

## How to Configure Web Application Monitoring version 6.x - 7.x

<https://campus.barracuda.com/doc/6160433/>

This feature applies to the Barracuda Web Security Gateway 610 and higher running firmware version 6.0 and higher. Some features, as noted below, are only available with version 8.0 and higher.

See also:

- [Using SSL Inspection](#)
- [Web and Desktop Application Control](#)
- [Application Filtering for Non Web Based Applications](#)
- [How to Configure Web Application Monitoring Version 8.x and Above](#)
- [How to Configure Web Application Monitoring Version 10 and Above](#)

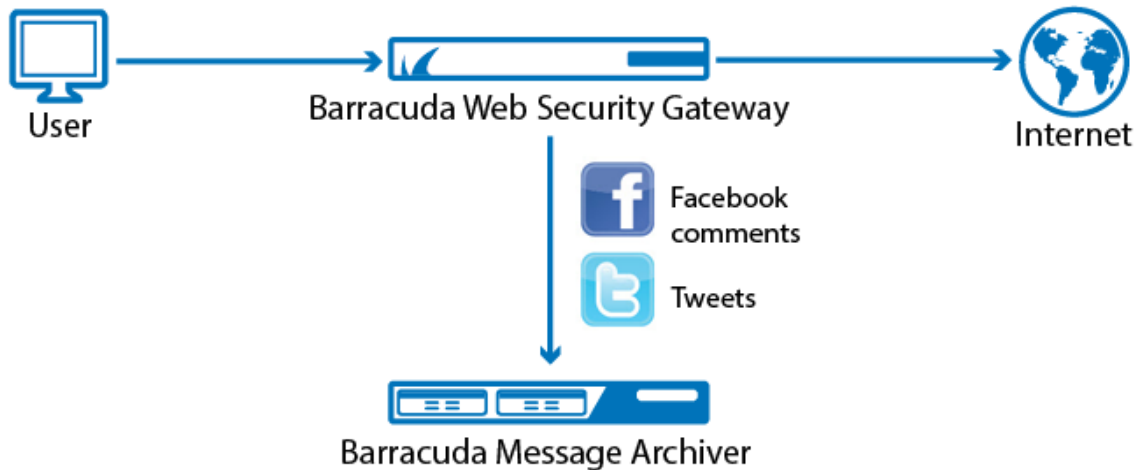
Due to recent vulnerabilities discovered with the SSL protocol, Barracuda Networks strongly recommends that you upgrade to 8.1.0.005 before using SSL Inspection. See the Barracuda Networks Security Updates blog post around this topic: [Barracuda delivers updated SSL Inspection feature](#). Available with the Barracuda Web Security Gateway 310 (limited) and higher.

## 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 fully indexed and tied to Active Directory credentials of users. The archived content is then as easy to search as MS Exchange emails. This process 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

On the **BASIC > 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 packages each interaction as an SMTP message and emails it to this address. This content is then marked for archiving. Archived messages are indexed and can be searched by source or content. 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:** If you want actions shown with an asterisk (\*) on the **BLOCK/ACCEPT > Web App Monitor** page to be archived, you must enable SSL Inspection. Example actions 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 6.x](#).

