## Splunk for Cisco IronPort WSA: User Guide

## Table of Contents

Introduction:	3
Supplement to Existing Splunk Documentation:	3
Logging In:	3
Report Usage:	3
Choosing a Time Range:	3
Find Data:	3
Export Data	3
Option 1	3
Option 2	3
Tables:	4
Sorting Columns	4
Choosing Fields	4
Report Descriptions:	4
Overview	4
Users	5
Web Sites	6
URL Categories	7
Application Visibility	7
Anti-Malware	8
Client Malware Risk	9
Web Reputation Filters	10
L4 Traffic Monitor	11
Reports by Drilldown	12
Malware Category Drilldown	12
Malware Threat Drilldown	12
Application Drilldown	
Application Type Drilldown	
Domain Drilldown	
URL Category Drilldown	
User Drilldown	
Reports by Location	12
Overview by Location	12
LIPL Categories by Location	12
Anti-Maiware by Location	

Web Reputation Filters by Location	12
Application Visibility by Location	12
Users by Location	12
Websites by Location	12
Web Tracking (form based search) Simple	13
Advanced	14
Sample Usage Scenarios	15
FAQ	16
Why does the overview report show more events than are in Splunk?	16
How may I improve performance when I perform ad hoc queries?	16
Why am I missing hosts? Why do I see extra hosts? How do I change the label of hosts?	16
How do I change the dropdown options on the web tracking report?	16
Why do I not see trafmon (L4TM) logs? Why do I only see data for specific departments?	17

## 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.



### Users

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

		USE	ers – spiuriki	orciscononport	WSA – Splunk 4.2.1	(90104)					
Users – SplunkforCi	scolronportWS.	+									1
splunk's ulturlity security									Logged in as add	in   App -   Managa	r   Alerts   Jobs   Log
Splunk for Claco Ironport WSA . Searches .									_		a Help   Ab
Usera Actons -											
90 Days -											
Top Users by Transactions Blocked				1	Top Users by Bandwidth Used						
rig user2 finance user2 finance user2 192.169.240.101 end user3 end user3 end user3				_	mfo useri mfo useri finance useri finance useri mfo useri eng useri eng useri eng useri eng useri eng useri				I	-	
eng_user5	1.000.000	2.000.000	3.000.000	4.000.000	guest_ūšēi6	2E12	4E12	6E12	8E12	10E12	1.2E13
	1,000,000	2,000,000	0,000,000	1,000,000				JE	0212	IVEIE	
		Transact	tions					KBy	tes		
line		Transact	tions					КВу	tes		
Users		Transact	tions					KBy	tes		
Users Results or page 10 -		Transact	lions					KBy	les		
Users Results per page T		Transact	tions					KByt	tes		
Users Results per page Pot Ataba User 30 - ext(-est, (P - 1) mice user 1	Bandwidh_Used	Transact	tions	Transactions_Complete Transactions	ed 1	Transactiona_Blocked	•	KByt	Total_Transac	tions I	
Users Reads propage K Potentia User, D.or, Clevel, P. 1 refs., suret min	Bandwidth_Uwed stroor IT 15 84900 TT	Transact	Time_Spect # 2002/127.00	Transactions_Complete 75405489 0155027	nd J	Transactions_Biocked	•	KByt	Total_Transac 754055405 010577877	Sons 1	
Users Results per page IC • Pace fails Users (D.e.g.Clear), (P. ) mfg_pare1 mfg_pare1 mf_pare1	Bandwidh, Usad 10708 /7 15 4460 00 15 7002 27 15	Transact	Time_Spect 9 24002102700 30402102700	Transactions_Complete 704558459 619576873 575669151	nd 1	Transactions_Blocked 6 4	•	KBy	Total_Transac 754050405 615576377 57566019	tions I	
Users Reach per page (K - ) Point table User 2, page (Clear (JP ) mig_arear) mig_arear Mig_arear Mig_arear	Bandwiddy, Usad 10000 73 TB 8460 00 TB 7002 25 TB 10704 34 TB	Transact	Time_Spect # 2+082137.00 3+042132.00 1+20315.00 3+0627.00	Treaseline, Complete Treaseline, Complete 619278873 619278873 57586493 2770776	ed i	Transactiona_Blocked 6 4 5	0	KBy	Total, Transac 754050405 015276570 572664019	dona 1	
Users Reach pr page R. • Poto fath User, D., er, Check, P. 1 mb_aser1 mb_as	Bandwiddy, Used 1070077 175 8460 00 79 7902 25 75 9750 24 75 925 24 75	Transact	Time_Spect # 2-0621:27:00 3-0621:22:00 1-02103:10:00 3-0627:05:00 3-0627:05:00	Tatasetione, Complete Tatabases 600570672 57086419 42207756 42207756	ed 1	Transactions, Blocked 6 4 1 3	۵	KBy	Total_Transac 784050495 615578577 578664019 422107716 412215322	tiona I	
Users Receipts program Politable User 2, per, Cherri, P 1 mig_sant mig_sant format_sant f	Bandwidth, Usad 1000071 75 8460 00 76 7502 27 75 2703 24 70 5621 43 76 4681 42 70	,	Time, Speet 0 2003/12/20 3042/12/20 1021220 1021220 1021220 1021220 1021220 102120 304227190	Tenastiera, Sorquiei Teldosto 69029873 97936415 42207708 42213349 39623086	nd 1	Transctions, Blocked 6 4 1 3 3 2411727	٥	KBy	Total_Teareas 754050405 61679677 57264019 42216776 412215302 36660633	tiona I	
Users Reads are raps V Pach table User J. D. g. et Clear(JP ) mig_aard mig_aard Reads Rea	Bandwidh, Usad 15705 /h 15 8480 00 15 7002 25 15 8793 4 15 8621 13 15 4651 12 15 44551 22 15	Transact	Time, Speet 6 >>06210200 >>06210200 >>06210200 >>0625100 >>0625100 >>0625100	Treasetion, Complete 19605689 610070873 57856618 412215349 36453569 208012741	ed I	Transactions_Blocked 6 4 1 3 3 2471/27 28	•	KBy	Total_Transac 754050405 010578677 57864019 422107716 412215362 36600633 24417267	tions )	
Users Reach propage K Pack tells Extends refsarc1 refsarc2 refsar	Bandwidd, Stard 11700 71 15 8400 013 7902 25 15 9521 37 9521 37 4051 12 15 4425 32 15 4425 32 15	,	Tem, Speed 9           2×08.21.27.00           3×08.21.27.00           3×08.21.27.00           3×08.21.27.00           3×08.21.27.00           3×08.21.20.00           3×08.21.20.00           3×08.21.20.00           3×08.22.20.00           3×08.22.20.00           3×1327.80.00	Transationa, Complete 19405040 619379473 57956495 42205796 42205796 42205300 26603060 26603060 26617241 202050492	ed 1	Transactions_Blocked           6           4           1           3           2471767           26	¢	KBy	Total_Transac 784858405 618578877 578864019 42210716 412215382 366606833 324417387 322158498	tions 2	
Users Resols or page Tem Pois Intel Marcola (Control (Contro) (	Bandwidh, Used 10000 71 73 8460 00 75 7102 25 73 9523 34 70 9521 43 70 4661 32 70 4625 32 75 4625 32 75 4625 32 75 3200 47 75	,	Time, Speciel 6           >005212.00           >005212.00           >005212.00           >005250.00           >005250.00           >005250.00           >005250.00           >005250.00           >005250.00           >005250.00           >005250.00           >005250.00           >005250.00           >005250.00           >005250.00           >005250.00           >005250.00           >005250.00           >015250.00	Tenastilora, Completi Tenastilora 6002/0027 570566/05 422077/06 42233549 2040/7241 22235492 2020960	nd 1	Transactions, Blocked           6           4           1           8           33           241/97           28           6           2	•	KBy	Total_Transa Tatal_Transa 1540640 61870877 67866403 4220776 41221587 236660033 234617367 232154408 236660033	Sons 9	

