Splunk for Cisco IronPort WSA: User Guide

Table of Contents

Introduction:

This manual covers the Splunk Cisco IronPort WSA Reporting Application for users of the application. This application provides reports and dashboards that can give you insight into data from the IronPort Web Security Appliance (WSA).

Supplement to Existing Splunk Documentation:

This guide serves a supplement to the existing body of documentation existing at http://docs.splunk.com.

It is not intended to replace existing Splunk materials or techniques regarding user experience. This guide will serve as a supplement by reviewing functionality as it relates to this application.

Logging In:

Information regarding login credentials and URL should be procured from the Splunk administrator(s). The credential should be entered at the Splunk Login page to access the SplunkforCiscoIronportWSA application.

Report Usage:

Choosing a Time Range:

Each report contains a Time Range Picker. This dropdown box (located in the report's upper left hand corner) allows you to specify the time range from which to pull reports. You may choose from pre-defined ranges or select a custom range. Smaller time range are generally more preferred – especially on the Web Tracking (ad hoc search) and L4TM reports which do not leverage summarized data optimization and report directly against raw data.

Find Data:

There are many pre-defined reports (described in below "Report Descriptions" section).

Additionally, the drilldown reports will allow you to specify specific information. For example, the User Drilldown report allows you to type the name of a specific user and re-run the report. Alternatively, this may be accomplished by clicking on a user ID wherever it is displayed in a table on any report. This is true of all drilldown reports.

Another way to search data is to navigate to the Web Tracking report. The advanced link will present more options narrow the scope of your search compared to the *simple* version which contains fewer options

Export Data

There are two options for manually exporting data.

Option 1

You may go to the Web Tracking form, search for desired data, and click the Export button in the upper right hand corner.

Option 2

If your Splunk administrator enabled PDF you may save any report as a PDF by choosing that option in the upper left corner of the report.

Tables:

Sorting Columns

You may click on any column header to sort by that column. Clicking on a column header again will reverse the order of the sort.

Choosing Fields

You may use the *Pick fields* link anywhere it exists to choose the columns displayed in a report's table. This is especially useful on the web tracking report to display individual URLs visited for specific domains and other information that is initially hidden to make the layout easier to navigate.

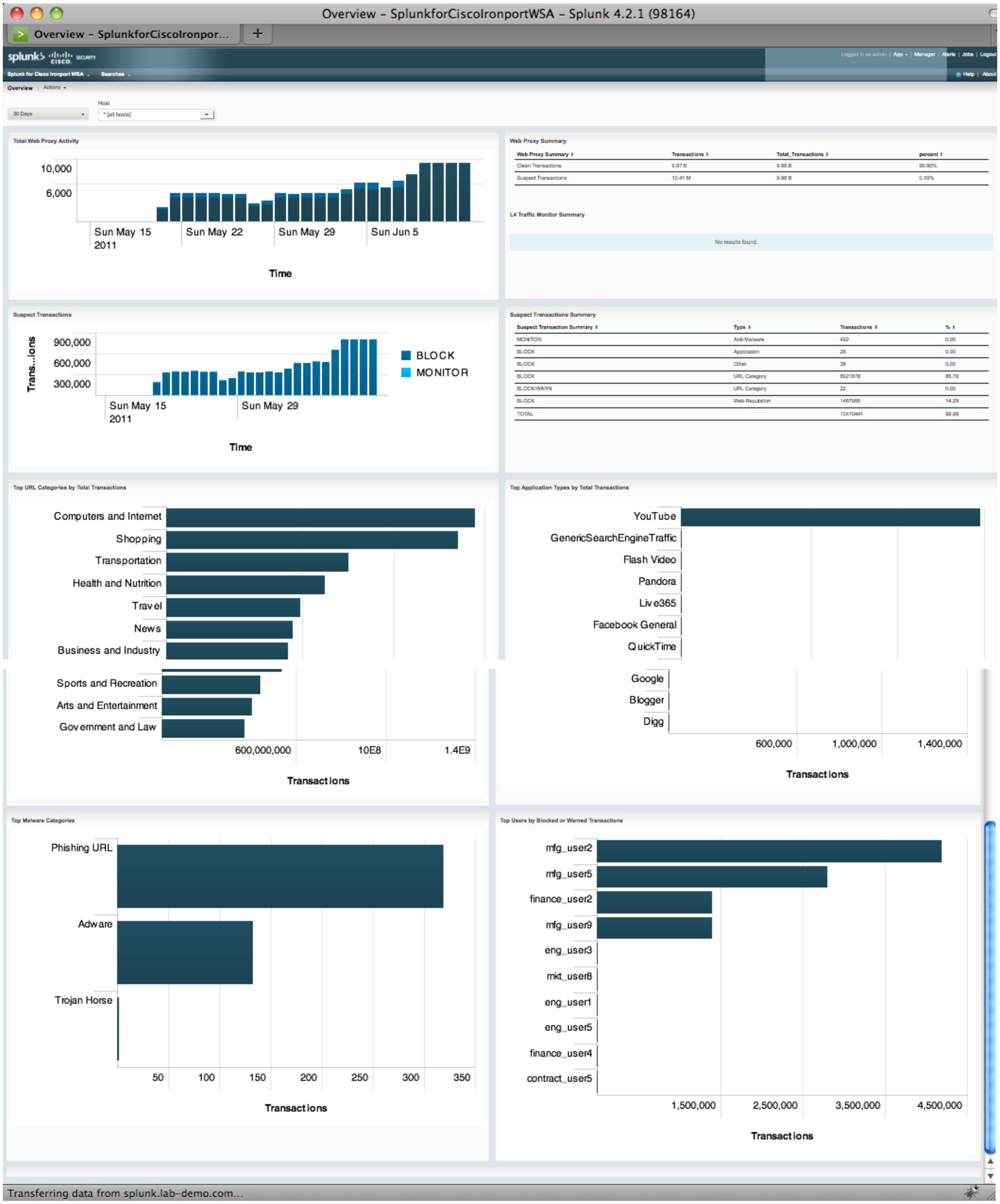
Drilling In

All tables that contain hyperlinked data may be clicked on to drilldown further. The target page will vary based on which column in the table was clicked (e.g. clicking on a user will take you to the user drilldown).

Report Descriptions:

Overview

The Overview report contains a high level view of appliances reporting to Splunk. The top of the report contains graphs and tables aggregating information received from access logs and L4TM logs. The bottom portion of the report details usage by user ID or IP address.



Web Proxy Summary

Web Proxy Summary	Transactions	Total_Transactions	percent
Clean Transactions	9.97 B	9.98 B	99.90%
Suspect Transactions	10.41 M	9.98 B	0.10%

L4 Traffic Monitor Summary

No results found.

