Using the Context Explorer

The FireSIGHT System Context Explorer displays detailed, interactive graphical information in context about the status of your monitored network, including data on applications, application statistics, connections, geolocation, indications of compromise, intrusion events, hosts, servers, Security Intelligence, users, files (including malware files), and relevant URLs. Distinct sections present this data in the form of vivid line, bar, pie, and donut graphs, accompanied by detailed lists.

You can easily create and apply custom filters to fine-tune your analysis, and you can examine data sections in more detail by simply clicking or hovering your cursor over graph areas. You can also configure the explorer's time range to reflect a period as short as the last hour or as long as the last year. Only users with the Administrator, Security Analyst, or Security Analyst (Read Only) user roles have access to the Context Explorer.

The FireSIGHT System dashboard is highly customizable and compartmentalized and updates in real time. In contrast, the Context Explorer is manually updated, designed to provide broader context for its data, and has a single, consistent layout designed for active user exploration.

You use the dashboard to monitor real-time activity on your network and appliances according to your own specific needs. Conversely, you use the Context Explorer to investigate a predefined set of recent FireSIGHT data in granular detail and clear context: for example, if you notice that only 15% of hosts on your network use Linux, but account for almost all YouTube traffic, you can quickly apply filters to view data only for Linux hosts, only for YouTube-associated application data, or both. Unlike the compact, narrowly focused dashboard widgets, the Context Explorer sections are designed to provide striking visual representations of system activity in a format useful to both expert and casual users of the FireSIGHT System.

Note that the data displayed depends on such factors as how you license and deploy your managed devices, whether you configure features that provide the data and, in the case of Series 2 appliances and Cisco NGIPS for Blue Coat X-Series, whether the appliance supports a feature that provides the data. For example, neither the DC500 Defense Center nor Series 2 devices or Cisco NGIPS for Blue Coat X-Series support advanced malware protection, so the DC500 Defense Center cannot display this data and Series 2 devices and Cisco NGIPS for Blue Coat X-Series do not detect it.

The following table summarizes some of the key differences between the dashboard and the Context Explorer.

Table 56-1 Comparison: Dashboard and Context Explorer

Feature	Dashboard	Context Explorer
Displayable data	Anything monitored by the FireSIGHT System	Applications, application statistics, geolocation, indications of compromise, intrusion events, files (including malware files), hosts, Security Intelligence events, servers, users, and URLs
Customizability	• Selection of widgets for a dashboard is customizable • Individual widgets can be customized to varying degrees	• Cannot change base layout • Applied filters appear in explorer URL and can be bookmarked for later use
Data update frequency	Automatic (default); user-configured	Manual
Data filtering	Possible for some widgets (must edit widget preferences)	Possible for all parts of the explorer, with support for multiple filters
Graphical context	Some widgets (particularly Custom Analysis) can display data in graph form	Extensive graphical context for all data, including uniquely detailed donut graphs
Links to relevant web interface pages	In some widgets	In every section
Time range of displayed data	User-configured	User-configured

For more information on the related FireSIGHT System dashboard, see Using Dashboards, page 55-1.

Understanding the Context Explorer

License: FireSIGHT

The Context Explorer comprises several distinct sections that together offer a complete overview of FireSIGHT data on your monitored network. The first section, a line chart of traffic and event counts over time, provides an at-a-glance picture of recent trends in your network's activity.

The other sections are sets of interactive graphs and lists that provide greater detail for indications of compromise, network, application, Security Intelligence, intrusion, file, geolocation, and URL data. Except for the traffic and events time graph, you can view or hide any section. You can also apply filters to constrain the data that appears in all sections; see Working with Filters in the Context Explorer, page 56-40 for more information.

For in-depth information on the content and function of Context Explorer sections, see the following topics:

- Understanding the Files Information Section, page 56-24
- Understanding the Geolocation Information Section, page 56-31
- Understanding the URL Information Section, page 56-34

For information on how to configure the Context Explorer as a whole, see the following topics:

- Refreshing the Context Explorer, page 56-37
- Setting the Context Explorer Time Range, page 56-38
- Minimizing and Maximizing Context Explorer Sections, page 56-38
- Drilling Down on Context Explorer Data, page 56-39

For information on configuring and using Context Explorer filters, see the following topics:

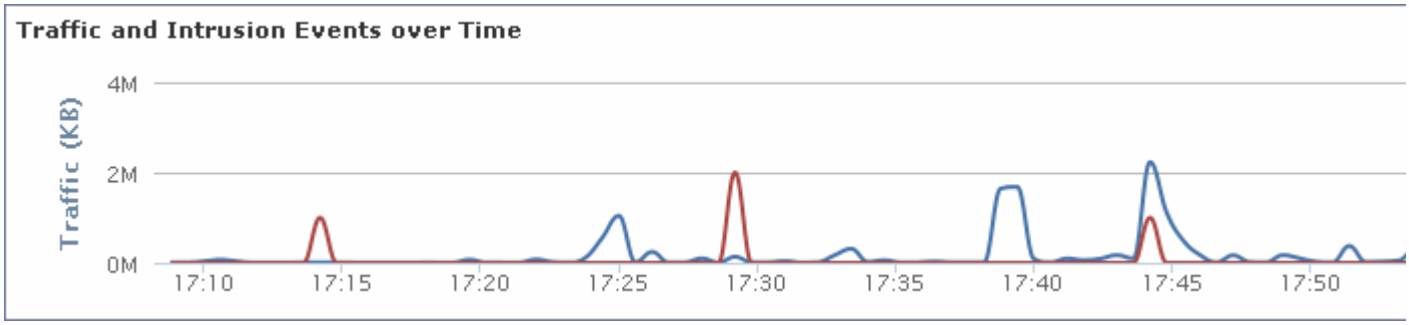
- Working with Filters in the Context Explorer, page 56-40
- Adding and Applying Filters, page 56-40
- Creating Filters with the Context Menu, page 56-44
- Bookmarking Filters, page 56-45

Understanding the Traffic and Intrusion Event Counts Time Graph

License: FireSIGHT

At the top of the Context Explorer is a line chart of traffic and intrusion events over time. The X-axis plots time intervals (which range from five minutes to one month, depending on the selected time window). The Y-axis plots traffic in kilobytes (blue line) and intrusion event count (red line).

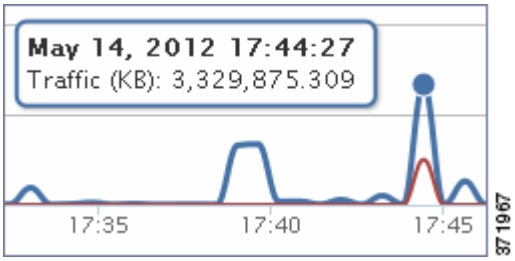
Note that the smallest X-axis interval is five minutes. To accommodate this, the system will round the beginning and ending points in your selected time range down to the nearest five-minute interval.



By default, this section shows all network traffic and all generated intrusion events for the selected time range. If you apply filters, the chart changes to display only traffic and intrusion events associated with the criteria specified in the filters. For example, filtering on the **OS Name** of `Windows` causes the time graph to display only traffic and events associated with hosts using Windows operating systems.

If you filter the Context Explorer on intrusion event data (such as a **Priority** of `High`), the blue Traffic line is hidden to allow greater focus on intrusion events alone.

You can hover your pointer over any point on the graph lines to view exact information about traffic and event counts. Hovering your pointer over one of the colored lines also brings that line to the forefront of the graph, providing clearer context.



This section draws data primarily from the Intrusion Events and Connection Events tables.

Understanding the Indications of Compromise Section

License: FireSIGHT

The Indications of Compromise (IOC) section of the Context Explorer contains two interactive sections that provide an overall picture of potentially compromised hosts on your monitored network: a proportional view of the most prevalent IOC types triggered, as well as a view of hosts by number of triggered indications.

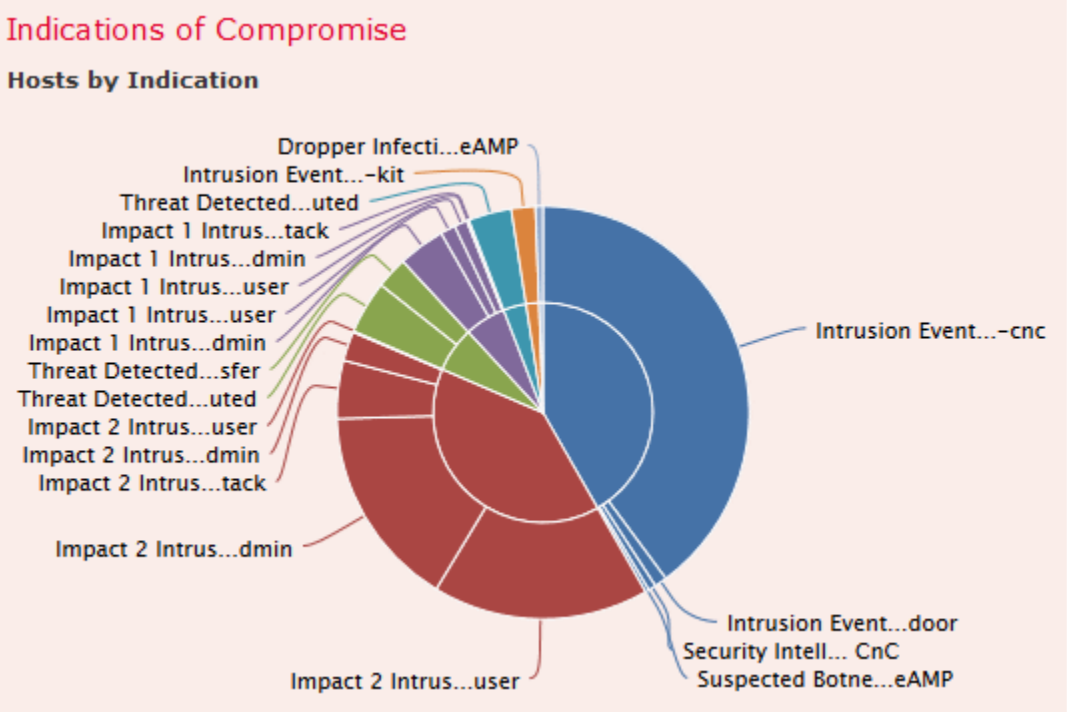
For more information on the graphs in the Indications of Compromise section, see the following topics:

- Viewing the Hosts by Indication Graph, page 56-4
- Viewing the Indications by Host Graph, page 56-5

Viewing the Hosts by Indication Graph

License: FireSIGHT

The Hosts by Indication graph, in donut form, displays a proportional view of the Indications of Compromise (IOC) triggered by hosts on your monitored network. The inner ring divides by IOC category (such as `CnC Connected` or `Malware Detected`), while the outer ring further divides that data by specific event type (such as `Impact 2 Intrusion Event – attempted-admin` or `Threat Detected in File Transfer`).



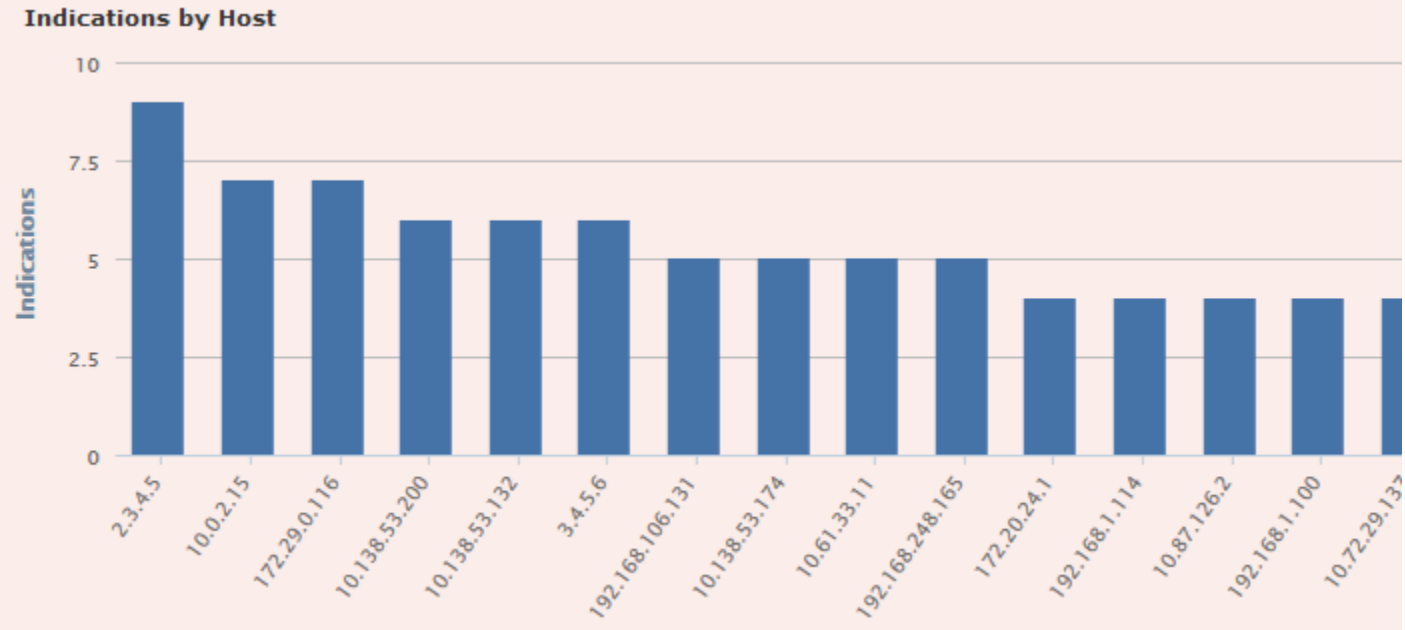
Hover your pointer over any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.

