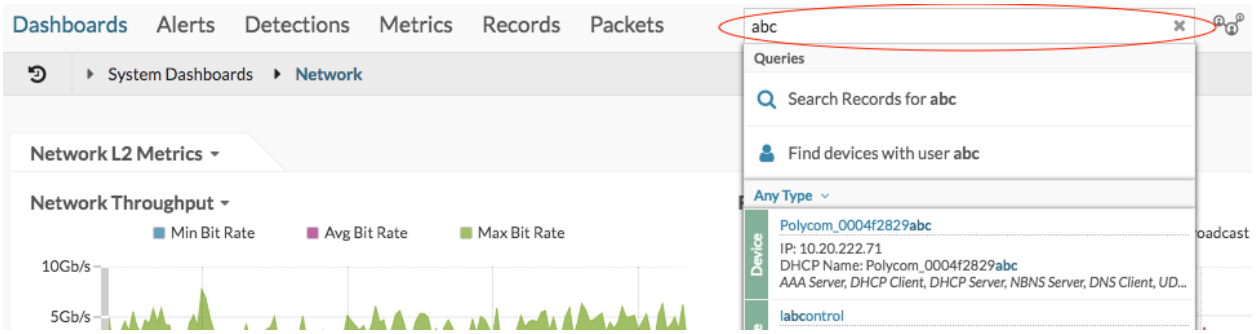
Find a device

Published: 2020-02-23

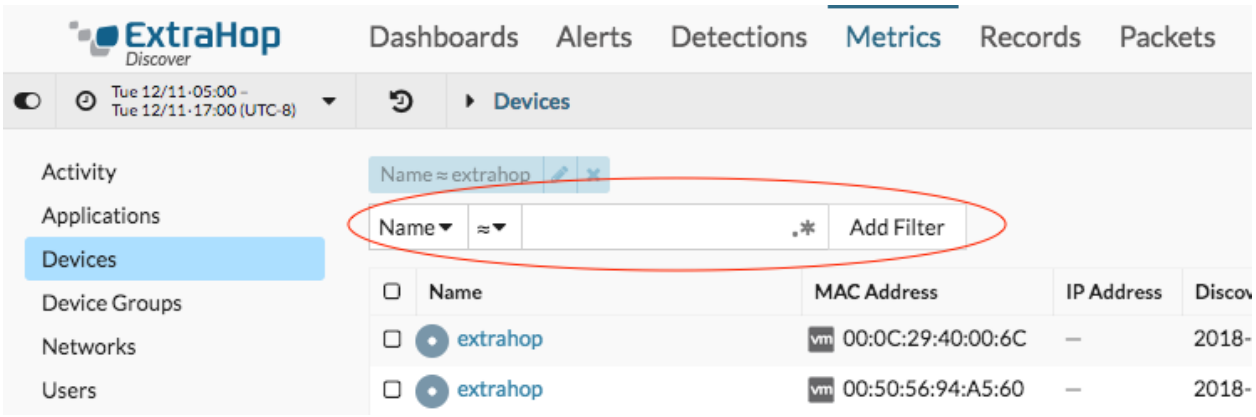
The ExtraHop system automatically discovers devices such as clients, servers, routers, load balancers, and gateways that are actively communicating with other devices over the wire. If you want to see network activity associated with a specific device, you can search for your device in the Discover or Command appliance, and then view traffic and protocol metrics on a protocol page.

There are several ways to search for a device:

- Perform a general search from the global search field at the top of the page and select the device you want from the results list.



- Perform a detailed search from the device list page in the Metrics section of the ExtraHop Web UI, where you can filter search results by device attributes.



- Perform a search by protocol activity from an activity group.
- Perform a search for peer devices talking to a device.

Search for a device by details

You can search for devices by information observed over the wire, such as IP address, MAC address, hostname, or protocol activity. You can also search for devices by customized information such as device tags.

The trifield filter enables you to search by multiple categories at once. For example, you can add filters for device name, IP address, and role to view results for devices that match all of the specified criteria.

