Avaya Solution & Interoperability Test Lab

Configuring Netgear ProSafe VPN Firewall FVX538 to Support Avaya VPNremote Phones using Xauth – Issue 1.0

Abstract

These Application Notes describe the steps to configure the Netgear ProSafe VPN Firewall FVX538 to support IPSec tunnel termination using Xauth authentication for Avaya VPNremote Phone.

1. Introduction

These Application Notes describe the steps to configure the Netgear ProSafe VPN Firewall FVX538 (FVX538) to support IPSec tunnel termination using Extended Authentication (Xauth) for the Avaya VPNremote Phone.

The Avaya VPNremote Phone is a software based IPSec Virtual Private Network (VPN) client integrated into the firmware of an Avaya IP 4600 Series 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 Telephone models supporting the Avaya VPNremote Phone firmware include the 4610SW, 4620SW, 4621SW, 4622SW and 4625SW.

Avaya VPNremote Phone firmware, used in these Application Notes, extends the support of head-end VPN gateways to include FVX538. The configuration steps described in these Application Notes utilize a FVX538 using the software version specified in **Table 1**.

The Avaya VPNremote Phone utilizes the Internet Key Exchange (IKE) protocol for IPSec tunnel establishment and authentication with the FVX538 Xauth allows security gateways to perform user authentication in a separate phase after the IKE authentication phase 1 exchange is complete. Avaya VPNremote Phone uses the pre-shared key to authenticate with the FVX538 and create a temporary secure path to allow Avaya VPNremote Phone end user to present credentials to the FVX538. After user authentication is successful, the FVX538 sends an IP address from a pre-configured IP Address Pool to Avaya VPNremote Phone.

1.1. Avaya VPNremote Phone Startup Events

The steps shown in **Figure 1** below describe the high level events that take place during the startup of a VPNremote Phone. The focus of these Application Notes is on the configuration of the Avaya VPNremote Phone and the FVX538 functioning as the IPSec VPN head-end.

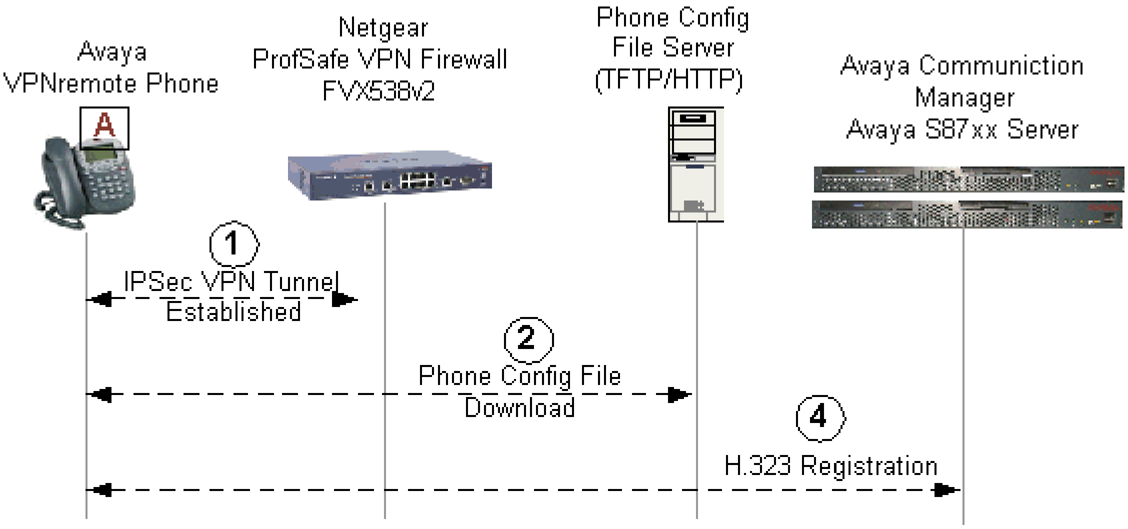


Figure 1: Avaya VPNremote Phone Startup Events

1. Avaya VPNremote Phone establishes an IPSec VPN tunnel upon boot up with the designated IPSec VPN head-end.

2. Avaya VPNremote Phone initiates a TFTP or HTTPS session with the phone configuration file server for configuration file download. (46vpnuprgade.scr, 46vpnsetting.txt, 46xxsettings.txt)

3. Avaya VPNremote Phone registers with Avaya Communication Manager and is ready for service.

2. Network Topology

The sample network implemented for these Application Notes is shown in **Figure 2.** The Corporate IP Network location contains the FVX538 functioning as a perimeter security device and VPN head-end. The Avaya S8710 Server and Avaya G650 Media Gateway are also located at the Corporate IP Network.

The Avaya VPNremote Phones are located in the public network and configured to establish an IPSec tunnel to the Public IP address of the FVX538. The 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 Communication Manager.

Avaya Communication Manager maps Avaya VPNremote Phones to the appropriate IP Network Region using this inner IP address and applies the IP Network Region specific parameters to Avaya VPNremote Phone. In these Application Notes, the G.729 codec with three 10ms voice samples per packet is assigned to Avaya VPNremote Phones.

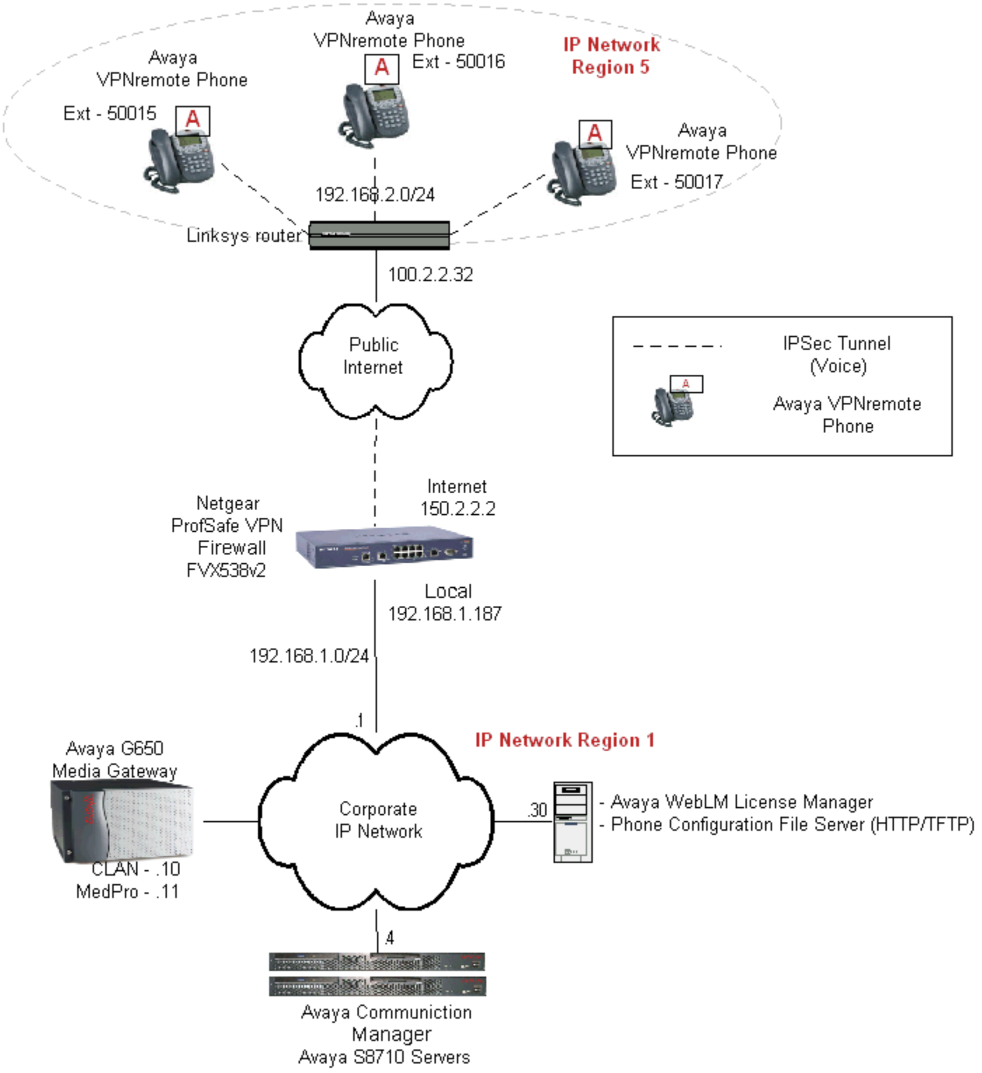


Figure 2: Network Diagram

3. Equipment and Software Validated

Table 1 lists the equipment and software/firmware versions used in the sample configuration provided.

