Specify the locality for IP addresses

Published: 2019-01-07

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. You can then monitor internal network connections to devices outside of your network with ExtraHop metrics and detections. These metrics and detections can help you determine if unauthorized devices are attempting to access your internal network. However, because some network environments include non-RFC1918 IP addresses as part of their internal network, you can change the internal or external classification for IP addresses from the Network Localities page. For example, you can specify that a remote office CIDR block contains internal IP addresses.

Note: Detections require a connection to the cloud-based ExtraHop Machine Learning Service.

Here are some important considerations:

- You must have full-write privileges to change the locality of IP addresses.
- You must enter a unique range of IP addresses.
- If you have an ExtraHop Command appliance, you must configure these settings in the Command appliance and in all connected Discover appliances.

1. Log into the Web UI of the Discover or Command appliance.
2. Click the System Settings icon in the upper right corner of the page and click **Network Localities**.
3. Click **Add a CIDR Block**.
4. In the CIDR BLOCK field, type a single IP address or CIDR block.
5. Select **Internal** or **External**, based on which classification you want to apply to the CIDR block.
6. Optional: In the DESCRIPTION field, type information about why you are configuring the locality of this CIDR block.
7. At the top of the page, click **Save**.
8. To add more entries, click **Add CIDR**, select the locality, and then click **Save**.

Next steps

To verify that the ExtraHop system no longer classifies an IP address as an external or internal, look at external metrics by completing the following steps:

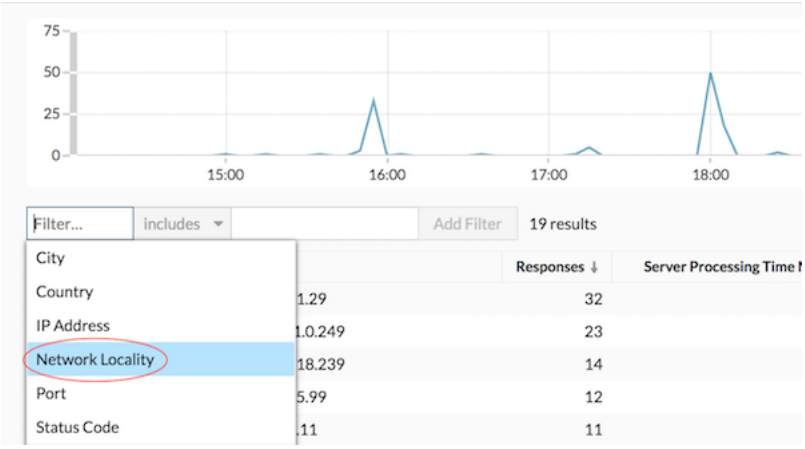
1. Click **Metrics** at the top of the page.
2. Scroll down the page and click the **TCP Devices** activity group. A protocol page appears that displays metrics for every device on your network with TCP activity.
3. In the TCP Connections section near the top of page, look for changes in the External Accepted and External Connected metrics. For example, if you classified a large CIDR block for a remote office as **Internal**, then the number of external connections should be lower.

Filter IP addresses by locality

You can choose whether to view only internal or external IP addresses in detail metric data.

1. Log into a Discover or Command appliance.
2. Drill down on a metric from a dashboard or protocol page by client, server, or IP address. A detail metric page appears that displays metric data listed by IP address.
3. Click **Any Field** and then click **Network Locality**, as shown in the following figure.

© 2019 ExtraHop Networks, Inc. All rights reserved.



4. Click **All Locations** and then click **Internal** or **External**.
5. Click **Add Filter**.

Detail metric data for internal or external devices is displayed. To remove the filter, click the **x** icon as shown in the following figure.