This graph draws data primarily from the Hosts and Indications of Compromise tables.

Viewing the Indications by Host Graph

License: FireSIGHT

The Indications by Host graph, in bar form, displays counts of unique Indications of Compromise (IOC) triggered by the 15 most IOC-active hosts on your monitored network.



Hover your pointer over any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.

This graph draws data primarily from the Hosts and Indications of Compromise tables.

Understanding the Network Information Section

License: FireSIGHT

The Network Information section of the Context Explorer contains six interactive graphs that display an overall picture of connection traffic on your monitored network: sources, destinations, users, and security zones associated with traffic, a breakdown of operating systems used by hosts on the network, as well as a proportional view of access control actions your FireSIGHT System has performed on network traffic.

For more information on the graphs in the Network Information section, see the following topics:

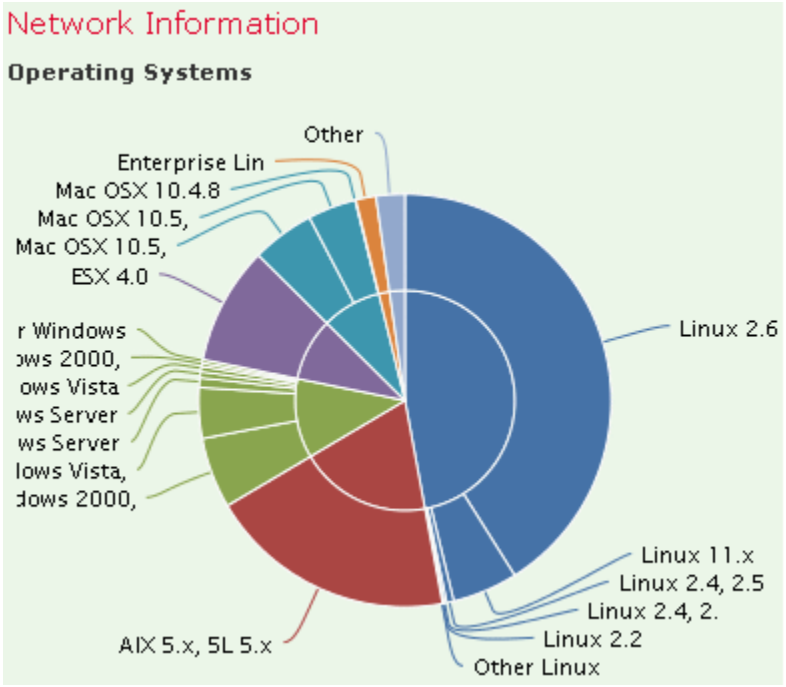
- Viewing the Operating Systems Graph, page 56-6
- Viewing the Traffic by Source IP Graph, page 56-7
- Viewing the Traffic by Source User Graph, page 56-8
- Viewing the Connections by Access Control Action Graph, page 56-9
- Viewing the Traffic by Destination IP Graph, page 56-10
- Viewing the Traffic by Ingress/Egress Security Zone Graph, page 56-11

Viewing the Operating Systems Graph

License: FireSIGHT

The Operating Systems graph, in donut form, displays a proportional representation of operating systems detected on hosts on your monitored network. The inner ring divides by OS name (such as `Windows` or `Linux`), while the outer ring further divides that data by specific operating system version (such as `Windows Server 2008` or `Linux 11.x`). Some closely related operating systems (such as Windows 2000, Windows XP, and Windows Server 2003) are grouped together. Very scarce or unrecognized operating systems are grouped under **Other**.

Note that this graph reflects all available data regardless of date and time constraints. If you change the explorer time range, the graph does not change.



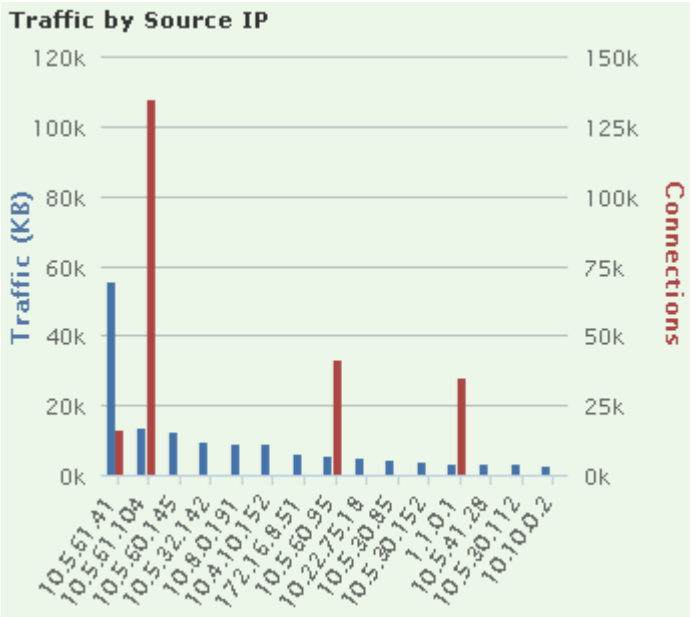
Hover your pointer over any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.

This graph draws data primarily from the Hosts table.

Viewing the Traffic by Source IP Graph

License: FireSIGHT

The Traffic by Source IP graph, in bar form, displays counts of network traffic (in kilobytes per second) and unique connections for the top 15 most active source IP addresses on your monitored network. For each source IP address listed, blue bars represent traffic data and red bars represent connection data.



Hover your pointer over any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.

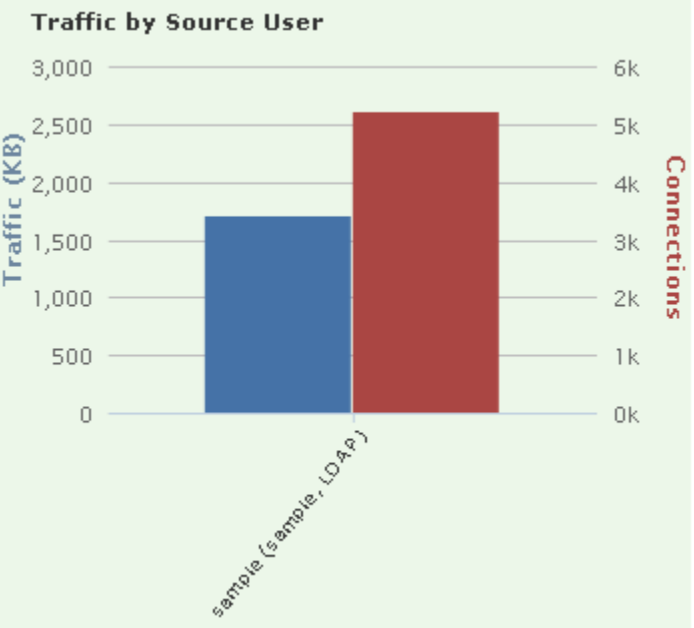
Note If you filter on intrusion event information, the Traffic by Source IP graph is hidden.

This graph draws data primarily from the Connection Events table.

Viewing the Traffic by Source User Graph

License: FireSIGHT

The Traffic by Source User graph, in bar form, displays counts of network traffic (in kilobytes per second) and unique connections for the top 15 most active source users on your monitored network. For each source IP address listed, blue bars represent traffic data and red bars represent connection data.



Hover your pointer over any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.

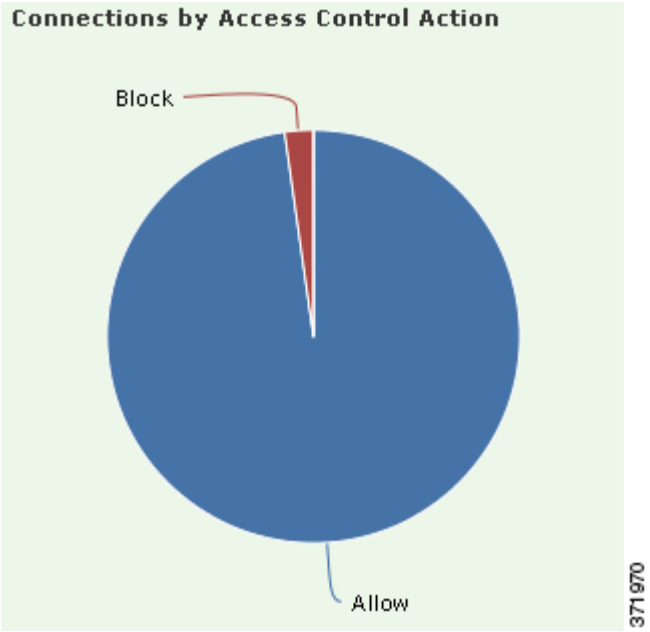
Note If you filter on intrusion event information, the Traffic by Source User graph is hidden.

This graph draws data primarily from the Connection Events table. Note that it displays only users reported by the User Agent.

Viewing the Connections by Access Control Action Graph

License: FireSIGHT

The Connections by Access Control Action graph, in pie form, displays a proportional view of access control actions (such as `Block` or `Allow`) that your FireSIGHT System deployment has taken on monitored traffic.



Hover your pointer over any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.

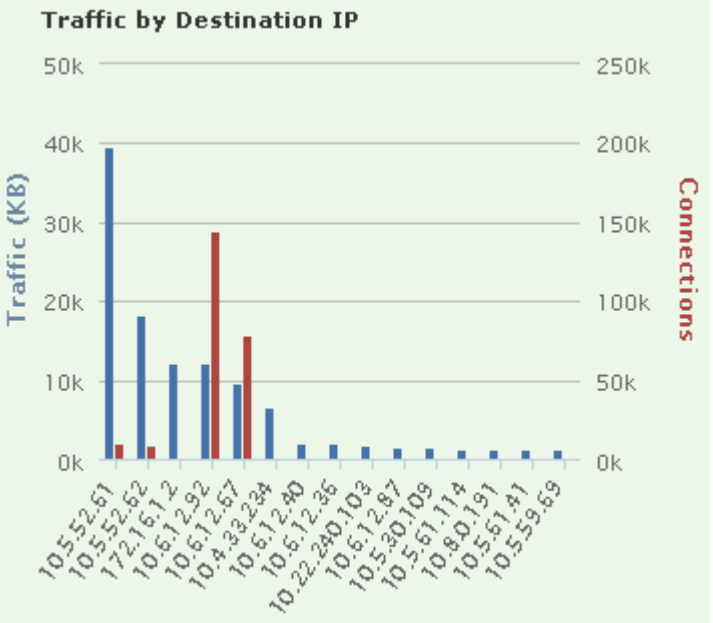
Note If you filter on intrusion event information, the Traffic by Source User graph is hidden.

This graph draws data primarily from the Connection Events table.

Viewing the Traffic by Destination IP Graph

License: FireSIGHT

The Traffic by Destination IP graph, in bar form, displays counts of network traffic (in kilobytes per second) and unique connections for the top 15 most active destination IP addresses on your monitored network. For each destination IP address listed, blue bars represent traffic data and red bars represent connection data.



Hover your pointer over any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.

Note If you filter on intrusion event information, the Traffic by Destination IP graph is hidden.

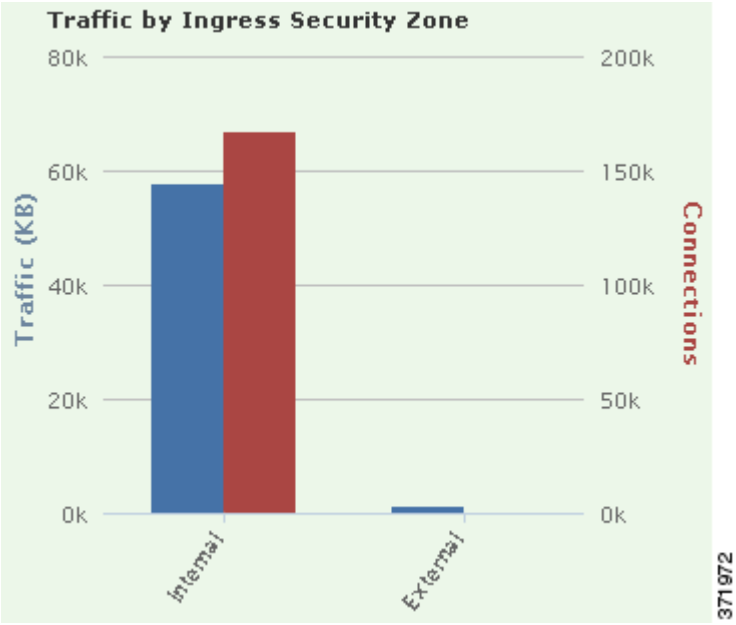
This graph draws data primarily from the Connection Events table.

