Mirror Wire Data with VMware

Published: 2021-10-26

The ExtraHop Discover virtual appliance 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 1000v or 1100v
  - Up to three virtual interfaces on the EDA 2000v or EDA 6100v
- Monitoring external mirrored traffic to the VM
- Monitoring external mirrored traffic to the VM (EDA 2000v or EDA 6100v)
- Monitoring both intra-VM and external mirrored traffic to the VM (EDA 2000v or 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

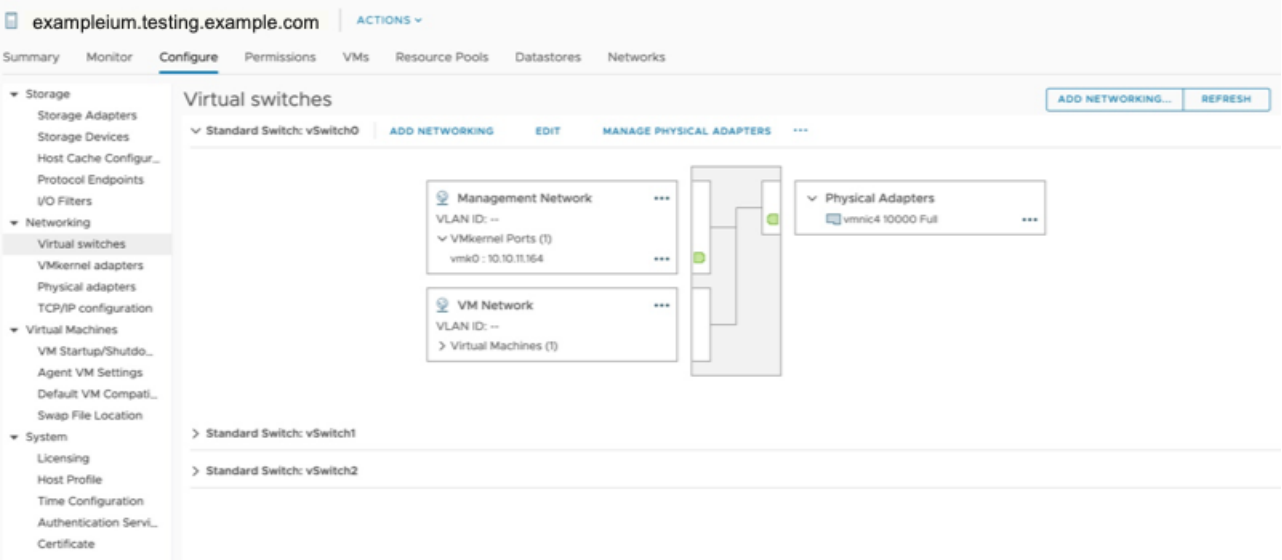
This scenario requires you to configure an interface on the ExtraHop system to receive ERSPAN traffic and configure the VMware server to mirror traffic from specified ports.

See Configure ERSPAN with VMware for configuration details.

Monitoring intra-VM traffic

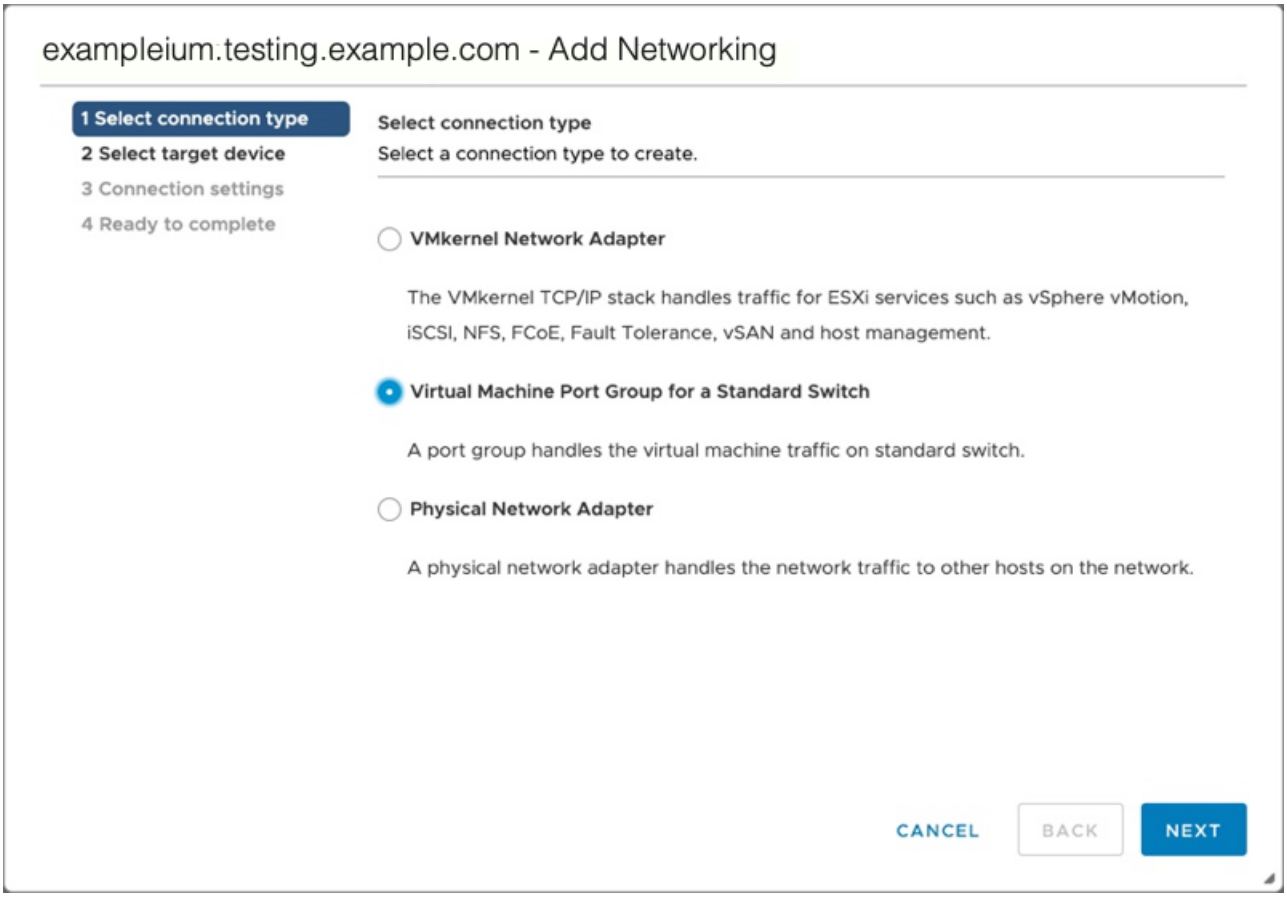
This scenario requires a second VM port group on the default virtual switch of the ESX host for monitoring traffic within the virtual switch as well as external traffic in and out of the switch.

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.

