

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.

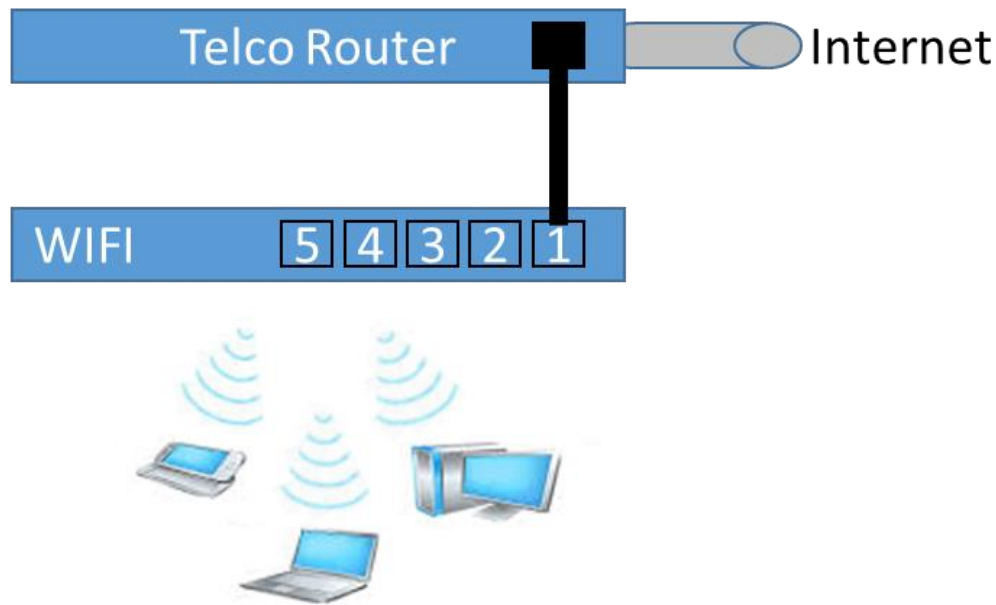


Figure 1 - Typical home network setup

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 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.

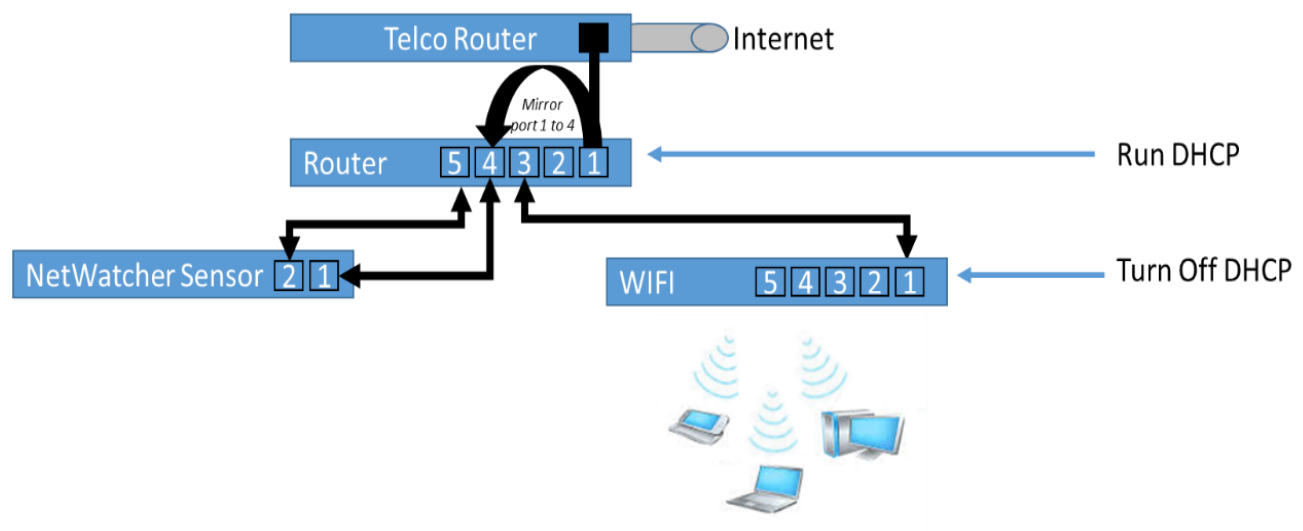


Figure 2 - Adding a router that does port mirroring and DHCP to network

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.

