Web Security Appliance Reports

This chapter contains the following sections:

- Overview Page, on page 1
- Users Page, on page 2
- User Count Page, on page 3
- Web Sites Page, on page 4
- URL Categories Page, on page 4
- Application Visibility Page, on page 5
- Anti-Malware Page, on page 5
- Advanced Malware Protection Page, on page 6
- File Analysis Page, on page 6
- AMP Verdict Updates Page , on page 6
- Client Malware Risk Page, on page 7
- Web Reputation Filters Page, on page 7
- L4 Traffic Monitor Page, on page 8
- SOCKS Proxy Page , on page 8
- Reports by User Location Page, on page 9
- Web Tracking Page , on page 9
- System Capacity Page, on page 12
- System Status Page, on page 13

Overview Page

The **Reporting > Overview** page provides a synopsis of the activity on the Web Security appliance. It includes graphs and summary tables for Web traffic processed by the Web Security appliance.

Table 1: System Overview

Section	Description
Web Proxy Traffic Characteristics	`Listing of Average transactions per second in past minute`, `Average bandwidth (bps) in past minute`, `Average response time (ms) in past minute`, and `Total current connections`.

Section	Description
System Resource Utilization	Listing of current `Overall CPU Load`, `RAM` and `Reporting / logging disk` usage. Click **System Status Details** to switch to the System Status page (see System Status Page, on page 13 for details). **Note** The CPU utilization value shown on this page and the CPU value shown on the System Status page may differ slightly because they are read separately, at differing moments.

Table 2: Time Range-based Categories and Summaries

Section	Description
Time Range: Choose a time range for the data displayed in the following sections. Options are Hour, Day, Week, 30 Days, Yesterday, or a Custom Range.	
Total Web Proxy Activity	Displays the actual number of transactions (vertical scale) as well as the approximate date that the (Web Proxy) activity occurred (horizontal timeline).
Web Proxy Summary	Allows you to view the percentage of Web Proxy activity that are suspect or clean Web Proxy activity.
L4 Traffic Monitor Summary	Reports on traffic monitored and blocked by the L4 Traffic Monitor.
Suspect Transactions	Allows you to view the web transactions that have been labeled as suspect by the various security components. Displays the actual number of transactions as well as the approximate date that the activity occurred.
Suspect Transactions Summary	Allows you to view the percentage of blocked or warned transactions that are suspect.
Top URL Categories: Total Transactions	Displays the top 10 URL categories that have been blocked.
Top Application Types: Total Transactions	Displays the top application types that have been blocked by the AVC engine.
Top Malware Categories: Monitored or Blocked	Displays all malware categories that have been detected.
Top Users: Blocked or Warned Transactions	Displays the users that are generating the blocked or warned transactions. Authenticated users are displayed username and unauthenticated users are displayed by IP address.

Users Page

The **Reporting > Users** page provides several links that allows you to view web traffic information for individual users. You can view how much time users on the network have spent on the Internet or on a particular website or URL, and how much bandwidth users have used.

Section	Description
Time Range (drop-down list)	A menu that allows to choose the time range of the data contained in the report.

Top Users by Transactions Blocked	Lists the users (vertical scale) that have the greatest number of blocked transactions (horizontal scale).
Top Users by Bandwidth Used	Displays the users (vertical scale) that are using the most bandwidth on the system (horizontal scale represented in gigabyte usage).
Users Table	Lists individual users and displays multiple statistics on each user.

User Details Page

The **User Details** page displays information about a specific user selected in the Users Table on the **Reporting > Users** page.

Section	Description
Time Range (drop-down list)	A menu that allows to choose the time range of the data contained in the report.
URL Categories by Total Transactions	Lists the specific URL categories that a specific user is using.
Trend by Total Transaction	Displays at what times the user accessed the web.
URL Categories Matched	Shows all matched URL categories during a specified time range for both completed and blocked transactions.
Domains Matched	Displays information about a specific Domain or IP address that this user has accessed. **Note** If you export this Domains data to a CSV file, be aware that only the first 300,000 entries are exported to the file.
Applications Matched	Displays specific application that a specific user is using as detected by the AVC engine.
Malware Threats Detected	Displays the top malware threats that a specific user is triggering.
Policies Matched	Displays a specific policy that is being enforced on this particular user.