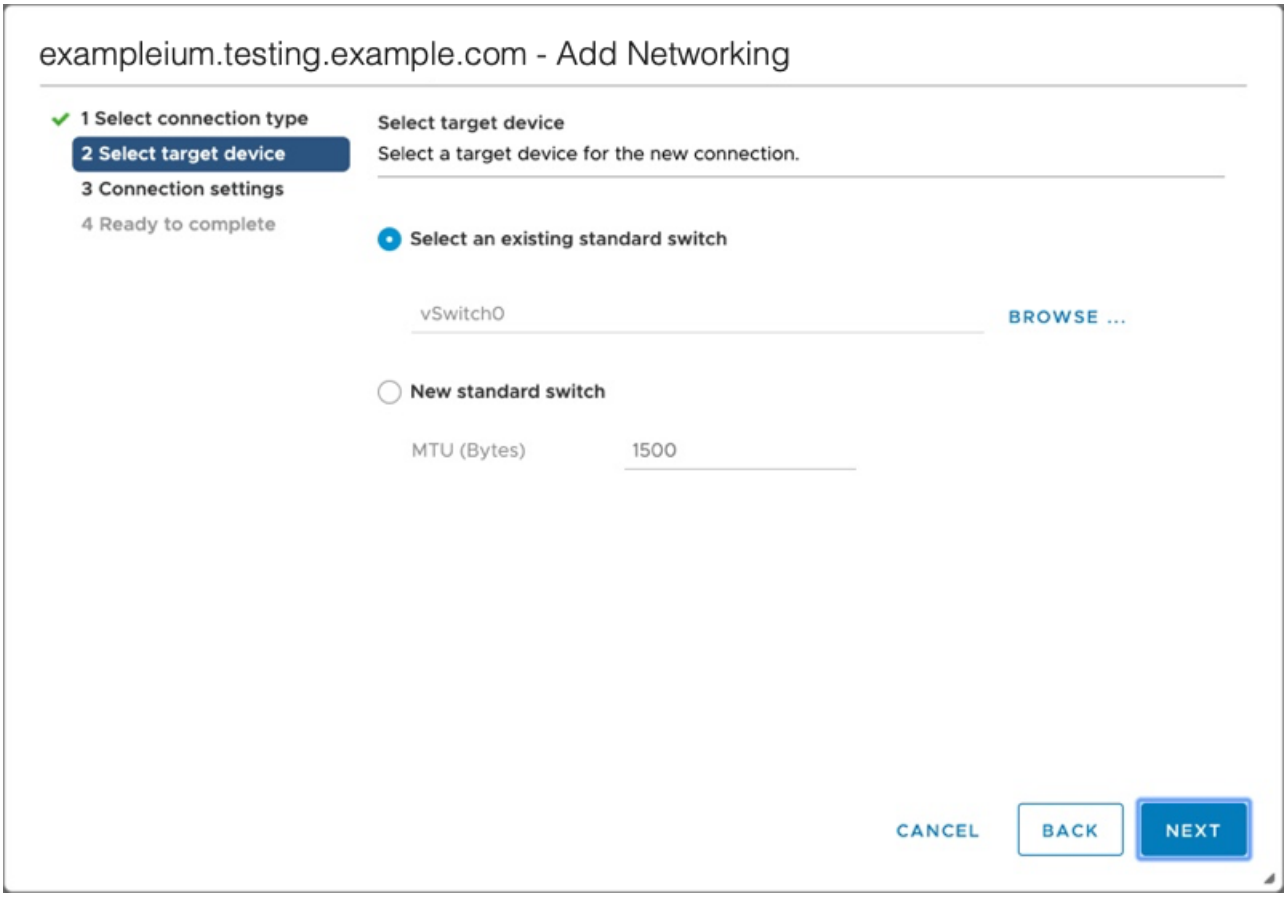


4. To add a port group to the vSwitch0, click **Add Networking**.
   The Add Networking window appears.
5. Select **Virtual Machine Port Group for a Standard Switch** as the connection type and then click **Next**.

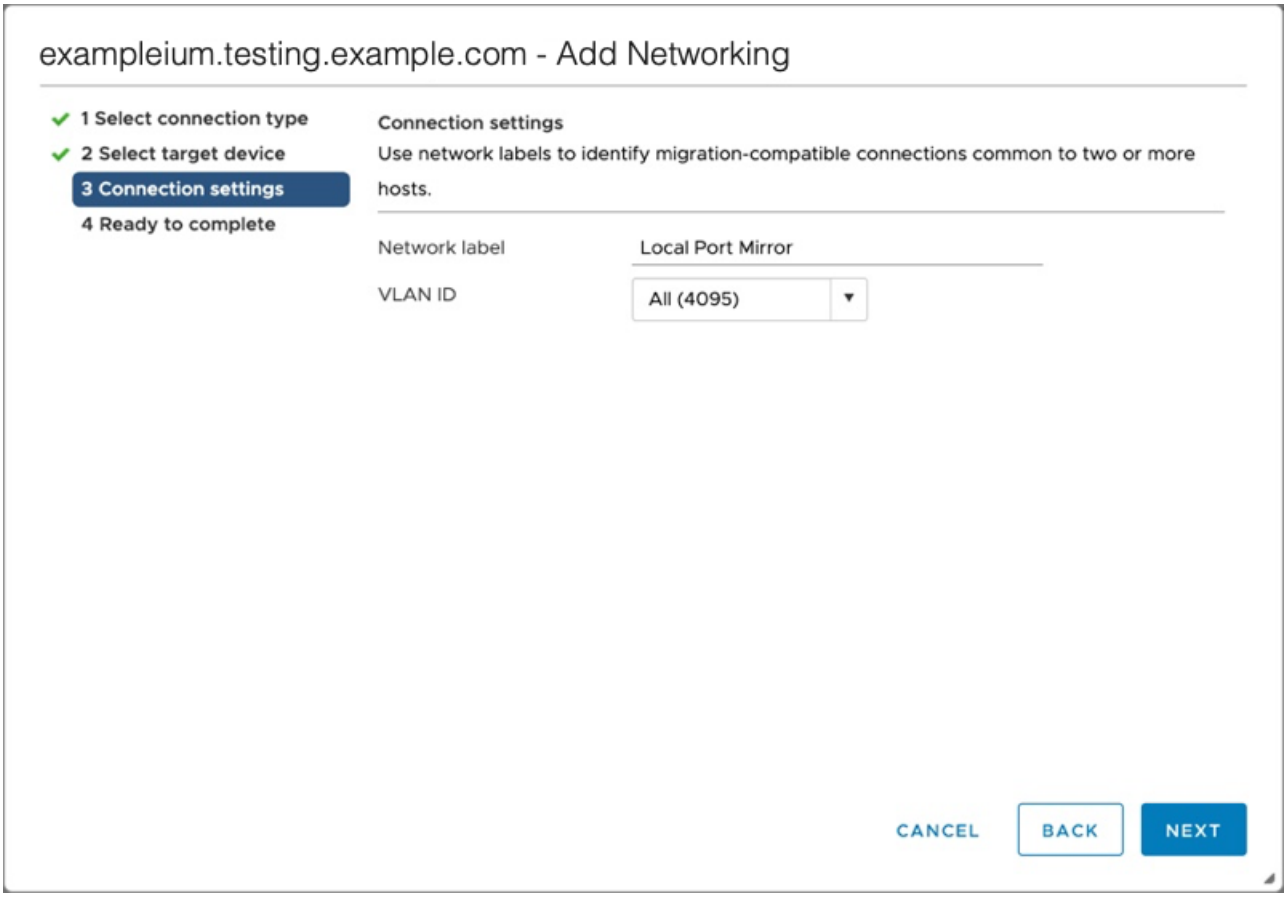
© 2021 ExtraHop Networks, Inc. All rights reserved.