Viewing the Traffic by Ingress/Egress Security Zone Graph

License: FireSIGHT

The Traffic by Ingress/Egress Security Zone graph, in bar form, displays counts of incoming or outgoing network traffic (in kilobytes per second) and unique connections for each security zone configured on your monitored network. You can configure this graph to display either ingress (the default) or egress security zone information, according to your needs.

For each security zone listed, blue bars represent traffic data and red bars represent connection data. For information about security zones, see Working with Security Zones, page 3-39.



Hover your pointer over any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information

Tip To constrain the graph so it displays only traffic by egress security zone, hover your pointer over the graph, then click **Egress** on the toggle button that appears. Click **Ingress** to return to the default view. Note that navigating away from the Context Explorer also returns the graph to the default Ingress view.

Note If you filter on intrusion event information, the Traffic by Ingress/Egress Security Zone graph is hidden.

This graph draws data primarily from the Connection Events table.

Understanding the Application Information Section

License: FireSIGHT

The Application Information section of the Context Explorer contains three interactive graphs and one table-format list that display an overall picture of application activity on your monitored network: traffic, intrusion events, and hosts associated with applications, further organized by the estimated risk or business relevance assigned to each application. The Application Details list provides an interactive list of each application and its risk, business relevance, category, and host count.

For all instances of “application” in this section, the Application Information graph set, by default, specifically examines application protocols (such as DNS or SSH). You can also configure the Application Information section to specifically examine client applications (such as PuTTY or Firefox) or web applications (such as Facebook or Pandora).

For more information on the graphs and list in the Application Information section, see the following topics:

- Viewing the Traffic by Risk/Business Relevance and Application Graph, page 56-13

- Viewing the Intrusion Events by Risk/Business Relevance and Application Graph, page 56-14
- Viewing the Hosts by Risk/Business Relevance and Application Graph, page 56-15
- Viewing the Application Details List, page 56-16

To configure the Application Information section focus:

Access: Admin/Any Security Analyst

Step 1 Select **Analysis > Context Explorer**.

The Context Explorer appears.

Step 2 Hover your pointer over the **Application Protocol Information** section. (Note that if you previously changed this setting in the same Context Explorer session, the section title may appear as **Client Application Information** or **Web Application Information** instead.)

The section option buttons appear at the upper right.

Step 3 Click **Application Protocol**, **Client Application**, or **Web Application**.

The Application Information section refreshes according to the option you selected.

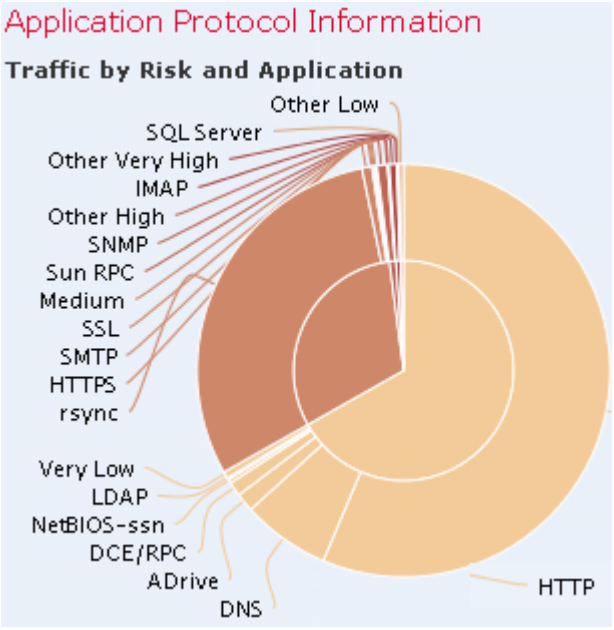
Note If you navigate away from the Context Explorer, this section reverts to its default state (Application Protocol).

Viewing the Traffic by Risk/Business Relevance and Application Graph

License: FireSIGHT

The Traffic by Risk/Business Relevance and Application graph, in donut form, displays a proportional representation of application traffic detected on your monitored network, arranged by the applications' estimated risk (the default) or estimated business relevance. The inner ring divides by estimated risk/business relevance level (such as `Medium` or `High`), while the outer ring further divides that data by specific application (such as `SSH` or `NetBIOS`). Scarcely detected applications are grouped under **Other**.

Note that this graph reflects all available data regardless of date and time constraints. If you change the explorer time range, the graph does not change.



Hover your pointer over any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.

Tip To constrain the graph so it displays traffic by business relevance and application, hover your pointer over the graph, then click **Business Relevance** on the toggle button that appears. Click **Risk** to return to the default view. Note that navigating away from the Context Explorer also returns the graph to the default Risk view.

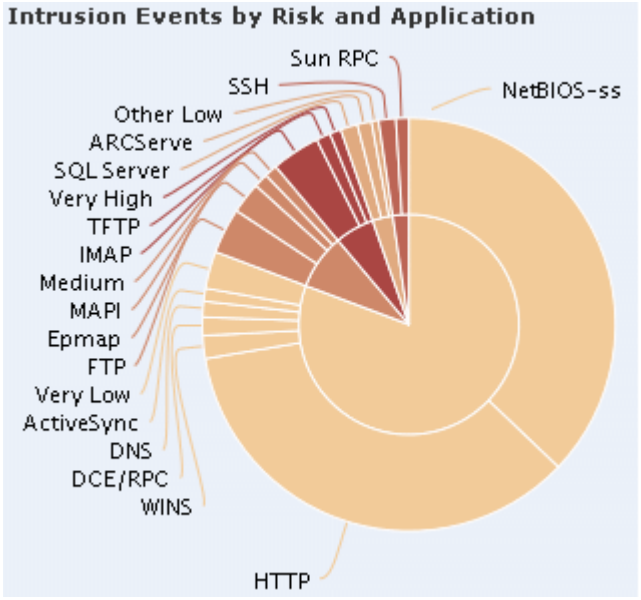
Note If you filter on intrusion event information, the Traffic by Risk/Business and Application graph is hidden.

This graph draws data primarily from the Connection Events and Application Statistics tables.

Viewing the Intrusion Events by Risk/Business Relevance and Application Graph

License: FireSIGHT

The Intrusion Events by Risk/Business Relevance and Application graph, in donut form, displays a proportional representation of intrusion events detected on your monitored network and the applications associated with those events, arranged by the applications' estimated risk (the default) or estimated business relevance. The inner ring divides by estimated risk/business relevance level (such as `Medium` or `High`), while the outer ring further divides that data by specific application (such as `SSH` or `NetBIOS`). Scarcely detected applications are grouped under **Other**.



Hover your pointer over any part of the donut graph to view more detailed information. Click any part of the graph to filter or drill down on that information, or (where applicable) to view application information.

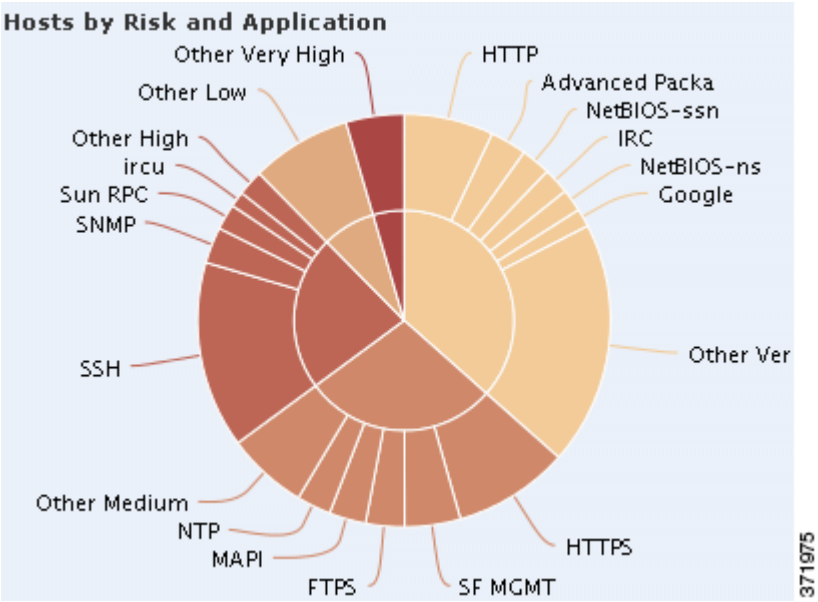
Tip To constrain the graph so it displays intrusion events by business relevance and application, hover your pointer over the graph, then click **Business Relevance** on the toggle button that appears. Click **Risk** to return to the default view. Note that navigating away from the Context Explorer also returns the graph to the default Risk view.

This graph draws data primarily from the Intrusion Events and Application Statistics tables.

Viewing the Hosts by Risk/Business Relevance and Application Graph

License: FireSIGHT

The Hosts by Risk/Business Relevance and Application graph, in donut form, displays a proportional representation of hosts detected on your monitored network and the applications associated with those hosts, arranged by the applications' estimated risk (the default) or estimated business relevance. The inner ring divides by estimated risk/business relevance level (such as `Medium` or `High`), while the outer ring further divides that data by specific application (such as `SSH` or `NetBIOS`). Very scarce applications are grouped under **Other**.



Hover your pointer over any part of the donut graph to view more detailed information. Click any part of the graph to filter or drill down on that information.

Tip To constrain the graph so it displays hosts by business relevance and application, hover your pointer over the graph, then click **Business Relevance** on the toggle button that appears. Click **Risk** to return to the default view. Note that navigating away from the Context Explorer also returns the graph to the default Risk view.

This graph draws data primarily from the Applications table.

Viewing the Application Details List

License: FireSIGHT

At the bottom of the Application Information section is the Application Details List, a table that provides estimated risk, estimated business relevance, category, and hosts count information for each application detected on your monitored network. The applications are listed in descending order of associated host count.

The Application Details List table is not sortable, but you can click on any table entry to filter or drill down on that information, or (where applicable) to view application information. This table draws data primarily from the Applications table.

Note that this list reflects all available data regardless of date and time constraints. If you change the explorer time range, the list does not change.

Understanding the Security Intelligence Section

License: Protection

Supported Devices: Any except Series 2

Supported Defense Centers: Any except DC500

The Security Intelligence section of the Context Explorer contains three interactive bar graphs that display an overall picture of traffic on your monitored network that is blacklisted or monitored by Security Intelligence. The graphs sort such traffic by category, source IP address, and destination IP address, respectively; both the amount of traffic (in kilobytes per second) and the number of applicable connections appear.

For more information on the graphs in the Security Intelligence section, see the following topics:

- Viewing the Security Intelligence Traffic by Category Graph, page 56-17
- Viewing the Security Intelligence Traffic by Source IP Graph, page 56-18
- Viewing the Security Intelligence Traffic by Destination IP Graph, page 56-18

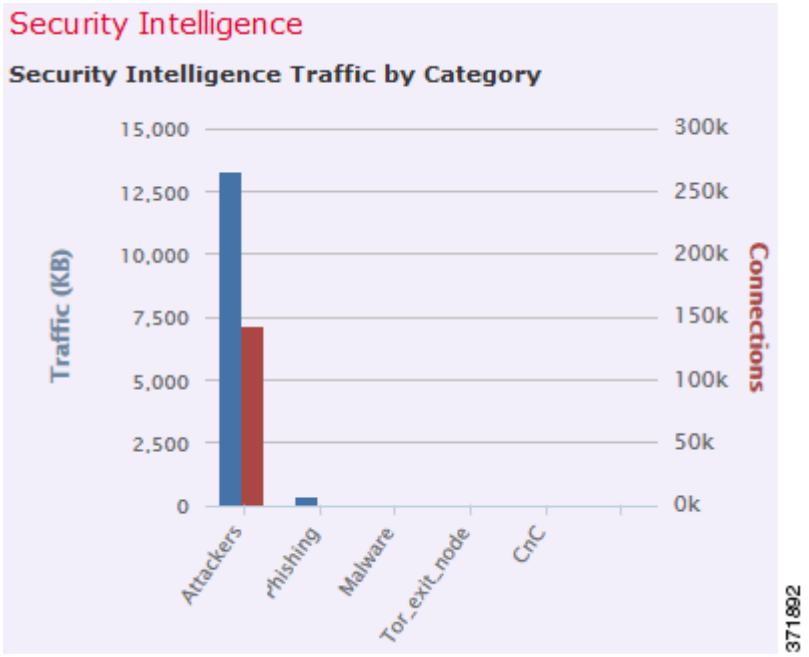
Viewing the Security Intelligence Traffic by Category Graph

License: Protection

Supported Devices: Any except Series 2

Supported Defense Centers: Any except DC500

The Security Intelligence Traffic by Category graph, in bar form, displays counts of network traffic (in kilobytes per second) and unique connections for the top Security Intelligence categories of traffic on your monitored network. For each category listed, blue bars represent traffic data and red bars represent connection data.