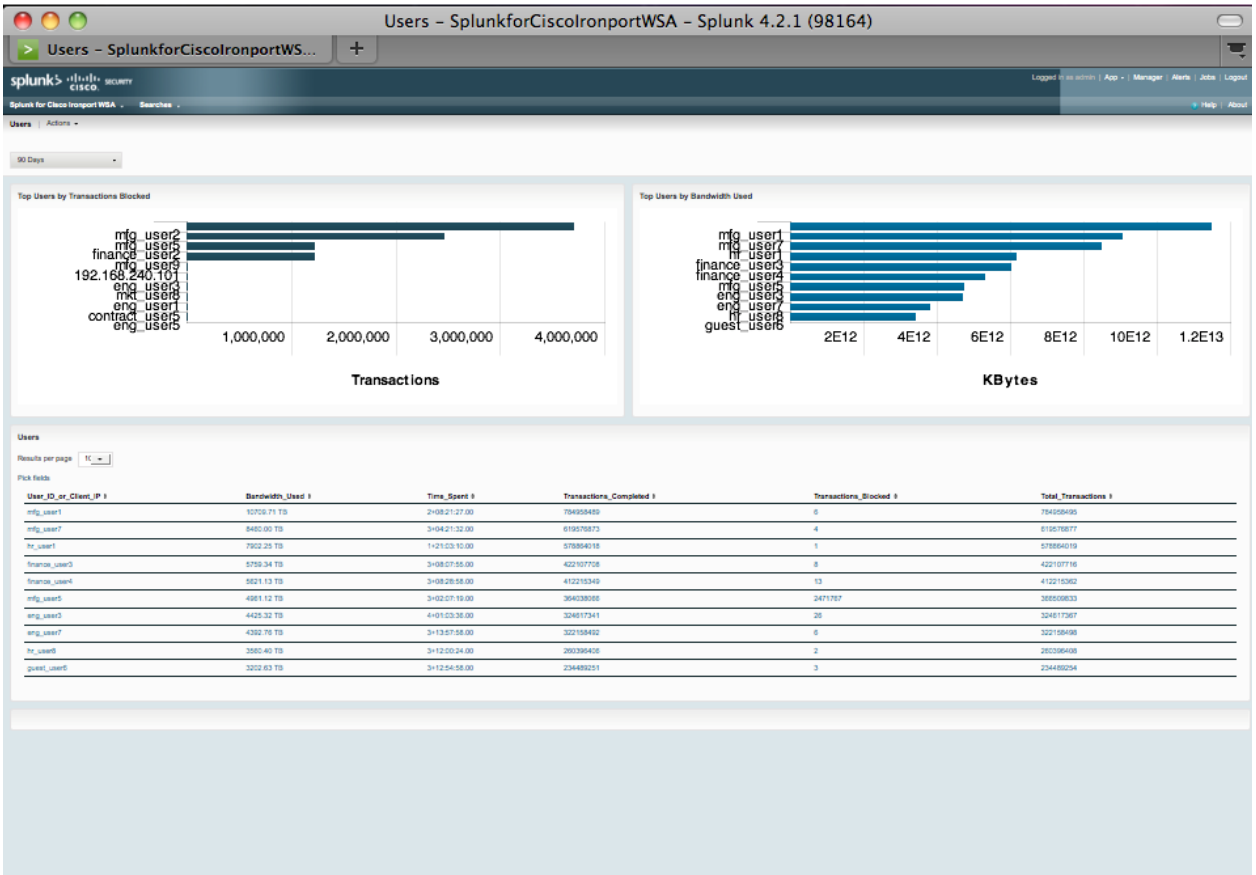
Suspect Transactions Summary

Suspect Transaction Summary	Type	Transactions	%
MONITOR	Anti-Malware	492	0.00
BLOCK	Application	26	0.00
BLOCK	Other	38	0.00
BLOCK	URL Category	8921878	85.70
BLOCK/WARN	URL Category	22	0.00
BLOCK	Web Reputation	1487985	14.29
TOTAL		10410441	99.99

Transferring data from splunk.lab-demo.com...

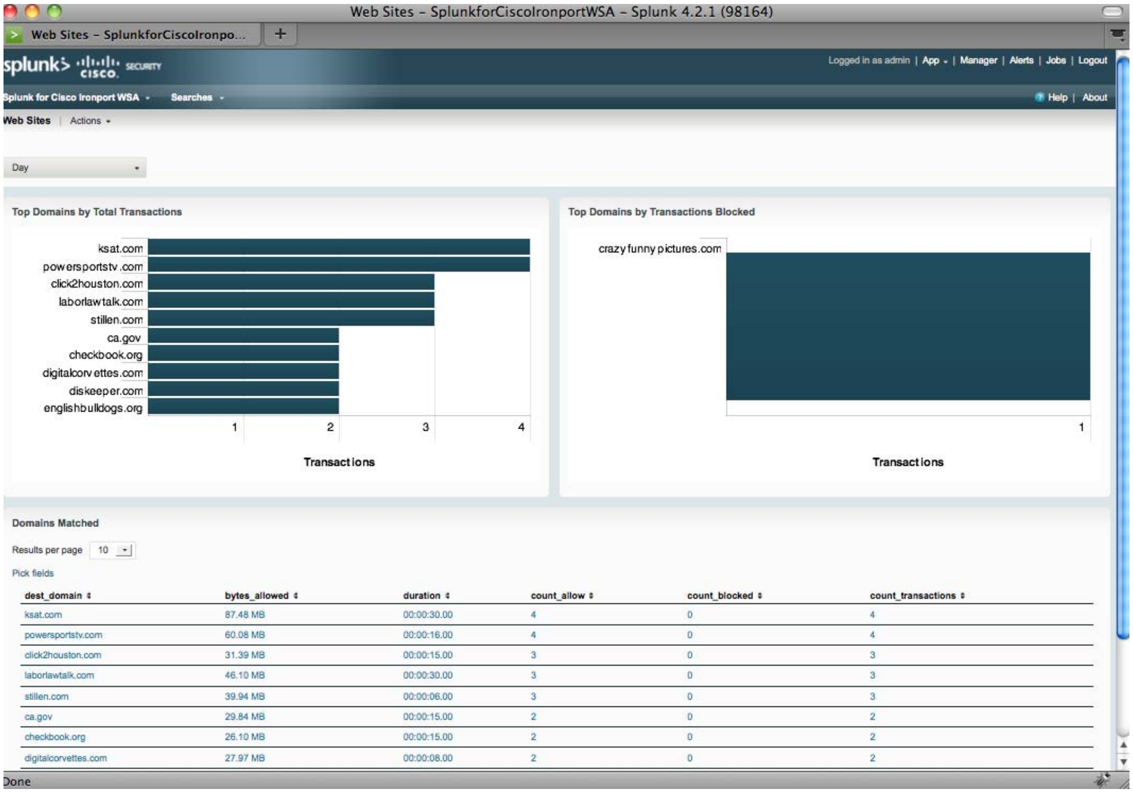
Users

The Users report shows usage information about all users. The drilldown report may be used to report on individuals.



