How to Configure Web Application Monitoring Version 9.x

https://campus.barracuda.com/doc/41110327/

This feature applies to the Barracuda Web Security Gateway 610 and higher running firmware version 9.0. Note: For Chromebook users with the Barracuda Chromebook Security Extension installed:

- Settings on the **BLOCK/ACCEPT > Web App Control** and **BLOCK/ACCEPT > Web App Monitor** pages do not apply, *and*
- Block/allow actions for G Suite are controlled by the Barracuda Chromebook Security Extension, not the Barracuda Web Security Gateway.

See also How to Configure Web Application Monitoring Version 10 and Above.

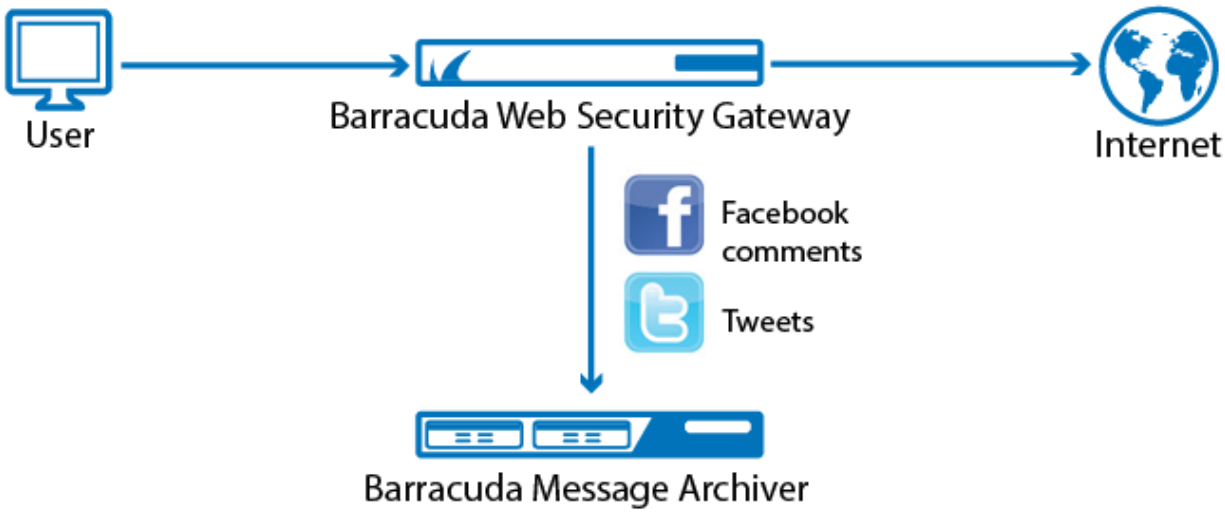
Capture and Archive Suspicious Content or Data Patterns in Chat, Email, and Other Social Media Communications

The Barracuda Web Security Gateway can inspect and catalog outbound content and forward it to an email address or external message archiver, like the Barracuda Message Archiver. These messages can be tied to the users' Active Directory credentials and fully indexed, making them as easy to search as MS Exchange emails. This ensures that social media communications from corporate networks are always available for access and retrieval for eDiscovery and audits as well as to create alerts for proactive monitoring.

Specific data patterns such as credit card numbers, Social Security numbers (U.S.), HIPAA and privacy information can also be detected to help prevent data leakage.

Use this feature to capture and archive chat, email, user registrations and other social media communications on social media portals. Set alerts to be sent to the administrator email address if certain data patterns are detected in outbound traffic, such as Social Security or credit card numbers, or HIPAA related content.

Figure 1: Web Activity Monitoring



How Archiving and Searching Monitored Web Activity Works

From the **BLOCK/ACCEPT > Web App Monitor** page, you can specify a **Web Activity Archiving Email Address** for archiving selected actions such as logins, chat, posts, comments and associated content. The Barracuda Web Security Gateway will package each interaction as an SMTP message and email it to this address, which can then be marked for archiving. Archived messages can then be indexed and searched by source or content, and alerts can be generated per policy you set in your archiving solution, or, specifically based on specific data patterns. For information about searching archived messages and using policy alerts with the Barracuda Message Archiver, see Understanding Basic and Advanced Search and Policy Alerts.

