

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

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

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

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



### **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:

📀 🗢 🧭 https://172.16.31.	1/main.html		🔎 💌 😵 Certif	icate error 😽 🗙	🥝 SonicWALL - Adm	inistration f 🗙			ŵ
Edit View Favorites Too	ils Help	🔍 Search 🛛 🍯	Site Safety 🗎 🔹	Weather 📑 Fa	icebook 🗐 🎽	2 0			
SONICWALL   Net	work Securi	ty Appliance						U) Wizards	Pielp Logou
								1	1ode: Configurat
Dashboard System	Network/	es							
Interfaces PortShield Groups	Accept							Show Po	rtShield Interfaces
Failover & LB Zones	Interface Set	tings							
DNS	<ul> <li>Name</li> </ul>	Zone	Group	IP Address	Subnet Mask	IP Assignment	Status	Comment	Configure
Address Objects	▼ X0	LAN		192.168.168.168	255.255.255.0	Static	100 Mbps full-duplex	Default LAN	Ø
Services	🔻 X1	WAN	Default LB Group	108.18.12.31	255.255.255.0	PPPoE Disconnect	100 Mbps full-duplex	Default WAN	Ø
Routing		WLAN		172.16.31.1	255.255.255.0	Static	300 Mbps half-duplex	Default WLAN	Ø
ARP	Add Inter	face PortShield Wizar	d						
MAC-IP Anti-spoof	3G/4G/Dial-un i	ise can be set at Network > Fail	over & LB						
DHCP Server	Interface Tea	offic Statistics							
Web Proxy	Interface fro	ine statistics							
Dynamic DNS	Name	Rx Unicast Packets	Rx Broadcast P	ackets Rx I	Bytes	Tx Unicast Packets	Tx Broadcast Pack	ets Tx Bytes	
Network Monitor	X0	0	0	157	46556	0	0	189290853	
3G/Modem	X1	146648	0	196	226779	112745	7	17775697	
Wirelace	W0	9279	1415	194	6600	9590	16	6883180	

#### The Netgear switch configuration:

NETGEAR'     Select Language:       Convert with Incorrection*     English • OUT       Switch Selection     X	🖉 Prosafe Plus Config	guration Utility		_ <b>_</b> _ ×
Switch Selection X Switch Selection	NETGE Connect with Innovation	AR' on"		Select Language:
Switch Selection     IP Setting	Switch Selection	n		
	"Switch Select	Place alocation with a	te canfigura	×
Product Name: GS105EV2 Network		Product Name:	GS105Ev2	Network
Switch Name: MAC Address: 6C:B0:CE:29:94:55		Switch Name: MAC Address:	6C:B0:CE:29:94:55	
Firmware Version: V1.2.0.5 DHCP Mode: Enable   Refresh		Firmware Version: DHCP Mode:	V1.2.0.5	
IP Address: 192.168.168.62		IP Address:	192.168.168.62	
Subnet Mask:         255.255.0           Gateway Address:         192.168.168.168		Subnet Mask: Gateway Address:	255.255.255.0 192.168.168.168	
*Password:		*Password:		
CANCEL APPLY APPLY			CANCEL	APPLY APPLY