### Web Sites





### URL Categories

0 0	URL Ca	ategories – SplunkforCiscolr	onportWSA - Splunk 4.2.1 (98164)		
URL Categories - SplunkforCise	colr +				<b>.</b>
splunk'> יוןייןןי ארטאדע cisco:				Logged in as admin   App	-   Manager   Alerts   Jobs   Logout
Splunk for Cisco ironport WSA - Searches -					🕐 Help   About
URL Categories   Actions - 90 Days -					
Top URL Categories by Total Transactions			Top URL Categories by Blocked and Warned Transaction	ns	
Computers and Internet Shopping Transportation Health and Nutrition Travel News Business and Industry Arts and Entertainment Sports and Recreation Gov emment and Law	600,000,000 Transact io	10E8 1.4E9	Pom Computers and Internet Filter Avoidance Instant Messaging Search Engines and Portals Gambling Adult Weapons Arts and Entertainment Hacking	3,000,000 5,000, Transactions	000 7,000,000
URI Ordenesies Matches					
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	
Transportation	10363.09 TB	0	750301200	758384383	
Health and Nutrition	8984 29 TB	0	858840173	858840181	
Travel	7608.46 TB	0	556642820	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	
Done					

## Application Visibility

	9 🔿 🔿	Ap	plication Visibility -	SplunkforCisco	olronportWSA - Splunk 4.2.1	(98164	)						C
	Application Visibility - Splunkf	orC +											7
	plunks studie source									Ligger(in	acistein ( <b>Aso</b> -	Manager   A	laria   John   Lo
	cisco.						_					_	
						_		_	_	_	_		- (ME)   A
	pication values of the second s												
	40 Days -												
	Top Applications Types by Total Transactions				Top Applications by Blocked Transactions								
	YouTube				GenericSearchEngineTraffic								
Facebook Chill       Control       Image: Contro       Image: Contr	GenericSearchEngine (raffic )				den en e		_		_			_	
Ling       Add	Facebook Ceneral Blogger				Facebook C hat Q uickTime								
Translow       Translow       Translow         parameter       parameter       parameter       parameter         rest       parameter       parameter       parameter       parameter         rest       parameter       parameter       parameter       parameter       parameter         rest       parameter       parameter       parameter       parameter       parameter       parameter         rest       parameter	Craigshist	400,000	800,000	1,200,000	-	20	40	60	80	100	120	140	160
ban		т	ransactions					т	ransac	tions			
y band band band band band band band band													
<form>         Image: Series       Image: Serie</form>	Application Types Matched												
	Results per page 10												
ndpdpational <td>PickTelda</td> <td></td>	PickTelda												
Mai     jai     jai     jai     jai     jai       Interpret     1340     2	a_avc_type 1	bytes_allowed 0	allowed	transactions 4	blocked_application #				court_transa	ctions I			
minipo     minipo </td <td>Mada</td> <td>10.15 78</td> <td>1156836</td> <td></td> <td>0</td> <td></td> <td></td> <td></td> <td>1158852</td> <td></td> <td></td> <td></td> <td></td>	Mada	10.15 78	1156836		0				1158852				
fands     104     10     0     0       Bayend     41740     3     4     4     4       Standard     1254     4     4     4     4       Standard     1264     2     2     2     4       Standard     4263     2     3     4     4       Standard     4263     4     5     4     4       Standard     4263     4     5     5     5       Standard     4263     5     6     5     5       Standard     5     5     5     5     5       Standard     5     5     5     5     5       Standard     5     6     6     6     6       Standard     5     6     6     6       Standard	Barch Engine	198.39 MB	9135		0				9392				
mpd     ind     in     in     in     in       Salamany     237     4     5     4       Salamany     42.0     2     2     2     2       Salamany     42.0     2     3     2     2       Salamany     10.0     3     2     3     2       Salamany     10.0     3     3     3     3       Salamany     10.0     3     3     3     3       Salamany     10.0     10.0     10.0     10.0     10.0	Facatook.	1.12.VB	113		0				129				
Anima     Anima     Anima     Anima     Anima     Anima       Second Anima     Anima     Anima     Anima     Anima       Second Anima <td>Biogong</td> <td>815.71 83</td> <td>2</td> <td></td> <td>0</td> <td></td> <td></td> <td></td> <td>73</td> <td></td> <td></td> <td></td> <td></td>	Biogong	815.71 83	2		0				73				
man     n     n     n     n       Statul Goldway     102     1     1     1       Reade Jointy     102     1     1     1       Reade Jointy     103     1     1     1       Reade Jointy     103     1     1     1       Reade Jointy     1     1     1     1       Reade J	Social Networking	229.98	4						+0				
Appendix     Appendix     Appendix     Appendix     Appendix       Appendix     Appendix     Appendix     Appendix     Appendix     Appendix       Appendix     Appendix     Appendix     Appendix     Appendix     Appendix     Appendix       Appendix     Appendix     Appendix     Appendix     Appendix     Appendix     Appendix       Appendix     Appendix     Appendix     Appendix     Appendix     Appendix     Appendix       Appendix     Appendix     Appendix     Appendix     Appendix     Appendix     Appendix     Appendix       Appendix     Appendix     Appendix     Appendix     Appendix     Appendix     Appendix     Appendix     Appendix       Appendix </td <td>Presentation / Conferences</td> <td>634.82.828</td> <td>21</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td>21</td> <td></td> <td></td> <td></td> <td></td>	Presentation / Conferences	634.82.828	21						21				
Weigner Schweizer Sch	Webmail	6.53 KB	1		0				8				
Approximate and a series of the series													
Appl         Appl <th< td=""><td>Application Matched</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></th<>	Application Matched												
JAPA         Jogn M         Jogn M <td>Results per page 11</td> <td></td>	Results per page 11												
https://dxituality.com/         https://dxituality.com/ <thtp: <="" dxituality.com="" th="">         https://dxituality</thtp:>	Pick fields												
Name         Jan         Jan         Jan         Jan         Jan           Constant_quark         Bap         <	x_ave_app 0	x_avc_type 1	bytes_slowed it	allowed_tr	ansactions 8 bloc	ked_application 1				unt_transactio			
Development         Instant	YouTube	Media	16.15 TB	1153000	0				11	53555			
Tandyand         Maya	GenericSearchEngineThatRo	Search Engine	190.00 MB	1560	0				.9	45			
Anion         Main         Staff         Applied         Appli	Flash Video	Media	854 02 MB	4224					4	24			
JAND         Mod         Under         Gal         Gal         Gal           Galvard         Galvard         Galvard         Gal         Galvard         Galv	Pordata	Meda	5.54 MS	488	.0				42	8			
Oach         Mas         710.401         70         8         03           Schad Gereit         Kals         1214         121         6         121           Schad Gereit         Kals         121         6         6         121           Staph Gereit         Schad Gereit         6         7         7         7           Staph Gereit         Schad Gereit         6         6         6         6           Staph Gereit         Schad Gereit         6         6         6         6           Staph Gereit         Schad Gereit         6<	LiveSICS	Meda	12.50 M3	425	0								
Instrument         Factor         Cardin         Cardin <thcardin< th=""> <thcard<tard<tard> <thca< td=""><td>QuickTime</td><td>Meda</td><td>221.84 MB</td><td>112</td><td></td><td></td><td></td><td></td><td>1</td><td>•</td><td></td><td></td><td></td></thca<></thcard<tard<tard></thcardin<>	QuickTime	Meda	221.84 MB	112					1	•			
mayar mayar 18.54.56 /2 /2 /2 /2 /2 /2 /2 /2 /2 /2 /2 /2 /2	Facebook General	Tacatzok	107MB	120	0				10				
70 (1997)	March 1	Jogging Records	014 D4 AB	10	0								
na ana a a a a a a a a a a a a a a a a	Crandel	Search Fooder	443.90 21	42									
		ARREST STOPPE	467 20 63	43									

