IP Office Technical Tip

Tip no: **196**
Release Date: **January 8, 2008**

Region: **GLOBAL**

Configuring a VPN Remote IP Phone with a Netgear FVX538 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 FVX538 Router Software	2.1.3-17
IP Phone Model	5610
IP Phone Firmware	2.3.252
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

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 if the router does not support direct media paths between two VPN endpoints. 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.

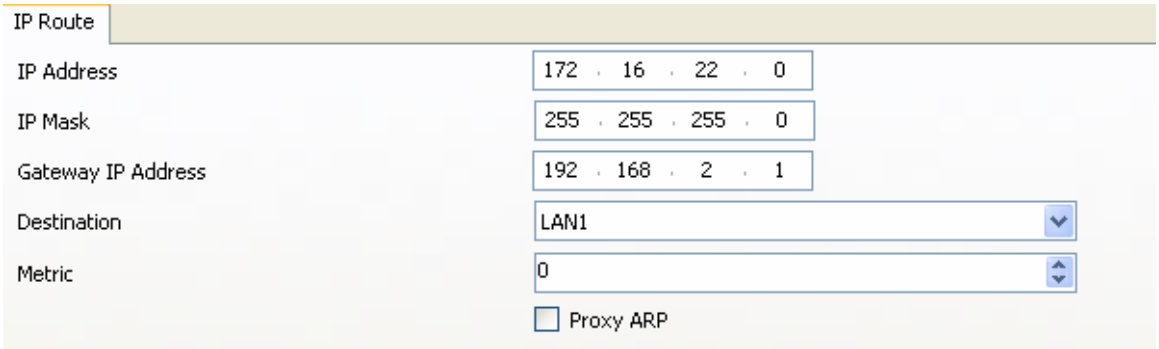
4. While the defaults for Encryption are set at 4500-4500 and these settings are preferred, there may be instances where (depending on what the Home router supports) the user may need to either disable this setting, or change to one of the other options.

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.

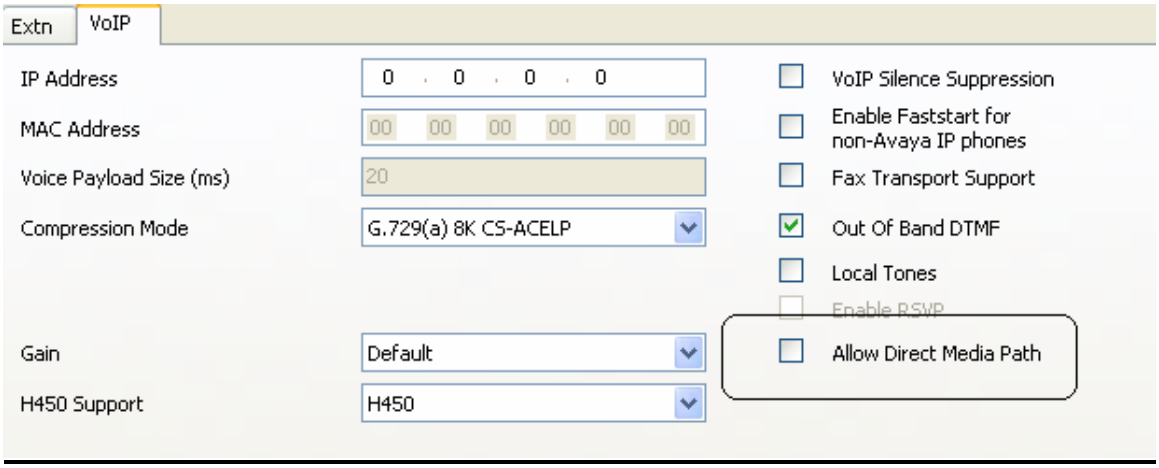
IP Office Configuration

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.



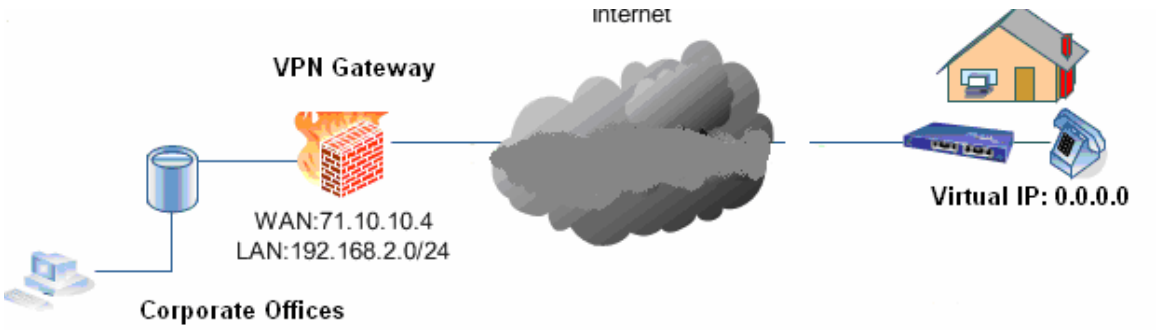
Modify the Extensions – VoIP Tab for those extensions that will be VPN Extensions, and uncheck the Direct Media Path Check Box. (As Required)



Netgear FVX538 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 FVX538 VPN Router.

Networking Scenario:



Mode Config and X-Auth

The advantage to using this method is that it is possible to configure the Netgear FVX538 to dynamically issue IP Addresses to the IP Phone. You do however need to create a user name to be used for authentication. This makes it easier to disable access to a specific device if the need should ever arise.
Please note that when using this option, you should select the Juniper PSK with X-Auth option on the VPN Remote Phone Profile.

Netgear FVX538 Mode Config and X-Auth

Once logged into the FVX538, Select the VPN Option.

Then select Mode Config and Create a New Mode Config Record

Edit Mode Config Record Settings				
Client pool				
Record Name		Vpn_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.

- TIP: Using the Serial Number of the IP Phone as the Username. Configure the 46vpnsetting.txt file and consider using the [SET NVVPNUSER %SERIALNUM%] option. Assign a common password to all Users and use the [SET NVVPNPSWD] option.
- Note: Some phones' Serial Numbers may contain letters, while others will be all numbers. Letters must be entered in Capitals, not lower case or the Router will not accept the username and authentication will fail

Edit VPN Client – User Database Settings	
Add New User	
Username	[Phones Serial Number]
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	
Mode Config Record	
Do you want to use Mode Config Record	Yes
Select Mode Config Record	Vpn_phone
General	
Policy Name	Vpn_phone

Direction / Type	Responder
Exchange Mode	Aggressive
Local	
Identifier Type	Local Wan IP
Identifier	Cannot be selected
Remote	
Identifier Type	FQDN
Identifier	VPNPHONE
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

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	
VPN Profile	Juniper with XAuth
Server	71.10.10.4
Username	[Phones Serial Number]
Password	1234567890
Group Name	VPNPHONE
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

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

Internet: http://www.avaya.com