Connections\netgear -
                                                 Initiator = IP ADDR=192.168.1.105,
prot = 0 port = 0
2-21: 14:22:16.973 My Connections\netgear - Responder = IP
SUBNET/MASK=44.1.1.0/255.255.255.0, prot = 0 port = 0
2-21: 14:22:16.973 My Connections\netgear - SENDING>>>> ISAKMP OAK QM *(HASH, SA,
NON, KE, ID 2x)
2-21: 14:22:16.973 My Connections\netgear - RECEIVED<<< ISAKMP OAK INFO *(HASH,
NOTIFY:STATUS_INITIAL_CONTACT)
2-21: 14:22:17.286 My Connections\netgear - RECEIVED<<< ISAKMP OAK QM *(HASH, SA,
NON, KE, ID 2x)
2-21: 14:22:17.286 My Connections\netgear - Filter entry 3 added: SECURE
192.168.001.105&255.255.255.255 044.001.001.000&255.255.255.000 044.002.002.002
 2-21: 14:22:17.286 My Connections\netgear - SENDING>>>> ISAKMP OAK QM *(HASH)
2-21: 14:22:17.333 My Connections\netgear - Loading IPSec SA (Message ID = 5EE6A314
OUTBOUND SPI = B1677C4 INBOUND SPI = BD981322)
```

# 10. Testing

The interoperability testing focused on verifying interoperability between the Avaya VPNremote Phone and Phone Manager Pro in Telecommuter mode and the Avaya IP Office using the configuration shown in **Figure 1**.

The following features were successfully tested in this configuration:

- 1. Basic operations that include call origination, termination, hold, transfer, and conference functionality.
- 2. Voicemail and Message Waiting Indication
- 3. Hunt Group operation at the Avaya VPNremote Phone and Phone Manager Pro.
- 4. Bridged and Line Appearance buttons at the Avaya VPNremote Phone.
- 5. Mobile Twinning at the Avaya VPNremote Phone.

A remote worker when using the Phone Manager Pro in telecommuter mode <u>does not</u> have the same functionality as a telephone co-located with the IP office. **Phone Manager Pro limitations are**:

- 1. Single Line appearance.
- 2. No bridged call appearances at the Phone Manager Pro or of the Phone Manager Pro extension at other IP Office users when in this mode.
- 3. The Mobile Twinning feature is not available when using the Phone Manager Pro.

## 11. Troubleshooting

This section offers some common configuration mismatches to assist in troubleshooting.

### 11.1. Incorrect User Name or Password

#### • Avaya VPNremote Phone display:

The display shows the following: Retrying in 7200 Secs Invalid password OR user name Press Edit to modify VPN Press MORE to see details

Press the **More** soft button to display the following: Showing Error 1/1 Invalid password OR user name Error Code: 3997700:0 Module:IKECFG:430

### • NETGEAR FVX538 WebUI: Monitoring → VPN Logs

```
1970 Jan 1 00:07:11 [FVX538] [IKE] Remote configuration for identifier "avaya"
found_
1970 Jan 1 00:07:11 [FVX538] [IKE] Received request for new phase 1 negotiation:
44.2.2.2[500] <=>33.1.1.150[2070]