1. Log into the Web UI on the Discover or Command appliance and then click **Metrics** at the top of the page.
2. Click **Devices** in the left pane.

3. Click **Name** and select one of the following categories:

Option	Description
Name	Filters devices by the discovered device name. For example, a discovered device name can include the IP address or hostname.
IP Address	Filters devices by the device IP address in IPv4, IPv6, or CIDR block.
MAC Address	Filters devices by the device MAC address.
Vendor	Filters devices by the device vendor name, as determined by the Organizationally Unique Identifier (OUI) lookup.
VLAN	Filters devices by the device VLAN tag. VLAN information is extracted from VLAN tags, if the traffic mirroring process preserves them on the mirror port. Only available if the devices_accross_vlans setting is set to False in the Running Config file.
Tag	Filters devices by user-defined device tags.
Role	Filters devices by the assigned device role, such as gateway, firewall, load balancer, and DNS Server.
Activity	Filters devices by protocol activity associated with the device. For example, selecting HTTP Server returns devices with HTTP server metrics, and any other device with a device role set to HTTP Server.
Discovery Time	Filters devices that were automatically discovered by the ExtraHop system within the specified time interval. For more information, see Create a device group based on discovery time.
Software	Filters devices by operating system software detected on the device.
DNS Name	Filters devices by the DNS name assigned to the device.
DHCP Name	Filters devices by the DHCP name assigned to the device.
NetBIOS Name	Filters devices by the NetBIOS name assigned to the device.
CDP Name	Filters devices by the CDP name assigned to the device.
Custom Name	Filters devices by the custom name assigned to the device.
Appliance	Filters by devices associated with a connected Discover appliance name. Only available from a Command appliance.

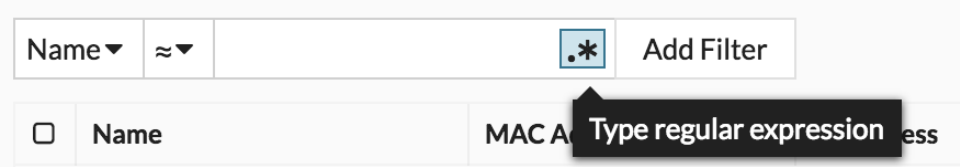
4. Select one of the following operators; the operators available are determined by the selected category:

Option	Description
=	Filters devices that are an exact match of the search field for the selected category.
≠	Filters devices that do not exactly match the search field.
≈	Filters devices that include the value of the search field for the selected category.
≈/	Filters devices that exclude the value of the search field for the selected category.
starts with	Filters devices that start with the value of the search field for the selected category.
exists	Filters devices that have a value for the selected category.
does not exist	Filters devices that do not have a value for the selected category.

5. In the search field, type the string to be matched, or select a value from the drop-down list. The input type is based on the selected category.

   For example, if you want to find devices based on Name, type the string to be matched in the search field. If you want to find devices based on Role, select from the drop-down list of roles.

   Tip: Depending on the selected category, you can click the Regex icon in the text field to enable matching by regular expression.



6. Click **Add Filter**.

Next steps

- Click the name of a device to view information on the Overview page for the device.
- Select any protocol from the left pane to view additional metrics.
- Click **Create Dynamic Group** from the upper right corner to create a group based on the filter criteria.
- Click the command menu and then select PDF or CSV to export the device list to a file.
- Change a device name
- Change a device role
- Add a tag to a device