User Count Page

The **Reporting** > **User Count** page displays information about the total number of authenticated and unauthenticated users of the appliance. The page lists the unique user count for the last 30 days, 90 days, and 180 days.

Note System computes the total user count of authenticted and unauthenticated users once a day.

For example, if you view the user count report on May 22, 23:59, at the latest, the system will display the total user count till May 22, 00:00.

Web Sites Page

The **Reporting > Web Sites** page is an overall aggregation of the activity that is happening on the Web Security appliance.

Section	Description
Time Range (drop-down list)	Menu allows you to choose the time range of the data contained in the report.
Top Domains by Total Transactions	Lists the top domains that are being visited on the site in a graph format.
Top Domains by Transactions Blocked	Lists the top domains that triggered a block action to occur per transaction in a graph format.
Domains Matched	Lists the domains that are that are being visited on the site in an interactive table. **Note** If you export this Domains data to a CSV file, be aware that only the first 300,000 entries are exported to the file.

URL Categories Page

The **Reporting > URL Categories** page can be used to view the URL categories that are being visited by users on the network. The URL Categories page can be used in conjunction with the Application Visibility Page and the Users Page to investigate a particular user and also what types of applications or websites that a particular user is trying to access.

Note The set of predefined URL categories is occasionally updated.

Section	Description
Time Range (drop-down list)	Choose the time range for your report.
Top URL Categories by Total Transactions	This section lists the top URL categories that are being visited on the site in a graph format.
Top URL Categories by Blocked and Warned Transactions	Lists the top URL that triggered a block or warning action to occur per transaction in a graph format.

Section	Description
URL Categories Matched	Shows the disposition of transactions by URL category during the specified time range, plus bandwidth used and time spent in each category. If the percentage of uncategorized URLs is higher than 15-20%, consider the following options: • For specific localized URLs, you can create custom URL categories and apply them to specific users or group policies. • You can report uncategorized and misclassified and URLs to the Cisco for evaluation and database update. • Verify that Web Reputation Filtering and Anti-Malware Filtering are enabled.

URL Category Set Updates and Reports

The set of predefined URL categories may periodically be updated automatically on your Web Security appliance.

When these updates occur, old category names will continue to appear in reports until the data associated with the older categories is too old to be included in reports. Report data generated after a URL category set update will use the new categories, so you may see both old and new categories in the same report.

Application Visibility Page

The **Reporting > Application Visibility** page shows the applications and application types used and blocked as detected by the Application Visibility and Control engine.

Section	Description
Time Range (drop-down list)	A menu that allows to choose the time range of the data contained in the report.
Top Application Types by Total Transactions	This section lists the top application types that are being visited on the site in a graph format.
Top Applications by Blocked Transactions	Lists the top application types that triggered a block action to occur per transaction in a graph format.
Application Types Matched	Allows you to view granular details about the application types listed in the Top Applications Type by Total Transactions graph.
Applications Matched	Shows all the application during a specified time range.

Anti-Malware Page

The **Reporting > Anti-Malware** page allows you to monitor and identify malware detected by the Cisco DVS engine.

Section	Description
Time Range (drop-down list)	A menu that allows to choose the time range of the data contained in the report.
Top Malware Categories Detected	Displays the top malware categories detected by the DVS engine.
Top Malware Threats Detected	Displays the top malware threats detected by the DVS engine.
Malware Categories	Displays information about particular malware categories that are shown in the Top Malware Categories Detected section.
Malware Threats	Displays information about particular malware threats that are shown in the Top Malware Threats section.

Malware Category Report Page

Step 1 Choose **Reporting > Anti-Malware**.

Step 2 In the Malware Categories interactive table, click on a category in the Malware Category column.

