IP Office Technical Tip

Tip no: 184

Release Date: August 14, 2007

Region: GLOBAL

Configuring a VPN Remote IP Phone with a Netgear FVS338 VPN Router

The following document assumes that the user/installer is familiar with configuring both the IP Office and VPN devices, as well as manually configuring IP hard phones. This document is for reference purposes only when creating the VPN tunnels and does not provide any details on how to configure any other aspect of either device.

Test Systems Software Versions and Basic Phone Settings

IP Office Core Software	4.0.7
Netgear FVS338 Router Software	2.0.0-139
IP Phone Model	5610
IP Phone Firmware	2.3.249
IP Office IP Address	192.168.2.5
TFTP/File Server	192.168.2.10
IP Phone IP Address	DHCP
IP Phone CallSV	192.168.2.5
IP Phone CallSVPort	1719 [Default]
IP Phone Router	DHCP
IP Phone Mask	DHCP
IP Phone FileSv	192.168.2.10
IP Phone 802.1Q	Auto
IP Phone VLAN ID	0
Password used during testing	1234567890

Notes

1. The IP Phones may require a Virtual IP Address to be configured in the VPN settings. Please take care in choosing a Virtual IP Range. Consider where the phone is most likely to be used and ensure that the Virtual IP Range selected will not conflict. For instance, many VPN IP Phones may be installed at user's homes. Typically a Home Router uses 192.168.0.x or 192.168.1.x as its internal network range therefore it is recommended that this is not used as a Virtual IP Address Range.

2. **IMPORTANT**: Many VPN Routers will not allow a direct media path to be established between two VPN Endpoints. It will be necessary to uncheck the Direct Media Path checkbox in the Extension Configuration in IP Office. Failure to do so will result in No Speech path when two VPN extensions try and establish a call.

3. Review the Sample 46vpnsetting.txt file for simplifying configuration settings on the IP Phones.

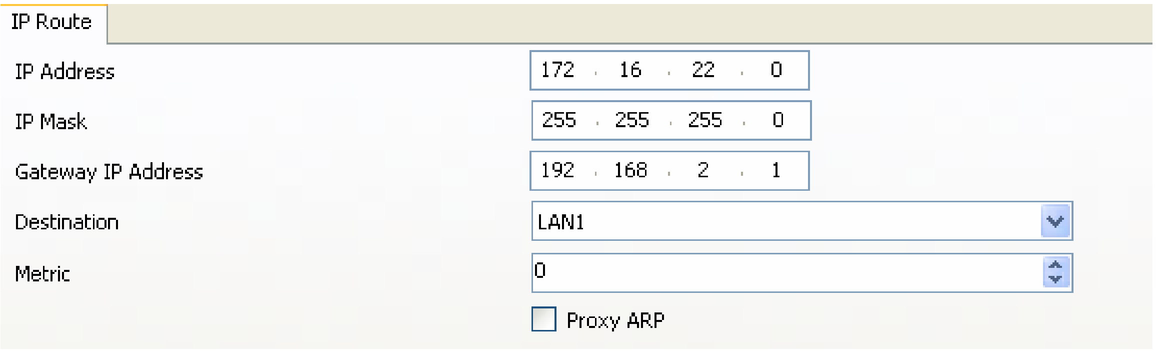
4. While the defaults for Encryption are set at 4500-4500 and these settings do work in most configurations, there may be instances where (depending on what the VPN Router and Home router supports) the user may need to either disable this setting, or change to one of the other options.

5. If manually configuring a Virtual IP Address on the IP Hard-phone, ensure that accurate records are kept of IP Address allocations to avoid IP Address conflicts.

