Web and Desktop Application Control

https://campus.barracuda.com/doc/39822163/

Desktop Applications Versus Web-Based Applications

The Barracuda Web Security Gateway offers administrators control over both desktop and web based applications. Common desktop applications include iTunes, Real Player and Jabber, which use both standards based and proprietary communication protocols. Web based applications include Facebook and LinkedIn and are primarily presented through a web browser. This article defines how the administrator can create block/allow policies and archive social media interactions with the Barracuda Web Security Gateway.

Managing Desktop (Non Web-Based) Applications

In the case of desktop applications, the Barracuda Web Security Gateway enables administrators to define block/allow policies on popular applications using the **BLOCK/ACCEPT > Applications** page. For instance, file sharing sites such as BitTorrent and communication apps such as AOL IM can be blocked as per corporate policy. These policies can be defined against authenticated and unauthenticated users to offer more access to a given set of users.

Further, entire protocols can be blocked such as FTP, POP, and SSH. See How to Block FTP and other Standard Protocols.

Managing Web-Based Applications

The Web Application Control feature offers administrators fine grained control over web applications. What this means is that, when the **SSL Inspection** feature is enabled on the Barracuda Web Security Gateway 410 and higher, administrators can create policies such as:

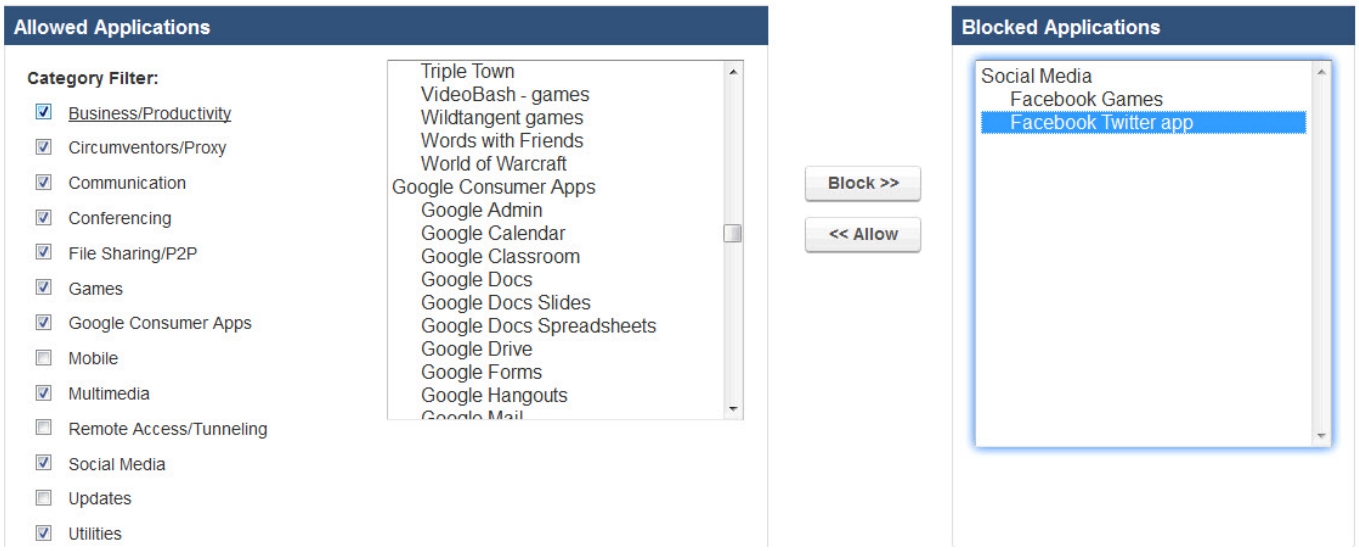
- Block certain portions of web based applications such as Facebook Chat and Facebook Sharing, while allowing users access to the rest of Facebook.
- Block access to Google Consumer Apps such as Google personal email accounts, but allow access to Google business (or education) email accounts. This feature requires Barracuda Web Security Gateway version 9.1 or higher. Because of the way Google now handles SSL certificates, there are currently some restrictions with SSL Inspection on Google sub domains. For details, see Google Restrictions With SSL Inspection. For examples of block/allow policies with Google business/education versus consumer accounts, see Google Workspace Control Over

HTTPS and How to Restrict YouTube Content On Your Network. For Chromebooks users, if you are running the Barracuda Web Security Gateway 10.1 or above, see How to Get and Configure the Barracuda Chromebook Security Extension.

With the Facebook example, the administrator can define what they deem permissible on their network without having to block all of Facebook. As shown in Figure 1 below, the Facebook Twitter app and Games have been added to the list on the right of **Blocked Applications.** See the **BLOCK/ACCEPT > Web App Control** page for more information and to configure.

Note that the Barracuda Web Security Gateway 210 does not support SSL Inspection, and if you are running version 11.0 or higher, (non web-based) Application blocking is not supported. You can alternatively block some or all HTTPS traffic by domain or by content category, but without granular control over web applications. This is also a common use case for the Barracuda Web Security Gateway 310 (running version 10.0 or above), since it offers limited SSL Inspection (only for Safe Search). For information on how to block/allow HTTPS traffic by domain or content category (does not include decryption of the URL contents), see HTTPS Filtering With the Barracuda Web Security Gateway.

Figure 1. Facebook is generally allowed, but the Facebook Twitter app and Games have been blocked by the administrator.



Monitoring Social Media Content

A powerful feature for meeting CIPA requirements and protecting students is the Web Application Monitoring function. This feature captures web activities such as comments and posts and packages the content in SMTP messages for email notifications and/or archiving. The monitoring feature allows administrators to track suspicious keywords that may signal potentially harmful behavior from a particular user. For more information about this feature, see How to Configure Web Application

Monitoring. This feature is available:

- With the Barracuda Web Security Gateway 610 and higher running version 7.0 and above *OR*
- With the Barracuda Web Security Gateway 410 and higher running version 10.0 and above

To configure, see the **BLOCK/ACCEPT > Web App Monitor** page in the Barracuda Web Security Gateway web interface.

The Barracuda Web Security Gateway receives periodic updates to its application and web application definitions to quickly react to the dynamics of the market. See Using SSL Inspection With the Barracuda Web Security Gateway and How to Configure SSL Inspection for details.

Figures