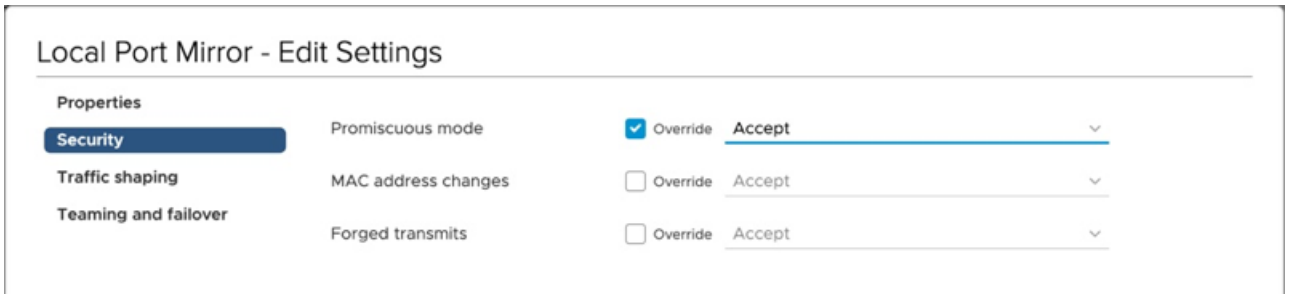
6. In the Select target device step, choose **Select an existing standard switch** and then click **Next**. The default switch is vSwitch0.



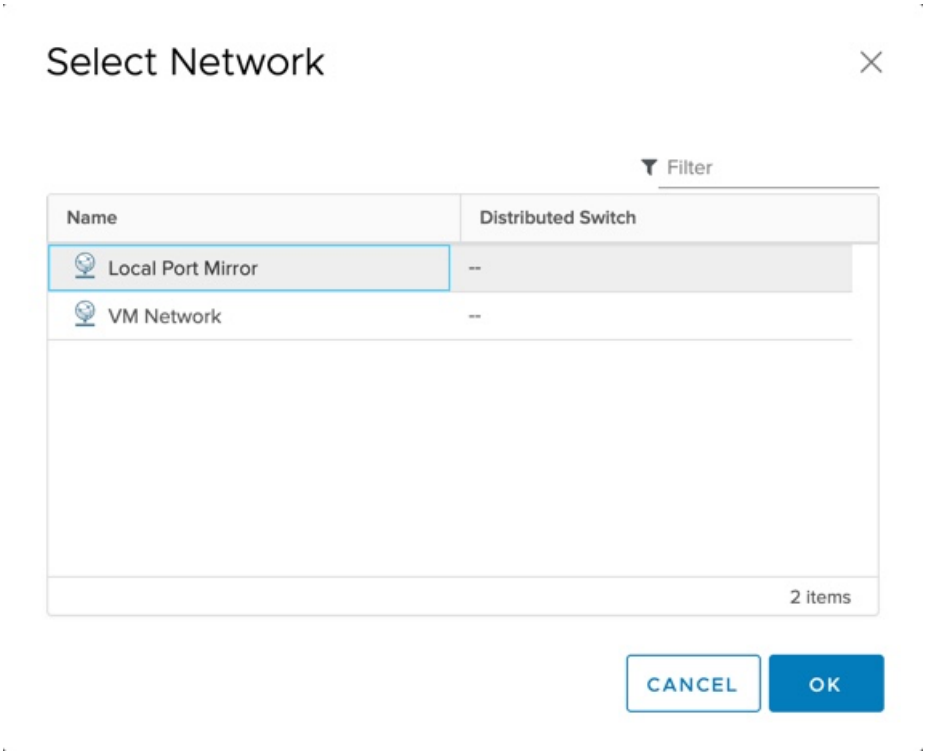
7. In the Connection settings step, assign a unique name to the new port group, click the **VLAN ID** drop-down menu, and select **All (VLAN 4095)**.



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**.



11. Click **VMs** from the top menu.
12. Right-click the name of the Discover appliance 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**.

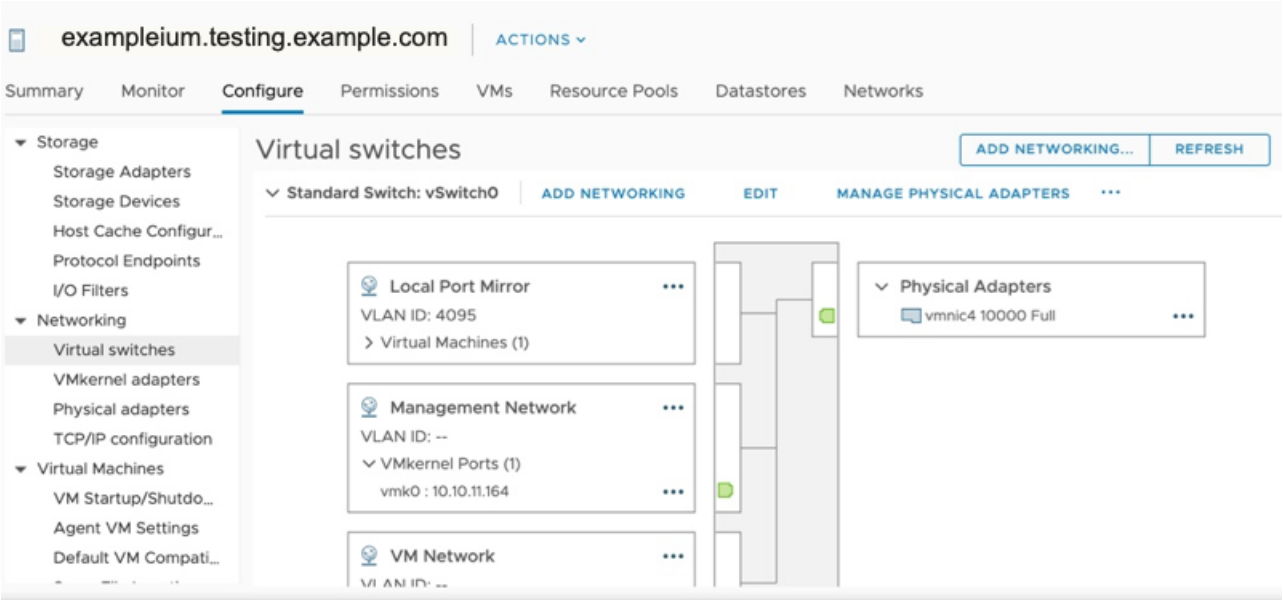


16. Verify that Local Port Mirror appears next to Network Adapter 2 in the Edit Settings window, and then click **OK**.
17. Restart the Discover virtual appliance to activate the new adapter setting.

