



**Application Notes for Configuring an VPN Tunnel using IPsec between Fortinet FortiGate Network Security Platforms and Appliances and Avaya 9600 Series IP Phones - Issue 1.1**

**Abstract**

These Application Notes describe the procedures for configuring a Virtual Private Network (VPN) tunnel using Internet Protocol Security (IPsec) between Fortinet FortiGate Network Security Platforms and Appliances and Avaya 9600 Series IP (H.323) Phones.

Fortinet offers security platform models to satisfy various deployment requirements from the FortiGate-20 series for small offices to the FortiGate-5000 series for very large enterprises, service providers and carriers. Each FortiGate includes a wide range of security and networking functions. These Application Notes focus on the FortiGate 60C VPN functionality using IPsec. Both the FortiGate 60C and 300C were compliance tested.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

# 1. Introduction

These Application Notes describe the procedures for configuring a Virtual Private Network (VPN) tunnel using Internet Protocol Security (IPsec) between Fortinet FortiGate Network Security Platforms and Appliances and Avaya 9600 Series IP (H.323) Phones.

Fortinet offers security platform models to satisfy various deployment requirements from the FortiGate-20 series for small offices to the FortiGate-5000 series for very large enterprises, service providers and carriers. Each FortiGate includes a wide range of security and networking functions, including:

- Firewall, VPN, and Traffic Shaping
- Intrusion Prevention System (IPS)
- Antivirus/Antispyware/Antimalware
- Integrated Wireless Controller
- Application Control
- Data Loss Prevention (DLP)
- Vulnerability Management
- IPv6 Support
- Web Filtering
- Anti-spam
- VoIP Support
- Layer 2/3 Routing
- WAN Optimization & Web Caching

These Application Notes focus on the FortiGate 60C VPN functionality using IPsec. Both the FortiGate 60C and 300C were compliance tested.

## 2. General Test Approach and Test Results

This section details the general approach to the testing, what was covered, and results of the testing.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

### 2.1. Interoperability Compliance Testing

The objective of the compliance testing was to verify interoperability between the Avaya 9600 Series IP phones with VPN mode enabled and the Fortinet FortiGate 60C. The testing focused on establishment of the VPN tunnel using IPsec and basic call functionality (voice paths, hold, resume, mute, transfer, conference, etc.) after the tunnel was established.

## 2.2. Test Results

All compliance test cases passed successfully with the following exception/observation:

- If the FortiGate is rebooted after a VPN tunnel is already established from a VPN phone, the phone will be out of service until the VPN phone is restarted. Note, the phone's display will indicate that the tunnel was lost and the phone will automatically attempt to reestablish the VPN tunnel; however since the phone is still using port 4500 for the current (lost) tunnel, and the FortiGate is only expecting new tunnels on port 500 after it is rebooted, the tunnel isn't reestablished until the phone restarts and then uses port 500 again. It is during the Internet Key Exchange (IKE) exchange that the VPN phone and FortiGate change from port 500 to 4500. Fortinet expects to have a fix for this issue by the time this document is published.

Fortinet has supplied the following statement with regards to the test results:

“This statement relates to the interoperability and compliance testing conducted in May 2012 at Avaya facilities in Colorado, USA, using the FortiGate 60C and 300C models running FortiOS v4.3.7 (4.0-MR3-patch7) firmware.

Fortinet, Inc confirms that the VPN and stateful firewall functionality demonstrated in the compliance testing with the Avaya Aura® Communication Manager 6.0.1 and Avaya 9600 Series IP (H.323) Deskphones is consistent across all FortiGate and FortiWIFI models which run FortiOS v4.3.7. Therefore, Fortinet believes the compliance testing results from the FortiGate 60C and 300C testing is representative of the results expected for any other FortiGate or FortiWIFI model.”

## 2.3. Support

For Fortinet FortiGate technical support and information, contact Fortinet at:

- **Phone:** 1-866-648-4638
- **Web:** [http://www.fortinet.com/support/contact\\_support.html](http://www.fortinet.com/support/contact_support.html)

### 3. Reference Configuration

The figure below shows the sample configuration used during compliance testing. A corporate office environment was created consisting of Avaya Aura® Communication Manager, various Avaya 9600 Series IP Phones, and a Fortinet FortiGate 60C. Additionally, two home office environments were created. Each home office had a home router with NAT enabled and two Avaya 9600 Series IP (H.323) phones. The phones, at the home offices, are used DHCP to obtain their IP address. Initially, the phones are assigned with IP address on the 192.168.1.0/24 network by their local router. When the phones establish with a VPN tunnel, they are assigned with IP address on the 10.64.28.0/24 network.