Equipment	Software Version
Avaya S8710 Server with G650 Media Gateway	Avaya Communication Manager 4.0.1 (R014x.00.1.731.2)
Avaya 4610SW IP Telephones	R2.3.2 – **Release 2** (a10b**VPN**232_1.bin)
Netgear ProSafe VPN Firewall FVX538	2.1.2-7

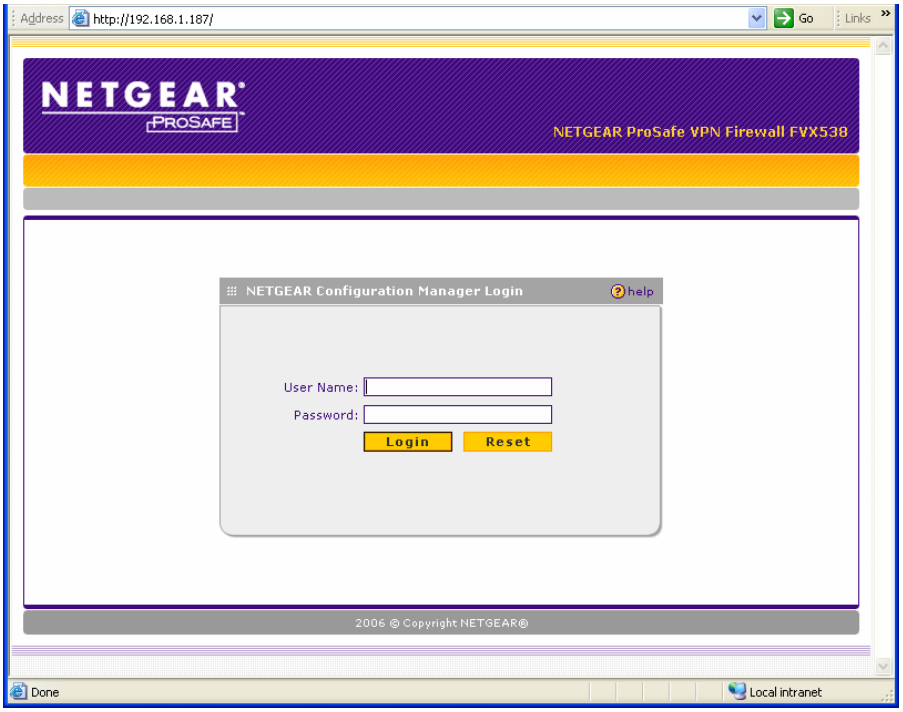
Table 1 – Equipment Version Information

4. Netgear ProSafe VPN Firewall FVX538 Configuration

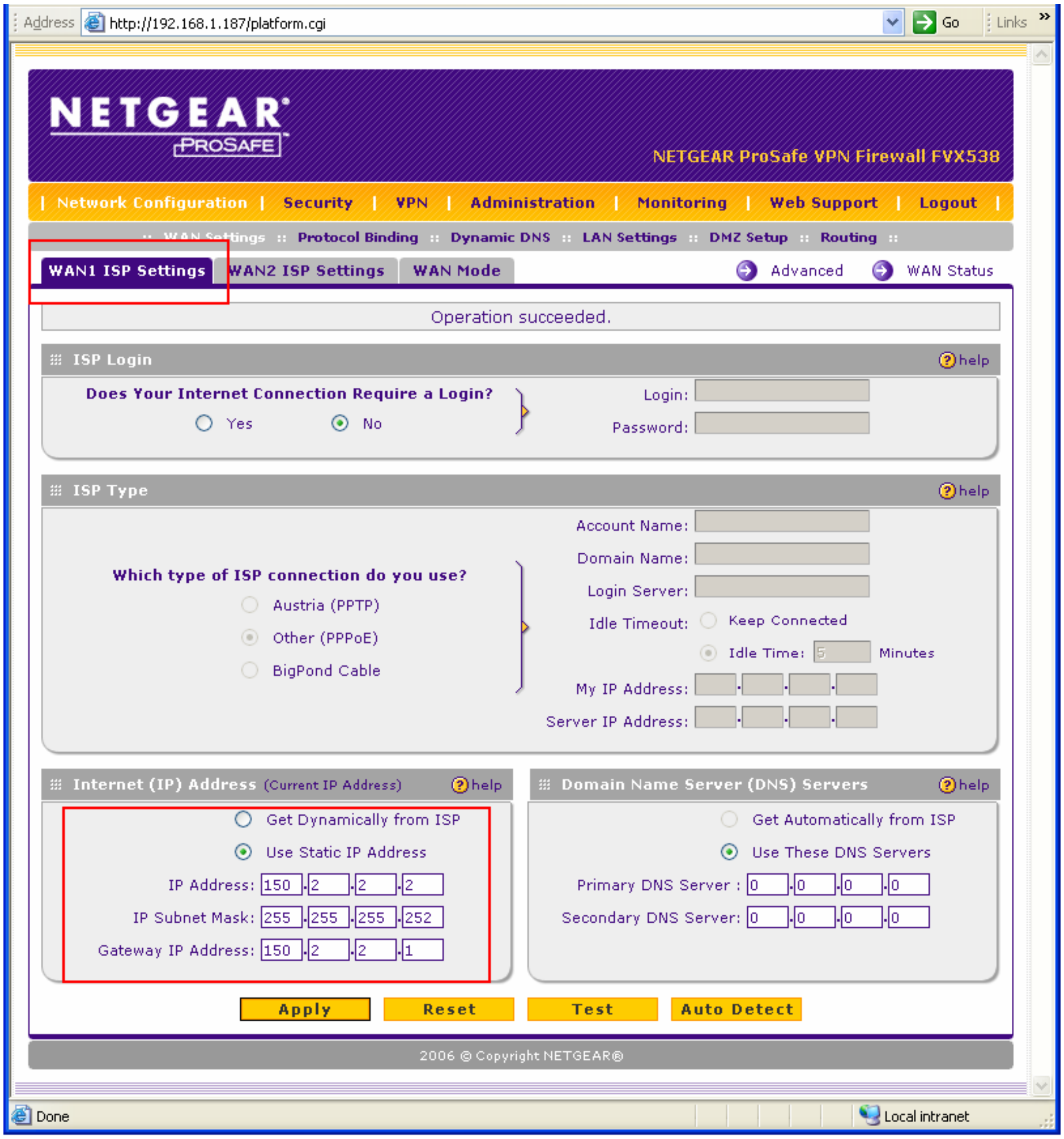
4.1. Access

These Application Notes assume the FVX538 have been configure with basic IP connectivity and is connected into the network. The FVX538 depicted in **Figure-2** has been configured with IP address 192.168.1.187 as its local IP address.

1. From a web browser, enter the FVX538 IP address of the local interface as the URL, **http://<IP address of FVX538>,** and the following FVX538 screen appears. Log in using appropriate User Name and Password.



2. Defined the WAN1 ISP Settins by selecting **Network Configuration →WAN Settings →WAN1 ISP Settins** from the top menu bar. The WAN1 interface is assigned IP address 150.2.2.2/30 in the sample network.


Address http://192.168.1.187/platform.cgi
Go
Links
NETGEAR PROSAFE
NETGEAR ProSafe VPN Firewall FVX538
| Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout |
:: WAN Settings :: Protocol Binding :: Dynamic DNS :: LAN Settings :: DMZ Setup :: Routing ::
WAN1 ISP Settings
WAN2 ISP Settings
WAN Mode
Advanced
WAN Status
help
Apply
Reset
Test
Auto Detect
2006 © Copyright NETGEAR®
Done
Local intranet

Operation succeeded.

ISP Login

Does Your Internet Connection Require a Login?

○ Yes ● No

Login:

Password:

ISP Type

Which type of ISP connection do you use?

○ Austria (PPTP)

● Other (PPPoE)

○ BigPond Cable

Account Name:

Domain Name:

Login Server:

Idle Timeout: ○ Keep Connected

● Idle Time: 5 Minutes

My IP Address: . . .

Server IP Address: . . .

Internet (IP) Address (Current IP Address)

