

Mirror Wire Data with VMware

Published: 2024-07-22

The ExtraHop virtual sensor can be configured to monitor network traffic in the following network configuration examples.

- [Monitoring traffic on multiple network interfaces or VLANs with ERSPAN](#)
- [Monitoring Intra-VM Traffic](#)
 - One virtual interface on the EDA 1100v
 - Up to three virtual interfaces on the EDA 6100v
- [Monitoring external mirrored traffic to the VM](#)
- [Monitoring external mirrored traffic to the VM \(EDA 6100v\)](#)
- [Monitoring both intra-VM and external mirrored traffic to the VM \(EDA 6100v\)](#)



Note: Monitoring external network-mirrored traffic requires an external NIC and an associated virtual switch.

Monitoring traffic on multiple network interfaces or VLANs with ERSPAN

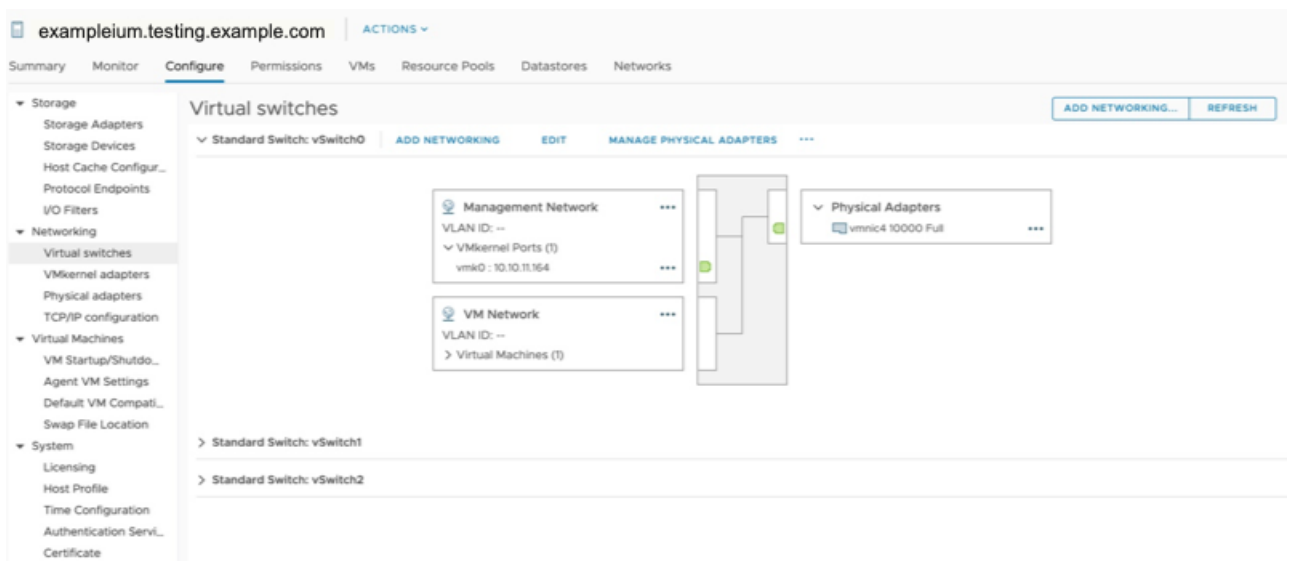
This scenario requires you to configure an interface on the ExtraHop system to receive ERSPAN traffic and configure the VMware server to mirror traffic from specified ports.

See [Configure ERSPAN with VMware](#) for configuration details.

Monitoring intra-VM traffic

This scenario requires a second VM port group on the default virtual switch of the ESX host for monitoring traffic within the virtual switch as well as external traffic in and out of the switch.

1. Start the VMware vSphere client and connect to your ESX server.
2. Select the ESX host at the top of the tree control in the left panel and then click the **Configure** tab.
3. In the **Networking** section, click Virtual Switches.



4. To add a port group to the vSwitch0, click **Add Networking**. The Add Networking window appears.
5. Select **Virtual Machine Port Group for a Standard Switch** as the connection type and then click **Next**.

exampleium.testing.example.com - Add Networking

1 Select connection type
2 Select target device
3 Connection settings
4 Ready to complete

Select connection type
Select a connection type to create.

VMkernel Network Adapter

The VMkernel TCP/IP stack handles traffic for ESXi services such as vSphere vMotion, iSCSI, NFS, FCoE, Fault Tolerance, vSAN and host management.