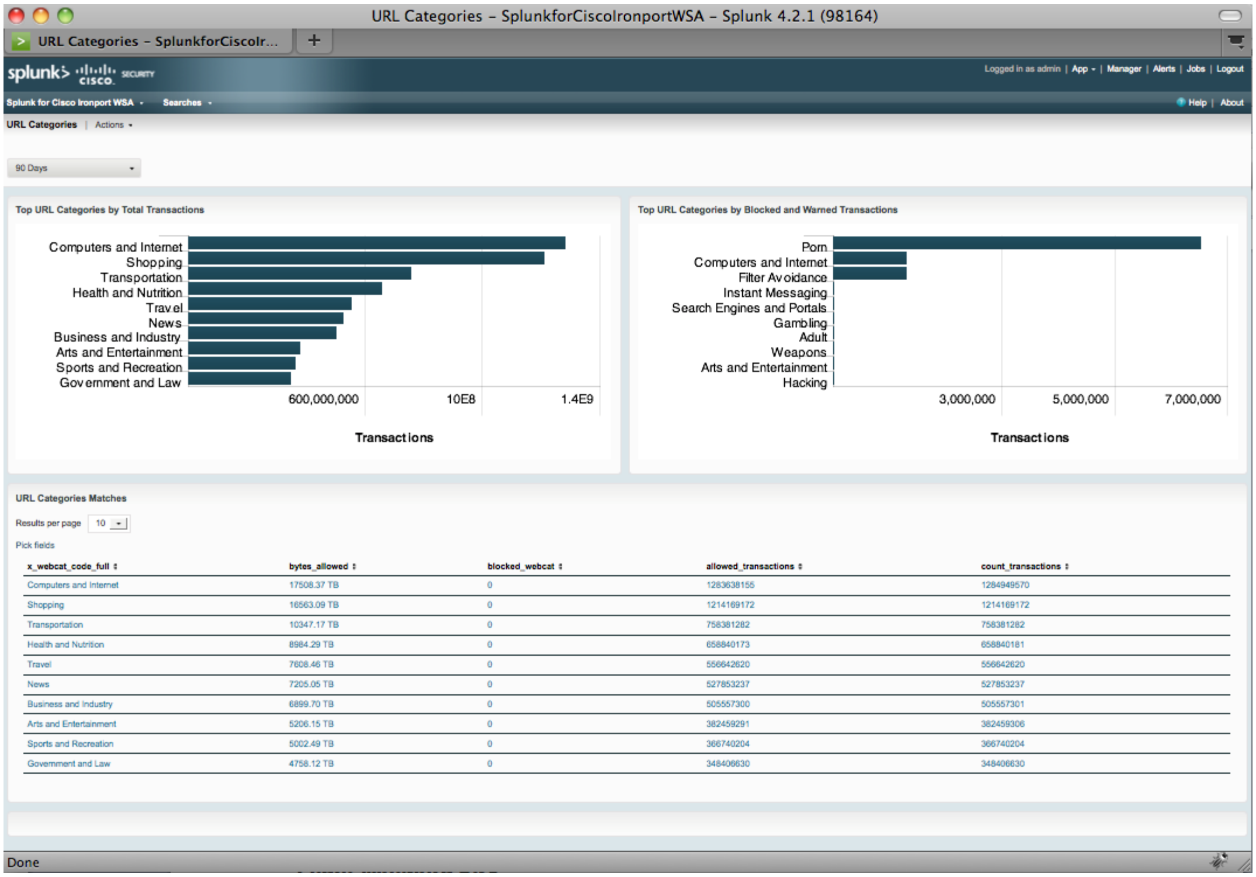
User_ID_or_Client_IP	Bandwidth_Used	Time_Spent	Transactions_Completed	Transactions_Blocked	Total_Transactions
mfg_user1	10709.71 TB	2+08:21:27.00	784958489	6	784958495
mfg_user7	8480.00 TB	3+04:21:32.00	619576873	4	619576877
hr_user1	7902.25 TB	1+21:03:10.00	578864018	1	578864019
finance_user3	5759.34 TB	3+08:07:55.00	422107708	8	422107716
finance_user4	5621.13 TB	3+08:28:58.00	412215349	13	412215362
mfg_user5	4961.12 TB	3+02:07:19.00	364038066	2471767	366509833
eng_user3	4425.32 TB	4+01:03:36.00	324617341	26	324617367
eng_user7	4392.76 TB	3+13:57:58.00	322158492	6	322158498
hr_user8	3580.40 TB	3+12:00:24.00	260396406	2	260396408
guest_user6	3202.63 TB	3+12:54:58.00	234489251	3	234489254

Web Sites



dest_domain	bytes_allowed	duration	count_allow	count_blocked	count_transactions
ksat.com	87.48 MB	00:00:30.00	4	0	4
powersportstv.com	60.08 MB	00:00:16.00	4	0	4
click2houston.com	31.39 MB	00:00:15.00	3	0	3
laborlawtalk.com	46.10 MB	00:00:30.00	3	0	3
stillen.com	39.94 MB	00:00:06.00	3	0	3
ca.gov	29.84 MB	00:00:15.00	2	0	2
checkbook.org	26.10 MB	00:00:15.00	2	0	2
digitalcorvettes.com	27.97 MB	00:00:08.00	2	0	2

URL Categories



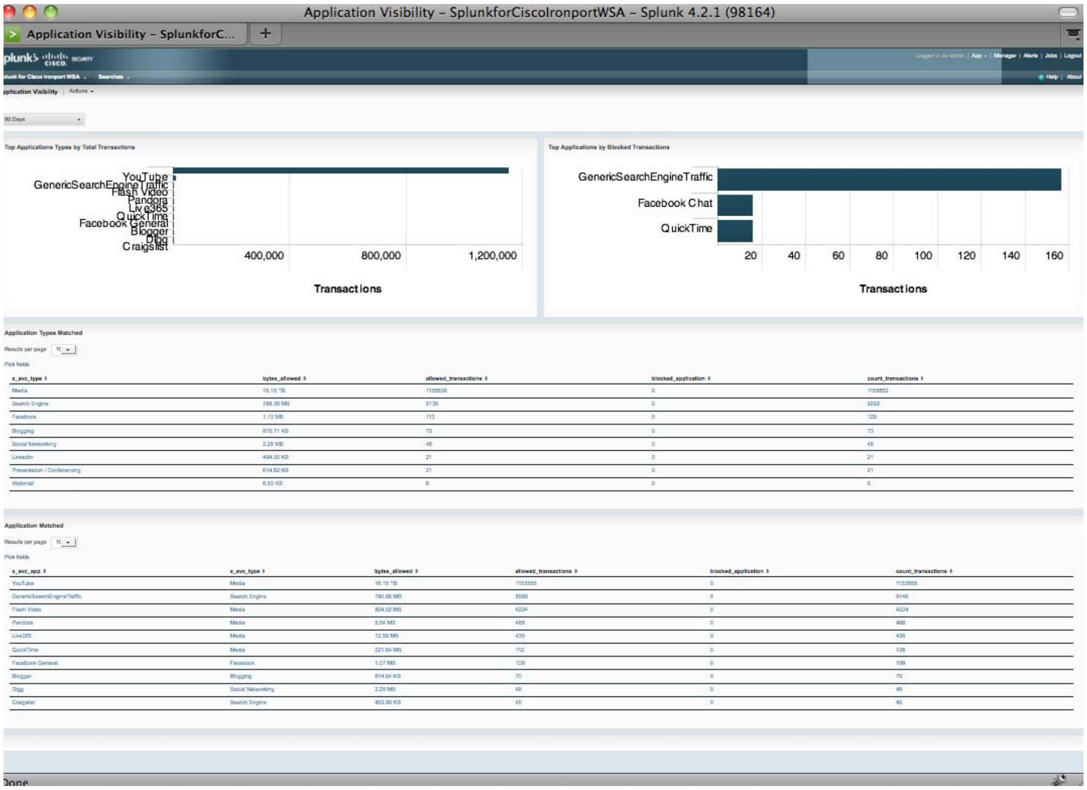
URL Categories Matches

Results per page 10

Pick fields

x_webcat_code_full	bytes_allowed	blocked_webcat	allowed_transactions	count_transactions
Computers and Internet	17508.37 TB	0	1283638155	1284949570
Shopping	16563.09 TB	0	1214169172	1214169172
Transportation	10347.17 TB	0	758381282	758381282
Health and Nutrition	8984.29 TB	0	658840173	658840181
Travel	7608.46 TB	0	556642620	556642620
News	7205.05 TB	0	527853237	527853237
Business and Industry	6899.70 TB	0	505557300	505557301
Arts and Entertainment	5206.15 TB	0	382459291	382459306
Sports and Recreation	5002.49 TB	0	366740204	366740204
Government and Law	4758.12 TB	0	348406630	348406630