○ Get Dynamically from ISP

● Use Static IP Address

IP Address: 150 . 2 . 2 . 2

IP Subnet Mask: 255 . 255 . 255 . 252

Gateway IP Address: 150 . 2 . 2 . 1

Domain Name Server (DNS) Servers

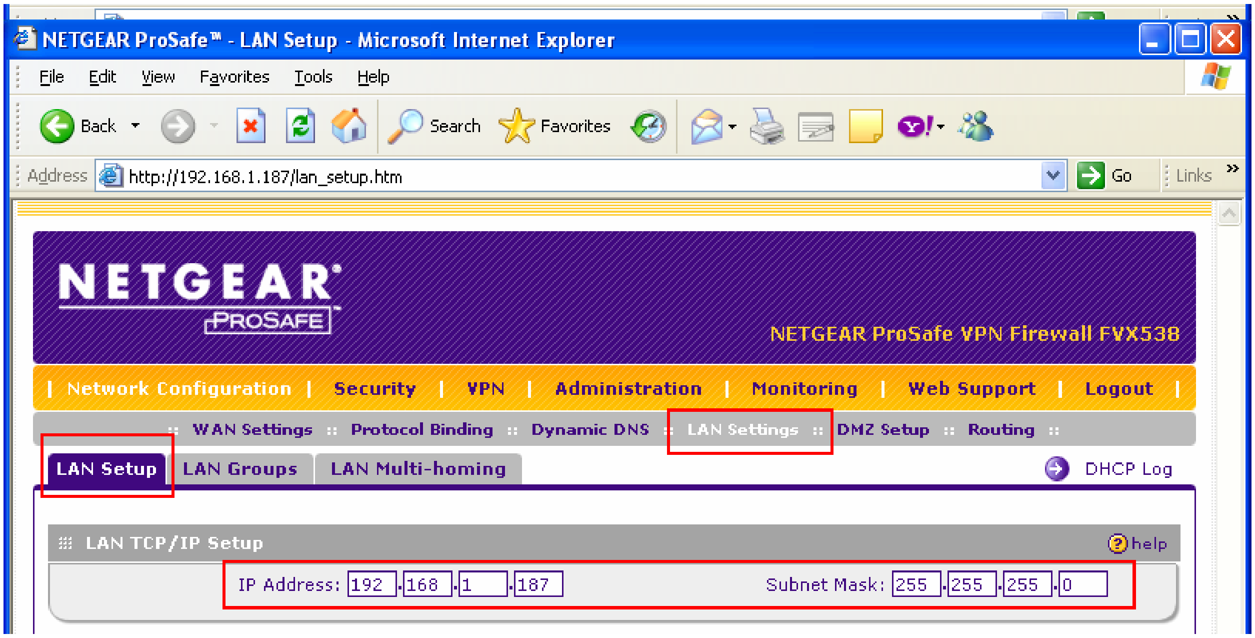
○ Get Automatically from ISP

● Use These DNS Servers

Primary DNS Server : 0 . 0 . 0 . 0

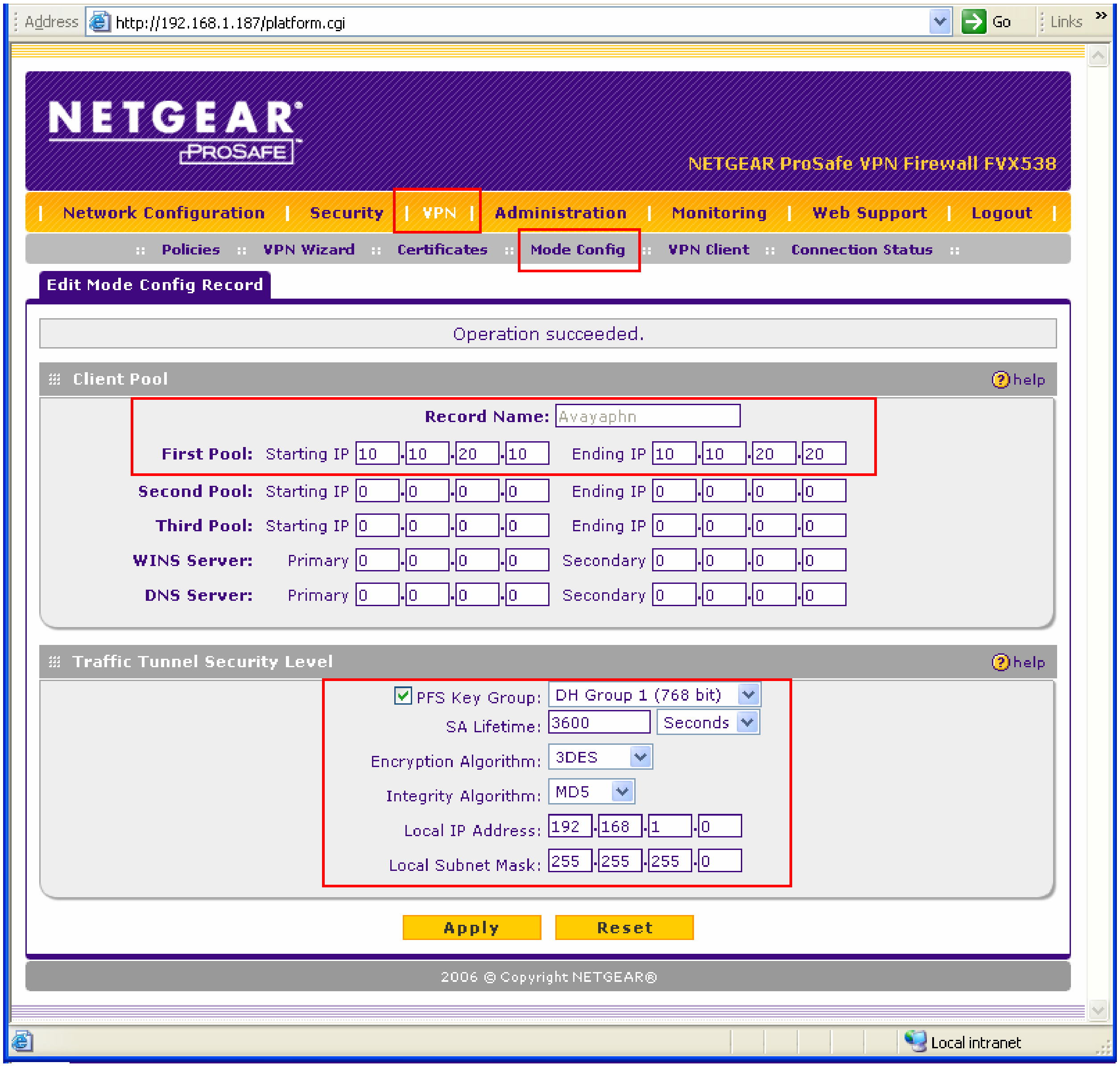
Secondary DNS Server: 0 . 0 . 0 . 0

3. Defined the LAN IP address by selecting **Network Configuration →LAN Settings → LAN Setup** from the top menu bar. The sample network uses IP address 192.168.1.187 with a network mask of 255.255.255.0.


NETGEAR ProSafe™ - LAN Setup - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.1.187/lan_setup.htm Go Links
NETGEAR PROSAFE
NETGEAR ProSafe VPN Firewall FVX538
Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout
WAN Settings :: Protocol Binding :: Dynamic DNS :: LAN Settings :: DMZ Setup :: Routing
LAN Setup LAN Groups LAN Multi-homing DHCP Log
LAN TCP/IP Setup help

IP Address: 192 . 168 . 1 . 187 Subnet Mask: 255 . 255 . 255 . 0

4. Select **VPN → Mode Config** to display the Edit Mode Config Record screen shown. The IKE Policies, Mode Config, and VPN Client under the **VPN** menu option must be administered in order to setup VPN for Avaya VPNremote Phone. The following screen capture shows the **Mode Config** used in the sample configuration. The **Mode Config** is used to define the IP address range to be assigned to Avaya VPNremote Phone and the authentication and encryption method used for tunnel traffic by the FVX538 gateway. In the sample network, the **Mode Config** named **Avayaphn** is set to assign an IP address from the First Pool which is defined as 10.10.20.10 – 10.10.20.20 inclusively. Furthermore, the **Mode Config** defines the Hashing algorithm (DH Group 1), encryption (3 DES), and the Integrity (MD5) algorithm used for tunnel establishment.



Operation succeeded.

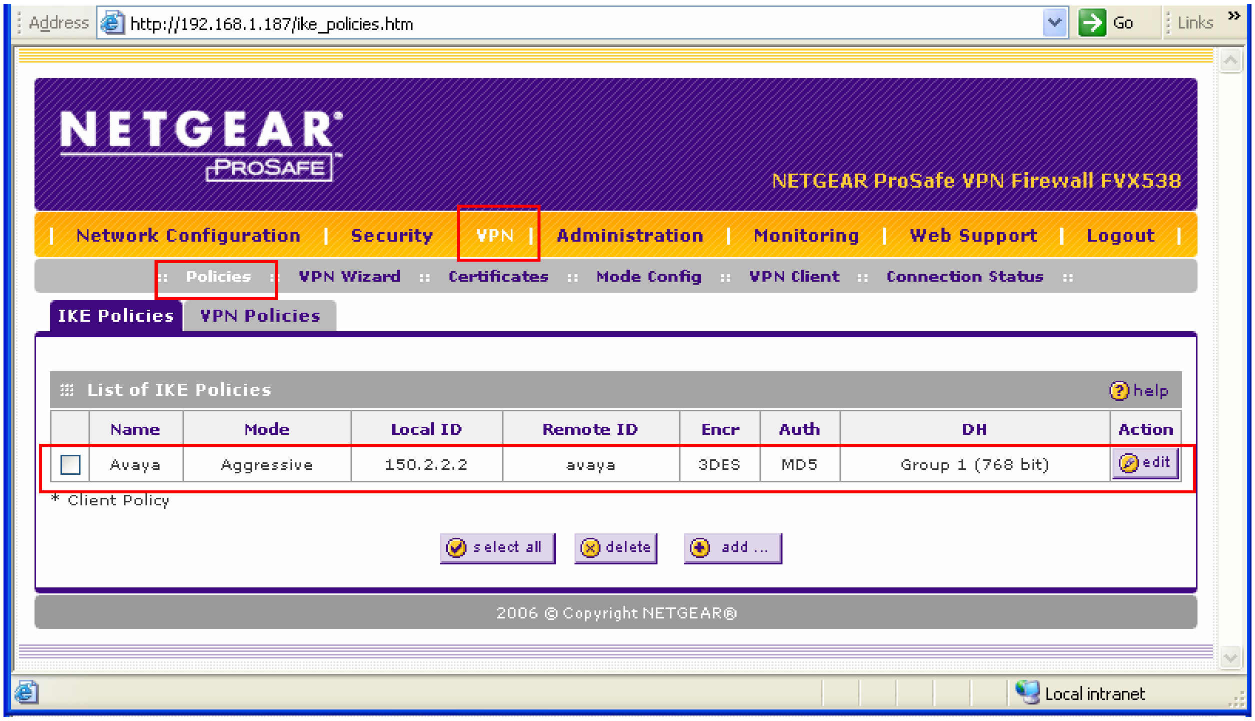
Client Pool

Record Name:	Avayaphn			
First Pool:	Starting IP	10 . 10 . 20 . 10	Ending IP	10 . 10 . 20 . 20
Second Pool:	Starting IP	0 . 0 . 0 . 0	Ending IP	0 . 0 . 0 . 0
Third Pool:	Starting IP	0 . 0 . 0 . 0	Ending IP	0 . 0 . 0 . 0
WINS Server:	Primary	0 . 0 . 0 . 0	Secondary	0 . 0 . 0 . 0
DNS Server:	Primary	0 . 0 . 0 . 0	Secondary	0 . 0 . 0 . 0

Traffic Tunnel Security Level

☑ PFS Key Group: DH Group 1 (768 bit)
SA Lifetime: 3600 Seconds
Encryption Algorithm: 3DES
Integrity Algorithm: MD5
Local IP Address: 192 . 168 . 1 . 0
Local Subnet Mask: 255 . 255 . 255 . 0

