Embracing Social Media with Cisco Cloud Web Security

The Solution

Cisco Cloud Web Security is a smart solution that offers dynamic content controls that can safely enable Web 2.0 within the enterprise while setting appropriate security limits. Cisco Cloud Web Security allows organizations to take advantage of the business benefits of Web 2.0, including social networking sites with embedded applications such as Facebook. Dynamically updated controls allow businesses to permit access to appropriate applications and content while preventing the use of those that might increase risk, drain productivity, or be a potential loss of confidential information. The Application Visibility and Control feature on Cisco Cloud Web Security goes beyond just Web 2.0 controls and encompasses security and control from a holistic viewpoint.

Granular Access

Cisco Cloud Web Security's granular, next-generation feature controls enable administrators to monitor or block actions such as status updates; video streaming; "liking," chatting, and messaging; and file and content uploads. Businesses can even build and implement a social networking policy that could make Facebook or another social networking site a "read only" website.

Encrypted Web Traffic Controls

Any solution that enables data to be controlled either entering or leaving the network must be able to decrypt SSL packets. Without support for SSL decryption, an IT organization leaves itself open to a large "blind spot," where defined policies are not enforceable.

Cisco Cloud Web Security Application Visibility and Control (AVC) allows security managers to define granular policy controls over this type of functionality. For example, a company could make personal banking sites exempt from decryption while setting policy for a social networking platform with many applications to be decrypted.

Application-Specific Reporting

Cisco Cloud Web Security has extended the depth and flexibility of its online management and reporting portal, ScanCenter, so that it includes detailed reports for application types and activities. Customers can use a new category of predefined reports to track social media usage or create their own reports.

Dynamic Updates

Social media platforms are constantly updating and changing their native applications. Additionally, external applications that run on those platforms are created and modified by third parties every day. Because these applications change constantly, the AVC engine updates its signatures to remain current with the available functionality and applications.

Malware Protection

Cisco Cloud Web Security customers are also protected from malware and virus attacks delivered via social media platforms. Utilizing Cisco Cloud Web Security's Outbreak Intelligence™ technology, all web traffic is analyzed in real time, including HTML, JavaScript, Flash, and active scripts. This analysis, when coupled with context scanlets, offers multiple indicators as to the security posture of each web request.

A Solution Guide: Controlling Facebook Activity

This section uses the process for controlling and monitoring Facebook activity to demonstrate the depth and flexibility of Cisco Cloud Web Security's AVC engine. Facebook users can install and use applications to enhance their experience. You can use the AVC engine to block part or all of Facebook.

There are different ways you can block applications or accomplish the end result you want. You can use the standard web filters instead of, or as well as, the application control. It is important that you place the rules containing application control filters in the correct order relative to any other rules in the policy, particularly if using the Delegated Administration feature. When a rule allows access to a certain web resource, any subsequent rule that blocks that access is ignored, and vice versa.

Facebook-related applications are classified into one of the following groups:

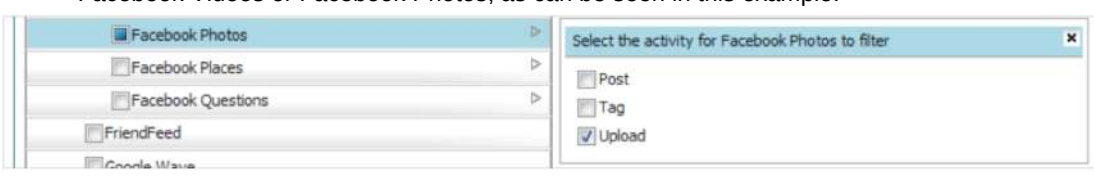
- **Native Facebook applications.** These applications are developed by Facebook and are usually hosted on the facebook.com domain. Native Facebook applications use the "Facebook Application_Name" naming convention, such as Facebook Photos.
- **External Facebook applications.** These applications are created and managed by third-party developers and are hosted outside of the facebook.com domain. External Facebook applications use the "Facebook Applications: Category" naming convention, such as Facebook Applications: Games. Due to the nature of Facebook and how it hosts many of its own and third-party applications, the AVC engine treats "Facebook" as a single application type, which includes both native and external Facebook applications.