Monitoring external mirrored traffic to the VM

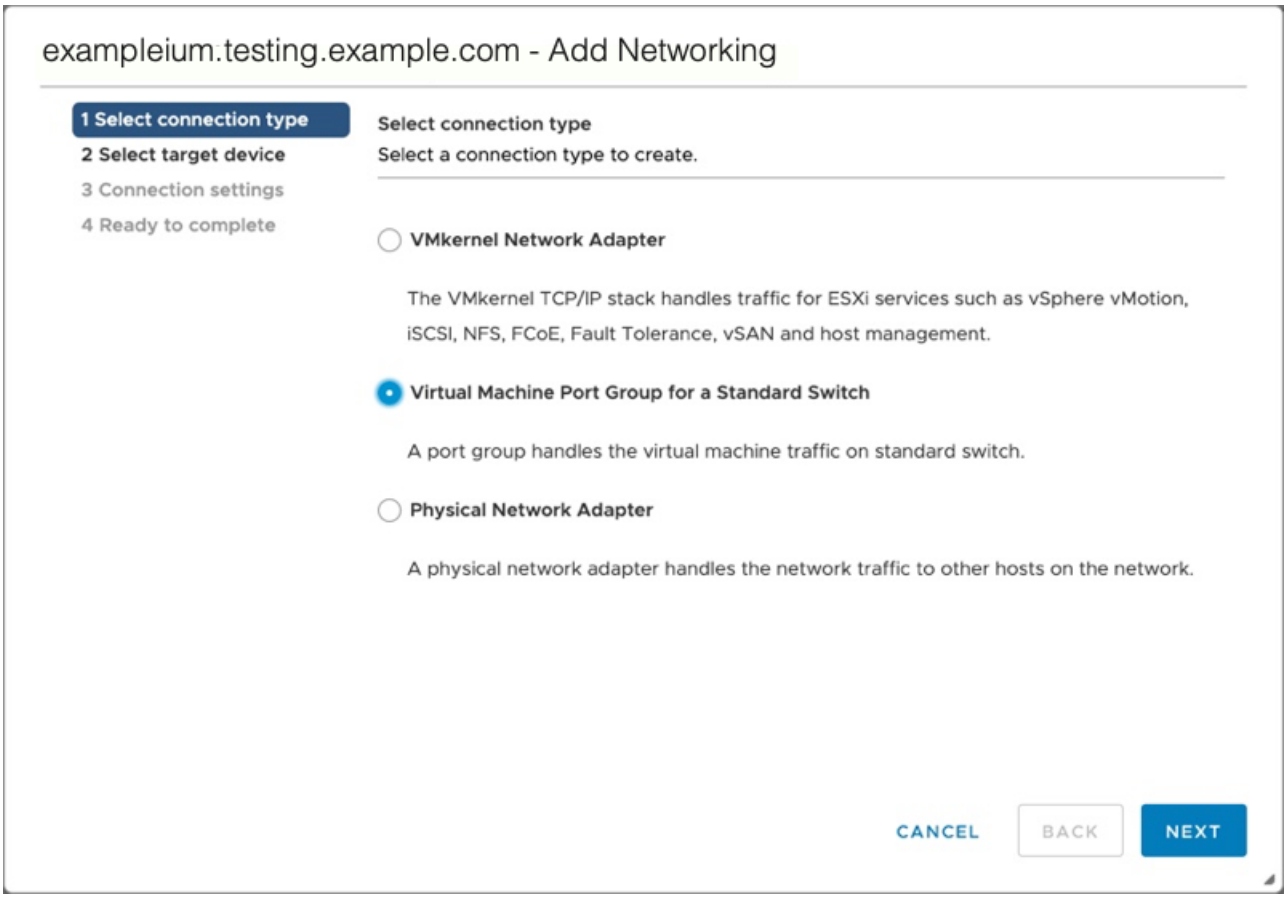
This scenario requires a second physical network interface and the creation of a second vSwitch associated with that NIC. This NIC then connects to a mirror, tap, or aggregator that copies traffic from a switch. This setup is useful for monitoring the intranet of an office.

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**.