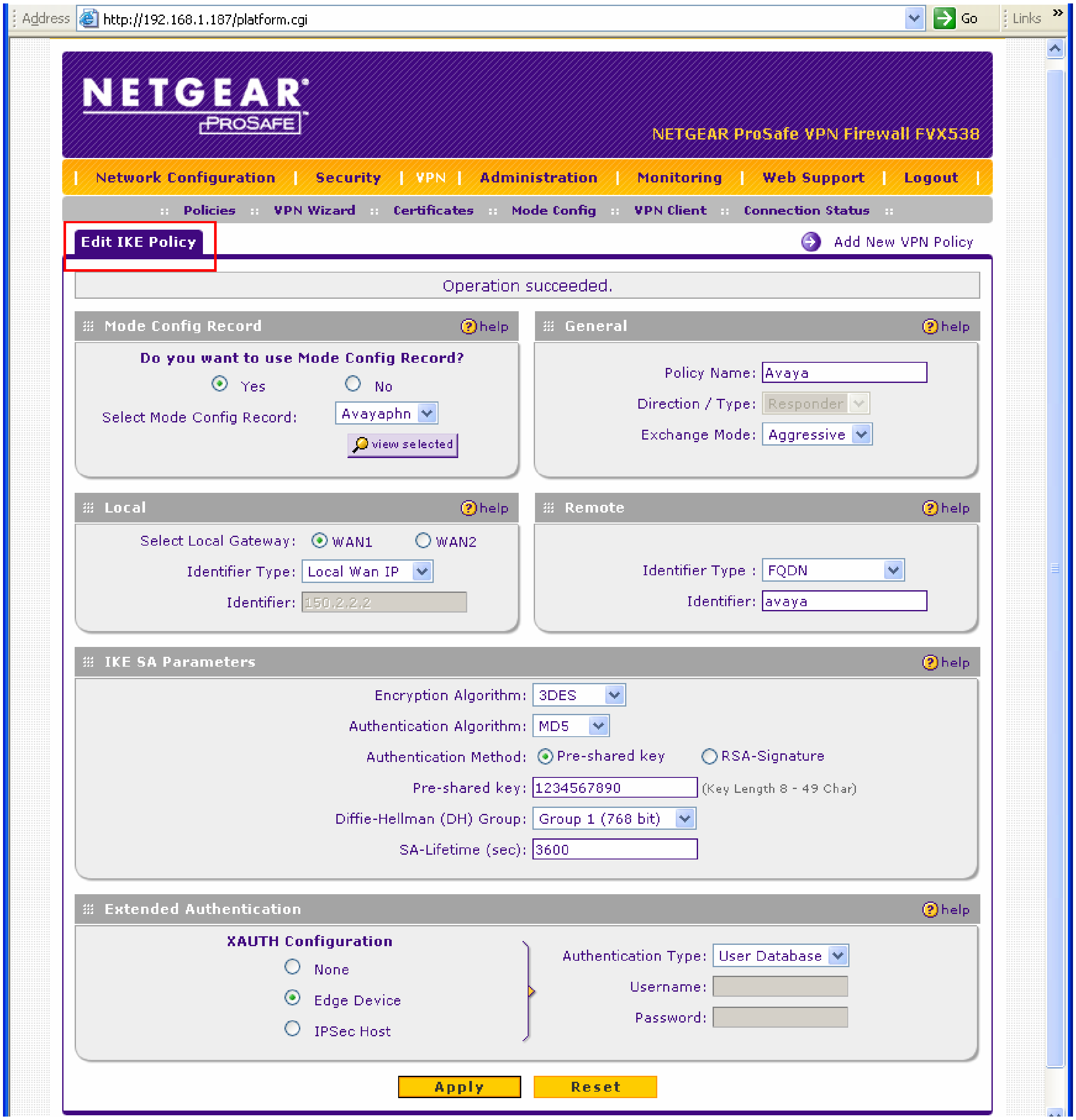
5. Defined the IKE Policies by selecting **VPN→Policies →IKE Policies** from the top menu bar. The sample network defined a IKE Policy named Avaya for Avaya VPNremote Phones. Note the **Mode Config**, **Avayaphn**, defined in Step 4 is used in the 2nd screen capture below



List of IKE Policies

	Name	Mode	Local ID	Remote ID	Encr	Auth	DH	Action
□	Avaya	Aggressive	150.2.2.2	avaya	3DES	MD5	Group 1 (768 bit)	edit

* Client Policy


Address http://192.168.1.187/platform.cgi
Go
Links
NETGEAR PROSAFE
NETGEAR ProSafe VPN Firewall FVX538
| Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout |
:: Policies :: VPN Wizard :: Certificates :: Mode Config :: VPN Client :: Connection Status ::
Add New VPN Policy
view selected
Apply
Reset

Edit IKE Policy

Operation succeeded.

Mode Config Record (help)

Do you want to use Mode Config Record? ● Yes ○ No

Select Mode Config Record: Avayaphn

General (help)

Policy Name: Avaya

Direction / Type: Responder

Exchange Mode: Aggressive

Local (help)

Select Local Gateway: ● WAN1 ○ WAN2

Identifier Type: Local Wan IP

Identifier: 150.2.2.2

Remote (help)

Identifier Type : FQDN

Identifier: avaya

IKE SA Parameters (help)

Encryption Algorithm: 3DES

Authentication Algorithm: MD5

Authentication Method: ● Pre-shared key ○ RSA-Signature

Pre-shared key: 1234567890 (Key Length 8 - 49 Char)

Diffie-Hellman (DH) Group: Group 1 (768 bit)

SA-Lifetime (sec): 3600

Extended Authentication (help)

XAUTH Configuration

○ None

● Edge Device

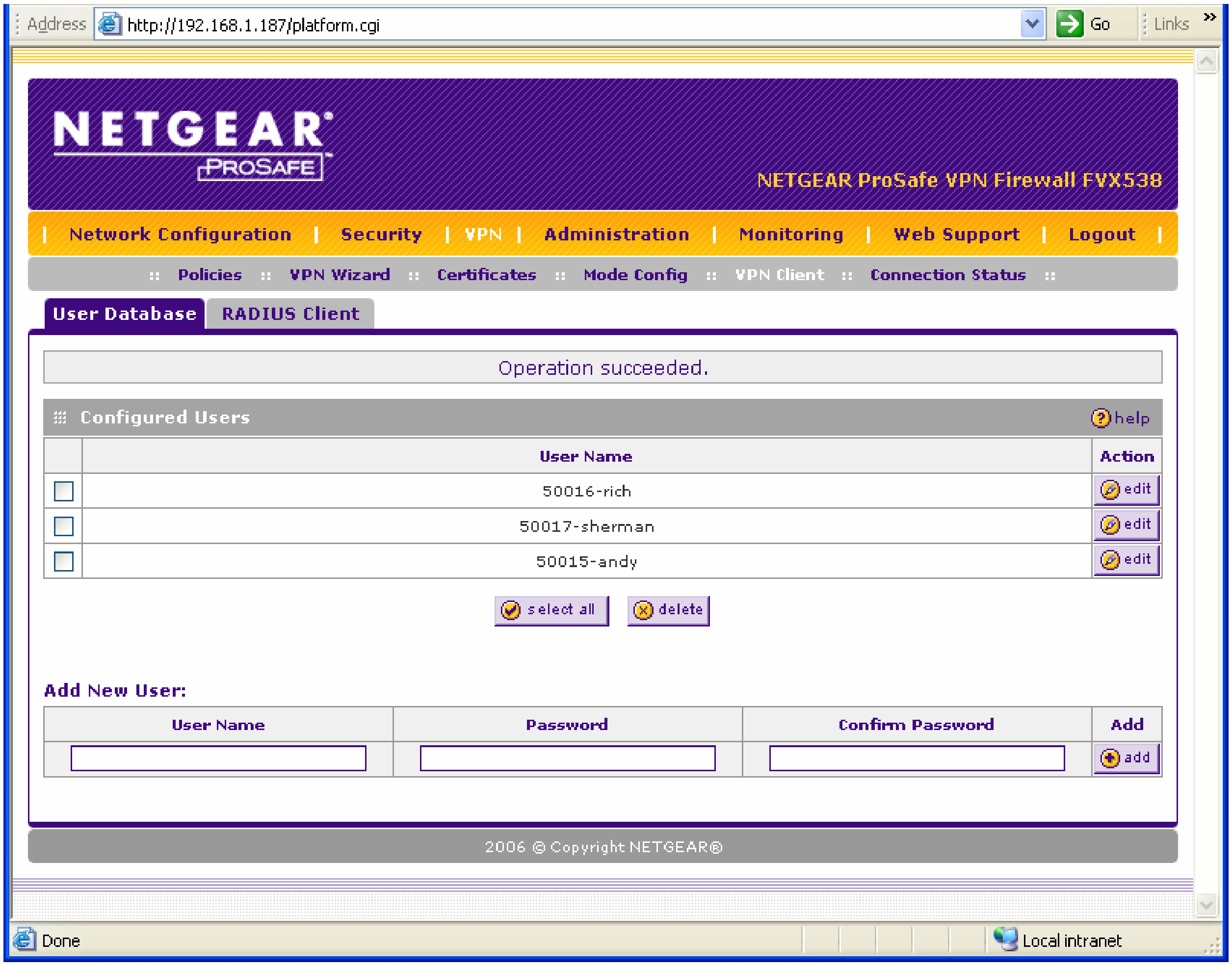
○ IPSec Host

Authentication Type: User Database

Username:

Password:

6. Defined the Xauth user by selecting **VPN→VPN Client→User Database** from the top menu bar. The **User Name** used in the sample configuration is composed of the phone extension and the user name to facilitate tracking. Other form of **User Name** may be used.


Address http://192.168.1.187/platform.cgi
Go
Links
NETGEAR ProSafe
NETGEAR ProSafe VPN Firewall FVX538
Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout
Policies :: VPN Wizard :: Certificates :: Mode Config :: VPN Client :: Connection Status
User Database
RADIUS Client
help
select all
delete
2006 © Copyright NETGEAR®
Done
Local intranet

Operation succeeded.

Configured Users

	User Name	Action
□	50016-rich	edit
□	50017-sherman	edit
□	50015-andy	edit

Add New User:

User Name	Password	Confirm Password	Add
			add

5. Avaya VPNremote Phone Configuration

5.1. 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 → **View IP Settings** soft button → **Miscellaneous** soft button → **Right arrow** hard 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.

5.2. 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 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 Servers 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, e.g. registered with Avaya Communication Manager, 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 enter the VPN Options menu.

2. The VPN configuration options menu is displayed. For 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 2** below.

Note: The values entered below are case sensitive.