die 1

### Anti-Malware

		A	nti Malv	ware - !	Splunkf	orCiscol	ronportWSA – Sp	olunk 4.2.1 (9	98164)				
Anti Malware -	SplunkforC	iscolro	. +										
lunk>	TY								Logged	in as admin	App -   Man	ager   Alerts	Jobs   Log
unk for Claco Ironport WSA •	Searches -												Help   Ab
Malware   Actions -													
Days +													
op Malware Categories Dete	cted						Top Malware Threats	Detected					
Adware	a a	-				3	Blackhol	e DNS URLs					
State March 1													
							Drive By W	/ebsite URLs		1			
Phiebing							1.06	mate Cleaner					
rinaming							Uli	mate cheaner					
							EIC	CAR-AV-Test					
					1.51.5								
												100	000
10	0 20	30	40	50	60	70			40	80	120	100	200
.11	0 20	30 Trar	40 nsactions	50	60	70			40	80 Tra	120 nsactions	160	200
11 alware Categories	0 20	30 Trar	40 nsactions	50	60	70			40	80 Tra	120 nsactions	100	200
alware Categories	0 20	30 Trar	40 Insactions	50	60	70			40	80 Tra	120 nsactions	100	200
alware Categories sults per page 10 <u>*</u>	0 20	30 Trar	40 Insactions	50	60	70			40	80 Tra	120 nsactions	100	200
11 alware Categories suits per page 10 • k fields x, wher, threat, type 1	0 20	30 Trar	40 Insactions	50	60	70	delected_transactions #		40 bioc	80 Tra	120 nsactions		200
14 alware Categories suits per page 10 • c/ fields x_wbrs_threat_type 1 Adware	0 20	30 Trar monite	40 Insactions	50	60	70	delected_transactions #		40 bloc 0	80 Tra	120 nsactions	100	200
alware Categories esuits parge 10 • ck fields <u>adware</u> Phahang	) 20	30 Trar monite	40 Insactions	50 s	60	70	delected_transactions † 66 20		40 bioc 0	80 Tra	120 nsactions	100	200
lalware Categories esuits per page 10 • ick fields x_wors_threat_type : Adware Philaving	) 20	30 Trar monite 20	40 Insact ions	50	60	70	delected_transactions # 69 20		40 bioc	80 Tra	120 nsact ions		200
talware Categories Issuits per page 10 • Isk fields x_whore, threat sype : Advans Phaning	0 20	30 Trar 09 20	40 Insactions	50	60	70	delected_transactions † 65 20		40 bioc 0	80 Tra	120 nsact ions		200
Ialware Categories esuits per page 10 • ck fields <u>x_whors_threat_type :</u> <u>Advare</u> Philating	0 20	30 Trar 09 20	40 Insactions	50	60	70	detected_transactions # 66 20		40 bloc 0	80 Tra	120 nsact ions		200
talware Categories issuits per page 10 • ick fields <u>*</u> , whor, shreat, sype t Adware Philaring issuits per page 10 •	0 20	30 Trar monite 69 20	40 Insact ions	50	60	70	delected_transactions 1 65 20		40 bloc 0	80 Tra	120 nsact ions		200
alware Categories souts per page 10 v x_wbrs_threat_yppe : Adware Phishing alware Threats souts per page 10 v ck feiss		30 Trar monite 69 20	40 msactions	50	60	70	detected_transactions = 09 20		40 bioc 0	80 Trai	120 nsactions		
Ialware Categories esuits per page 10 * ck feids x.whor, threat, sype 1 Adware Philating Ialware Threats esuits per page 10 * ck feids malaces 1 Bathaten (1) 1918 is	20 	30 Trar 09 20	40 nsact ions ored_transact	50	60	insactions #	detected_transactions s 69 20 Notect	ed_transactions 1	40 bioc 0	80 Trai tked_transac	120 nsactions tions 1		