Virtual Machine Port Group for a Standard Switch

A port group handles the virtual machine traffic on standard switch.

Physical Network Adapter

A physical network adapter handles the network traffic to other hosts on the network.

[CANCEL](#) [BACK](#) [NEXT](#)

6. In the Select target device step, choose **Select an existing standard switch** and then click **Next**. The default switch is vSwitch0.

exampleium.testing.example.com - Add Networking

✓ 1 Select connection type
2 Select target device
3 Connection settings
4 Ready to complete

Select target device
Select a target device for the new connection.

Select an existing standard switch

vSwitch0 [BROWSE ...](#)

New standard switch

MTU (Bytes)

[CANCEL](#) [BACK](#) [NEXT](#)

7. In the Connection settings step, assign a unique name to the new port group, click the **VLAN ID** drop-down menu, and select **All (VLAN 4095)**.

exampleium.testing.example.com - Add Networking

✓ 1 Select connection type
 ✓ 2 Select target device
 3 Connection settings
 4 Ready to complete

Connection settings
Use network labels to identify migration-compatible connections common to two or more hosts.

Network label: Local Port Mirror

VLAN ID: All (4095) ▼

CANCEL BACK NEXT

8. Click **Next**.
9. Click **Finish**.
10. Set the Remote Port Mirror to Promiscuous Mode as follows.
 - a) In the vSwitch0 section, click the edit menu icon ... next to the new port group and click **Edit**.
 - b) Click **Security**.
 - c) Select the override checkbox next to Promiscuous mode set the Promiscuous Mode to **Accept**, and then click **OK**.

Local Port Mirror - Edit Settings

Properties
 Security
 Traffic shaping
 Teaming and failover

Promiscuous mode	<input checked="" type="checkbox"/> Override	Accept ▼
MAC address changes	<input type="checkbox"/> Override	Accept ▼
Forged transmits	<input type="checkbox"/> Override	Accept ▼

11. Click **VMs** from the top menu.
12. Right-click the name of the sensor virtual machine and click **Edit Settings**.
13. Click **Network Adapter 2**.
14. Select **Browse** from the drop-down menu.
15. Click **Local Port Mirror**, and then click **OK**.

Select Network



Filter

Name	Distributed Switch
Local Port Mirror	--
VM Network	--

2 items

16. Verify that Local Port Mirror appears next to Network Adapter 2 in the Edit Settings window, and then click **OK**.
17. Restart the sensor to activate the new adapter setting.

Monitoring external mirrored traffic to the VM

This scenario requires a second physical network interface and the creation of a second vSwitch associated with that NIC. This NIC then connects to a mirror, tap, or aggregator that copies traffic from a switch. This setup is useful for monitoring the intranet of an office.

1. Start the VMware vSphere client and connect to your ESX server.
2. Select the ESX host at the top of the tree control in the left panel and then click the **Configure** tab.
3. Click **Networking**.

The screenshot shows the 'Virtual switches' configuration page in vSphere. The left sidebar contains a navigation menu with categories like Storage, Networking, and Virtual Machines. The main area is titled 'Virtual switches' and shows a configuration for 'Standard Switch: vSwitch0'. It lists several virtual machines connected to the switch: 'Local Port Mirror' (VLAN ID: 4095), 'Management Network' (VLAN ID: --), and 'VM Network'. A physical adapter 'vmnic4 10000 Full' is also shown connected to the switch. Buttons for 'ADD NETWORKING...', 'EDIT', and 'MANAGE PHYSICAL ADAPTERS' are visible at the top of the configuration area.

This view shows how the virtual switch is configured. It displays the physical NIC to which the vSwitch is tied (vmnic4 is eth0) and which networking components are connected to that vSwitch.

4. To add a second vSwitch, click **Add Networking**. The Add Network Wizard window appears.
5. Select **Virtual Machine Port Group for a Standard Switch** as the connection type and then click **Next**.

The screenshot shows the 'Add Networking' wizard in vSphere. The wizard is titled 'exampleium.testing.example.com - Add Networking' and shows a progress bar with four steps: 1. Select connection type (current), 2. Select target device, 3. Connection settings, and 4. Ready to complete. The 'Select connection type' step is active, showing three options: 'VMkernel Network Adapter', 'Virtual Machine Port Group for a Standard Switch' (selected), and 'Physical Network Adapter'. The 'Virtual Machine Port Group for a Standard Switch' option is selected, and its description is visible: 'A port group handles the virtual machine traffic on standard switch.' Buttons for 'CANCEL', 'BACK', and 'NEXT' are at the bottom right.

