Monitoring considerations

Sensor introduction

The network sensor monitors the traffic on your network and transmits it to the cloud service for analysis.

You may download the sensor software and setup instructions from the web portal for your network.

This document will cover:

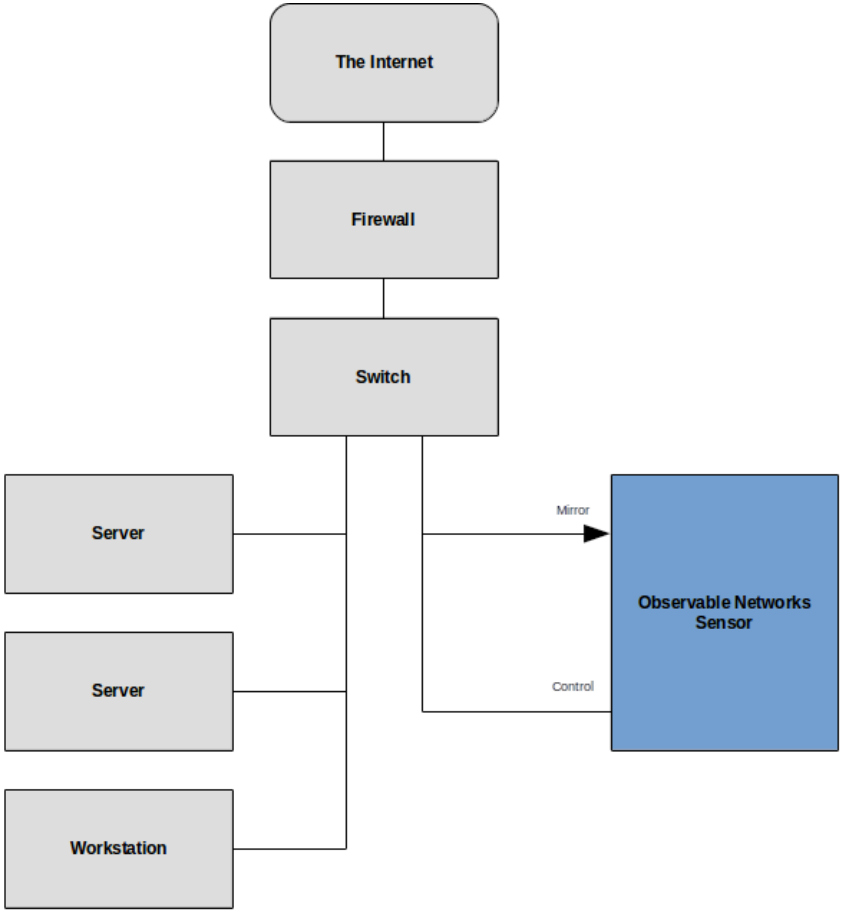
- Where to place the sensor
- How to configure your switch or router to send traffic to the sensor

Sensor network interfaces

A sensor needs to have at least two network interfaces. One “Control” interface, and at least one “Mirror” interface.

The Control interface connects to the Internet. See the sensor setup guide for how to configure the control interface.

The Mirror interface connects to a special port on a switch (or router) that replicates the data from other ports.



Mirror interface setup

Most managed switches can be configured to replicate traffic. Different switch vendors call this capability by different names.

- Cisco: Switch Port Analyzer (SPAN)
- Juniper, Netgear, ZyXEL: Port mirror
- Others: Monitor port, Analyzer port, Tap port

You may also use a passive tap device to replicate traffic. Common vendors include NetOptics and Gigamon.

Switch configuration

The user's guide for your particular switch model should have the correct configuration steps for setting up a mirror port.

For Cisco switches with IOS software, a typical configuration looks like:

```
monitor session 1 source interface Vlan10
monitor session 1 destination interface Gig1/0/3
```

See Cisco's documentation for other examples.

For Juniper switches, see Juniper's documentation. You may need to search for your particular switch model.

For Netgear switches, check Netgear's support page. The Software Administration Manual for your particular model should include a section on port mirroring.

For more examples, see the Wireshark Switch Reference page.

Mirror interface considerations

When setting up a mirror interface, keep in mind that it will be sending copies of all source traffic (both inbound and outbound) to the destination:

- Take note of how much traffic is expected at peak, and ensure that it is less than the capacity of the sensor's mirror interface link (e.g., 1 Gbps or 10 Gbps).
- Many switches will drop packets from the *source* interfaces if a mirror port destination is configured with too much traffic, which will cause problems on the LAN.
- You may use multiple mirror interfaces on a sensor; the sensor is not limited to a single control interface and a single mirror interface.

Virtualized environment mirroring

If your sensor is running as a virtual machine, you'll want to make both sure the virtual host and virtual network are configured properly.

For VMware:

- Promiscuous mode setup
- Information on promiscuous mode

You may need to set the VLAN ID to 4095.

For VirtualBox:

- In the Settings for your host, go to the Network tab and select the Adapter to be used for the Mirror interface.
- In the Advanced Options section, set Promiscuous mode to Allow.

Sensor placement

You may wish to place multiple sensors in your network to get a view of all traffic.

The diagram on the next page shows possible deployment locations.

Multiple-sensor deployments are usually only needed for larger networks. Use the “Contact Us” form on the web portal if you need help determining where to place your sensors.

Sensor placement examples