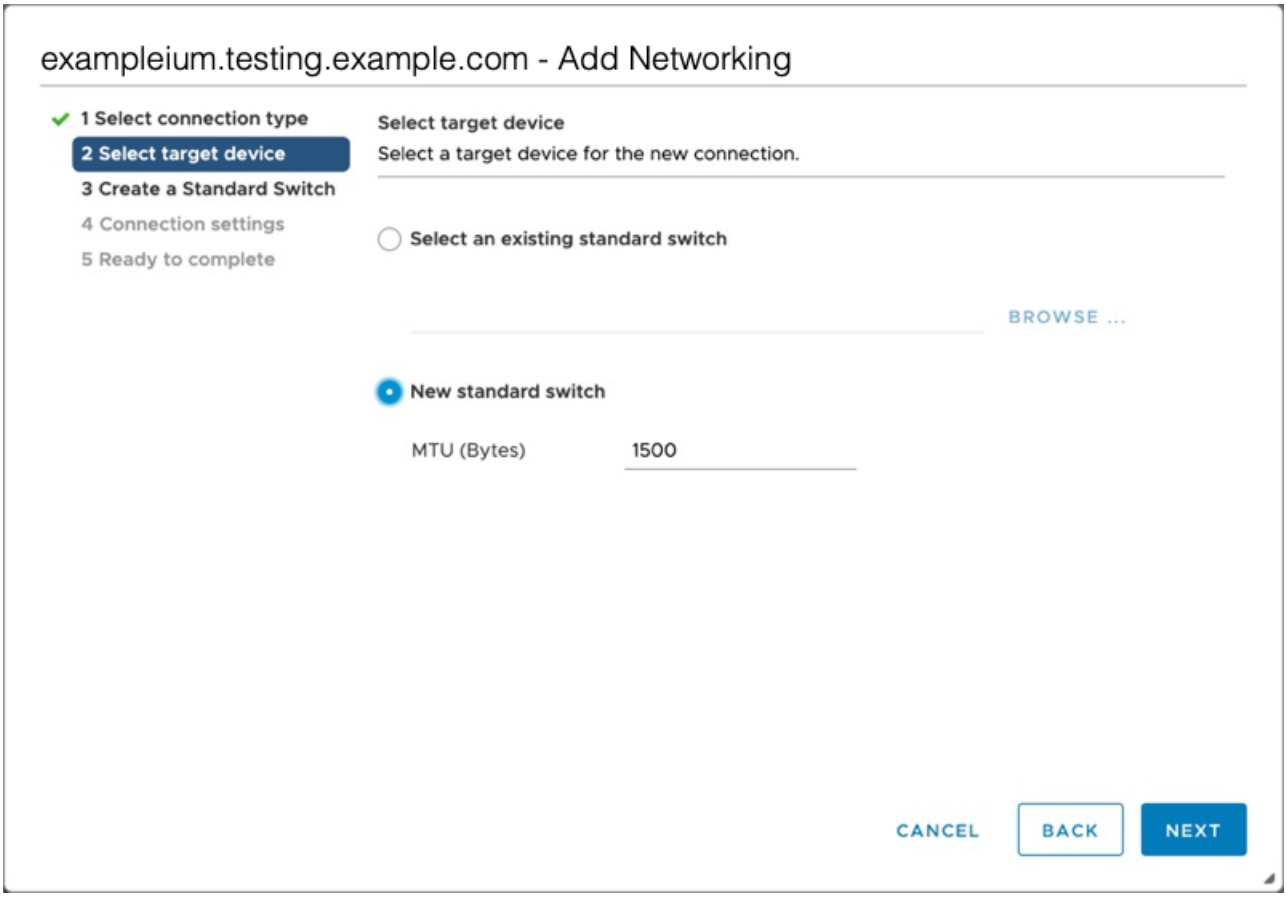


This view shows how the virtual switch is configured. It displays the physical NIC to which the vSwitch is tied (vmnic4 is eth0) and which networking components are connected to that vSwitch.

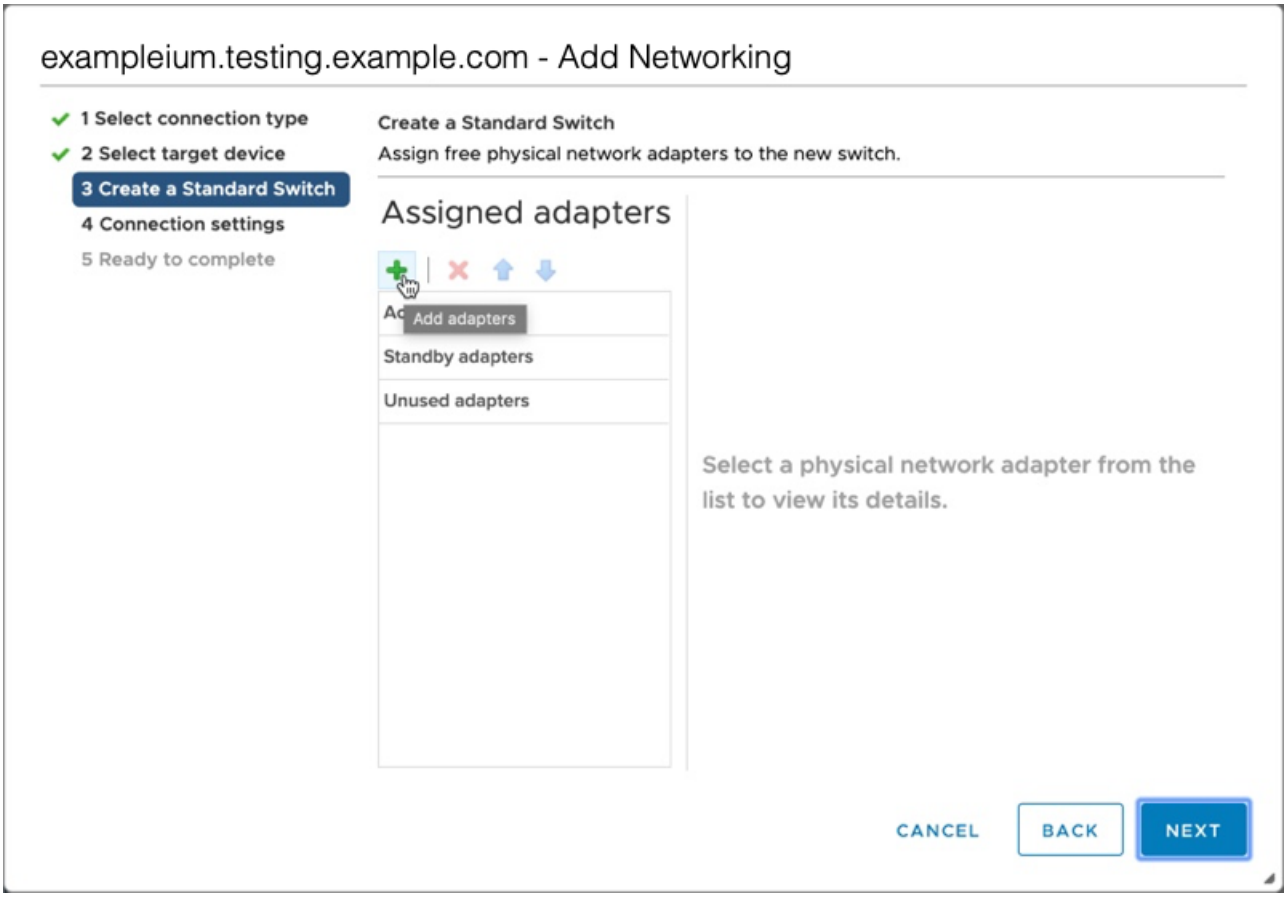
4. To add a second vSwitch, click **Add Networking**. The Add Network Wizard window appears.
5. Select **Virtual Machine Port Group for a Standard Switch** as the connection type and then click **Next**.