IETCEAD.							094055
onnect with Innovation						Select Language:	GSTUDEV
						English 🔻	QUIT
Network System V	LAN Q	oS Help					<u> </u>
Switch Selection							
	Ple	ase select a	switch to configu	·•			
"Switch Selection				-			
	Disci	overed Switche	s				
		CE 1055-2	Switch Name	MAC Address	IP Address	Located on IP Ne	twork
	•	03103242		00.00.00.29.94.55	192.100.100.02	192.100.100.00	
opyright © NETGEAR, Inc. safe Plus Configuration Utility-G51	105E <del>v</del> 2		_				_1
opyright©NETGEAR, Inc. safe Plus Configuration Utility-GS1	105E¥2						_⊥ GS105E∖
opyright © NETGEAR, Inc. safe Plus Configuration Utility-CST IETGEAR: nect with Innovation <sup>-</sup>	105E¥2					Select Language:	الـــ GS105E
opyright © NETGEAR, Inc. safe Plus Configuration Utility-CST IETGEAR: ned with Innovation <sup>®</sup> Vetwork System VI	LOSEv2	oS Help				Select Language: English 🛛 🔻	II GS105Ev QUIT
opyright © NETGEAR, Inc. safe Plus Configuration Utility-GST IETGEAR. Incod with Innovation Network System VI Iatus   Maintenance   Monitor	LAN Q.	oS Heip Cast Manag	ement			Select Language: English 🛛 🔻	]] GS105Es QUIT
opyright © NETGEAR, Inc. safe Plus Configuration Utility-651 IETGEAR: uned with Innovation Network System VI tatus Maintenance Monito	LOSEv2	oS Help Cast   Manag	ement			Select Language:	LI GS105Ev QUIT
opyright © NETGEAR, Inc. safe Plus Configuration Utility-651 IETGEAR. Ined with Innovation Network System VI tatus Maintenance Monitor > Port Statistics	LAN Qa ting Multic Po	oS Heip Cast Manag rt Mirroring	ement			Select Language: English 💌	]] GS105Ev QUIT
opyright © NETGEAR, Inc. safe Plus Configuration Utility-651 Incet with Innovation Network System VI tatus   Maintenance   Monitol Port Statistics "Mirroring	LAN Q. ring Multi Po Port	oS Help Cast Manag rt Mirroring Mirroring Confi	ement			Select Language: English 💌	⊑∐ GS105Ev OUIT
opyright © NETGEAR, Inc. safe Plus Configuration Utility-651 IEEE CEAR Incel with Innovation Network System VI tatus   Maintenance   Monitor Port Statistics *Mirroring Cable Tester	105Ev2 LAN Q. ring   Multid Pot	oS Help Cast Manag rt Mirroring Mirroring Confi Mirroring	ement iguration			Select Language: English 💌	GS105Ev QUIT
appright © NETGEAR, Inc. safe Plus Configuration Utility-651 IEEE CEAR. Incet with Innovation Vetwork System VI tatus Maintenance Monitor Port Statistics *Mirroring • Cable Tester	LAN Querring Multit	oS Help Cast Manag rt Mirroring Mirroring Confi Mirroring	ement iguration Enable			Select Language: English 💌	 GS105Ev 
opyright © NETGEAR, Inc. safe Plus Configuration Utility-651 IEEE CEAR Incel with Innovation Network System VI tatus Maintenance Monitor Port Statistics "Mirroring Cable Tester	LAN Q4 ring Multit Pot Pot Pot Pot	oS Help Cast Manag rt Mirroring Mirroring Confi Mirroring rce Port t	ement iguration Enable 💌	02 03	04	Select Language: English 💌	 GS105Ev Quit
opyright © NETGEAR, Inc. safe Plus Configuration Utility-651 Incet with Innovation* Network System VI tatus Maintenance Monitor Port Statistics *Mirroring • Cable Tester	LAN Q4 ring Multit Por Por	oS Help Cast Manag rt Mirroring Mirroring Confi Mirroring rce Port t	ement iguration Enable •	02 03	04	Select Language: English ¥	LIS GS105Ev QUIT
opyright © NETGEAR, Inc. safe Plus Configuration Utility-CSI Inter Configuration Utility-CSI Inter Configuration Utility-CSI Inter Configuration Utility-CSI Network System VI System VI Network System VI System System	LAN Q4 ring Multit Pot Pot D	oS Help Cast Manag rt Mirroring Mirroring Confi Mirroring rce Port t	ement iguration Enable •	02 03	04	Select Language: English V	LI GS105Ev QUIT
opyright © NETGEAR, Inc. safe Plus Configuration Utility-651 Incet with Innovation* Network System VI tatus Maintenance Monitor Port Statistics *Mirroring Cable Tester	LAN Q4 ring Multit Por Por D	oS Help Cast Manag rt Mirroring Mirroring Confi Mirroring rce Port t t	ement iguration Enable • 01 × 05 •		04	Select Language: English V	LIS GS105Ev QUIT
opyright © NETGEAR, Inc. safe Plus Configuration Utility-GSI IETCEEAR: Inced with Innovation* Network System VI tatus Maintenance Monitor > Port Statistics * Wirroring > Cable Tester	LAN Q4 ring Multit Por Por D	oS Help Cast Manag rt Mirroring Mirroring Confi Mirroring rce Port t t	ement iguration Enable • 01 × 05 •	02 03	04	Select Language: English V	LIS GS105Ev QUIT
opyright © NETGEAR, Inc. safe Plus Configuration Utility-GSI IETCEEAR: Incd with Innovation* Vetwork System VI tatus   Maintenance   Monitor > Port Statistics * Wirroring > Cable Tester	LAN Q4 ring Multit Por Por D	oS Help Cast Manag rt Mirroring Mirroring Confi Mirroring rce Port t	ement iguration Enable •		04	Select Language: English V	LIS GS105Ev QUIT
opyright © NETGEAR, Inc. safe Plus Configuration Utility-GSI Incet with Innovation* Network System VI tatus Maintenance Monitor Port Statistics *Mirroring Cable Tester	LAN Q4 ring Multit Pot Pot D	oS Help Cast Manag rt Mirroring t Mirroring Confi Mirroring rce Port t t	ement iguration Enable •		04	Select Language: English V	LIS GS105Ev QUIT
opyright © NETGEAR, Inc. safe Plus Configuration Utility-GST IEEEEEEEE Network System VI tatus Maintenance Monitor > Port Statistics *Mirroring > Cable Tester	LAN Qa ring Multid Por Dur	oS Help Cast Manag rt Mirroring Mirroring Confi Mirroring rce Port t t	ement guration Enable •		04	Select Language: English +	
sopyright © NETGEAR, Inc.	LAN Qa ring Multid Por Dur	oS Help Cast Manag rt Mirroring Mirroring Confi Mirroring rce Port t t	ement guration Enable •		04	Select Language: English +	LIE GS105Ev QUIT
sopyright © NETGEAR, Inc.	LAN Q. cing Multi Po Por D	oS Help Cast Manag rt Mirroring Mirroring Confi Mirroring rce Pott t	ement guration Enable •		04	Select Language: English +	LL GS105Ev QUIT
opyright © NETGEAR, Inc safe Plus Configuration Utility-GST IEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEE	LAN Qa ring Multi Po Por D	oS Help Cast Manag rt Mirroring Mirroring Confi Mirroring rce Port t t	ement guration Enable •		04	Select Language: English +	LI GS105Ev QUIT
opyright © NETGEAR, Inc. safe Plus Configuration Utility-651 EEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEEE	LAN Q. cing Multi Po Por D	oS Help Cast Manag rt Mirroring Mirroring Confi Mirroring rce Pot t t	ement guration Enable •		04	Select Language: English +	LI GS105Ev QUIT

