Web Reporting

Why Is Web Reporting So Important?

A human resources representative wants to ensure that web users on the company network are following acceptable use policies. A network security administrator wants to examine whether the company network is being exposed to malware threats through employees' smartphones. A network operations manager wants to monitor bandwidth usage in order to plan capacity and refine bandwidth control policies.

The web reporting capabilities of the Cisco® IronPort® M-Series and S-Series can provide accurate, real-time information in all of these cases. The reporting and tracking features of the Cisco IronPort M-Series and S-Series can give managers visibility and insight into current operational data to help them refine policies, plan infrastructure, and measure productivity.

Two Purpose-Optimized Databases for Web Reporting and Tracking

The Cisco IronPort S-Series and M-series appliances have two purpose-optimized proprietary databases for reporting and tracking, rather than a single generic database. Appropriate database technology is applied to each query for rapid generation of real-time reports. Reporting on the M-series is designed to operate efficiently and save computing resources.

Web Reporting & Web Tracking: An Integrated System for Real-Time Information

Web tracking maintains a record of individual web transactions with information such as IP/username, domain name, time accessed, and other details. Web reporting aggregates web tracking information in real time and displays it in a high-level, easy-to-use graphical format.

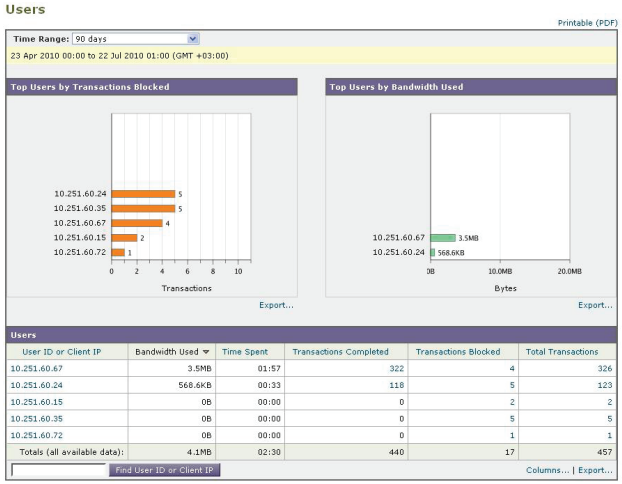
The M-Series appliance aggregates data from all managed appliances in near-real time. The Centralized Web Reporting feature generates high-level reports that allow administrators to understand what is happening on their network.

Each S-Series appliance has on-box reporting functionality as well. On-box reports are the same as those on the M-series, but they only contain data for a particular box.

You can run reports in real time to view an interactive display of system activity over a specific period of time, or you can schedule reports and run them at regular intervals. Web reporting also allows you to export raw data to a file.

Web tracking allows administrators to see transaction-level detail for a particular user, domain, or category. Administrators can drill down and across from high level reports to get more granular information about a user, URL, or transaction.

The Users Report shows Top Users by Transactions Blocked and Top Users by Bandwidth Used. User IPs or Client IDs can be clicked for more granular detail on that particular user's web activity.



How Can Web Reporting & Tracking Improve Employee Productivity?

Web reporting allows human resources administrators to view top websites, URL categories (URL categories of interest may include "Gambling" or "Sports"), and applications accessed, as well as time spent and bandwidth used.

With the web tracking capabilities of the Cisco IronPort M-Series, administrators have granular visibility into employees' usage of resource-intensive applications such as Facebook, YouTube, or instant messaging.

Reporting functionality helps administrators determine the websites, URL categories, and applications that employees can access on company devices.

How Can Web Reporting & Tracking Improve My Organization's IT Security?

Comprehensive reports allow network security administrators to identify and troubleshoot malware threats, potential infections, and botnet activity. With centralized web reporting, system administrators can view the biggest threats to their network, which users are encountering the most blocks or warnings, and which websites and URL categories are posing the biggest risk.