Application Visibility


Application Visibility – SplunkforCiscoIronportWSA – Splunk 4.2.1 (98164)
Application Visibility – SplunkforC...
plunk> cisco SECURITY
Logged in as admin | App | Manager | Alerts | Jobs | Logout
lunk for Cisco Ironport WSA
Searches
Help | About
pplication Visibility | Actions
90 Days
Top Applications Types by Total Transactions
YouTube
GenericSearchEngineTraffic
Flash Video
Pandora
Live365
QuickTime
Facebook General
Blogger
Digg
Craigslist
400,000
800,000
1,200,000
Transactions
Top Applications by Blocked Transactions
GenericSearchEngineTraffic
Facebook Chat
QuickTime
20
40
60
80
100
120
140
160
Transactions
Done

Application Types Matched

Results per page 10

Pick fields

x_avc_type	bytes_allowed	allowed_transactions	blocked_application	count_transactions
Media	16.15 TB	1158836	0	1158852
Search Engine	198.39 MB	9136	0	9292
Facebook	1.13 MB	113	0	129
Blogging	815.71 KB	73	0	73
Social Networking	2.29 MB	48	0	48
LinkedIn	494.00 KB	21	0	21
Presentation / Conferencing	614.82 KB	21	0	21
Webmail	6.53 KB	8	0	8

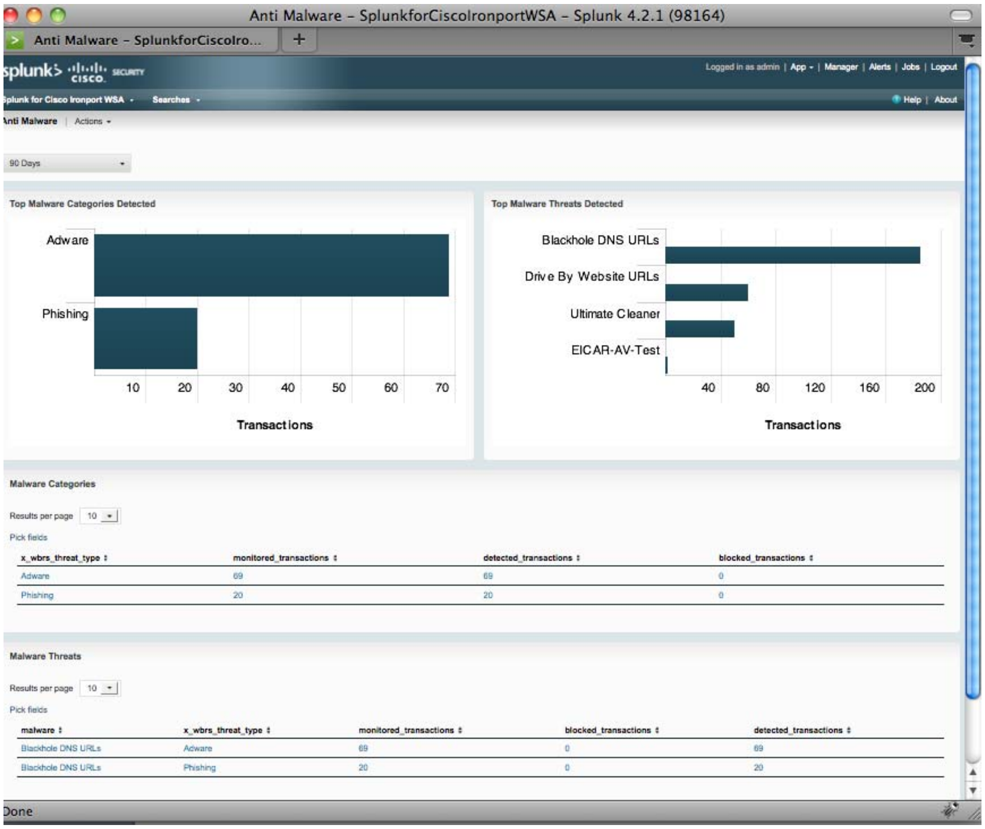
Application Matched

Results per page 10

Pick fields

x_avc_app	x_avc_type	bytes_allowed	allowed_transactions	blocked_application	count_transactions
YouTube	Media	16.15 TB	1153555	0	1153555
GenericSearchEngineTraffic	Search Engine	190.66 MB	8989	0	9146
Flash Video	Media	804.02 MB	4224	0	4224
Pandora	Media	5.54 MB	488	0	488
Live365	Media	12.59 MB	435	0	435
QuickTime	Media	221.64 MB	112	0	128
Facebook General	Facebook	1.07 MB	109	0	109
Blogger	Blogging	814.54 KB	70	0	70
Digg	Social Networking	2.29 MB	48	0	48
Craigslist	Search Engine	453.99 KB	45	0	45

Anti-Malware


Anti Malware – SplunkforCiscoIronportWSA – Splunk 4.2.1 (98164)
Anti Malware – SplunkforCiscoIro...
Logged in as admin | App | Manager | Alerts | Jobs | Logout
Splunk for Cisco Ironport WSA
Searches
Help | About
Anti Malware | Actions
90 Days
Top Malware Categories Detected
Adware
Phishing
10
20
30
40
50
60
70
Transactions
Top Malware Threats Detected
Blackhole DNS URLs
Drive By Website URLs
Ultimate Cleaner
EICAR-AV-Test
40
80
120
160
200
Transactions
Done

Malware Categories

Results per page 10

Pick fields

x_wbrs_threat_type	monitored_transactions	detected_transactions	blocked_transactions
Adware	69	69	0
Phishing	20	20	0