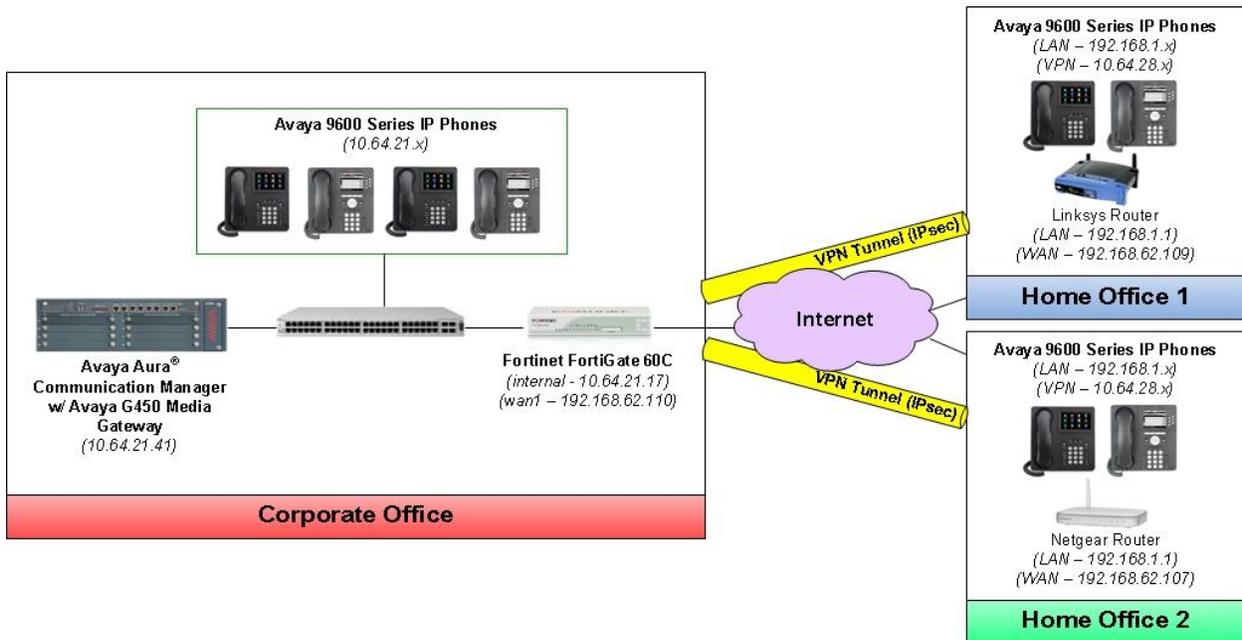


Figure 1: Fortinet FortiGate VPN Configuration

### 4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager running on Avaya S8300D Server with G450 Gateway	Avaya Aura® Communication Manager 6.0.1 (R016x.00.1.510.1) with Patch 19528
Avaya 9600 Series IP Phones (H.323) <ul style="list-style-type: none"> <li>96x0</li> <li>96x1</li> </ul>	<ul style="list-style-type: none"> <li>96xx-IPT-H323-R3_1_4-031612</li> <li>96x1-IPT-H323-R6_2_0_09_02812</li> </ul>
Fortinet FortiGate 60C	v4.0,build0535,120511 (MR3 Patch 7)

## 5. Configure Avaya 9600 Series IP Phones

This section describes the steps required to configure the VPN settings on Avaya 9600 Series IP Phones. Note that VPN-enabled firmware must be installed on the phone prior to the phone being deployed at a remote location.

The Avaya 96xx Series IP Phone configuration can be administered centrally from an HTTP server through the 46xxsettings.txt file or locally on the phone. The parameters that were configured during compliance testing are shown below. The default values were used for all other VPN parameters. For security purposes, actual public IP addresses used during compliance testing were changed to 192.168.x.x in this section.

**SET NVVPNMODE = 1** enables the VPN client  
**SET VPNPROC = 2** enables VPN procedure View & Modify privileges

**SET NVSGIP = 192.168.62.110** sets the IP address used to access the Fortinet FortiGate  
**SET NVMCIPADD = 10.64.21.41** sets the IP address used to access Communication Manager

**SET NVVPNUSERTYPE = 1** sets user type to “Any”  
**SET NVVPNUSER = test** sets VPN user name  
**SET NVNVPNPSWD = test** sets VPN user’s password  
**SET NVPNPSWDTYPE = 1** saves VPN user’s password in flash

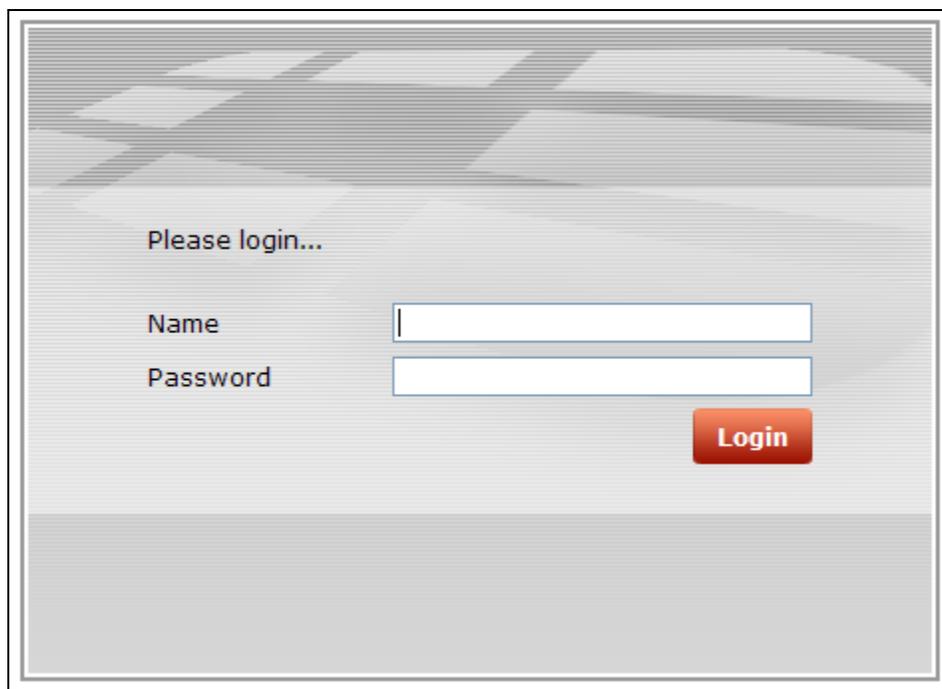
**SET NVIKECONFIGMODE = 1** enables IKE configuration mode  
**SET NVIKEEXCHGMODE = 1** sets the exchange method to Aggressive for IKE Phase 1  
**SET NVIKEIDTYPE = 11** sets the IKE Identifier type for the IKE-ID  
**SET NVIKEID = ipsecvpn** sets the IKE-ID used during Phase 1 negotiation  
**SET NVIKEAUTHTYPE = 4** sets authentication method to PSK with XAUTH  
**SET NVVPNSVENDOR = 4** sets the security gateway Vendor to “other”  
**SET NVIKEPSK = interop123** sets the PSK (note in actual deployments, it is recommended that user enter his/her Preshared Key using phone's dial pad rather than storing the value in the phone)  
**SET NVIKEDHGRP = 5** sets the value of the DH group used during Phase 1 negotiation  
**SET NVPFSDHGRP = 5** sets the value of the DH group used during Phase 2 negotiation

## 6. Configure Fortinet FortiGate 60C

This section describes the steps required to configure the Fortinet FortiGate 60C VPN functionality. It is assumed that the basic installation and configuration of the FortiGate has already been completed. For security purposes, actual public IP addresses used during compliance testing were changed to 192.168.x.x in this section.

### 6.1. Web-based Manager

Using HTTP or a secure HTTPS connection from any management computer running a web browser, connect to the FortiGate web-based manager to configure and manage the FortiGate unit. Enter the IP address of the FortiGate 60C in a web browser. Log in using appropriate credentials.



The image shows a screenshot of the FortiGate web-based manager login interface. The page has a light gray background with a subtle geometric pattern. At the top, there is a header area with a dark gray background and a white geometric pattern. Below the header, the text "Please login..." is displayed in a dark gray font. Underneath, there are two input fields: "Name" and "Password". The "Name" field is a white rectangular box with a thin blue border. The "Password" field is a white rectangular box with a thin blue border. To the right of the "Password" field, there is a red button with the word "Login" in white text. The entire login form is enclosed in a thin black border.

