

How to setup the NetWatcher Virtual Machine on a computer with 2 network cards running VMware Player connected to a managed switch

For this to work you should ensure you do not have any firewall software running on the computer hosting the NetWatcher sensor Virtual Machine and that you are not blocking the following 'outbound' at the firewall:

- TCP 8443 => <u>www.defensative.com</u>
- UDP 443 => vpn.netwatcher.com
- TCP 443 => index.docker.io
- TCP 443 => registry-1.docker.io
- TCP 443 => public.update.core-os.net

Here is the environment:

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



Computer Network Ports	Switch
LAN 1	Port 5 (Mirror)
LAN 2	Port 4 (access to Internet / able to get DHCP address)



$Step \ 1: {\tt Download \ the \ Virtual \ Sensor \ and \ install \ it \ on \ the \ computer}$



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 4 Computer (LAN 2) running the NetWatcher sensor (Internet access). Must be able to get DHCP address
- Port 5 Computer (LAN 1) running the NetWatcher sensor Mirror port.

In this example we are Mirroring all traffic from Port 1 on the switch to Port 5



Prosafe Plus Configuration Utility-GS105Ev2						- 0	×
NETGEAR'					Select Lang	GS10	5Ev2
Network System VLAN Status Maintenance Monitoring	QoS Help MultiCast Manage	ment			English		
Port Statistics	Port Mirroring						
*Mintoring	Port Mirroring Config	puration					
Caule rester	Mirroring	Enable					
	Source Port						
	Port	01 	02	03	04	05	
	Destination Port	05	•				
							_
					CANCEL	APPL	- 7
Copyright @ 1996-2014 Netgear @							

Step 4 – Set up LAN 1 on the computer and configure it to connect to the VMware player VMnet1

Computer Network Ports	VMware Ports	VMware Config	Switch
LAN 1	VMnet1	Custom: VMnet1 (Host Only)	Port 5 (Mirror)



Virtual Machine Settings	or Woncellor () Page No. or	
Hardware Options		
Device Memory Processors Hard Disk (SCSI) Network Adapter Display	Summary 8 GB 4 50 GB Custom (VMnet1) Bridged (Automatic) Auto detect	Device status Connected Connect at power on Network connection Bridged: Connected directly to the physical network Replicate physical network connection state Configure Adapters NAT: Used to share the host's IP address Host-only: A private network shared with the host Custom: Specific virtual network VMnet1 (Host-only) CLAN segment: LAN Segments Advanced
	Remove Remove	
		OK Cancel Help

Step 5 – Setup LAN 2 on the computer and configure it to connect to the VMware player

Computer Network Ports	VMware Ports	VMware Config	Switch
LAN 2	VMnet8	Bridged	Port 4 (access to Internet / able to get DHCP address)



Virtual Machine Settings	or Monophies () Pager Nor or	
Hardware Options		
Device Memory Processors Hard Disk (SCSI) Network Adapter Display Display	Summary 8 GB 4 50 GB Custom (VMnet1) Bridged (Automatic) Auto detect	Device status Connected Connect at power on Network connection Bridged: Connected directly to the physical network Replicate physical network connection state Configure Adapters MAT: Used to share the host's IP address MAT: Used to share the host's IP address Mat: Specific virtual network VMnet0 LAN segment: LAN Segments Advanced
	Add <u>R</u> emove	
		OK Cancel Help

Step 6 - Verify Setup

6.1 Verify in Control Panel Network Connections that both network cards and both VMware adapters exist. In this example LAN 1 is the Sensor port that attaches to the Mirror on the switch and LAN 2 is the port that attaches to the internet.



Control Panel > Network and Internet	t ▶ Network Connections ▶	▼ 4, Search Network Co	nnections
Organize 🔻			≡ - □ 0
Name	Status	Device Name	Connectivity
Local Area Connection	Network	Realtek PCIe GBE Family Controller	Internet access
Local Area Connection 2	Network	Realtek PCIe GBE Family Controller #2	Internet access
VMware Network Adapter VMnet1	Enabled	VMware Virtual Ethernet Adapter for VMnet1	
VMware Network Adapter VMnet8	Enabled	VMware Virtual Ethernet Adapter for VMnet8	
< [4

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

RetWatcher - OVF - VMware Workstation 12 Player (Non-commercial use only)	
<u>P</u> layer ▼ ▼ ⊕ [⊐] ဩ	*
This is localhost (Linux x86_64 4.3.6-coreos) 00:28:54 SSH host key: SHA256:Rc5LlmtsLvN56GRiKq23EN6ZP41D/rOgbyQj86B00RA SSH host key: SHA256:E3uRAtg29uznxkovuOxiItkPaeBCLgff4BiIrQSsps4 SSH host key: SHA256:MRuaZ5HRT1pBOXffw3LUXnXAomYLE21nIUz9oz/DtyU SSH host key: SHA256:DrW2YKMkkka+Inhw5Fn/cbi8LFgBFX36tcP12XtNO2o eno16777736: 192.168.139.130 fe80::20c:29ff:fefb:c6f3 eno33554960: 192.168.1.123 fe80::20c:29ff:fefb:c6fd	(DSA) (ECDSA) (ED25519) (RSA)
localhost login:	
This is localhost (Linux x86_64 4.3.6-coreos) 01:20:36 SSH host key: SHA256:Rc5LlmtsLvN56GRiKq23EN6ZP41D/rOgbyQj86B00RA SSH host key: SHA256:E3uRAtg29uznxkovuOxiItkPaeBCLgff4BiIrQSsps4 SSH host key: SHA256:MRuaZ5HRT1pBOXffw3LUXnXAomYLE21nIUZ9oz/DtyU SSH host key: SHA256:DrW2YKMkkka+Inhw5Fn/cbi8LFgBFX36tcP12XtNO2o eno16777736: fe80::20c:29ff:fefb:c6f3 eno33554960: 192.168.1.123 fe80::d664:6ec9:ee0d:2d94 localhost login: _	(DSA) (ECDSA) (ED25519) (RSA)