SecureWatch Analytics User's Guide

Corero Network Security, Inc.

Part Number: 9902-0805-00

March 9, 2015

Legal and Copyright Information

Corero Network Security, Inc. (Corero) reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of Corero to provide notification of such revision or change. Corero provides this documentation without warranty, term, or condition of any kind, either implied or expressed, including, but not limited to, the implied warranties, terms or conditions of merchantability, satisfactory quality, and fitness for a particular purpose. Corero may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

If you are a United States government agency, this documentation and the software described herein are provided to you subject to the following:

This paragraph applies to all acquisitions of the software by or for the United States Government, or by any prime contractor or subcontractor (at any tier) under any contract, grant, cooperative agreement or other activity with the United States Government (collectively, the "Government"). All technical data and computer software are commercial in nature and developed solely at private expense. The software and documentation respectively are "commercial computer software" and "commercial computer software documentation" as defined in DFARS 252.227-7014 (June 1995) and "commercial items" as defined in FAR 2.101(a) and, to the maximum extent permitted by law, are provided with only such rights as are provided in Corero's standard commercial license for the software and documentation and this notice. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (November 1995) or FAR 52.227-14 (June 1987), whichever is applicable. Corero's standard commercial license for the software and documentation and this notice shall govern the Government's use of the software, documentation, and technical data, and shall supersede any conflicting contractual terms or conditions. If these terms and conditions fail to meet the Government's needs or is inconsistent in any respect with Federal law, the Government must return the software and the documentation unused to Corero. The following additional statement applies only to acquisitions governed by DFARS Subpart 227.4 (October 1988): "Restricted Rights – Use, duplication and disclosure by the Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 (OCT. 1988)." The Contractor is Corero Network Security, Inc.

You agree not to remove or deface any portion of any legend provided on any licensed program or documentation contained in, or delivered to you in conjunction with, this document.

No part of this documentation may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from Corero.

If there is any software on removable media described in this documentation, it is furnished under a license agreement which is located on the Corero web site.

For warranty, licensing and maintenance agreement information, visit
http://www.corero.com/support/End_User_Agreements.html.

First Line of Defense, ReputationWatch, SecureWatch, SmartWall, and Agile Inspection Engine are registered trademarks of Corero Network Security, Inc.

All other trademarks and registered trademarks are the property of their respective holders.

Table of Contents

Overview

Corero SecureWatch Analytics is designed to assist with the analysis of security conditions that are detected by Corero Network Security's SmartWall Threat Defense System. This application is available via a globally accessible web portal or via a local web server that is hosted on a SecureWatch Managed Service Appliance at the customer’s site. Once logged in to the application, you can easily review and drill down on current and historical forensic data that was reported by all of the Corero appliances that are protecting your security infrastructure.

If you are a security partner, the web portal for security partners allows you to maintain multiple customers easily from one easy-to-use interface. The only requirements to use this application are that you have a supported web browser, credentials to log in to the application, and are a Corero customer or partner with SmartWall Threat Defense System appliances that you need to monitor.

Accessing SecureWatch Analytics

This section describes how to access SecureWatch Analytics via the web portal or the local web application.

Accessing the SecureWatch Analytics Portal

Corero SecureWatch Analytics is available via a globally accessible web portal. The portal is a powerful tool for reviewing security event information from all of your Corero SmartWall Threat Defense System appliances from the convenience of your favorite browser, from wherever you are. For partners who are maintaining Corero appliances for multiple customers, the portal application enables you to switch between customers easily.

1. Point a supported web browser at https://securewatch.corero.com .
2. Authenticate with your credentials when the login page appears.
   Contact Corero customer service (customer.service@corero.com) if you do not have credentials or have forgotten your password.

Accessing the SecureWatch Analytics Locally Hosted Web Application

Corero SecureWatch Analytics is available also by pointing a web browser to the SecureWatch Managed Service Appliance that is hosted at a customer’s site.

1. Point a supported web browser to the IP address of the local server and use this URL: https://securewatch.corero.com:8000

2. Authenticate with your credentials when the login page appears.
   Contact Corero customer service (customer.service@corero.com) if you do not have credentials or have forgotten your password.

Supported Web Browsers

Corero SecureWatch Analytics supports the use of these web browsers:

- Firefox 10.x and latest
- Internet Explorer 7, 8, 9, and 10
- Safari (latest)
- Chrome (latest)

Correcting Access Problems

The most common problem that occurs when accessing SecureWatch Analytics via the portal or the local web application is that no data is shown when the home page opens. Typically, this is just a timing issue between the browser and the application. If this occurs, use one of these methods to populate the display:

- Press refresh (F5) and reload the page. If that fails, wait a minute and try to refresh again.
- The portal application is slower than the locally hosted application, which has a higher priority. If searches from the portal application fail, try accessing the application using the loc-

ally hosted web server.

- If you continue to experience access problems, contact customer.service@corero.com

Considerations For Searching the SecureWatch Analytics Application

Some important information to keep in mind when querying data in SecureWatch Analytics:

Display

- Sometimes, individual charts and tables can take a long time to populate. Look in the lower right corner for a status bar, prefixed with the text, "Loading".
- If you don't see any data during a period for which you expect to see data, wait a few seconds and try your search again.
- Changing a field in the selector bar via a dropdown menu defines a new search that runs immediately. Results should begin to appear within a few seconds.
- The time required to populate graphs increases considerably when the Time Frame is extended.

Execution

- Local user access to the system takes precedence over queries running via the portal.
- If you type search criteria into fields in the Security Drilldown page, you need to click the **Search** button to start the search.
- The data that is displayed in any chart or table can be exported to a CSV-format file by clicking on the small down arrow in the lower left hand corner of the chart or table. This down arrow is hidden from view until you move the mouse toward its general location.
- When viewing results in a table, use the page selector on the bottom right of the table to scroll through pages of ten client IP addresses at a time.
- The Top Client IP and Top Server IP tables rely on "whois" to populate the hostname field. If DNS connectivity and "whois" are blocked from running on the local server, it may take several minutes for these tables to populate.

Performance

- Multiple users running searches on a system at the same time can affect performance and search time.
- Starting and stopping searches in progress affects system performance. For best performance, let searches finish running, and minimize rapid midstream search direction changes, if possible.

Resolution and Time Zones Used in Time-Based Charts

All times shown in time-based charts are displayed using the time zone that is local to the user's client.

The resolution used in time-based charts is set automatically. The following table shows the resolutions used for various selectable time frames.

Time Frame	**Resolution**
15 minutes	1 minute
60 minutes	1 minute
4 hours	1 minute
Up to 6 hours	1 minute

Today	5 minutes
Last 24 hours	5 minutes
Yesterday	5 minutes
Last 7 days	30 minutes
Last 30 days	1 hour
Longer than 30 days	1 day

Basic Analytics Screens

SecureWatch Analytics comprises four basic screens which provide access to a number of useful data displays, as well as tools for presenting and querying the data in those displays.

The Home screen acts as a dashboard; clicking something of interest in one of the displays on the Home screen focuses on that point of interest in the Security Drilldown screen, providing a more detailed look at it.

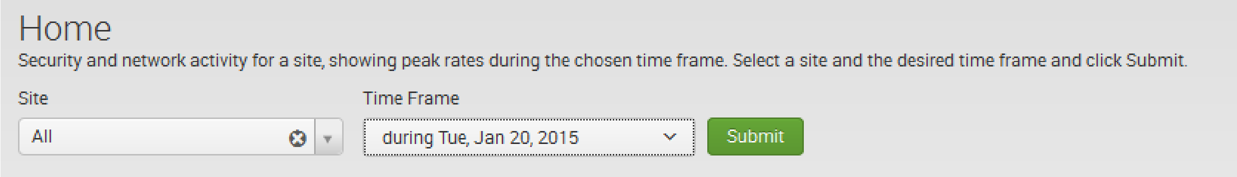
The Top Charts screen provides a set of tools that show you the elements of your security infrastructure that have experienced the greatest activity or utilization over the time frame you've specified.

The Export screen enables you to extract PDU data to a file for forensic analysis, providing controls for filtering syslog events and PDU data for exporting them to other applications, such as Wireshark.

Home Screen

The Home screen appears when you log in to Corero SecureWatch Analytics. It provides a tool bar followed by graphs and tables of analytical security information. Use the dropdown menus in the tool bar to search available data, and click on a line in a chart or a row in a table to drill down on that element and examine it in greater detail in the Security Drilldown screen.

Home Screen Selection Area Field Descriptions



Security and network activity for a site, showing peak rates during the chosen time frame. Select a site and the desired time frame and click Submit.

Site: All

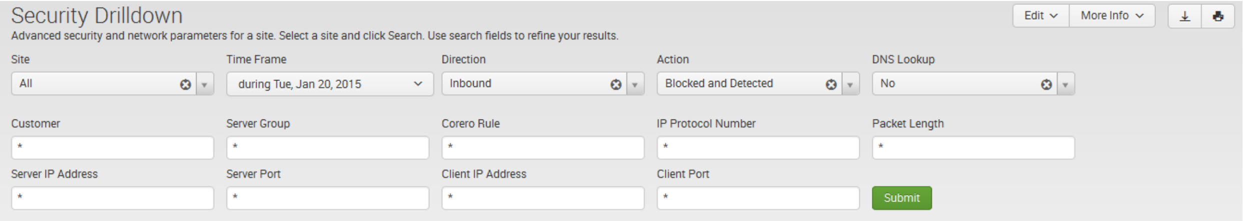
Time Frame: during Tue, Jan 20, 2015

- **Select Site** – This dropdown contains a list of sites, or security groupings, that are configured for the customer.
- **Time Frame** –This dropdown contains a list of time ranges that can be applied to the results that are displayed. The default for this field is to show all data from the start of the day.

Security Drilldown Screen

Clicking on a line in a chart or a row in a table in the Home screen displays the Security Drilldown screen. The Security Drilldown screen search fields are populated based on elements you selected in the Home screen, or otherwise selected previously in the Security Drilldown screen. To drill down deeper into the table, keep clicking on lines or rows until you reach the level of detail you want. If you prefer to type, you can type directly into the search fields and click on the **Search** button. You can reset the search criteria by clicking on **Home** to return to the Home screen.

Security Drilldown Screen Selection Area Field Descriptions


Security Drilldown

Advanced security and network parameters for a site. Select a site and click Search. Use search fields to refine your results.