The System→Dashboard→Status screen is displayed after logging in.

**FortiGate 60C**

Help Wizard Logout **FORTINET**

System Dashboard Status Usage Network Config Admin Certificates Monitor

Router Policy Firewall Objects UTM Profiles VPN User WiFi Controller Log&Report

Widget Dashboard

**System Information**

Host Name	FGT60C3G12004480 [Change]
Serial Number	FGT60C3G12004480
Operation Mode	NAT [Change]
HA Status	Standalone [Configure]
System Time	Tue Jun 5 13:36:12 2012 [Change]
Firmware Version	v4.0,build0535,120511 (MR3 Patch 7) [Update] [Details]
System Configuration	Last Backup: Fri May 25 17:38:54 2012 [Backup] [Restore]
Current Administrator	admin [Change Password] / 1 in Total [Details]
Uptime	6 day(s) 20 hour(s) 25 min(s)
Virtual Domain	Disabled [Enable]

**Unit Operation**

FortiAnalyzer FortiManager FortiGuard

FortiGate 60C

INTERNAL

1 2 3 4 5 WAN1 WAN2 DMZ

Reboot Shutdown

**License Information**

**Support Contract**

Registration	Registered (Login: mjherman@avaya.com) [Login Now] ✓
Hardware	8 x 5 support (Expires: 2012-07-20) ✓
Firmware	8 x 5 support (Expires: 2012-07-20) ✓
Enhanced Support	24 x 7 support (Expires: 2012-07-20) ✓
Comprehensive Support	24 x 7 support (Expires: 2012-07-20) ✓

**FortiGuard Services**

AntiVirus	Licensed (Expires 2012-07-20) ✓
IPS	Licensed (Expires 2012-07-20) ✓

**Alert Message Console**

- 2012-06-04 16:42:48 Failed admin authentication attempt for admin
- 2012-06-04 16:42:44 Failed admin authentication attempt for admin
- 2012-05-30 15:36:11 New firmware is available from FortiGuard
- 2012-05-29 17:11:01 System restart

**Top Sessions (By Source Address - 2012-06-05 13:36:15)**

10.64.21.66	8
wan1	4
205.168.62.107	2

## 6.2. Configure Network

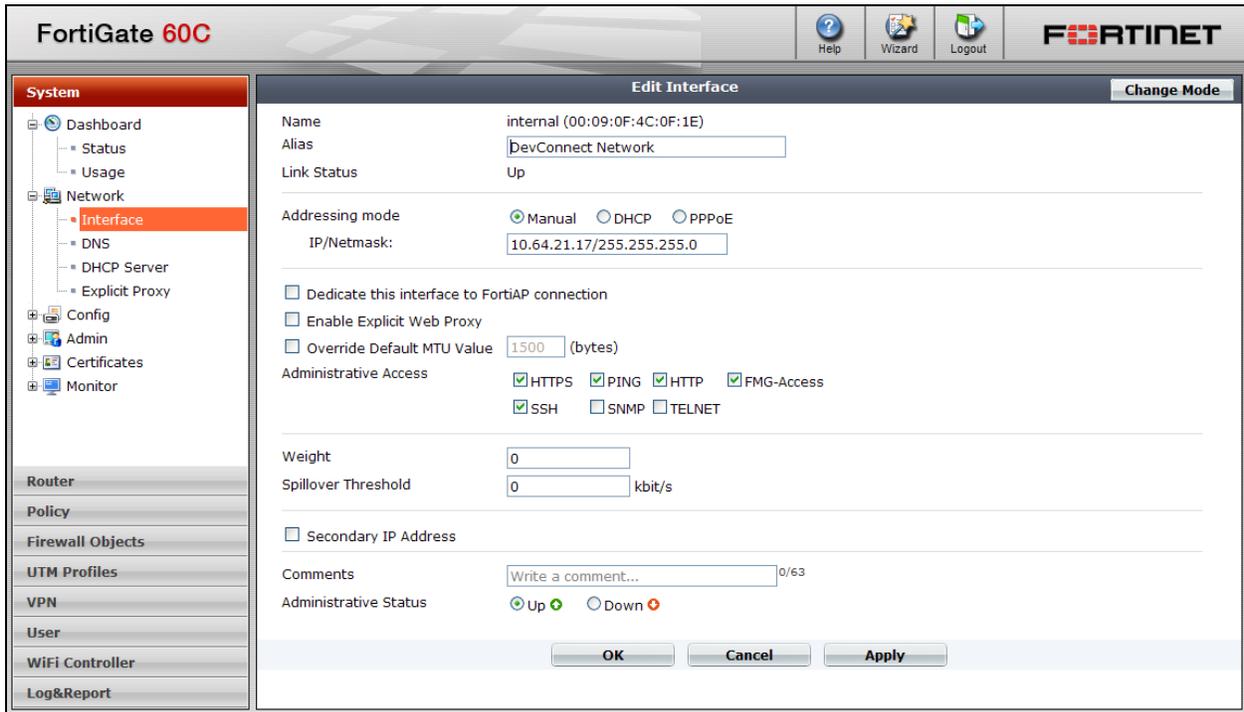
Navigate to **System**→**Network**→**Interface**. Configure the **internal** (private) and **wan1** (public) network interfaces.

The screenshot shows the FortiGate 60C web interface. The left sidebar is expanded to 'System' > 'Network' > 'Interface'. The main content area displays a table of network interfaces. The 'internal' interface is selected, indicated by a checked checkbox.