Note: SSL Inspection must be enabled for actions shown with an asterisk (*) on the **BLOCK/ACCEPT > Web App Monitor** page to be archived. Examples include:

- Facebook *user registration* and *login*
- Google *chat message*
- Twitter *send tweet, login, direct message, user registration*

For a complete list of actions for which SSL Inspection must be enabled for capture, see the **BLOCK/ACCEPT > Web App Monitor** page.

For more information about SSL Inspection, see Using SSL Inspection With the Barracuda Web Security Gateway and How to Configure SSL Inspection.

Example of Social Media Archiving

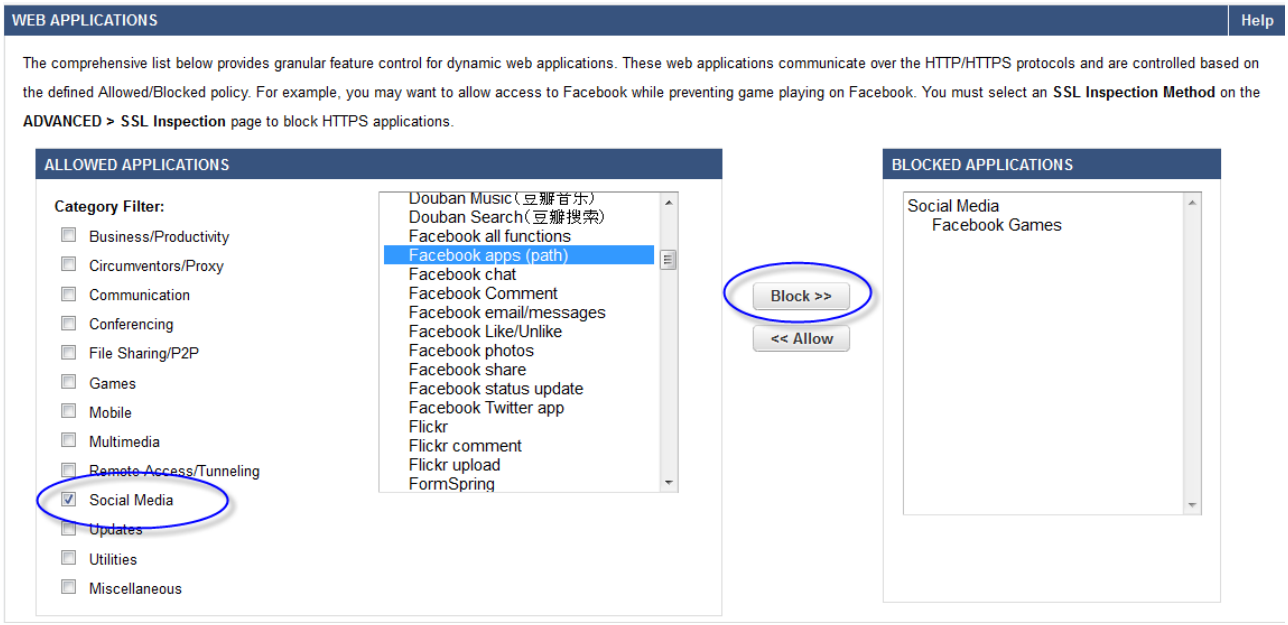
You might want to allow users in the organization to use Facebook to view and make comments and

use messaging, but you want to capture the content. You might also want to block games and/or other Facebook apps to protect your network from viruses and malware.

To regulate web 2.0 applications over HTTPS, you must configure SSL Inspection from the **ADVANCED > SSL Inspection** page and set up SSL certificates. See How to Configure SSL Inspection.

To configure Web Application Monitoring, first set up your block/accept policies for social media. Here is the process for the example mentioned above:

1. From the **BLOCK/ACCEPT > Web App Control** page, in the **Application Navigator,** make sure that **Social Media** is selected.
   In the **Allowed Applications** list box, hold the CTRL key and click **Facebook Games** and **Facebook apps**. Click **Block**.
   Those applications will move to the **Blocked Applications** list box.



2. Save your changes. In this example, you have left *chat, comment,* and other Facebook apps in the **Allowed Applications** list, moving the applications you want to block, such as apps and games to the **Blocked Applications** list.
3. From the **BLOCK/ACCEPT > Web App Monitor** page, enable the application actions whose content you want to archive. In this example, you would **Enable Facebook Comments** and **Message** for monitoring. After you enable any actions on the page, the Barracuda Web Security Gateway will capture the content from each action, package it as an SMTP message and email it to the **Web Activity Archiving Email Address** you specify on the page.
4. Select either predefined categories of suspicious keywords to monitor and/or archive using the built-in Barracuda database, and/or specify custom words in the **Create New Custom**

Keyword Category section. Suspicious keyword categories include pornography, cyberbullying and terrorism, for example.