6. In the Select target device step, select **New standard switch**, and then click **Next**.

exampleium.testing.example.com - Add Networking

✓ 1 Select connection type
2 Select target device
3 Create a Standard Switch
4 Connection settings
5 Ready to complete

Select target device
Select a target device for the new connection.

Select an existing standard switch

[BROWSE ...](#)

New standard switch

MTU (Bytes)

[CANCEL](#) [BACK](#) [NEXT](#)

7. In the Create a Standard Switch step, click the Add adapters icon (+).

exampleium.testing.example.com - Add Networking

✓ 1 Select connection type
✓ 2 Select target device
3 Create a Standard Switch
4 Connection settings
5 Ready to complete

Create a Standard Switch
Assign free physical network adapters to the new switch.

Assigned adapters

+ × ↑ ↓

Ad Add adapters

Standby adapters

Unused adapters

Select a physical network adapter from the list to view its details.

CANCEL BACK NEXT

8. Select the NIC interface for external traffic mirroring, and then click **OK**.

Add Physical Adapters to the Switch



Network Adapters

vmnic1
vmnic1000402
vmnic2
vmnic3

All Properties CDP LLDP

Adapter Name	Mellanox Technologies MT27500 Family [ConnectX-3] vmnic1000402
Location	PCI 0000:41:00.0
Driver	nmlx4_en
Status	
Status	Connected
Actual speed, Duplex	10000 Mb, Full Duplex
Configured speed, Duplex	10000 Mb, Full Duplex
Networks	10.20.192.1-10.20.255.254 (VLAN1020) 192.168.12.1-192.168.15.254 (VLAN5) 10.10.0.1-10.10.15.254 (VLAN1010) 10.10.0.1-10.10.15.254 0.0.0.1-255.255.255.254 (VLAN4)
Network I/O Control	
Status	Allowed
SR-IOV	
Status	Not supported
Cisco Discovery Protocol	
Version	2

CANCEL

OK

- Verify the assigned adapter and then click **Next**.

exampleium.testing.example.com - Add Networking

✓ 1 Select connection type
 ✓ 2 Select target device
3 Create a Standard Switch
 4 Connection settings
 5 Ready to complete

Create a Standard Switch
Assign free physical network adapters to the new switch.

Assigned adapters

+ | × | ↑ | ↓
 Active adapters
 (New) vmnic1000402
 Standby adapters
 Unused adapters

All	Properties	CDP	LLDP
Adapter	Mellanox Technologies: [ConnectX-3]		
Name	vmnic1000402		
Location	PCI 0000:41:00.0		
Driver	nmlx4_en		
Status			
Status	Connected		
Actual speed, Duplex	10000 Mb, Full Duplex		
Configured speed, Duplex	10000 Mb, Full Duplex		
Networks	10.20.192.1-10.20.255.2 192.168.12.1-192.168.15.: 10.10.0.1-10.10.15.254 (10.10.0.1-10.10.15.254 0.0.0.1-255.255.255.25		
Network I/O Control			
Status	Allowed		
SR-IOV			

CANCEL BACK NEXT

10. In the Connection settings step, type a unique name in the Network label field, select **All (VLAN 4095)** from the VLAN ID drop-down menu, and then click **Next**.

exampleium.testing.example.com - Add Networking

✓ 1 Select connection type
 ✓ 2 Select target device
 ✓ 3 Create a Standard Switch
 4 Connection settings
 5 Ready to complete

Connection settings
 Use network labels to identify migration-compatible connections common to two or more hosts.

Network label: Remote Port Mirror
 VLAN ID: All (4095)

CANCEL BACK NEXT

11. Review your settings and then click **Finish**.
12. Set the Remote Port Mirror to Promiscuous Mode as follows.
 - a) Click **Edit** next to vSwitch1.

Virtual switches

> Standard Switch: vSwitch0
 > Standard Switch: vSwitch2
 ▼ Standard Switch: vSwitch1 ADD NETWORKING EDIT MANAGE PHYSICAL ADAPTERS ...