1970 Jan 1 00:07:11 [FVX538] [IKE] Beginning Aggressive mode.
1970 Jan 1 00:07:11 [FVX538] [IKE] Received unknown Vendor ID_
1970 Jan 1 00:07:11 [FVX538] [IKE] Received Vendor ID: draft-ietf-ipsec-nat-t-ike-
02
1970 Jan 1 00:07:11 [FVX538] [IKE] Received unknown Vendor ID_
                  - Last output repeated 2 times -
1970 Jan 1 00:07:11 [FVX538] [IKE] Received Vendor ID: draft-ietf-ipsra-isakmp-
xauth-06.txt_
1970 Jan 1 00:07:11 [FVX538] [IKE] For 33.1.1.150[2070], Selected NAT-T version:
draft-ietf-ipsec-nat-t-ike-02_
1970 Jan 1 00:07:13 [FVX538] [IKE] Floating ports for NAT-T with peer
33.1.1.150[4500]_
1970 Jan 1 00:07:13 [FVX538] [IKE] NAT-D payload matches for 44.2.2.2[4500]_
1970 Jan 1 00:07:13 [FVX538] [IKE] NAT-D payload does not match for
33.1.1.150[4500]_
1970 Jan 1 00:07:13 [FVX538] [IKE] NAT detected: Peer is behind a NAT device_
1970 Jan 1 00:07:13 [FVX538] [IKE] Sending Xauth request to 33.1.1.150[4500]
1970 Jan 1 00:07:13 [FVX538] [IKE] ISAKMP-SA established for 44.2.2.2[4500]-
33.1.1.150[4500] with spi:3f03ccbff2fe21e2:de07e15640ea38b8_
1970 Jan 1 00:07:13 [FVX538] [IKE] Received attribute type "ISAKMP_CFG_REPLY" from
33.1.1.150[4500]
1970 Jan 1 00:07:13 [FVX538] [IKE] 0.0.0.0 IP address has been released by remote
peer._
1970 Jan 1 00:07:13 [FVX538] [IKE] Login failed for user "joe"_
1970 Jan 1 00:07:13 [FVX538] [IKE] Sending Informational Exchange: delete payload[]_
           1 00:07:13 [FVX538] [IKE] Failed to find proper address pool with id -1_
1970 Jan
1970 Jan 1 00:07:13 [FVX538] [IKE] an undead schedule has been deleted: 'ph1_main'.
1970 Jan 1 00:07:13 [FVX538] [IKE] Received mode config from 33.1.1.150[4500], but
we do not have ISAKMP-SA._
```

Solution & Interoperability Test Lab Application Notes ©2008 Avaya Inc. All Rights Reserved. • NETGEAR ProSafe VPN Client → Log Viewer



### 11.2. Mismatched Phase 1 Proposal

#### • Avaya VPNremote Phone display:

Retrying in 30 Secs IKE Phasel no response Press EDIT to modify VPN Press MORE to see details

Press the **More** soft button to display the following: Showing Error 1/2 Error Code: 3997700:0 Module:IKMPD:142

Press the Next soft button to display the following: Showing Error 2/2 Error Code: 3997700:0 Module:IKECFG:459 • NETGEAR FVX538 WebUI: Monitoring → VPN Logs

```
1970 Jan 1 00:27:40 [FVX538] [IKE] Remote configuration for identifier "avaya"
found_
1970 Jan 1 00:27:40 [FVX538] [IKE] Received request for new phase 1 negotiation:
44.2.2.2[500] <=>33.1.1.150[2070]
1970 Jan 1 00:27:40 [FVX538] [IKE] Beginning Aggressive mode._
1970 Jan 1 00:27:40 [FVX538] [IKE] Received unknown Vendor ID_
1970 Jan 1 00:27:40 [FVX538] [IKE] Received Vendor ID: draft-ietf-ipsec-nat-t-
ike-02___
1970 Jan 1 00:27:40 [FVX538] [IKE] Received unknown Vendor ID_
                  - Last output repeated 2 times -
1970 Jan 1 00:27:40 [FVX538] [IKE] Received Vendor ID: draft-ietf-ipsra-isakmp-
xauth-06.txt_
1970 Jan 1 00:27:40 [FVX538] [IKE] For 33.1.1.150[2070], Selected NAT-T version:
draft-ietf-ipsec-nat-t-ike-02_
1970 Jan 1 00:27:40 [FVX538] [IKE] Rejected phase 1 proposal as Peer's hashtype
"MD5" mismatched with Local "SHA"._
1970 Jan 1 00:27:40 [FVX538] [IKE] No suitable proposal found for
33.1.1.150[2070].
1970 Jan 1 00:27:40 [FVX538] [IKE] Failed to get valid proposal for
33.1.1.150[2070]._
```

• NETGEAR ProSafe VPN Client → Log Viewer

```
2-21: 16:14:13.051 My Connections\netgear - Initiating IKE Phase 1 (IP
ADDR=44.2.2.2)
 2-21: 16:14:13.239 My Connections\netgear - SENDING>>>> ISAKMP OAK AG (SA, KE,
NON, ID, VID 6x)
2-21: 16:14:28.567 My Connections\netgear - message not received!