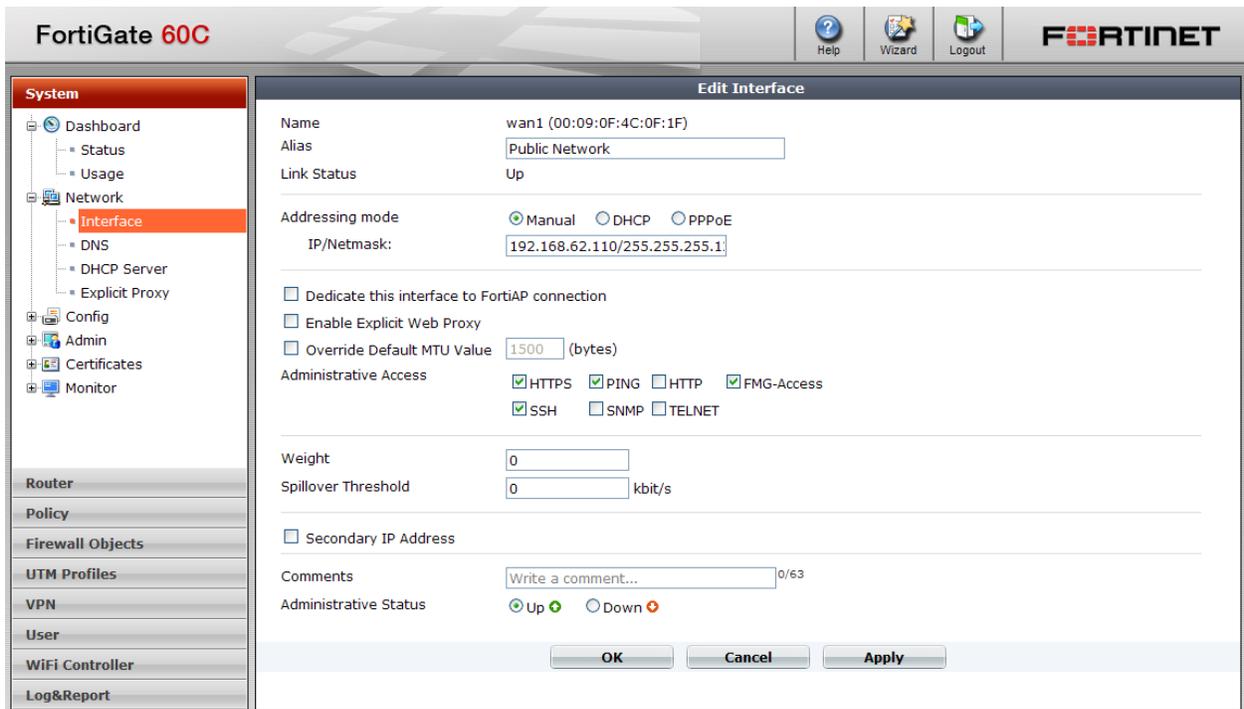
	Name	IP/Netmask	Access	Administrative Status	Link Status	Type	Ref.
<input type="checkbox"/>	dmz	10.10.10.1 / 255.255.255.0	HTTPS,PING,FMG-Access	⬆	⬆	Physical	0
<input checked="" type="checkbox"/>	internal (DevConnect Network)	10.64.21.17 / 255.255.255.0	HTTP,HTTPS,PING,SSH,FMG-Access	⬆	⬆	Physical	5
<input type="checkbox"/>	wan1 (Public Network)	205.168.62.110 / 255.255.255.128	HTTPS,PING,SSH,FMG-Access	⬆	⬆	Physical	5
<input type="checkbox"/>	wan2	192.168.101.99 / 255.255.255.0	PING,FMG-Access	⬆	⬆	Physical	0

To modify an existing interface, check the checkbox next to the interface and then click **Edit**.

The **Edit Interface** screen is displayed. Enter an **Alias** (optional) and the **IP/Netmask** for the interface. The **internal** interface used during compliance testing is shown below.



The **wan1** interface configuration used during compliance testing is shown below.

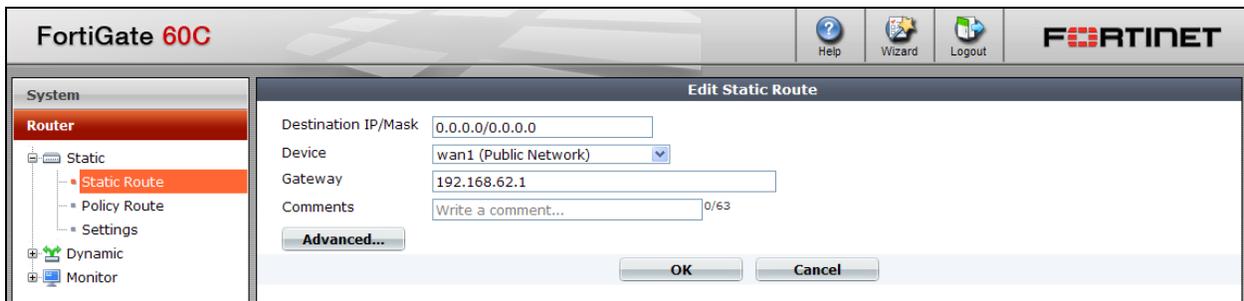


### 6.3. Configure Router

Navigate to **Router**→**Static Route**. Only one default static route to the public interface was created for compliance testing.

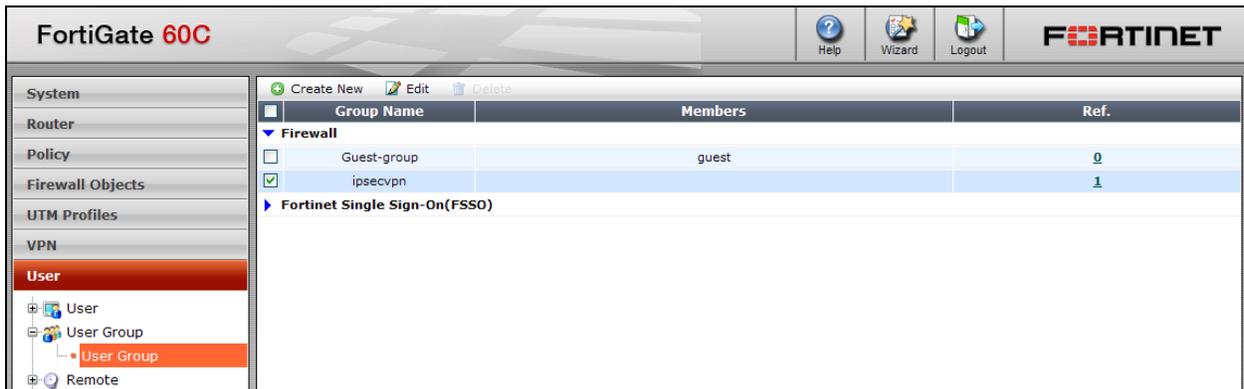


The configuration of the static route is shown below.