Site: All

Time Frame: during Tue, Jan 20, 2015

Direction: Inbound

Action: Blocked and Detected

DNS Lookup: No

Customer: *

Server Group: *

Corero Rule: *

IP Protocol Number: *

Packet Length: *

Server IP Address: *

Server Port: *

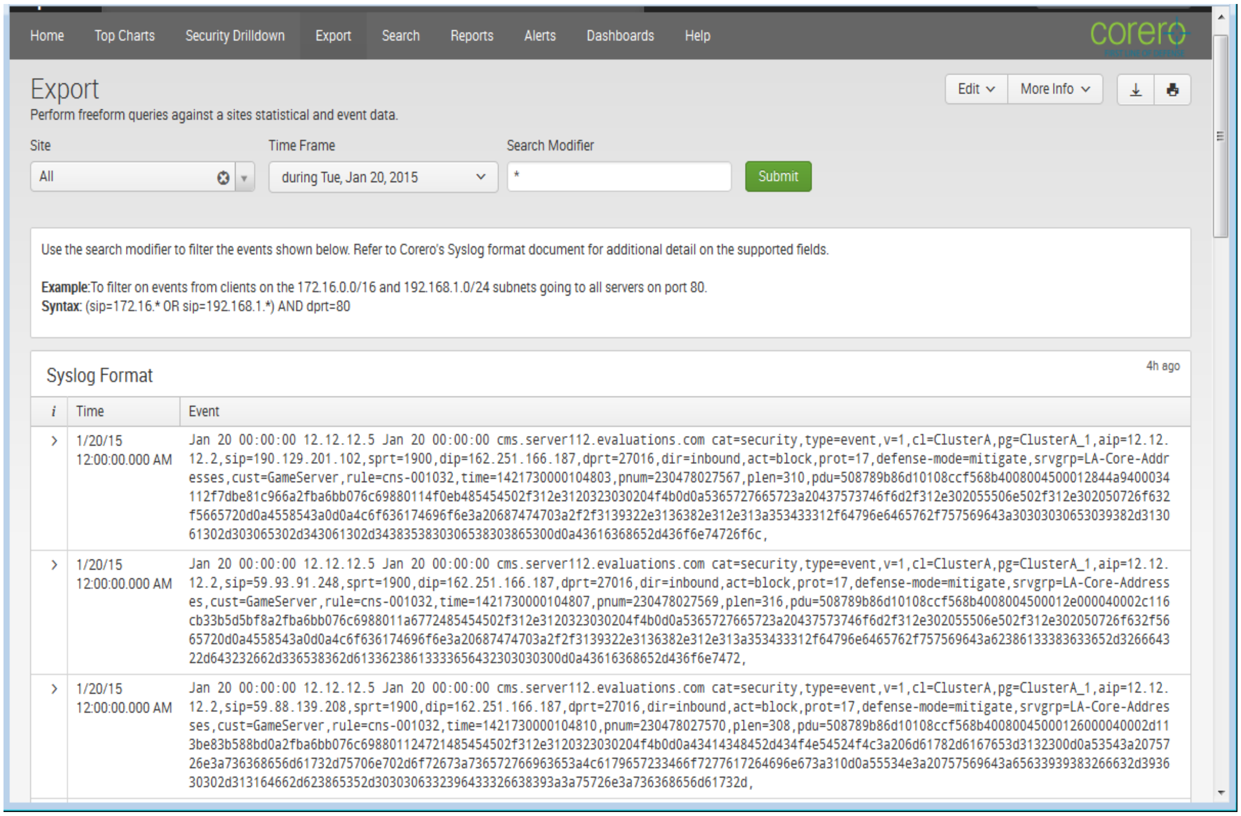
Client IP Address: *

Client Port: *

- **Site** – This dropdown contains a list of sites, or other security groupings, that are configured for a customer or the local system.
- **Time Frame** – Define a time range to constrain the results that are displayed. The default for this field is to show all data from the start of the current day.
- **Direction** – Choose **Inbound**, **Outbound**, or **Inbound and Outbound**.
- **Action** – Filter results according to what was done with packets that triggered rules. Choose **Blocked**, **Detected**, or **Blocked and Detected**.
- **DNS Lookup** – Indicate whether DNS is used to correlate IP addresses with domain names. Choose **Yes** or **No**. The default is **No**.
- **Customer** – Type the name of a customer by which to filter.
- **Server Group** – Type the name of a server group by which to filter.
- **Corero Rule** – Specify a Corero rule by which to filter the results.
- **IP Protocol Number** – Type the IANA-assigned ID for a protocol by which you want to filter. For example: 1 for ICMP, 6 for TCP, 17 for UDP, etc.
- **Packet Length** – Specify the packet size, in bytes, by which to filter.
- **Server IP Address** – Filter the query based on a destination IP address.
- **Server Port** – Filter the query based on the destination port that was accessed when a security event was triggered.
- **Client IP Address** – Filter the query based on a source IP address.
- **Client Port** – Filter the query based on the port number at the source.
- **Submit** button – Click this to execute the filters you've specified.

Export Screen

The Export screen (displayed below) enables you to extract PDU data to a file for forensic analysis, providing controls for filtering syslog events and PDU data for exporting them to other applications, such as Wireshark.



Export

Perform freeform queries against a sites statistical and event data.

Site: All

Time Frame: during Tue, Jan 20, 2015

Search Modifier: *

Submit

Use the search modifier to filter the events shown below. Refer to Corero's Syslog format document for additional detail on the supported fields.

Example:To filter on events from clients on the 172.16.0.0/16 and 192.168.1.0/24 subnets going to all servers on port 80.
Syntax: (sip=172.16.* OR sip=192.168.1.*) AND dprt=80

Syslog Format

4h ago

i	Time	Event
›	1/20/15 12:00:00.000 AM	Jan 20 00:00:00 12.12.12.5 Jan 20 00:00:00 cms.server112.evaluations.com cat=security,type=event,v=1,cl=ClusterA,pg=ClusterA_1,aip=12.12.12.2,sip=190.129.201.102,sprt=1900,dip=162.251.166.187,dprt=27016,dir=inbound,act=block,prot=17,defense-mode=mitigate,srvgrp=LA-Core-Addresses,cust=GameServer,rule=cns-001032,time=1421730000104803,pnum=230478027567,plen=310,pdu=508789b86d10108ccf568b4008004500012844a9400034112f7dbe81c966a2fba6bb076c69880114f0eb485454502f312e3120323030204f4b0d0a5365727665723a20437573746f6d2f312e302055506e502f312e302050726f632f5665720d0a4558543a0d0a4c6f636174696f6e3a20687474703a2f2f3139322e3136382e312e313a353433312f64796e6465762f757569643a30303030653039382d313061302d303065302d343061302d3438353830306538303865300d0a43616368652d436f6e74726f6c,
›	1/20/15 12:00:00.000 AM	Jan 20 00:00:00 12.12.12.5 Jan 20 00:00:00 cms.server112.evaluations.com cat=security,type=event,v=1,cl=ClusterA,pg=ClusterA_1,aip=12.12.12.2,sip=59.93.91.248,sprt=1900,dip=162.251.166.187,dprt=27016,dir=inbound,act=block,prot=17,defense-mode=mitigate,srvgrp=LA-Core-Addresses,cust=GameServer,rule=cns-001032,time=1421730000104807,pnum=230478027569,plen=316,pdu=508789b86d10108ccf568b400800450012e000040002c116cb33b5d5bf8a2fba6bb076c6988011a6772485454502f312e3120323030204f4b0d0a5365727665723a20437573746f6d2f312e302055506e502f312e302050726f632f5665720d0a4558543a0d0a4c6f636174696f6e3a20687474703a2f2f3139322e3136382e312e313a353433312f64796e6465762f757569643a62386133383633652d326664322d643232662d336538362d613362386133336564323030300d0a43616368652d436f6e7472,
›	1/20/15 12:00:00.000 AM	Jan 20 00:00:00 12.12.12.5 Jan 20 00:00:00 cms.server112.evaluations.com cat=security,type=event,v=1,cl=ClusterA,pg=ClusterA_1,aip=12.12.12.2,sip=59.88.139.208,sprt=1900,dip=162.251.166.187,dprt=27016,dir=inbound,act=block,prot=17,defense-mode=mitigate,srvgrp=LA-Core-Addresses,cust=GameServer,rule=cns-001032,time=1421730000104810,pnum=230478027570,plen=308,pdu=508789b86d10108ccf568b40080045000126000040002d113be83b588bd0a2fba6bb076c698801124721485454502f312e3120323030204f4b0d0a43414348452d434f4e54524f4c3a206d61782d6167653d3132300d0a53543a2075726e3a736368656d61732d75706e702d6f72673a736572766963653a4c6179657233466f7277617264696e673a310d0a55534e3a20757569643a65633939383266632d393630302d313164662d623865352d3030306332396433326638393a3a75726e3a736368656d61732d,

Filter event data by site and by time range to display the corresponding syslog events and PDU data. You can refine your results further by specifying an arbitrary search string in the Search Modifier field to narrow the results specifically to only those that match the string.

A set of icons appears at the bottom left of each pane in the tab; click the **Export** icon to write the filtered results to a file (up to a maximum of 1,000). For example, PDU data can be exported for use in Wireshark. Do this by exporting the PDU data in the **Raw Events** format.

In Wireshark, choose **Import** and select **Hexadecimal** as the format of the file. Make sure also to click on the **Date/Time** check box and specify a format of `%D %T`.

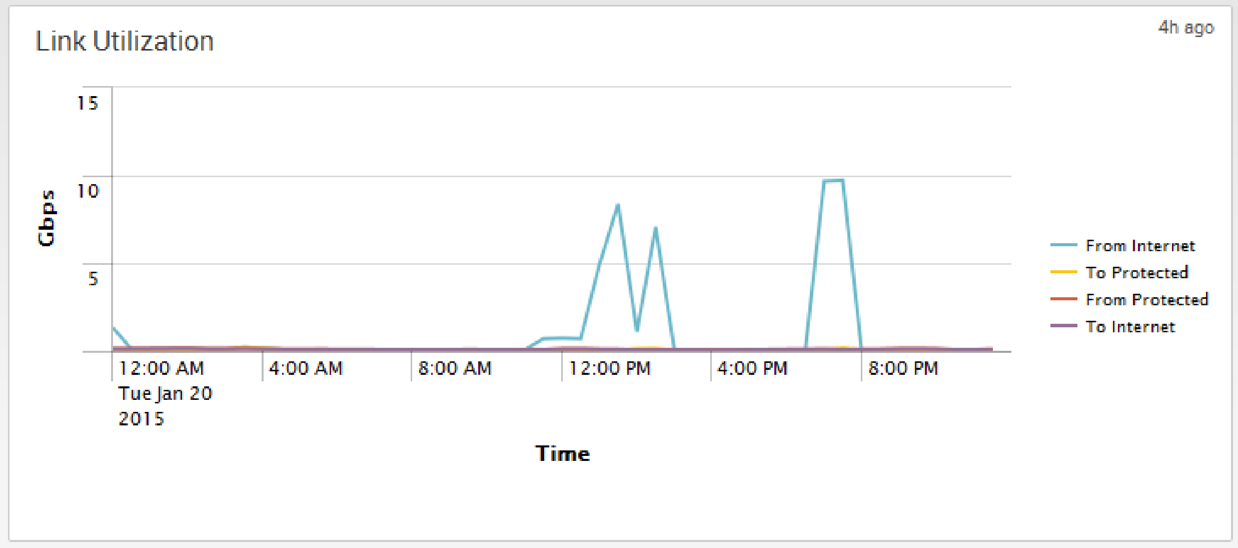
Analytics Tools

SecureWatch Analytics provides these tools for assessing the nature of the traffic that your network encounters:

- Link Utilization Time Chart
- Packets Per Second Time Chart
- Flow Usage Time Chart
- Setup Rates Time Chart
- Top 10 Rule Types Blocked Chart
- Top 10 Rule Types Detected Chart
- Blocked Events Table
- Detected Events Table

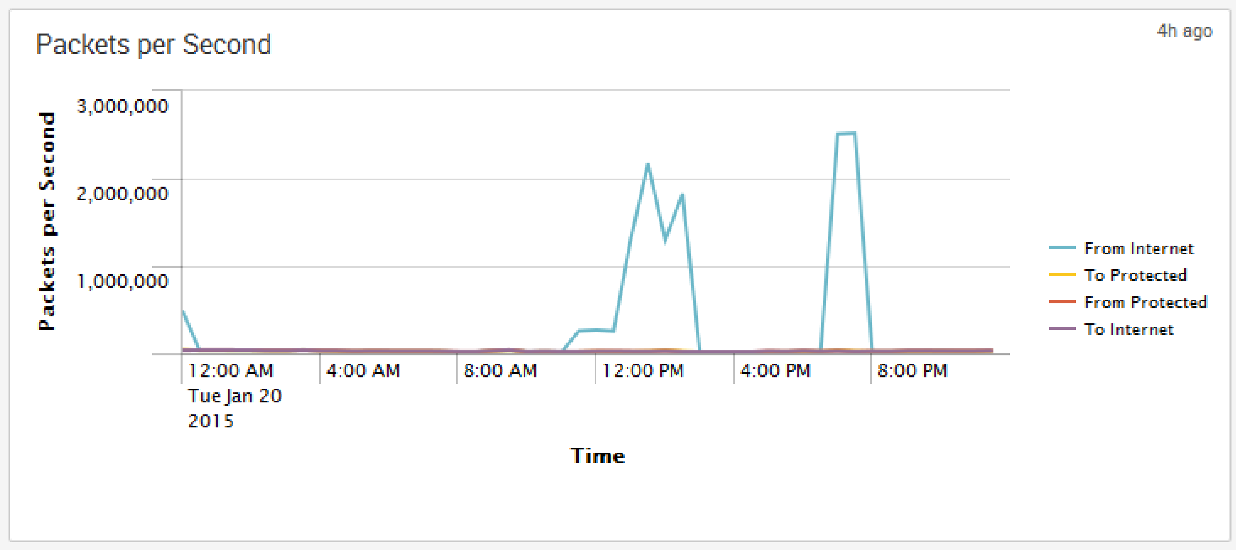
Link Utilization Time Chart

The Link Utilization graph displays the average inbound and outbound traffic volume, in Gbps, reported by all Corero appliances at the selected customer and site over time.