The controls that are applied to users are determined by where the user is located in the Facebook interface. For example, users can view photos from both Facebook Photos and from their Facebook Walls. That means when the user is viewing another person's photo in their photo album, the controls for Facebook Photos apply, but when the user is viewing the same photo on their own Wall, the controls for Facebook General apply.

Configuring Facebook Controls

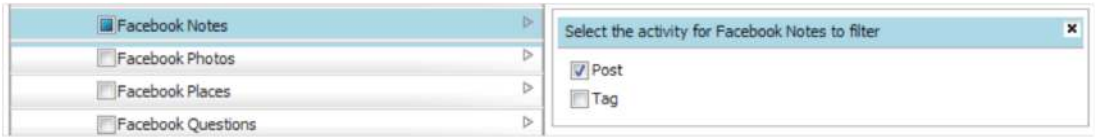
Like other application types, you can block or allow the complete Facebook application type or any of the particular applications included in that type. You can also apply more granular controls to most native Facebook applications by configuring different application activities and behaviors, such as blocking the posting of text. You can implement more granular controls to native Facebook applications using any of the following applications behaviors:

- **Block File Upload.** This behavior blocks uploading of files to native Facebook applications, such as Facebook Videos or Facebook Photos, as can be seen in this example:

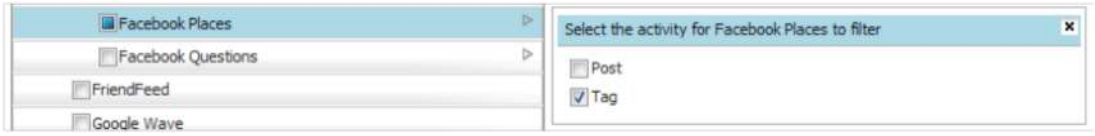


This application behavior does not affect links to external photos or videos, such as videos posted on YouTube.

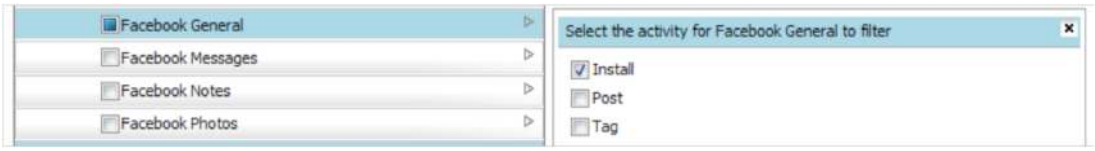
- **Block Posting Text.** This behavior prevents users from entering text in fields, such as comments, status updates, or notes, as in the example below. Blocking this behavior for an application is similar to making the application read-only.



- **Block Like/Tag.** This behavior blocks the ability to "like" a Facebook object, such as a status update or photo, by clicking the Like link. It also blocks the ability to tag people in Facebook objects, such as photos, videos, and places, as in this example:



- **Block Installation of Third Party Applications.** This behavior prevents users from installing external Facebook applications, as can be seen here:



Understanding Facebook General

Any area of Facebook.com that is not explicitly covered under one of the native Facebook applications is covered under the "Facebook General" native application. This includes users' Wall and Profile pages, for example.

Some Facebook objects that are included in a native Facebook application, such as photographs in Facebook Photos, might also appear on a user's Wall. When users view their own Walls, access to objects on the Wall is determined by the settings configured for the Facebook General application. For example, if you configure the Block Like/Tag behavior control for Facebook Photos, but not for Facebook General, users can click the Like link for photes from their Wall, but not from a photo album.