Press the ► 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:	**150.2.2.2**	IP address of the FVX538 WAN1 interface
User Name:	**50016-rich**	User created in **Section 4.1, Step 6**
Password:	********	Must match user password entered in **Section 4.1, Step 6**
Group Name:	**avaya**	Must match the **Remote ID** entered in **Section 4.1, Step 5**
Group PSK:	**1234567890**	Must match the **Pre-shared Key** entered in **Section 4.1, Step 5**
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:	-	

Configuration Options	Value	Description
IKE Parameters:	**DH1-3DES-MD5**	Must match SA proposals from **Section 4.1, Step 5**
IKE ID Type:	**FQDN**	
Diffie-Hellman Grp	**1**	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:	**MD5**	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**	
IPSec Parameters:	**DH1-3DES-MD5**	Must match SA proposals from **Section 4.1. Step 4**
Encryption Alg:	**3DES**	Can be set to "Any" to accept VPN Concentrator settings
Authentication Alg:	**MD5**	Can be set to "Any" to accept VPN Concentrator settings
Diffie-Hellman Grp	**1**	Can be set to "Detect" to accept VPN Concentrator settings
Protected Net:		
Remote Net #1:	**192.168.1.0/24**	Access to all private nets
File Srvr:	**172.28.10.15**	TFTP/HTTP Phone File Srv
Connectivity Check:	**First Time**	Test initial IPSec connectivity
Copy TOS:	**Yes**	Maintain phone TOS setting on Corp Network for QoS
QTest	**Disable**	Can be either Enable or Disable to allow user access to QTest feature.

Table 2 – Avaya VPNremote Phone Configuration

3. The Avaya VPNremote Phone can interoperate with several VPN head-end vendors. 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 Avaya VPNremote Phone.

   Press the **Profile** soft button at the bottom of Avaya VPNremote Phones 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 aligned with 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.

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
```

6. Avaya Communication Manager Configuration

All the commands discussed in this section are executed on Avaya Communication Manager using the System Access Terminal (SAT). This section assumes that basic configuration on Avaya Communication Manager has already been completed.

As shown in **Figure 2**, Avaya VPNremote Phones are assigned to IP Network Region 5 using ip-network-map in Avaya Communication Manager based on the IP address range of the FVX538 IP Address Pool. IP Network Region 5 is then assigned to a codec set configured with the G.729 codec. The Main Campus is assigned to IP Network Region 1 using the G.711 codec.

6.1. Avaya VPNremote Phone Administration

An Avaya VPNremote Phone is administered the same as other Avaya IP telephones within Avaya Communication Manager. Even though the Avaya VPNremote Phone is physically located outside of the corporate network, the AvayaVPNremote Phone will behave the same as other Avaya IP telephones located locally on the corporate LAN once the VPN tunnel has been established.

For additional information regarding the administration of Avaya Communication Manager, refer to [3].

6.2. IP Codec Sets Configuration

Use the **`change ip-codec-set n`** command to configure IP Codec Set parameters where n is the IP Codec Set number. Configure the highlighted fields shown below. All remaining fields can be left at the default values.

1. Use the **`change ip-codec-set 1`** command to define a codec set for the G.711 codec as shown below.

```
change ip-codec-set 1                                          Page   1 of   2

                          IP Codec Set

    Codec Set: 1

    Audio         Silence      Frames   Packet
    Codec         Suppression  Per Pkt  Size(ms)
 1: G.711MU            n         2        20
 2:
 3:
```

2. Use the **`change ip-codec-set 2`** command to define a codec set for the G.729 (30ms) codec as shown below.

```
change ip-codec-set 2                                           Page   1 of   2

                          IP Codec Set

    Codec Set: 2

    Audio         Silence      Frames   Packet
    Codec         Suppression  Per Pkt  Size(ms)
 1: G.729              n         3        30
 2:
 3:
```

3. Use the **`list ip-codec-set`** command to verify the codec assignments.

```
list ip-codec-set

                                IP CODEC SETS

Codec  Codec 1     Codec 2     Codec 3     Codec 4     Codec 5
Set

  1    G.711MU
  2    G.729
  3
  4
```

6.3. IP Network Map Configuration

Use the **`change ip-network-map`** command to define the IP address to Network Region mapping for Avaya VPNremote Phones.

```
change ip-network-map                                         Page   1 of  32
                         IP ADDRESS MAPPING

                                                              Emergency
                                       Subnet                 Location
 From IP Address  (To IP Address   or Mask)  Region    VLAN   Extension
  10. 10. 10. 10   10. 10. 10.  20            5        n
    .   .   .         .   .   .                        n
    .   .   .         .   .   .                        n
    .   .   .         .   .   .                        n
```

6.4. IP Network Regions Configuration

Use the **`change ip-network-region n`** command to configure IP Network Region parameters where n is the IP Network Region number. Configure the highlighted fields shown below. All remaining fields can be left at the default values.

Intra-region and **Inter-region IP-IP Direct Audio** determines the flow of RTP audio packets. Setting these fields to “yes” enables direct IP connectivity for RTP packets. **Codec Set 1** is used for IP Network Region 1 as described in **Section 6.2**.

```
change ip-network-region 1                                    Page   1 of  19


                               IP NETWORK REGION
  Region: 1
Location: 1      Authoritative Domain: avaya.com
    Name: Main Campus
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? y
   UDP Port Max: 3327
DIFFSERV/TOS PARAMETERS                  RTCP Reporting Enabled? y
 Call Control PHB Value: 46      RTCP MONITOR SERVER PARAMETERS
        Audio PHB Value: 46       Use Default Server Parameters? y
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                         RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

Page 3 of the IP-Network-Region form, shown below, defines the codec set to use for intra-region and inter-region calls. Avaya VPNremote Phones are mapped to Region 5. Calls within IP Network Region 1 use Codec Set 1 (G.711MU) while calls between IP Network Region 1 and IP Network Region 5 use Codec Set 2 (G.729).

```
change ip-network-region 1                                      Page   3 of  19

                   Inter Network Region Connection Management

 src dst  codec  direct                                     Dynamic CAC
 rgn rgn   set    WAN    WAN-BW-limits  Intervening-regions   Gateway   IGAR
 1   1     1
 1   5     2       y          :NoLimit                                   n
 1   3
 1   4
```

Use the **`change ip-network-region 5`** command to configure IP Network Region 5 parameters. Configure the highlighted fields shown below. All remaining fields can be left at the default values. Noticed that **Intra-region IP-IP Direction Audio** is set to **no**.

```
change ip-network-region 5                                      Page   1 of  19
                               IP NETWORK REGION
  Region: 5
Location:         Authoritative Domain:
    Name: Netgear Firewall FVX538
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: no
      Codec Set: 2              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? y
   UDP Port Max: 3028
```

Page 3 defines the codec set to use for intra-region and inter-region calls. Avaya VPNremote Phones are mapped to Region 5. Calls within IP Network Region 5, i.e. a Avaya VPNremote Phone calling another Avaya VPNremote Phone, use Codec Set 2 (G.729). Calls between IP Network Region 5 and IP Network Region 1 will also use Codec Set 2 (G.729).

```
change ip-network-region 5                                      Page   3 of  19

                   Inter Network Region Connection Management

 src dst  codec  direct                                     Dynamic CAC
 rgn rgn   set    WAN    WAN-BW-limits  Intervening-regions   Gateway   IGAR
 5   1     2       y          :NoLimit                                   n
 5   2
 5   3
 5   4
 5   5     2
```

7. Verification

7.1. Avaya VPNremote Phone IPSec Statistics

Once the Avaya VPNremote Phone establishes an IPSec tunnel, registers with Avaya Communication Manager and becomes functional, from the telephone keypad, press the **OPTIONS** hard button (with √ icon). From the telephone keypad, press the ► hard button until the **VPN Status…** option appears. Select **VPN Status…** The VPN statistics of the active IPSec tunnel will be displayed. Use the ► hard button to access the next screen. Press the **Refresh** soft button to update the displayed statistics.

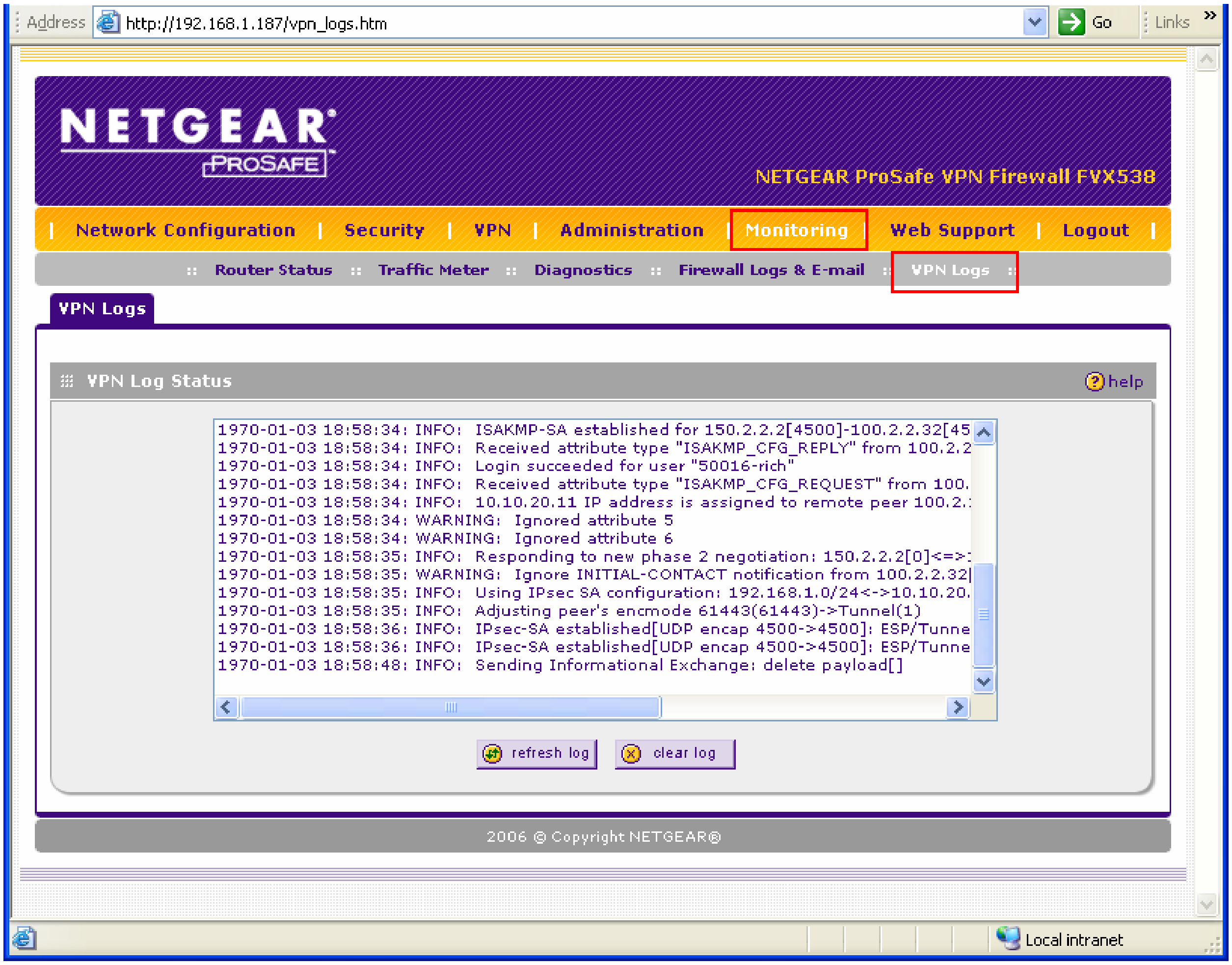
The list below shows the statistics from Avaya VPNremote Phone used in the sample configuration.