### Client Malware Risk

Client M	Malware R	isk – Splur	ıkforCi	+											
lunks alada	NOWTY										Loggert i	n ee estreto (	App -   Mar	nager   Aleri	e   Jobe   Li
k for Class Ironport W	ISA . Searches														• Help ( A
t Malware Risk   A	cioni •														
Days	•														
b Proxy - Top Client	a by Malware Risk						L4 Traffic Monitor - Top Clin	enta by Malware Risk							
guest md contract guest contract md finance	user2 user3 user3 user3 user3 user4 user4										-				
guest	üšēi6	20 4	40 60	80	100	120	192:168:2	40:44 100	200	300	400	500	600	700	800
			Troppo	atlana							Transa	ctions			
s Proxy - Clienta by	Malware Risk		Transa	ctions							i i u i i i u				
b Proxy - Clants by uts per page 11 <u>+</u> mer_id 1 u	Malware Risk	bytes_blocked #	nontored_regesta i	montore	d_responses 1	triccked_rec	exts I blocked_responses	I moniformed_b	ansactions #	bio	cked_transa	ctions 1	Cetecte	ed_ <del>bransset</del> i	174 B
b Proxy - Clients by ulls per page 10 user_jit 1 u past_user2 A	Malware Risk J ser_domain # C	bytes_blocked ≠ Dis Dis	monitored_requests (	monitore	d_responses I	blocked_rec 0	esta 8 biocked_responses 0	i manifored_s	ansactions +	0 0	cked_transa	ctions 8	Collector 100	rd_transacti	25# \$
a Prozy - Clients by da per page 10 - ser_jd 1 u sart_user2 A sd_user1 A sd_user3 A	Malware Rosk 	bytes,biocked ∳ Da Su Sa	monitored_regette # 100 75 45	monitore 0	d_responses i	biocked_reg 0 0	esta I biocked_responses 0 0	I monbored_s tos 73 43	anazcilora #	0 0 0	cked_transa	ctions 1	cetecte 109 79 48	id_transacti	25# Ø
b Proxy - Clients by als per page 10 see, id 1 anst_uner2 - A bt_uner1 - A st_uner1 - A struct_uner3 - A	Malware Risk 	bydes_blocked # Db Db Db Db	monitored_requite # 100 75 45	monitore D D D D D	d_responses i	biocked_reg 0 0 0	nata I biocked_responses 0 0 11 0	I monitored_5 109 79 43 45	anazctions #	<b>bio</b> 0 0 0 0	cked_transa	ctions 8	celecte 100 79 48 45	id_transacti	27.8. B
Proxy - Clients by its per page 11	Matware Risk	bydes_blocked # Db Db Db Db Db Db	rontond_regets   100 75 48 45 42	maniferer D D D D D D	d_responses I	biocked_rec 0 0 0 0 0 0	nets I blocked_responses 0 0 0 0 0 0 0	I monifored_5 1009 73 43 45 42	anazcilora #	<b>old</b> 0 0 0 0 0 0	cked_transa	ctions 1	catecta 109 79 48 45 42	id_transacti	27.6 Ø
Procy - Clients by its per page 10	Malware Rok	bydes_blocksd # Db Db Db Db Db Db	rontoned_negastic I 100 33 45 42 42 41 42 42 43 45 45 45 45 45 45 45 45 45 45	monitore D D D D D D D D	d_responses i	biosked_reg 0 0 0 0 0 0	anta B biocked_responses 0 0 0 0 0 0 0 0	I mothered 5 909 73 43 43 43 43 43 43	anactions #	840 0 0 0 0 0	cked_transa	ctions #	cetects 109 79 48 45 42 41	id_Pansacti	558 B
Proxy - Clients by     As per page     It      ser_id i     wast_user2 A     di_seer1 A     di_seer1 A     arract_user3 A     arract_user3 A     arract_user3 A     di_seer1 A     di_seer1 A     di_seer3 A     di_seer3 A     di_seer4 A     di_seer4 A	Malware Rok	bydes_blocked # Db Db Db Db Db Db Db Db Db Db Db Db Db	rentered_requisis 1 100 35 48 45 42 41 40 40		d_responses I	bioskad_reg 0 0 0 0 0 0 0 0	este 8 biocked_responses 0 0 0 0 0 0 0 0 0 0 0	I mothored_3 100 173 43 43 43 43 43 43 43 43 43 43 43 43 43	ansactions #	240 0 0 0 0 0 0 0 0 0 0 0	ckeci_transa	ctions #	celecte 108 79 48 45 42 41 40 40	id_transacti	554 V
b Proxy - Clients by dis per page K ser_id t un part_user2 A dis sert	Malware Rock	bydes_blocked # Dh Dh Dh Dh Dh Dh Dh Dh Dh Dh Dh Dh Dh	ranseries (1994)		d_responses I	biosted_req 0 0 0 0 0 0 0 0 0 0 0 0 0	esta 8 biocked_responses 0 0 0 0 0 0 0 0 0 0 0 0 0 0	I mothored_3 109 73 43 43 43 43 43 43 40 43 40 33	antections #	840 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	cked_transa	ctions 8	celecte 109 79 48 45 42 41 40 40 39	id_transactiv	55.8 P
b Proxy - Cleats by use per page 16 - part, user2 A 101, user1 A 101, user1 A 101, user3 A part, user3 A part, user3 A part, user3 A part, user4 A part, user4 A part, user4 A	Malware Rook	bySen_biocked # Dis Dis Dis Dis Dis Dis Dis Dis Dis Dis	ranser ranser monitored_requests ( 100 75 45 45 45 45 40 40 20 20 20 20 20	nseitere D D D D D D D D D D D D D	4,mportes I	biasked_req 0 0 0 0 0 0 0 0 0 0 0 0	esta I biocked_responses 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	I monifianed_0 100 70 43 45 43 43 43 43 43 43 43 33 33 33	anactions 0	840 0 0 0 0 0 0 0 0 0 0	sked_transa	cliors 1	catacta 108 79 48 45 42 41 40 40 29 39	id_Pansacti	27.8 B