User Experience When Accessing Facebook

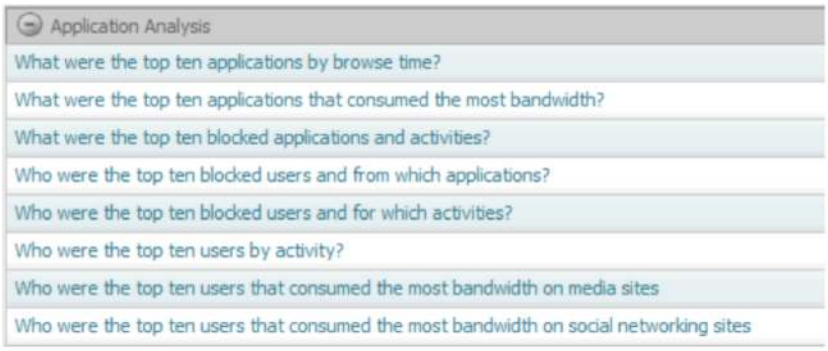
When the AVC engine blocks Facebook and other application content, it sends an end-user notification page by default. Hoever, due to how these applications display content in the web browser, it quite often does not show the end-user notification page. When you block a Facebook application or application behavior, users are prevented from performing the intended action, but it is not always clear to users that their actions are explicitly being blocked by the AVC controls.

Additionally, there are multiple ways to accomplish most tasks in Facebook. For example, users can reach a page to upload photos using different paths. Users trying to access blocked Facebook content may observe different responses depending on the application they are accessing, the path used to reach the application, and how the applicable access policy is configured to handle the application and application behaviors.

Viewing Reports

Some organizations may have a more open policy concerning the control of web applications but may still want a high level of visibility into their usage. Regardless of whether you choose to control application access or not—and the degree to which you do so—a comprehensive reporting platform that provides that visibility is an important part of the AVC engine. In addition to the comprehensive range of web usage reports available through Cisco Cloud Web Security's Web Intelligence Reporting platform, meaningful reports on web application usage can also be run.

A number of predefined reports are available for a detailed visibility into application usage. You could see, for example, which web applications have consumed the most bandwidth or taken up the most time. You could run reports on users' activities, see details of users' sites and activities that were blocked through your policy, or concentrate on media or social networking sites.



A separate set of similar predefined reports is available for analyzing users' activities on Facebook. This allows you to see usage of Facebook applications and activities by browse time or bandwidth, any that were blocked, and user reports.

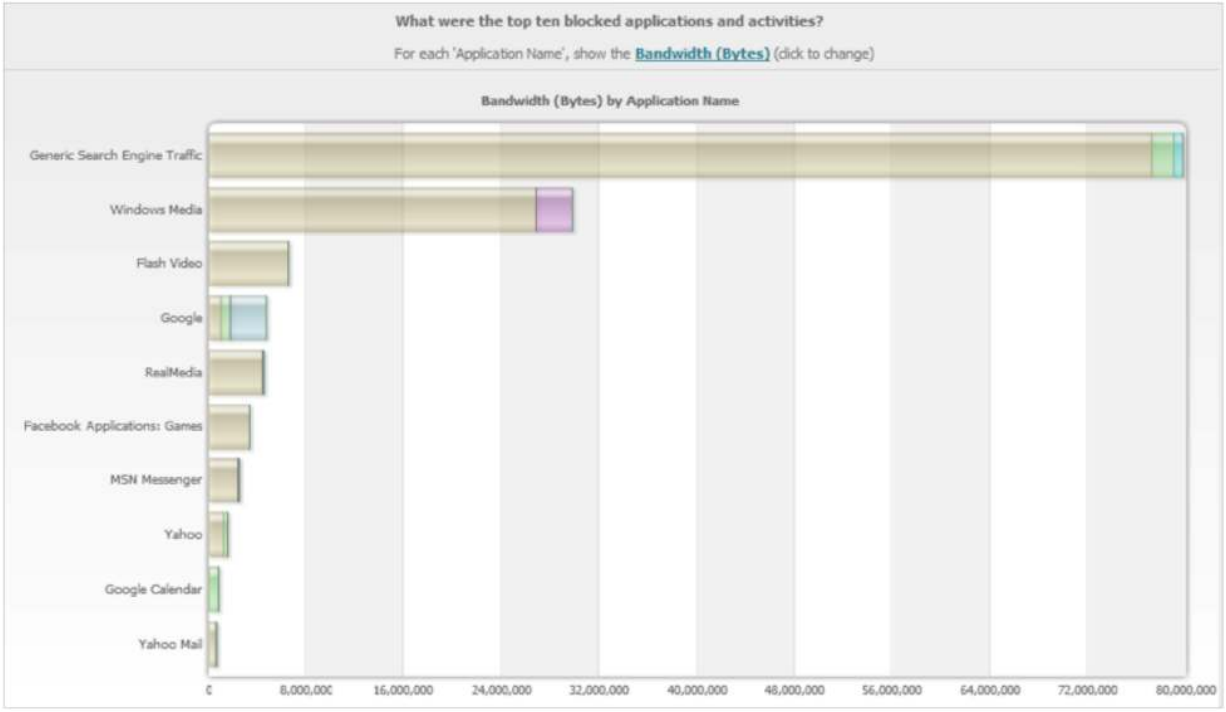
But predefined reports are only the beginning. You can further customize these reports using the Application Name and Application Activity attributes, on their own, paired together, or in combination with any of over 80 other existing reporting attributes, which can be used for searching or for filtering.