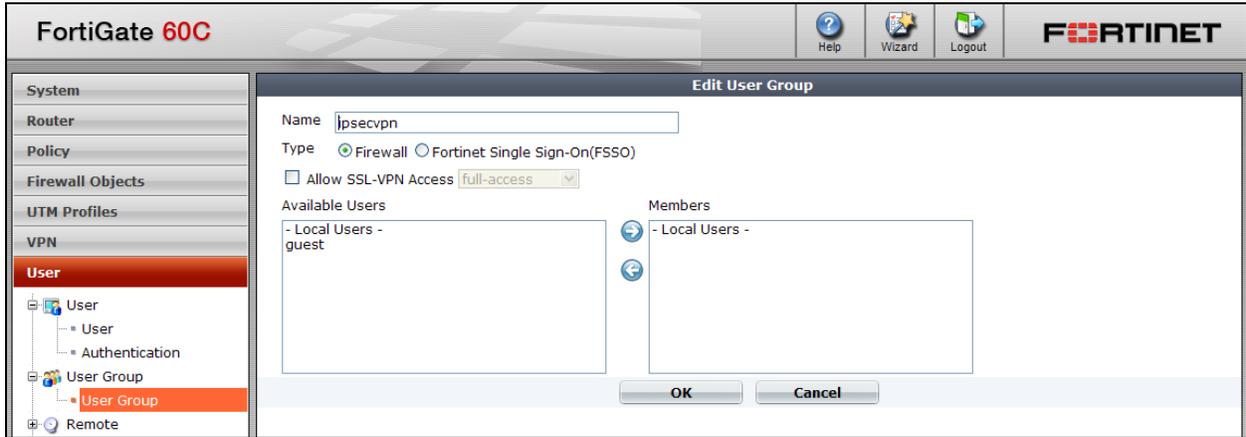


### 6.4. Configure User Group

Navigate to **User**→**User Group**. Create or Modify an existing group. The user group **ipsecvpn** was used for compliance testing. To view/modify an existing group, check the appropriate checkbox and click **Edit**.

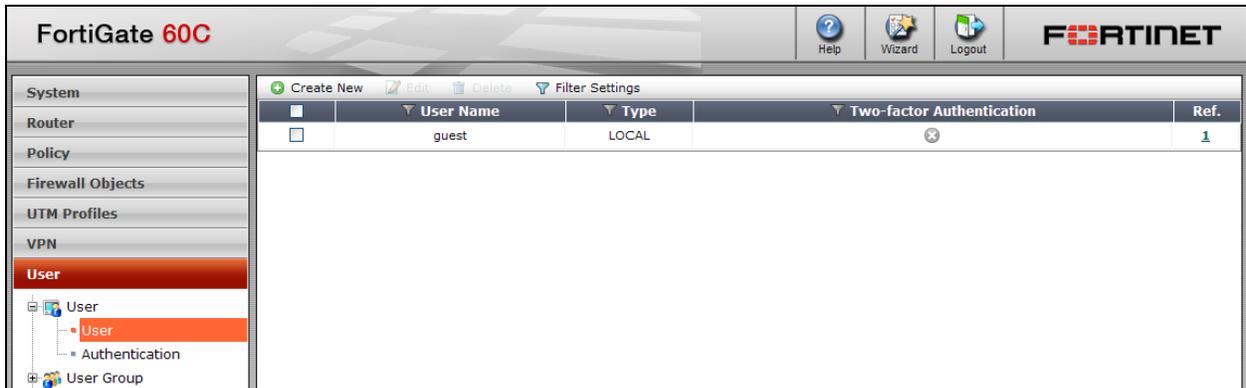


The **Edit User Group** screen is displayed. The screen below shows the values used for the **ipsecvpn** user group.

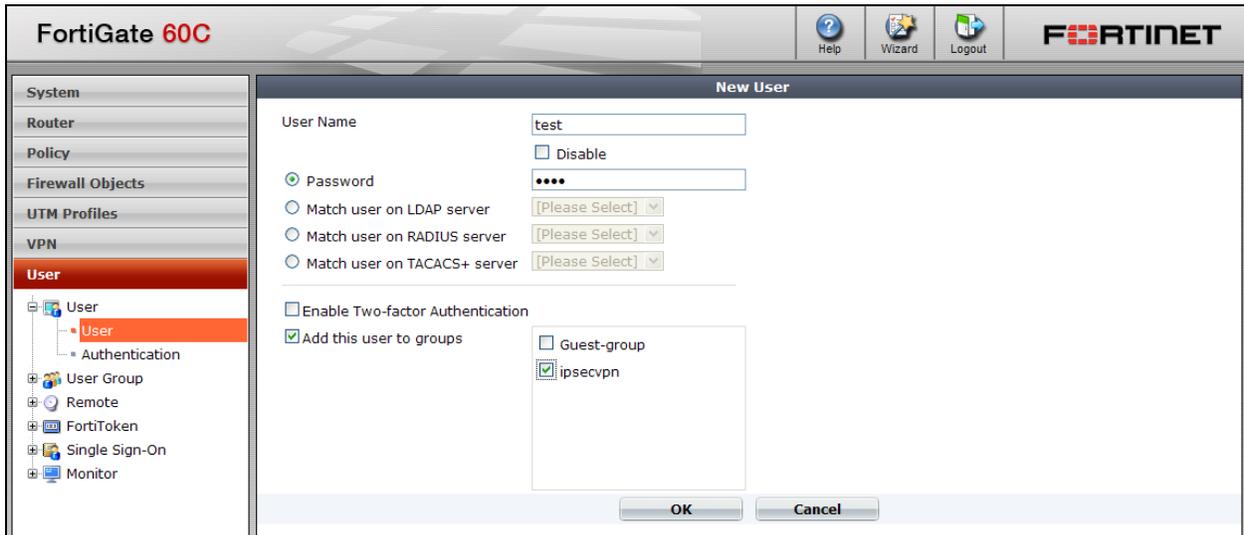


## 6.5. Configure User

Navigate to **User**→**User**→**User**. Click **Create New** to add a new user.