Search for devices by protocol activity

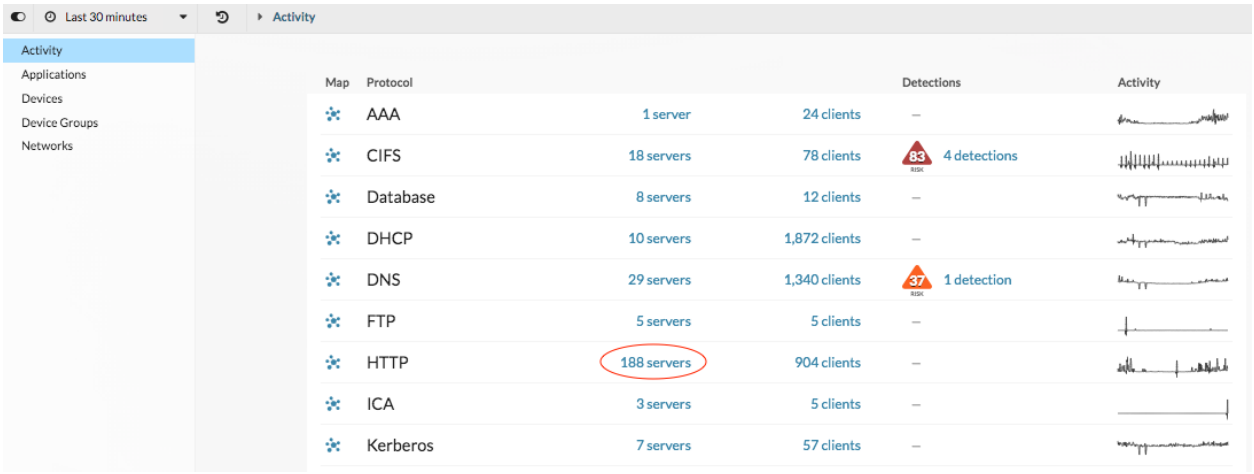
The Activity page displays all protocols that are actively communicating over the wire during the selected time interval. You can quickly locate a device that is associated with a protocol, or discover a decommissioned device that is still actively communicating over a protocol.

In the following example, we show you how to search for a web server within the group of HTTP servers.

1. Log into the Web UI on the Discover or Command appliance and click **Metrics** at the top of the page. The Activity page appears, which lists all the protocols with traffic in the selected time interval.

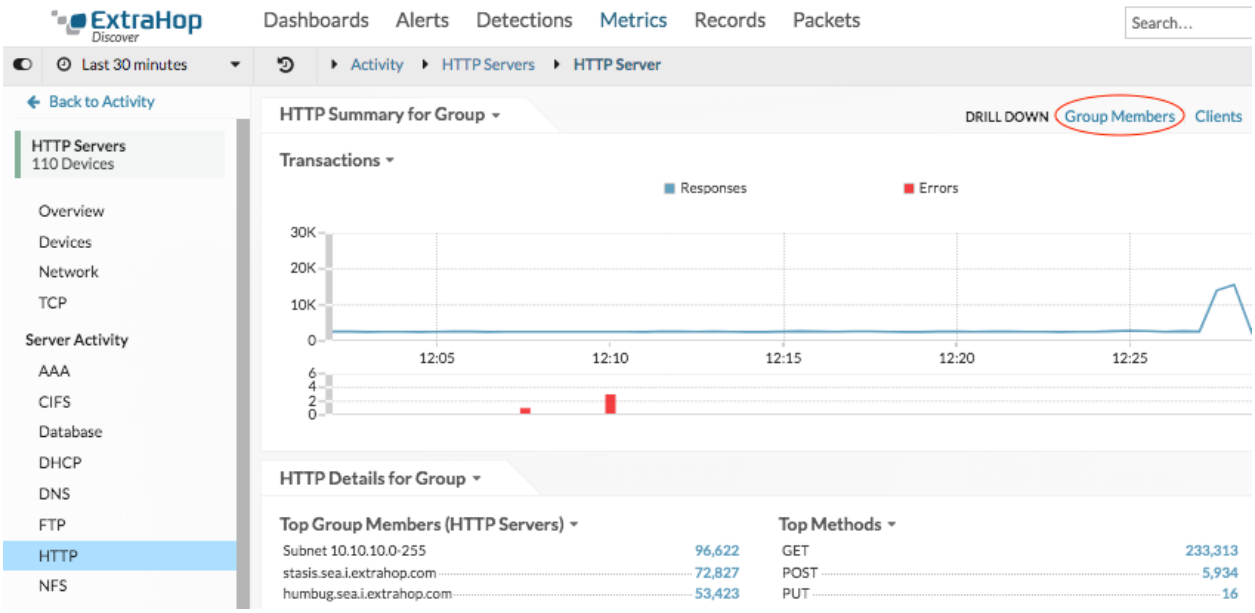
If you do not see the protocol you want, the ExtraHop system might not have observed that type of protocol traffic over the wire yet, or the protocol might require a module license. For more information, see the I don't see the protocol traffic I was expecting? section in the License FAQ.

