

NetWatcher Setup – How to setup NetWatcher in a simple small office environment

What if you want to use the NetWatcher sensor/service to monitor the security of your networks traffic and you only have a router from your Internet Services Provider (ISP) that does not support DHCP and a WIFI device that does support DHCP? See figure 1 below.

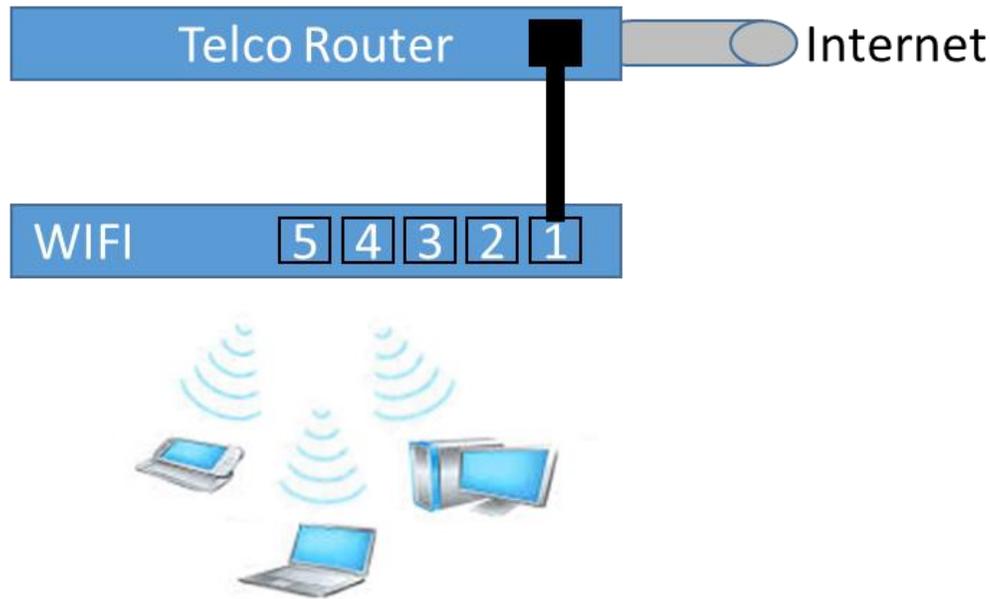


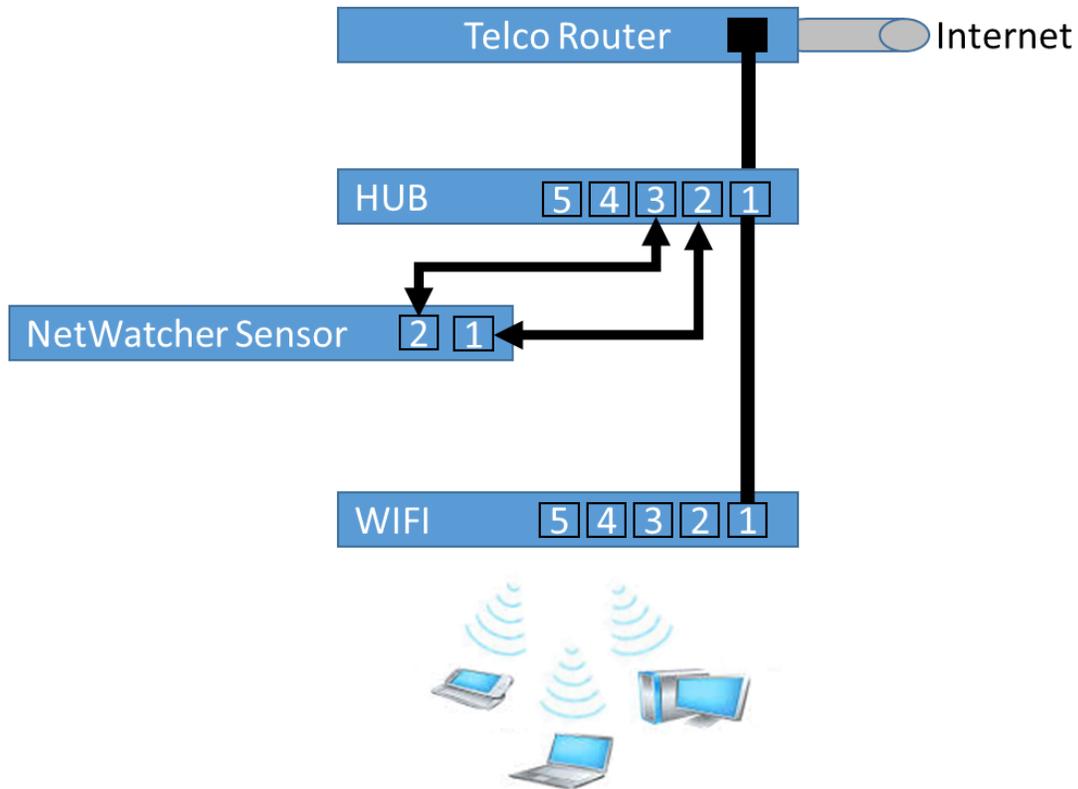
Figure 1 - Typical home network setup

Most WIFI devices do not support “Port Mirroring” and this is traditionally what a network sensor that does deep packet inspection requires. Unfortunately, the lack of a port mirroring feature means that you may need to add additional hardware to monitor the network traffic.

There are a few options in regards to setting up port mirroring on your network--There is a ‘good’, ‘better’, ‘best’ approach.

The BAD approach

You might ask, 'why not just add a simple Hub' and attach the sensor there?