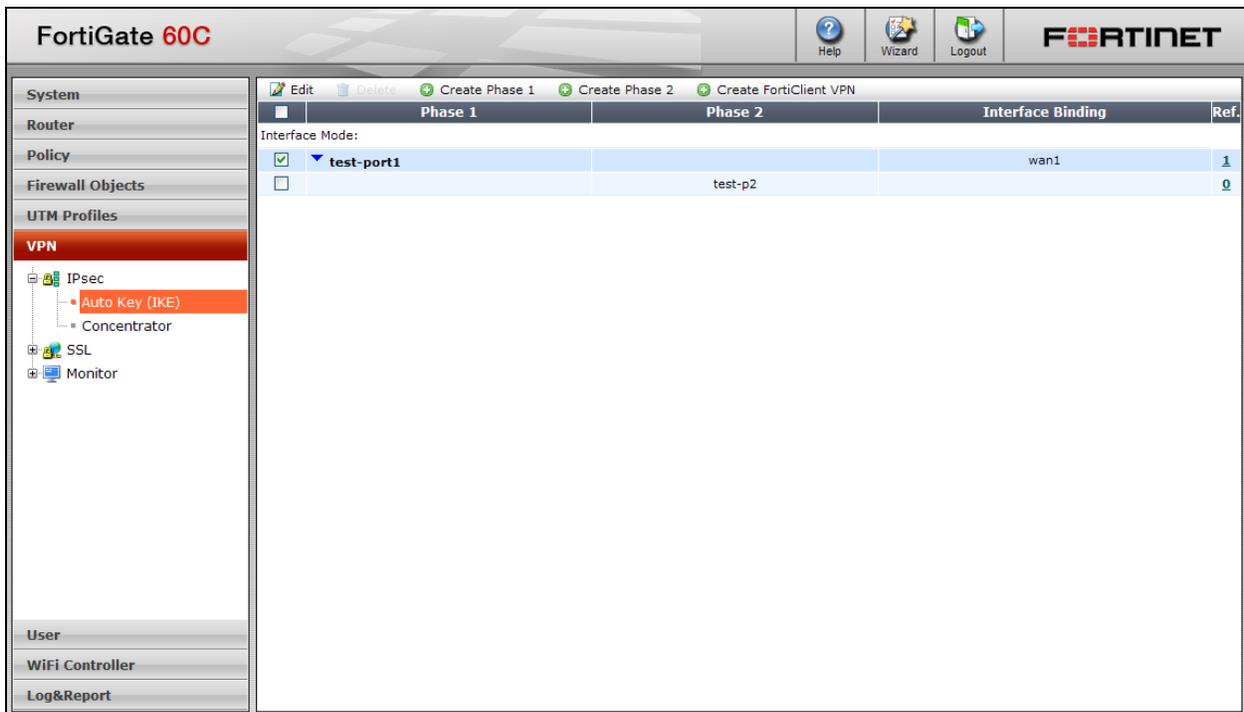


The **New User** screen is displayed. Enter a **User Name** and **Password**. Check the box for **Add this user to groups** and check the user group created in **Section 6.4**.



## 6.6. Configure VPN

With the web-based manager, navigate to **VPN→IPsec→Auto Key (IKE)**. As shown below, **test-port1** for Phase 1 and **test-p2** for Phase 2 were created for compliance testing. To view or modify Phase1 check the appropriate checkbox and click **Edit**.



The **Edit Phase 1** screen is shown below with the configuration used during testing. Select **Dialup User** for the **Remote Gateway** and set the **Mode** to **Aggressive**. This allows the FortiGate to dynamically add tunnel routes as IPsec connections are made from the VPN phones.

**FortiGate 60C** Help Wizard Logout **FORTINET**

**System**  
Router  
Policy  
Firewall Objects  
UTM Profiles  
**VPN**  
IPsec  
Auto Key (IKE)  
Concentrator  
SSL  
Monitor  
User  
WiFi Controller  
Log&Report

**Edit Phase 1**

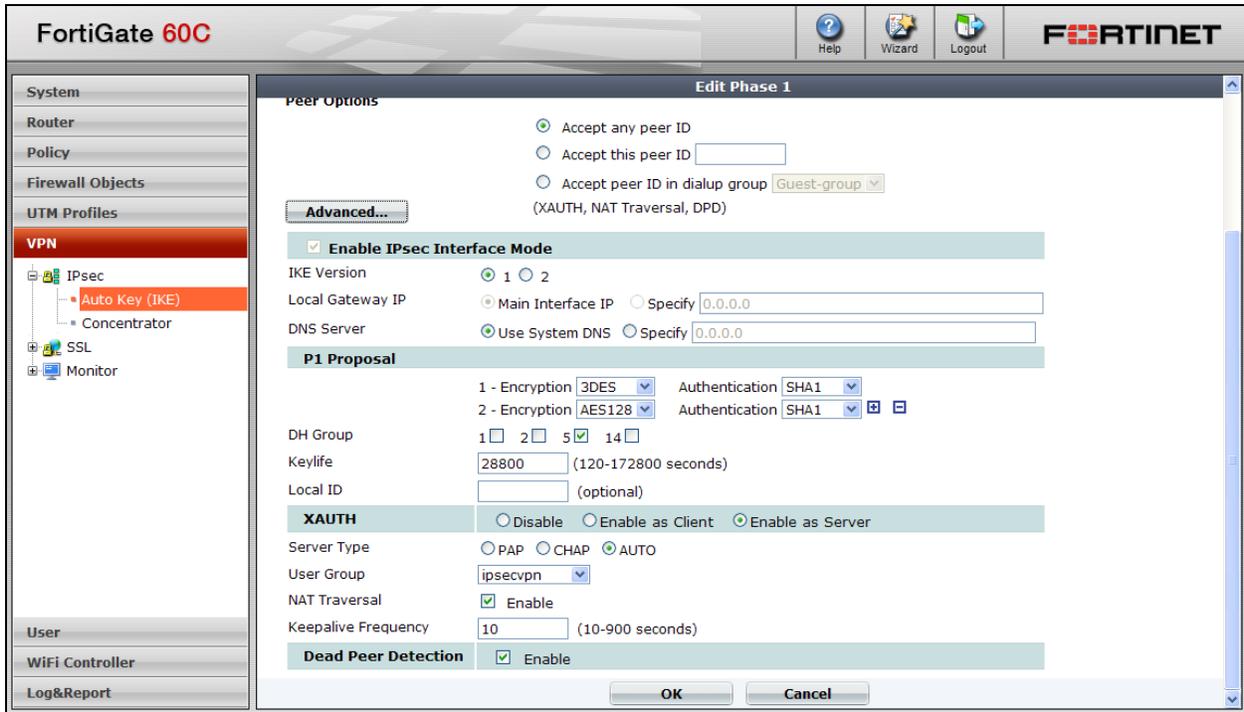
Name: test-port1  
Remote Gateway: Dialup User  
Local Interface: wan1(Public Network)  
Mode:  Aggressive  Main (ID protection)  
Authentication Method: Preshared Key  
Pre-shared Key: .....