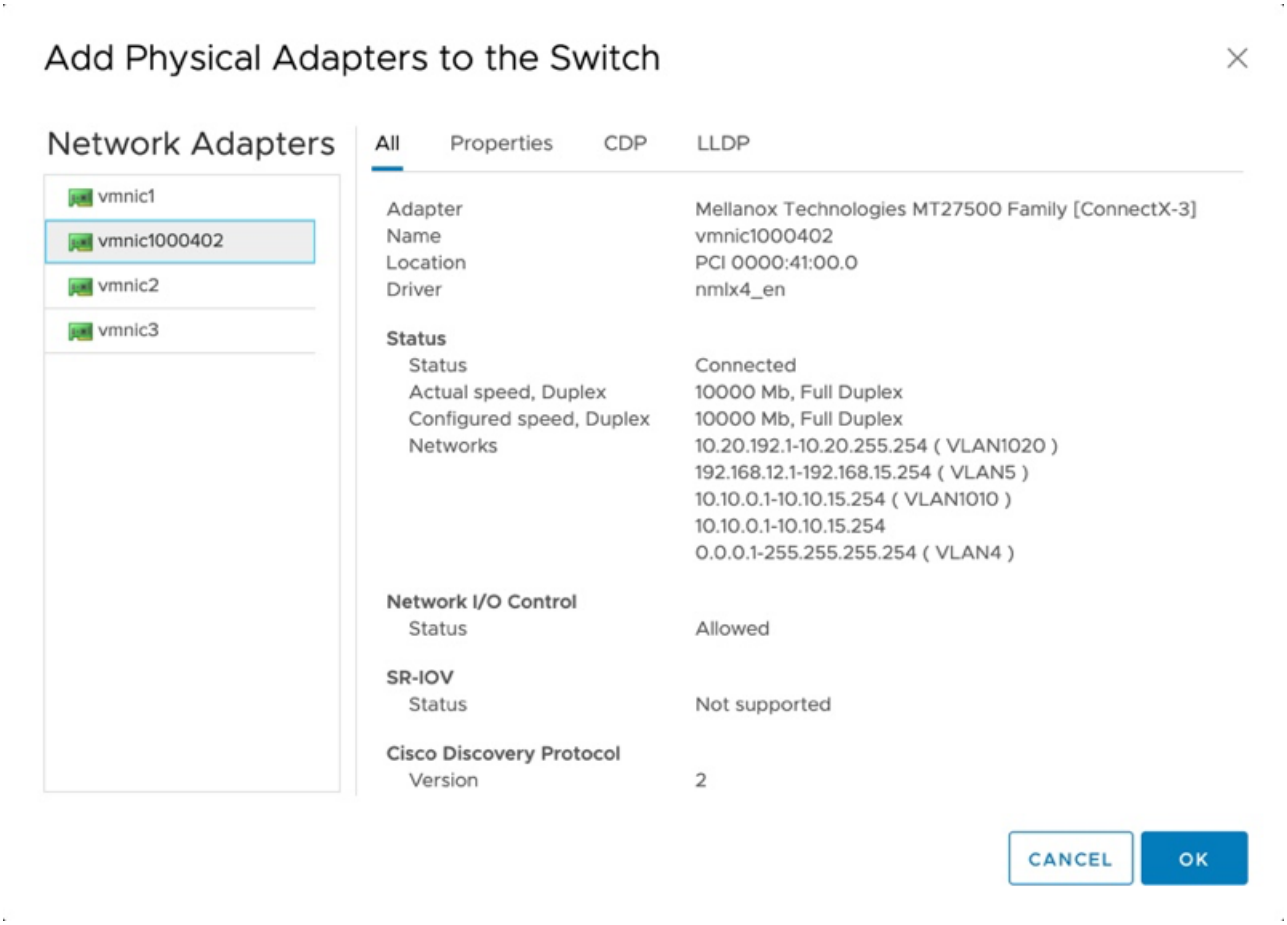
6. In the Select target device step, select **New standard switch**, and then click **Next**.



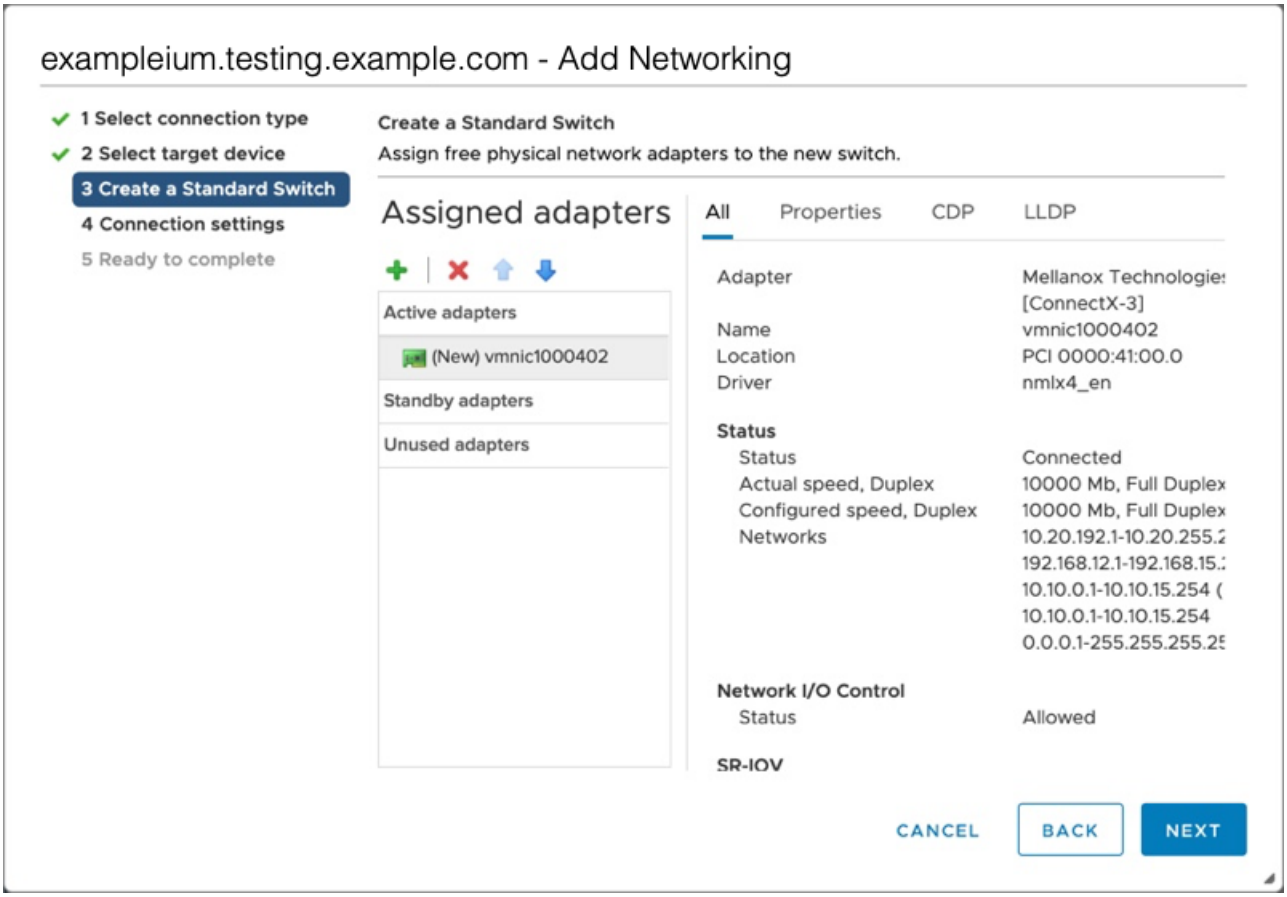
7. In the Create a Standard Switch step, click the Add adapters icon (**+**).