VPN Status…	
PKT S/R	**47/39**
FRAG RCVD	**0**
Comp/Decomp	**0/0**
Auth Failures	**0**
Recv Errors	**0**
Send Errors	**0**
Gateway	**150.2.2.2**
Outer IP	**192.168.2.202**
Inner IP	**10.10.20.12**
Gateway Version	**KAME/raccoon..**
Inactivity Timeout	**0**
DH1-3DES-MD5-120 hrs	

7.2. Netgear ProSafe VPN Firewall FVX538 Logging

The FVX538 VPN logs displays the current event log contents of the FVX538 to the WEB GUI. The VPN Logs snapshot shown below contains the IKE Phase1 and IKE Phase2 events logged as a single Avaya VPNremote Phone successfully authenticates and establishes an IPSec tunnel. Key events are highlighted in bold.

To access to the FVX538 event log, select **Monitoring→VPN logs.**



```
1970-01-03 18:58:34: INFO:  ISAKMP-SA established for 150.2.2.2[4500]-100.2.2.32[45
1970-01-03 18:58:34: INFO:  Received attribute type "ISAKMP_CFG_REPLY" from 100.2.2
1970-01-03 18:58:34: INFO:  Login succeeded for user "50016-rich"
1970-01-03 18:58:34: INFO:  Received attribute type "ISAKMP_CFG_REQUEST" from 100.
1970-01-03 18:58:34: INFO:  10.10.20.11 IP address is assigned to remote peer 100.2.
1970-01-03 18:58:34: WARNING:  Ignored attribute 5
1970-01-03 18:58:34: WARNING:  Ignored attribute 6
1970-01-03 18:58:35: INFO:  Responding to new phase 2 negotiation: 150.2.2.2[0]<=>
1970-01-03 18:58:35: WARNING:  Ignore INITIAL-CONTACT notification from 100.2.2.32|
1970-01-03 18:58:35: INFO:  Using IPsec SA configuration: 192.168.1.0/24<->10.10.20.
1970-01-03 18:58:35: INFO:  Adjusting peer's encmode 61443(61443)->Tunnel(1)
1970-01-03 18:58:36: INFO:  IPsec-SA established[UDP encap 4500->4500]: ESP/Tunne
1970-01-03 18:58:36: INFO:  IPsec-SA established[UDP encap 4500->4500]: ESP/Tunne
1970-01-03 18:58:48: INFO:  Sending Informational Exchange: delete payload[]
```

Below is a log output in a text format from a similar user authentication session.

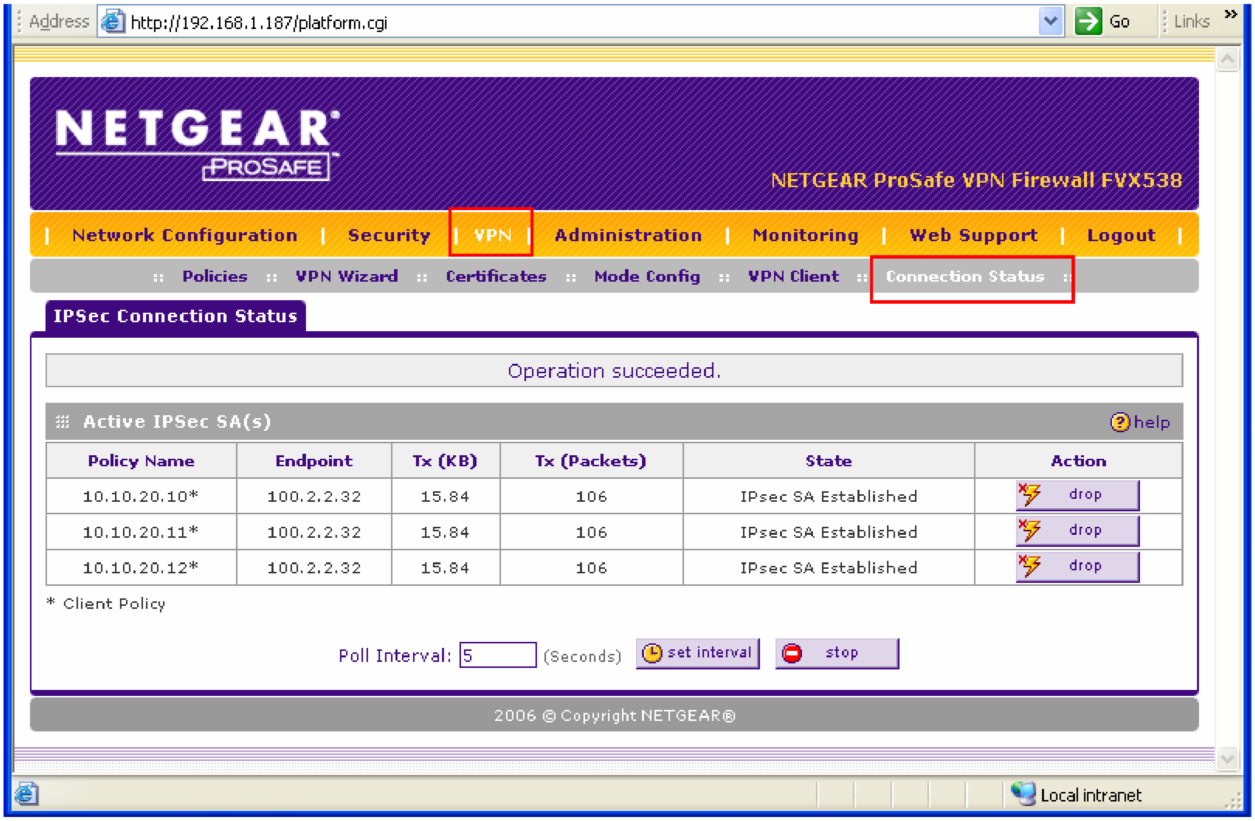
```
1970-01-04 12:26:41: INFO:  Remote configuration for identifier "avaya" found
1970-01-04 12:26:41: INFO:  Received request for new phase 1 negotiation:
150.2.2.2[500]<=>100.2.2.32[32907]
1970-01-04 12:26:41: INFO:  Beginning Aggressive mode.
1970-01-04 12:26:41: INFO:  Received unknown Vendor ID
1970-01-04 12:26:41: INFO:  Received Vendor ID: draft-ietf-ipsec-nat-t-ike-02

1970-01-04 12:26:41: INFO:  Received unknown Vendor ID
1970-01-04 12:26:41: INFO:  Received unknown Vendor ID
1970-01-04 12:26:41: INFO:  Received unknown Vendor ID
1970-01-04 12:26:41: INFO:  Received Vendor ID: draft-ietf-ipsra-isakmp-xauth-06.txt
1970-01-04 12:26:41: INFO:  For 100.2.2.32[32907], Selected NAT-T version: draft-ietf-
ipsec-nat-t-ike-02
1970-01-04 12:26:42: INFO:  Floating ports for NAT-T with peer 100.2.2.32[4500]
1970-01-04 12:26:42: INFO:  NAT-D payload matches for 150.2.2.2[4500]
1970-01-04 12:26:42: INFO:  NAT-D payload does not match for 100.2.2.32[4500]
1970-01-04 12:26:42: INFO:  NAT detected: Peer is behind a NAT device
1970-01-04 12:26:42: INFO:  Sending Xauth request to 100.2.2.32[4500]
1970-01-04 12:26:42: INFO:  ISAKMP-SA established for 150.2.2.2[4500]-100.2.2.32[4500]
with spi:471ddea951b63a21:b1ae4519ce42e92d
1970-01-04 12:26:42: INFO:  Received attribute type "ISAKMP_CFG_REPLY" from
100.2.2.32[4500]
1970-01-04 12:26:42: INFO:  Login succeeded for user "50016-rich"
1970-01-04 12:26:42: INFO:  Received attribute type "ISAKMP_CFG_REQUEST" from
100.2.2.32[4500]
1970-01-04 12:26:42: INFO:  10.10.20.12 IP address is assigned to remote peer
100.2.2.32[4500]
1970-01-04 12:26:42: WARNING:  Ignored attribute 5
1970-01-04 12:26:42: WARNING:  Ignored attribute 6
1970-01-04 12:26:43: INFO:  Responding to new phase 2 negotiation:
150.2.2.2[0]<=>100.2.2.32[0]
1970-01-04 12:26:43: WARNING:  Ignore INITIAL-CONTACT notification from
100.2.2.32[4500] because it is only accepted after phase1.
1970-01-04 12:26:43: INFO:  Using IPsec SA configuration: 192.168.1.0/24<-
>10.10.20.0/24
1970-01-04 12:26:43: INFO:  Adjusting peer's encmode 61443(61443)->Tunnel(1)
1970-01-04 12:26:44: INFO:  IPsec-SA established[UDP encap 4500->4500]: ESP/Tunnel
100.2.2.32->150.2.2.2 with spi=130471672(0x7c6d6f8)
1970-01-04 12:26:44: INFO:  IPsec-SA established[UDP encap 4500->4500]: ESP/Tunnel
150.2.2.2->100.2.2.32 with spi=3284438177(0xc3c48ca1)
```

7.3. Netgear ProSafe VPN Firewall FVX538 Active Sessions

The active VPN sessions to the FVX538 can be viewed by selecting **VPN→ Connection Status** from the top menu of the web management interface.