**Peer Options**

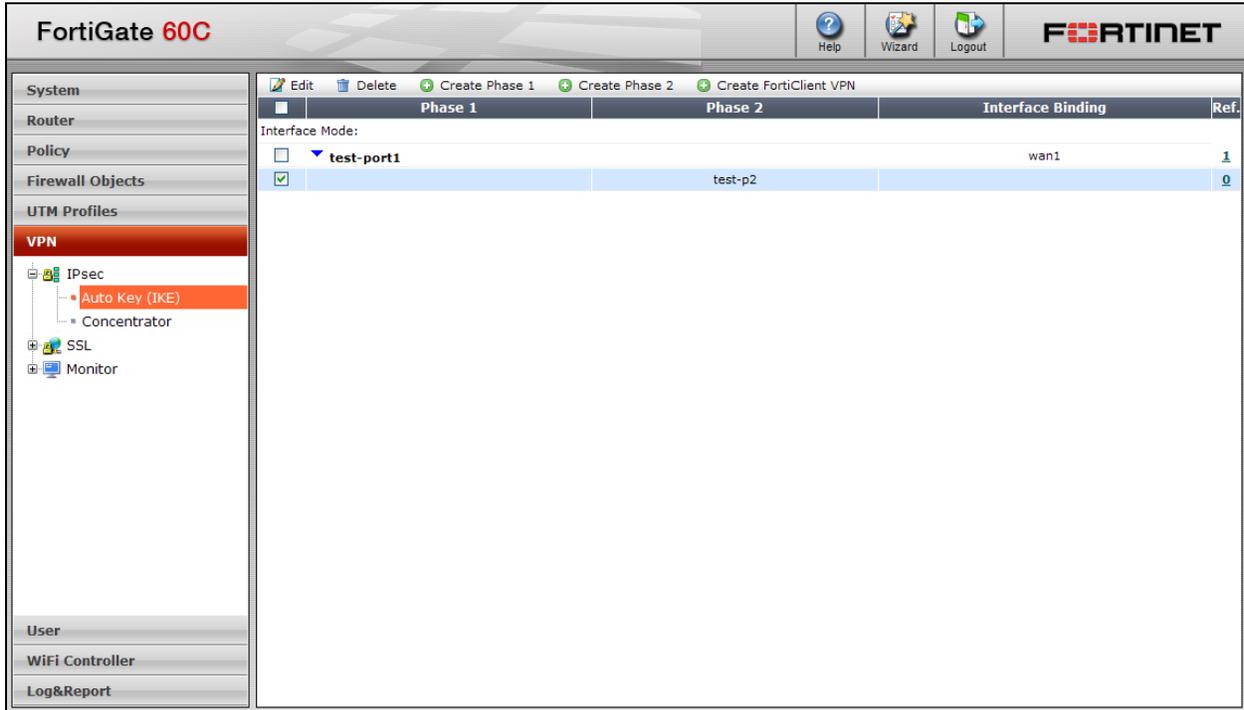
Accept any peer ID  
 Accept this peer ID:   
 Accept peer ID in dialup group: Guest-group  
(XAUTH, NAT Traversal, DPD)

**Advanced...** OK Cancel

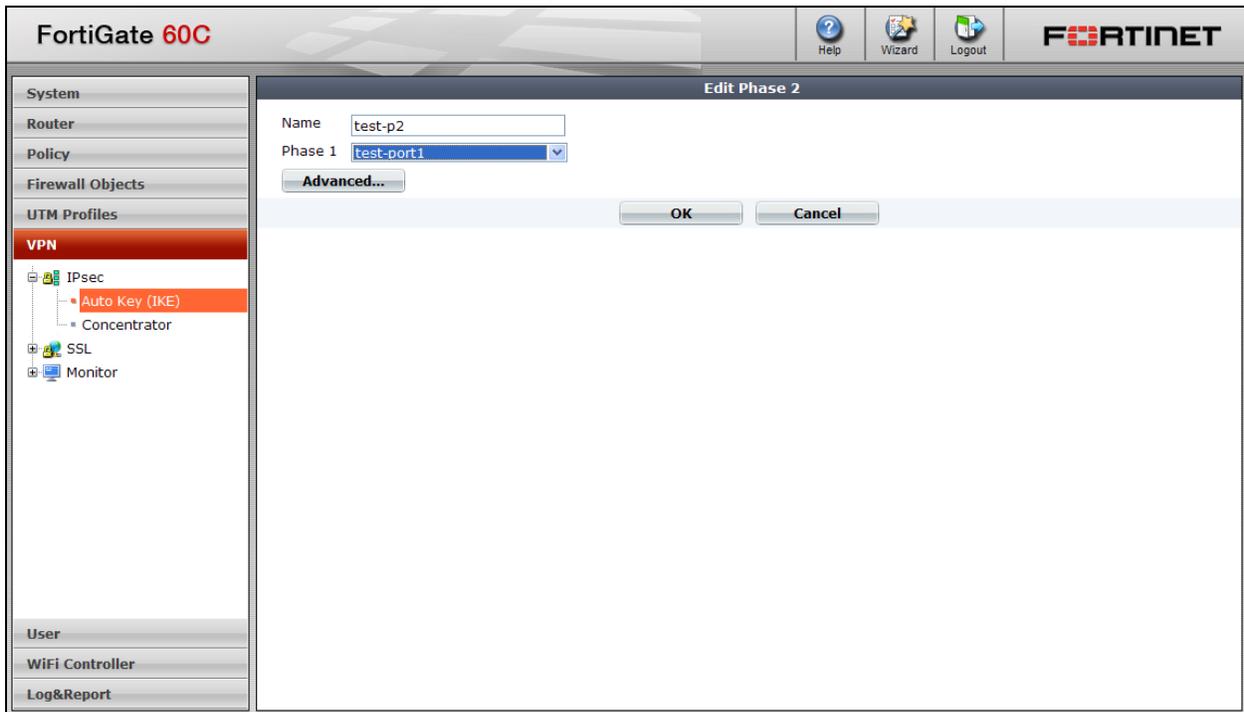
Click the **Advanced...** button to view more details. Note, the **Enable IPsec Interface Mode** checkbox was checked, and **XAUTH** was set to **Enable as Server** with the **User Group** created earlier (i.e. **ipsecvpn**) selected.



Navigate back to **VPN→IPsec→Auto Key (IKE)**. To view or modify Phase 2 check the appropriate checkbox and click **Edit**.



The **Edit Phase 2** screen is shown below with the configuration used during testing.