2. Click the number of HTTP servers, as shown in the following figure.



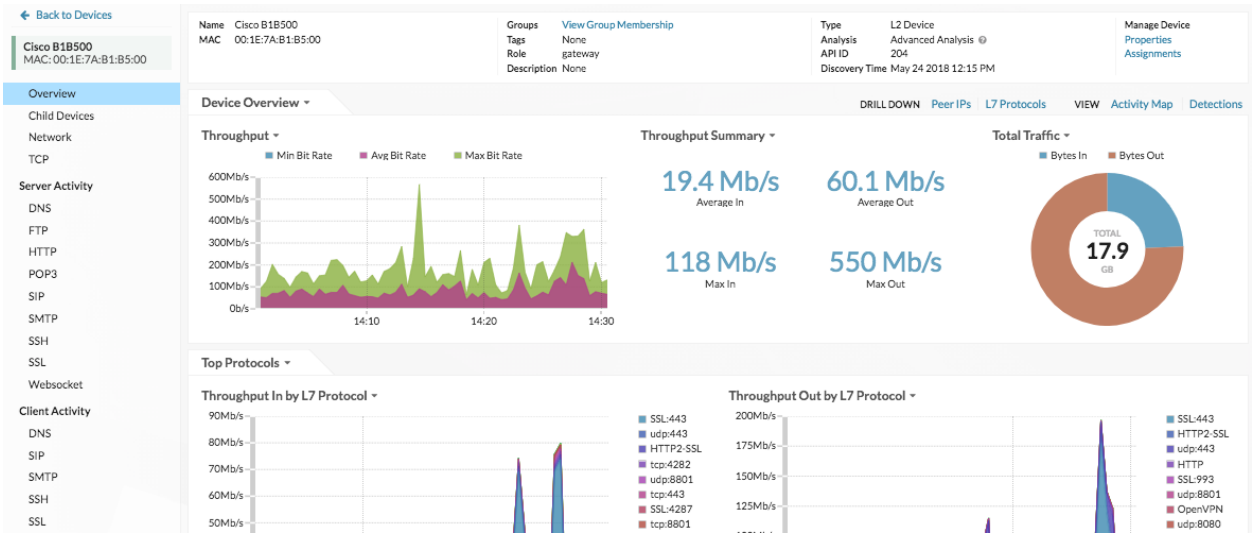
The page displays traffic and protocol metrics associated with the group of HTTP servers.

3. In the top of the page, click **Group Members**, as shown in the following figure.



The page displays all of the devices that sent HTTP responses over the wire during the selected time interval.

4. Click a device name in the table.
The page displays traffic and protocol metrics associated with that device, similar to the following image.



Next steps

- Investigate additional metrics by selecting another protocol in the Server Activity or Client Activity sections in the left pane.
- Change a device name.

Search for devices accessed by a specific user

From the Users page, you can see active users and the devices they have logged into during the specified time interval.

Tip: Search for users from the global search field at the top of the page.

This procedure shows you how to perform a search from the Users page.