There are 2 reasons this approach will not work. The first is that the NetWatcher sensor may not be able to get a DHCP address from the Hub or Telco Router. The second and most important reason is that the NetWatcher sensor would only see the IP Address and MAC of the WIFI router and not the devices behind the router.

The GOOD approach

Let's first explain the 'good' way. This is to add a router that does port mirroring and DHCP to the network. *Note that with any of these options you may be able to replace your ISP provided router with this new router assuming and save yourself some dollars on your monthly bill (check with your ISP).*

This 'good' approach would look something like the following in figure 2.

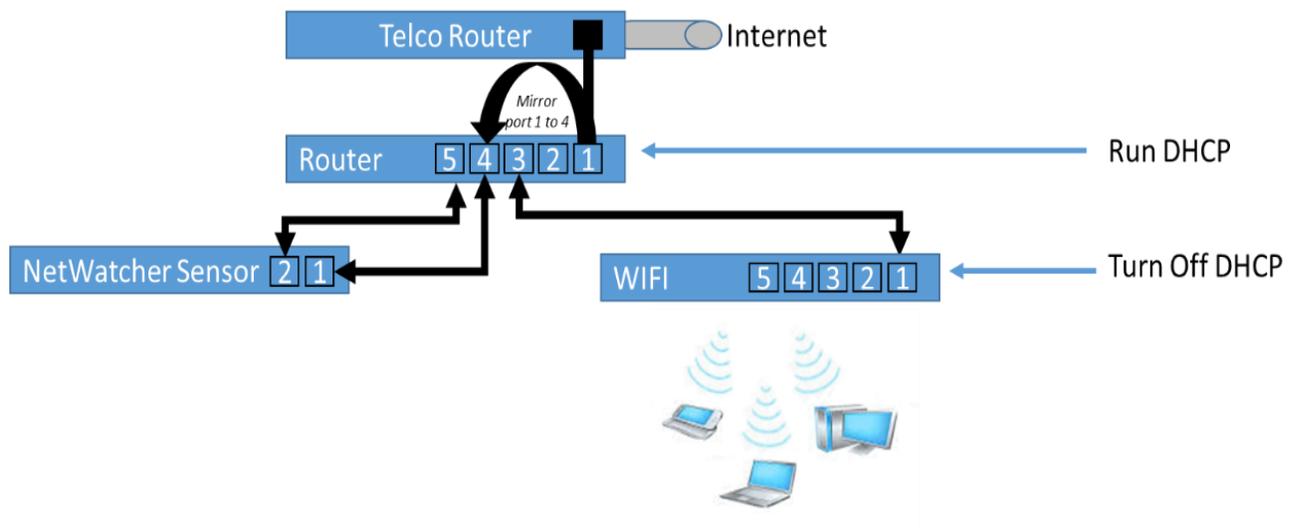


Figure 2 - Adding a router that does port mirroring and DHCP to network

With this 'good' enough setup you have to turn off DHCP on the WIFI router and run DHCP on the new router. If you did not turn off DHCP on the WIFI you would only see the IP address and MAC address of the WIFI router in all packets and that would not allow you to determine what device connecting to the wireless (and reported by NetWatcher) may have an issue.