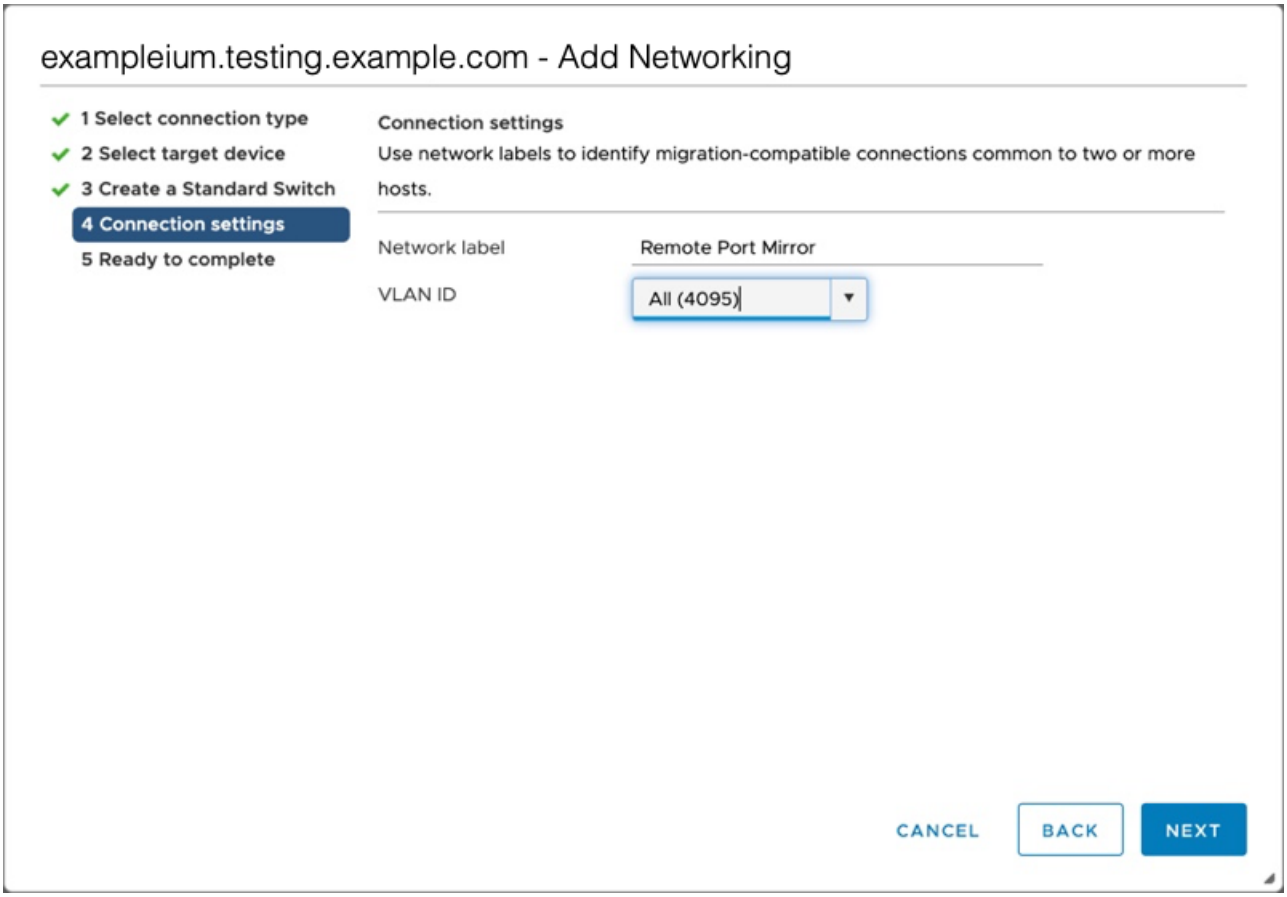
8. Select the NIC interface for external traffic mirroring, and then click **OK**.



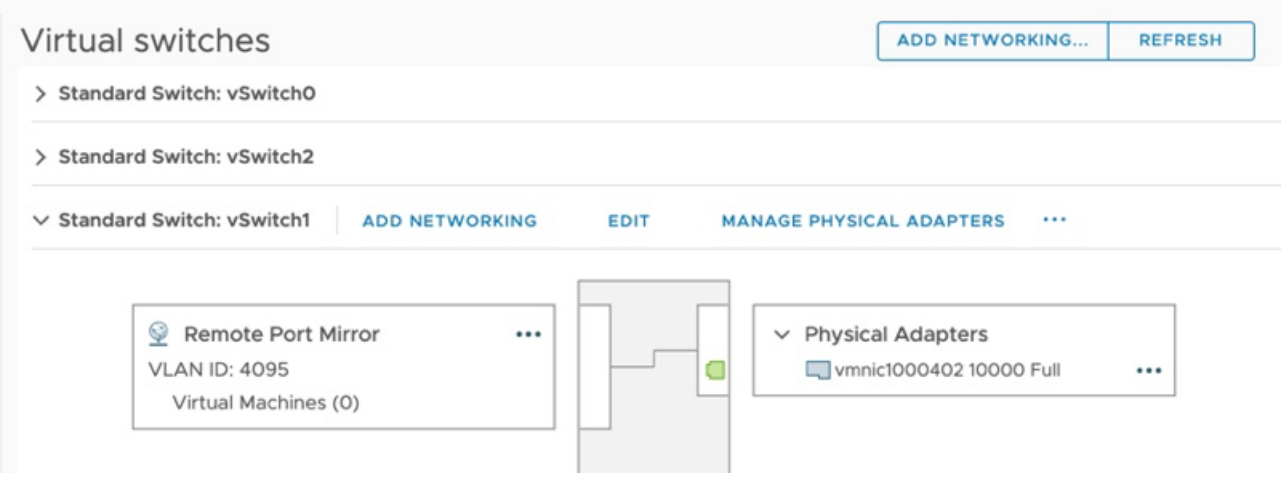
9. Verify the assigned adapter and then click **Next**.



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**.

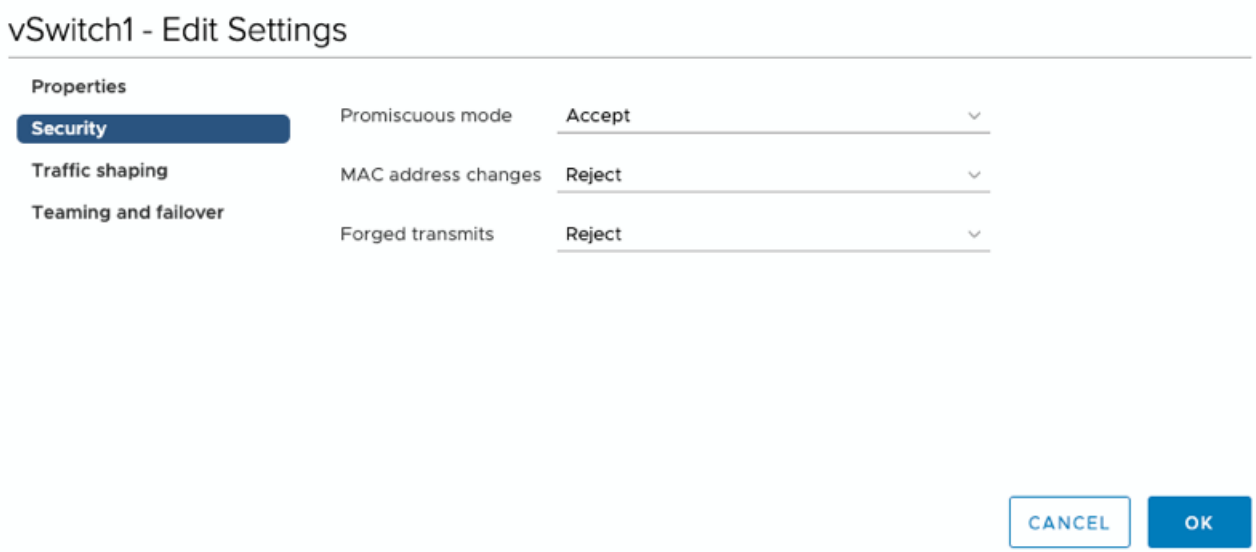


11. Review your settings and then click **Finish**.
12. Set the Remote Port Mirror to Promiscuous Mode as follows.
    a) Click **Edit** next to vSwitch1.

