# How Mirroring Works

Published: 2021-08-31

ExtraHop is a passive system.

Its wire data feed comes entirely from mirrored traffic. This is an improvement from traditional methods of collecting wire data with packet analyzers. With ExtraHop, the traffic is mirrored directly into the system and then reassembled into full per-client sessions and transaction streams, offering you the entire transaction payload in real time to analyze. There are two ways to mirror traffic into ExtraHop: network-based mirroring and host-based mirroring. This topic discusses the differences between the two.

## Network-based mirroring

The big advantage with network based mirroring is that you can set it up at the network level, capturing traffic from multiple hosts with a minimum amount of configuration. There are different types of network-based mirroring, each designed for mirroring traffic to a target in a particular situation. The big challenge with all the network-based mirroring strategies is that they rely heavily on the capabilities of the hardware on your network (physical or virtual). If you're running a virtual ExtraHop appliance, the hypervisor you're running (and even the version of hypervisor) also plays into the equation. That said, if you can take advantage of network-based mirroring you'll probably want to because after it's set up, it requires less administrative effort to maintain.

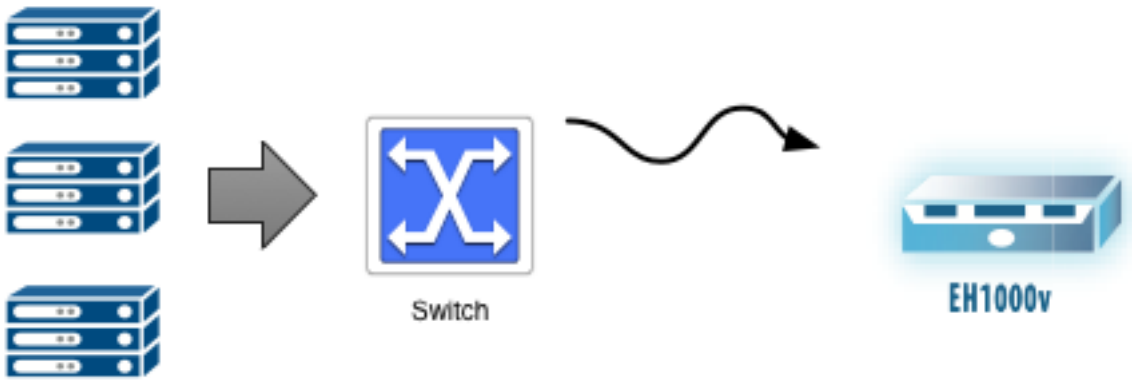
There are three main types of network-based mirroring.

**Note:** If you're using AWS, you don't have access to the network fabric, which means network-based mirroring is not available for you. Go to host-based mirroring section instead.

### SPAN

The SPAN port is the name of the port on Cisco switches that mirrors traffic. SPAN stands for Switched Port ANalyzer (SPAN). Different vendors have different names, but spanning has become synonymous for a port on a switch that mirrors traffic. The key thing about a SPAN is that it's all local traffic. You can configure any of the ports on the switch to mirror traffic to an ExtraHop system that has access to the SPAN port.

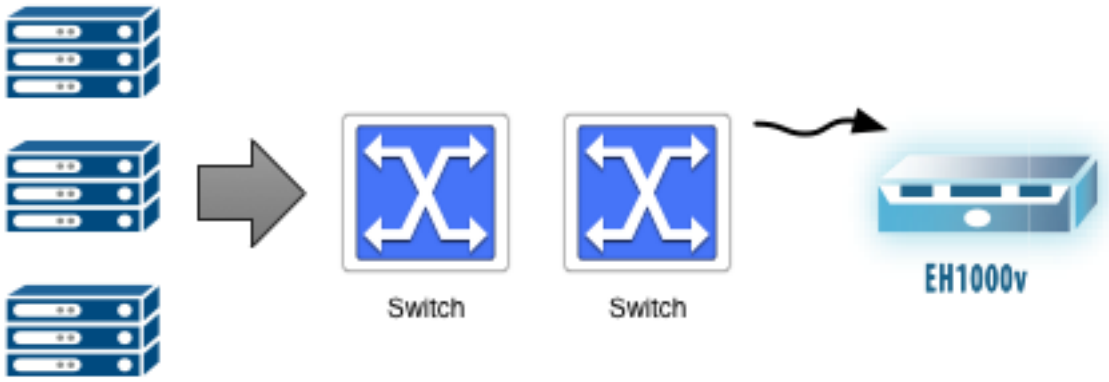
Promiscuous mode is similar to SPAN, but instead of mirroring only select local port traffic to the SPAN port, promiscuous mode mirrors all the traffic from every port. Any traffic that comes through the switch is mirrored to your ExtraHop system.




