Reporting

https://campus.barracuda.com/doc/41107441/

The **BASIC > Reports** page allows you to configure and generate reports of various types, based on all logged information. You can either generate a one-time report or configure the Barracuda Web Application Firewall to automatically generate the reports on an hourly, daily, weekly, or monthly basis. Reports can be emailed to specific email addresses or sent to an FTP server.

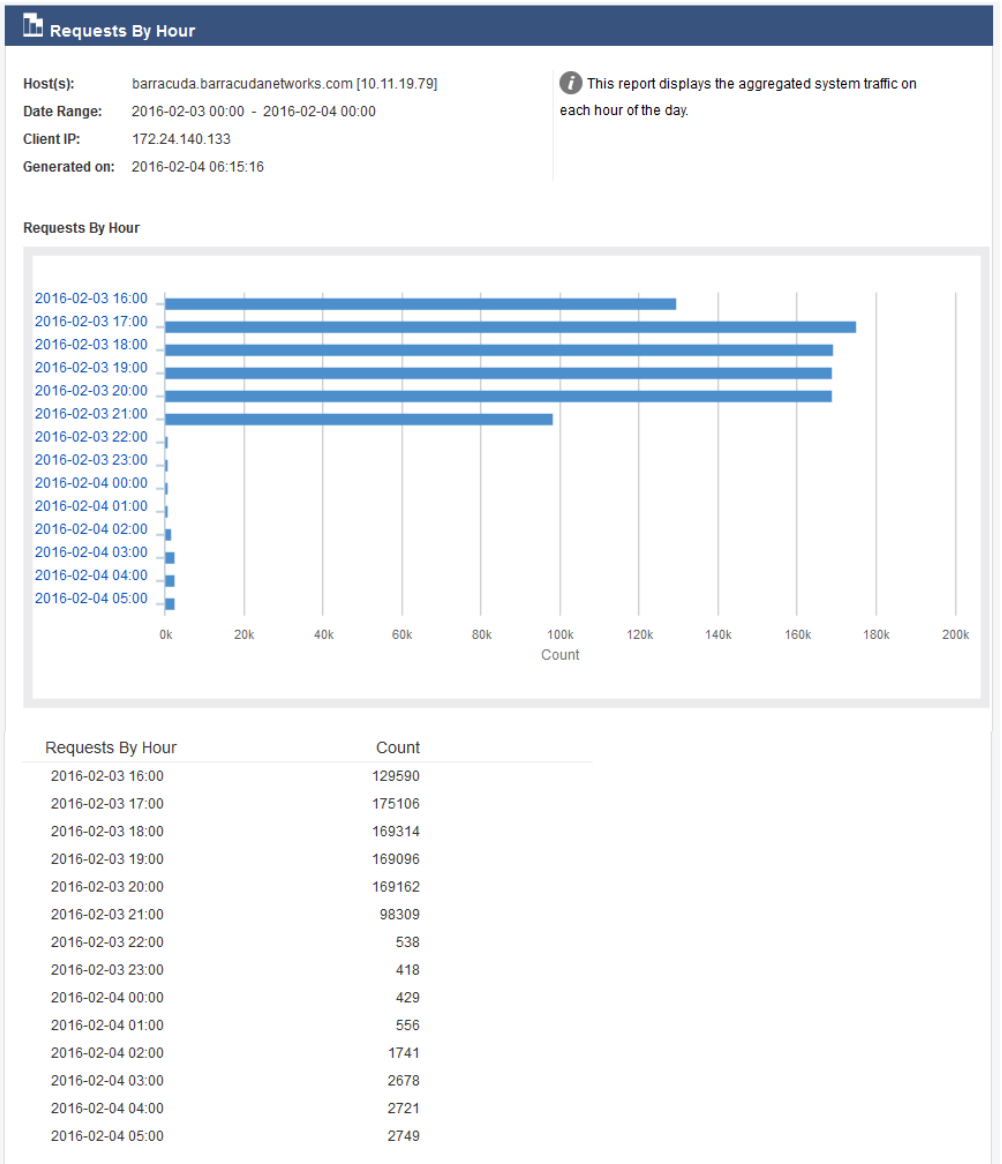
The Barracuda Web Application Firewall reports are broadly classified into following groups:

- Security Reports
- Summary Reports
- PCI DSS Reports
- Administration/Audit Reports
- Configuration Summary Reports
- Traffic Reports
  - Aggregated System Traffic Reports
  - Client Traffic Reports
  - Service Traffic Reports
  - Server Traffic Reports

Filtering a Report

You can apply a filter to the “Security” and “Traffic” reports and limit a report to specific data. For example, the **Requests By Hour** report under “Traffic” displays the number of requests received each hour in last 24 hours. To view the number of requests received from a particular client IP address, specify the client IP address in the filter and view the report. To apply a filter for the example above, perform the following steps:

1. Go to the **BASIC > Reports** page.
2. In the **Report Options** section, click **Show Advanced Options**.
3. Select **Client IP** from the **Traffic Filter** drop-down list and enter the IP address of the client.
4. Scroll down to the **Traffic** section and click **Show Report** next to **Request By Hour**.



Requests By Hour	Count
2016-02-03 16:00	129590
2016-02-03 17:00	175106
2016-02-03 18:00	169314
2016-02-03 19:00	169096
2016-02-03 20:00	169162
2016-02-03 21:00	98309
2016-02-03 22:00	538
2016-02-03 23:00	418
2016-02-04 00:00	429
2016-02-04 01:00	556
2016-02-04 02:00	1741
2016-02-04 03:00	2678
2016-02-04 04:00	2721
2016-02-04 05:00	2749

Drilling Down a Report

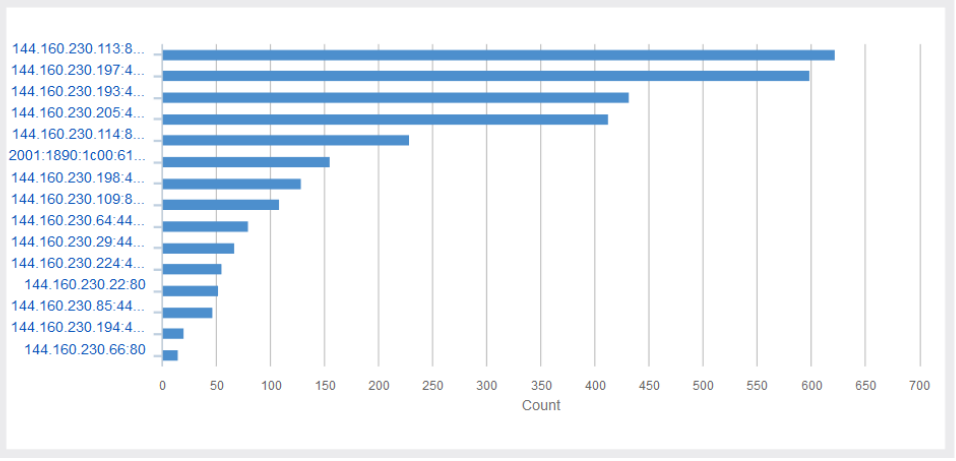
You can drill down some of the reports under “Security” and “Traffic” to view data in more detail. For example, the **Attacks By Services** report displays the number of attacks on the services. Click the drill down link in the data to view different categories of attacks on the services.

