Web Security Management Examples

This chapter contains the following sections:

Web Security Management Examples

This appendix illustrates and describes a number of common ways to implement features of the Cisco Content Security Management appliance, and includes the following sections:

Web Security Appliance Examples

This section describes examples using a Security Management appliance and Web Security appliances.

Note All of these scenarios assume that you have enabled web reporting and web tracking on the Security Management appliance *and* on your Web Security appliances. For information on how to enable web tracking and web reporting, see Using Centralized Web Reporting and Tracking

Example 1: Investigating a User

This example demonstrates how a system administrator would investigate a particular user at a company.

In this scenario, a manager has gotten a complaint that an employee is visiting inappropriate web sites at work. To investigate this, the system administrator now needs to track the details of their web activity.

Once the web activity is tracked, a web report is generated with information about the employee's browsing history.

Step 1 On the Security Management appliance, choose **Web > Reporting > Users**.

Step 2 In the **Users** table, click on the **User ID** or **Client IP address** you want to investigate.

If you do not know the User ID or the Client IP address, type what you can remember of the User ID or Client IP address in text field, and click on **Find User ID or Client IP address**. The IP address does not need to be an exact match to return results. The Users table is populated with the User ID and Client IP addresses that you have specified. In this example, we are looking for information on Client IP address `10.251.60.24`.

Step 3 Click on IP address **`10.251.60.24`**.

The User Details page appears for `10.251.60.24`.

From the User Details page you can determine the URL Categories by Total Transactions, Trend by Total Transaction, URL Categories Matched, Domains Matched, Applications Matched, Malware Threats Detected, and Policies Matched.

These categories allow you to find out if, for example, user `10.251.60.24` was trying to access blocked URLs, which could be viewed in the Transactions Blocked column under the Domains section on the page.

Step 4 Click **Export** under the Domains Matched table to view the entire list of Domains and URLs that the user tried to access.

From here you can use the Web Tracking feature to track and view this specific user's web usage.

Note It is important to remember that web reporting allows you to retrieve all the domain information that a user goes to, not necessarily the specific URL that is accessed. For information on a specific URL that the user is accessing, what time they went to that URL, whether that URL is allowed, etc., use the Proxy Services tab on the Web Tracking page.

Step 5 Choose **Web > Reporting > Web Tracking**.

Step 6 Click the **Proxy Services** tab.

Step 7 In the User/Client IP Address text field type in the user name or IP address.

In this example we are searching for web tracking information for user `10.251.60.24`.

The search results appear.

From this page you can view a full list of transactions and URLs visited by the user of the computer that is assigned to the IP Address `10.251.60.24`.

Related Topics

The following table lists each of the topics discussed in this example. Click on the link for details on each topic.

Table 1: Related Topics for Investigating a User

Feature Name	Feature Information
User Page	Users Report (Web)
User Details Page	User Details (Web Reporting)
Exporting Report Data	Exporting Reporting and Tracking Data
Proxy Services tab on the Web Tracking page	Searching for Transactions Processed by Web Proxy Services

Example 2: Tracking a URL

In this scenario, a Sales manager wants to find out what the top five visited web sites are at their company are for the last week. Additionally, the manager wants to know which users are going to those websites.

Step 1 On the Security Management appliance, choose **Web > Reporting > Web Sites**.

Step 2 From the Time Range drop-down list, choose **Week**.

Step 3 Scroll down to the Domains section to view the domains, or web sites that have been visited.

The top 25 web sites that have been visited will be displayed in the Domains Matched table. In the same table you can click on the link in the Domain or IP column to view the actual web sites for a particular address or user.

Related Topics

The following table lists each of the topics discussed in this example. Click on the link for details on each topic.

Table 2: Related Topics for Tracking a URL

Feature Name	Feature Information
Web Sites Page	Web Sites Report

Example 3: Investigating Top URL Categories Visited

In this scenario, the Human Resources manager wants to know what the top three URL categories her employees are visiting over the 30 days. Additionally, a network manager wants to get this information to monitor bandwidth usage, to find out what URLs are taking up the most bandwidth on her network.

The example below is to show how you can gather data for several people covering several points of interest, while only having to generate one report.

Step 1 On the Security Management appliance, choose **Web > Reporting > URL Categories**.

From the URL Categories page in this example, you can see that of the top 10 URL Categories by Total Transactions graph reveals, there were 282 K of Uncategorized URLs that were accessed, as well as Instant Messaging, Hate Speech and Tattoo sites, and so forth.

At this point you can export that raw data to an Excel spreadsheet, by clicking the **Export** link and send this file to the Human Resources manager. But remember, your network manager wants to know the bandwidth usage by each URL.

Step 2 NEEDS NEW ILLO - SKIP Scroll down to the **URL Categories Matched** table, to view the Bandwidth Used column.

From the **URL Categories Matched** table, you can see the Bandwidth Usage for all of the URL Categories. Again, you can click the **Export** link and send this file to the Network manager. For finer granularity though, click on the Instant Messaging link to find out which users are taking up the bandwidth. The following page appears.

From this page, the network manager can see the top 10 users for Instant Messaging sites.

This pages reveals that in the last 30 days, user 10.128.4.64 has spent 19 hours and 57 minutes on an Instant Messaging site; and the bandwidth usage for this time was 10.1 MB.

Related Topics

The following table lists each of the topics discussed in this example. Click on the link for details on each topic.

Table 3: Related Topics for Investigating the Top URL Categories

Feature Name	Feature Information
URL Categories Page	URL Categories Report
Exporting Report Data	Exporting Reporting and Tracking Data