### How to Configure Social Media Archiving

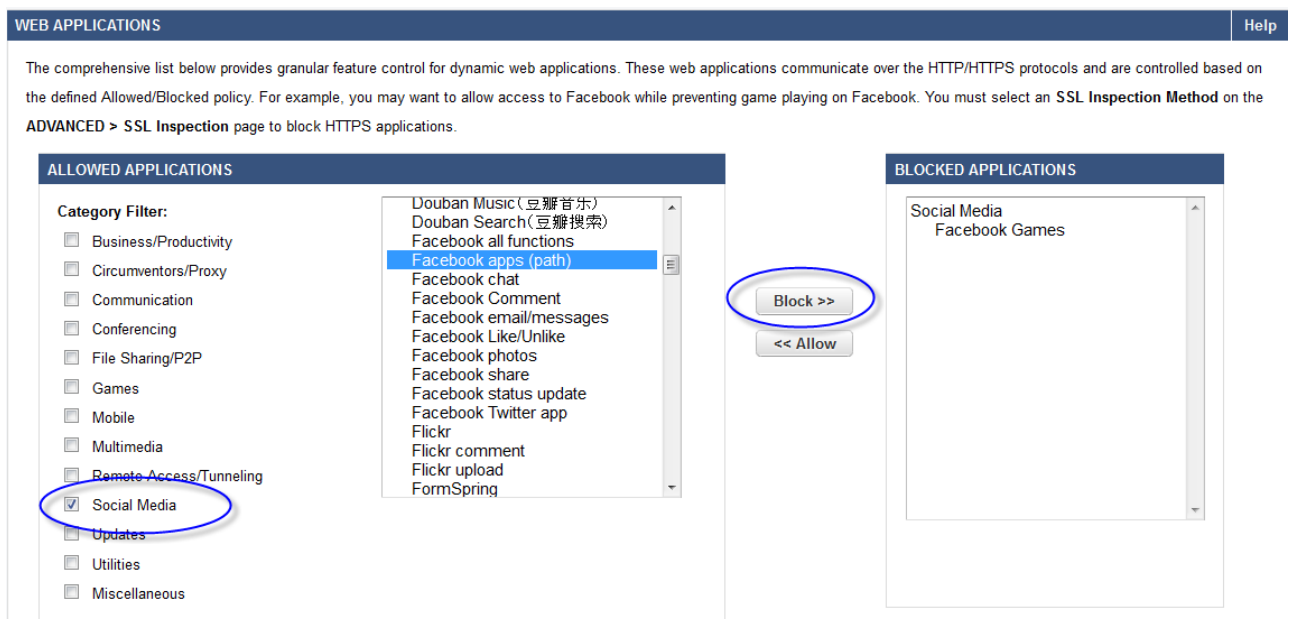
As an example scenario, you might want to allow users in the organization to use Facebook to view

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.

If you want to regulate web 2.0 applications over HTTPS, then you must configure SSL Inspection from the **ADVANCED > SSL Inspection** page and set up SSL certificates. See [How to Configure SSL Inspection 7.0](#).

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

1. On the **BLOCK/ACCEPT > Web App Control** page, in the **Application Navigator**, ensure that **Social Media** is checked.  
In the **Allowed Applications** list box, hold the CTRL key and click **Facebook Games** and **Facebook apps**. Click **Block**.  
Those applications then appear in 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. On 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.

---

## 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
- Social security numbers
- Privacy terms
- HIPAA compliance terms

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:

- 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.






**BASIC** **BLOCK/ACCEPT** **USERS/GROUPS** **ADVANCED**

Status Web Log Application Log **Web App Monitor Log** Remote Devices Audit Log IP Configuration  
Administration Reports Virus Checking Infection Activity Warned Activity Temporary Access Requests

**WEB APPLICATION MONITORING LOGS** [Help](#)

Filter:  Pattern:

Page     Displaying 1 - 40 of 11

Date	Source IP	Username	Summary	Destination	Detail
2014-10-24 13:30:07	192.168.6.135	demodc:mhall	 Facebook Chat Message	<a href="https://facebook.com/ajax/mercury/s...">https://facebook.com/ajax/mercury/s...</a>	redhead
2014-10-24 13:00:17	10.17.17.23	demodc:csquincy	 Google Search	<a href="https://www.google.com/search?q=...">https://www.google.com/search?q=...</a>	Search Term: nude
2014-10-24 13:30:13	192.168.1.180	demodc:kbruns	 Facebook Chat Message	<a href="https://facebook.com/ajax/mercury/s...">https://facebook.com/ajax/mercury/s...</a>	farts
2014-10-24 14:00:11	192.168.7.79	demodc:rbranson	 Twitter Tweet	<a href="https://twitter.com/i/tweet/create=">https://twitter.com/i/tweet/create=</a>	crossdress
2014-10-24 13:45:11	192.168.7.123	demodc:klouden	 Facebook Chat Message	<a href="https://facebook.com/ajax/mercury/s...">https://facebook.com/ajax/mercury/s...</a>	cowgirl

## Figures

1. Social Media ArchivingBWSG.png
2. Web App Control Example.png
3. WebAppMonitorLog8.0.jpg

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.