Through centralized web reporting, network security administrators can monitor, troubleshoot, and analyze trends for web-based threats found by the Cisco IronPort Dynamic Vectoring and Streaming (DVS) engine and verdict engines from Sophos, Webroot, and McAfee. These threats can range from adware, browser hijackers, phishing, and pharming attacks to more malicious threats such as rootkits, Trojan horses, worms, system monitors, and keyloggers.

In addition to the DVS and verdict engines, Cisco IronPort S-Series appliances have Web Reputation Filters that analyze web server behavior and assign a reputation score to a URL to determine the likelihood that it contains URL-based malware. Data such as how long a specific domain has been registered, where a website is hosted, or whether a web server is using a dynamic IP address is used to judge the trustworthiness of a given URL. Web tracking functionality gives network security administrators granular information about the reputation scores of websites accessed by users.

Web Reporting

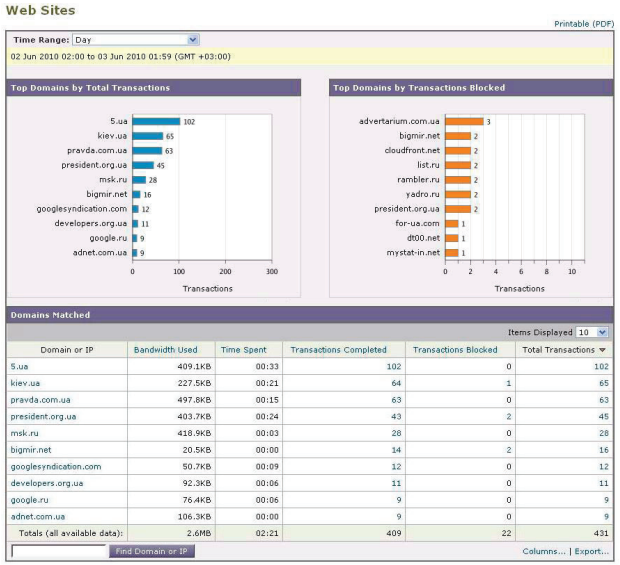
Cisco IronPort S-Series appliances are equipped with a Layer 4 Traffic Monitor that listens to network traffic that comes in over all ports, which can help network security administrators monitor potential botnet activity. Layer 4 Traffic Monitor reports display the ports that have the most malware connections.

How Can Centralized Web Reporting Help My Organization Plan IT Infrastructure?

Network operations personnel can use the system capacity report to track growth over time and plan for system capacity. Over time, web usage volume inevitably rises; appropriate monitoring ensures that additional capacity or configuration changes can be applied proactively.

With centralized web reporting, network administrators can track when web security appliances are exceeding recommended CPU capacity, the number of transactions per second and latency, as well as response time and proxy buffer memory. This allows administrators to determine when configuration optimization or additional appliances are needed.

Top Websites Report shows Top Domains by Total Transactions and Top Domains by Transactions Blocked. Individual domains can be clicked for a detailed report of transactions.



Which Cisco IronPort Security Management Appliance Is Right for My Organization?

- **Cisco IronPort M1070:** Recommended for large enterprises
- **Cisco IronPort M670:** Recommended for midsize companies
- **Cisco IronPort M160:** Recommended for businesses with less than 2000 users

Which Cisco IronPort Web Security Appliance Is Right for My Organization?

- **Cisco IronPort S670:** Recommended for organizations with more than 10,000 users
- **Cisco IronPort S370:** Recommended for organizations with 1000 to 10,000 users
- **Cisco IronPort S160:** Recommended for small businesses and branch offices with up to 1000 users

Based on your organization's tracking needs, the exact sizing for M-Series appliances and S-Series appliances may be different from the information presented here. Reporting is available for 12 months of data on all appliances.

Where Should I Go for More Information?

The best way to understand the benefits of Cisco IronPort products is to participate in the Try Before You Buy program. To receive a fully functional evaluation appliance to test in your network, free for 30 days, visit http://www.ironport.com/how_to_buy/.

C45-622022-00 10/10