Applications and activities:

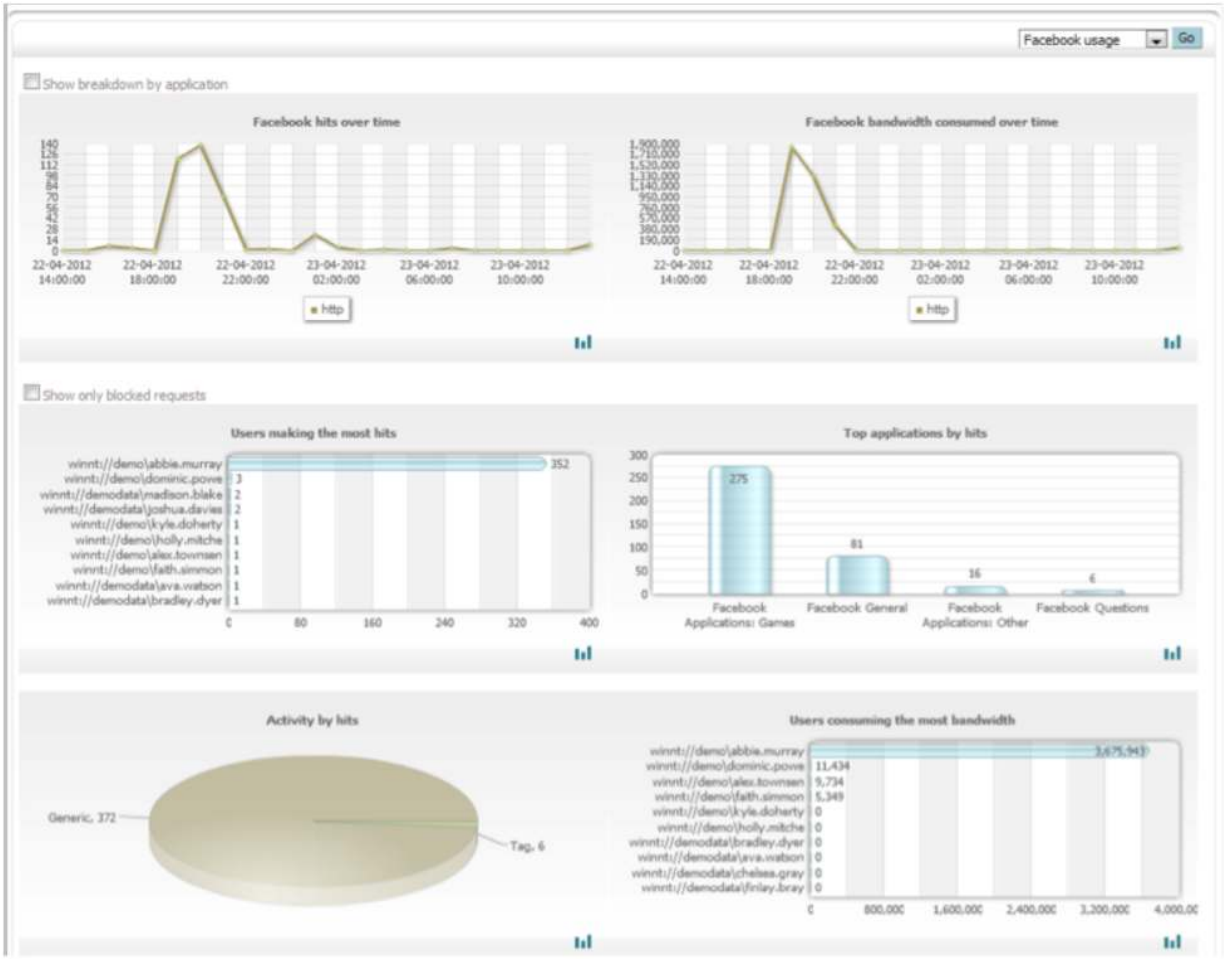
Downloaded files that took up the most bandwidth, and the applications from where they were downloaded:

Users that were blocked the highest number of times while attempting to upload files to web applications of a video nature, and their blocked files:

Reports can be displayed in a number of ways, including colorful graphs:



A useful dashboard summarizing Facebook activities in six separate graphs can be displayed as well.



Some of the reports can be broken down by activities, and others can be set to show only blocked requests. You can then drill down into any of these reports at the click of a button to customize the reports by changing the time bracket or search attributes, or adding filters to your search, saving them as your own customized reports, exporting them to PDF or CSV format, or scheduling them for automated delivery.

Using AVC with HTTPS Applications

To be able to control encrypted web applications, HTTPS inspection is required. This process is similar to the existing HTTPS inspection service. HTTPS inspection for AVC will also provide more granular reporting on application usage. To enable HTTPS inspection of applications, a policy for HTTPS inspection should be added, and this should include a rule with a filter for AVC.

Add a rule to your HTTPS policy (or add to an existing rule) with the application filter selected. This is independent of the other HTTPS filter settings, so you can inspect only applications without inspecting other HTTPS traffic if necessary. AVC HTTPS inspection requires downloading certificates to clients, as with standard HTTPS inspection.

When inspecting HTTPS applications, more detailed results will be seen for the application names in reports. For example, without HTTPS inspection, an application name may be seen as Facebook General, but when inspected, this will be seen as Facebook Applications: Games.

Rules and Guidelines

Consider the following rules and guidelines when configuring Facebook controls:

- Blocking Facebook General is the same as blocking the entire Facebook application type.
- You can prevent users from uploading photos and videos to Facebook from the web interface, but users can still upload photos and videos by sending emails with attachments to their Facebook email account. To prevent users from uploading photos and videos by email, configure your outgoing mail server, such as the Cisco IronPort Email Security appliance, to block email sent to the m.facebook.com domain.
- Some third party websites, such as cnn.com and espn.com, interact with Facebook to display or modify content in a user's Facebook account. The AVC engine blocks some of these sites from posting content to Facebook, but it cannot block all sites or all updates.
- When you block Facebook Chat, users may receive chat messages, but cannot send chat messages. Additionally, users do not see anyone else online, but others can see them online. When your users try to reply to received chat messages, the intended recipient never receives the message, which essentially blocks communication.

For More Information

Cisco Cloud Web Security is the pioneer and largest global provider of cloud web security, ensuring a safe and productive Internet environment for businesses. Cisco Cloud Web Security solutions keep malware off corporate networks and allow businesses to control and secure the use of the web. As a cloud solution, Cisco Cloud Web Security eliminates the burden of purchasing and maintaining infrastructure in-house, significantly lowering the total cost of ownership. Powered by its proactive, multilayered Outbreak Intelligence™ threat detection technology, Cisco Cloud Web Security processes billions of web requests and millions of blocks each month for customers in more than 100 countries.

For more information, visit http://www.cisco.com/web/products/security/cloud_web/index.html

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA C22-708775-01 09/12