5. Define a **Suspicious Keywords Alert Email Address** to which the Barracuda Web Security Gateway should send alerts when selected content is detected in traffic from the web-based applications you select on the page.

Detecting Sensitive Data Patterns

Social media and other application communications as noted above may also be searched for data patterns such as credit card numbers and HIPAA compliance terms, for example.

To help defend against potential data breaches, use the **Data Pattern Categories to Monitor** section to select applicable data patterns to detect in web applications that you enable on the **BLOCK/ACCEPT > Web App Monitor** page.

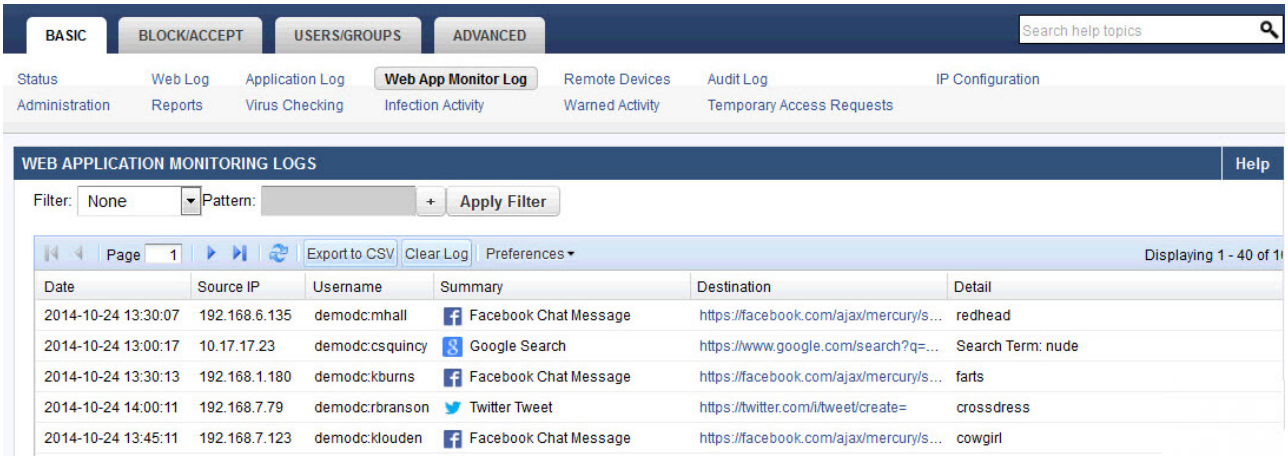
To configure this feature:

- Select from a predefined set of filters to quickly set up data pattern categorization policies against the web-based applications listed on the page, such as Facebook and Twitter. These predefined filters include the following:
  - **Credit Card** – AMEX, DINER, DISCOVER, ENROUTE, CHASE, MC, VIS, VOYAGER
  - **Social Security –** Social Security Number (United States format)
  - **Privacy –** birth date, Driver's License (United States format), expiration date, phone number
  - **HIPAA –** address, birth date, Driver's License, expiration date, phone number
- Enter a **Suspicious Keywords Alert Email Address** in the **Web Activity Notification** section of the **BLOCK/ACCEPT > Web App Monitor** page if you want to receive an alert when these data patterns are detected in the applications you select.
- If you also want to archive these communications, enter a **Web Activity Archiving Email Address** in the **Web Activity Notification** section of the page. After you enable any actions on the page, the Barracuda Web Security Gateway will capture the content from each action in which the selected data patterns are detected, package it as an SMTP message and email it to that email address.

Web App Monitor Log

The **BASIC > Web App Monitor Log** lists all chat, email, user registrations and other social media interaction traffic it processes per settings you configure on the **BLOCK/ACCEPT Web App Monitor** page. Fields logged are:

- **Date** - Date and time of the request.
- **Source IP** - IP address of the client that originated the request.
- **Username** - The name of the user that sent the request.
- **Summary** - The action represented in the request. For example, *Facebook Comment*.
- **Destination** - URL visited in the request.
- **Details** - Detailed information about the actions: search engine keywords, word from a *Facebook Comment*, etc.



Figures