Retransmitting!
2-21: 16:14:28.567 My Connections\netgear - SENDING>>>> ISAKMP OAK AG
(Retransmission)
 2-21: 16:14:43.708 My Connections\netgear - message not received!
Retransmitting!
 2-21: 16:14:43.708 My Connections\netgear - SENDING>>>> ISAKMP OAK AG
(Retransmission)
 2-21: 16:14:58.739 My Connections\netgear - message not received!
Retransmitting!
 2-21: 16:14:58.739 My Connections\netgear - SENDING>>>> ISAKMP OAK AG
(Retransmission)
2-21: 16:15:13.739 My Connections\netgear - Exceeded 3 IKE SA negotiation
attempts
```

### 11.3. Mismatched Phase 2 Proposal

• Avaya VPNremote Phone display:

Retrying in 30 Secs IKE Phase2 no response Press EDIT to modify VPN Press MORE to see details

Press the **More** soft button to display the following: Showing Error 1/2 IKE Phase2 proposal mismatch Error Code: 3997698:14 Module:NOTIFY:444

Press the **Next** soft button to display the following: Showing Error 2/2 IKE Phase2 no response Error Code: 3997700:0 Module:IKECFG:1184

#### NETGEAR FVX538 WebUI: Monitoring → VPN Logs

1970 Jan 1 00:57:32 [FVX538] [IKE] Remote configuration for identifier "avaya" found 1970 Jan 1 00:57:32 [FVX538] [IKE] Received request for new phase 1 negotiation: 44.2.2.2[500]<=>33.1.1.150[2070]\_ 1970 Jan 1 00:57:32 [FVX538] [IKE] Beginning Aggressive mode.\_ 1 00:57:32 [FVX538] [IKE] Received unknown Vendor ID\_ 1970 Jan 1970 Jan 1 00:57:32 [FVX538] [IKE] Received Vendor ID: draft-ietf-ipsec-nat-t-ike-02 1970 Jan 1 00:57:32 [FVX538] [IKE] Received unknown Vendor ID\_ - Last output repeated 2 times -1970 Jan 1 00:57:32 [FVX538] [IKE] Received Vendor ID: draft-ietf-ipsra-isakmpxauth-06.txt\_ 1970 Jan 1 00:57:32 [FVX538] [IKE] For 33.1.1.150[2070], Selected NAT-T version: draft-ietf-ipsec-nat-t-ike-02\_ 1970 Jan 1 00:57:34 [FVX538] [IKE] Floating ports for NAT-T with peer 33.1.1.150[4500] 1970 Jan 1 00:57:34 [FVX538] [IKE] NAT-D payload matches for 44.2.2.2[4500]\_ 1970 Jan 1 00:57:34 [FVX538] [IKE] NAT-D payload does not match for 33.1.1.150[4500] 1970 Jan 1 00:57:34 [FVX538] [IKE] NAT detected: Peer is behind a NAT device\_ 1970 Jan 1 00:57:34 [FVX538] [IKE] Sending Xauth request to 33.1.1.150[4500]\_ 1970 Jan 1 00:57:34 [FVX538] [IKE] ISAKMP-SA established for 44.2.2.2[4500]-33.1.1.150[4500] with spi:a618784f357856ae:4facabc6c9e2d690\_ 1970 Jan 1 00:57:34 [FVX538] [IKE] Received attribute type "ISAKMP\_CFG\_REPLY" from 33.1.1.150[4500] 1970 Jan 1 00:57:34 [FVX538] [IKE] Login succeeded for user "rich"\_ 1970 Jan 1 00:57:34 [FVX538] [IKE] Received attribute type "ISAKMP\_CFG\_REQUEST" from 33.1.1.150[4500] 1970 Jan 1 00:57:34 [FVX538] [IKE] 10.10.10 IP address is assigned to remote peer 33.1.1.150[4500]\_ 1970 Jan 1 00:57:34 [FVX538] [IKE] Ignored attribute 5\_ 1970 Jan 1 00:57:34 [FVX538] [IKE] Ignored attribute 6\_ 1970 Jan 1 00:57:36 [FVX538] [IKE] Responding to new phase 2 negotiation: 44.2.2.2[0]<=>33.1.1.150[0] 1970 Jan 1 00:57:36 [FVX538] [IKE] Ignore INITIAL-CONTACT notification from 33.1.1.150[4500] because it is only accepted after phase1.