Reporting With the Barracuda Web Security Gateway Version 11 and Above

https://campus.barracuda.com/doc/51189335/

This article addresses the built-in reporting feature of the Barracuda Web Security Gateway, configurable on the **BASIC > Reports** page. Note that the Barracuda Web Security Gateway stores approximately 6 months worth of reporting data, and this may vary with the amount of internet traffic.

If you are running the Barracuda Web Security Gateway version 11.0 and higher, you may also purchase and connect a Barracuda Reporting Server. The Barracuda Reporting Server generates more accurate, customizable reports that offloads processing from the Barracuda Web Security Gateway, resulting in performance gains in filtering capacity. You can also connect multiple Barracuda Web Security Gateways to have an aggregate view of reporting data on the Barracuda Reporting Server.

See the Barracuda Reporting Server for more information about the product. If you have purchased a Barracuda Reporting Server and are ready to connect it to the Barracuda Web Security Gateway, see Reporting with the Barracuda Reporting Server.

For reporting purposes, Barracuda recommends a maximum Active Directory (AD) group size of 1000 users.

Use the **BASIC > Reports** page to choose from more than 80 different system reports that can help you keep track of activity performed by the Barracuda Web Security Gateway. You can either generate a system report on-demand or configure the Barracuda Web Security Gateway to automatically generate the system reports on an hourly, daily, weekly, or monthly basis and email the reports to specific email addresses or send them to an FTP or SMB server.

Some reports may contain URLs that are on block lists. If your Barracuda Web Security Gateway is sending reports via email through an email security product, such as the Barracuda Email Security Gateway or Barracuda Essentials for Email Security service, make sure to add the IP address of the Barracuda Web Security Gateway to the **IP and Port Exemptions** list on the **BLOCK/ACCEPT > IP Block/Exempt** page. This prevents bad URLs from causing the emailed report to be blocked. If you are sending reports through another spam filtering device or service, make sure to specifically allow the IP address of the Barracuda Web Security Gateway on that solution.

Reports can be anchored on user activity, content, or bandwidth usage and are grouped as follows:

For Human Resources, Teachers, and Managers

These reports are user-friendly, easy-to-read, and provide the following critical information:

- **Productivity** reports reflecting user activity with social networking and other applications; for example:
  - Top Users by Browse Time on Gaming Sites
  - Top Social Networking Domains by Requests – May determine which domains you want to block, warn, or monitor
  - Top YouTube Users by Bandwidth
  - Top Facebook Users by Browse Time
  - Top Users by Browse Time on Social Networking Sites
- **Safety and Liability** reports; for example:
  - Top Users by Requests to Intolerance and Hate Sites
  - Top Users by Requests to Anonymizer Sites. An anonymizer is a tool that attempts to make activity on the Internet untraceable. It is a proxy server computer that acts as an intermediary and privacy shield between a client computer and the rest of the Internet, hiding the client computer's identity (IP address).
  - Suspicious Keywords by Users – For detection of possible cyberbullying, or mention of weapons or terrorism. See the **BLOCK/ACCEPT > Web App Monitor** page for details.

For IT and System Administrators

These report types show infection activity, blocked virus downloads, bandwidth usage by time frame, and many other system performance-related reports**,** such as:

- **Infection Activity**
  - Malware Blocks – IP addresses from which requests were made to known spyware sites.
  - Virus Blocks – A list of blocked virus downloads during the specified time frame.
- **Web Activity**
  - Session time or browse time, by hour, or by time of day.
  - Popular IP addresses to which requests were made.
  - Categories (e.g., adult, gaming, leisure) by bandwidth, number of requests, browse time, and more.
  - Users by session time, browse time, bandwidth, and more.
- **Administrative**
  - Audit Reports for the Web Security Gateway track logins and logouts to the web interface, as well as changes to the configuration by role.
  - Temporary Access Request Log – Log of activity by teachers who have been given credentials to request temporary access for their students to domains that are typically regulated by system administrators. See Temporary Access for Education.
  - Temporary Access Requests by Domains, Users, or Categories.
- **Network Activity**
  - TCP Connection Usage
  - Daily Bandwidth
  - Web Requests Log
- **Summary**

- Internet, Network, and User activity summaries
- Total Usage

For a complete list and detailed descriptions of the system reports, see the online help on the **BASIC > Reports** page.

Accurately Reporting User Browsing Times

Embedded web content is intelligently detected by the Barracuda Web Security Gateway to maximize reporting accuracy. For example, a site such as **cnn.com** embeds requests to Facebook, Twitter, and other social networks. While a user visiting the news site might not explicitly click on any of the embedded links, the embedded content still makes periodic web requests. On a report, this could appear as if the user visited CNN, Facebook, and Twitter and spent 15 minutes on each site.

While this is technically accurate, it can misrepresent the user's actions on reports that are reviewed by the Human Resources department, for example. In most cases, the Barracuda Web Security Gateway can make the distinction between such embedded requests – also known as "referred requests" – and actual user visits, but there are some limitations due to the behavior of some client applications. Consequently, reports reflect estimates of actual user browse and session times.

In calculating browse times, the Barracuda Web Security Gateway uses the HTTP referrer (sic) header to make the distinction between embedded requests and user visits. However, it is important to note that there are various client applications that limit the accuracy of calculating browse times. Here are several examples:

- Javascript that downloads assets from another site and may not set the referral;
- iOS apps that request web assets and do not set the referral;
- Android apps that request web assets place the app package name in the referral.

Session Time Versus Browse Time

Session time is the time calculated for each browsing session generated, with an idle timeout value of about 3 minutes. So if, for example, a user visits cnn.com, but does not click anything else for more than 3 minutes, that is one session of 3 minutes for that user on cnn.com. If the user does click around cnn.com within the 3 minute time frame, the session continues to increase in length until there is a 3-minute idle time.

Browse time as shown in reports is the sum of all estimated session times in a particular grouping (domain, category, user, etc).

Additional Notes on Reporting

- **Maximum AD Group Size**: For reporting purposes, Barracuda recommends a maximum Active Directory (AD) group size of 1000 users.
- **Bar Graphs versus Line Graphs**: When creating HTML reports:
  - bar graphs are used for graphs containing 50 records or fewer.
  - line graphs are used for graphs containing over 50 records
- **Clearing Traffic Logs**: Navigate to the **BASIC > Web Log** page and click **Clear Log**.