Using ASA FirePOWER Reporting

You can view reports on various time periods to analyze the traffic on your network. Reports aggregate information on various aspects of your network traffic. In most cases, you can drill down from general information to specific information. For example, you can view a report on all users, then view details about specific users.

Overview and detail reports include multiple report components such as top policies and web categories. These reports show the most often occurring items of that type for the report you are viewing. For example, if you are viewing the detail report for a specific user, the top policies show the policy hits most associated with that user.

Understanding Available Reports

License: Any

Available reports include the main reports available in the ASA FirePOWER module. You can view these reports from the ASA FirePOWER Reporting menu.

In general, you can click on many items, including names and View More links, to get more detailed information about individual items or about the monitored category as a whole.

Network Overview

This report shows summary information about the traffic in the network. Use this information to help identify areas that need deeper analysis, or to verify that the network is behaving within general expectations.

Users

This report shows the top users of your network. Users who fail active authentication are represented in user reports under the username ANONYMOUS, unless you enabled guest access, in which case the username is Guest. Users who do not have a mapping because they were not required to authenticate are shown as their IP address. Use this information to help identify anomalous activity for a user.

Tip User names are available only when user identity information is associated with traffic flows. If you want to ensure that user identity is available in reports for the majority of traffic, the access control policy should use active authentication.

Applications

This report displays applications, which represent the content or requested URL for HTTP traffic detected in the traffic that triggered an intrusion event. Note that if the module detects an application protocol of HTTP, but cannot detect a specific web application, the module supplies a generic web browsing designation here.

Web categories

This report shows which categories of web sites, such as gambling, advertisements, or search engines and portals are being used in the network based on the categorization of web sites visited. Use this information to help identify the top categories visited by users and to determine whether your access control policies are sufficiently blocking undesired categories.

Policies

This report shows how your access control policies have been applied to traffic in the network. If you deleted the policy, the name is appended with "- DELETED." Use this information to help evaluate policy efficacy.

Ingress zones

This report displays the ingress security zone of the packet that triggered an event. Only this security zone field is populated in a passive deployment.

Egress zones

This report displays, for an inline deployment, the egress security zone of the packet that triggered the event. This security zone field is not populated in a passive deployment.

Destinations

This report shows which applications, such as Facebook, are being used in the network based on the analysis of the traffic in the network. Use this information to help identify the top applications used in the network and to determine whether additional access control policies are needed to reduce the usage of unwanted applications.

Attackers

This report displays the source IP addresses, used by the sending hosts, that triggered an event.

Targets

This report displays the destination IP addresses, used by the receiving hosts, that triggered an event.

Threats

This report displays the unique identifying number and explanatory text assigned to each detected threat to your network.

Files logs

This report displays the type of files detected, for example, HTML or MSEXE.

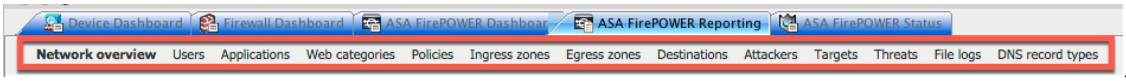
Report Basics

License: Any

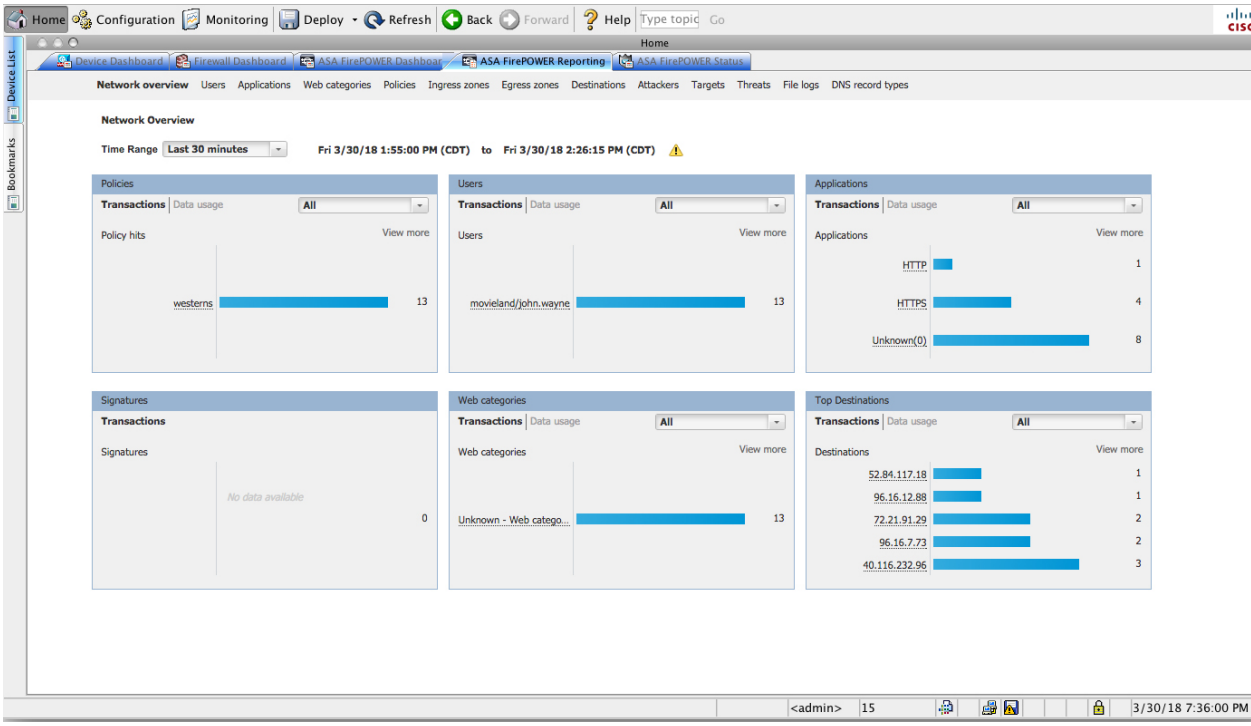
The following sections explain the basics of using reports. These topics apply to reports in general and not to any single specific report.