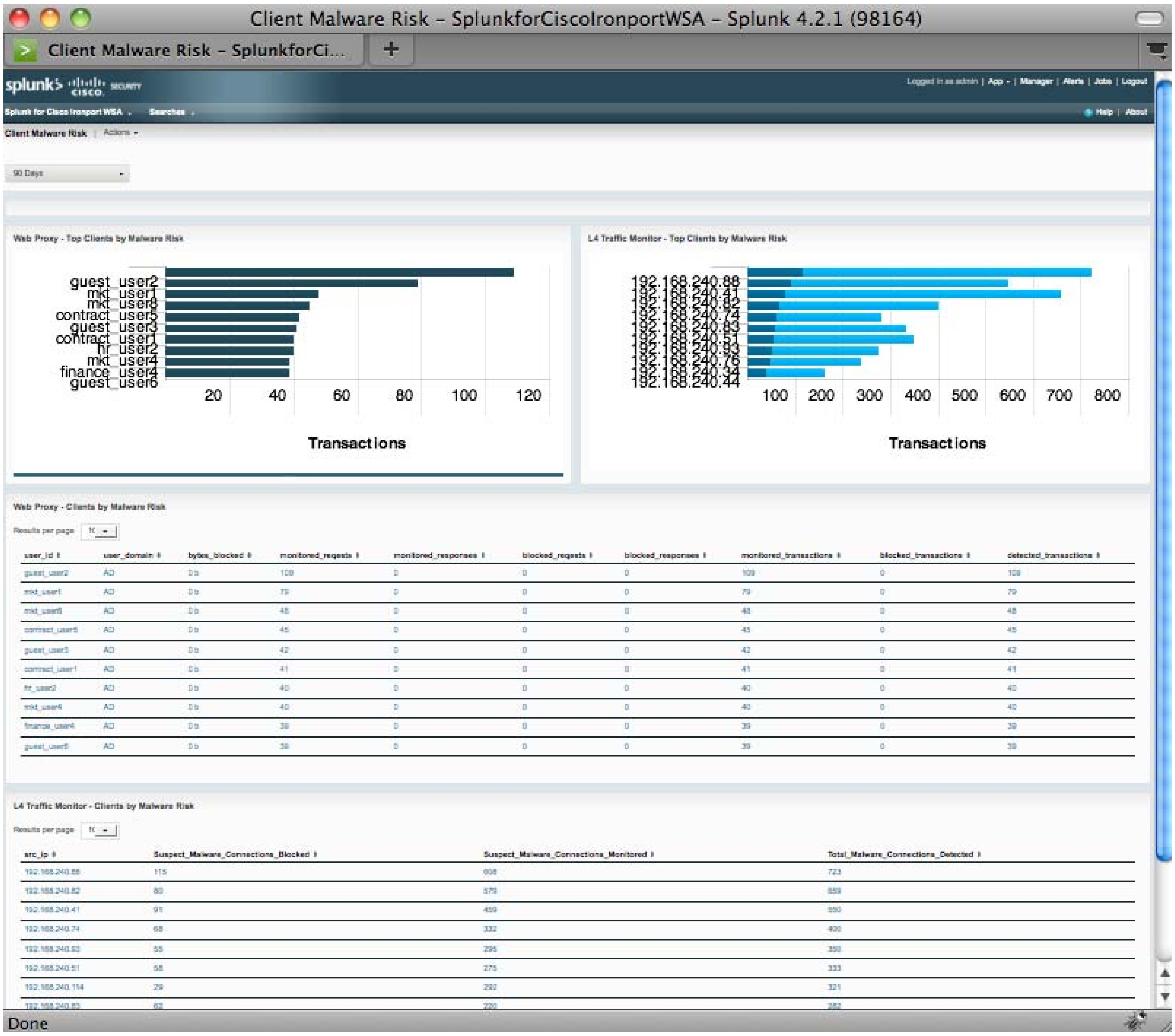
Malware Threats

Results per page 10

Pick fields

malware	x_wbrs_threat_type	monitored_transactions	blocked_transactions	detected_transactions
Blackhole DNS URLs	Adware	69	0	69
Blackhole DNS URLs	Phishing	20	0	20

Client Malware Risk



Web Proxy - Clients by Malware Risk

Results per page 10

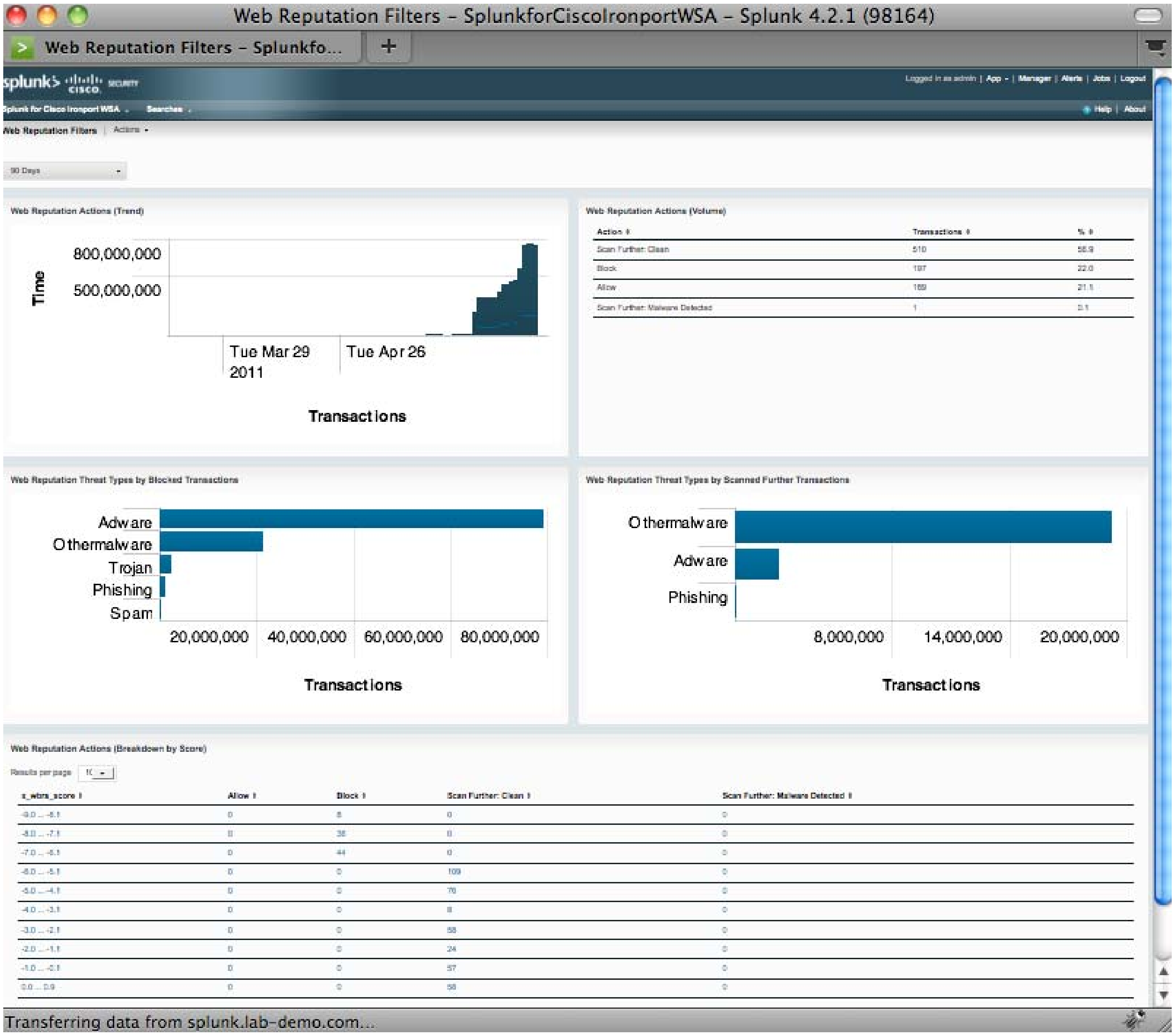
user_id	user_domain	bytes_blocked	monitored_reqests	monitored_responses	blocked_reqests	blocked_responses	monitored_transactions	blocked_transactions	detected_transactions
guest_user2	AD	0 b	109	0	0	0	109	0	109
mkt_user1	AD	0 b	79	0	0	0	79	0	79
mkt_user8	AD	0 b	48	0	0	0	48	0	48
contract_user5	AD	0 b	45	0	0	0	45	0	45
guest_user3	AD	0 b	42	0	0	0	42	0	42
contract_user1	AD	0 b	41	0	0	0	41	0	41
hr_user2	AD	0 b	40	0	0	0	40	0	40
mkt_user4	AD	0 b	40	0	0	0	40	0	40
finance_user4	AD	0 b	39	0	0	0	39	0	39
guest_user6	AD	0 b	39	0	0	0	39	0	39

L4 Traffic Monitor - Clients by Malware Risk

Results per page 10

src_ip	Suspect_Malware_Connections_Blocked	Suspect_Malware_Connections_Monitored	Total_Malware_Connections_Detected
192.168.240.88	115	608	723
192.168.240.82	80	579	659
192.168.240.41	91	459	550
192.168.240.74	68	332	400
192.168.240.83	55	295	350
192.168.240.51	58	275	333
192.168.240.114	29	292	321
192.168.240.93	62	220	282

Web Reputation Filters


Web Reputation Filters – SplunkforCiscoIronportWSA – Splunk 4.2.1 (98164)
Web Reputation Filters – Splunkfo...
splunk> cisco SECURITY
Logged in as admin | App | Manager | Alerts | Jobs | Logout
Splunk for Cisco Ironport WSA
Searches
Help | About
Web Reputation Filters
Actions
90 Days

Web Reputation Actions (Trend)

Web Reputation Actions (Volume)