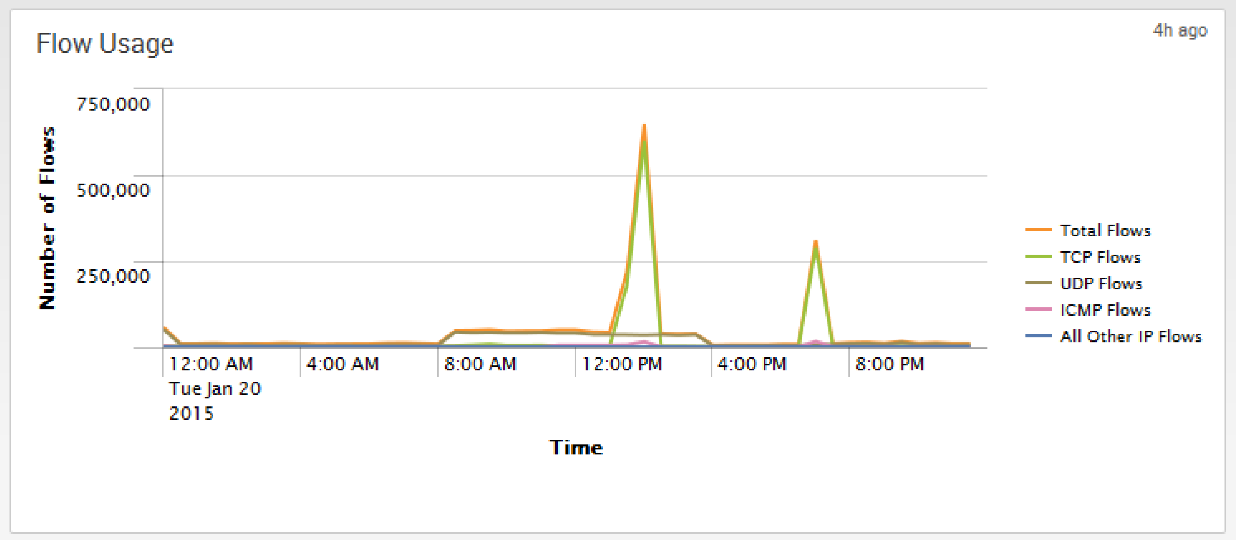
Packets Per Second Time Chart

The Packets Per Second graph shows the average inbound and outbound packets per second reported by all Corero appliances at the selected customer and site over time.



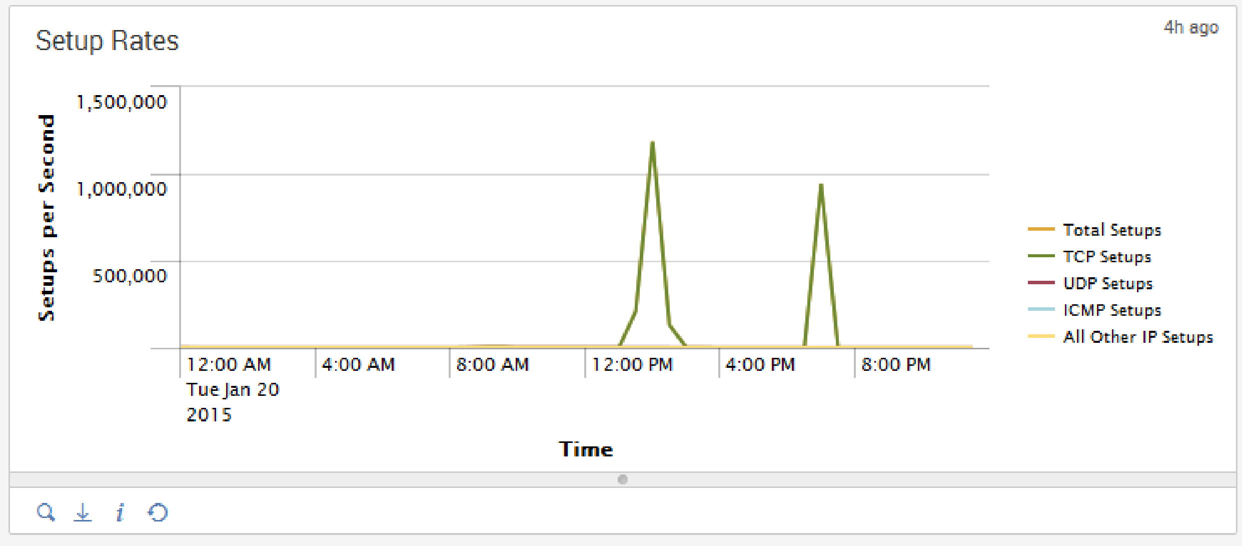
Flow Usage Time Chart

The Flow Usage graph displays the number of flows that are being monitored by all Corero appliances at the selected customer and site over time.



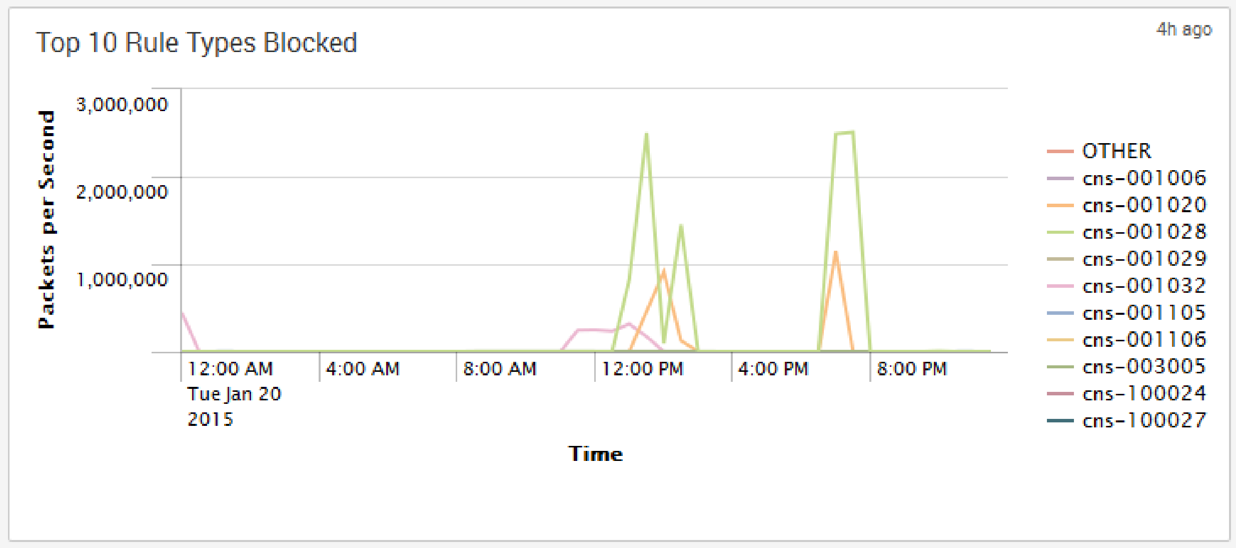
Setup Rates Time Chart

The Setup Rates graph displays the number of flow setups that are being tracked by all Corero appliances at the selected customer and site over time.



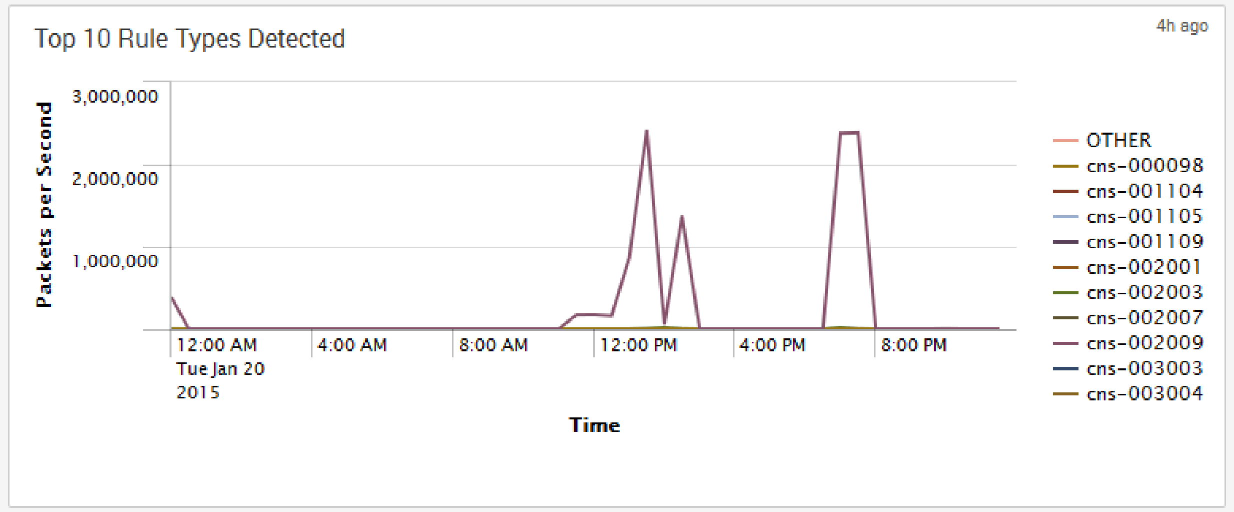
Top 10 Rule Types Blocked Chart

This chart shows the ten rules set to Block that were triggered most (based on packets per second) in the specified time period:



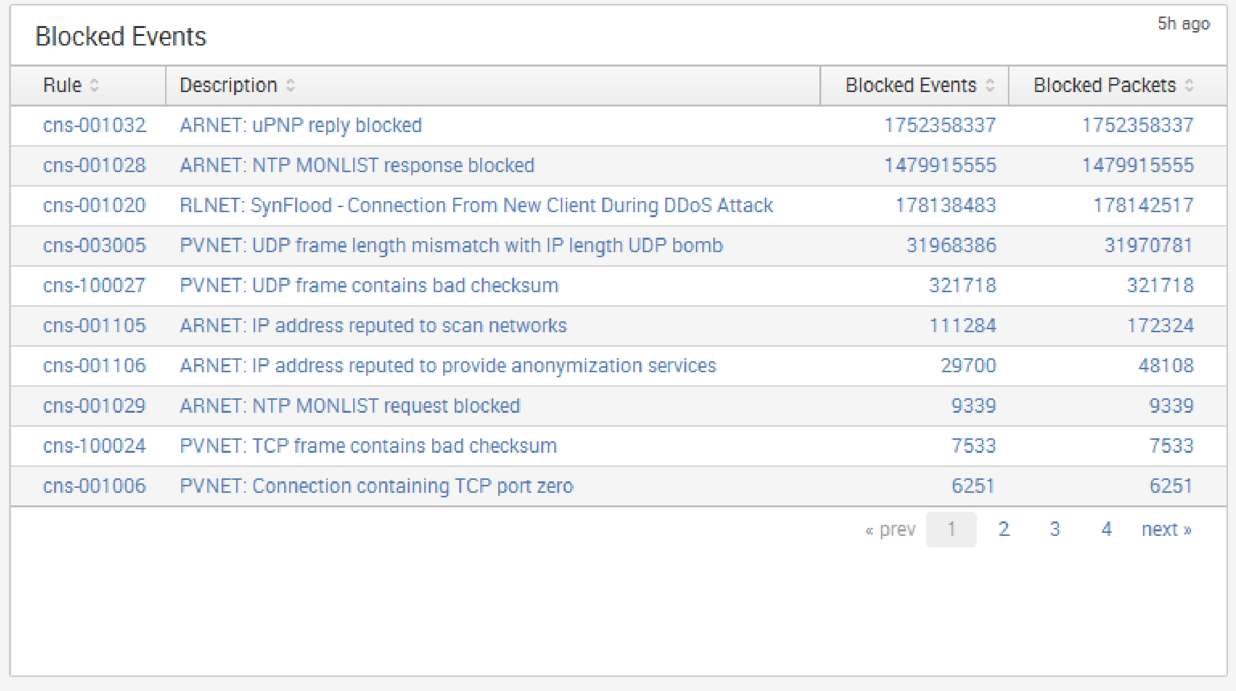
Top 10 Rule Types Detected Chart

This chart shows the ten rules set to Detect that were triggered most (based on packets per second) in the specified time period:



Blocked Events Table

This table shows the number of events and packets associated with triggered rules that were set to Block. The chart can be sorted using any field; by default, it is sorted in decreasing order of the number of events associated with each rule.



