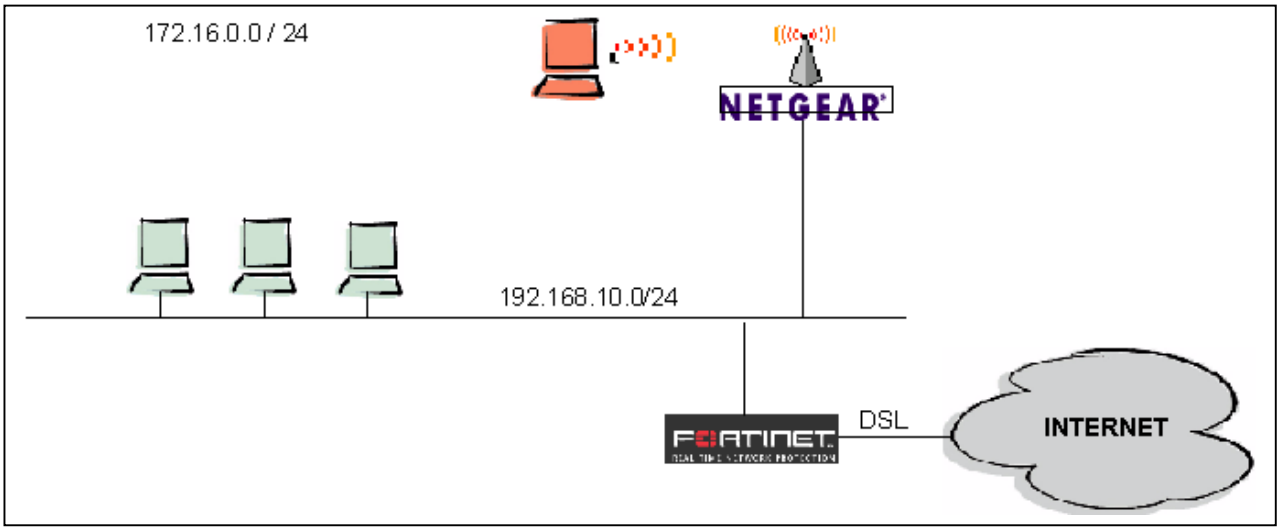
The purpose of this document is to provide you with the necessary steps to configure a Netgear ProSafe Dual-Band Wireless VPN Firewall (Model No. FWAG114) to be integrated within your Network Environment. With this document, I also wrote security aspects to provide as much security as possible.

For further details on technical specs, please refer the www.netgear.com .

It's not my intension to replace any official documentation, however, I thought some mandatory configuration suggestions would help you to secure your network, without spending some days, to address all proper parameters, you may need to think of.



The drawing above shows the network and connection I've made. Because FWAG114 incorporates AutoUplink technology, there is no need to worry about cross-over cables. Get your physical connection done and power on the Gateway.

Security Aspect No. 1

Especially with DSL flat rate, I usually have Internet connection all time open, when being in my home office. Because my family is using Internet as well, it might stay up all day long. If you do not use any wireless devices, I consider to switch off the FWAG114 (I will use the proper terminology "**Access Point**" in this document). When looking at the drawing, you realize, that internet connection is done with a FortiGate-50 to provide DSL into my home.

For interest on FortiGate-50 DSL installation, have a look on another TechNote I made:

www.bemsel.com/TechTip/RBE_FTG_DSL.pdf

If you already run a DHCP Server, different to IP Net 192.168.0.0/24, than I consider to use temporarily a static IP Address other than 192.168.0.1 to connect to the Configuration Web Interface.

To logon, open a web browser and type http://192.168.0.1

- Default Username: admin
- Default Password: password

Once you are logged on for the first time, a configuration wizard starts. Usually, you can run the wizard, but for security aspect, I consider a different approach.

System can now detect the connection type Of WAN port, or you can configure it by yourself. Do you want the system to detect the connection type?

⊙ No. I Want To Configure By Myself.

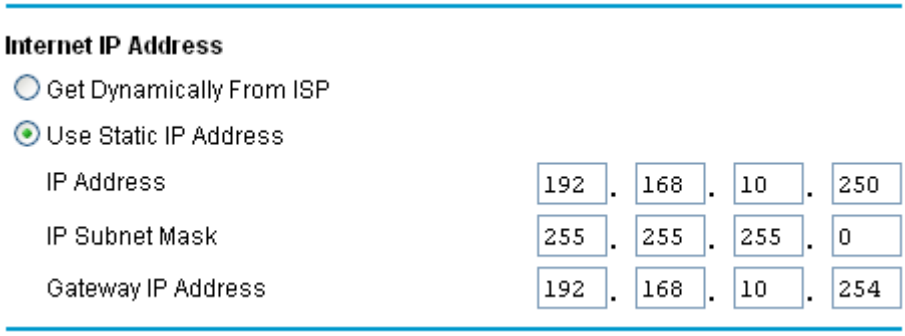
Click on **NEXT**

Does your Internet Connection Require a Login?