IP Office Configuration

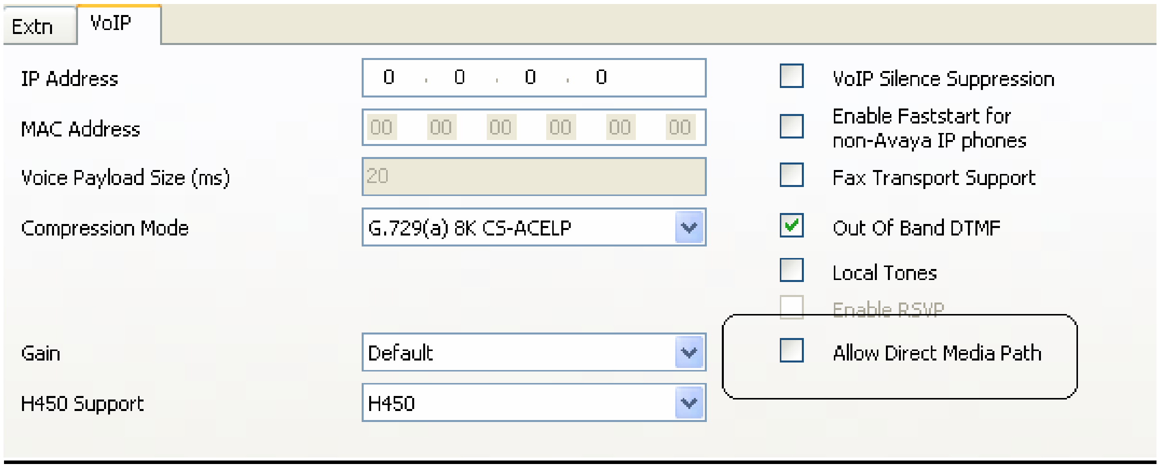
Using IP Office Manager, Open the Configuration and Select IP Routes.

Add a New IP Route for the Virtual LAN Network to be used in the environment.



IP Address	172 . 16 . 22 . 0
IP Mask	255 . 255 . 255 . 0
Gateway IP Address	192 . 168 . 2 . 1
Destination	LAN1
Metric	0
	☐ Proxy ARP

Modify the Extensions – VoIP Tab for those extensions that will be VPN Extensions, and uncheck the Direct Media Path Check Box.



IP Address	0 . 0 . 0 . 0
MAC Address	00 00 00 00 00 00
Voice Payload Size (ms)	20
Compression Mode	G.729(a) 8K CS-ACELP
Gain	Default
H450 Support	H450

□ VoIP Silence Suppression

□ Enable Faststart for non-Avaya IP phones

□ Fax Transport Support

☑ Out Of Band DTMF

□ Local Tones

□ Enable RSVP

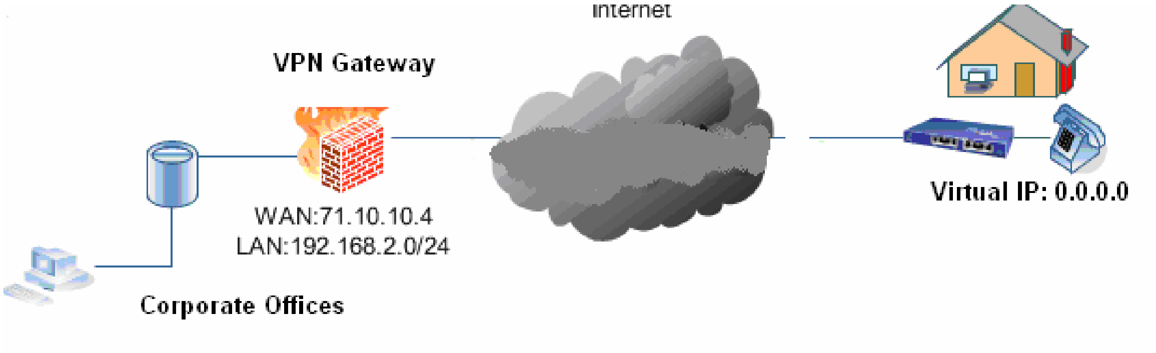
□ Allow Direct Media Path

Netgear FVS-338 VPN Router VPN Configuration settings

There are two methods that can be used to establish VPN connectivity between the VPN Remote Phone and the Netgear FVS338 VPN Router.