### RSPAN

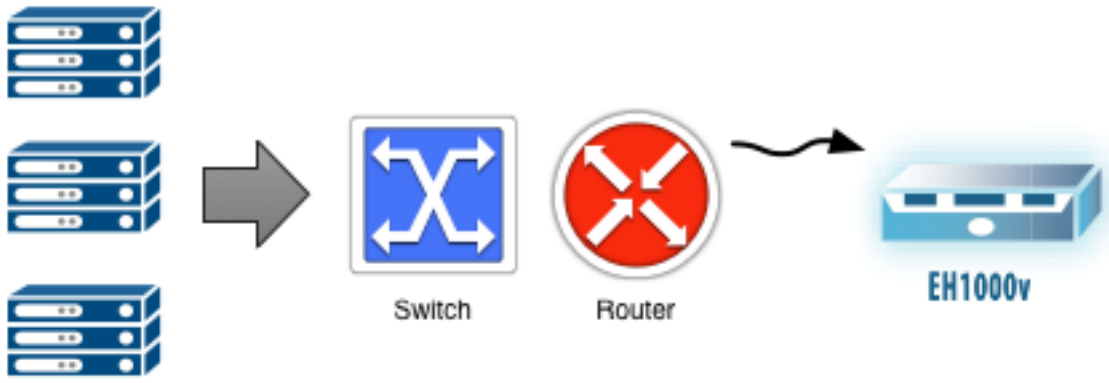
RSPAN is useful if the traffic you're interested in mirroring is more than one switch away from where you can attach your ExtraHop system. The "R" in RSPAN stands for remote. You're spanning all the traffic from

one switch through any number of additional switches to your target ExtraHop system using a dedicated mirroring VLAN. Each switch in the path needs to be configured to carry the dedicated VLAN that contains the mirror traffic.




### ERSPAN

If a Layer 3 (L3) boundary (such as a Router, Firewall, or Layer 3 Switch) sits between the traffic you want to mirror and where you can attach your ExtraHop system, ERSPAN might be helpful to you. To cross the Layer 3 boundary, ERSPAN encapsulates the mirror traffic in a GRE tunnel addressed to the IP address of a capture interface on the ExtraHop system. The encapsulated mirror traffic navigates the network just as any other packet would.



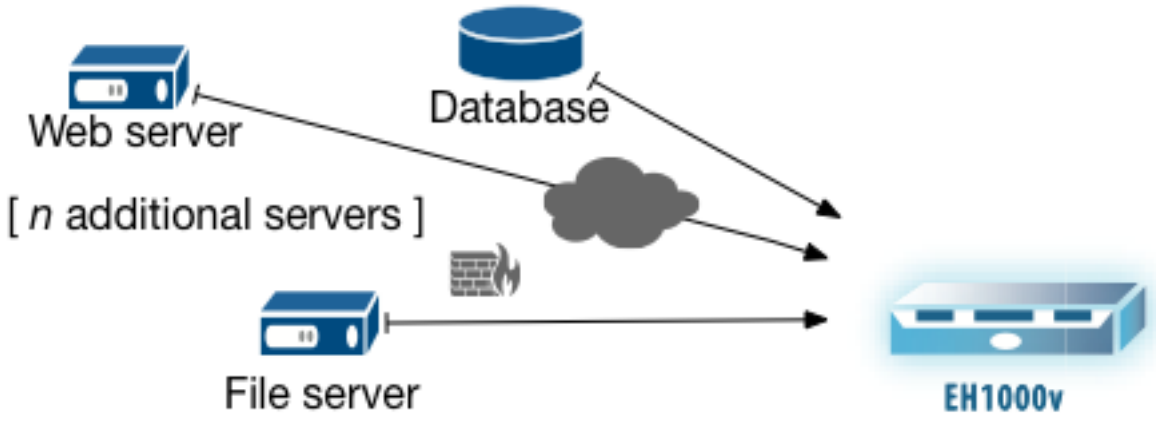

## Host-based mirroring

If network-based mirroring won't work for you, then host-based mirroring is a reliable way to get traffic into the ExtraHop system.

### Packet forwarder

Host-based mirroring requires that you install a packet forwarder on each host you want to monitor. The big advantage of the packet forwarder is that it works with any type of network gear you have. It works independent of the type or version of hypervisor you are running. Host-based mirroring is a way of configuring the adapter on a host to duplicate and forward all traffic to the ExtraHop system. You can install the packet forwarder software on Windows and Linux hosts.

The packet forwarder (also called RPCAP and a software tap) is analogous to a network tap, which is an unobtrusive hardware device for mirroring traffic from a network.


Web server
Database
[ n additional servers ]
File server
EH1000v