b Proxy - Clients by an per page TC - ser. Jul 1 Stand ser. Jul 2 Stand set, Juard A set, Juard	Matware Rok	bydes_blocksd # Db Db Db Db Db Db Db Db Db Db Db Db Db	ranser montowed_requests I 100 100 40 40 40 40 30 30 30 30 80 80 80 80 80 80 80 80 80 8	manifarea 0 0 0 0 0 0 0 0 0	4,78500566 I	biocost rec	atta I biocced_responses 0 0 11 0 11 0 11 0 0 11 0 0 0 0 0 0	I mortifored_3 109 79 48 45 43 40 40 40 40 40 39 39 39	anaciore (		cked_transa	ctions #	celectr 100 79 48 45 42 41 40 39 39 39	id_transactiv	554 3
Procy - Clients by error of a ser page K - error of a ser page K - error of a ser page K - error of a ser page K - roffic Monitor - Client - roffic Monitor - Client - roffic Monitor - Client - c, p 4 - 10.5201 (5)	Matware Rok	bydes_blocked # Do Do Do Do Do Do Do Do Do Do Do Do Do	1 ranser montowed_requests / 100 48 48 48 49 40 40 50 50 50 50 50 50 50 50 50 50 50 50 50		4,79500566 8	biocost rec	asta I biocled_responses 0 0 11 0 0 11 0 0 0 0 0 0 0 0 0 0 0 0 0	8 montbarred_8 109 779 48 43 43 43 43 43 43 43 43 43 39 39 39	attactions #	800 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	cked_trans	ctions 1	<b>cetecte</b> 109 79 48 45 47 41 40 39 29	id_banaath	
a Procy - Clients by ser_jd 1 U U ser_jd 1	Matware Rok	bydes, biodess # Dis Dis Dis Dis Dis Dis Dis Dis Dis Dis	11/2/15/2/ montowed_requests // 100 100 48 46 46 40 40 39 20 50 50 50 50 50 50 50 50 50 5		d, responses 1	biocod_rec 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	asta I biocled_responses 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0	I monthered_A 100 48 43 43 43 43 43 43 43 43 43 40 33 33 39	Total 723	bis 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	orrections,	ctions 1	2000000 100 77 48 45 42 41 42 42 41 42 20 20 20	id_Parssell	255 B
a Procy - Clients by           ubs per page         16	Matware Rook	bytes, blocksd # Db Db Db Db Db Db Db Db Db Db Db Db K K Malwark, Corrections	rentend regets (		d, responses 1	biocost_rec 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	netions_Meritared 3	I monthered_A 109 43 43 43 43 43 40 40 35 35 39	tetal 723 250	ble 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	cked_trans	ctions i	colacte 100 77 48 45 47 41 45 47 41 45 33 39	id_Parsacti	ana 8
b Proxy - Clients by           da per page         10	Materier Rok	bytes_blocksd # Db Db Db Db Db Db Db Db Db Db Db Db Db	rantand_regets 1 100 100 100 100 100 100 100 1		d, responses 1	biocesd_rec 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	exts ) blocked_responses	<ul> <li>monitored_s</li> <li>109</li> <li>109</li> <li>41</li> <li>43</li> <li>44</li> <li>44</li> <li>45</li> <li>46</li> <li>47</li> <li>48</li> <li>49</li> <li>49</li> <li>40</li> <li>40<td>attactions # Total 723 659 659 659 659 659 659 659 659</td><td>bio 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0</td><td>cked_trans</td><td>ctions i</td><td>Collection           103           77           48           45           42           40           33           39</td><td>id, Parsstift</td><td>254 B</td></li></ul>	attactions # Total 723 659 659 659 659 659 659 659 659	bio 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	cked_trans	ctions i	Collection           103           77           48           45           42           40           33           39	id, Parsstift	254 B
Procy - Clients by     mer_id i	Matware Risk.	Nydea, blockes # Da Da Da Da Da Da Da Da Da Da Da Da Da	ranset manifered regards 1 100 170 173 48 46 46 40 40 30 30 30 30 30 30 30		d_responses I 8475 8475 8475 8475 8475 8475 8475 8475	biosted_req 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	exis I blocked_responses	<ul> <li>monitored_t</li> <li>109</li> <li>779</li> <li>43</li> <li>43</li> <li>43</li> <li>43</li> <li>43</li> <li>43</li> <li>43</li> <li>33</li> <li>33</li> <li>33</li> </ul>	anactions # total 723 859 420 420 230	816 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	cked_burnes	ctions 8	2014ct1 1139 779 48 45 42 41 40 40 39 39 39	id_Parsself	
b Procy - Clients by ans per page [16] 2 aer_jid 1 2 aer_jid 2 aer_jid 3 A dot_samt A A dot_samt A A dot_samt A A correct_samt A correct_samt A correct_	Matware Risk	bydes_blocked # Dh Dh Dh Dh Dh Dh Dh Dh Dh Dh Dh Dh Dh	I rariser mentowst_regests   109 109 40 40 40 40 40 30 30 30 Blocked		4,75507566 I	biocked_rec 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	nsta I biocos responses 0 0 0 0 0 0 0 0 0 0 0 0 0	I morbare, s 109 73 43 43 43 43 41 40 40 43 33 23 23	anactions # fotal 723 859 800 800 800 800 800 800 800 800 800 80	bleb	cked_bunes	ctions 8	2000 2000 2000 2000 2000 2000 2000 200	id fransatik	