Action	Transactions	%
Scan Further: Clean	510	55.9
Block	197	22.0
Allow	189	21.1
Scan Further: Malware Detected	1	0.1

Web Reputation Threat Types by Blocked Transactions

Web Reputation Threat Types by Scanned Further Transactions

Web Reputation Actions (Breakdown by Score)

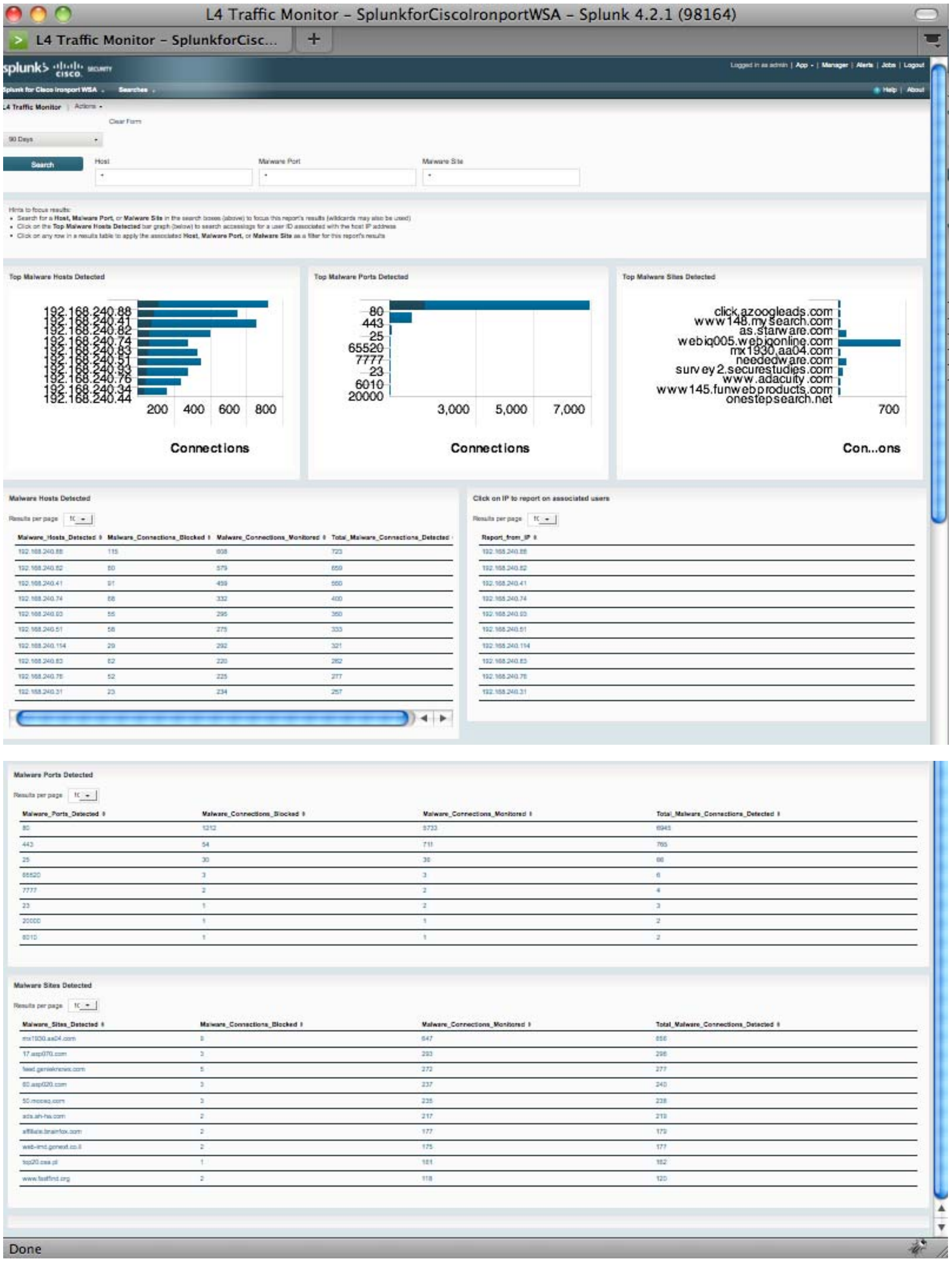
Results per page 10

x_wbrs_score	Allow	Block	Scan Further: Clean	Scan Further: Malware Detected
-9.0 ... -8.1	0	8	0	0
-8.0 ... -7.1	0	38	0	0
-7.0 ... -6.1	0	44	0	0
-6.0 ... -5.1	0	0	109	0
-5.0 ... -4.1	0	0	76	0
-4.0 ... -3.1	0	0	8	0
-3.0 ... -2.1	0	0	58	0
-2.0 ... -1.1	0	0	24	0
-1.0 ... -0.1	0	0	57	0
0.0 ... 0.9	0	0	58	0

Transferring data from splunk.lab-demo.com...

L4 Traffic Monitor

The L4 Traffic Monitor report is a aggregate and drilldown report in one. Drilldowns from this page will refresh this page with the targeted drilldown information loaded. This report has tips for more powerful uses (i.e. correlating L4TM data using accesslog data using this report).



90 Days

Host: *

Malware Port: *

Malware Site: *

Hints to focus results:

- Search for a **Host, Malware Port,** or **Malware Site** in the search boxes (above) to focus this report's results (wildcards may also be used)
- Click on the **Top Malware Hosts Detected** bar graph (below) to search accesslogs for a user ID associated with the host IP address
- Click on any row in a results table to apply the associated **Host, Malware Port,** or **Malware Site** as a filter for this report's results

Malware Hosts Detected

Results per page 10

Malware_Hosts_Detected	Malware_Connections_Blocked	Malware_Connections_Monitored	Total_Malware_Connections_Detected
192.168.240.88	115	608	723
192.168.240.82	80	579	659
192.168.240.41	91	459	550
192.168.240.74	68	332	400
192.168.240.93	55	295	350
192.168.240.51	58	275	333
192.168.240.114	29	292	321
192.168.240.83	62	220	282
192.168.240.76	52	225	277
192.168.240.31	23	234	257

Click on IP to report on associated users

Results per page 10

Report_from_IP
192.168.240.88
192.168.240.82
192.168.240.41
192.168.240.74
192.168.240.93
192.168.240.51
192.168.240.114
192.168.240.83
192.168.240.76
192.168.240.31

Malware Ports Detected

Results per page 10

Malware_Ports_Detected	Malware_Connections_Blocked	Malware_Connections_Monitored	Total_Malware_Connections_Detected
80	1212	5733	6945
443	54	711	765
25	30	38	68
65520	3	3	6
7777	2	2	4
23	1	2	3
20000	1	1	2
6010	1	1	2

Malware Sites Detected

Results per page 10

Malware_Sites_Detected	Malware_Connections_Blocked	Malware_Connections_Monitored	Total_Malware_Connections_Detected
mx1930.aa04.com	9	647	656
17.asp070.com	3	293	296
feed.genieknows.com	5	272	277
60.asp020.com	3	237	240
50.mooaq.com	3	235	238
ads.ah-ha.com	2	217	219
affiliate.brainfox.com	2	177	179
web-imd.gonext.co.il	2	175	177
top20.osa.pl	1	181	182
www.fastfind.org	2	118	120

Reports by Drilldown

Below is a list of the drilldown reports available. They have detailed information compared to the aggregate parent reports from which they came. In addition to accessing them by clicking into them from parent reports – they may also be accessed via the menu system and manual searches may be done for individual components…