Hover your pointer over any part of the graph to view more detailed information. Click any part of the graph to drill down on that information.

Note If you filter on intrusion event information, the Security Intelligence Traffic by Category graph is hidden.

This graph draws data primarily from the Security Intelligence Events table.

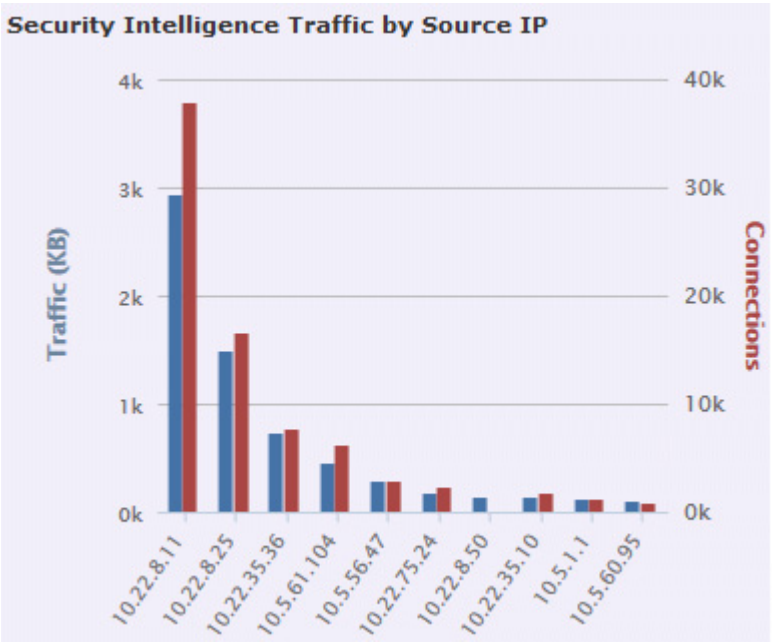
Viewing the Security Intelligence Traffic by Source IP Graph

License: Protection

Supported Devices: Any except Series 2

Supported Defense Centers: Any except DC500

The Security Intelligence Traffic by Source IP graph, in bar form, displays counts of network traffic (in kilobytes per second) and unique connections for the top source IP addresses of Security Intelligence-monitored traffic on your monitored network. For each category listed, blue bars represent traffic data and red bars represent connection data.



Hover your pointer over any part of the graph to view more detailed information. Click any part of the graph to drill down on that information.

Note If you filter on intrusion event information, the Security Intelligence Traffic by Source IP graph is hidden.

This graph draws data primarily from the Security Intelligence Events table.

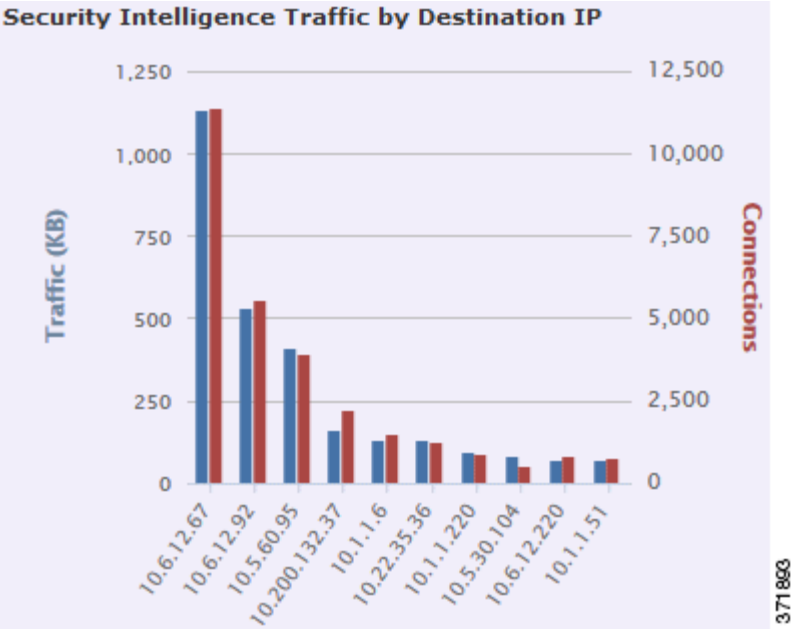
Viewing the Security Intelligence Traffic by Destination IP Graph

License: Protection

Supported Devices: Any except Series 2

Supported Defense Centers: Any except DC500

The Security Intelligence Traffic by Destination IP graph, in bar form, displays counts of network traffic (in kilobytes per second) and unique connections for the top destination IP addresses of Security Intelligence-monitored traffic on your monitored network. For each category listed, blue bars represent traffic data and red bars represent connection data.



Hover your pointer over any part of the graph to view more detailed information. Click any part of the graph to drill down on that information.

Note If you filter on intrusion event information, the Security Intelligence Traffic by Destination IP graph is hidden.

This graph draws data primarily from the Security Intelligence Events table.

Understanding the Intrusion Information Section

License: Protection

The Intrusion Information section of the Context Explorer contains six interactive graphs and one table-format list that display an overall picture of intrusion events on your monitored network: impact levels, attack sources, target destinations, users, priority levels, and security zones associated with intrusion events, as well as a detailed list of intrusion event classifications, priorities, and counts.

For more information on the graphs and list in the Network Information section, see the following topics:

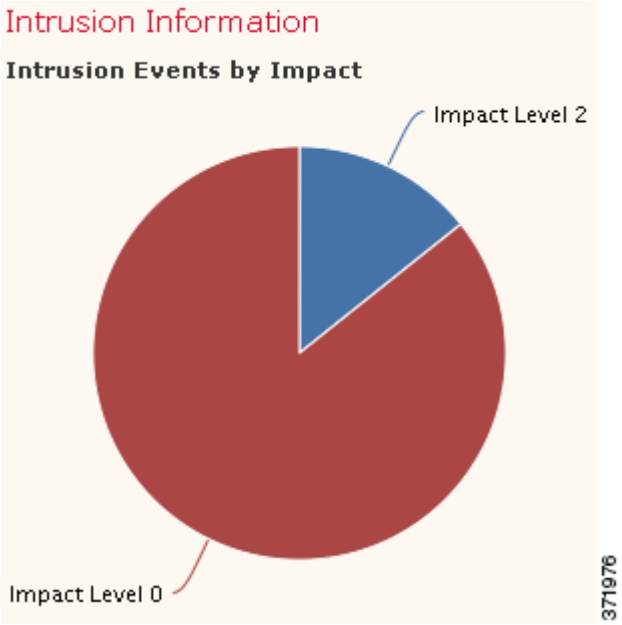
- Viewing the Intrusion Events by Impact Graph, page 56-20
- Viewing the Top Attackers Graph, page 56-20
- Viewing the Top Users Graph, page 56-21
- Viewing the Intrusion Events by Priority Graph, page 56-22
- Viewing the Top Targets Graph, page 56-23

- Viewing the Top Ingress/Egress Security Zones Graph, page 56-23
- Viewing the Intrusion Event Details List, page 56-24

Viewing the Intrusion Events by Impact Graph

License: Protection

The Intrusion Events by Impact graph, in pie form, displays a proportional view of intrusion events on your monitored network, grouped by estimated impact level (from 0 to 4).



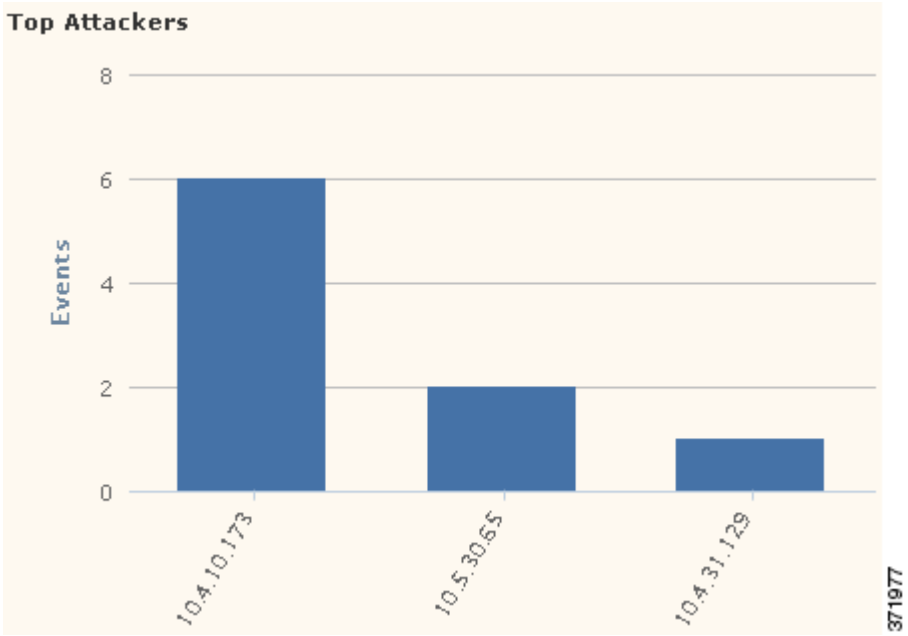
Hover your pointer over any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.

This graph draws data primarily from the IDS Statistics and Intrusion Events tables.

Viewing the Top Attackers Graph

License: Protection

The Top Attackers graph, in bar form, displays counts of intrusion events for the top attacking host IP addresses (causing those events) on your monitored network.



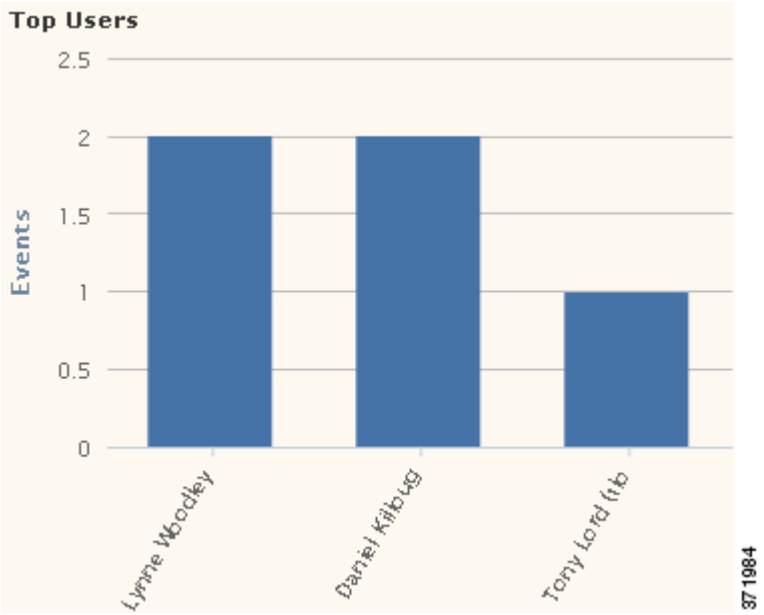
Hover your pointer over any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.

This graph draws data primarily from the Intrusion Events table.

Viewing the Top Users Graph

License: Protection

The Top Users graph, in bar form, displays users on your monitored network that are associated with the highest intrusion event counts, by event count.



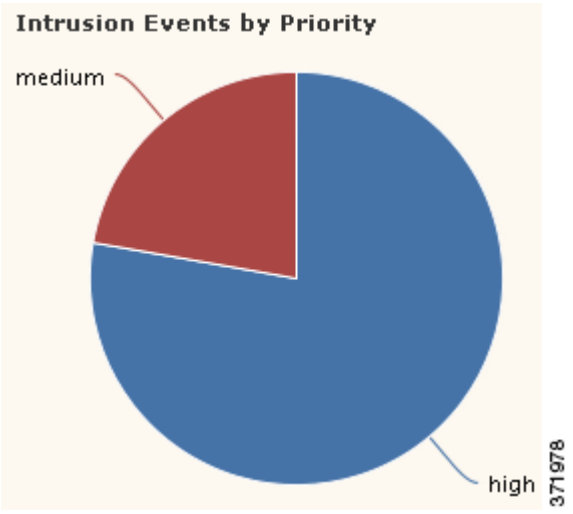
Hover your pointer over any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.

This graph draws data primarily from the IDS User Statistics and Intrusion Events tables. Note that it displays only users reported by the User Agent.

Viewing the Intrusion Events by Priority Graph

License: Protection

The Intrusion Events by Priority graph, in pie form, displays a proportional view of intrusion events on your monitored network, grouped by estimated priority level (such as `High`, `Medium`, or `Low`).



