

Find all devices talking to external IP addresses

Published: 2019-02-10

The following steps show you how to find all of the external IP addresses that your internal devices are talking to. You can then see if any devices are making or receiving unauthorized connections from other devices outside of your network.



Tip: By default, any device with an RFC1918 IP address (included in a 10/8, 172.16/12, or 192.168/16 CIDR block) that the ExtraHop system automatically discovers is classified as an internal device. Because some network environments include non-RFC1918 IP addresses as part of their internal network, you can [specify the locality of an IP address](#) on the Network Localities page.

1. Log into the Web UI on the Discover or Command appliance.
2. Click **Metrics** at the top of the page.
3. Click **Activity Groups** in the left pane.
4. Click **TCP Devices**. At the top of the page, the External Accepted and External Connected metrics display how many IP addresses outside of your internal network are actively connected to all of your network devices.
5. Click the blue metric value for either metric.
6. In the Drill Down by... section, select **Group Member**. A detail metric page appears and shows all of the names of your network devices and the number of connections to external IP addresses.
7. Click on a device name that you want to investigate. A protocol page for that device appears, which contains metrics related to the device.

Next steps

- [Search for peer devices](#)
- [Monitor a device for external IP address connections](#)