Getting Started with Reports

To run reports, log in to your ASA FirePOWER module and click **Home** > **ASA FirePOWER Reporting**. Available report types are displayed across the top of the window as the following figure shows



Following is an example of the Network Overview report. Click any underlined text to get more information about it



Understanding Report Data

License: Any

Report data is collected immediately from the device, so there is little lag time between the data reflected in a report and network activity. However, keep the following points in mind when analyzing the data:

- Data is collected for traffic that matches an access control policy applied to your ASA FirePOWER module.
- Data is aggregated into 5 minute buckets, and 30 minute and one hour graphs show data points in 5 minute increments. At the end of the hour, the 5 minute buckets are aggregated into one hour buckets, which are subsequently aggregated into day and week buckets. The 5 minute buckets are kept for 7 days, the one hour buckets for 31 days, and the day buckets for up to 365 days. The farther back you look, the more aggregated the data. When you query for old data, you get the best results if you align your queries to the availability of these data buckets. All day calculations are based on UTC time; the time on the server or your client is ignored.

Note If a data point is missing, for example, because the device was unreachable for longer than 5 minutes, there will be gaps in line charts.

Drilling into Reports

License: Any

Reports include many links to help you drill down to the information that you need. Mouse over items to see which ones might take you to more information about the item.

For example, in a typical reporting item, you can click the View More link to go to the summary report for that item.

You can also get to a detail report on a specific item by clicking the item in a summary report. For example, clicking Hypertext Transfer Protocol (HTTP) in the applications summary report takes you to the applications detail report for HTTP.

Changing the Report Time Range

License: Any

When you view a report, you can change the time range that defines the information to include in the report using the Time Range list. The time range list appears at the top of each report, and allows you to select predefined time ranges, such as the last hour or week, or to define a custom time range with specific start and end times. The time range you select is carried over to any other report that you view until you change the selection.

Reports automatically update every 10 minutes.

Tip The module bases time on the time zone defined on the device, not the zone configured on your workstation.

Table 1: Time Ranges for reports

Time Range	Data Returned In
Last 30 minutes	30 complete minutes in five minute intervals, plus up to five additional minutes.

Time Range	Data Returned In
Last hour	60 complete minutes in five minute intervals, plus up to five additional minutes.
Last 24 hours	One hour intervals for the last 24 hours rounded to the previous hour boundary. For example, if the current time is 13:45, the Last 24 Hour period is from 13:00 yesterday to 13:00 today.
Last 7 days	One hour intervals for the last seven days rounded to the previous hour boundary.
Last 30 days	One day intervals for the last 30 days starting from the previous midnight.
Custom Range	The time range you define. Edit boxes are displayed for start date, start time, end date, and end time; click in each box and select the desired value. Click **Apply** to update the report when you are finished. When constructing a custom time range, you should align your range with the availability of data buckets. For ranges 7-31 days in the past, align your query on the hour. For older ranges, align them on the day; for ranges over a year, align them on the week.In all cases, use UTC time to determine the day boundaries; the time zone of the query, server, and client do not relate to the data bucket. For example, if the time zone is Pacific Daylight Time (PDT), and you are querying data from 40 days ago, use 4PM on day 1 and 4PM on day 2 to align with UTC (8 hour offset to PDT).