Malware Category Drilldown

Malware Threat Drilldown

Application Drilldown

Application Type Drilldown

Domain Drilldown

URL Category Drilldown

User Drilldown

Reports by Location

These reports are available via the menu and are similar to their parent reports PLUS they contain information as broken down by location of user…

Overview by Location

URL Categories by Location

Anti-Malware by Location

Web Reputation Filters by Location

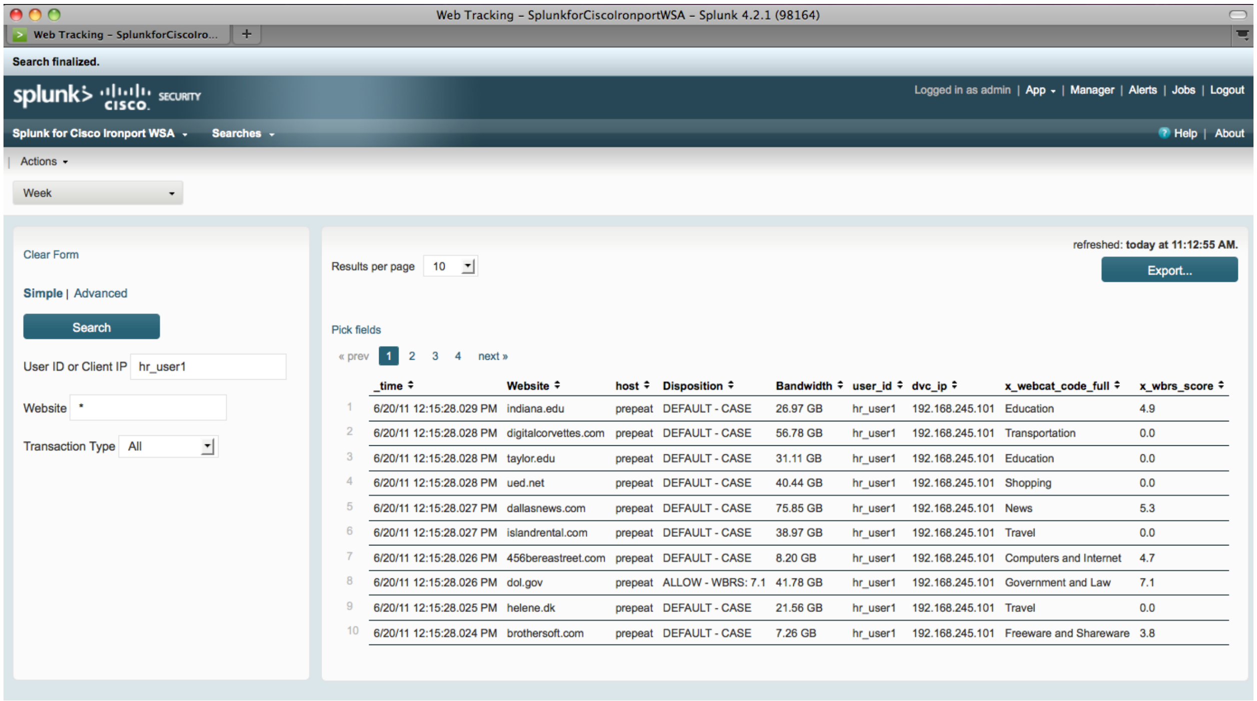
Application Visibility by Location

Users by Location

Websites by Location

Web Tracking (form based search)

Simple



Web Tracking – SplunkforCiscoIronportWSA – Splunk 4.2.1 (98164)
Web Tracking – SplunkforCiscoIro...
Search finalized.
splunk> cisco SECURITY
Logged in as admin | App | Manager | Alerts | Jobs | Logout
Splunk for Cisco Ironport WSA
Searches
Help | About
Actions
Week
Clear Form
Simple | Advanced
Search

User ID or Client IP: hr_user1

Website: *

Transaction Type: All

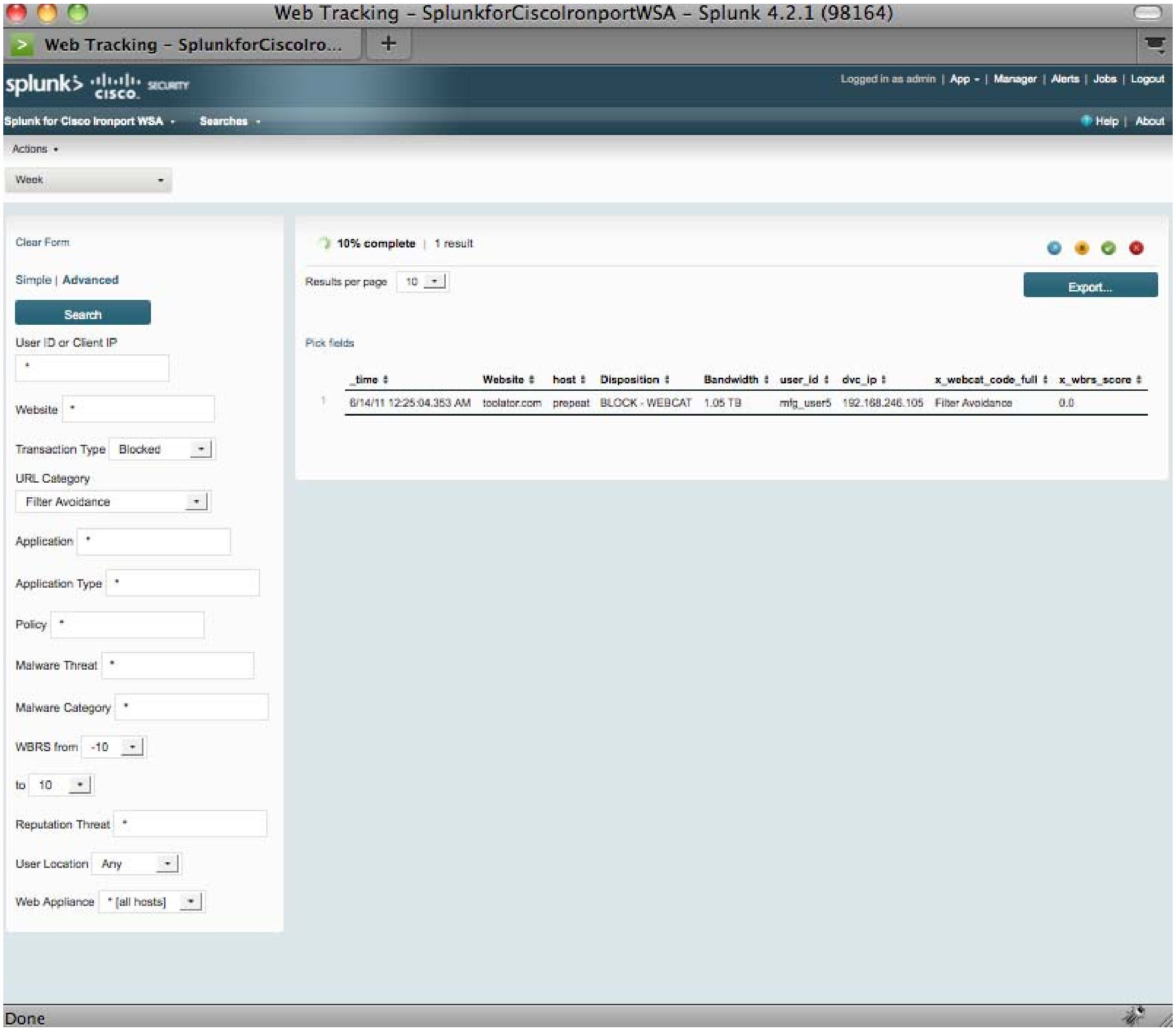
refreshed: today at 11:12:55 AM.

