Suspicious and Sensitive Keyword Tracking

https://campus.barracuda.com/doc/17629457/

Enabling the **SSL Inspection** feature is necessary to use the **Keyword Tracking** option. See Using SSL Inspection With the Barracuda Web Security Gateway and related articles to understand this feature and what is required to use it safely. Using SSL inspection involves creating and/or installing SSL certificates in the Barracuda Web Security Gateway and, for self-signed certificates, in all client browsers.

Due to recent vulnerabilities discovered with the SSL protocol, Barracuda strongly recommends that you upgrade to 8.1.0.005 before using SSL Inspection. For more information, see the Barracuda Networks Security Updates blog post around this topic: Barracuda Delivers Updated SSL Inspection Feature.

Keyword Tracking is available with the Barracuda Web Security Gateway 410 and higher.

The Barracuda Web Security Gateway can identify, track and report on suspicious keywords in filtered social media traffic for notification and reporting purposes. For identifying cyberbullying, profanity, terrorism, adult content and other suspicious social media communications, Barracuda Networks employs a *suspicious keywords* lexicon to which you can add custom keywords you want the Barracuda Web Security Gateway to scan for and flag in captured social media traffic.

You can configure alerts, as described below, to be sent when these keywords are detected in captured traffic. Social media activity monitored/captured with this feature is available:

- On the **Web App Monitor Log** page
- In reports
- In alert emails, configured on the **BLOCK/ACCEPT > Web App Monitor** page (see Figure 1 for an example alert email)
- In SMTP messages emailed to an email address or archiving solution, configured on the **BLOCK/ACCEPT > Web App Monitor** page

The Barracuda Web Security Gateway can also inspect and catalog outbound content for, and send alerts on, specific data patterns such as credit card numbers, Social Security numbers (U.S.), HIPAA and privacy information to help prevent data leakage. For more information about how this feature works, see How to Configure Web Application Monitoring.

How to Configure Suspicious and Sensitive Keyword Tracking

1. From the **BLOCK/ACCEPT > Web App Monitor** page, enable web application monitoring for

specific actions you select in Facebook, Twitter, Google and other popular social media portals. Granularity of actions includes chat, login, wall post, user registration, sending email and more.
2. Optionally specify a **Web Activity Archiving Email Address** on the page, and the Barracuda Web Security Gateway will package each interaction as an SMTP message and email it to that address. 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. For information about searching archived messages and using policy alerts with the Barracuda Message Archiver, see Understanding Basic and Advanced Search and Policy Alerts.
3. Enable tracking and flagging of (suspicious) Keyword Categories and/or Data Pattern Categories by selecting the categories you want to scan for in the web applications and actions enabled on the page. Click **Save** after making your selections to update the configuration. A report summarizing content policy violations based on the selected Keyword Categories and Data Patterns will be emailed to the **Keywords Alert Email Address** you define in this section.

Figure 1: Example alert message to the administrator

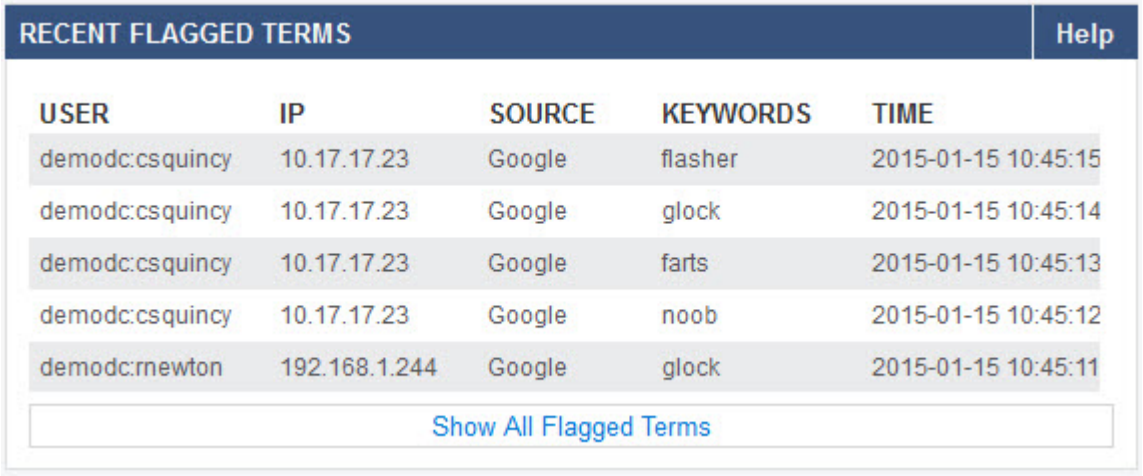
4. Optionally create your own custom keyword categories and associated words to scan for in searches and social media activities. For each custom keyword category, enter your own words, each on a new line, that you wish to include in the keyword group. Click **Add.** The new keyword category is added to the table.
5. Enable **SSL Inspection** on the **ADVANCED > SSL Inspection** page and create or upload an SSL certificate. Follow instructions in How to Configure SSL Inspection to choose the best way to set up your SSL certificate.

Suspicious Keywords Shown on the Dashboard page

The **BASIC > Dashboard** page includes a section showing **Recent Flagged Terms** from the suspicious keywords lexicon that were identified in captured social media interactions, as shown in

Figure 2 below. Click the Show All Flagged Terms link to see the **BLOCK/ACCEPT > Web App Monitor Log** page, listing all recent flagged terms and details.

Figure 2: Recent Flagged Terms (suspicious keywords) in captured social media interactions



slang, pornography, terrorism, cyberbullying, cyber, bullying

Figures

1. WAMalertMsg.jpg
2. RecentFlaggedTerms.jpg
3. search.jpg