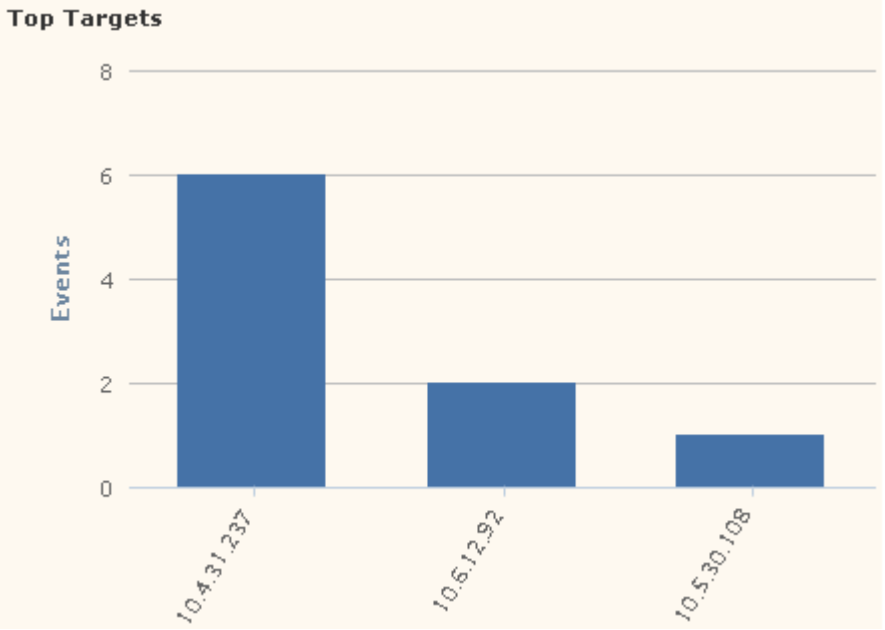
Hover your pointer over any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.

This graph draws data primarily from the Intrusion Events table.

Viewing the Top Targets Graph

License: Protection

The Top Targets graph, in bar form, displays counts of intrusion events for the top target host IP addresses (targeted in the connections causing those events) on your monitored network.



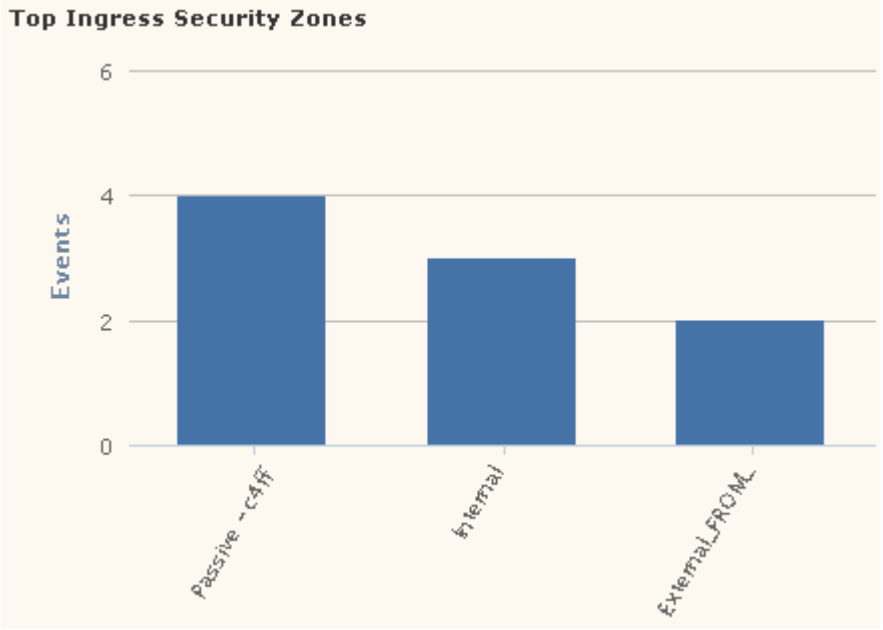
Hover your pointer over any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.

This graph draws data primarily from the Intrusion Events table.

Viewing the Top Ingress/Egress Security Zones Graph

License: Protection

The Top Ingress/Egress Security Zones graph, in bar form, displays counts of intrusion events associated with each security zone (ingress or egress, depending on graph settings) configured on your monitored network. For information about security zones, see Working with Security Zones, page 3-39.



Hover your pointer over any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.

Tip To constrain the graph so it displays only traffic by egress security zone, hover your pointer over the graph, then click **Egress** on the toggle button that appears. Click **Ingress** to return to the default view. Note that navigating away from the Context Explorer also returns the graph to the default Ingress view.

This graph draws data primarily from the Intrusion Events table.

You can configure this graph to display either ingress (the default) or egress security zone information, according to your needs.

Viewing the Intrusion Event Details List

License: Protection

At the bottom of the Intrusion Information section is the Intrusion Event Details List, a table that provides classification, estimated priority, and event count information for each intrusion event detected on your monitored network. The events are listed in descending order of event count.

The Intrusion Event Details List table is not sortable, but you can click on any table entry to filter or drill down on that information. This table draws data primarily from the Intrusion Events table.

Understanding the Files Information Section

License: Protection or Malware

Supported Devices: feature dependent

Supported Defense Centers: feature dependent

The Files Information section of the Context Explorer contains six interactive graphs that display an overall picture of file and malware events on your monitored network. Five of the graphs display the file types, file names, and malware dispositions of the files detected in network traffic, as well as the hosts sending (uploading) and receiving (downloading) those files. The final graph displays the malware threats detected on your network and, if you have a FireAMP subscription, on the endpoints where your users installed FireAMP Connectors.

Note If you filter on intrusion information, the entire Files Information Section is hidden.

Note that you must have a Malware license and enable malware detection for Files Information graphs to include network-based malware data. Note also that the DC500 Defense Center and Series 2 devices and Cisco NGIPS for Blue Coat X-Series do not support advanced malware protection, so the DC500 Defense Center cannot display this data and Series 2 devices and Cisco NGIPS for Blue Coat X-Series do not detect it. See Understanding Malware Protection and File Control, page 37-2.

For more information on the graphs in the Files Information section, see the following topics:

- Viewing the Top File Types Graph, page 56-25
- Viewing the Top File Names Graph, page 56-26
- Viewing the Files by Disposition Graph, page 56-27
- Viewing the Top Hosts Sending Files Graph, page 56-28
- Viewing the Top Hosts Receiving Files Graph, page 56-29
- Viewing the Top Malware Detections Graph, page 56-30

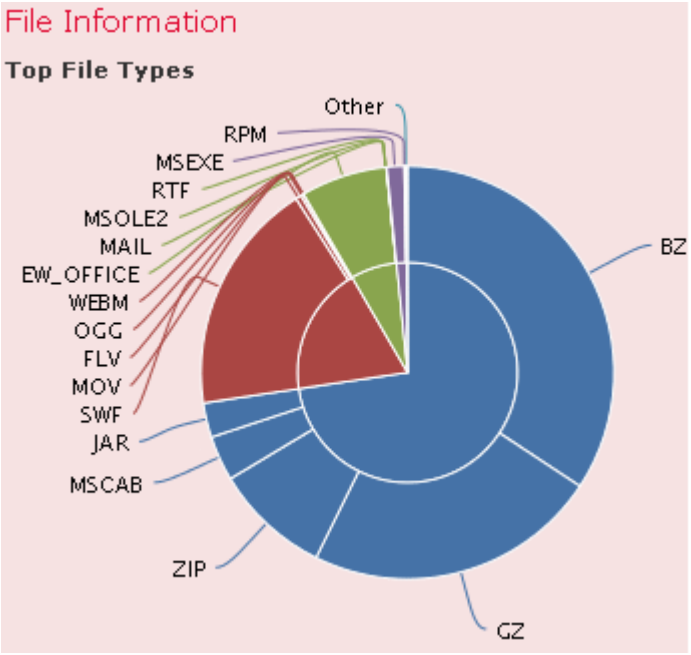
Viewing the Top File Types Graph

License: Protection or Malware

Supported Devices: feature dependent

Supported Defense Centers: feature dependent

The Top File Types graph, in donut form, displays a proportional view of the file types detected in network traffic (outer ring), grouped by file category (inner ring).



Hover your pointer over any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.

Note that you must have a Malware license and enable malware detection for this graph to include network-based malware data. Note also that the DC500 Defense Center and Series 2 devices and Cisco NGIPS for Blue Coat X-Series do not support advanced malware protection, so the DC500 Defense Center cannot display this data and Series 2 devices and Cisco NGIPS for Blue Coat X-Series do not detect it. See Understanding Malware Protection and File Control, page 37-2.

This graph draws data primarily from the File Events table.

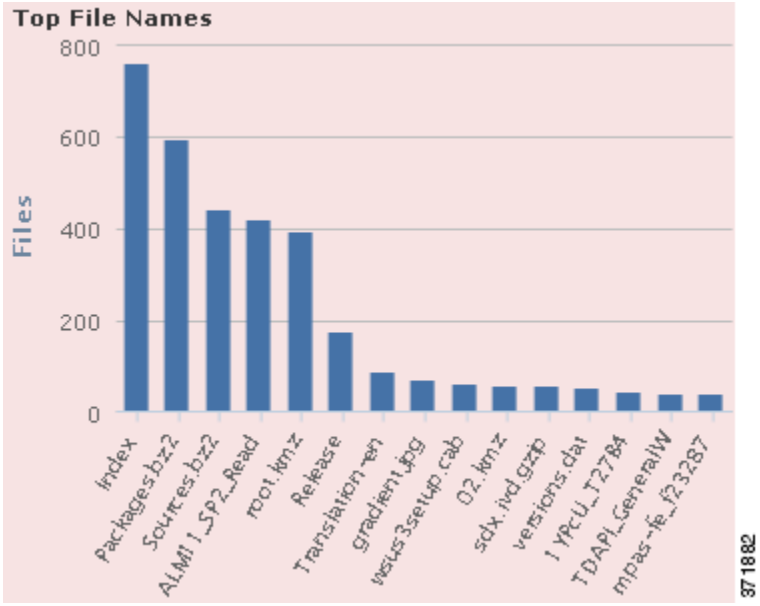
Viewing the Top File Names Graph

License: Protection or Malware

Supported Devices: feature dependent

Supported Defense Centers: feature dependent

The Top File Names graph, in bar form, displays counts of the top unique file names detected in network traffic.



Hover your pointer over any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.

Note that you must have a Malware license and enable malware detection for this graph to include network-based malware data. Note also that the DC500 Defense Center and Series 2 devices and Cisco NGIPS for Blue Coat X-Series do not support advanced malware protection, so the DC500 Defense Center cannot display this data and Series 2 devices and Cisco NGIPS for Blue Coat X-Series do not detect it. See Understanding Malware Protection and File Control, page 37-2.

This graph draws data primarily from the File Events table.

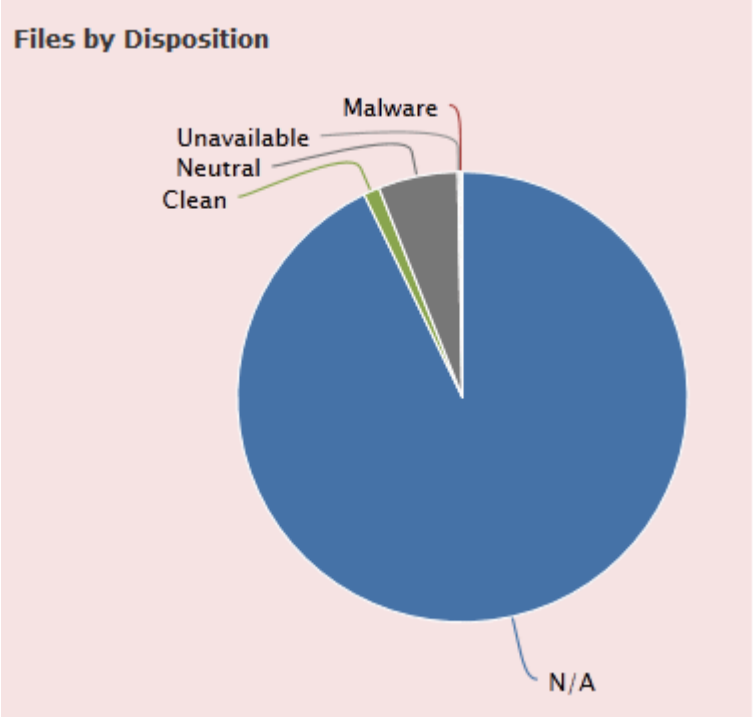
Viewing the Files by Disposition Graph

License: Protection or Malware

Supported Devices: feature dependent

Supported Defense Centers: feature dependent

The Top File Types graph, in pie form, displays a proportional view of the malware dispositions for files detected in network traffic. Note that only files for which the Defense Center performed a Collective Security Intelligence Cloud lookup (which requires a Malware license) have dispositions. Files that did not trigger a cloud lookup have a disposition of `N/A`. The disposition `Unavailable` indicates that the Defense Center could not perform a malware cloud lookup. See Understanding Malware Protection and File Control, page 37-2 for descriptions of the other dispositions.