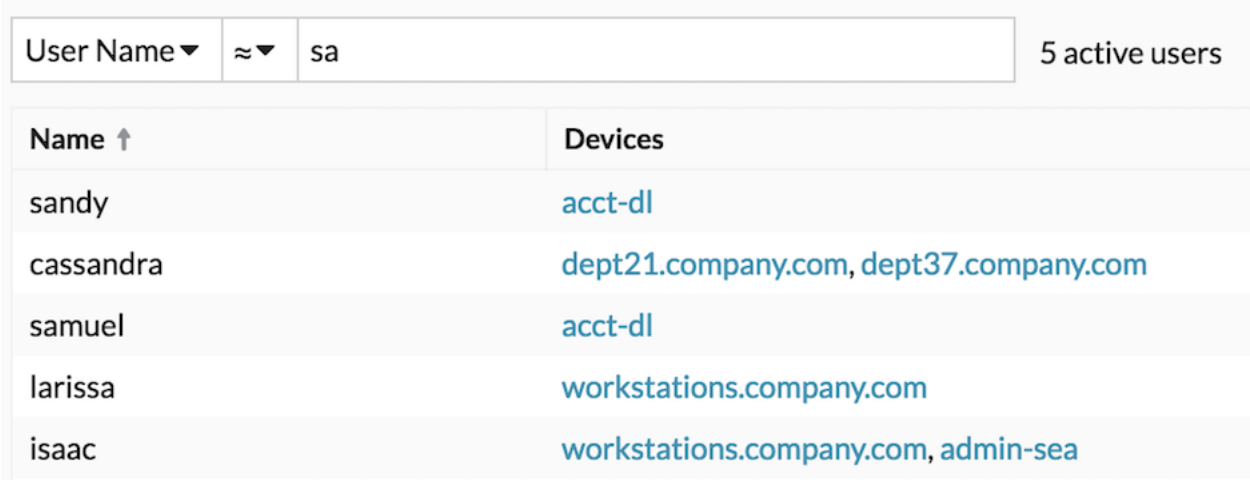
1. Log into the Web UI on the Discover or Command appliance and then click Metrics at the top of the page.
2. Click Users in the left pane.
3. From the search bar, select one of the following categories from the drop-down list:

Option	Description
User Name	Search by user name to learn which devices the user has accessed.
Device Name	Search by device name to learn which users have accessed the device. The user name is extracted from the authentication protocol, such as LDAP or Active Directory.

4. Select one of the following operators from the drop-down list:

Option	Description
=	Search for a name or device that is an exact match of the text field.
≠	Search for names or devices that do not exactly match the text field.
≈ (default)	Search for a name or device that includes the value of the text field.
≈/	Search for a name or device that excludes the value of the text field.

5. In the text field, type the name of the user or device you want to match or exclude.
The Users page displays a list of results similar to the following figure:



Next steps
Click the name of a device to open the Overview page for that device and view all of the users that have accessed the device during the specified time interval.

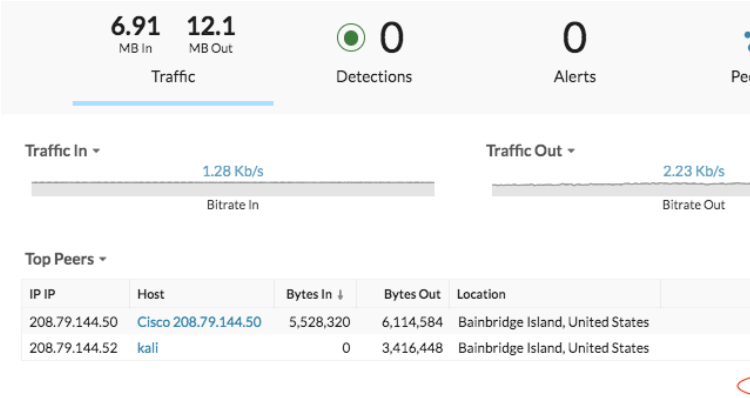
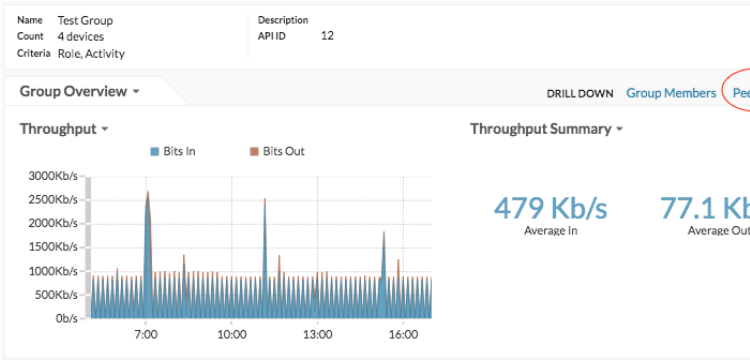
Search for peer devices

If you want to know which devices are actively talking to each other, you can drill down by Peer IPs from a device or device group protocol page.

