Cisco Advanced Web Security Reporting

Introduction

Cisco® Advanced Web Security Reporting Application is a reporting solution that rapidly indexes and analyzes logs produced by Cisco Web Security Appliances (WSA) and Cisco Cloud Web Security (CWS). This tool provides scalable reporting for customers with high traffic and storage needs. It allows reporting administrators to gather detailed insight into web usage and malware threats.

Directory-Group-Based Reporting

With Advanced Web Security Reporting Application, administrators can generate reports based on a group or user ID, as defined within a central authentication server such as Active Directory. Reports can be created easily along functional or geographical boundaries that have been defined by the authentication groups. Roles can be created to allow managers to view reports only for a defined set of directory groups (such as the groups that they manage), protecting the privacy of individuals who are not within those groups.

Detailed Layer 4 Traffic Monitor Visibility

Administrators can run reports on activities on nonweb ports. These Layer 4 Traffic Monitor (L4TM) reports connect hosts associated with particular ports and users, and they can be used to identify malicious behavior on nonstandard ports - behavior that would evade many traditional web-security solutions.

SOCKS Reporting

For customers using Socket Secure (SOCKS) proxy settings, administrators get information about SOCKS traffic.

Historical Data Import

Historical logs can be imported during forensic investigations. Logs from any time period can be imported into the reporting tool for analysis, allowing human resources and legal personnel to conduct forensic investigations spanning several years. Administrators can focus on a specific user's web activity, if needed.

Advanced Malware Protection Reporting

Featuring file reputation scoring and blocking, static and dynamic file analysis (sandboxing), and file retrospection for the continuous analysis of threats, even after they have traversed the WSA and CWS. This reporting application consolidates data provided by the Cisco Advanced Malware Protection solution that produces a single pane of glass for even richer analysis for administrators to gather more detailed insight into web usage and malware threats.

Who Should Use Web Reporting?

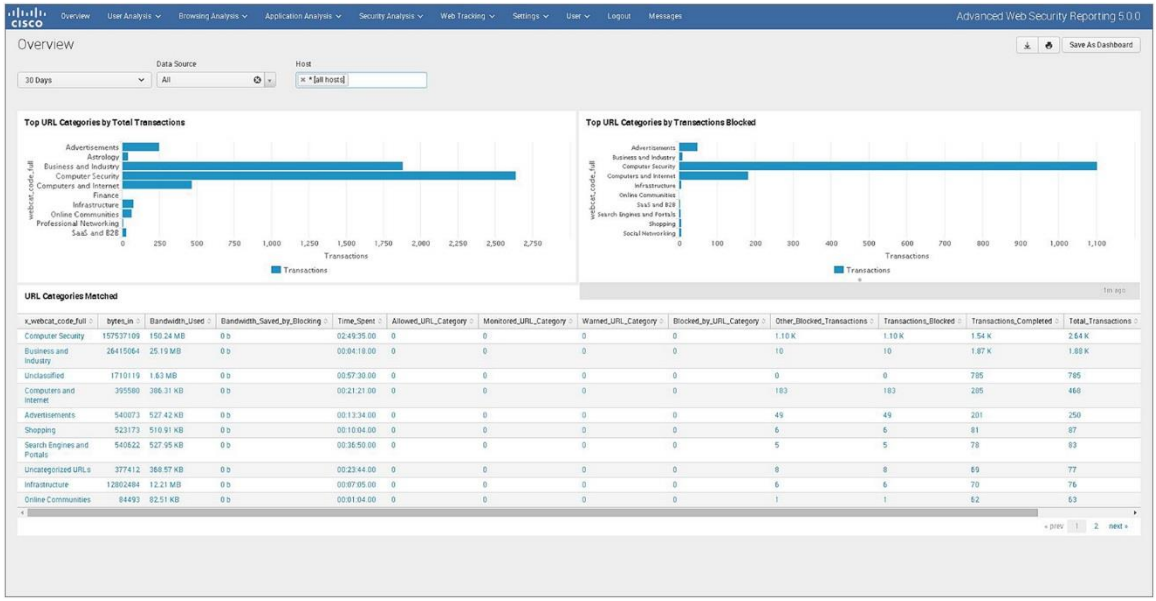
Built-in reporting capabilities on Cisco Web Security and Security Management Appliances fulfill the reporting needs of most Cisco customers. Advanced Web Security Reporting is an alternative reporting solution for customers who need extended storage for high transaction volumes or directory-group-based reporting. It also serves as a "single pane of glass" for customers who have deployed a hybrid web security solution. The Cisco Web Reporting report format is identical to reports already available on Cisco S-Series and M-Series appliances.

What Does the Latest Release of Cisco Web Reporting Include?

- **Unified Web Security Reporting:** The Cisco Advanced Web Security Reporting Application integrates diverse information into a single display for easier monitoring of your web security, regardless of deployment (Figure 1). The reporting application polls log data collected from multiple Cisco WSAs and CWS for predefined reports. Customers can also perform ad-hoc searches using the flash timeline view and web-tracking forms.
- **Scale and Performance:** Release 4.0 of the Advanced Cisco Web Security Reporting Application aligns with the introduction of data tiers across seat bands, allowing for purchase flexibility based on daily log volume requirements.
  - Low tier: This version meets the limited data needs of current customers who use 2 MB of data per user per day.
  - High tier: This version is for Hybrid Web Security and Enterprise License Agreement (ELA) customers whose users have higher data requirements (6 MB per user per day).

* Please note that these options include only a license for Web Security Reporting. The offering does not include Configuration and Policy Management licenses. For example, it does not include the SMA, the Cisco CWS Log Extraction license, which is required for standalone CWS application reporting, or unified Cisco WSA and CWS reporting using this solution.

Figure 1. Reports for URL Categories and Transactions Blocked



System Requirements

Advanced Web Security Reporting runs on Microsoft Windows and Red Hat Linux. Refer to “Requirements for Advanced Web Security Reporting” section in release notes for details on the system requirements for specific release of Advanced Web Security Reporting application.

Please talk to your Cisco account team and refer to the documentation to understand the hardware specifications you will need to run the Cisco Web Reporting Application at your organization.

Cisco Capital

Financing to Help You Achieve Your Objectives

Cisco Capital can help you acquire the technology you need to achieve your objectives and stay competitive. We can help you reduce CapEx. Accelerate your growth. Optimize your investment dollars and ROI. Cisco Capital financing gives you flexibility in acquiring hardware, software, services, and complementary third-party equipment. And there’s just one predictable payment. Cisco Capital is available in more than 100 countries. Learn more.

For More Information

More information can be found by referencing the ordering guide, release notes, and user guide.

Get Started: Download the Single Installer for Linux and Windows.

Questions: Please contact your Cisco Partner Account Manager.

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 C78-729104-04 07/16