Networking Scenario:

Option 1: Mode Config with X-Auth

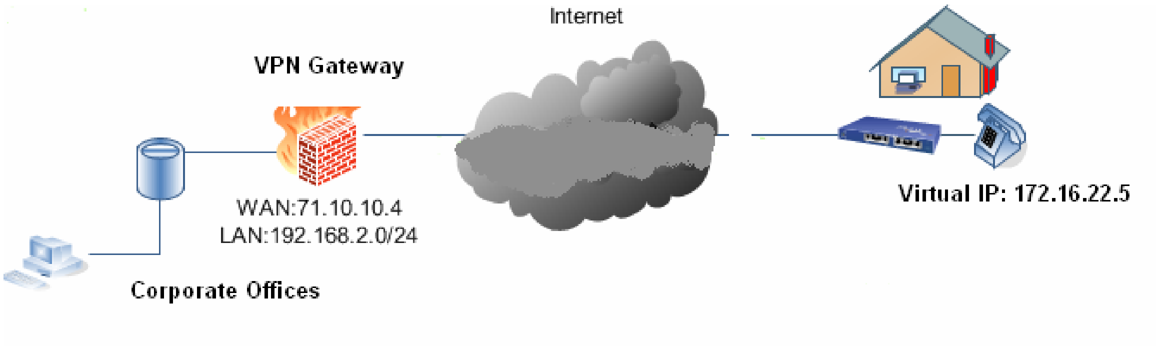


Using Mode Config and X-Auth

The major advantage to using this method is that it is possible to configure the Netgear FVS 388 to dynamically issue IP Addresses to the IP Phone. You do however need to create a user name to be used for authentication; however it is also possible to create a username using the Phones MAC address. This makes it very easy to disable access to a specific device if the need should ever arise.
The vpn settings file can also be configured to use the MAC address for the username authentication
Please note that when using this option, you should select the Juniper PSK with X-Auth option on the VPN Remote Phone Profile.

For configuration settings, refer to pages 6 - 8

Option 2: VPN and IKE Policy



Using a Client VPN Policy

You can either create the policy using the Wizard and go back and edit the settings, or create the IKE and VPN Auto Policy and configure the settings required. Tip: If creating the policy without using the Wizard, Create the IKE policy first and then create the VPN Auto Policy, which will need to be associated to the IKE Policy.

For configuration settings, refer to pages 9 - 12

Netgear FVS338 Option 1: Using Mode Config and X-Auth

Once logged into the FVS338, Select the VPN Option.

Then select Mode Config and Create a New Mode Config Record

Edit Mode Config Record Settings - Option 1				
Client pool				
Record Name	phone			
First Pool	Starting IP	172.16.22.101	Ending IP	172.16.22.110
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	WINS Server IP	Secondary	WINS Server IP
DNS Server	Primary	DNS Server IP	Secondary	DNS Server IP
Traffic Tunnel Security Level				
PFS Key Group – Checked	DH Group 2 [1024 bit]			
SA Lifetime	3600 seconds			
Encryption Algorithm	3DES			
Integrity Algorithm	SHA-1			
Local IP Address	192.168.2.0			
Local Subnet Mask	255.255.255.0			

Once Completed select the VPN Client option, and create a new user. For starters keep things simple and use an easy username and password. But consider using the MAC address as the username for the phones once ready for deployment, and review the options available to you in the 46vpnsetting.txt file for simplifying the configuration of the phones

Edit VPN Client – User Database Settings - Option 1	
Add New User	
Username	vpnphone
Password	1234567890
Confirm password	1234567890

Now Select the Policies Menu and Create a New IKE Policy. Note that as you are using a Mode Config, a VPN policy will not be used as these have already been configured in the Mode Config settings screen.

Edit IKE Policy Settings - Option 1	
Mode Config Record	
Do you want to use Mode Config Record	Yes
Select Mode Config Record	phone
General	
Policy Name	phone
Direction / Type	Cannot be selected (Responder)

Exchange Mode	Aggressive
Local	
Identifier Type	Local Wan IP
Identifier	Cannot be selected
Remote	
Identifier Type	FQDN
Identifier	fvs_remote
IKE SA Parameters	
Encryption Algorithm	3DES
Authentication Algorithm	SHA-1
Authentication Method	Pre Shared Key
Pre Shared Key	1234567890
Diffie-Hellman (DH)	Group 2 (1024 bit)
SA-Lifetime (secs)	3600
Extended Authentication	
XAUTH Configuration	Select Edge Device
Authentication Type	User Database

Option 1: VPN Remote Phone Settings

Please ensure that when selecting the VPN Profile to be used, select the option for Juniper with X-Auth