\_ 1970 Jan 1 00:57:36 [FVX538] [IKE] Using IPsec SA configuration: 44.1.1.0/24<->10.10.10.0/24\_ 1970 Jan 1 00:57:36 [FVX538] [IKE] Adjusting peer's encmode 61443(61443)->Tunnel(1)\_ 1970 Jan 1 00:57:36 [FVX538] [IKE] Peer's Proposal:\_ 1970 Jan 1 00:57:36 [FVX538] [IKE] (proto\_id=ESP spisize=4 spi=d84b94af spi p=00000000 encmode=Tunnel regid=0:0) 1970 Jan 1 00:57:36 [FVX538] [IKE] (trns\_id=3DES encklen=0 authtype=hmac-md5)\_ 1970 Jan 1 00:57:36 [FVX538] [IKE] Local Proposal:\_ 1970 Jan 1 00:57:36 [FVX538] [IKE] (proto\_id=ESP spisize=4 spi=00000000 spi\_p=00000000 encmode=Tunnel regid=4500:4500)\_ 1970 Jan 1 00:57:36 [FVX538] [IKE] (trns\_id=3DES\_encklen=0\_authtype=hmac-sha) 1970 Jan 1 00:57:36 [FVX538] [IKE] Phase 2 proposal by 33.1.1.150[0] did not match.\_ 1970 Jan 1 00:57:36 [FVX538] [IKE] No suitable policy found for 33.1.1.150[0]\_ 1970 Jan 1 00:57:36 [FVX538] [IKE] Sending Informational Exchange: notify payload[NO-PROPOSAL-CHOSEN]\_ 1970 Jan 1 00:57:36 [FVX538] [IKE] Responding to new phase 2 negotiation: 44.2.2.2[0]<=>33.1.1.150[0] 1970 Jan 1 00:57:36 [FVX538] [IKE] Ignore INITIAL-CONTACT notification from 33.1.1.150[4500] because it is only accepted after phase1.\_ 1970 Jan 1 00:57:36 [FVX538] [IKE] Using IPsec SA configuration: 44.1.1.0/24<->10.10.10.0/24

Solution & Interoperability Test Lab Application Notes ©2008 Avava Inc. All Rights Reserved. IPO-NTGR-FVX538.doc • NETGEAR ProSafe VPN Client → Log Viewer

```
2-21: 16:26:25.739 My Connections\netgear - Initiating IKE Phase 1 (IP ADDR=44.2.2.2)
 2-21: 16:26:25.989 My Connections\netgear - SENDING>>>> ISAKMP OAK AG (SA, KE, NON,
ID. VID 6x)
 2-21: 16:26:26.411 My Connections\netgear - RECEIVED<<< ISAKMP OAK AG (SA, KE, NON,
ID, HASH, VID 3x, NAT-D 2x, VID)
 2-21: 16:26:26.411 My Connections\netgear - Peer is NAT-T draft-02 capable
 2-21: 16:26:26.411 My Connections\netgear - NAT is detected for Client
 2-21: 16:26:26.411 My Connections\netgear - Floating to IKE non-500 port
2-21: 16:26:26.520 My Connections\netgear - SENDING>>>> ISAKMP OAK AG *(HASH, NAT-D
2x, NOTIFY:STATUS_REPLAY_STATUS, NOTIFY:STATUS_INITIAL_CONTACT)
 2-21: 16:26:26.520 My Connections\netgear - Established IKE SA
 2-21: 16:26:26.520 My Connections\netgear - MY COOKIE bl 2d 5c c8 4f ba 14 la
2-21: 16:26:26.520 My Connections\netgear - HIS COOKIE 33 de 7c 5f 3c ff bl aa
 2-21: 16:26:26.676 My Connections\netgear - Initiating IKE Phase 2 with Client IDs
(message id: 3DECF9A5)
 2-21: 16:26:26.676 My Connections\netgear -
                                                       Initiator = IP ADDR=192.168.1.105, prot
= 0 \text{ port} = 0