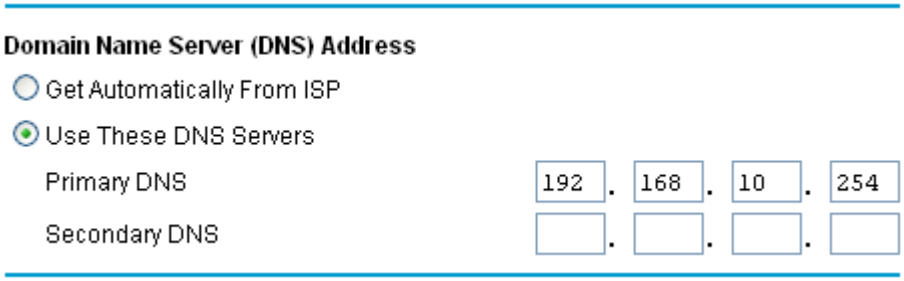
Actually, I do not use a internet connection in this setup at all. All Internet related communication is done with my FortiGate Firewall.

In this case, it is not necessary to provide any login information. Just ignore and continue with IP Address settings.

Remember, that I do not use my Access Point to connect to the Internet, directly. I've configured Internet IP Address to my wired LAN.



DNS is provided by my Internet Gateway. So, I also do not resolve IP Address on the Internet.



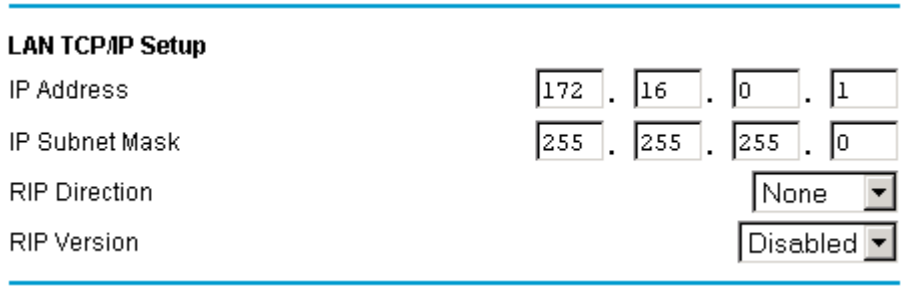
Next, I will have to provide LAN Settings, which means in this case. DHCP Service for local wireless devices.

Security Aspect No. 2

Wireless Devices are quiet easy to attach to the local Network, as they do not require cables. By offering DHCP Service, every wireless device could connect automatically to the Access Point, as long there are no other restrictions and security settings established. I do have 4 wireless device available, so I restrict access based on their MAC Addresses.

Any other wireless device won't be able to connect, as long as a possible intruder has not changed the local MAC Address with one reflects to my settings.

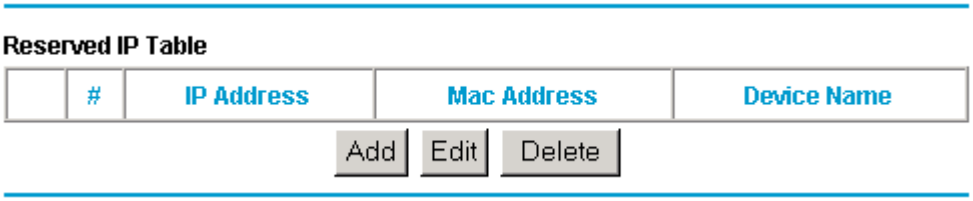
Go to Advanced Settings – LAN IP Setup.



Next, activate "Use router as DHCP server" and do not offer more DHCP leases as you really need. Next few steps will be restrictions on MAC Addresses.

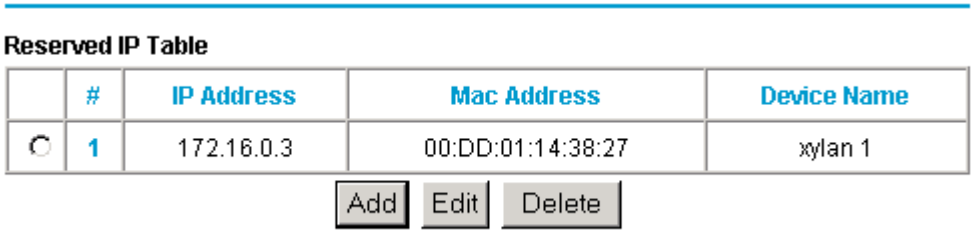
Usually, you find MAC Addresses on the wireless cards. If not, open a DOS box and type "ipconfig –all" to get the local MAC Address.

Click on ADD



Provide an IP Address out of the range, previously defined on DHCP Server.

Click on Apply and the entry will be performed



Finally, click on APPLY. The device will reboot.

Security Aspect No. 3

What do you think anybody would use as a password to get into a router, switch, Operating System, etc. Of course, always try default username and password first. It's an absolutely must to change them. If you can't rename username "admin", than at least change the password to something cryptic, but easy to remember, incl. Upper case, Lower case, Number and special characters, like "$§&.

Change default Admin password

Go to MAINENTANCE and click on Set Password

Type the default password: password
Type the new password: <whatever>
Confirm the new password: <whatever>

Click on **APPLY**

The are a couple of more Security Aspects I will address in the next TechNotes.

Check out my website www.bemsel.com/TechTip