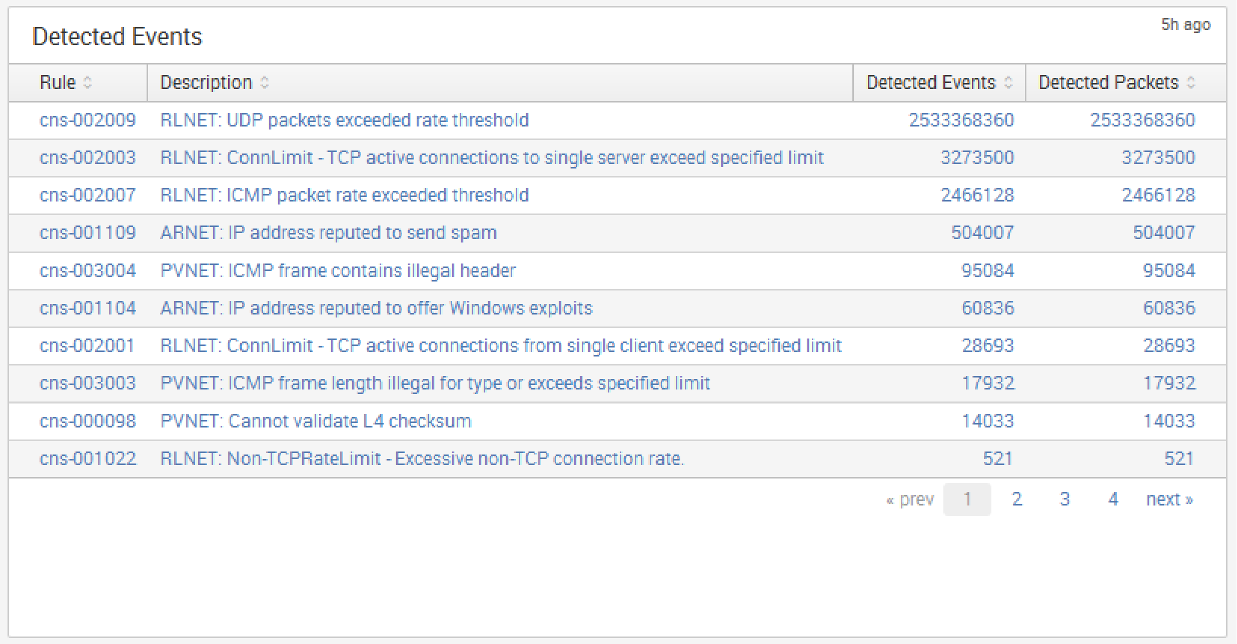
Blocked Events

5h ago

Rule	Description	Blocked Events	Blocked Packets
cns-001032	ARNET: uPNP reply blocked	1752358337	1752358337
cns-001028	ARNET: NTP MONLIST response blocked	1479915555	1479915555
cns-001020	RLNET: SynFlood - Connection From New Client During DDoS Attack	178138483	178142517
cns-003005	PVNET: UDP frame length mismatch with IP length UDP bomb	31968386	31970781
cns-100027	PVNET: UDP frame contains bad checksum	321718	321718
cns-001105	ARNET: IP address reputed to scan networks	111284	172324
cns-001106	ARNET: IP address reputed to provide anonymization services	29700	48108
cns-001029	ARNET: NTP MONLIST request blocked	9339	9339
cns-100024	PVNET: TCP frame contains bad checksum	7533	7533
cns-001006	PVNET: Connection containing TCP port zero	6251	6251

Detected Events Table

This table shows the number of events and packets associated with triggered rules that were set to Detect. The chart can be sorted using any field; by default, it is sorted in decreasing order of the number of events associated with each rule.



Detected Events

5h ago

Rule	Description	Detected Events	Detected Packets
cns-002009	RLNET: UDP packets exceeded rate threshold	2533368360	2533368360
cns-002003	RLNET: ConnLimit - TCP active connections to single server exceed specified limit	3273500	3273500
cns-002007	RLNET: ICMP packet rate exceeded threshold	2466128	2466128
cns-001109	ARNET: IP address reputed to send spam	504007	504007
cns-003004	PVNET: ICMP frame contains illegal header	95084	95084
cns-001104	ARNET: IP address reputed to offer Windows exploits	60836	60836
cns-002001	RLNET: ConnLimit - TCP active connections from single client exceed specified limit	28693	28693
cns-003003	PVNET: ICMP frame length illegal for type or exceeds specified limit	17932	17932
cns-000098	PVNET: Cannot validate L4 checksum	14033	14033
cns-001022	RLNET: Non-TCPRateLimit - Excessive non-TCP connection rate.	521	521

Top Charts

Click **Top Charts** in the Analytics application tool bar to display the Top Charts screen. This screen provides a set of tools that show you the elements of your security infrastructure that have experienced the greatest activity or utilization over the specified time frame. Each of the Top Charts shows that type of activity/utilization as a percentage of the total at that time. These tools are useful in helping you to identify and characterize excessive or otherwise aberrant activity that may indicate attacks on your server infrastructure.

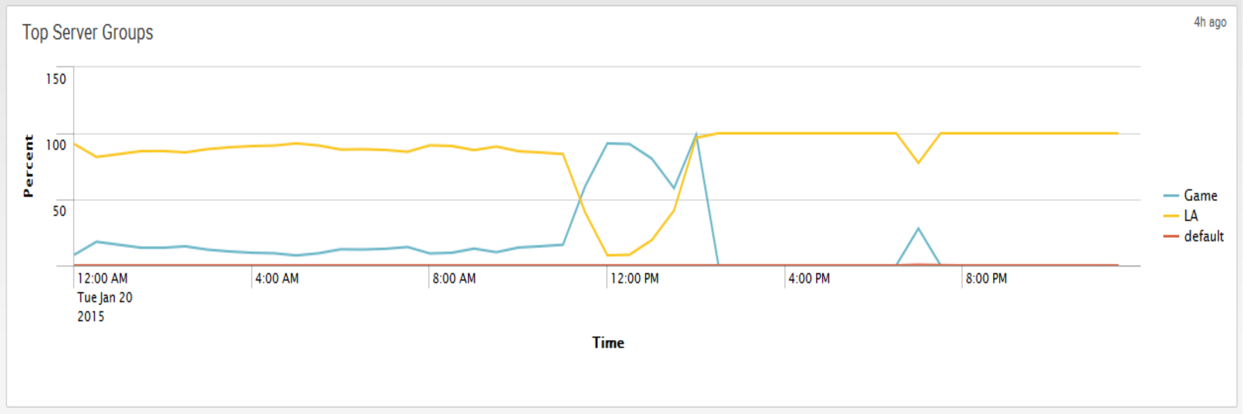
The Top Charts include:

- Top Server Groups
- Top Source IP Addresses
- Top Destination IP Addresses
- Top Source Ports
- Top Destination Ports
- Top TTL Values
- Top IP Packet Lengths

Control the content of your top charts by specifying the site and time frame for which to display data. Each chart shows the five largest contributors for that statistic, plus an "Other" entry that comprises all contributors that are not among the top five.

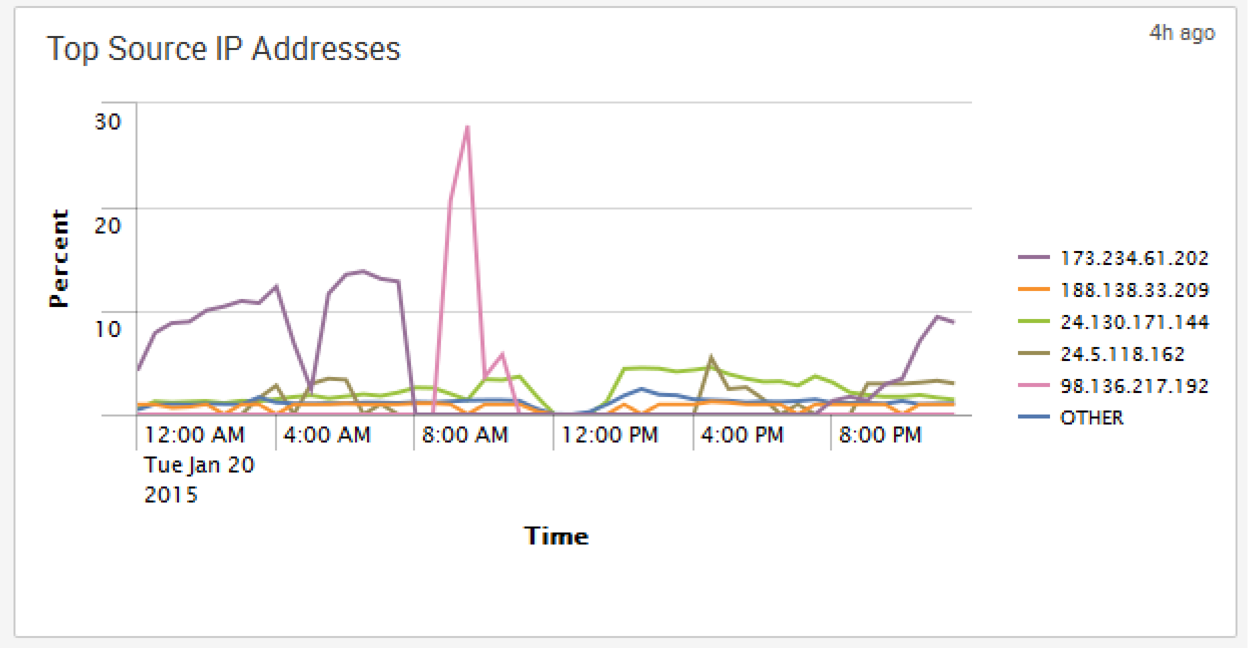
Top Server Groups

The Top Server Groups chart shows the five most heavily accessed server groups in the selected site for the specified time frame.