When you drill down by Peer IP address, you can investigate a list of peer devices, view performance or throughput metrics associated with peer devices, and then click on a peer device name to view additional protocol metrics.

1. Log into the Web UI on the Discover or Command appliance.
2. Click **Metrics** and then select **Device** or **Device Group** in the left pane.
3. Search for a device or device group, and then click the name from the list of results.
The Overview page for that selected device or device group appears.
4. Click one of the following links:

Option	Description
For devices	Click **View More Peer IPs**, located at the bottom of the Top Peers chart.

Option	Description
	
For device groups	Click **Peer IPs**, located in the Details section near the upper right corner of the page.
	

A list of peer devices appears, which are broken down by IP address. You can investigate network bytes and packets information for each peer device, as shown in the following

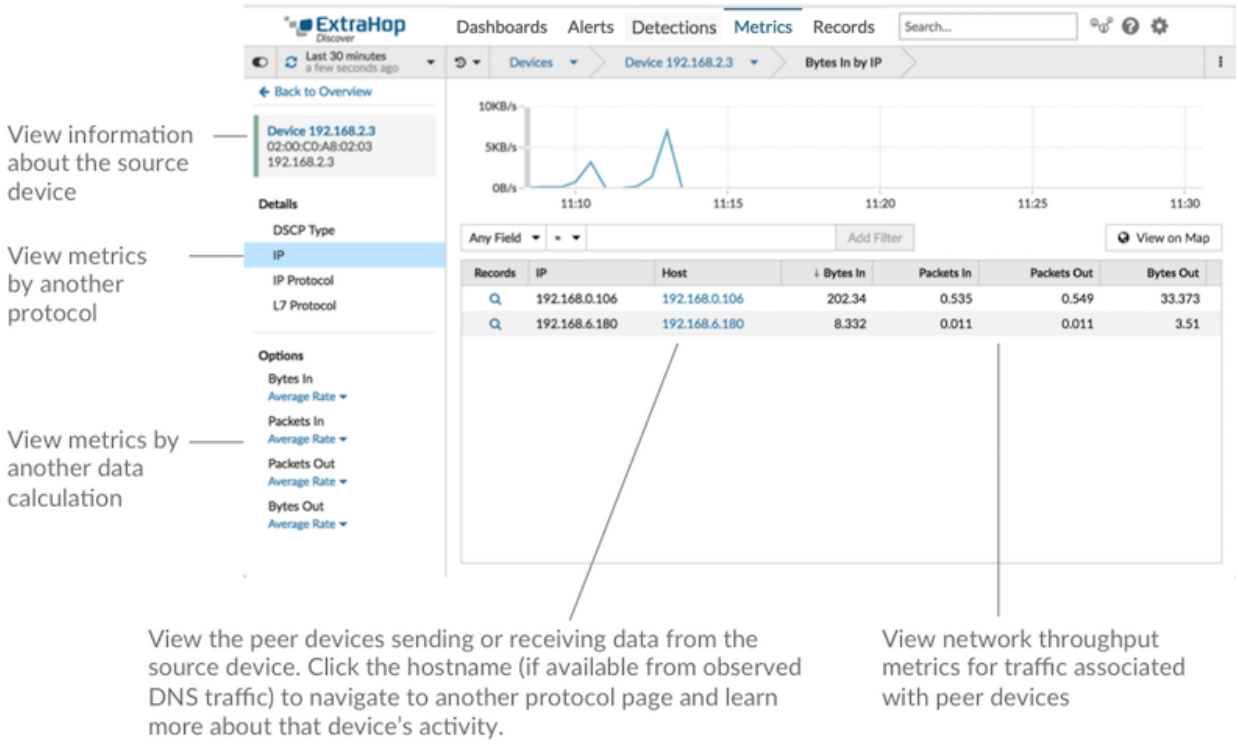


figure.

Next steps

- Add a tag to a device