### Web Reputation Filters





### 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).

L4 Traffic Monitor	- N	tor - spiulikiorcisc	Shorthout and - Shi	unk 4.2.1 (98164)
	- SplunkforCisc			
nk5 allalla secon				Lagged in as admin   App -   Manager   Alerta   Jobs   I
CISCO. br Cisco ironport WSA . Searches				a 140 i
ic Monitor   Actors -				
Cear Form				
ys -				
Search Host	Maiwane Port	Maiware Str		
•				
in free success				
arch for a Host, Malware Port, or Malware 5 ok on the Top Malware Hosta Detected bar	Site in the search boxes (above) to focus this report's resu graph (below) to search accessings for a user ID associat	Its (wildcards may also be used) ad with the bost IP address		
ick on any now in a results table to apply the a	mochield Host, Malware Port, or Malware Site as a lite	r for this report's results		
Malware Hosts Detected		op Malware Ports Detected		Top Malware Siles Detected
100 100 040 00		00		aliak az soslanda nam
192 188 240 41		443		www148.mysearch.com
192 168 240 74		65520		webiq005.webiqonline.com
182 168 240 51		7777		neededware.com
192 168 240 76		6010		www.adacuity.com
192:188:240:44	00 400 600 800	20000	A E 000 7 000	onestepsearch.net
2	00 400 600 800	3,00	0 5,000 7,000	700
	Connection		anna et la na	0
	Connections	C	onnections	Conons
ware Hosta Detected			Click on IP to report on associated use	19
uts per page 10 -			Results per page 10 +	
Alware_Hosts_Detected # Malware_Conv	ections_Blocked I Valware_Connections_Monitored	e Total_Malware_Connections_Detected	Report_from_IP 8	
122. NB8 240.88 115	1035	723	102.165.240.85	
177.168.240.52 80	575	650	192.108.040.82	
12,108,240,41 91	429	400	122, 105, 240, 41	
10.108.240.03 55	295	350	192.168.240.92	
92 988 240 51 58	275	333	192.165.240.91	
122.168.240.154 29	232	321	122.155.240.114	
12:108:240.83 82	225	262	152.168.240.85	
	234	257	122.158.240.31	
22 888 240 31 23				
122 158 240 31 23				
22.158.240.51 25		)) 4   + (		
22 198 240 31 23		)) 4   +		
22.155.240.31 23		) 4 1		
alwars Ports Detected		)) 4   +		
Allerina Ports Detected	Minute Constanting Stream 1	)) 4   +	Markens I	
alware Forts Detected multi-per page K Kalawar, Ports, Detected II 80	Malerin, Contractioni, Backed I	Mainine, Co 2733	rreetons_Vanbarrd	Total_Malaxin_Convectors_Detected 1 0043
Alexan Parts Detected mills are page. If an Weiwen, Parts, Detected II Weiwen, Parts, Detected II 443	Walarm_Contractions_Booked & 1912 54	<b>Keiner, Co</b> 172 71	rnettons, Marbored I	Total_Malwam_Connectors_Detected   0943 705
Alazina Parta Detected Insila per paga It Malware, Parta, Detected I Malware, Parta, Detected I 15 40 40 25	Maleone, Contractione, Disclard 9 519 30 30	100 arrows (20 172) 173 28	vectors, Machined 1	Total, Mahaine, Connectore, Detected I IID43 705 00
12 103 240 21 23	Valuare_Connections_Blocked 8 1312 54 30 2	Nation, Co 972 70 31 3 3	wetten, Mertland I	Total_Mahains_Connectors_Detected # 6943 795 60 6 4
122 M3 240 21 23 alware Ports Detected miles per page 10 1 1 Marines, Ports, Detected 8 80 40 40 25 80 7777 72 23	Mahara, Connection, Bocked 1 1213 54 30 3 2 1	Materia, Co 973 78 39 39 30 32 3 2 3 2 3 2 3 3 3 3 3 3 3 3 3 3 3	rrecton, Markined I	Total, Maharan, Connectore, Datacher I 0041 705 01 0 4 3
12 103 240 21 23 alware Ports Detected mile per page Molecular Detected 402 403 50 502 7777 727 23 2000 20 20 20 20 20	Valuers, Connection, Blocked 1 Gro 54 20 2 2 1 1		rrection, Martional k	Toria_Malaurin_Connectore_Datacted 1 0943 700 00 4 4 3 2
123 M3240.21 23 alware Parts Detacted mits are page (************************************	Valence, Connections, Disclod 1 120 54 30 3 2 1 1 1 1	Malarin, Co     0722     710     30     2     2     1     1	nneston, Westernel I	Total_Malexin_Convectors_Detected 1 Bits Tota 0 4 3 2 2
Alexans Partis Obtacted auto see page It Markens, Partis Detacted I Markens, Partis, Detacted I 40 40 40 40 40 40 40 40 40 40	Valvers, Contractions, Booked 8 100 24 20 2 2 2 2 1 1 1 1 1	Molecu, Ca           5723         719           70         30         3           2         2         2           1         2         1           2         1         1	meston, Madand 1	Total_Malwan_Connectore_Detected 1 0940 00 0 0 4 2 2
Abairs Ports Detected abairs Stars Detected abairs Stars Detected	Valuare_Connections_Blocked 8 310 54 30 3 2 1 1 1 1 1	Materies, Co 172 173 174 174 1 1 1 1	weation, Mariand 1	Total_Materix, Connectors_Detected 1 EXIS RS 0 0 0 1 2 2 2
12 103 240 241 23 alware Parts Detected mile par page (K_+) Mainers, Parts Detected 8 80 409 25 800 2777 23 2000 805 80 80 80 80 80 80 80 80 80 80	Walvare, Connection, Booked 8 507 54 30 7 2 1 1 1 1	Mainer, Co           972           70           30           2           1           1	rrecton, Montored I	Tota Mahain, Soonedore, Datache 1 Bit NS B B 4 3 2 2 2
12 103 240 21 23  abere Ports Detected  abere Ports Detected  abere Ports Detected  442 2 3 650 7777 23 20 50 50 50 50 50 50 50 50 50 50 50 50 50	Maharan, Connection, Bocked 1 1273 54 30 3 2 3 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1		reation, Variane I	Total, Maharan, Connectiona, Detected J 004 0 0 0 0 2 2 Total, Walaran, Connectiona, Detected J
23 23 24 24 25 25 25 26 26 26 27 27 26 26 26 27 27 26 26 26 27 27 26 26 26 27 27 26 26 26 27 27 26 26 26 27 27 26 26 27 27 26 27 26 27 26 27 27 26 27 26 27 27 27 26 27 27 26 27 27 26 27 27 26 27 27 26 27 27 26 27 27 26 27 27 26 27 27 26 27 27 26 27 27 26 27 27 26 27 27 27 26 27 27 27 27 27 27 27 27 27 27 27 27 27	Malean, Contraction, Backed I 100 34 30 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3	Malvern, Co     0723     713     3     2     2     1     1     Malvern, Co     7     1     1     Malvern, Co     7     1     1     Malvern, Co     7     1	meston, Ventend I	Total_Malawin_Connectors_Datacted 1  043  05  0  0  0  2  2  2  Total_Malawin_Connectors_Datacted 1  55