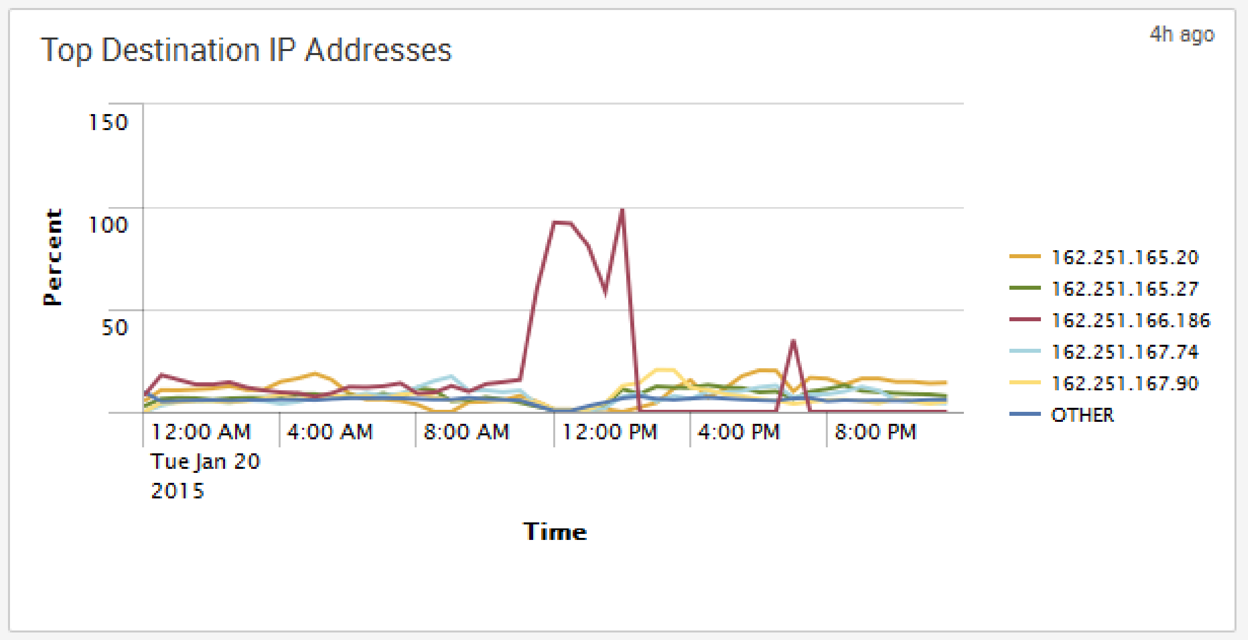
Top Source IP Addresses

The Top Source IP Addresses chart shows the five IP addresses from which the most inbound traffic originated during the specified time frame.



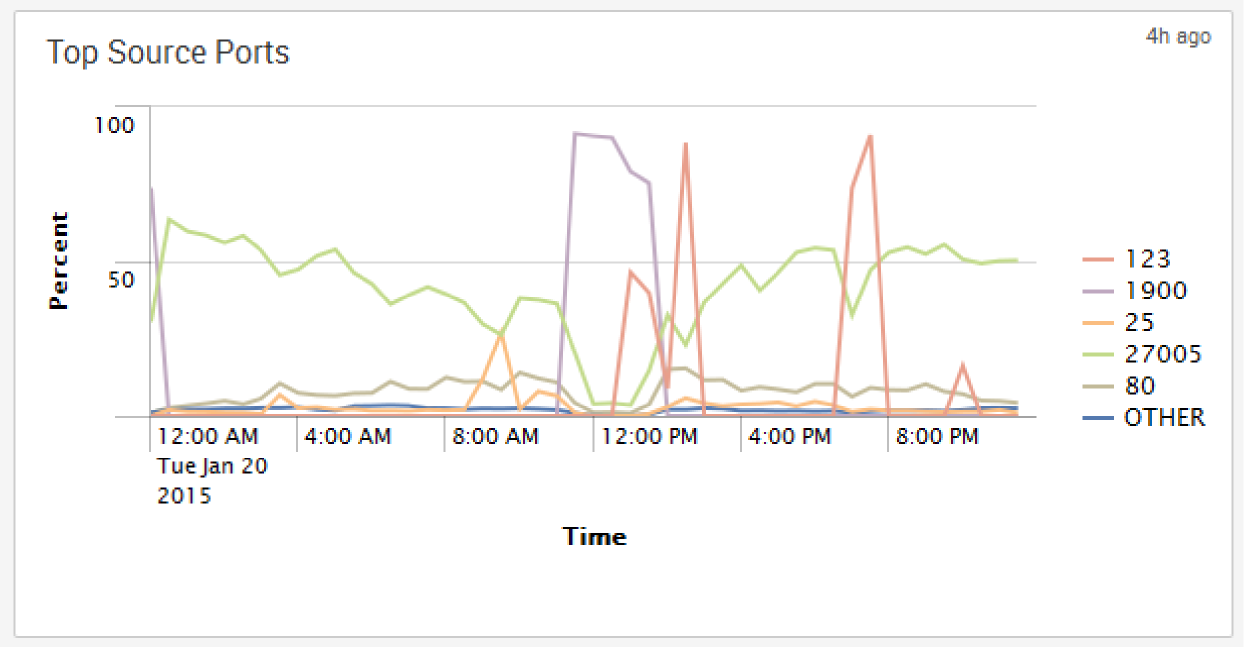
Top Destination IP Addresses

The Top Destination IP Addresses chart shows the five IP addresses to which the most inbound traffic was directed during the specified time frame.



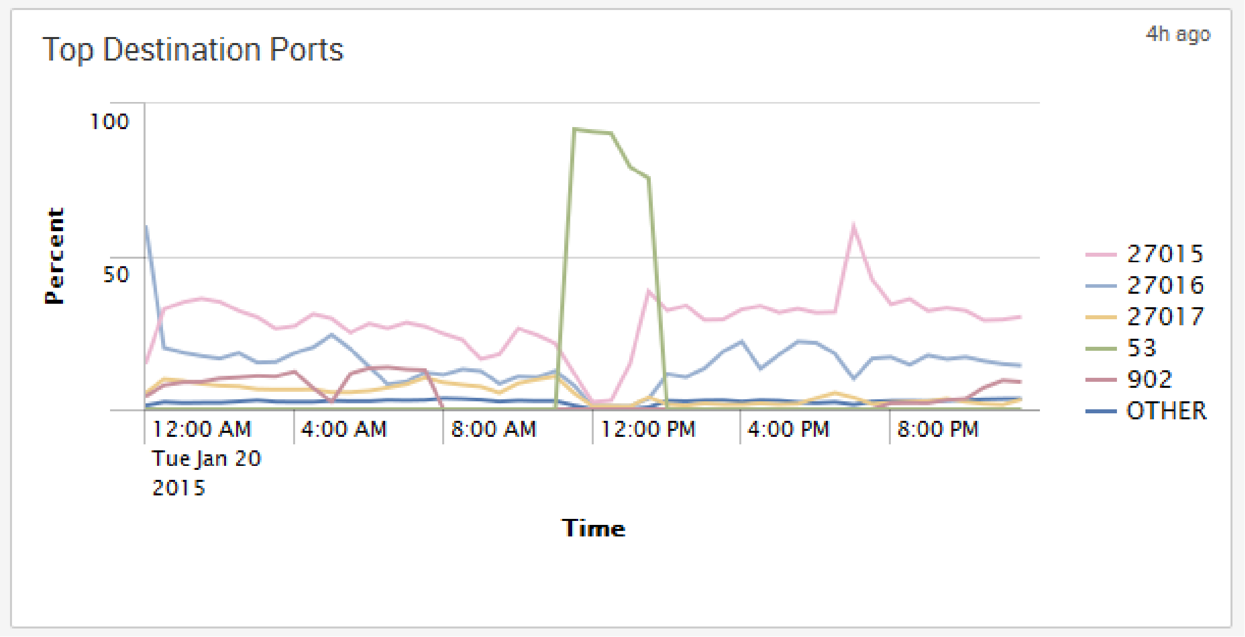
Top Source Ports

The Top Source Ports chart shows the five port IDs from which the most inbound traffic originated during the specified time frame.



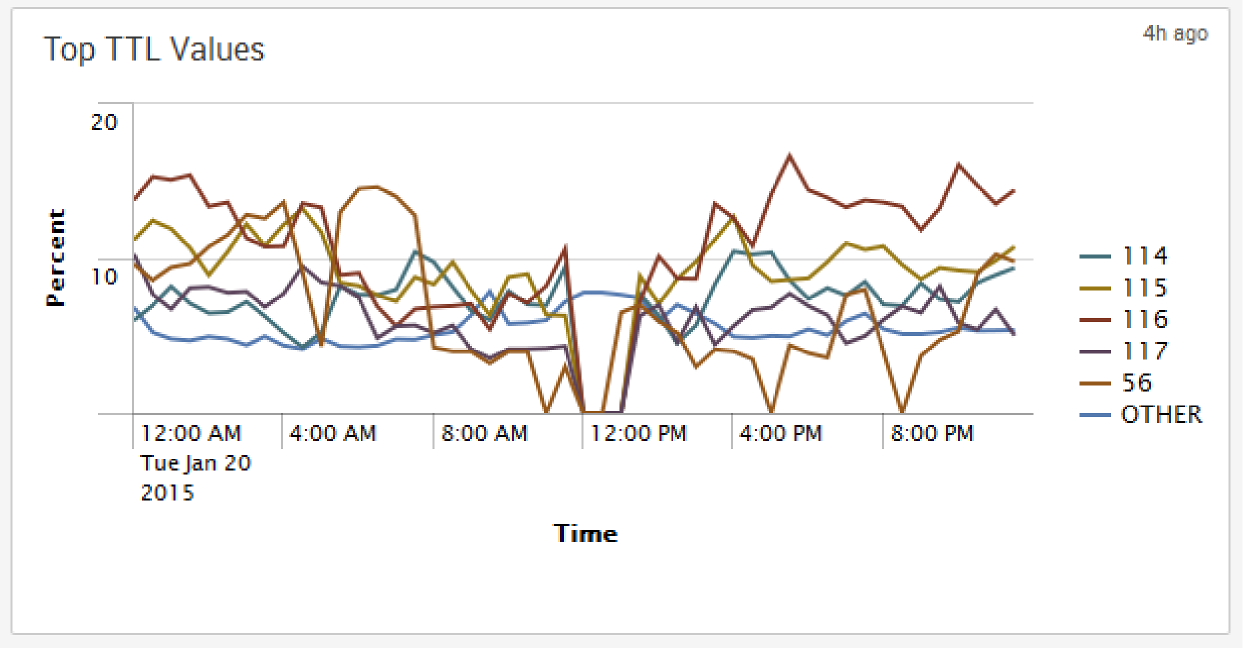
Top Destination Ports

The Top Destination Ports chart shows the five port IDs to which the most inbound traffic was directed during the specified time frame.



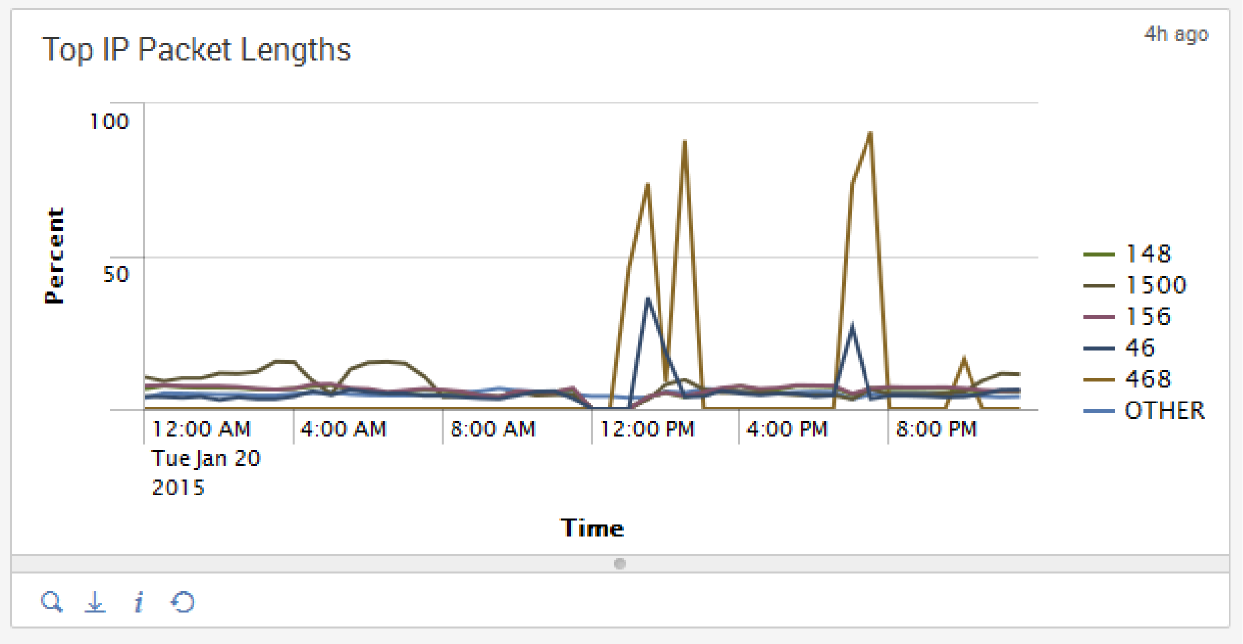
Top TTL Values

The Top TTL Values chart shows the five time-to-live values that occurred most frequently among inbound packets during the specified time frame. A disproportionate or otherwise unusual number of packets with the same TTL value may be indicative of an attack.