Controlling the Data Displayed in Reports

License: Any

Overview and detail reports include several subordinate reports such as Top Policies and Web Categories. Each report panel includes controls that let you view different aspects of the data. You can use the following controls:

Transactions or Data Usage

Click these links to view charts based on the number of transactions or the amount of data in the transactions.

All, Denied, Allowed

The unlabeled list in the upper right of each report includes these options. Use them to change whether you see denied connections only, allowed connections only, or all connections whether denied or allowed.

View More

Click the View More link to go to the report for the item you are viewing. For example, clicking View More in the Web Categories chart of the Destinations report takes you to the Web Categories report. If you are viewing the report in a detailed report, you go to the detailed Web Categories report for the item you are viewing details about.

Understanding Report Columns

License: Any

Reports typically contain one or more tables to present information in addition to the information displayed in graphical format.

- The meaning of many columns is modified by the report in which they are included. For example, the transactions column shows the number of transactions for the type of item reported on. You can also toggle the values between raw numbers and as a percentage of the total reported raw values for the item by clicking **Values** or **Percentages**.
- You can change the sort order of the columns by clicking the column heading.

The following table explains the standard columns that you can find in the various reports. The standard columns are in all reports, the variable columns appear in the reports for those items only.

Table 2: Report Columns

Column	Description
Transactions	The total number of transactions for the reported item. In top-level reports, the number is a link; click it to open the Event Viewer with the events table filtered based on the item you are viewing.The number of events shown can differ from the transaction count, especially for queries of older time periods, because events are removed from storage as disk space is depleted and new events arrive. Queries of time periods over 30 days ago might return no matching events. Conversely, you might see more events than transactions, if the item was not one of the top N in each 5 minute bucket covered by the time range, because transaction counts do not include these periods.
Transactions allowed	The number of transactions that were allowed for the reported item.
Transactions denied	The number of transactions that were blocked (based on policy) for the reported item.
Total bytes	The sum of bytes sent and received for the reported item.
Bytes received	The number of bytes received for the reported item.
Total Bytes Sent	The number of bytes sent for the reported item.

Example Report

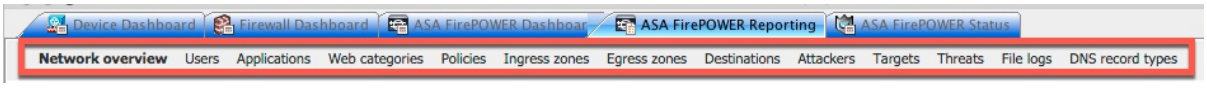
This section discusses how to run the Policies report. You can use the tasks discussed in this procedure to run any other reports you wish.

To run reports:

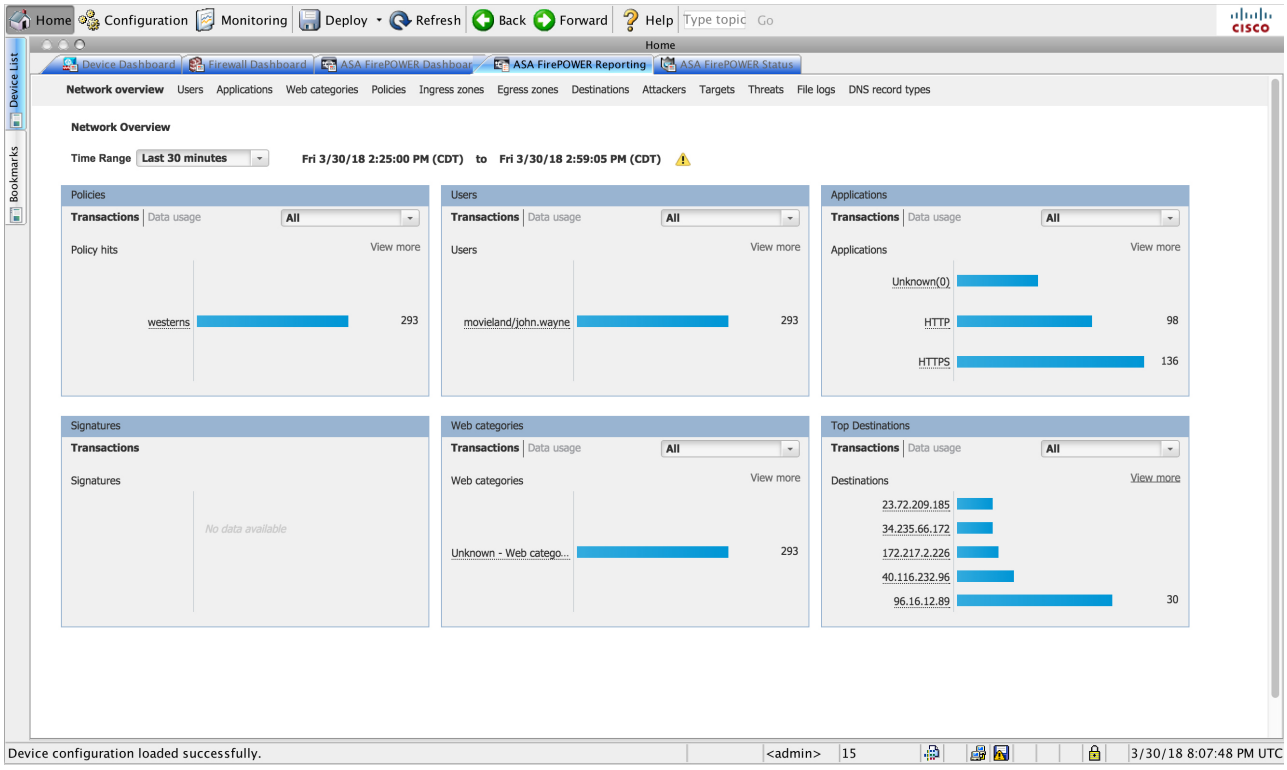
Step 1 Log in to your ASA FirePOWER module.