Hover your pointer over any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.

Note that you must have a Malware license and enable malware detection for this graph to include network-based malware data. Note also that the DC500 Defense Center and Series 2 devices and Cisco NGIPS for Blue Coat X-Series do not support advanced malware protection, so the DC500 Defense Center cannot display this data and Series 2 devices and Cisco NGIPS for Blue Coat X-Series do not detect it. See Understanding Malware Protection and File Control, page 37-2.

This graph draws data primarily from the File Events table.

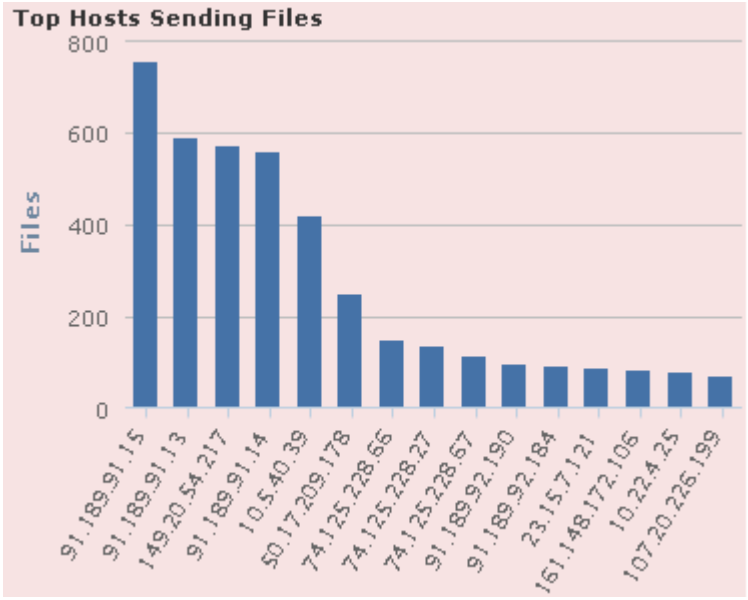
Viewing the Top Hosts Sending Files Graph

License: Protection or Malware

Supported Devices: feature dependent

Supported Defense Centers: feature dependent

The Top Hosts Sending Files graph, in bar form, displays counts of the number of files detected in network traffic for the top file-sending host IP addresses.



Hover your pointer over any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.

Tip To constrain the graph so it displays only hosts sending malware, hover your pointer over the graph, then click **Malware** on the toggle button that appears. Click **Files** to return to the default files view. Note that navigating away from the Context Explorer also returns the graph to the default files view.

Note that you must have a Malware license and enable malware detection for this graph to include network-based malware data. Note also that the DC500 Defense Center and Series 2 devices and Cisco NGIPS for Blue Coat X-Series do not support advanced malware protection, so the DC500 Defense Center cannot display this data and Series 2 devices and Cisco NGIPS for Blue Coat X-Series do not detect it. See Understanding Malware Protection and File Control, page 37-2.

This graph draws data primarily from the File Events table.

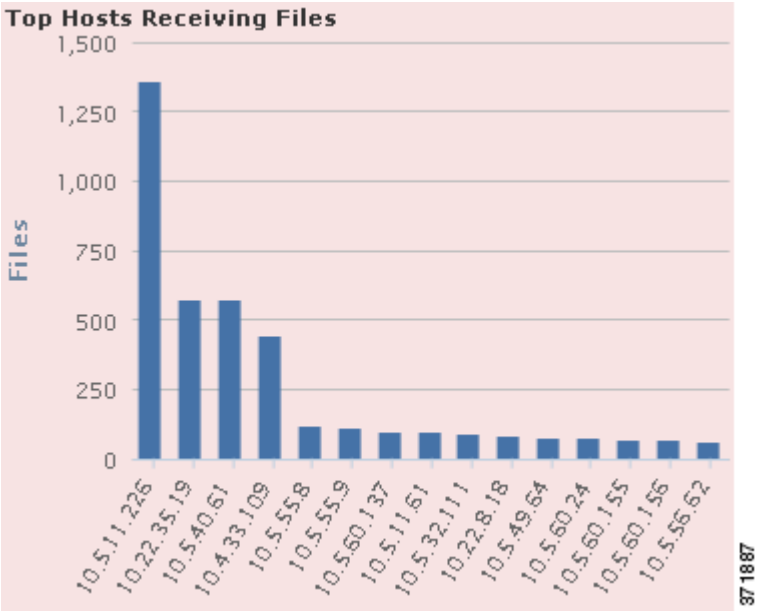
Viewing the Top Hosts Receiving Files Graph

License: Protection or Malware

Supported Devices: feature dependent

Supported Defense Centers: feature dependent

The Top Hosts Receiving Files graph, in bar form, displays counts of the number of files detected in network traffic for the top file-receiving host IP addresses.



Hover your pointer over any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.

Tip To constrain the graph so it displays only hosts receiving malware, hover your pointer over the graph, then click **Malware** on the toggle button that appears. Click **Files** to return to the default files view. Note that navigating away from the Context Explorer also returns the graph to the default files view.

Note that you must have a Malware license and enable malware detection for this graph to include network-based malware data. Note also that the DC500 Defense Center and Series 2 devices and Cisco NGIPS for Blue Coat X-Series do not support advanced malware protection, so the DC500 Defense Center cannot display this data and Series 2 devices and Cisco NGIPS for Blue Coat X-Series do not detect it. See Understanding Malware Protection and File Control, page 37-2.

This graph draws data primarily from the File Events table.

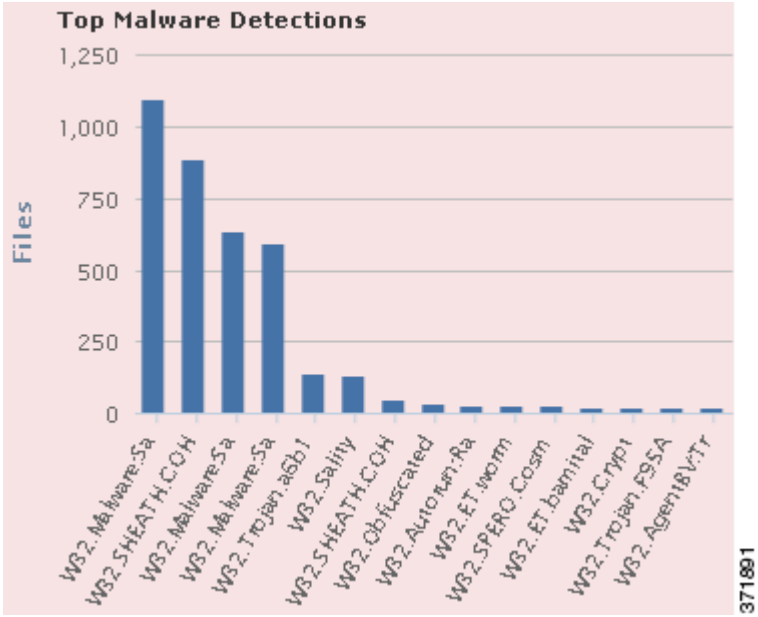
Viewing the Top Malware Detections Graph

License: Protection or Malware

Supported Devices: feature dependent

Supported Defense Centers: feature dependent

The Top Malware Detections graph, in bar form, displays counts of the top malware threats detected on your network and, if you have a FireAMP subscription, on the endpoints where your users installed FireAMP Connectors.



Hover your pointer over any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.

Note that you must have a Malware license and enable malware detection for this graph to include network-based malware data. Note also that the DC500 Defense Center and Series 2 devices and Cisco NGIPS for Blue Coat X-Series do not support advanced malware protection, so the DC500 Defense Center cannot display this data and Series 2 devices and Cisco NGIPS for Blue Coat X-Series do not detect it. See Understanding Malware Protection and File Control, page 37-2.

This graph draws data primarily from the File Events and Malware Events tables.

Understanding the Geolocation Information Section

License: FireSIGHT

Supported Defense Centers: Any except DC500

The Geolocation Information section of the Context Explorer contains three interactive donut graphs that display an overall picture of countries with which hosts on your monitored network are exchanging data: unique connections by initiator or responder country, intrusion events by source or destination country, and file events by sending or receiving country.

For more information on the graphs in the Geolocation Information section, see the following topics:

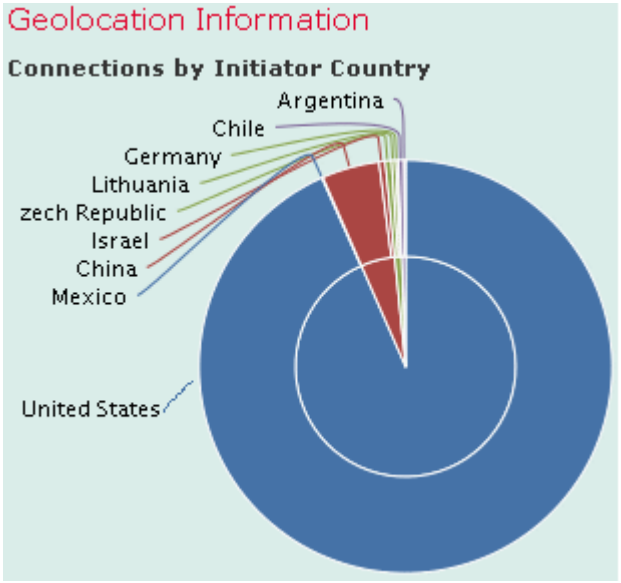
- Viewing the Connections by Initiator/Responder Country Graph, page 56-31
- Viewing the Intrusion Events by Source/Destination Country Graph, page 56-32
- Viewing the File Events by Sending/Receiving Country Graph, page 56-33

Viewing the Connections by Initiator/Responder Country Graph

License: FireSIGHT

Supported Defense Centers: Any except DC500

The Connections by Initiator/Responder Country graph, in donut form, displays a proportional view of the countries involved in connections on your network as either the initiator (the default) or the responder. The inner ring groups these countries together by continent. For information about geolocation information, see Using Geolocation, page 58-20. For information about connection data, see Working with Connection & Security Intelligence Data, page 39-1.



Hover your pointer over any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.

Tip To constrain the graph so it displays only countries acting as the responder in connections, hover your pointer over the graph, then click **Responder** on the toggle button that appears. Click **Initiator** to return to the default view. Note that navigating away from the Context Explorer also returns the graph to the default Initiator view.

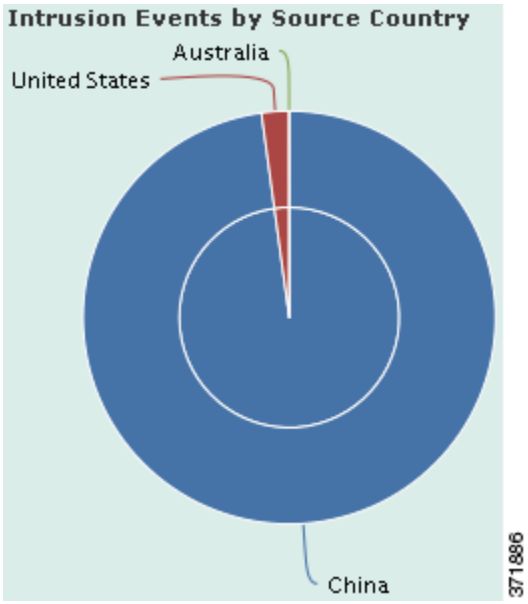
This graph draws data primarily from the Connection Summary Data table.

Viewing the Intrusion Events by Source/Destination Country Graph

License: FireSIGHT

Supported Defense Centers: Any except DC500

The Intrusion Events by Source/Destination Country graph, in donut form, displays a proportional view of the countries involved in intrusion events on your network as either the source of the event (the default) or the destination. The inner ring groups these countries together by continent. For information about geolocation information, see Using Geolocation, page 58-20. For information about intrusion event data, see Working with Intrusion Events, page 41-1.



Hover your pointer over any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.

Tip To constrain the graph so it displays only countries acting as the destinations of intrusion events, hover your pointer over the graph, then click **Destination** on the toggle button that appears. Click **Source** to return to the default view. Note that navigating away from the Context Explorer also returns the graph to the default Source view.