VPN Remote Phone Configuration - Option 1	
VPN Profile	Juniper with XAuth
Server	71.10.10.4
Username	vpnphone
Password	1234567890
Group Name	fvs_remote
Group PSK	1234567890
IKE Parameters	
IKE ID Type	FQDN
Diffie Hellman Group	2
Encryption ALG	3DES
Authentication ALG	Sha1
IKE Xchange Mode	Aggressive
IKE Config Mode	Enabled
XAUTH	Enable
Cert Expiry Check	Disable
Cert DN Check	Disable
IPSEC Parameters	
Encryption ALG	3DES
Authentication ALG	Sha1
Diffie Hellman Group	2
VPN Start Mode	Boot
Password Type	Save in Flash

Encapsulation	4500-4500
Protected Nets	
Virtual IP	0.0.0.0
Remote Net #1	192.168.2.0/24
Remote Net #2	
Remote Net #3	
Copy TOS	No
Connectivity Check	Always

Netgear FVS338 Option 2 – IKE and VPN Policy Settings

To Create a VPN and IKE Policy, either the Wizard can be used to setup most of the basic settings, and then each profile with specific needs, or create the IKE and VPN Policy without the Wizard. If creating the VPN policy without the wizard, it helps to have the IKE Policy created before creating the VPN Policy.

If you use the Wizard, Select the VPN Client option rather than the VPN Gateway option to be sure to create the correct policy.

Details of settings used during testing are listed below.

The settings below can be referred to regardless of whether the wizard was used or not to create the policy.

Once logged into the FVS338, Select the VPN Option.

Create a New IKE Policy. (Policies Tab)

Edit IKE Policy Settings - Option 2	
Mode Config Record	
Do you want to use Mode Config Record	No
Select Mode Config Record	Cannot be selected
General	
Policy Name	ip
Direction / Type	Responder
Exchange Mode	Aggressive
Local	
Identifier Type	Local Wan IP
Identifier	Cannot be selected
Remote	
Identifier Type	FQDN
Identifier	fvx_remote
IKE SA Parameters	
Encryption Algorithm	3DES
Authentication Algorithm	SHA-1
Authentication Method	Pre Shared Key
Pre Shared Key	1234567890
Diffie-Hellman (DH)	Group 2 (1024 bit)
SA-Lifetime (secs)	28800
Extended Authentication	
XAUTH Configuration	None
Authentication Type	N/A

Once the IKE policy has been successfully created, create a new VPN Auto Policy

Edit VPN Policy Settings - Option 2	
General	
Policy Name	ip
Policy Type	Auto
Remote Endpoint	Remote_fvx
Traffic Selection	
Local IP	Subnet
Start IP Address	192.168.2.0
Subnet Mask	255.255.255.0
Remote IP	Any
Traffic Tunnel Security Level	
PFS Key Group – Checked	DH Group 2 [1024 bit]
SA Lifetime	3600 seconds
Encryption Algorithm	3DES
Integrity Algorithm	SHA-1
Local IP Address	192.168.2.0
Local Subnet Mask	255.255.255.0

Option 2: VPN Remote Phone Settings

VPN Remote Phone Configuration - Option 2	
VPN Profile	Generic PSK
Server	71.10.10.4
IKE ID	fvx_remote
PSK – (Pre Shared Key)	1234567890
IKE Parameters	
IKE ID Type	FQDN
Diffie Hellman Group	2
Encryption ALG	3DES
Authentication ALG	Sha1
IKE Xchange Mode	Aggressive
IKE Config Mode	Disabled
XAUTH	Disable
Cert Expiry Check	Disable
Cert DN Check	Disable
IPSEC Parameters	
Encryption ALG	3DES
Authentication ALG	Sha1
Diffie Hellman Group	2

VPN Start Mode	Boot
Password Type	Save in Flash
Encapsulation	4500-4500
Protected Nets	
Virtual IP	172.16.22.5
Remote Net #1	192.168.2.0/24
Remote Net #2	
Remote Net #3	
Copy TOS	No
Connectivity Check	Always

Issued by:
Avaya SSD Tier 4 Support
Contact details:-

EMEA/APAC
Tel: +44 1707 392200
Fax: +44 (0) 1707 376933
Email: gsstier4@avaya.com

NA/CALA
Tel: +1 732 852 1955
Fax: +1 732 852 1943
Email: IPOUST4ENG@Avaya.com