Top IP Packet Lengths

The Top IP Packet Lengths chart shows the five packet length values that occurred most frequently among inbound packets during the specified time frame.



Drilldown Charts

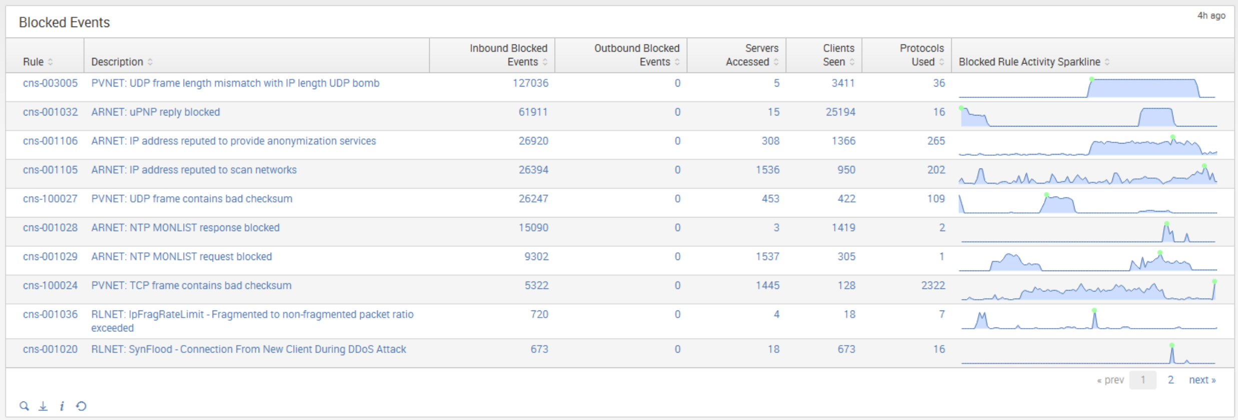
The Drilldown charts show greater detail.

The Drilldown charts include:

- Blocked Events
- Detected Events
- Servers Involved in Security Events
- Top Server Ports That Are Involved in Security Events Table
- Clients Involved in Security Events
- Client Ports Involved in Security Events
- Packet Lengths Involved in Security Events
- Syslog Events

Blocked Events

This chart provides detailed information about each event associated with the trigger of a blocking rule during the specified time interval.



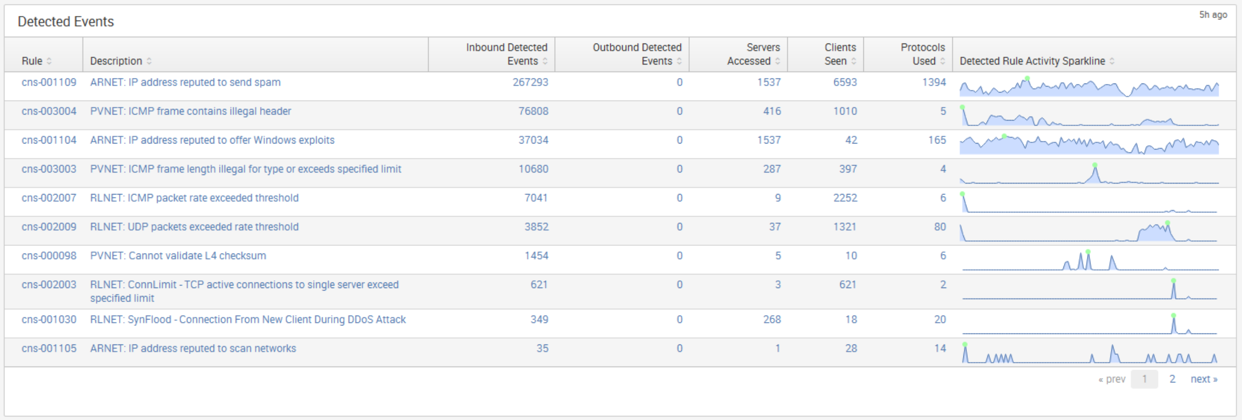
Blocked Events

4h ago

Rule	Description	Inbound Blocked Events	Outbound Blocked Events	Servers Accessed	Clients Seen	Protocols Used	Blocked Rule Activity Sparkline
cns-003005	PVNET: UDP frame length mismatch with IP length UDP bomb	127036	0	5	3411	36	
cns-001032	ARNET: uPNP reply blocked	61911	0	15	25194	16	
cns-001106	ARNET: IP address reputed to provide anonymization services	26920	0	308	1366	265	
cns-001105	ARNET: IP address reputed to scan networks	26394	0	1536	950	202	
cns-100027	PVNET: UDP frame contains bad checksum	26247	0	453	422	109	
cns-001028	ARNET: NTP MONLIST response blocked	15090	0	3	1419	2	
cns-001029	ARNET: NTP MONLIST request blocked	9302	0	1537	305	1	
cns-100024	PVNET: TCP frame contains bad checksum	5322	0	1445	128	2322	
cns-001036	RLNET: IpFragRateLimit - Fragmented to non-fragmented packet ratio exceeded	720	0	4	18	7	
cns-001020	RLNET: SynFlood - Connection From New Client During DDoS Attack	673	0	18	673	16	

Detected Events

This chart provides detailed information about each event associated with the trigger of a detecting rule during the specified time interval:



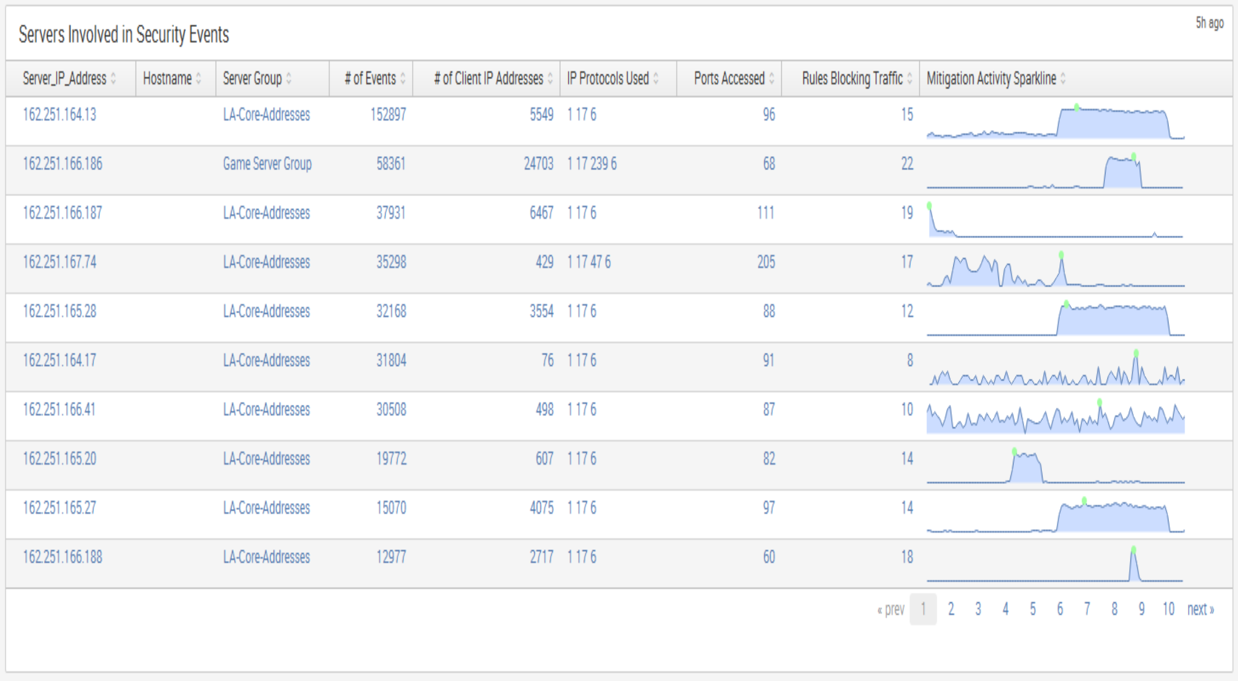
Detected Events

5h ago

Rule ⇕	Description ⇕	Inbound Detected Events ⇕	Outbound Detected Events ⇕	Servers Accessed ⇕	Clients Seen ⇕	Protocols Used ⇕	Detected Rule Activity Sparkline ⇕
cns-001109	ARNET: IP address reputed to send spam	267293	0	1537	6593	1394	
cns-003004	PVNET: ICMP frame contains illegal header	76808	0	416	1010	5	
cns-001104	ARNET: IP address reputed to offer Windows exploits	37034	0	1537	42	165	
cns-003003	PVNET: ICMP frame length illegal for type or exceeds specified limit	10680	0	287	397	4	
cns-002007	RLNET: ICMP packet rate exceeded threshold	7041	0	9	2252	6	
cns-002009	RLNET: UDP packets exceeded rate threshold	3852	0	37	1321	80	
cns-000098	PVNET: Cannot validate L4 checksum	1454	0	5	10	6	
cns-002003	RLNET: ConnLimit - TCP active connections to single server exceed specified limit	621	0	3	621	2	
cns-001030	RLNET: SynFlood - Connection From New Client During DDoS Attack	349	0	268	18	20	
cns-001105	ARNET: IP address reputed to scan networks	35	0	1	28	14	

Servers Involved in Security Events

This chart lists the servers associated with any security event that has been identified by the SmartWall Threat Defense System. The chart can be sorted using any field; by default, it is sorted in decreasing order of the number of events associated with each server.