Active IPSec tunnels are shown in the display. The screen capture below shows the current **Active IPSec SA(s)** to the FVX538 gateway.


Address
Go
Links
NETGEAR
PROSAFE
NETGEAR ProSafe VPN Firewall FVX538
| Network Configuration | Security | VPN | Administration | Monitoring | Web Support | Logout |
:: Policies :: VPN Wizard :: Certificates :: Mode Config :: VPN Client :: Connection Status ::
IPSec Connection Status
help
set interval
stop
Local intranet

Address: http://192.168.1.187/platform.cgi

Operation succeeded.

Active IPSec SA(s)

Policy Name	Endpoint	Tx (KB)	Tx (Packets)	State	Action
10.10.20.10*	100.2.2.32	15.84	106	IPsec SA Established	drop
10.10.20.11*	100.2.2.32	15.84	106	IPsec SA Established	drop
10.10.20.12*	100.2.2.32	15.84	106	IPsec SA Established	drop

* Client Policy

Poll Interval: 5 (Seconds)

2006 © Copyright NETGEAR®

8. Trouble Shooting

This section offers some common configuration mismatches between Avaya VPNremote Phone and the Netgear ProSafe VPN Firewall FVX538 to assist in troubleshooting. The key events of the logs are highlighted in bold. These log messages was generated using the “Original” Display Mode.

8.1. Incorrect User Name

- **Avaya VPNremote Phone display:**
  Initial display shows the following:
  ```
  Enter Username and Password
  Password:
  ```

  After a short period of time with no input (5 minutes) the display shows the following:
  Invalid password OR user name

  Press the **More** soft button to display the following:
  ```
  Error Code: 3997700:0
  Module:IKECFG:430
  ```

- **FVX538 event Log:**

```
1970-01-04 13:14:37: INFO:  Remote configuration for identifier "avaya"
found
1970-01-04 13:14:37: INFO:  Received request for new phase 1
negotiation: 150.2.2.2[500]<=>100.2.2.32[32907]
1970-01-04 13:14:37: INFO:  Beginning Aggressive mode.
1970-01-04 13:14:37: INFO:  Received unknown Vendor ID
1970-01-04 13:14:37: INFO:  Received Vendor ID: draft-ietf-ipsec-nat-t-
ike-02

1970-01-04 13:14:37: INFO:  Received unknown Vendor ID
1970-01-04 13:14:37: INFO:  Received unknown Vendor ID
1970-01-04 13:14:37: INFO:  Received unknown Vendor ID
1970-01-04 13:14:37: INFO:  Received Vendor ID: draft-ietf-ipsra-isakmp-
xauth-06.txt
1970-01-04 13:14:37: INFO:  For 100.2.2.32[32907], Selected NAT-T
version: draft-ietf-ipsec-nat-t-ike-02
1970-01-04 13:14:38: INFO:  Floating ports for NAT-T with peer
100.2.2.32[4500]
1970-01-04 13:14:38: INFO:  NAT-D payload matches for 150.2.2.2[4500]
1970-01-04 13:14:38: INFO:  NAT-D payload does not match for
100.2.2.32[4500]
1970-01-04 13:14:38: INFO:  NAT detected: Peer is behind a NAT device
1970-01-04 13:14:38: INFO:  Sending Xauth request to 100.2.2.32[4500]
1970-01-04 13:14:38: INFO:  ISAKMP-SA established for 150.2.2.2[4500]-
100.2.2.32[4500] with spi:0a86dcc846438e9e:69ad3dde1e6aaf11
1970-01-04 13:14:38: INFO:  Received attribute type "ISAKMP_CFG_REPLY"
from 100.2.2.32[4500]
1970-01-04 13:14:38: INFO:  0.0.0.0 IP address has been released by
remote peer.
1970-01-04 13:14:38: INFO:  Login failed for user "50016-rich1"
1970-01-04 13:14:38: INFO:  Sending Informational Exchange: delete
payload[]
```

```
1970-01-04 13:14:38: ERROR:  Failed to find proper address pool with id
-1
1970-01-04 13:14:38: ERROR:  Received mode config from 100.2.2.32[4500],
but we do not have ISAKMP-SA.
```

8.2. Incorrect User Password

- **Avaya VPNremote Phone display:**
  Initial display shows the following:

  After a short period of time with no input (5 minutes) the display shows the following:
  `Invalid password or username`

  Press the **More** soft button to display the following:
  ```
  Error Code: 3276801:0
  Module:IKECFG:430
  ```

- **FVX538 event Log:**

```
1970-01-04 13:12:50: INFO:  Remote configuration for identifier "avaya"
found
1970-01-04 13:12:50: INFO:  Received request for new phase 1
negotiation: 150.2.2.2[500]<=>100.2.2.32[32907]
1970-01-04 13:12:50: INFO:  Beginning Aggressive mode.
1970-01-04 13:12:50: INFO:  Received unknown Vendor ID
1970-01-04 13:12:50: INFO:  Received Vendor ID: draft-ietf-ipsec-nat-t-
ike-02

1970-01-04 13:12:50: INFO:  Received unknown Vendor ID
1970-01-04 13:12:50: INFO:  Received unknown Vendor ID
1970-01-04 13:12:50: INFO:  Received unknown Vendor ID
1970-01-04 13:12:50: INFO:  Received Vendor ID: draft-ietf-ipsra-isakmp-
xauth-06.txt
1970-01-04 13:12:50: INFO:  For 100.2.2.32[32907], Selected NAT-T
version: draft-ietf-ipsec-nat-t-ike-02
1970-01-04 13:12:50: INFO:  Floating ports for NAT-T with peer
100.2.2.32[4500]
1970-01-04 13:12:51: INFO:  NAT-D payload matches for 150.2.2.2[4500]
1970-01-04 13:12:51: INFO:  NAT-D payload does not match for
100.2.2.32[4500]
1970-01-04 13:12:51: INFO:  NAT detected: Peer is behind a NAT device
1970-01-04 13:12:51: INFO:  Sending Xauth request to 100.2.2.32[4500]
1970-01-04 13:12:51: INFO:  ISAKMP-SA established for 150.2.2.2[4500]-
100.2.2.32[4500] with spi:07eb45bb9e199368:0b94acd8f2cf7ecb
1970-01-04 13:12:51: INFO:  Received attribute type "ISAKMP_CFG_REPLY"
from 100.2.2.32[4500]
1970-01-04 13:12:51: INFO:  0.0.0.0 IP address has been released by
remote peer.
1970-01-04 13:12:51: INFO:  Login failed for user "50016-rich"
1970-01-04 13:12:51: INFO:  Sending Informational Exchange: delete
payload[]
1970-01-04 13:12:51: ERROR:  Failed to find proper address pool with id
-1
1970-01-04 13:12:51: ERROR:  Received mode config from 100.2.2.32[4500],
but we do not have ISAKMP-SA.
```

8.3. Mismatched Phase 1 Proposal

- **Avaya VPNremote Phone display:**

  ```
  IDE Phase1 no reponse
  ```

  Press the **More** soft button to display the following:

  ```
  Error Code: 3997700:0
  Module:IKMPD:142
  ```

  Press the **Next** soft button to display the following:

  ```
  Error Code: 3997700:0
  Module:IKECFG:459
  ```

- **FVX538 event Log:**

```
1970-01-04 13:15:55: INFO:  Remote configuration for identifier "avaya"
found
1970-01-04 13:15:55: INFO:  Received request for new phase 1
negotiation: 150.2.2.2[500]<=>100.2.2.32[32907]
1970-01-04 13:15:55: INFO:  Beginning Aggressive mode.
1970-01-04 13:15:55: INFO:  Received unknown Vendor ID
1970-01-04 13:15:55: INFO:  Received Vendor ID: draft-ietf-ipsec-nat-t-
ike-02

1970-01-04 13:15:55: INFO:  Received unknown Vendor ID
1970-01-04 13:15:55: INFO:  Received unknown Vendor ID
1970-01-04 13:15:55: INFO:  Received unknown Vendor ID
1970-01-04 13:15:55: INFO:  Received Vendor ID: draft-ietf-ipsra-isakmp-
xauth-06.txt
1970-01-04 13:15:55: INFO:  For 100.2.2.32[32907], Selected NAT-T
version: draft-ietf-ipsec-nat-t-ike-02
1970-01-04 13:15:55: WARNING:  Rejected phase 1 proposal as Peer's
encryption type "AES-CBC" mismatched with Local "3DES-CBC".
1970-01-04 13:15:55: WARNING:  Rejected phase 1 proposal as Peer's
hashtype "SHA" mismatched with Local "MD5".
1970-01-04 13:15:55: WARNING:  Rejected phase 1 proposal as Peer's
dh_group "1024-bit MODP group" mismatched with Local "768-bit MODP
group".
1970-01-04 13:15:55: ERROR:  No suitable proposal found for
100.2.2.32[32907].
1970-01-04 13:15:55: ERROR:  Failed to get valid proposal for
100.2.2.32[32907].
1970-01-04 13:16:00: WARNING:  Rejected phase 1 proposal as Peer's
dh_group "1024-bit MODP group" mismatched with Local "768-bit MODP
group".
1970-01-04 13:16:00: ERROR:  No suitable proposal found for
100.2.2.32[32907].
1970-01-04 13:16:00: ERROR:  Failed to get valid proposal for
100.2.2.32[32907].
```

8.4. Mismatched Phase 2 Proposal

- **Avaya VPNremote Phone display:**

  ```
  IKE Phase2 no response
  ```

Press the **More** soft button to display the following:

```
IKE Phase1 send notify
Error Code: 3997698:14
Module:NOTIFY:444
```