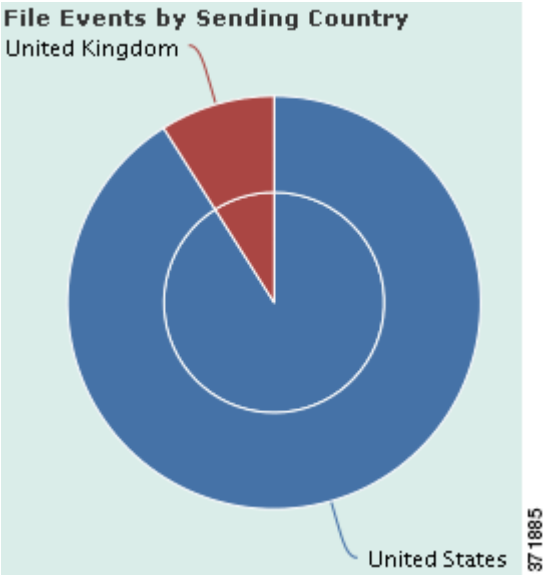
This graph draws data primarily from the Intrusion Events table.

Viewing the File Events by Sending/Receiving Country Graph

License: FireSIGHT

Supported Defense Centers: Any except DC500

The File Events by Sending/Receiving Country graph, in donut form, displays a proportional view of the countries detected in file events on your network as either sending (the default) or receiving files. The inner ring groups these countries together by continent. For information about geolocation information, see Using Geolocation, page 58-20. For information about file event data, see Working with File Events, page 40-7.



Hover your pointer over any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.

Tip To constrain the graph so it displays only countries receiving files, hover your pointer over the graph, then click **Receiver** on the toggle button that appears. Click **Sender** to return to the default view. Note that navigating away from the Context Explorer also returns the graph to the default Sender view.

This graph draws data primarily from the File Events table.

Understanding the URL Information Section

License: FireSIGHT or URL Filtering

Supported Devices: feature dependent

Supported Defense Centers: feature dependent

The URL Information section of the Context Explorer contains three interactive bar graphs that display an overall picture of URLs with which hosts on your monitored network are exchanging data: traffic and unique connections associated with URLs, sorted by individual URL, URL category, and URL reputation. You cannot filter on URL information.

Note If you filter on intrusion event information, the entire URL Information Section is hidden.

Note that you must have a URL Filtering license and enable URL Filtering for URL filtering graphs to include URL category and reputation data. Note also that neither the DC500 Defense Center nor Series 2 devices support URL filtering by reputation and category, so the DC500 Defense Center cannot display this data and Series 2 devices do not detect it. See Blocking URLs, page 16-8.

For more information on the graphs in the URL Information section, see the following topics:

- Viewing the Traffic by URL Graph, page 56-35

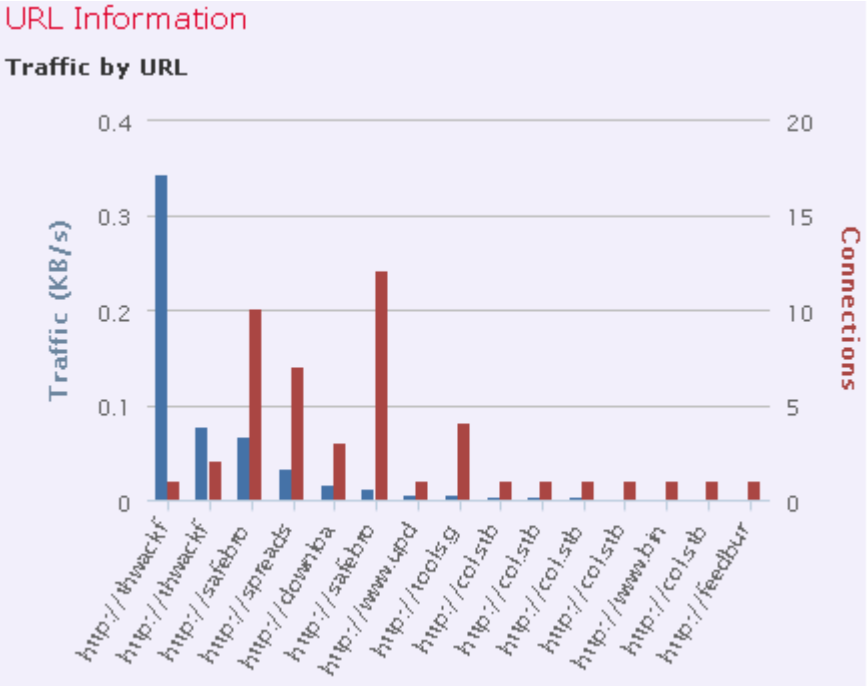
Viewing the Traffic by URL Graph

License: FireSIGHT or URL Filtering

Supported Devices: feature dependent

Supported Defense Centers: feature dependent

The Traffic by URL graph, in bar form, displays counts of network traffic (in kilobytes per second) and unique connections for the top 15 most requested URLs on your monitored network. For each URL listed, blue bars represent traffic data and red bars represent connection data.



Hover your pointer over any part of the graph to view more detailed information. Click any part of the graph to drill down on that information.

Note If you filter on intrusion event information, the Traffic by URL graph is hidden.

Note that you must have a URL Filtering license and enable URL Filtering for URL filtering graphs to include URL category and reputation data. Note also that neither the DC500 Defense Center nor Series 2 devices support URL filtering by reputation and category, so the DC500 Defense Center cannot display this data and Series 2 devices do not detect it. See Enabling Cloud Communications, page 64-27.

This graph draws data primarily from the Connection Events table.

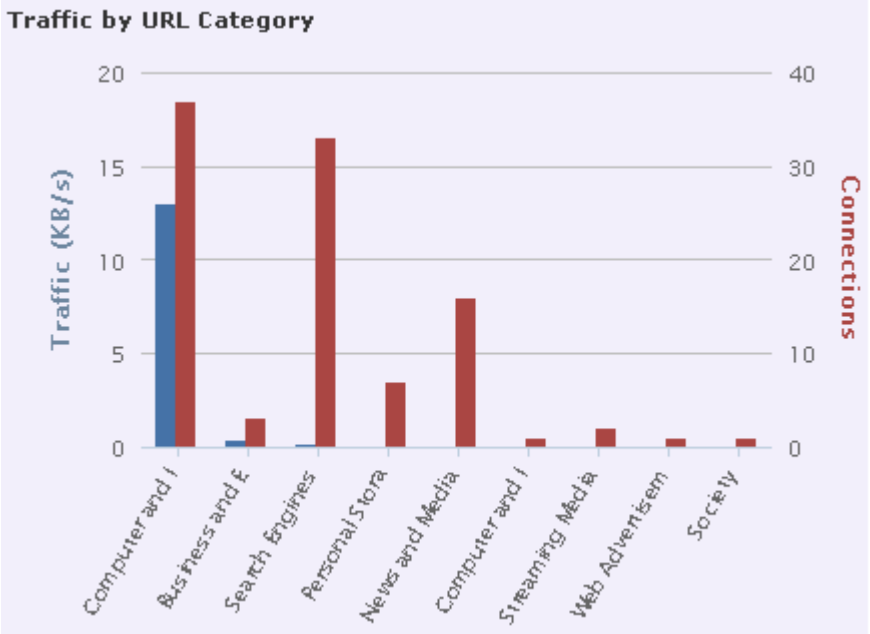
Viewing the Traffic by URL Category Graph

License: URL Filtering

Supported Devices: feature dependent

Supported Defense Centers: feature dependent

The Traffic by URL Category graph, in bar form, displays counts of network traffic (in kilobytes per second) and unique connections for the most requested URL categories (such as `Search Engines` or `Streaming Media`) on your monitored network. For each URL category listed, blue bars represent traffic data and red bars represent connection data.



Hover your pointer over any part of the graph to view more detailed information. Click any part of the graph to drill down on that information.

Note If you filter on intrusion event information, the Traffic by URL Category graph is hidden.

Note that you must have a URL Filtering license and enable URL Filtering for URL filtering graphs to include URL category and reputation data. Note also that neither the DC500 Defense Center nor Series 2 devices support URL filtering by reputation and category, so the DC500 Defense Center cannot display this data and Series 2 devices do not detect it. See Performing Reputation-Based URL Blocking, page 16-10.

This graph draws data primarily from the URL Statistics and Connection Events tables.

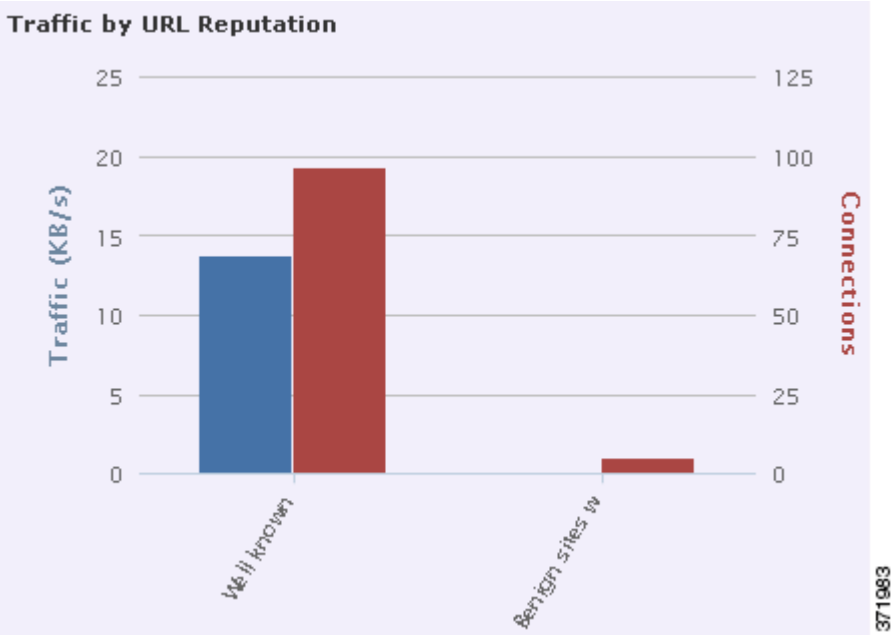
Viewing the Traffic by URL Reputation Graph

License: URL Filtering

Supported Devices: feature dependent

Supported Defense Centers: feature dependent

The Traffic by URL Reputation graph, in bar form, displays counts of network traffic (in kilobytes per second) and unique connections for the most requested URL reputation groups (such as `Well known` or `Benign sites with security risks`) on your monitored network. For each URL reputation listed, blue bars represent traffic data and red bars represent connection data.



Hover your pointer over any part of the graph to view more detailed information. Click any part of the graph to drill down on that information.

Note If you filter on intrusion event information, the Traffic by URL Reputation graph is hidden.

Note that you must have a URL Filtering license and enable URL Filtering for URL filtering graphs to include URL category and reputation data. Note also that neither the DC500 Defense Center nor Series 2 devices support URL filtering by reputation and category, so the DC500 Defense Center cannot display this data and Series 2 devices do not detect it. See Performing Reputation-Based URL Blocking, page 16-10.

This graph draws data primarily from the URL Statistics and Connection Events tables.

Refreshing the Context Explorer

License: FireSIGHT

The Context Explorer does not automatically update the information it displays. To incorporate new data, you must manually refresh the explorer.

Note that, although reloading the Context Explorer itself (by refreshing the browser program or navigating away from, then back to, the Context Explorer) refreshes all displayed information, this does not preserve any changes you made to section configuration (such as the Ingress/Egress graphs and the Application Information section) and may cause delays in loading.

To refresh the Context Explorer:

Access: Admin/Any Security Analyst

Step 1 On the Context Explorer, click **Reload** at the upper right.

The explorer updates to display the latest information within your selected time range. Note that the **Reload** button is grayed out until your refresh is finished.

Setting the Context Explorer Time Range

License: FireSIGHT

You can configure the Context Explorer time range to reflect a period as short as the last hour (the default) or as long as the last year. Note that when you change the time range, the Context Explorer does not automatically update to reflect the change. To apply the new time range, you must manually refresh the explorer.

Changes to the time range persist even if you navigate away from the Context Explorer or end your login session.

To change the Context Explorer time range:

Access: Admin/Any Security Analyst

Step 1 From the **Show the last** drop-down list, select a time range.

Step 2 Optionally, to view data from the new time range, click **Reload**.

All sections of the Context Explorer update to reflect the new time range.

Tip Clicking **Apply Filters** also applies any time range updates.

Minimizing and Maximizing Context Explorer Sections

License: FireSIGHT

You can minimize and hide one or more sections of the Context Explorer. This is useful if you want to focus on only certain sections, or if you want a simpler view. You cannot minimize the Traffic and Intrusion Event Counts Time Graph.

Note that Context Explorer sections retain the minimized or maximized states that you configure even if you refresh the page or log out of the appliance.

To minimize a Context Explorer section:

Access: Admin/Any Security Analyst

Step 1 Click the minimize icon (−) in a section's title bar.

To maximize a Context Explorer section:

Access: Admin/Any Security Analyst

Step 1 Click the maximize icon (□) in a minimized section's title bar.