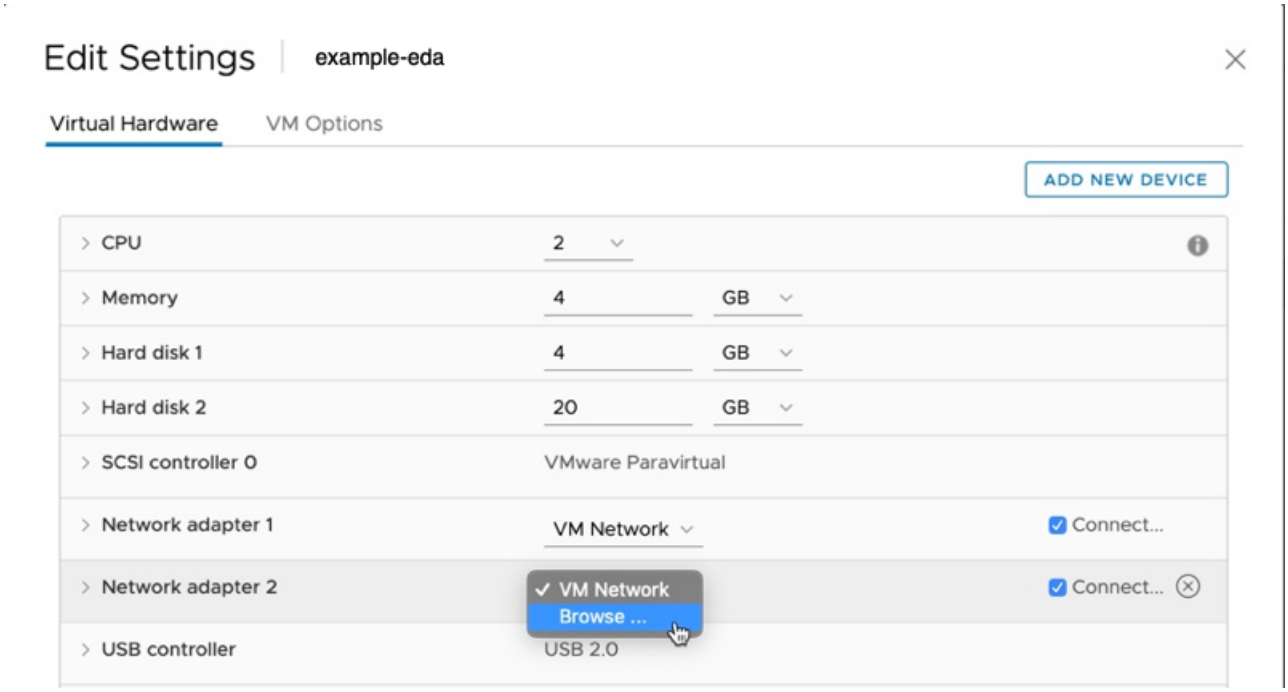


    b) Click the **Security** tab, set the Promiscuous Mode to **Accept**, and then click **OK**.

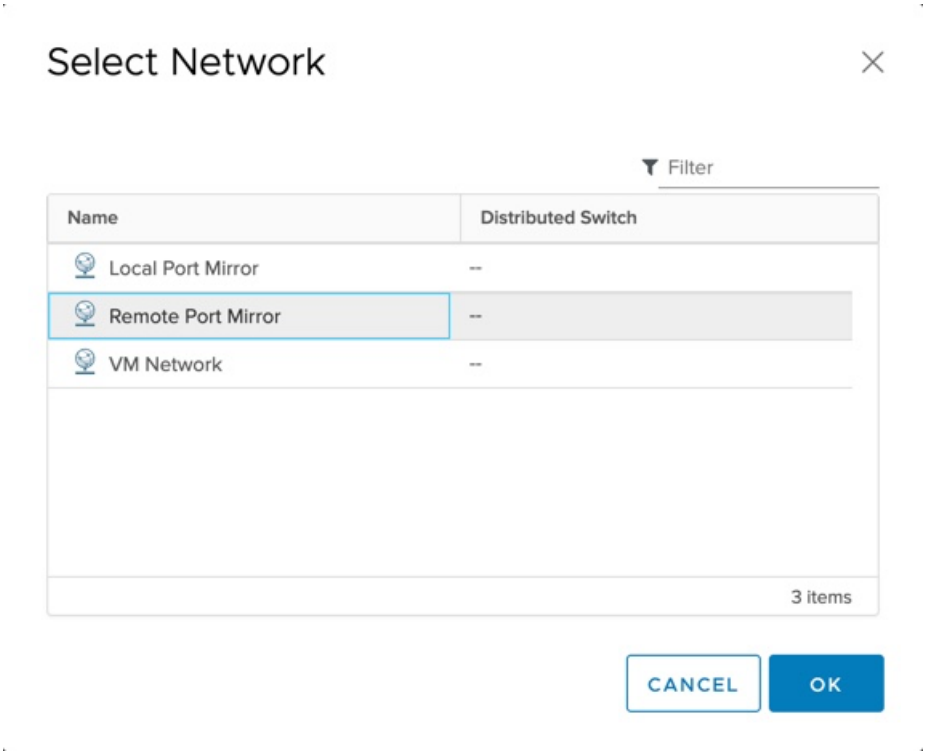
> **Note:** Mac address changes and Forged transmits are set to **Accept** by default. You can change these settings to **Reject** if required for your environment.



13. In the left panel, select the ExtraHop virtual appliance.
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.



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



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

Monitoring external mirrored traffic to the VM (EDA 2000v or 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.

1. Start the VMware vSphere client and connect to your ESX server.
2. Select the ESX host at the top of the navigation tree in the left panel and then click the **Configure** tab.
3. Click **Networking** and then click **Add Networking**.
4. Select **Virtual Machine Port Group for a Standard Switch** as the connection type and then click **Next**.
5. In the Select target device step, choose **Select an existing standard switch** and then click **Next**. The default switch is vSwitch0.
6. 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)**.
7. Click **Next** and then click **Finish**.
8. Set the Remote Port Mirror to Promiscuous Mode as follows.
   a) Click **Edit** next to vSwitch2.
   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.
9. In the left panel, select the ExtraHop virtual appliance.
10. Click the **Actions** drop-down menu and then select **Edit Settings...**.
11. Click **Network Adapter 3** and then click **Browse...** from the drop-down menu.
12. Click **Remote Port Mirror 2**, and then click **OK**.
13. 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 2000v or 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