How to setup the NetWatcher Virtual machine on a laptop with 1 network card connected to a Netgear ProSafe managed switch in promiscuous mode.

Note that with this configuration you are using the same Lan port on the virtual switch for outbound access to the NetWatcher cloud as well as doing deep packet inspection.

For this to work you should ensure that:

- You are not blocking UDP 443 outbound.
- You do not have any firewall software running on the laptop that would block the sensor.

Here is the typical test environment. 1 - the laptop running <u>VMware player</u> and the NetWatcher sensor. 2 - an inexpensive managed switch (<u>Netgear ProSAFE</u> is great). 3 - an internet connection and possibly other computers attached to the switch.



Step 1: Download the Virtual Sensor and install it on the laptop

Download NetWatcher Sensor VM				
	🗸 NetWatcher	Invite a friend and get one month free	🛞 Steve 📄 🔺 Logout (*	
 How to login to the portal: You should have received an email to access the NetWatcher.com portal earlier. If you can't find it, log in to https://portal.netwatcher.com/login with your email address and reset your password. 	Databaserd Reports Advance Orescell Subjections Set Advance Orescell Subjections Set Advance Orescell Set Advances Orescell Set Advances	Support Configure Advance Support (and configure advance) Agents Agents	4 Q	
How to download the Virtual Machine/Sensor:	Display: 100	¢ 1 >		
 Once you log in to your account, navigate to <u>https://portal.netwatcher.com/configure/sensors</u>, click on your sensor, and press download. It will take a while to download as it's a large file. We use <u>http://www.7-zip.org</u> for compression and there is no password. There are two parts, extract the first one and it will continue into the second one. 	NetWatcher Dashboard Baports Alarr Conton Suboyuna You	Invite a friend and get one month free s Support Configure Adva	Steve Steve Legent	
Unzip, then untar downloaded .xz file.	My Sensors × madwolf-virtual1			
	Sensor Details Sensor Id: 60074846- Name: Incoherry Date: 2015-18-19 Groups Urbail Machine: Consum Sensor	1351-44a-327-993x87-489x versant 11132-19	padg	

Step 2: Setup a Mirror port on the switch.

In this example configuration in the figure below you setup port mirroring under "System | Monitoring"

- Port 1 connection to the internet.
- Port 3 The laptop running the NetWatcher sensor. Must be able to get an IP address via DHCP.
- Port 4 another computer generating traffic on the switch (red cable above)

Prosafe Plus Configuration Utility-GS105Ev2						- 🗆 ×
NETGEAR Conned with Innevention Network System VLAN Status Maintenance Monitoring	QoS Help MultiCast Manage	ement			Select Lan	GS105Ev2 guage: ↓ QUIT
 Port Statistics Mirroring Cable Tester 	Port Mirroring Port Mirroring Config Mirroring Source Port	guration Enable	•			
	Port Destination Port	01 x 03	02	03	04	05
Copyright © 1996–2014 Netgear ®						

**We are mirroring all traffic from port 1 (internet) to port 3 (sensor)

Step 3 – Turn off one of the network adapters (VMnet5)

√irtual Machine Settin	gs	×
Hardware Options		
Device	Summary 4 GB 4 50 GB Custom (VMoetS) Bridged (Automatic) Auto detect Auto detect Remove	Device status Connected Connect at power on Network connection Replicate physical network connection state Configure Adopters NAT: Used to share the host's IP address Host-only: A private network shared with the host Coston: Specific virtual network VMnets LAN Segment: LAN Segments Advanced
		OK Cancel Help

Step 4 – Put the second lan port in Bridged mode and choose Advanced to choose the adapters you want bridged.

evice	Summary	Device status
Memory	4 GB	Connected
Processors	4	Connect at nower on
Hard Disk (SCSI)	50 GB	
Network Adapter	Custom (VMnet5)	Network connection
Network Adapt	Bridged (Automatic)	Bridged: Connected directly to the physical network
Display	Auto detect	Peoplicate physical network connection state
		Replicate physical network connection state
		Configure Adapters
utomatic Bridgir	ng Settings 🛛 🗡	○ NAT: Used to share the host's IP address
Soloct the best pet	work adapter(c) you want to	O Host-only: A private network shared with the host
automatically bridge	e:	Custom: Specific virtual network
_		VMnet0
ASIX AX88179	USB 3.0 to Gigabit Ethernet Adapter	
Microsoft Wi-F	i Direct Virtual Adapter	ULAN segment:
Microsoft Host	ed Network Virtual Adapter	\sim
Intel(R) Dual B	and Wireless-N 7260	
TAP-Windows	Adapter V9	LAN Segments Advanced
TAP-Windows	Adapter V9	
ОК	Cancel Help	
		The second se
	-	1

Step 5 – Verify you have an IP address

Step into the VM and press enter. The VM will show the sensor's IP address as seen in the figure below.

NetWatcher - OVF - VMware Workstation 12 Player (Non-commercial use o –) ×
Player ▼ 📕 ▼ 🖧 🖂 🧏	*
 655.6646021 device vethdbdd019 entered promiscuous mode 655.6646021 docker0: port 2(vethdbdd019) entered forwarding state 655.6722401 docker0: port 2(vethdbdd019) entered forwarding state 655.6744101 IPv6: ADDRCONF(NETDEV_CHANGE): veth8118ef3: link become: 655.6808151 docker0: port 2(vethdbdd019) entered disabled state 655.795941 eth0: renamed from veth8118ef3 655.795041 docker0: port 2(vethdbdd019) entered forwarding state 655.795041 eth0: renamed from veth8118ef3 655.795041 docker0: port 2(vethdbdd019) entered forwarding state 655.8006531 docker0: port 2(vethdbdd019) entered forwarding state 655.3799631 docker0: port 2(vethdbdd019) entered forwarding state 657.3799631 docker0: port 2(vethdbdd019) entered disabled state 657.3830591 veth8118ef3: renamed from eth0 657.4406591 docker0: port 2(vethdbdd019) entered disabled state 	s ready
This is localhost (Linux x86_64 4.2.2-coreos-r1) 15:26:07 SSH host key: SHA256:Rc5LlmtsLvN556GRiKq23EN6ZP41D/r0gbyQj86B00RA (DSA) SSH host key: SHA256:MRuaZ5HRT1pB0Xffw3LUXnXAomYLE21n1U29oz/DtyU (ED25 SSH host key: SHA256:DrW2YKMkkka+Inhw5Fn/cbi8LFgBFX36tcP12XtN02o (RSA) eno16777736: eno33554960: 10.20.1.61 fe80::20c:29ff:fe9c:b97b localhost login: [1115.597498] hrtimer: interrupt took 3834357 ns	519)