Advanced Web Reporting for the Cisco S-Series Web Security Appliance

Introduction

Advanced Web Reporting is an off-box reporting solution that rapidly indexes and analyzes logs produced by Cisco® S-Series Web Security Appliances. This Splunk-based tool provides scalable reporting for customers with high traffic and storage needs, enabling reporting administrators to gather detailed insight into web usage and malware threats.

Directory-Group-Based Reporting

With Advanced Web Reporting, administrators can generate reports based on a group or user ID as defined within a central authentication server such as Active Directory. Reports can easily be created 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 ones that they manage), protecting the privacy of individuals not within those groups.

Detailed Layer 4 Traffic Monitor (L4TM) Visibility

Advanced Web Reporting enables administrators to run reports on activities on non-web ports. These L4TM reports connect hosts associated with particular ports and users, and can be used to identify malicious behavior on non-standard ports, which would evade many traditional web security solutions.

SOCKS Reporting

For customers using SOCKS proxy settings, Advanced Web Reporting enables administrators to get information about SOCKS traffic.

Historical Data Import

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

Who Should Use Advanced Web Reporting?

On-box reporting on Cisco M-Series and S-Series appliances fulfills the reporting needs of the majority of customers. Advanced Web Reporting is an alternative reporting solution for customers that need extended storage for high transaction volumes or directory-group-based reporting. Advanced Web Reporting’s report format is identical to reports available on-box on the S-Series and M-Series appliances.

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

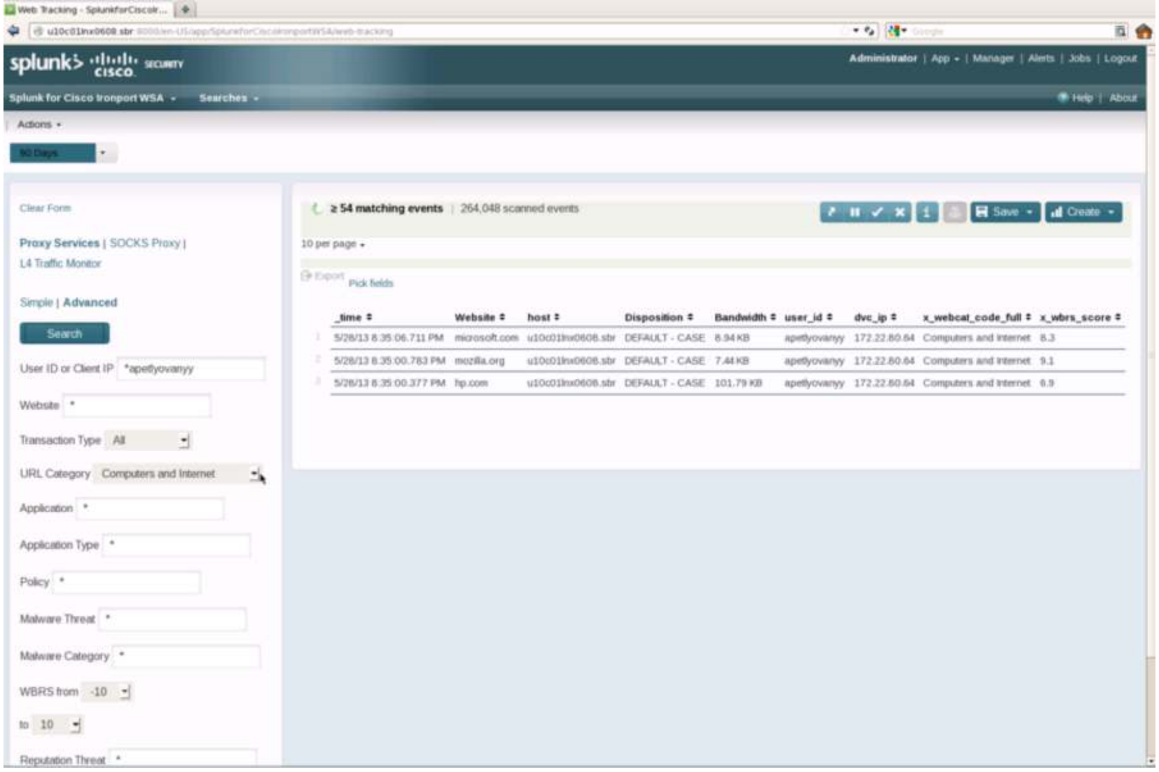
What does the latest release of Cisco Advanced Web Reporting include?

New reporting functionality. Advanced Web Reporting now provides the same reports as a Cisco Web Security Appliance running AsyncOS® 7.7. Reports include SOCKS reports and web tracking and form-based search for SOCKS and L4TM transactions.

Support for Splunk 5.0. Advanced Web Reporting is supported on the Splunk 5.0 platform.

Heavy-duty performance tests. Cisco tested the WSA Advanced Web Reporting feature with much larger volumes of data, and published report load times. These test results can be found in the “Sizing and Scaling Recommendations” section at the beginning of the user guide.

Figure 1. Splunk Reports for URL Categories and Transactions Blocked


Web Tracking - SplunkforCiscoIr...
u10c01lnx0608.sbr
splunk> cisco SECURITY
Administrator | App ▾ | Manager | Alerts | Jobs | Logout
Splunk for Cisco Ironport WSA ▾
Searches ▾
Help | About
Actions ▾
90 Days
Clear Form
Proxy Services | SOCKS Proxy | L4 Traffic Monitor
Simple | Advanced
Search
10 per page ▾
Export
Pick fields
Save ▾
Create ▾

≥ 54 matching events | 264,048 scanned events

User ID or Client IP: *apetlyovanyy

Website: *

Transaction Type: All

URL Category: Computers and Internet

Application: *

Application Type: *

Policy: *

Malware Threat: *

Malware Category: *

WBRS from: -10

to: 10

Reputation Threat: *

	_time	Website	host	Disposition	Bandwidth	user_id	dvc_ip	x_webcat_code_full	x_wbrs_score
1	5/28/13 8:35:06.711 PM	microsoft.com	u10c01lnx0608.sbr	DEFAULT - CASE	8.94 KB	apetlyovanyy	172.22.80.64	Computers and Internet	8.3
2	5/28/13 8:35:00.783 PM	mozilla.org	u10c01lnx0608.sbr	DEFAULT - CASE	7.44 KB	apetlyovanyy	172.22.80.64	Computers and Internet	9.1
3	5/28/13 8:35:00.377 PM	hp.com	u10c01lnx0608.sbr	DEFAULT - CASE	101.79 KB	apetlyovanyy	172.22.80.64	Computers and Internet	6.9

System Requirements

Advanced Web Reporting runs on Windows and Red Hat Linux. There is no support for virtualization for production instances of Advanced Web Reporting. Reference hardware can be commodity-grade with the minimum specifications below.

- Intel x86 64-bit chip architecture with 2 CPUs, 4 cores per CPU, and 2.5 to 3 GHz per core
- 16 GB RAM
- (4) 300-GB SAS hard disks at 10,000 rpm each in RAID 10 (800 IOPS or better)
- Gigabit Ethernet network interface card (NIC); a second NIC for a management network is recommended

Note: These hardware specifications are recommended for organizations with more than 25,000 users.

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.

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

For More Information

Contact your Cisco account team to request an evaluation version of Advanced Web Reporting.

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.**

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Printed in USA

C78-729104-00 07/13

© 2013 Cisco and/or its affiliates. All rights reserved. This document is Cisco Public.