Remote Port Mirror
 VLAN ID: 4095
 Virtual Machines (0)

Physical Adapters
 vmnic1000402 10000 Full

- b) Click the **Security** tab, set the Promiscuous Mode to **Accept**, and then click **OK**.



Note: Mac address changes and Forged transmits are set to **Accept** by default. You can change these settings to **Reject** if required for your environment.

vSwitch1 - Edit Settings

Properties		
Security	Promiscuous mode	Accept
Traffic shaping	MAC address changes	Reject
Teaming and failover	Forged transmits	Reject

CANCEL

OK

13. In the left panel, select the ExtraHop virtual sensor.
14. Click the **Actions** drop-down menu and then select **Edit Settings....**
15. Click **Network Adapter 2** and then click **Browse...** from the drop-down menu.

Edit Settings | example-eda ×

Virtual Hardware | VM Options ADD NEW DEVICE

> CPU	2	▼	i
> Memory	4	GB	▼
> Hard disk 1	4	GB	▼
> Hard disk 2	20	GB	▼
> SCSI controller 0	VMware Paravirtual		
> Network adapter 1	VM Network		☑ Connect...
> Network adapter 2	<div style="border: 1px solid #007bff; padding: 2px; display: inline-block;"> ✓ VM Network Browse ... </div>		☑ Connect... (X)
> USB controller	USB 2.0		

16. Click **Remote Port Mirror**, and then click **OK**.

Select Network



Filter

Name	Distributed Switch
Local Port Mirror	--
Remote Port Mirror	--
VM Network	--

3 items

- Restart the ExtraHop VM to activate the new adapter setting.

Monitoring external mirrored traffic to the VM (EDA 6100v)

In this scenario, you must create a third and fourth physical network interface and two more vSwitches associated with those NICs. These NICs then connect to a mirror, tap, or aggregator that copies traffic from a switch.

- Start the VMware vSphere client and connect to your ESX server.
- Select the ESX host at the top of the navigation tree in the left panel and then click the **Configure** tab.
- Click **Networking** and then click **Add Networking**.
- Select **Virtual Machine Port Group for a Standard Switch** as the connection type and then click **Next**.
- In the Select target device step, choose **Select an existing standard switch** and then click **Next**. The default switch is vSwitch0.
- In the Connection settings step, assign a unique name to the new port group (Remote Port Mirror 2, for example), click the **VLAN ID** drop-down menu, and select **All (VLAN 4095)**.
- Click **Next** and then click **Finish**.
- Set the Remote Port Mirror to Promiscuous Mode as follows.
 - Click **Edit** next to vSwitch2.
 - Click the **Security** tab, set the Promiscuous Mode to **Accept**, and then click **OK**.



Note: Mac address changes and Forged transmits are set to **Accept** by default. You can change these settings to **Reject** if required for your environment.

- In the left panel, select the ExtraHop virtual sensor.
- Click the **Actions** drop-down menu and then select **Edit Settings...**
- Click **Network Adapter 3** and then click **Browse...** from the drop-down menu.
- Click **Remote Port Mirror 2**, and then click **OK**.
- Repeat steps 3 through 10 to add a fourth vSwitch.

14. Restart the ExtraHop VM to activate the new adapter setting.

Monitoring both intra-VM and external mirrored traffic to the VM (EDA 6100v)

In this scenario, you can monitor a mix of intra-VM and external mirrored traffic on up to three virtual interfaces.





1. To monitor intra-VM traffic on one or more virtual interfaces, create a VM port group on the default virtual switch of the ESX host for each interface as described in [Monitoring Intra-VM Traffic](#).
2. To monitor external mirrored traffic on one or more virtual interfaces, create a physical network interface and corresponding vSwitch for each interface as described in [Monitoring External Mirrored Traffic to the VM](#).
3. Click **Network Adapter x** and select an option from the **Network label** drop-down list for each interface.

Mirroring VLANs

To mirror VLANs, you must either set the destination port on the port mirror configuration to VLAN Trunking or set the exact VLAN ID on the ports of the VLANs you are mirroring.

Related documentation

For information about configuring RSPAN, ERSPAN, and RPCAP to monitor remote devices, see the following topics.

- [Configure RSPAN with VMware](#) 
- [Configure ERSPAN with VMware](#) 
- [Configure ERSPAN with the Nexus 1000V](#) 
- [Packet Forwarding with RPCAP](#) 

For information about mirroring traffic with VMware, see [Mirror Wire Data with VMware](#).