

Configure ERSPAN with VMware

Published: 2024-04-02

The Encapsulated Remote Switched Port Analyzer (ERSPAN) enables you to monitor traffic on multiple network interfaces or VLANs and then send the monitored traffic to one or more destinations. The ExtraHop system supports the VMware Encapsulated Remote Mirroring Source packet mirror feature, an ERSPAN-like capability.

The following procedures explain how to configure an interface on the ExtraHop system to receive ERSPAN traffic and how to configure the VMware server with the vSphere Web Client.

For more information about configuring networking on the ExtraHop system, see the [ExtraHop Admin UI Guide](#).

For more information about configuring the VMware vSphere server, see [Working with Port Mirroring](#) in the VMware documentation.

Configure the ExtraHop interface settings

1. Log in to the Administration settings on the ExtraHop system through `https://<extrahop-hostname-or-IP-address>/admin`.
2. In the Network Settings, click **Connectivity**.
3. In the Interfaces section, click **Interface 1**.



Note: If you select **Interface 1** for management and **Interface 2** for ERSPAN, you cannot configure both interfaces on the same subnet.

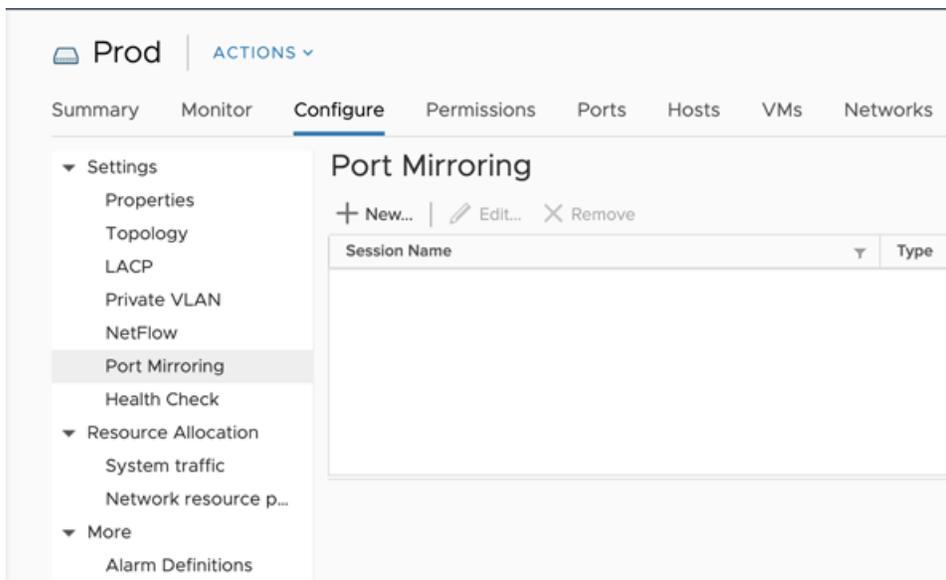
4. Select **Management + RPCAP/ERSPAN/VXLAN/GENEVE Target** from the **Interface Mode** drop-down list.
5. Complete the remaining fields and then click **Save**.
6. Optional: Depending on your configuration, configure or disable the remaining interfaces.



Note: For more information about setting up network interfaces, see the [Connectivity](#) section in the ExtraHop Administration Guide.

Configure port mirroring on the vSphere server

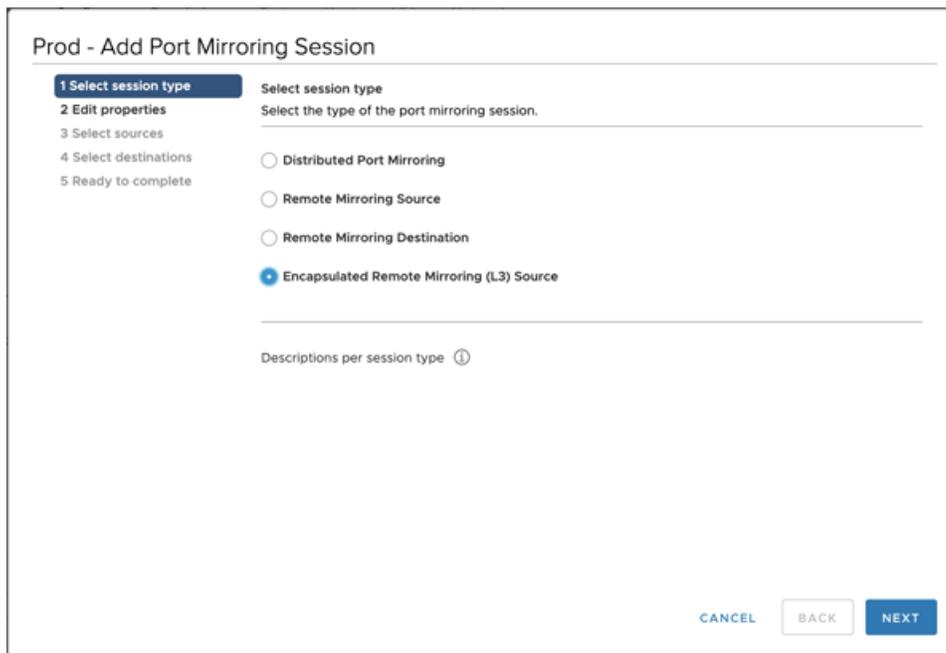
1. Log in to the vSphere Web Client and select the vSphere distributed switch (VDS) from which you want to monitor traffic.
2. Click the **Settings** tab.
3. In the Settings section, click **Port Mirroring**.