Malware Threat Report Page

Step 1 Choose **Reporting > Anti-Malware**.

Step 2 In the Malware Threat table, click on a category in the Malware Category column.

Advanced Malware Protection Page

See File Reputation Filtering and File Analysis.

File Analysis Page

See File Reputation and File Analysis Reporting and Tracking.

AMP Verdict Updates Page

See File Reputation Filtering and File Analysis.

Client Malware Risk Page

The **Reporting > Client Malware Risk** page is a security-related reporting page that can be used to monitor client malware risk activity. The Client Malware Risk page also lists client IP addresses involved in frequent malware connections, as identified by the L4 Traffic Monitor (L4TM).

Section	Description
Time Range (drop-down list)	A menu that allows you to choose the time range of the data contained in the report.
Web Proxy: Top Clients by Malware Risk	This chart displays the top ten users that have encountered a malware risk.
L4 Traffic Monitor: Malware Connections Detected	This chart displays the IP addresses of the computers in your organization that most frequently connect to malware sites.
Web Proxy: Clients by Malware Risk	The Web Proxy: Clients by Malware Risk table shows detailed information about particular clients that are displayed in the Web Proxy: Top Clients by Malware Risk section.
L4 Traffic Monitor: Clients by Malware Risk	This table displays IP addresses of computers in your organization that frequently connect to malware sites.

Client Detail Page for Web Proxy - Clients by Malware Risk

The **Client Details** page shows all the web activity and malware risk data for a particular client during the specified time range.

Step 1 Choose **Reporting > Client Malware Risk**.

Step 2 In the **Web Proxy - Client Malware Risk** section, click a user name in the “User ID / Client IP Address” column.

What to do next

User Details Page, on page 3

Web Reputation Filters Page

The **Reporting > Web Reputation Filters** page is a security-related reporting page that allows you to view the results of your set Web Reputation Filters for transactions during a specified time range.

Section	Description
Time Range (drop-down list)	A menu that allows to choose the time range of the data contained in the report.
Web Reputation Actions (Trend)	Displays the total number of web reputation actions (vertical) against the time specified (horizontal timeline).

Section	Description
Web Reputation Actions (Volume)	Displays the web reputation action volume in percentages by transactions.
Web Reputation Threat Types by Blocked Transactions	Displays the threat types that were blocked due to a low reputation score.
Web Reputation Threat Types by Scanned Further Transactions	Displays the threat types that resulted in a reputation score that indicated to scan the transaction.
Web Reputation Actions (Breakdown by Score)	Displays the web reputation scores broken down for each action.

L4 Traffic Monitor Page

The **Reporting > L4 Traffic Monitor** page is a security-related reporting page that displays information about malware ports and malware sites that the L4 Traffic Monitor has detected during the specified time range. It also displays IP addresses of clients that frequently encounter malware sites.

The L4 Traffic Monitor listens to network traffic that comes in over all ports on the appliance and matches domain names and IP addresses against entries in its own database tables to determine whether to allow incoming and outgoing traffic.

Section	Description
Time Range (drop-down list)	A menu that allows you to choose a time range on which to report.
Top Client IPs	Displays, in graph format, the IP addresses of computers in your organization that most frequently connect to malware sites.
Top Malware Sites	Displays, in graph format, the top malware domains detected by the L4 Traffic Monitor.
Client Source IPs	Displays the IP addresses of computers in your organization that frequently connect to malware sites.
Malware Ports	Displays the ports on which the L4 Traffic Monitor has most frequently detected malware.
Malware Sites Detected	Displays the domains on which the L4 Traffic Monitor most frequently detects malware.

SOCKS Proxy Page

The **Reporting > SOCKS Proxy** Page allows you to view data and trends for transactions processed through the SOCKS proxy, including information about top destinations and users.

Reports by User Location Page

The **Reporting > Reports by User Location** page allows you to find out what activities your local and remote users are conducting.