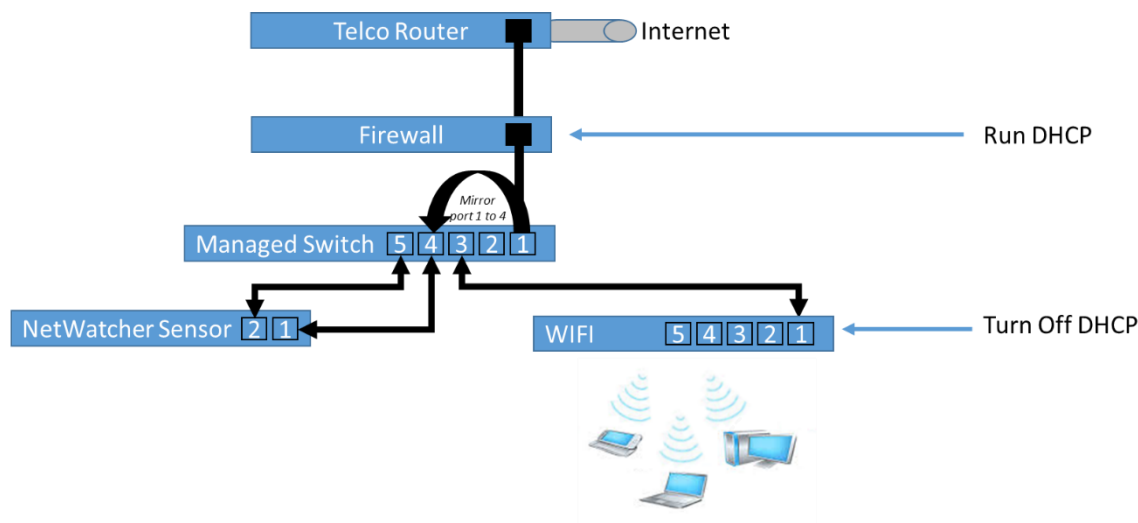


Figure 3 - Adding a firewall and managed switch to the network

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)

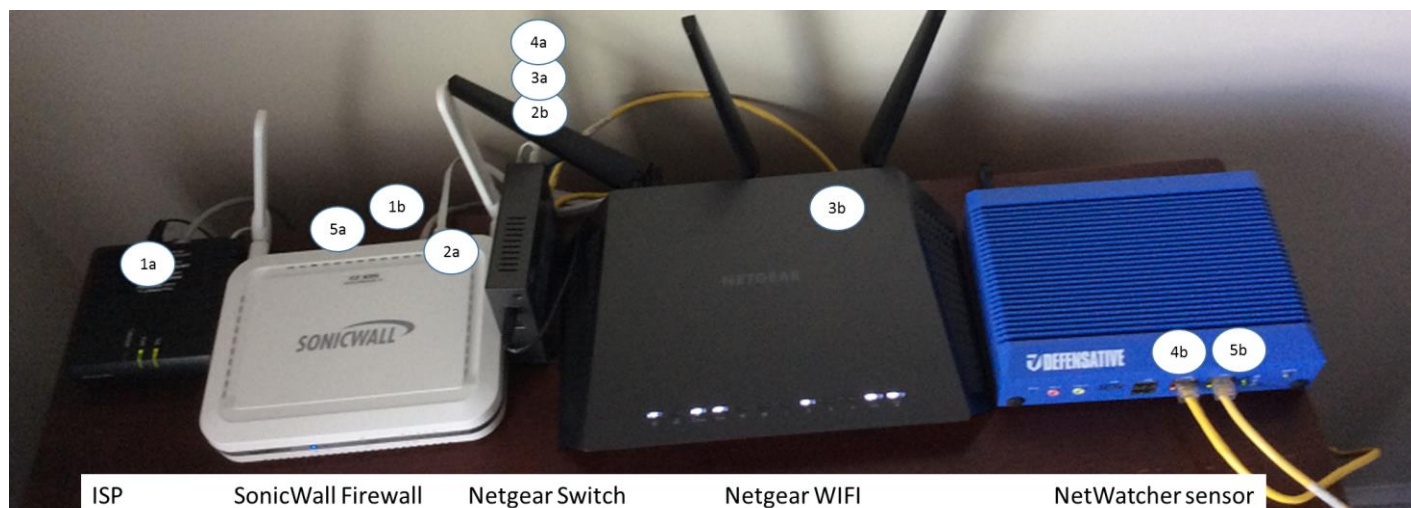
Here is an example of a managed switch you might want to consider:

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:

SonicWALL - Administration for C0EAE4610360 - Windows Internet Explorer

https://172.16.31.1/main.html

File Edit View Favorites Tools Help

SONICWALL Network Security Appliance

Wizards Help Logout

Mode: Configuration

Dashboard
System
Network

Interfaces

PortShield Groups
Failover & LB
Zones
DNS
Address Objects
Services
Routing
NAT Policies
ARP
MAC-IP Anti-spoof
DHCP Server
IP Helper
Web Proxy
Dynamic DNS
Network Monitor
3G/Modem
Wireless

Network /
Interfaces

Accept Show PortShield Interfaces

Interface Settings

Name	Zone	Group	IP Address	Subnet Mask	IP Assignment	Status	Comment	Configure
X0	LAN		192.168.168.168	255.255.255.0	Static	100 Mbps full-duplex	Default LAN	
X1	WAN	Default LB Group	108.18.12.31	255.255.255.0	PPPoE Disconnect	100 Mbps full-duplex	Default WAN	
W0	WLAN		172.16.31.1	255.255.255.0	Static	300 Mbps half-duplex	Default WLAN	

Add Interface... PortShield Wizard

3G/4G/Dial-up use can be set at **Network > Failover & LB**

Interface Traffic Statistics

Name	Rx Unicast Packets	Rx Broadcast Packets	Rx Bytes	Tx Unicast Packets	Tx Broadcast Packets	Tx Bytes
X0	0	0	15746556	0	0	189290853
X1	146648	0	196226779	112745	7	17775697
W0	9279	1415	1946600	9590	16	6883180

Status: WAN interface X1 Connected

The Netgear switch configuration:

ProSAFE Plus Configuration Utility

NETGEAR

Select Language: English QUIT

Network System VLAN QoS Help

Switch Selection

IP Setting

Product Name: GS105Ev2

Switch Name:

MAC Address: 6C:B0:CE:29:94:55

Firmware Version: V1.2.0.5

DHCP Mode: Enable Refresh

IP Address: 192.168.168.62

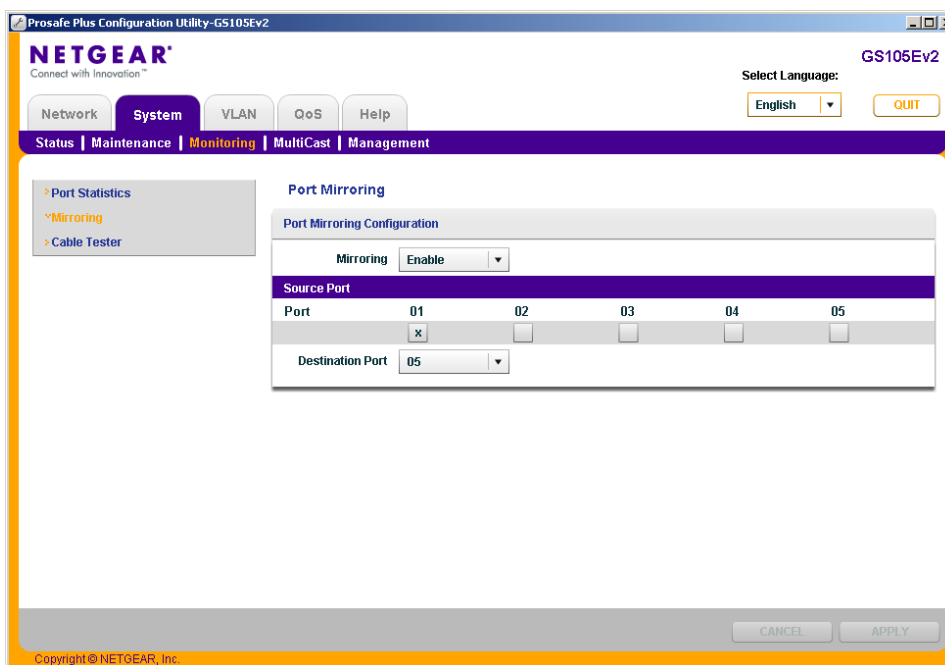
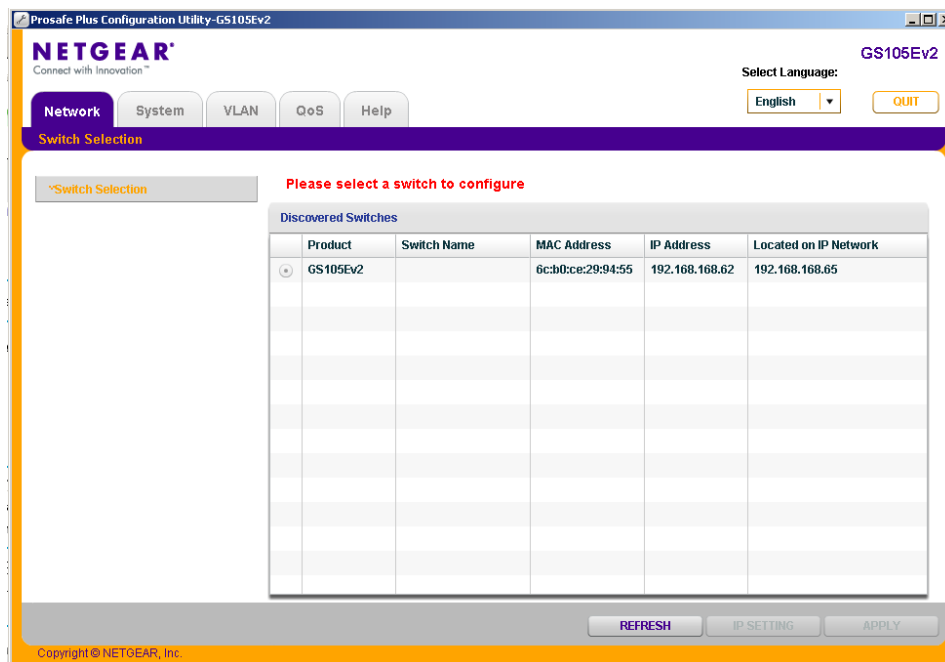
Subnet Mask: 255.255.255.0

Gateway Address: 192.168.168.168

*Password:

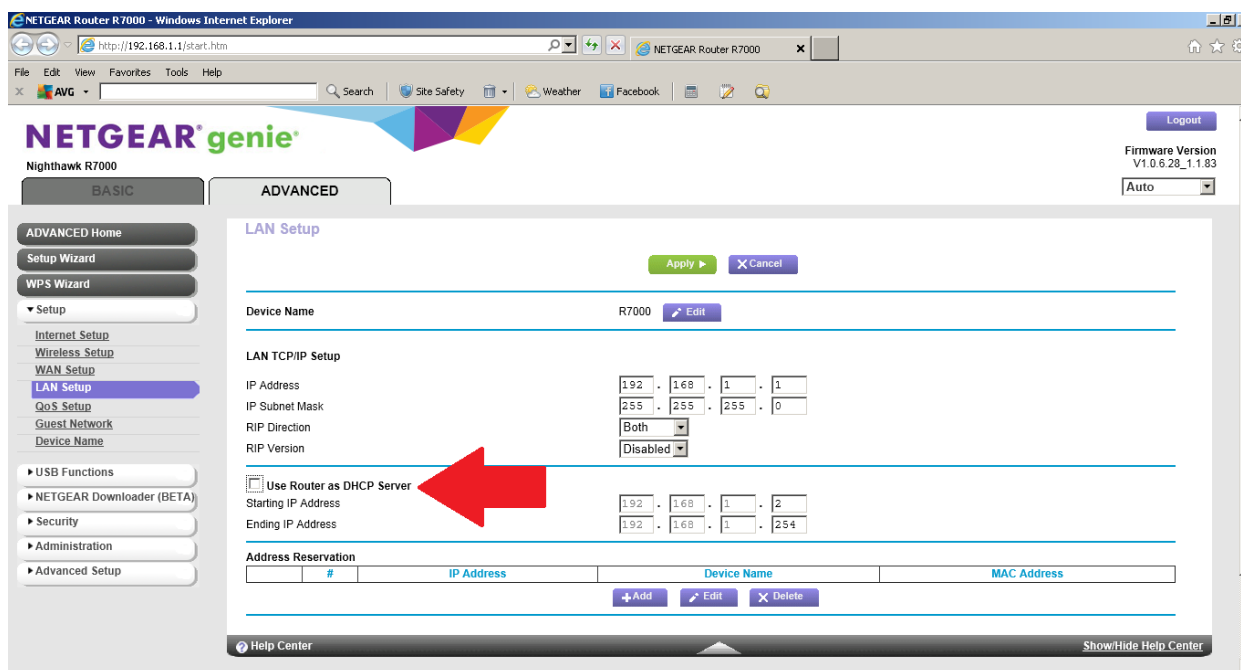
CANCEL APPLY APPLY

Copyright © NETGEAR, Inc.



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.

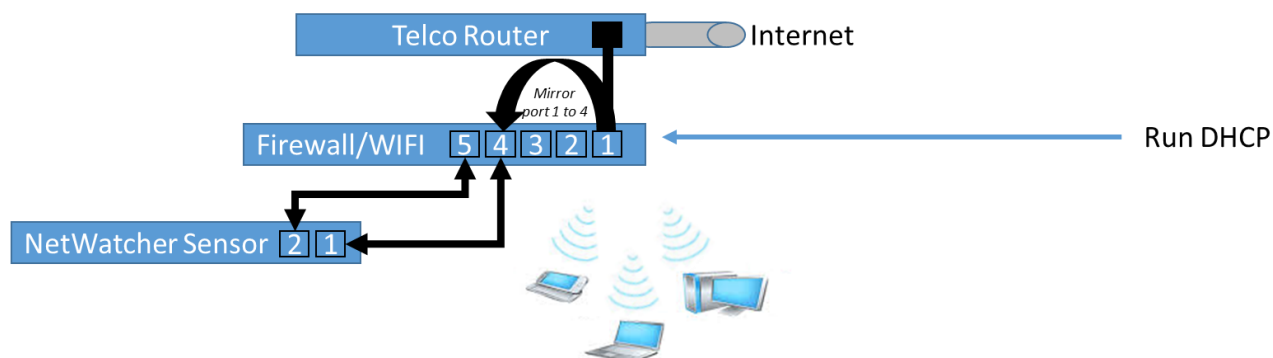


Figure 4 - Use Firewall / WIFI that supports port mirroring

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)