Here is an example of a router you may want to consider:

1. <https://www.ubnt.com/edgemax/edgerouter-poe/>

The BETTER approach

The 'better' approach is to add a firewall that also provides DHCP to this network. The firewall provides the necessary inbound protection to the network and the managed switch provides the ability to do a mirror port. In this setup you also have to turn off DHCP on the WIFI device and then turn on DHCP on the firewall to ensure you see all the traffic's IP addresses and MAC addresses of the devices connecting to the WIFI.

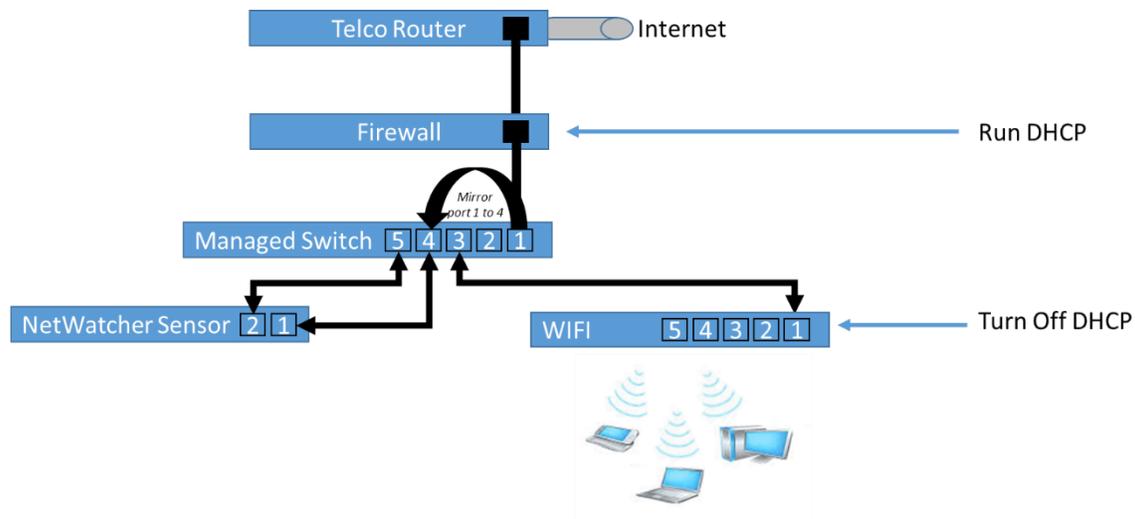


Figure 3 - Adding a firewall and managed switch to the network

Here is an example of a Firewall you might want to consider:

1. <http://www.sonicwall.com/products/sonicwall-tz/> (note you would not need the wireless option)