23 42 M3 240 31 23 44 425 Perio Detected main per page FC= Mainers, Ports, Detected 4 4 4 4 4 5 6 4 4 5 6 6 7 7777 7 7 7 7 7 7 7 7 7 7 7 7 7	Valuers_Connections_Booked 8 1012 94 30 3 2 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Molecure, Col           2723         719           30         2         2           2         2         1           1         1         1           2         1         1           3         2         2           1         1         1           4         4         7           1         1         1           447         23         1	meston, Wastond 1	Total, Nahara, Connectore, Detected 9  Total, Nahara, Connectore, Detected 9  R  Total, Walkers, Connectore, Detected 9  Total, Walkers, Connectore, Detected 9  20  20  20  20  20  20  20  20  20  2
122 M3 240 21 23  ahviere Pierts Detected  with up rage	Maharm, Connections, Blocked 1 1317 54 30 3 3 1 1 1 1 1 1 1 1 1 1 1 3 5 5 5 5 5 5	Materies, Co           1723         783           28         3         2           2         3         2         3           2         3         3         2           3         2         3         3         3           2         3         3         3         3           3         2         3         3         3           4         5         5         5         5           5         7         3         3         3         3           27         23         23         23         23         27         27	meton, Motored 1	Total, Maharan, Connectione, Datached 1 0:4 0 1 2 2 5 5 5 5 5 5 5 5 5 5 5 5 5
12 103 240 241 23  abase Parts Detected  abase Parts Detected  abase Parts Detected  442  3  442  3  442  3  442  3  442  3  442  3  442  443  442  444	Makern, Connections, Brocked 8 070 54 20 2 3 3 1 1 1 1 5 5 5 5 5 5 5	Maleure, Co.           273           711           38           2           2           1           1           4           647           201           21           22           23           24           1           1	rrection, Variante I	Total, Malaura, Connectora, Datacted 1
122 M3 240 21 23  abelars Ports Detected mith per page (*C)  443 55 650 650 7777 73 25 650 7777 73 72 72 72 72 72 72 72 72 72 72 72 72 72	Malean, Contraction, Backed 1 177 24 20 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3		recton, Ventone I	Total_Malaurin_Connections_Datacted 1 0041 700 00 00 00 0 0 0 0 0 0 0 0 0 0 0 0 0
تلك بلك يكون الله الله الله الله الله الله الله الل	Malasm_Contection_Booked 8 4 3 3 4 3 3 4 3 4 3 4 5 5 5 5 5 5 5 5 5	Molecut, Ce           2723         719           39         3         2           2         2         2           3         2         2           1         3         2           2         2         2           3         2         2           4         4         7           2         2         2           2         2         2           2         2         2           27         23         2           27         23         2           27         23         2           27         23         2           27         23         2           27         23         2           27         2         3           27         2         3           27         2         3           27         2         3           27         2         3           27         2         3           27         2         3           27         2         3	vectors, Markova I	Total_Nations_Connections_Detected #           ID45           ID45
122 103 240 247 23 abaies Paris Detected mile are page (€) 409 200 200 200 200 200 200 200 200 200 2	Malware, Connections, Blocked 1 312 30 3 3 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Matern, Co.         1713           1713         1713           1713         1713           171         171           171         171           171         171           171         171           171         171           171         171           172         171           173         171           174         175	recton, Motored 1	Total Maleura, Connections, Dataches 1 0043 00 01 0 0 0 0 0 0 0 0 0 0 0 0 0
تلك الله عليه الله الله الله الله الله الله الله ا	Makara, Connection, Booked 8 137 54 30 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3		recton_Mextend I	Total, Maleura, Connections, Databatil 1           004           005           01           02           20           20           21           22           23           24           25           26           27           28           210           211           212           213           214
122 M3 240 21 23  abaies Ports Detected math propage  (*	Maleare, Contractione, Backed 9 54 20 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3	Kalvere, Co 0722 171 39 2 2 1	rection, Matteret I	Total_Malaurin_Connectiona_Datactical 1           0041           004           01           01           02           201           213           172           172           172           172           173           174           175           175
	Malerin, Connection, Backed 8 120 24 3 2 2 2 2 1 1 1 1 1 1 1 1 1 1 1 2 2 2 2	Molecon, Co 973 19 30 3 2 2 3 1 1 Molecon, Co 4 5 2 2 3 1 1 1 1 1 1 1 1 1 1 1 1 1	recton, Ventone I	Total, Nations, Connections, Collected 8           8041           805           6           6           7           2 </td