Results per page: 10

Export...
Pick fields
« prev 1 2 3 4 next »

	_time	Website	host	Disposition	Bandwidth	user_id	dvc_ip	x_webcat_code_full	x_wbrs_score
1	6/20/11 12:15:28.029 PM	indiana.edu	prepeat	DEFAULT - CASE	26.97 GB	hr_user1	192.168.245.101	Education	4.9
2	6/20/11 12:15:28.028 PM	digitalcorvettes.com	prepeat	DEFAULT - CASE	56.78 GB	hr_user1	192.168.245.101	Transportation	0.0
3	6/20/11 12:15:28.028 PM	taylor.edu	prepeat	DEFAULT - CASE	31.11 GB	hr_user1	192.168.245.101	Education	0.0
4	6/20/11 12:15:28.028 PM	ued.net	prepeat	DEFAULT - CASE	40.44 GB	hr_user1	192.168.245.101	Shopping	0.0
5	6/20/11 12:15:28.027 PM	dallasnews.com	prepeat	DEFAULT - CASE	75.85 GB	hr_user1	192.168.245.101	News	5.3
6	6/20/11 12:15:28.027 PM	islandrental.com	prepeat	DEFAULT - CASE	38.97 GB	hr_user1	192.168.245.101	Travel	0.0
7	6/20/11 12:15:28.026 PM	456bereastreet.com	prepeat	DEFAULT - CASE	8.20 GB	hr_user1	192.168.245.101	Computers and Internet	4.7
8	6/20/11 12:15:28.026 PM	dol.gov	prepeat	ALLOW - WBRS: 7.1	41.78 GB	hr_user1	192.168.245.101	Government and Law	7.1
9	6/20/11 12:15:28.025 PM	helene.dk	prepeat	DEFAULT - CASE	21.56 GB	hr_user1	192.168.245.101	Travel	0.0
10	6/20/11 12:15:28.024 PM	brothersoft.com	prepeat	DEFAULT - CASE	7.26 GB	hr_user1	192.168.245.101	Freeware and Shareware	3.8

Advanced



Web Tracking – SplunkforCiscoIronportWSA – Splunk 4.2.1 (98164)
Web Tracking – SplunkforCiscoIro...
splunk> cisco SECURITY
Logged in as admin | App | Manager | Alerts | Jobs | Logout
Splunk for Cisco Ironport WSA
Searches
Help | About
Actions
Clear Form
Simple | Advanced
Search
Pick fields
Export...
Done

Week

10% complete | 1 result

Results per page 10

User ID or Client IP	*
Website	*
Transaction Type	Blocked
URL Category	Filter Avoidance
Application	*
Application Type	*
Policy	*
Malware Threat	*
Malware Category	*
WBRS from	-10
to	10
Reputation Threat	*
User Location	Any
Web Appliance	* [all hosts]

	_time	Website	host	Disposition	Bandwidth	user_id	dvc_ip	x_webcat_code_full	x_wbrs_score
1	8/14/11 12:25:04.353 AM	toolator.com	prepeat	BLOCK - WEBCAT	1.05 TB	mfg_user5	192.168.246.105	Filter Avoidance	0.0

Sample Usage Scenarios

Finding information

The following usage scenarios illustrate how to use Splunk to find information.

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 look at the employee's web usage trends and transaction history. The administrator generates reports about the employee's browsing history.

- Choose **Users** from the Splunk for Cisco IronPort WSA dropdown menu (click on Splunk for Cisco IronPort WSA at the top left corner of the page to get the drop down menu). The Users page appears.

2. In the **Users** table, click on the User ID or Client IP address you want to investigate. The **User Drilldown** page appears for the User ID or Client IP.

   If you cannot see the User ID or Client IP address you want to investigate in the Users table, click on any User ID or Client IP to be led to the **User Drilldown** page. Enter in all or part of the User ID or Client IP address in the text box and click **Search**.

3. From the **User Drilldown** 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 for a particular User ID or Client IP.

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

4. If you want to print the data, click on **Actions** next to the User Drilldown title. Select **Print** from the dropdown menu.

   The administrator now wants to see the user's transaction history. They follow the steps below:

5. Click on Splunk for Cisco IronPort WSA at the top of the page to access the dropdown menu. Select **Web Tracking** at the bottom of the menu.

6. In the User/Client IP Address text field type in the user name or IP address, then click **Search.**

   The users transaction history appears. Click on "Pick fields" above the transaction list to change the information displayed for each transaction.

7. Export the data to a CSV file by clicking **Export** at the top right corner.

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.

1. On the Splunk application, choose **Web Sites** from the Splunk for Cisco IronPort WSA dropdown menu (click on Splunk for Cisco IronPort WSA at the top left corner of the page to get the drop down menu). The Web Sites page appears.

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

3. Scroll down to the **Domains Matched** table to view the top 25 domains that have been visited. Click on a domain you want to investigate. This leads to the **Domain Drilldown** page, which shows the users who have visited that domain in order of frequency.

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.

1. On the Splunk application, choose **URL Categories** from the Splunk for Cisco IronPort WSA dropdown menu (click on Splunk for Cisco IronPort WSA at the top left corner of the page to get the drop down menu). The **URL Categories** page appears.

   From the **URL Categories** page, you can see the top 10 URL Categories by Total Transactions graph.

   At this point you can export this report to PDF, by clicking **Actions** (next to the URL Categories title at the top of the page) and selecting **Schedule for PDF Delivery**. This file can be sent to the Human Resources manager. But remember, your network manager wants to know the bandwidth usage by each URL.

2. Scroll down to the **URL Categories Matches** table to view the **Bytes Allowed** column. This shows the bandwidth usage for each URL Category. You can select **Schedule for PDF Delivery** to send this file to the Network Manager.

   For finer granularity, click on a specific URL Category. You will be led to a **URL Category Drilldown** page that shows which users have the most transactions in a category. Scroll down to see the **Web Users** table. The **Bytes Allowed** column shows you which users have used the most bandwidth.

FAQ

Why does the overview report show more events than are in Splunk?

The summary information exists in a separate index. Information in the summary index is a condensed version of the raw data where superfluous data (i.e. data not needed to present reports) has been quelled. This allows reports to load quicker. As this information is stored in a separate index – the raw data may 'roll off' per the settings configured by the Splunk administrator(s) but its aggregated information may still exist in the summary index and therefore be available for reports.

How may I improve performance when I perform ad hoc queries?

Craft your ad hoc searches to be as specific as possible so that they return only information needed. Returning superfluous event data is more costly in terms of searching and retrieving all the rows. Searching for a specific user will be quicker than searching for all users. Searching for a specific user who visited a specific domain will be quicker still

Narrow your time range to an appropriate window. Do not select 90 days when 30 days will meet the reporting need

Why am I missing hosts?

Why do I see extra hosts?

How do I change the label of hosts?

Only Splunk administrators are able to control the hosts you see on the Overview report and Web Tracking report. Contact your Splunk administrator with details of host you would like to add, remove, or rename.

How do I change the dropdown options on the web tracking report?

Only Splunk administrators are able to control the options you see in the dropdown fields in the Web Tracking form. Contact your Splunk administrator with details of changes you would like to make regarding hosts, malware categories, transaction types, and URL categories

Why do I not see trafmon (L4TM) logs?

Why do I only see data for specific departments?

The SplunkforCiscoIronportWSA application may be configured for role-based access. In this configuration users may be restricted to viewing data from specific departments (or groups). If this configuration is enabled L4TM data will only be available to administrators (as L4TM data is not linked to a department or role). Please contact your Splunk administrator for additional details.