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:

ENETGEAR Router R7000 - Windows Inte	ernet Explorer				_ 8 ×
🔄 🔄 🗸 🌈 http://192.168.1.1/start.htr	n	م	💌 🔄 🔀 🧔 NETGEAR Router R7000 🗙		A 🛪 🔅
File Edit View Favorites Tools Help × <b>¥ AVG</b> •	Q Search	🧊 Site Safety 🛛 🔹 🖉 We	ather 🛐 Facebook 🔤 🎲 🔯		
NETGEAR <sup>®</sup> g	enie				Logout Firmware Version V1.0.6.28_1.1.83
BASIC	ADVANCED				Auto 💌
ADVANCED Home	LAN Setup				
Setup Wizard			Apply  Cancel		
▼ Setup	Device Name		R7000 🍞 Edit		_
Internet Setup Wireless Setup	LAN TCP/IP Setup				
LAN Setup	IP Address		192 . 168 . 1 . 1		
QoS Setup Guest Network	IP Subnet Mask RIP Direction		Both •		
Device Name	RIP Version		Disabled 💌		
NETGEAR Downloader (BETA)	Use Router as DHCP Serv Starting IP Address	er	192 . 168 . 1 . <b>2</b>		
Security	Ending IP Address		192 . 168 . 1 . 254		
Administration	Address Reservation				
Auvanceu setup	#	IP Address	Device Name +Add	MAC Address	*
	Help Center			Show	Hide Help Center

**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

Telco Router Internet Firewall/WIFI 5 4 3 2 1 NetWatcher Sensor 2 1

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