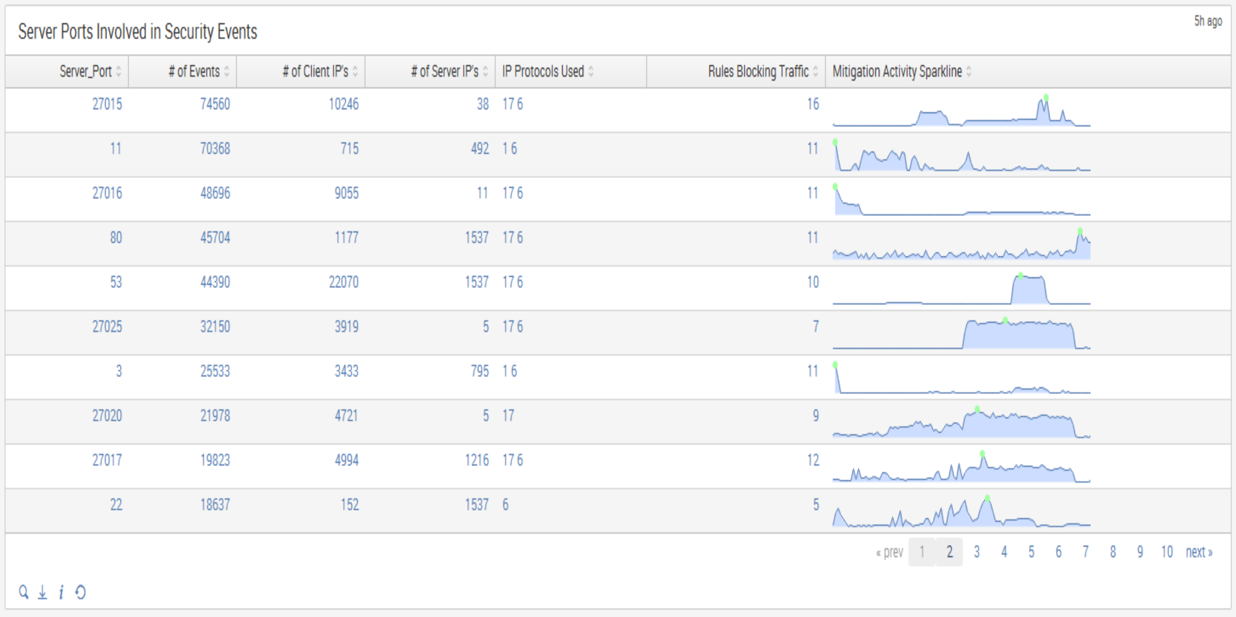
Servers Involved in Security Events

5h ago

Server_IP_Address	Hostname	Server Group	# of Events	# of Client IP Addresses	IP Protocols Used	Ports Accessed	Rules Blocking Traffic	Mitigation Activity Sparkline
162.251.164.13		LA-Core-Addresses	152897	5549	1 17 6	96	15	
162.251.166.186		Game Server Group	58361	24703	1 17 239 6	68	22	
162.251.166.187		LA-Core-Addresses	37931	6467	1 17 6	111	19	
162.251.167.74		LA-Core-Addresses	35298	429	1 17 47 6	205	17	
162.251.165.28		LA-Core-Addresses	32168	3554	1 17 6	88	12	
162.251.164.17		LA-Core-Addresses	31804	76	1 17 6	91	8	
162.251.166.41		LA-Core-Addresses	30508	498	1 17 6	87	10	
162.251.165.20		LA-Core-Addresses	19772	607	1 17 6	82	14	
162.251.165.27		LA-Core-Addresses	15070	4075	1 17 6	97	14	
162.251.166.188		LA-Core-Addresses	12977	2717	1 17 6	60	18	

Server Ports Involved in Security Events Table

The Top Server Ports That Are Involved in Security Events table displays the top 50 server ports that inbound blocked security events were triggered for during the time period. This report is created by reviewing top talker reports to determine the most active destination server port during a given time period based on a time based statistical sampling algorithm. These destination ports are cross-referenced with security event information to determine what security events are triggering due to this activity. Click on one of the rows to drill down to the server port in that row.

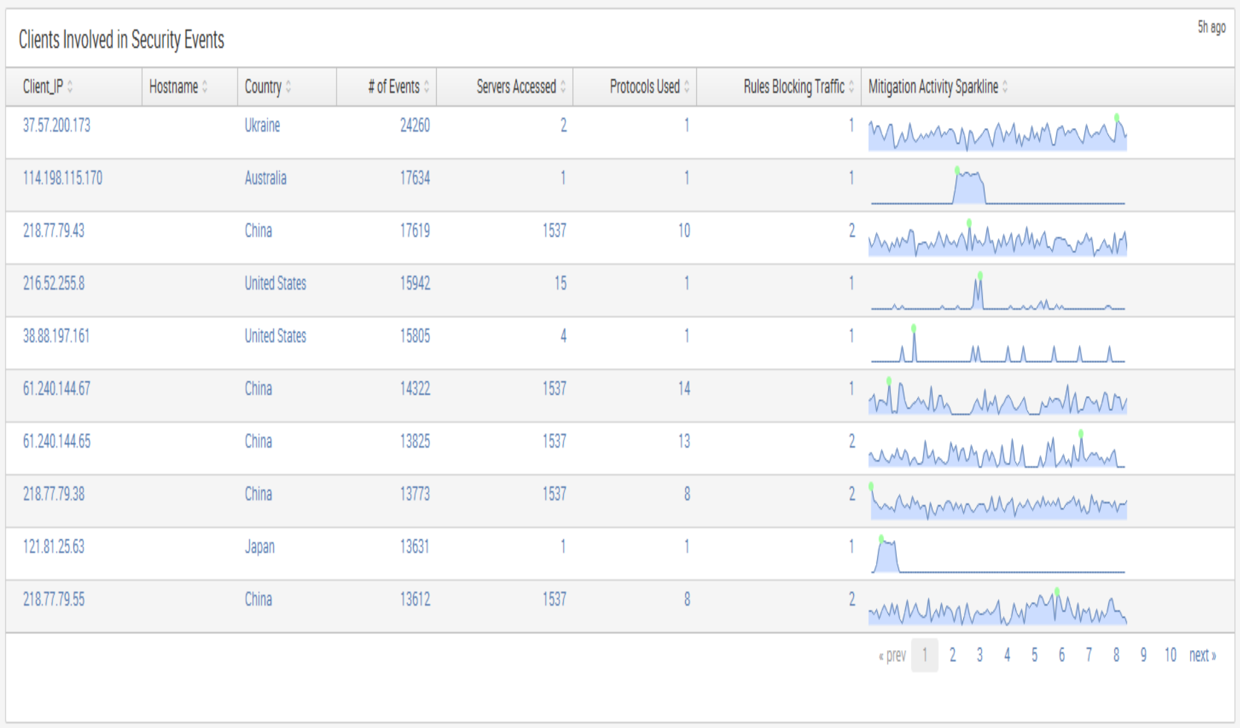


Server Ports Involved in Security Events

Server_Port	# of Events	# of Client IP's	# of Server IP's	IP Protocols Used	Rules Blocking Traffic	Mitigation Activity Sparkline
27015	74560	10246	38	17 6	16	
11	70368	715	492	1 6	11	
27016	48696	9055	11	17 6	11	
80	45704	1177	1537	17 6	11	
53	44390	22070	1537	17 6	10	
27025	32150	3919	5	17 6	7	
3	25533	3433	795	1 6	11	
27020	21978	4721	5	17	9	
27017	19823	4994	1216	17 6	12	
22	18637	152	1537	6	5	

Clients Involved in Security Events

This chart lists the clients associated with any security event that has been identified by the SmartWall Threat Defense System. The chart can be sorted using any field; by default, it is sorted in decreasing order of the number of events associated with each client.



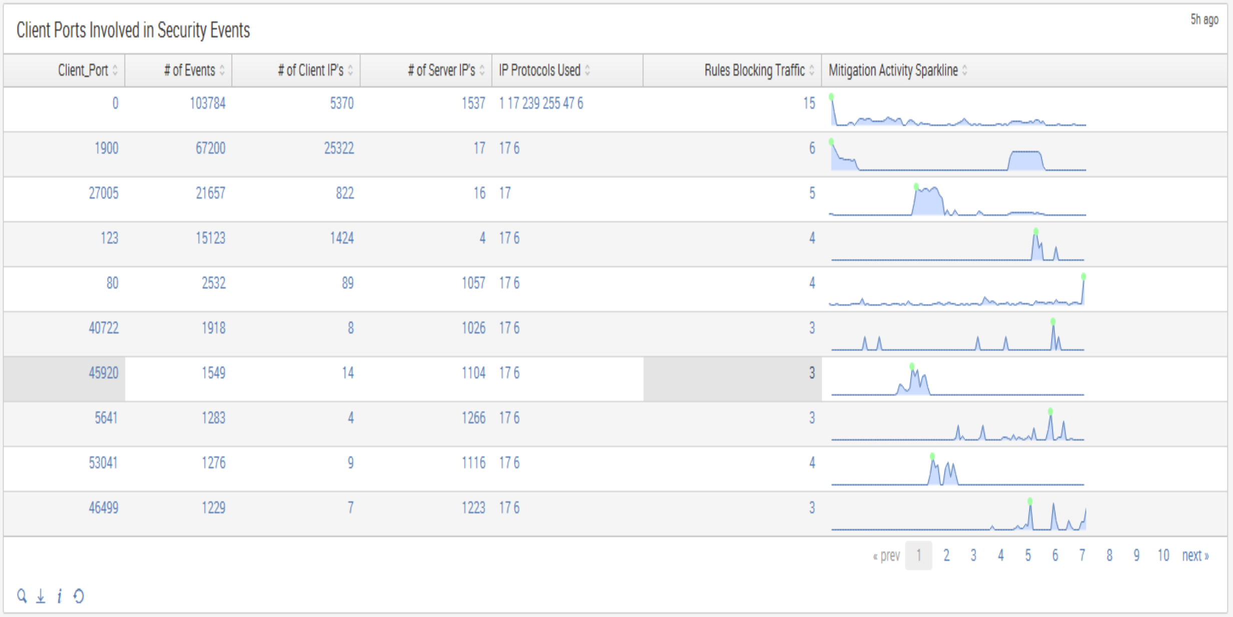
Clients Involved in Security Events

5h ago

Client_IP	Hostname	Country	# of Events	Servers Accessed	Protocols Used	Rules Blocking Traffic	Mitigation Activity Sparkline
37.57.200.173		Ukraine	24260	2	1	1	
114.198.115.170		Australia	17634	1	1	1	
218.77.79.43		China	17619	1537	10	2	
216.52.255.8		United States	15942	15	1	1	
38.88.197.161		United States	15805	4	1	1	
61.240.144.67		China	14322	1537	14	1	
61.240.144.65		China	13825	1537	13	2	
218.77.79.38		China	13773	1537	8	2	
121.81.25.63		Japan	13631	1	1	1	
218.77.79.55		China	13612	1537	8	2	

Client Ports Involved in Security Events

This chart lists the client ports associated with any security event that has been identified by the SmartWall Threat Defense System. The chart can be sorted using any field; by default, it is sorted in decreasing order of the number of events associated with each client port.



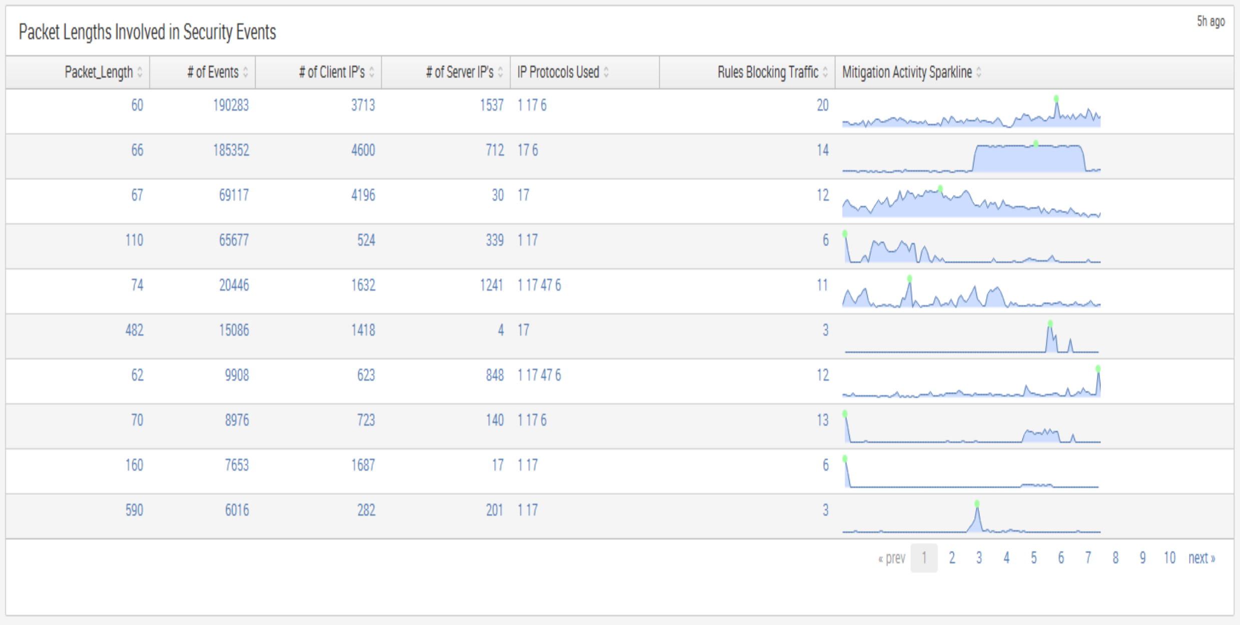
Client Ports Involved in Security Events

5h ago

Client_Port	# of Events	# of Client IP's	# of Server IP's	IP Protocols Used	Rules Blocking Traffic	Mitigation Activity Sparkline
0	103784	5370	1537	1 17 239 255 47 6	15	
1900	67200	25322	17	17 6	6	
27005	21657	822	16	17	5	
123	15123	1424	4	17 6	4	
80	2532	89	1057	17 6	4	
40722	1918	8	1026	17 6	3	
45920	1549	14	1104	17 6	3	
5641	1283	4	1266	17 6	3	
53041	1276	9	1116	17 6	4	
46499	1229	7	1223	17 6	3	

Packet Lengths Involved in Security Events

This chart lists the packet lengths associated with any security event that has been identified by the SmartWall Threat Defense System. A disproportionate or otherwise unusual number of packets with the same packet length may be indicative of an attack. The chart can be sorted using any field; by default, it is sorted in decreasing order of the number of events associated with each client.