Step 2 Click **Home** > **ASA FirePOWER Reporting**.

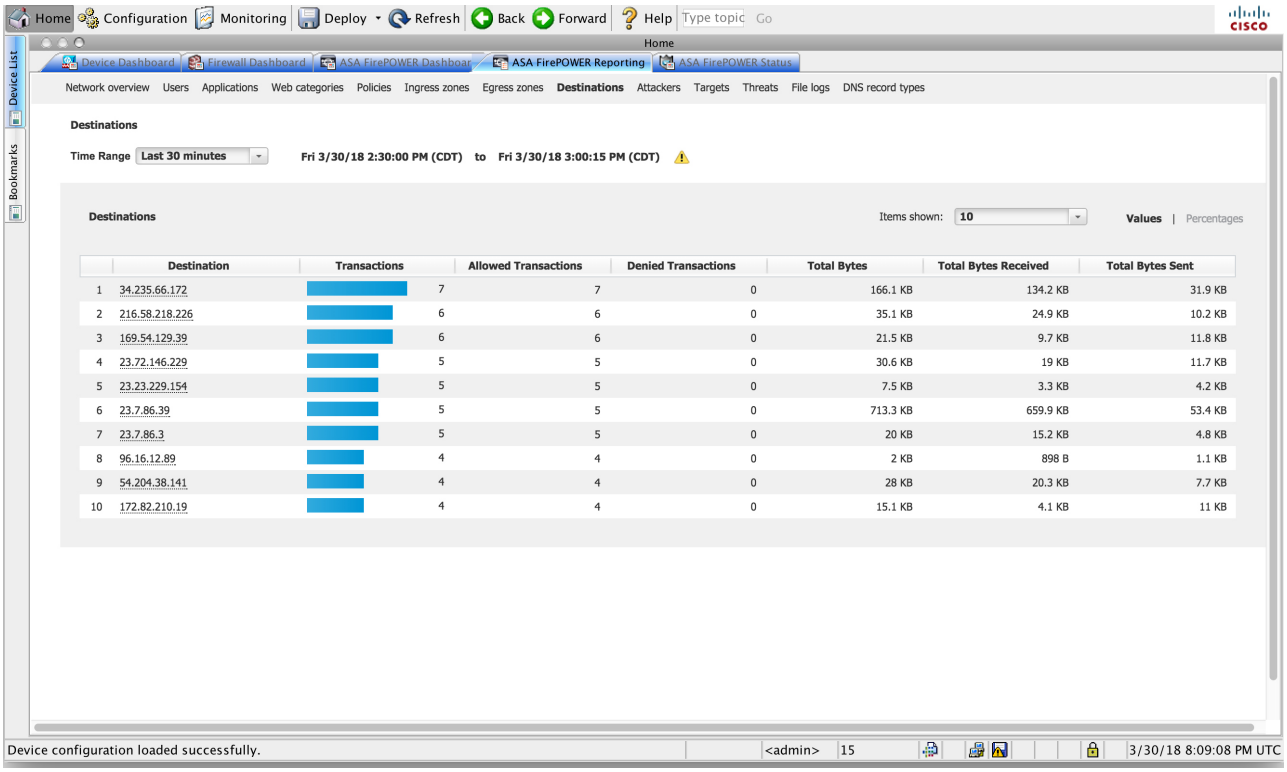
Available report types are displayed across the top of the window as the following figure shows.



Step 3 Many reports enable you to view details about categories contained in the report. For example, click **Network**



Step 4 In the Network Overview report results, click the name of any Top Destinations to get more information about destinations.



The results display summary information and details about the destinations.

(Optional.) Click **View More** to view additional details.