Attacks By Service

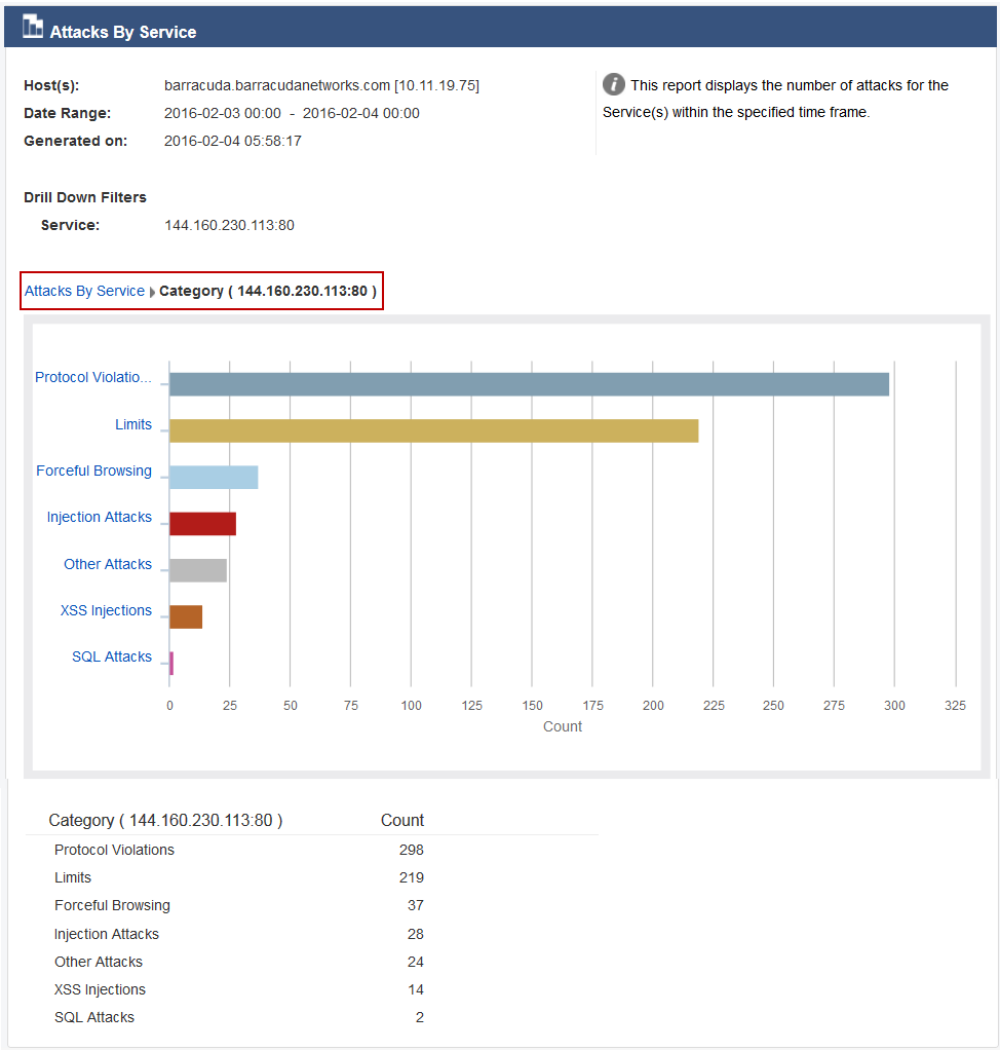
Host(s): barracuda.barracudanetworks.com [10.11.19.75]
Date Range: 2016-02-03 00:00 - 2016-02-04 00:00
Generated on: 2016-02-04 05:58:17

This report displays the number of attacks for the Service(s) within the specified time frame.

Attacks By Service



Attacks By Service	Count	Drilldown
144.160.230.113:80	622	Domain Time Category Client
144.160.230.197:443	599	Domain Time Category Client
144.160.230.193:443	432	Domain Time Category Client
144.160.230.205:443	413	Domain Time Category Client
144.160.230.114:80	229	Domain Time Category Client
2001:1890:1c00:6110::f:1001:80	155	Domain Time Category Client
144.160.230.198:443	129	Domain Time Category Client
144.160.230.109:8080	109	Domain Time Category Client
144.160.230.64:443	80	Domain Time Category Client
144.160.230.29:443	67	Domain Time Category Client
144.160.230.224:443	55	Domain Time Category Client
144.160.230.22:80	52	Domain Time Category Client
144.160.230.85:443	47	Domain Time Category Client
144.160.230.194:443	20	Domain Time Category Client
144.160.230.66:80	15	Domain Time Category Client



Schedule a Report

1. Go to the **BASIC > Reports** page.
2. (Optional) In the **Report Options** section, click **Show Advanced Options** and configure filters for **Security** and **Traffic** reports.
3. Select the check box(es) next to the report type(s) under the report group (**Security**, **Traffic**, **Audit and System**, **Config Summary** and **PCI Reports**).
4. In the **Schedule Report** section, enter a name for the report, select how you want the report to be delivered (Email or FTP), and how frequently you want the report to be generated automatically.

   As a best practice, use a unique account for this integration point and grant it the least level of privileges required, coordinating with the administrator. This account requires read privileges on the Reporting server *only for the specific path you indicate* in the next field. For additional information, see Security for Integrating with Other Systems - Best Practices .

5. Click **Apply**.

In this Section:

Figures

1. Request By Hour - Client IP.png
2. Attacks By Service.png
3. Attacks By Service - Category.png