Drilling Down on Context Explorer Data

License: feature dependent

If you want to examine graph or list data in more detail than the Context Explorer allows, you can drill down to the table views of the relevant data. (Note that you cannot drill down on the Traffic and Intrusion Events over Time graph.) For example, drilling down on an IP address in the Traffic by Source IP graph displays the Connections with Application Details view of the Connection Events table, including only data associated with the source IP address you selected.

Depending on the type of data you examine, additional options can appear in the context menu. Data points that are associated with specific IP addresses offer the option to view host or whois information on the IP address you select. Data points associated with specific applications offer the option to view application information on the application you select. Data points associated with a specific user offer the option to view that user's user profile page. Data points associated with an intrusion event message offer the option to view the rule documentation for that event's associated intrusion rule, and data points associated with a specific IP address offer the option to blacklist or whitelist that address.

The context menu that you use to drill down on data also contains options to filter that data. For more information on filtering, see Working with Filters in the Context Explorer, page 56-40.

To drill down on data in the Context Explorer:

Access: Admin/Any Security Analyst

Step 1 Select **Analysis > Context Explorer**.

The Context Explorer appears.

Step 2 In any section but Traffic and Intrusion Events over Time, click a data point that you want to investigate.

The context menu pop-up window appears nearby.

Step 3 Depending on the data point you selected, you have several options:

- To view more details of this data in a table view, select **Drill into Analysis**.

  A new window opens with a detailed table view of the data you selected.

- If you selected a data point associated with a specific IP address and want more information about the associated host, select **View Host Information**.

  A new window opens with a host profile page for the IP address you selected. For more information on host attributes and host profiles, see Using Host Profiles, page 49-1.

- If you selected a data point with a specific IP address and want to make a whois search on that address, select **Whois**.

A new window opens with the results of a whois query for the IP address you selected.

- If you selected a data point associated with a specific application and want more information about that application, select **View Application Information**.

  A new window opens with information on the application you selected. For more information about application attributes, see Understanding Application Detection, page 45-10.

- If you selected a data point associated with a specific user and want more information about that user, select **View User Information**.

  A new window opens with a user profile page for the user you selected. For more information on user details, see Understanding User Details and Host History, page 50-62.

- If you selected a data point associated with a specific intrusion event message and want more information about the associated intrusion rule, select **View Rule Documentation**.

  A new window opens with a rule details page relevant to the event you selected. For more information on intrusion rule details, see Viewing Rule Details, page 32-5.

- If you selected a data point associated with a specific IP address and want to add that IP address to the Security Intelligence global blacklist or whitelist, select the appropriate option: **Blacklist Now** or **Whitelist Now**. Confirm your choice in the pop-up window that appears.

  The IP address is blacklisted or whitelisted. For more information, see Working with the Global Whitelist and Blacklist, page 3-7.

  These options are not listed on the DC500 Defense Center, which does not support Security Intelligence data.

Working with Filters in the Context Explorer

License: FireSIGHT

Beyond the basic, wide-ranging data that the Context Explorer initially displays, you have the option to filter that data for a more granular contextual picture of activity on your network. Filters encompass all types of FireSIGHT data except URL information, support exclusion as well as inclusion, can be applied quickly by clicking on Context Explorer graph data points, and affect the entire explorer. You can apply up to 20 filters at once to create a highly specific portrait tailored to the needs of your network and organization. Filters that you apply are reflected in the Context Explorer URL so you can bookmark useful filter sets in your browser program for later use.

For information on using filters in the Context Explorer, see the following topics:

Adding and Applying Filters

License: feature dependent

Supported Devices: feature dependent

Supported Defense Centers: feature dependent

You can add filters to Context Explorer data in several ways:

- from the Add Filter window
- from the context menu pop-up window, when you select a data point in the explorer
- from the Context Explorer icon ( ) or from text links that appear in certain detail view pages (Application Detail, Host Profile, Rule Detail, and User Profile). Clicking these links automatically opens and filters the Context Explorer according to the relevant data on the detail view page. For example, clicking the Context Explorer link on a user detail page for the user `jenkins` constrains the explorer to show only data associated with that user

This section focuses on creating filters from scratch with the Add Filter window. For information on using the context menu to create quick filters from Context Explorer graph and list data, see Creating Filters with the Context Menu, page 56-44.

The Add Filter window, which you access by clicking the plus icon (+) under **Filters** at the top left of the Context Explorer, contains only two fields: **Data Type** and **Filter**.

The Data Type drop-down list contains many different types of FireSIGHT System data you can use to constrain the Context Explorer. After you select a data type, you then enter a specific value for that type in the **Filter** field (for example, a value of `Asia` for the type **Continent**). To assist you, the Filter field presents several grayed-out example values for the data type you select. (These are erased when you enter data in the field.)

The following table lists the data types available as filters, with examples and brief definitions of each. Note that The DC500 Defense Center does not display and Series 2 devices and Cisco NGIPS for Blue Coat X-Series do not detect data for features they do not support. See the Supported Access Control Capabilities by Device Model table for a summary of Series 2 device and Cisco NGIPS for Blue Coat X-Series features.

Table 56-2 Filter Data Types

Type	Example Values	Definition
Access Control Action	`Allow`, `Block`	Action taken by your access control policy to allow or block traffic
Application Category	`web browser`, `email`	General classification of an application's most essential function
Application Name	`Facebook`, `HTTP`	Name of an application
Application Risk	`Very High`, `Medium`	Estimated security risk of an application
Application Tag	`encrypts communications`, `sends mail`	Additional information about an application; applications can have any number of tags, including none
Application Type	`Client`, `Web Application`	Type of an application: application protocol, client, or web application
Business Relevance	`Very Low`, `High`	Estimated relevance of an application to business activity (as opposed to recreation)
Continent	`North America`, `Asia`	Continent associated with a routable IP address detected on your monitored network
Country	`Canada`, `Japan`	Country associated with a routable IP address detected on your monitored network
Device	`device1.example.com`, `192.168.1.3`	Name or IP address of a device on your monitored network

Table 56-2 Filter Data Types (continued)

Type	Example Values	Definition
Event Classification	`Potential Corporate Policy Violation`, `Attempted Denial of Service`	Capsule description of an intrusion event, determined by the classification of the rule, decoder, or preprocessor that triggered it
Event Message	`dns response`, `P2P`	Message generated by an event, determined by the rule, decoder, or preprocessor that triggered it
File Disposition	`Malware`, `Clean`	Cloud-determined disposition of a file for which the Defense Center performed a malware cloud lookup
File Name	`Packages.bz2`	Name of a file detected in network traffic
File SHA256	any 32-bit string	SHA-256 hash value of a file for which the Defense Center performed a malware cloud lookup
File Type	`GZ`, `SWF`, `MOV`	File type detected in network traffic
File Type Category	`Archive`, `Multimedia`, `Executables`	General category of file type detected in network traffic
IP Address	`192.168.1.3`, `2001:0db8:85a3::0000/24`	IPv4 or IPv6 addresses, address ranges, or address blocks Note that searching for an IP address returns events where that address was either the source or the destination for the event
Impact Level	`Impact Level 1`, `Impact Level 2`	Estimated impact of an event on your monitored network
Inline Result	`dropped`, `would have dropped`	Whether traffic was dropped, would have been dropped, or was not acted upon by the system
IOC Category	`High Impact Attack`, `Malware Detected`	Category for a triggered Indication of Compromise (IOC) event
IOC Event Type	`exploit-kit`, `malware-backdoor`	Identifier associated with a specific Indication of Compromise (IOC), referring to the event that triggers it
Malware Threat Name	`W32.Trojan.a6b1`	The name of a malware threat
OS Name	`Windows`, `Linux`	Name of an operating system
OS Version	`XP`, `2.6`	Specific version of an operating system
Priority	`high`, `low`	Estimated urgency of an event
Security Intelligence Category	`Malware`, `Spam`	Category of risky traffic, as determined by Security Intelligence
Security Zone	`My Security Zone`, `Security Zone X`	A set of interfaces through which traffic is analyzed and, in an inline deployment, passes
SSL	`yes`, `no`	SSL- or TLS-encrypted traffic
User	`wsmith`, `mtwain`	Identity of a user logged in to a host on your monitored network

In the Filter field, you can input special search parameters such as `*` and `!` essentially as you can in event searches. You can create exclusionary filters by prefixing filter parameters with the `!` symbol. For more information on the search constraints typically supported by the FireSIGHT System, see Using Wildcards and Symbols in Searches, page 60-5.

When multiple filters are active, values for the same data type are treated as OR search criteria: all data that matches at least one of the values appears. Values for different data types are treated as AND search criteria: to appear, data must match at least one value for each filtered data type. For example, data that appears for the filter set of `Application: 2channel`, `Application: Reddit`, and `User: edickinson` must be associated with the user `edickinson` **AND** either the application `2channel` **OR** the application `Reddit`.

After you confirm a data type and value for your filter, a filter widget appears at the top left of the page, displaying the new filter's data type and value.

Because you may want to configure multiple filters before you apply them, and because the Context Explorer may take time to fully reload all sections, filters that you add are not automatically applied. To apply filters, you must click **Apply Filters**. Filters that are configured, but not yet applied, appear faded. You can have up to 20 filters at a time, and you can delete individual filters by clicking the delete icon (✖) on the filter's widget. If you want to delete all filters at once, you can click the **Clear** button.

Note that some filter types are incompatible with others: for example, filters that relate to intrusion events (such as **Device** and **Inline Result**) cannot be applied at the same time as connection event-related filters (such as **Access Control Action**) because the system cannot sort connection event data by intrusion event data. The system automatically prevents incompatible filters from simultaneously applying; when one filter type is more recently activated, filters of the incompatible type are hidden as long as the incompatibility exists.

Note that the data displayed depends on such factors as how you license and deploy your managed devices, whether you configure features that provide the data and, in the case of Series 2 appliances, whether the appliance supports a feature that provides the data. For example, because neither the DC500 Defense Center nor Series 2 devices support URL filtering by category and reputation, the DC500 Defense Center does not display data for this feature and Series 2 devices do not detect this data.

To create a new filter from the Add Filter window:

Access: Admin/Any Security Analyst

Step 1 Select **Analysis > Context Explorer**.

The Context Explorer appears.

Step 2 Under **Filters** at the top right, click the plus icon (✚).

The Add Filter pop-up window appears.

Step 3 From the **Data Type** drop-down list, select the data type you want to filter on.

The Filter field populates with example values for that data type.

Step 4 In the **Filter** field, type the data type value you want to filter on.

Step 5 Click **OK**.

Your filter is added. The Context Explorer reappears and a corresponding filter widget appears.

Step 6 Optionally, repeat the previous steps to add more filters until you have the filter set you need. Note that because the Context Explorer does not automatically refresh, your filters are not applied when you add them.

Step 7 Click **Apply Filters**.

Your filters are applied and the Context Explorer refreshes to reflect the filtered data.

To delete a filter:

Access: Admin/Any Security Analyst

Step 1 Click the delete icon (✖) on any filter widget.

The filter is deleted.

To clear all filters:

Access: Admin/Any Security Analyst

Step 1 Click the **Clear** button that appears to the right of the filter widgets.

All filters are cleared.

Note that this button does not appear if no filters have been created.

Creating Filters with the Context Menu

License: FireSIGHT

While exploring Context Explorer graph and list data, you can click on data points, then use the context menu to quickly create a filter based on that data, either inclusive or exclusive. If you use the context menu to filter on information of data type Application, User, or Intrusion Event Message, or any individual host, the filter widget includes a widget information icon that links to the relevant detail page for that data type (such as Application Detail for application data). Note that you cannot filter on URL data.

You can also use the context menu to investigate specific graph or list data in more detail. For information, see Drilling Down on Context Explorer Data, page 56-39.

To create a filter from the context menu:

Access: Admin/Any Security Analyst

Step 1 Select **Analysis > Context Explorer**.

The Context Explorer appears.

Step 2 In any explorer section except Traffic and Intrusion Events over Time or sections that contain URL data, click a data point you want to filter on.

The context menu pop-up window appears nearby.

Step 3 You have two options:

- To add a filter for this data, click **Add Filter**.

  The filter is added and its widget appears at upper left.

- To add an exclusion filter for this data, click **Add Exclude Filter**. The filter, when applied, displays all data **not** associated with the excluded value.

The filter is added and its widget appears at upper left. Exclude filters display an exclamation point before the filter value.

To view filter detail:

Access: Admin/Any Security Analyst

Step 1 Click the information icon ( ) on any eligible filter widget.

A new window opens with the detail page relevant to the filter's data type.

Bookmarking Filters

License: FireSIGHT

Filters function as a simple, agile tool to get the precise FireSIGHT data context you need at any given time. They are not intended as permanent configuration settings, and disappear when you navigate away from the Context Explorer or end your session. However, your organization may use certain filter combinations frequently. To preserve filter settings for later use, you can create a browser bookmark of the Context Explorer with your preferred filters applied. Because applied filters are incorporated in the Context Explorer page URL, loading a bookmark of that page also loads the corresponding filters.