### **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

00		Web Tracki	ng – SplunkforCisco	olronpor	tWSA – Splunk 4.2.1	(98164)				
≥ Web Tracking – SplunkforCiscolro 📘 🕂										
Search finalized.										
splunk'> 'Il'I'l' security cisco.								Logged in as adr	nin   App -   Manager   A	Alerts   Jobs   Logout
Splunk for Cisco Ironport WSA 🗸 Searches 🚽										🕜 Help   About
Actions -										
Week -										
Clear Form	Results	per page 10 🗾							refreshed: to	Export
Simple   Advanced										
Search	Pick fiel	lds								
User ID or Client IP hr_user1	« prev	1 2 3 4 next	»							
		_time ‡	Website +	host ‡	Disposition +	Bandwidth 🕈	user_id ‡	dvc_ip ‡	x_webcat_code_full \$	x_wbrs_score \$
Website *	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
Transaction Type All	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

\varTheta 😲 😳	Web Tracking - SplunkforCiscolronportWSA - Splunk 4.2.1 (98164)	
Web Tracking - Splunkford	Liscolro +	
splunk's ulturlity security	Logged in as admin   J	op -   Manager   Alerts   Jobs   Logout
plunk for Cisco Ironport WSA • Searches •		🐢 Help   About
Actions +		
Week -		
Clear Form	10% complete   1 result	
Simple   Advanced	Results per page 10 -	Export
Search User ID or Client IP	Pick fields	
•	_time \$ Website \$ host \$ Disposition \$ Bandwidth \$ user_id \$ dvc_ip \$ x_w	vebcat_code_full # x_wbrs_score #
Website *	6/14/11 1225/04.353 AM toolator.com prepeat BLOCK - WEBCAT 1.05 TB mfg_user5 192.168.246.105 Filte	r Avoidance 0.0
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] .		
Done		the la

## 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.

- 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.
- 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.

 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.

 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.