Activities include:

- URL categories that are being accessed by the local and remote users.
- Anti-Malware activity that is being triggered by sites the local and remote users are accessing.
- Web Reputation of the sites being accessed by the local and remote users.
- Applications that are being accessed by the local and remote users.
- Users (local and remote).
- Domains accessed by local and remote users.

Section	Description
Time Range (drop-down list)	A menu that allows to choose the time range of the data contained in the report.
Total Web Proxy Activity: Remote Users	Displays the activity of your remote users (vertical) over the specified time (horizontal).
Web Proxy Summary	Displays a summary of the activities of the local and remote users on the network.
Total Web Proxy Activity: Local Users	Displays the activity of your remote users (vertical) over the specified time (horizontal).
Suspect Transactions Detected: Remote Users	Displays the suspect transactions that have been detected due to Access Policies defined for remote users (vertical) over the specified time (horizontal).
Suspect Transactions Summary	Displays a summary of suspected transactions of the remote users on the network.
Suspect Transactions Detected: Local Users	Displays the suspect transactions that have been detected due to Access Policies defined for your remote users (vertical) over the specified time (horizontal).
Suspect Transactions Summary	Displays a summary of suspected transactions of the local users on the network.

Web Tracking Page

Use the Web Tracking page to search for and get details about individual transactions or patterns of transactions that may be of concern. Depending on your needs, search in one of the following tabs:

Web Tracking Page	Link to Task
Transactions processed by the Web Proxy	Searching for Transactions Processed by the Web Proxy , on page 10

Web Tracking Page	Link to Task
Transactions processed by the L4 Traffic Monitor	Searching for Transactions Processed by the L4 Traffic Monitor , on page 12
Transactions processed by the SOCKS Proxy	Searching for Transactions Processed by the SOCKS Proxy , on page 12

Searching for Transactions Processed by the Web Proxy

You can use the **Proxy Services** tab on the **Reporting > Web Tracking** page to track and report on web usage for a particular user or for all users.

You can view search results for the type of transactions logged (blocked, monitored, warned, and completed) during a particular time period. You can also filter the data results using several criteria, such as URL category, malware threat, and application.

Note The Web Proxy only reports on transactions that include an ACL decision tag other than OTHER-NONE.

Step 1 Choose **Reporting > Web Tracking**.

Step 2 Click the **Proxy Services** tab.

Step 3 Configure the settings.

Setting	Description
Time Range	Choose the time range on which to report.
User/Client IP	(Optional) Enter an authentication username as it appears in reports or a client IP address that you want to track. You can also enter an IP range in CIDR format. When you leave this field empty, the search returns results for all users.
Website	(Optional) Enter a website that you want to track. When you leave this field empty, the search returns results for all websites.
Transaction Type	Choose the type of transactions that you want to track, either All Transactions, Completed, Blocked, Monitored, or Warned.

Step 4 (Optional) Expand the Advanced section and configure the fields to filter the web tracking results with more advanced criteria.

Setting	Description
URL Category	To filter by a URL category, select **Filter by URL Category** and type the first letter of a URL category by which to filter. Choose the category from the list that appears.

Setting	Description
Application	To filter by an application, select **Filter by Application** and choose an application by which to filter. To filter by an application type, select **Filter by Application Type** and choose an application type by which to filter.
Policy	To filter by the name of the policy responsible for the final decision on this transaction, select **Filter by Action Policy** and enter a policy group name (Access Policy, Decryption Policy, or Data Security Policy) by which to filter. See the description for PolicyGroupName in the section Web Proxy Information in Access Log Files for more information.
Advanced Malware Protection	See About Web Tracking and Advanced Malware Protection Features.
Malware Threat	To filter by a particular malware threat, select **Filter by Malware Threat** and enter a malware threat name by which to filter. To filter by a malware category, select **Filter by Malware Category** and choose a malware category by which to filter.
WBRS	In the WBRS section, you can filter by web reputation score and by a particular web reputation threat. • To filter by web reputation score, select **Score Range** and select the upper and lower values by which to filter. Or, you can filter for websites that have no score by selecting **No Score**. • To filter by web reputation threat, select **Filter by Reputation Threat** and enter a web reputation threat by which to filter.
AnyConnect Secure Mobility	To filter by the location of users (either remote or local), select **Filter by User Location** and choose a user type by which to filter.
User Request	To filter by transactions that were initiated by the client, select **Filter by User-Requested Transactions**. **Note** When you enable this filter, the search results include some "best guess" transactions.

