Reporting

https://campus.barracuda.com/doc/17629485/

Some of the reports and features noted in this article are specific to the Barracuda Web Security Gateway version 8 and higher. **Note:** For reporting purposes, Barracuda Networks recommends a maximum Active Directory (AD) group size of 1000 users.

Report Set Grouped by Use Cases

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.

Important Some reports may contain URLs that are on block lists. If your Barracuda Web Security Gateway is sending reports via email through a Barracuda Email Security Gateway, 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 to prevent 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 add the IP address of the Barracuda Web Security Gateway to the Allow List on that solution.

Reports can be anchored on user activity, content or bandwidth usage and, in version 7.0 and higher, 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
  - ... and many more
- **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, mention of weapons,terrorism. See the **BLOCK/ACCEPT > Web App Monitor** page for details.

For IT, 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, browse time by hour or time of day.
  - Popular IP addresses to which requests were made.
  - Categories (i.e. adult, gaming, leisure, etc.) by bandwidth, number of requests, browse time.
  - Users by session time, browse time.
- **Administrative**
  - Audit Log for tracking 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 for 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. The Barracuda Web Security Gateway can make the distinction between such embedded requests – also known as "referred requests" – and actual user visits in most cases, but there are some limitations due to the behavior of some client applications. Consequently, reports reflect estimates of actual user browse and session times.

Important

In calculating browse times, the Barracuda Web Security Gateway uses the HTTP refererr (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 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

Basic report settings are configured on the **BASIC > Reports** page. The following options are advanced settings, configured on the pages noted:

- **Maximum AD Group Size** – For reporting purposes, Barracuda Networks recommends a maximum Active Directory (AD) group size of 1000 users.

- **Bar Graph versus Line Graph** – When creating HTML reports with graphs which contain more than 50 records, a line graph is displayed. For 50 records or less, a bar graph is displayed.
- **To Clear Traffic Logs** – See the **BASIC > Web Log** page.
- Before running reports based on new local users/groups, you must do a full LDAP sync. Use the **Sync Now** button to force an immediate sync on the **USERS/GROUPS > Authentication** page.

On the **ADVANCED > Log/Report Settings** page:

- **Show Full URL in Logs** – Setting this feature to *Yes* means that the Barracuda Web Security Gateway will capture the query string portion of URLs in the **Web Log**.
- **Enable Privacy Option** – When enabled, this option prevents user names from appearing in the traffic log or any reports.
- **Anonymize NTLM User** – Setting to *Yes* logs NTLM users as *Anonymous*.
- **Report Retention Days** – Use to indicate the number of days, up to 6 months, for which you want the Barracuda Web Security Gateway to store reporting data.
- **Reports From address** – Configure the email address from which the Barracuda Web Security Gateway emails reports.
- **Enable Referrer Tracking in Reports** – To simplify report results, browse sessions are grouped by referer. If this feature is enabled, both the referer domain and the referer category are captured in the syslog. For details about syslog output, see Syslog and the Barracuda Web Security Gateway in Barracuda Campus.

On the **BASIC > Reports** page:

- **Hide Custom Categories from reports** – Checking this box means that activity related to Custom Categories you have defined are not included in the report data.