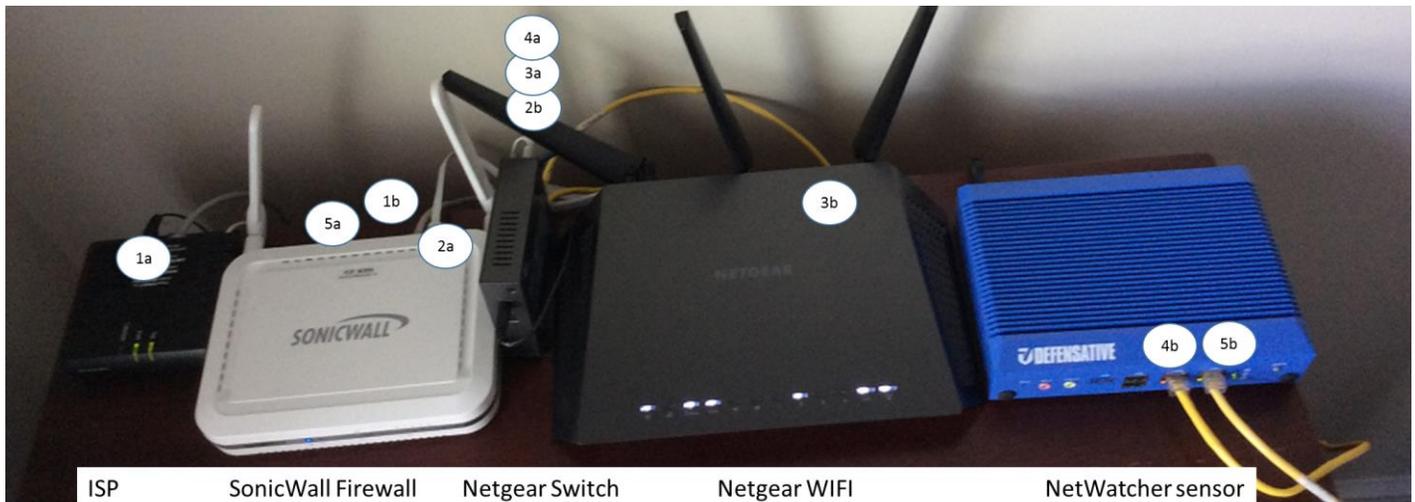
Here is an example of a managed switch you might want to consider:

1. <http://www.netgear.com/business/products/switches/>

Example of this approach

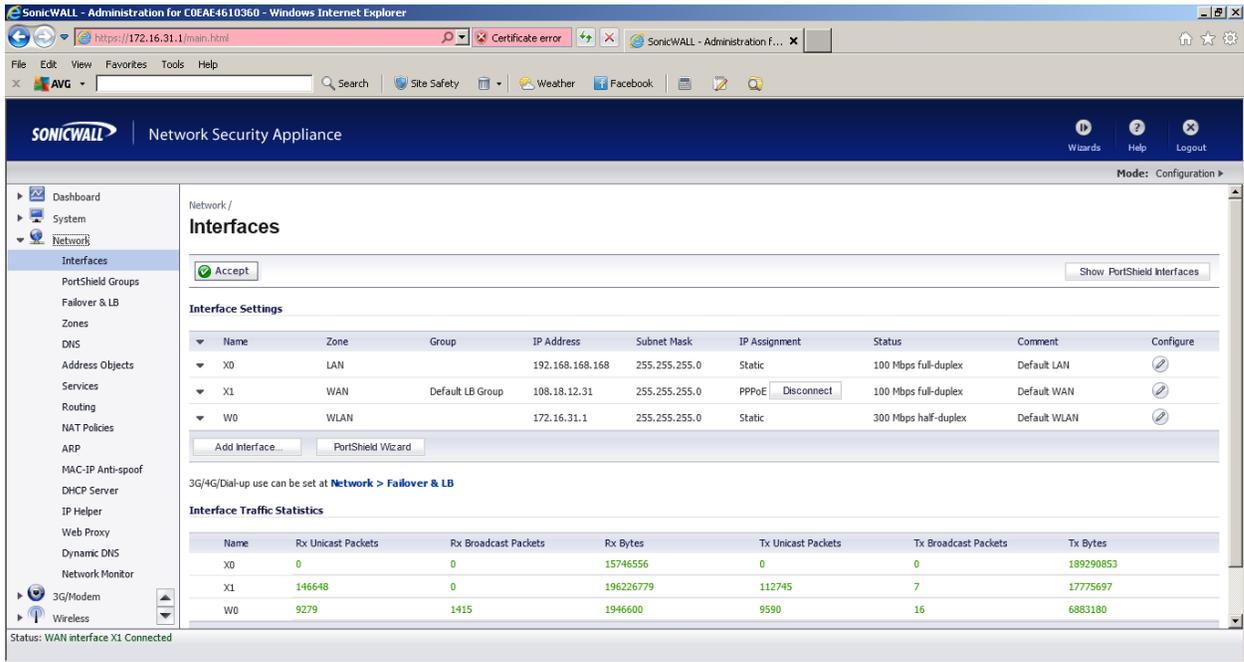
This examples uses the following equipment:

- Firewall: SonicWall model number TZ105 wireless N
- Switch: NETGEAR ProSAFE GS105Ev2
- WIFI: NETGEAR - Nighthawk Dual-Band Wireless-AC1900 Router with 4-Port Ethernet Switch
- NetWatcher sensor

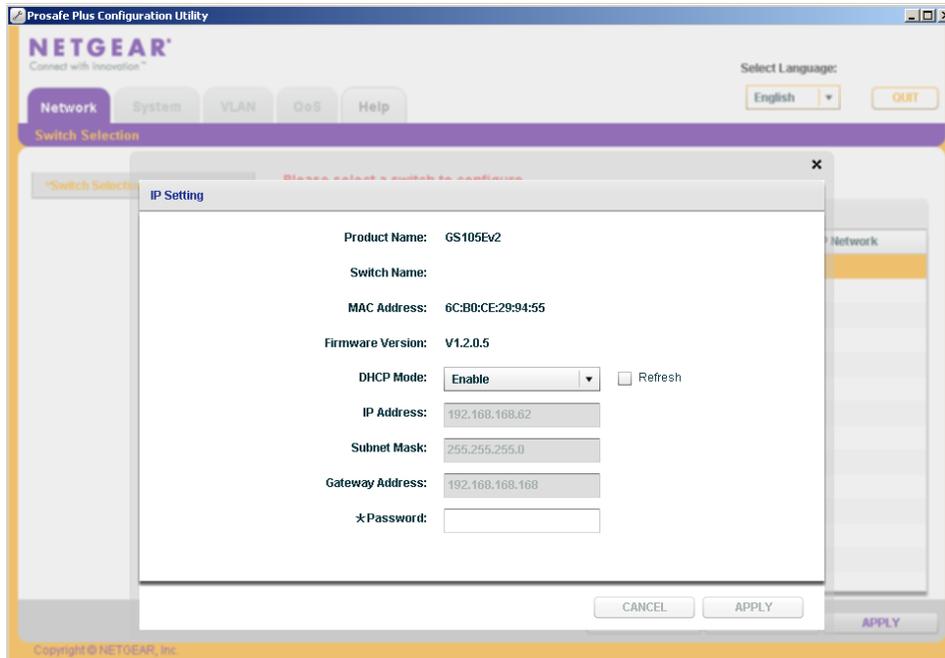


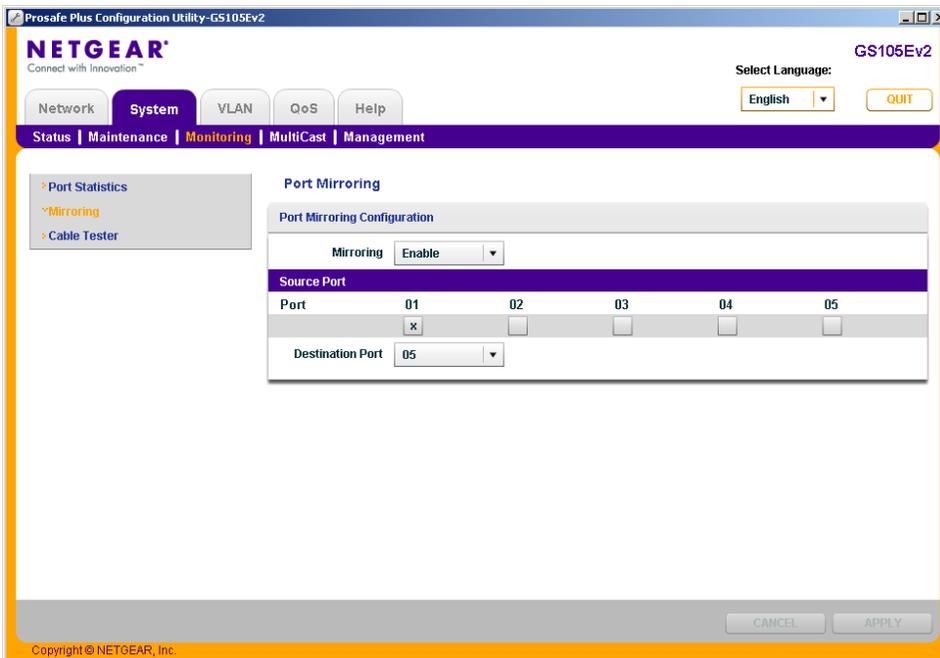
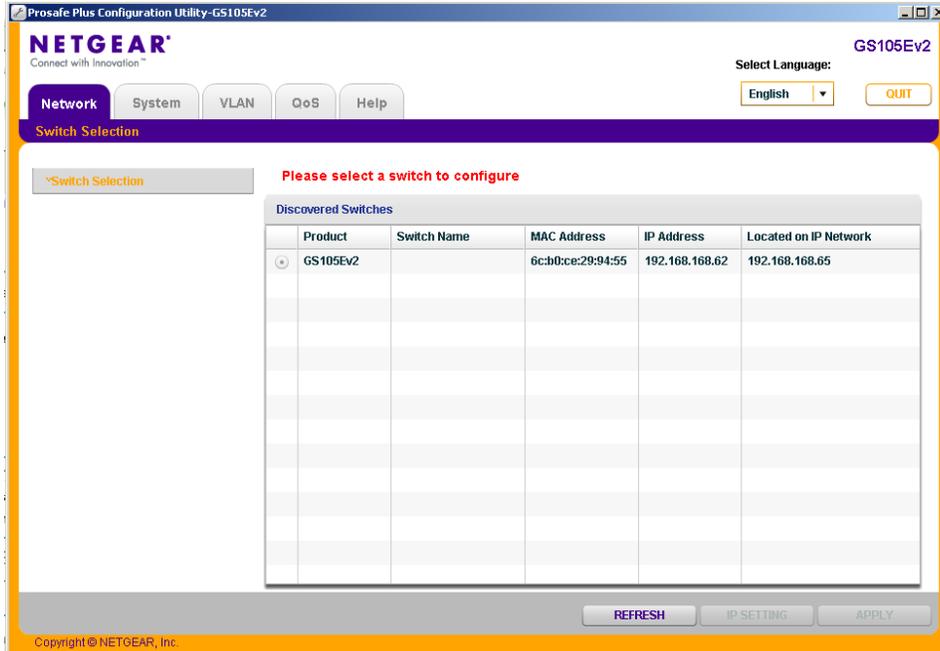
- The ISP (1a) is connected into the SonicWall's WAN port (1b)
- The SonicWall's LAN port (2a) is connected into the Netgear Switch port 1 (2b)
- The Netgear Switch port 2 (3a) is connected into the Nighthawk WIFI's port 2 (3b)
- The Netgear Switch port 4 (4a) is connected into the NetWatcher sensor port 1 (4b) -- **Important: The Netgear switch port 4 is the mirror port.**
- The NetWatcher sensor port 2 (5b) is connected to the SonicWall port 3 (5a)

The SonicWall's configuration:



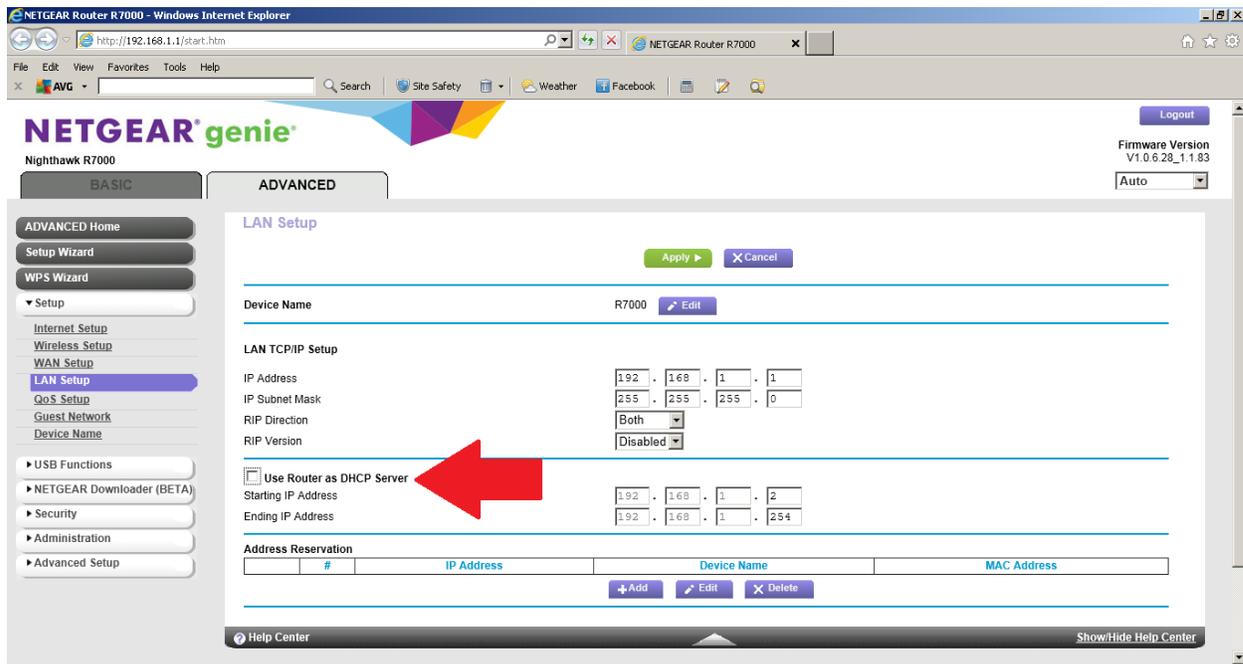
The Netgear switch configuration:





Note how we are mirroring all traffic on Port 1 (internet traffic) to Port 4 where the NetWatcher sensor will be connected.

The Nighthawk WIFI configuration:



VERY IMPORTANT: Note how we turned off DHCP (red arrow) as this will allow any device connected to this WIFI to get an IP address from the SonicWall. This is a key step that will allow us to see all the traffic behind the WIFI and corresponding IP addresses.

The BEST approach

The 'best' approach is to use a firewall that offers both port mirroring and WIFI and DHCP.

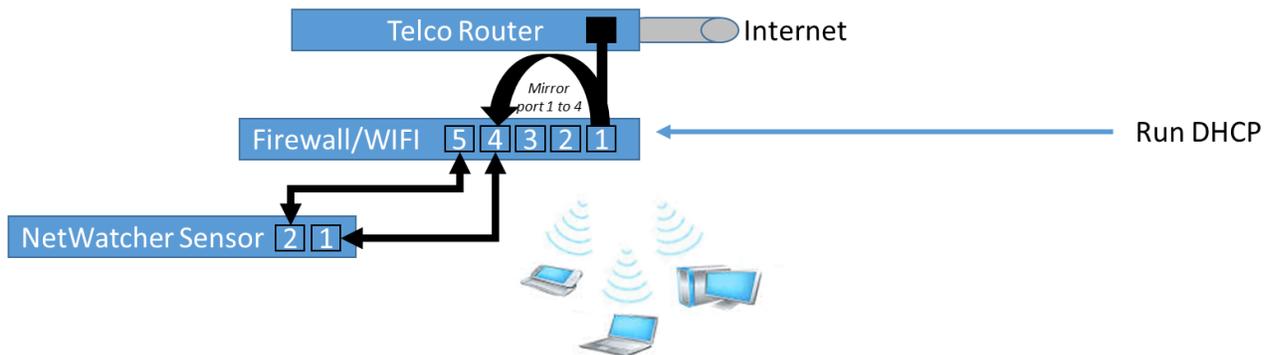


Figure 4 - Use Firewall / WIFI that supports port mirroring

Here is an example of a firewalls that also offer WIFI and port mirroring that you may want to consider:

1. <http://www.sonicwall.com/products/nsa-250m/> (note you would need the wireless option)