2-21: 16:26:26.676 My Connections\netgear -
                                                       Responder = IP
SUBNET/MASK=44.1.1.0/255.255.255.0, prot = 0 port = 0
 2-21: 16:26:26.676 My Connections\netgear - SENDING>>>> ISAKMP OAK QM *(HASH, SA,
NON, KE, ID 2x)
 2-21: 16:26:26.676 My Connections\netgear - RECEIVED<<< ISAKMP OAK INFO *(HASH,
NOTIFY:STATUS_INITIAL_CONTACT)
2-21: 16:26:26.879 My Connections\netgear - RECEIVED<<< ISAKMP OAK INFO *(HASH,
NOTIFY:NO_PROPOSAL_CHOSEN)
 2-21: 16:26:26.879 My Connections\netgear - Discarding IPSec SA negotiation
 2-21: 16:26:26.895 My Connections\netgear - Discarding IKE SA negotiation
 2-21: 16:26:26.895 My Connections\netgear - Deleting IKE SA (IP ADDR=44.2.2.2)
2-21: 16:26:26.895 My Connections\netgear - MY COOKIE bl 2d 5c c8 4f ba 14 la
2-21: 16:26:26.895 My Connections\netgear - HIS COOKIE 33 de 7c 5f 3c ff bl aa
 2-21: 16:26:26.895 My Connections\netgear - SENDING>>>> ISAKMP OAK INFO *(HASH, DEL)
```

# 12. Conclusion

The Avaya VPNremote Phone and Phone Manager Pro combined with NETGEAR FVX538 ProSafe VPN Firewall and NETGEAR ProSafe VPN client provide a secure solution for remote worker telephony over broadband Internet connection.

# 13. Definitions and Abbreviations

DHCP	Dynamic Host Configuration Protocol
IKE	Internet Key Exchange (An IPSec control protocol)
ISAKMP	Internet Security Association and Key Management Protocol
IPSec	Internet Protocol Security
MD5	Message Digest 5
NAT	Network Address Translation
PFS	Perfect Forward Secret
Phase 1	IKE negotiations used to create an ISAKMP security association.
Phase 2	IKE negotiations used to create IPSec security associations.
RTP	Real-Time Transport Protocol
SA	Security Association
SHA-1	Secure Hash Algorithm 1
VPN	Virtual Private Network

The following terminology is used throughout this document.

## 14. References

#### Avaya Application Notes and Resources Web Site:

http://www.avaya.com/gcm/master-usa/en-us/resource/index.htm

#### Avaya Product Support Web Site:

http://support.avaya.com/japple/css/japple?PAGE=Home

- [1] Application Notes for Converting an Avaya 4600 Series IP Telephone to an Avaya VPNremote Phone Issue 1.0.
- [2] Avaya VPNremote for the 4600 Series IP Telephones Release 2.1 Administrator Guide, Doc ID: 19-600753, Issue 3, June 2007
- [3] Administrators Guide for Avaya IP Office, Doc ID: 39DHB0002UKAA, October 2007.
- [4] IP Office 4.1 Phone Manager User Guide, Doc ID: 15-600988 Issue 16c, October, 2007.

#### **NETGEAR Product Support Web Site:**

http://www.netgear.com

- [5] NETGEAR FVX538 ProSafe VPN Firewall 200 Installation Guide, 201-10595-02, June 2006.
- [6] NETGEAR FVX538 ProSafe VPN Firewall 200 Reference Manual, v1.0, 202-10062-04, August 2006.

#### ©2008 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 DevConnect Program at <u>devconnect@avaya.com</u>.