Step 5 Click **Search**.

Results are sorted by time stamp, with the most recent result at the top.

The number in parentheses below the "Display Details" link is the number of related transactions spawned by the user-initiated transaction, such as images loaded, javascripts run, and secondary sites accessed.

Step 6 (Optional) Click **Display Details** in the Transactions column to view more detailed information about each transaction.

Note If you need to view more than 1000 results, click the **Printable Download** link to obtain a CSV file that includes the complete set of raw data, excluding details of related transactions.

Tip If a URL in the results is truncated, you can find the full URL in the access log.

To view details for up to 500 related transactions, click the **Related Transactions** link.

What to do next

- URL Category Set Updates and Reports , on page 5
- Malware Category Descriptions
- About Web Tracking and Advanced Malware Protection Features

Searching for Transactions Processed by the L4 Traffic Monitor

The L4 Traffic Monitor tab on the **Reporting > Web Tracking** page provides details about connections to malware sites and ports. You can search for connections to malware sites by the following types of information:

- Time range
- Site, using IP address or domain
- Port
- IP address associated with a computer in your organization
- Connection type

The first 1000 matching search results are displayed.

Searching for Transactions Processed by the SOCKS Proxy

You can search for transactions that meet a variety of criteria, including blocked or completed transactions; users; and destination domain, IP address, or port.

Step 1 Choose **Web > Reporting > Web Tracking**.

Step 2 Click the **SOCKS Proxy** tab.

Step 3 To filter results, click **Advanced**.

Step 4 Enter search criteria.

Step 5 Click **Search**.

What to do next

SOCKS Proxy Page , on page 8

System Capacity Page

The **Reporting > System Capacity** page displays current and historical information about resource usage on the Web Security appliance.

When choosing time ranges for viewing data on the System Capacity page, the following is important to remember:

- **Hour Report.** The Hour report queries the minute table and displays the exact number of items, such as bytes and connection, that have been recorded by the appliance on an minute by minute basis over a 60 minute period.

- **Day Report.** The Day report queries the hour table and displays the exact number of items, such as bytes and connection, that have been recorded by the appliance on an hourly basis over a 24 hour period. This information is gathered from the hour table.

The Week Report and 30 Days Report work similarly to the Hour and Day Reports.

System Status Page

Use the **Reporting > System Status** page to monitor the System Status. This page displays the current status and configuration of the Web Security appliance.

This Section...	Displays
Web Security Appliance Status	• System uptime • System resource utilization — CPU usage, RAM usage, and percentage of disk space used for reporting and logging. The CPU utilization value shown on this page and the CPU value shown on the system Overview page (Overview Page, on page 1) may differ slightly because they are read separately, at differing moments. RAM usage for a system that is working efficiently may be above 90%, because RAM that is not otherwise in use by the system is used by the web object cache. If your system is not experiencing serious performance issues and this value is not stuck at 100%, the system is operating normally. **Note** Proxy Buffer Memory is one component that uses this RAM.
Proxy Traffic Characteristics	• Transactions per second • Bandwidth • Response time • Cache hit rate • Connections
High Availability	Status of High Availability service.
External Services	• Identity Services Engine

This Section...	Displays
Current Configuration	Web Proxy settings: • Web Proxy Status — enabled or disabled. • Deployment Topology. • Web Proxy Mode — forward or transparent. • IP Spoofing — enabled or disabled. L4 Traffic Monitor settings: • L4 Traffic Monitor Status — enabled or disabled. • L4 Traffic Monitor Wiring. • L4 Traffic Monitor Action — monitor or block. Web Security Appliance Version Information Hardware information

Related Topics

System Capacity Page, on page 12