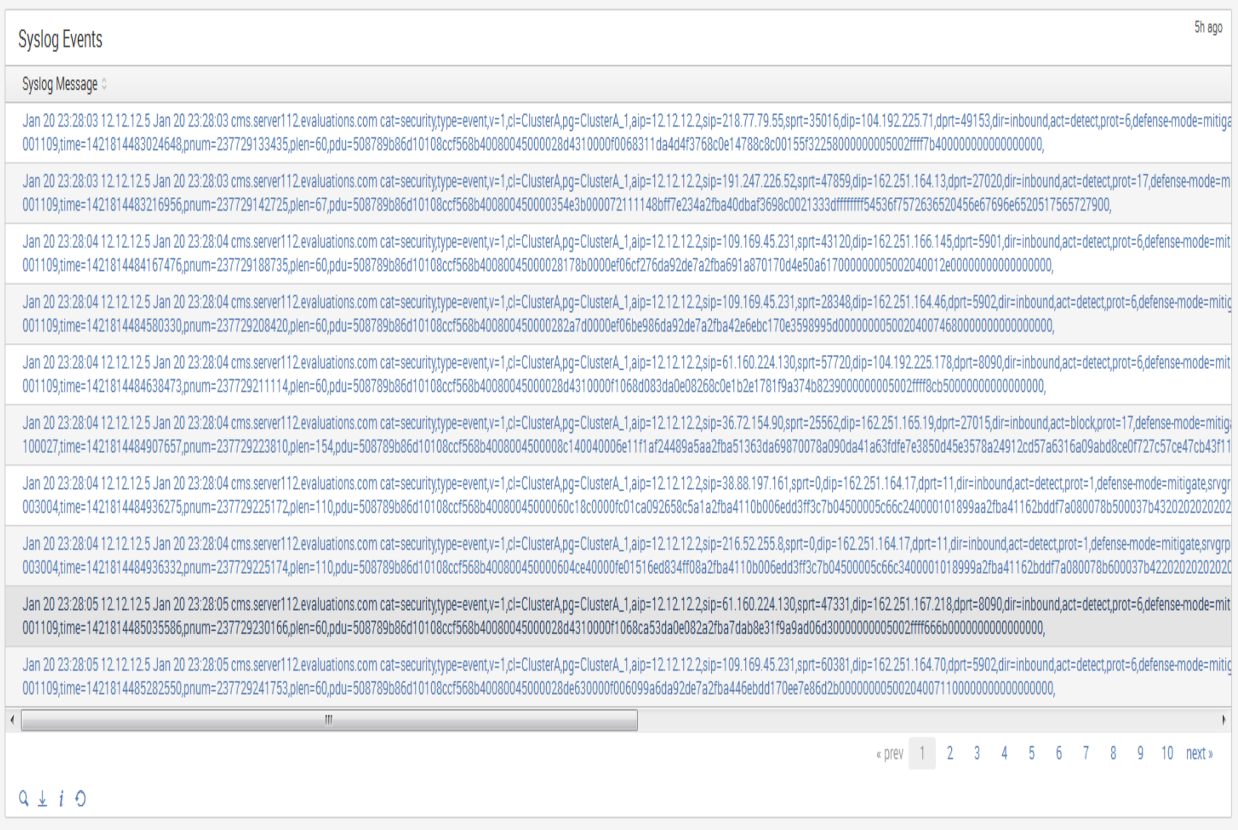


Packet Lengths Involved in Security Events

Packet_Length	# of Events	# of Client IP's	# of Server IP's	IP Protocols Used	Rules Blocking Traffic	Mitigation Activity Sparkline
60	190283	3713	1537	1 17 6	20	
66	185352	4600	712	17 6	14	
67	69117	4196	30	17	12	
110	65677	524	339	1 17	6	
74	20446	1632	1241	1 17 47 6	11	
482	15086	1418	4	17	3	
62	9908	623	848	1 17 47 6	12	
70	8976	723	140	1 17 6	13	
160	7653	1687	17	1 17	6	
590	6016	282	201	1 17	3	

Syslog Events

This chart lists the syslog events that are associated with the data that you are examining.



```
Jan 20 23:28:03 12.12.12.5 Jan 20 23:28:03 cms.server112.evaluations.com cat=security,type=event,v=1,cl=ClusterA,pg=ClusterA_1,aip=12.12.12.2,sip=218.77.79.55,sprt=35016,dip=104.192.225.71,dprt=49153,dir=inbound,act=detect,prot=6,defense-mode=mitiga
001109,time=1421814483024648,pnum=237729133435,plen=60,pdu=508789b86d10108ccf568b40080045000028d4310000f0068311da4d4f3768c0e14788c8c00155f3225800000000005002ffff7b4000000000000000000,

Jan 20 23:28:03 12.12.12.5 Jan 20 23:28:03 cms.server112.evaluations.com cat=security,type=event,v=1,cl=ClusterA,pg=ClusterA_1,aip=12.12.12.2,sip=191.247.226.52,sprt=47859,dip=162.251.164.13,dprt=27020,dir=inbound,act=detect,prot=17,defense-mode=m
001109,time=1421814483216956,pnum=237729142725,plen=67,pdu=508789b86d10108ccf568b400800450000354e3b00007211148bff7e234a2fba40dbaf3698c0021333dffffffff54536f7572636520456e67696e6520517565727900,

Jan 20 23:28:04 12.12.12.5 Jan 20 23:28:04 cms.server112.evaluations.com cat=security,type=event,v=1,cl=ClusterA,pg=ClusterA_1,aip=12.12.12.2,sip=109.169.45.231,sprt=43120,dip=162.251.166.145,dprt=5901,dir=inbound,act=detect,prot=6,defense-mode=mit
001109,time=1421814484167476,pnum=237729188735,plen=60,pdu=508789b86d10108ccf568b40080045000028178b0000ef06cf276da92de7a2fba691a870170d4e50a61700000000005002040012e0000000000000000,

Jan 20 23:28:04 12.12.12.5 Jan 20 23:28:04 cms.server112.evaluations.com cat=security,type=event,v=1,cl=ClusterA,pg=ClusterA_1,aip=12.12.12.2,sip=109.169.45.231,sprt=28348,dip=162.251.164.46,dprt=5902,dir=inbound,act=detect,prot=6,defense-mode=mitig
001109,time=1421814484580330,pnum=237729208420,plen=60,pdu=508789b86d10108ccf568b400800450000282a7d0000ef06be986da92de7a2fba42e6ebc170e3598995d000000005002040074680000000000000000,

Jan 20 23:28:04 12.12.12.5 Jan 20 23:28:04 cms.server112.evaluations.com cat=security,type=event,v=1,cl=ClusterA,pg=ClusterA_1,aip=12.12.12.2,sip=61.160.224.130,sprt=57720,dip=104.192.225.178,dprt=8090,dir=inbound,act=detect,prot=6,defense-mode=mit
001109,time=1421814484638473,pnum=237729211114,plen=60,pdu=508789b86d10108ccf568b40080045000028d4310000f1068d083da0e08268c0e1b2e1781f9a374b823900000000005002ffff8cb5000000000000000,

Jan 20 23:28:04 12.12.12.5 Jan 20 23:28:04 cms.server112.evaluations.com cat=security,type=event,v=1,cl=ClusterA,pg=ClusterA_1,aip=12.12.12.2,sip=36.72.154.90,sprt=25562,dip=162.251.165.19,dprt=27015,dir=inbound,act=block,prot=17,defense-mode=mitig
100027,time=1421814484907657,pnum=237729223810,plen=154,pdu=508789b86d10108ccf568b4008004500008c140040006e11f1af24489a5aa2fba51363da69870078a090da41a63fdfe7e3850d45e3578a24912cd57a6316a09abd8ce0f727c57ce47cb43f11

Jan 20 23:28:04 12.12.12.5 Jan 20 23:28:04 cms.server112.evaluations.com cat=security,type=event,v=1,cl=ClusterA,pg=ClusterA_1,aip=12.12.12.2,sip=38.88.197.161,sprt=0,dip=162.251.164.17,dprt=11,dir=inbound,act=detect,prot=1,defense-mode=mitigate,srvgr
003004,time=1421814484936275,pnum=237729225172,plen=110,pdu=508789b86d10108ccf568b40080045000060c18c0000fc01ca092658c5a1a2fba4110b006edd3ff3c7b04500005c66c240000101899aa2fba41162bddf7a080078b500037b432020202020202

Jan 20 23:28:04 12.12.12.5 Jan 20 23:28:04 cms.server112.evaluations.com cat=security,type=event,v=1,cl=ClusterA,pg=ClusterA_1,aip=12.12.12.2,sip=216.52.255.8,sprt=0,dip=162.251.164.17,dprt=11,dir=inbound,act=detect,prot=1,defense-mode=mitigate,srvgrp
003004,time=1421814484936332,pnum=237729225174,plen=110,pdu=508789b86d10108ccf568b400800450000604ce40000fe01516ed834ff08a2fba4110b006edd3ff3c7b04500005c66c3400001018999a2fba41162bddf7a080078b600037b42202020202020

Jan 20 23:28:05 12.12.12.5 Jan 20 23:28:05 cms.server112.evaluations.com cat=security,type=event,v=1,cl=ClusterA,pg=ClusterA_1,aip=12.12.12.2,sip=61.160.224.130,sprt=47331,dip=162.251.167.218,dprt=8090,dir=inbound,act=detect,prot=6,defense-mode=mit
001109,time=1421814485035586,pnum=237729230166,plen=60,pdu=508789b86d10108ccf568b40080045000028d4310000f1068ca53da0e082a2fba7dab8e31f9a9ad06d30000000005002ffff666b0000000000000000,

Jan 20 23:28:05 12.12.12.5 Jan 20 23:28:05 cms.server112.evaluations.com cat=security,type=event,v=1,cl=ClusterA,pg=ClusterA_1,aip=12.12.12.2,sip=109.169.45.231,sprt=60381,dip=162.251.164.70,dprt=5902,dir=inbound,act=detect,prot=6,defense-mode=mitig
001109,time=1421814485282550,pnum=237729241753,plen=60,pdu=508789b86d10108ccf568b40080045000028de630000f006099a6da92de7a2fba446ebdd170ee7e86d2b0000000050020400711000000000000000000,
```