4. Click **New...** to create a port mirroring session to mirror vSphere distributed switch traffic to specific physical switch ports.

Tip: For detailed information about creating a port mirroring session, see your vSphere documentation.

- a) In the Select session type section, select **Encapsulated Remote Mirroring (L3) Source** and click **Next**.



- b) In the **Edit properties** section, configure the following settings:

- **Name:** Specify the name.
- **Status:** Select **Enabled** from the drop-down list.
- **Encapsulation type:** Select **ERSPAN Type II** from the drop-down list

Note: GRE is a supported encapsulation type; however, you must configure [Network Overlay Decapsulation](#) for NVGRE on the sensor.

Prod - Add Port Mirroring Session

1 Select session type
2 Edit properties
 3 Select sources
 4 Select destinations
 5 Ready to complete

Edit properties
 Specify a name and the properties of the port mirroring session.

Name: Session 0
 Status: Enabled
 Session type: Encapsulated Remote Mirroring (L3) Source
 GRE
ERSPAN Type II
 ERSPAN Type III
 Session ID: 0

Advanced properties
 Mirrored packet length: Enable 60
 Sampling rate: 1
 Description:

CANCEL BACK NEXT

c) In the Select sources section, select existing ports or create new source ports and then click **Next**.

Warning: Do not include any VMkernel (vmk) ports, any ports connected to the virtual Reveal(x) sensor, or any ports that might be carrying the ERSPAN data created by this mirror. Adding these ports will compound the traffic destined for the sensor and disrupt the networking capabilities of the dvSwitch, causing any hosts or interfaces participating in the dvSwitch to become permanently unavailable.

d) In the Select Ports section, select virtual ports to include in this mirror.

Warning: Do not include any VMkernel (vmk) ports, any ports connected to the virtual Reveal(x) sensor, or any ports that might be carrying the ERSPAN data created by this mirror. Adding these ports will compound the traffic destined for the sensor and disrupt the networking capabilities of the dvSwitch, causing any hosts or interfaces participating in the dvSwitch to become permanently unavailable.

Select Ports

Port ID	Port Name	Connected Entity	Host	Runtime MAC Addr...	Port Group Name
<input checked="" type="checkbox"/>	0	mike-linu-3	mike-esxi-4.ad...	--	Core
<input checked="" type="checkbox"/>	1	PAN_Migrati...	mike-esxi-4.ad...	--	Core
<input type="checkbox"/>	14	vmk1	mike-esxi-3.ad...	00:50:56:69:dc:ba	NFS
<input checked="" type="checkbox"/>	164	mike-pavm-a	mike-esxi-4.ad...	--	traps-5-user
<input checked="" type="checkbox"/>	2	mike-serv-2	mike-esxi-4.ad...	00:50:56:b5:1f:40	Core
<input checked="" type="checkbox"/>	204	mike-pavm-a	mike-esxi-4.ad...	--	Demo
<input checked="" type="checkbox"/>	205	mike-wtst-1	mike-esxi-3.ad...	--	Demo
<input checked="" type="checkbox"/>	206	mike-wtst-2	mike-esxi-3.ad...	--	Demo
<input checked="" type="checkbox"/>	207	mike-kali-1	mike-esxi-3.ad...	--	Demo
<input checked="" type="checkbox"/>	208	CbArtifactKit	mike-esxi-3.ad...	--	Demo
<input checked="" type="checkbox"/>	209	test-esxi-1	mike-esxi-4.ad...	--	Demo

CANCEL OK

e) Click **Next**.

f) In the Select destinations section, click the plus sign (+) to add the IP address or addresses that should receive the mirrored traffic.

Prod - Add Port Mirroring Session

- ✓ 1 Select session type
- ✓ 2 Edit properties
- ✓ 3 Select sources
- 4 Select destinations**
- 5 Ready to complete

Select destinations
Select the destination ports and the uplinks of the port mirroring session.

+ ×

IP Address

10.75.1.127

CANCEL BACK NEXT

g) In the Ready to complete section, verify the settings and then click **Finish**.

Prod - Add Port Mirroring Session

- ✓ 1 Select session type
- ✓ 2 Edit properties
- ✓ 3 Select sources
- ✓ 4 Select destinations
- 5 Ready to complete**

Ready to complete
Review the settings for the new port mirroring session before finishing the wizard.

Name	Session 0
Status	Enabled
Session type	Encapsulated Remote Mirroring (L3) Source
Encapsulation type	ERSPAN Type II
Session ID	0
Advanced properties	
Sampling rate	Mirror 1 of 1 packets
Number of source ports	84
Destination IP addresses	10.75.1.127
Description	--

CANCEL BACK FINISH

Tip: Consider turning off TCP segmentation offloading on the operating systems where the mirrored traffic is coming from.