Press the **Next** soft button to display the following:

```
IKE Phase2 no reponse
Error Code: 3997700:0
Module:IKECFG:1184
```

- **FVX538 event Log:** (some non-relevant log entries removed for brevity)

```
1970-01-04 13:19:43: INFO:  Remote configuration for identifier "avaya" found
1970-01-04 13:19:43: INFO:  Received request for new phase 1 negotiation:
150.2.2.2[500]<=>100.2.2.32[32907]
1970-01-04 13:19:43: INFO:  Beginning Aggressive mode.
1970-01-04 13:19:43: INFO:  Received unknown Vendor ID
1970-01-04 13:19:43: INFO:  Received Vendor ID: draft-ietf-ipsec-nat-t-ike-02

1970-01-04 13:19:43: INFO:  Received unknown Vendor ID
1970-01-04 13:19:43: INFO:  Received unknown Vendor ID
1970-01-04 13:19:43: INFO:  Received unknown Vendor ID
1970-01-04 13:19:43: INFO:  Received Vendor ID: draft-ietf-ipsra-isakmp-xauth-
06.txt
1970-01-04 13:19:43: INFO:  For 100.2.2.32[32907], Selected NAT-T version:
draft-ietf-ipsec-nat-t-ike-02
1970-01-04 13:19:44: INFO:  Floating ports for NAT-T with peer 100.2.2.32[4500]
1970-01-04 13:19:44: INFO:  NAT-D payload matches for 150.2.2.2[4500]
1970-01-04 13:19:44: INFO:  NAT-D payload does not match for 100.2.2.32[4500]
1970-01-04 13:19:44: INFO:  NAT detected: Peer is behind a NAT device
1970-01-04 13:19:44: INFO:  Sending Xauth request to 100.2.2.32[4500]
1970-01-04 13:19:44: INFO:  ISAKMP-SA established for 150.2.2.2[4500]-
100.2.2.32[4500] with spi:e402b8223f0263e1:60b47d1bcffba685
1970-01-04 13:19:44: INFO:  Received attribute type "ISAKMP_CFG_REPLY" from
100.2.2.32[4500]
1970-01-04 13:19:44: INFO:  Login succeeded for user "50016-rich"
1970-01-04 13:19:44: INFO:  Received attribute type "ISAKMP_CFG_REQUEST" from
100.2.2.32[4500]
1970-01-04 13:19:44: INFO:  10.10.20.10 IP address is assigned to remote peer
100.2.2.32[4500]
1970-01-04 13:19:44: WARNING:  Ignored attribute 5
1970-01-04 13:19:44: WARNING:  Ignored attribute 6
1970-01-04 13:19:46: INFO:  Responding to new phase 2 negotiation:
150.2.2.2[0]<=>100.2.2.32[0]
1970-01-04 13:19:46: WARNING:  Ignore INITIAL-CONTACT notification from
100.2.2.32[4500] because it is only accepted after phase1.
1970-01-04 13:19:46: INFO:  Using IPsec SA configuration: 192.168.1.0/24<-
>10.10.20.0/24
1970-01-04 13:19:46: INFO:  Adjusting peer's encmode 61443(61443)->Tunnel(1)
1970-01-04 13:19:46: WARNING:  Peer's Proposal:
1970-01-04 13:19:46: WARNING:   (proto_id=ESP spisize=4 spi=2eebb84f
spi_p=00000000 encmode=Tunnel reqid=0:0)
1970-01-04 13:19:46: WARNING:    (trns_id=RIJNDAEL encklen=192 authtype=hmac-
sha)
1970-01-04 13:19:46: WARNING:  Local Proposal:
1970-01-04 13:19:46: WARNING:   (proto_id=ESP spisize=4 spi=00000000
spi_p=00000000 encmode=Tunnel reqid=4500:4500)
1970-01-04 13:19:46: WARNING:    (trns_id=3DES encklen=0 authtype=hmac-md5)
1970-01-04 13:19:46: WARNING:  Phase 2 proposal by 100.2.2.32[0] did not match.
1970-01-04 13:19:46: ERROR:  No suitable policy found for 100.2.2.32[0]
1970-01-04 13:19:46: INFO:  Sending Informational Exchange: notify payload[NO-
PROPOSAL-CHOSEN]
1970-01-04 13:19:46: INFO:  Responding to new phase 2 negotiation:
150.2.2.2[0]<=>100.2.2.32[0]
1970-01-04 13:19:46: WARNING:  Ignore INITIAL-CONTACT notification from
100.2.2.32[4500] because it is only accepted after phase1.
```

```
1970-01-04 13:19:46: INFO:  Using IPsec SA configuration: 192.168.1.0/24<-
>10.10.20.0/24
1970-01-04 13:19:46: INFO:  Adjusting peer's encmode 61443(61443)->Tunnel(1)
1970-01-04 13:19:46: WARNING:  Peer's Proposal:
1970-01-04 13:19:46: WARNING:   (proto_id=ESP spisize=4 spi=2eebb84f
spi_p=00000000 encmode=Tunnel reqid=0:0)
1970-01-04 13:19:46: WARNING:    (trns_id=RIJNDAEL encklen=192 authtype=hmac-
sha)
1970-01-04 13:19:46: WARNING:  Local Proposal:
1970-01-04 13:19:46: WARNING:   (proto_id=ESP spisize=4 spi=00000000
spi_p=00000000 encmode=Tunnel reqid=4500:4500)
1970-01-04 13:19:46: WARNING:    (trns_id=3DES encklen=0 authtype=hmac-md5)
1970-01-04 13:19:46: WARNING:  Phase 2 proposal by 100.2.2.32[0] did not match.
1970-01-04 13:19:46: ERROR:  No suitable policy found for 100.2.2.32[0]
1970-01-04 13:19:47: INFO:  Sending Informational Exchange: notify payload[NO-
PROPOSAL-CHOSEN]
1970-01-04 13:19:49: ERROR:  Failed to get IPsec SA configuration for:
0.0.0.0/0<->10.10.20.10/32
```

8.5. No IP Pool Addresses Available

- **Avaya VPNremote Phone display:**
  ```
  Downloading configuration
  ```

- **FVX538 event Log:**
  ```
  09/14/2007 12:31:51  0 Sys [05] Event Log Cleared.
  09/14/2007 12:34:19  0 Security [16] Session: IPSEC[50016-rich] attempting login
  09/14/2007 12:34:19  0 Security [06] Session: IPSEC[50016-rich] has no active
  sessions
  09/14/2007 12:34:19  0 Security [06] Session: IPSEC[50016-rich] rich L has no
  active accounts
  09/14/2007 12:34:19  0 tIsakmp [05] Oakley Aggressive Mode proposal accepted
  from 50016-rich (100.2.2.32)
  09/14/2007 12:34:20  0 Security [06] Session: IPSEC[50016-rich]:4 SHARED-SECRET
  authenticate attempt...
  09/14/2007 12:34:20  0 Security [06] Session: IPSEC[50016-rich]:4 attempting
  authentication using LOCAL
  09/14/2007 12:34:20  0 Security [16] Session: IPSEC[50016-rich]:4 authenticated
  using LOCAL
  09/14/2007 12:34:20  0 Security [16] Session: IPSEC[50016-rich]:4 bound to group
  /Base/LocalAuth/rich L
  09/14/2007 12:34:20  0 Syslog [25] Session: IPSEC[50016-rich]:4 Incoming client
  version (unknown), minimum version (unknown) push action (none), action not
  needed
  09/14/2007 12:34:20  0 Security [06] Session: IPSEC[50016-rich]:4 Building group
  filter permit all
  09/14/2007 12:34:20  0 Security [06] Session: IPSEC[50016-rich]:4 Applying group
  filter permit all
  09/14/2007 12:34:20  0 Security [14] Session: IPSEC[No Access Network]:Access
  Network Passed - 100.2.2.32
  09/14/2007 12:34:20  0 Security [16] Session: IPSEC[50016-rich]:4 authorized
  09/14/2007 12:34:20  0 tIsakmp [05] ISAKMP SA established with 50016-rich
  (100.2.2.32)
  09/14/2007 12:34:20  0 Security [15] Session: IPSEC[50016-rich]:4 physical
  addresses: remote 100.2.2.32 local 120.2.2.2
  09/14/2007 12:34:20  0 Security [14] Session: IPSEC[50016-rich]:4 IP address
  assignment failed
  ```

8.6. Graceful Reboot of VPNremote Phone

- **Avaya VPNremote Phone display:**
  ```
  Rebooting...
  ```

- **FVX538 event Log:**
  ```
  1970-01-04 13:25:30: INFO:  Purged IPsec-SA with proto_id=ESP and
  spi=2038503861(0x798119b5).
  ```

9. Conclusion

The Avaya VPNremote Phone combined with FVX538, provides a secure solution for remote worker telephony over any broadband Internet connection. The Avaya VPNremote Phone Xauth implementation demonstrated successful interoperability with the Netgear ProSafe VPN Firewall FVX538.

10. References

Avaya Application Notes and Resources Web Site:

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

Avaya Product Support Web Site:

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

[1] ***Avaya VPNremote for the 4600 Series IP Telephones Release 2.1 Administrator Guide,*** Doc ID: 19-600753, Issue 3, June 2007

[2] ***VPNremote for 4600 Series IP Telephone Installation and Configuration Quick Start,*** Doc ID: 19-601608, Issue 2, June 2007

[3] ***Administrators Guide for Avaya Communication Manager*****,** Doc ID: 03-300509, Issue 3.1, February 2007

[4] ***Application Notes for Configuring Avaya WebLM License Manager for Avaya VPNremote™ Phone Release 2,*** Issue 1.0, October 25 2006, Avaya Application Note

Netgear Product Support Web Site:

http://www.netgear.com/

[5] ***ProSafe VPN Firewall FVX538 Reference manual,*** January 2007, Doc # 202-10062-05 v1.0

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 Solution & Interoperability Test Lab at interoplabnotes@list.avaya.com