Confirm the IKE Configuration Method is enabled, which can only be done through the FortiGate command line interface. Use a secure shell client to access the FortiGate. After logging in, use the **config**, **edit**, and **set** commands shown in bold below to set the **type** and **mode-cfg** values. The **type** keyword determines whether the administrator is creating a server or a client. Setting **type** to dynamic creates a server configuration, otherwise the configuration is a client. The **mode-cfg** keyword enables the IKE Configuration Method.

```
config vpn ipsec phase1-interface
  edit "test-port1"
    set type dynamic
    set interface "wan1"
    set xauthtype auto
    set mode aggressive
    set mode-cfg enable
    set proposal 3des-sha1 aes128-sha1
    set authusrgrp "ipsecvpn"
    set ipv4-start-ip 10.64.28.164
    set ipv4-end-ip 10.64.28.173
    set ipv4-netmask 255.255.255.0
    set dns-mode auto
    set unity-support disable
    set psksecret ENC
Cw/KXthp0PQlKB+ZxCYrUYLqfYDOKr9+/Zu6fUnA13RBdgn0yXCNxbx+M7IHUMDAm4G6pZ1r6XL4XedB/SHThA
17W/2a2YWowLSz77JuCIMGTNVk
  next
end
```

Note, the PSK is encrypted in the configuration and can be copied verbatim between FortiGate units. For reference, the Phase 2 configuration is also shown below.

```
config vpn ipsec phase2-interface
  edit "test-p2"
    set keepalive enable
    set phasename "test-port1"
    set proposal 3des-sha1 aes128-sha1
  next
end
```

## 6.7. Policy

Navigate to **Policy**→**Policy**→**Policy**. The screen below shows the policies defined during compliance testing. The policy for “test-port1” references the IPsec tunnel configuration made earlier.

Seq.#	Source	Destination	Authentication	Schedule	Service	Action	Log
▼ internal(DevConnect Network) -> test-port1 (1)							
1	all	all		always	ANY	ACCEPT	
▼ internal(DevConnect Network) -> wan1(Public Network) (1)							
2	all	all		always	ANY	ACCEPT	
▼ test-port1 -> internal(DevConnect Network) (1)							
3	all	all		always	ANY	ACCEPT	
▼ Implicit (1)							
4	all	all		always	ANY	DENY	

To view or modify an existing policy, click on the policy row to high-light it, right-click and then select **Edit**.

The screenshot shows the FortiGate 60C web interface. The left sidebar contains a navigation tree with 'Policy' selected. The main area displays a table of policies. A context menu is open over the first policy row, with 'Edit' selected.

Seq.#	Source	Destination	Authentication	Schedule	Service	Action	Log
▼ internal(DevConnect Network) -> test-port1 (1)							
1	all	all		always	ANY	ACCEPT	
▼ internal(DevConnect Network) -> wan1(Public)							
2	all	all		always	ANY	ACCEPT	
▼ test-port1 -> internal(DevConnect Network) (1)							
3	all	all		always	ANY	ACCEPT	
▼ Implicit (1)							
4	all	all		always	ANY	DENY	

The screen below shows the configuration of the **internal (DevConnect Network) → test-port1** policy. Note that during compliance testing, this tunnel for the IPSec tunnel interface does not require a NAT configuration since it joins the two trusted subnets on either end of the IPSec tunnel.

The other policies shown above were configured similarly.

The screenshot displays the FortiGate 60C configuration interface. The main window is titled "Edit Policy" and shows the configuration for a policy named "internal (DevConnect Network)". The configuration details are as follows:

- Source Interface/Zone: internal (DevConnect Network)
- Source Address: all
- Destination Interface/Zone: test-port1
- Destination Address: all
- Schedule: always
- Service: ANY
- Action: ACCEPT

Additional options and their states:

- Log Allowed Traffic
- Enable NAT
- Enable Identity Based Policy
- Resolve User Names Using FSSO Agent
- UTM
- Traffic Shaping
- Enable Endpoint Security (Dropdown: [Please Select])

The comments field is empty, with a character count of 0/63. At the bottom, there are "OK" and "Cancel" buttons.

## 6.8. Configure VPN Phone DHCP IP Address Pool

The VPN phones were assigned IP address for a pool of IP address on the 10.64.28.0/24 network by the FortiGate 60C. To set the IP address pool range, use a secure shell client to access the FortiGate. After logging in, use the **config**, **edit**, and **set** commands shown in bold below to set the **ipv4-start-ip**, **ipv4-end-ip**, and **ipv4-netmask** values.

```
config vpn ipsec phase1-interface
  edit "test-port1"
    set type dynamic
    set interface "wan1"
    set xauthtype auto
    set mode aggressive
    set mode-cfg enable
    set proposal 3des-sha1 aes128-sha1
    set authusrgrp "ipsecvpn"
    set ipv4-start-ip 10.64.28.164
    set ipv4-end-ip 10.64.28.173
    set ipv4-netmask 255.255.255.0
    set dns-mode auto
    set unity-support disable
    set psksecret ENC
Cw/KXthp0PQ1KB+ZxCYrUYLqfYDOKr9+/Zu6fUnA13RBdgn0yXCNxbx+M7IHUMDAm4G6pZ1r6XL4XedB/SHThA
17W/2a2YWowLSz7JuCIMGTNVk
  next
end
```

## 7. Verification Steps

The following steps can be used to verify the configuration:

- Verify VPN connections are successfully established from the VPN phones.
- Verify calls placed between all VPN users and corporate users are successful.
- Verify messages can be left for the VPN phones and that the message waiting indicator on each phone functions correctly.

## 8. Conclusion

These Application Notes describe the procedures for configuring a Virtual Private Network (VPN) tunnel using Internet Protocol Security (IPsec) between Fortinet FortiGate Security Platforms and Appliances and Avaya 9600 Series IP (H.323) Phones. All compliance test cases passed successfully with the one exception/observation noted in **Section 2.2**.

## 9. Additional References

This section references the product documentation relevant to these Application Notes.

Avaya product documentation is available at <http://support.avaya.com>.

Fortinet product documentation is available at <http://docs.fortinet.com/fgt.html>.

[1] *Administering Avaya Aura® Communication Manager*, March 2012

[2] *FortiGate Desktop Install Guide*, March 2009

[3] *FortiOS™ Handbook v3*, March 2012

[4] *FortiOS™ CLI Reference*, February 2012

---

**©2012 Avaya Inc. All Rights Reserved.**

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at [devconnect@avaya.com](mailto:devconnect@avaya.com).