Lumen® Managed Security Services

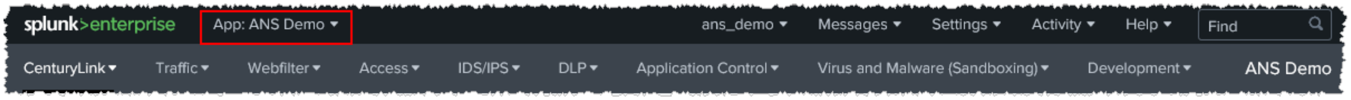
User guide for historical reporting for Security Solutions portal (powered by Splunk)

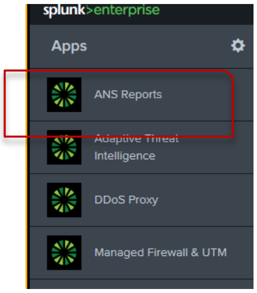
February 2022

Table of contents

About the Adaptive Network Security application

Lumen offers flexible reporting options via the security analytics application. The Adaptive Network Security service reports utilize a common layout and an intuitive user interface. This consists of a filter header to narrow down reporting results and one or more dashboard panels to list or visualize the report data. Common visualizations include time, bar, and pie charts. The following sections summarize the general features applied to each report within the ANS Reports section of the App: drop-down.





Dashboards & reports by service feature

The Lumen Adaptive Network Security product includes a range of services for customers to choose from. Each service feature is represented by a menu item and includes a dashboard and a report view (with the exception of the Adaptive Network Security Dashboard, which has no associated report view). Dashboards offer an overview of critical indicators of a service, while reports center on a table view of the underlying logged records.

- **Adaptive Network Security dashboard**—displays the landing page of the reporting application that combines important metrics from all features in distinct panels.
- **Traffic**—displays a report of traffic allowed and denied by firewall policy. (Requires that the All Traffic option under Policy Logging be selected during service setup.) Reports show how traffic was managed in response to such policies.
- **Webfilter**—displays the status of how internet content resources are used based on a category, domain, or IP address. These settings are defined for a specific user or IP address based on settings identified during service setup. Web Filtering classifies and blocks URLs and emails to help protect computers from infection. It controls the use of internet resources based on URL, content, and IP addresses, blocking and inspecting downloaded content for malicious code before it reaches a user's device.
- **Access**—displays information of successful and unsuccessful mobility endpoint client authentication status and top client duration in hours. Mobility or Site secure access is to a private network and the internet via Lumen internet access or third-party internet access.
- **IPS/IDS** (Intrusion Prevention and Detection Services)—displays intrusion prevention (dropped) and intrusion detection (detected) events over time identified in the status field as well distribution over time and top source and destination pairs. IPS/IDS provides management and monitoring, detection and prevention capabilities at the customer's network edge. Traffic matching signatures of known attacks generate incident reports and may also be

blocked on a per-signature basis.

- **DLP** (Data Loss Protection)—displays potential data loss attempts to send sensitive data including credit card and SSN information. DLP monitors, prevents, and reports on attempts to send sensitive data, including credit card and SSN information.
- **Application Control**—displays actions (pass or block) based on application usage. These setting are defined for a specific user, group, or IP address based on settings identified during service setup. Application Control identifies and enforces application use on the network.
- **Virus and Malware (Sandboxing)**—displays potential infections based on signatures and actions taken: analytics (sent to the sandbox for analysis), monitored, passthrough, blocked. Summaries of Top IP address, Agents, URLs, Files, Targeted Hosts, and Malware are displayed.

Filters and customization

At the top of each dashboard and report page, a filter section allows you to constrain and filter report results. You can customize a dashboard or report by picking a time range and using additional text and drop-down controls at the top of each page.

Note: The report pages for all Adaptive Network Security services follow the same layout.

Common controls include:

- **Time Range**—interval for viewing search results. (Note the Real-time option is no longer valid.)
- **Sampling**—some features include large numbers of logged events, which could negatively affect the query performance over longer time ranges. To accommodate dashboard searches over longer periods, a sampling rate can be applied. (A warning message appears under the filter section if the available data for the selected time range is insufficient to support the selected sampling rate.)
- **Any Field**—allows user to filter the display based on entered search criteria
- **Status**—disposition of the traffic and actions based on firewall policy rules
- **Priority**—indicates severity of event that caused the log message
- **Gateway or Device**—the firewall physical device that inspects traffic and enforces security compliance policies
- **Firewall Instance**—customer virtual network firewall instance with customer configured policies
- **Filter Mode**—identifies how many filter criteria is displayed. Default is Basic with pre-defined filter options. All Options displays all filter criteria options.
- **Export** button—**Export PDF** generates a PDF file that includes all chart visualizations and table data. **Print** allows you to print report data to a selected printer.

Note: Most filter controls are preset with the * wild card character that match any value. Entering a value and pressing either the enter or tab keys, or selecting a specific value from a drop down, reloads the page data with the filter in effect. For text controls, the * character can be used for partial matches. (For instance, the entry "10.8*" for an IP address filter matches any IP addresses starting with "10.8".) To remove a filter, click the x button inside a drop-down or delete the content of a text input field.

Each page displays only a few filter controls by default. This is the Basic filter set. To expand the filter section, open the **Filter Mode** drop-down, then select **All Options**.

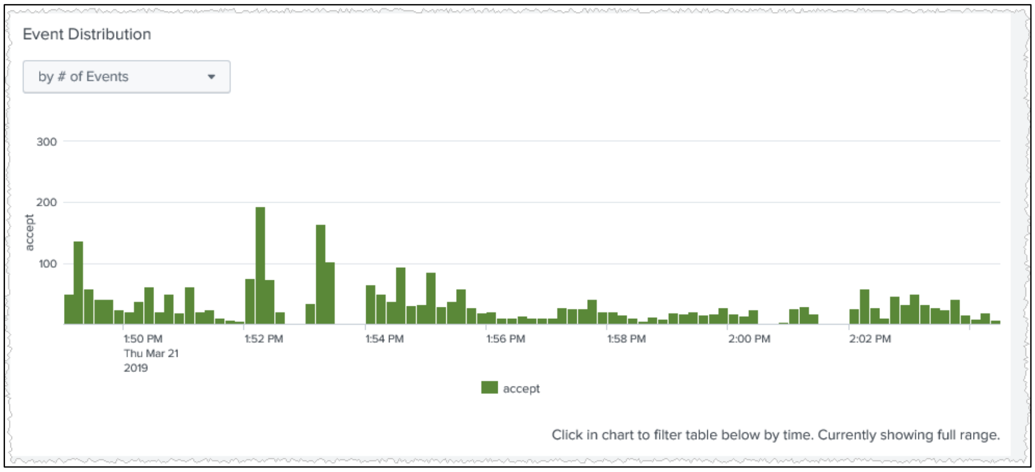
Note: Reports with many filter controls often hide those controls by default and only show those when needed, as controlled by the Filter Mode drop-down. **All Options** expands the view to show all available controls.

Filter controls apply to specific attributes, but each page also includes the **Any Field** text input control that searches against any native attribute of a data event. **Any Field** does not match against attributes that have been added in the report, such as Location or IP address.

Some drop downs include a number in parenthesis after the option value. This represents the number of occurrences of this option value in the current result set (without filtering, other than **Time Range** and **Any Field**).

Detailed views

Clicking on a dashboard panel opens a summary view of the underlying data in the report page (as indicated by the change of the cursor symbol (hand) when hovering over data text or a chart).



Click in chart to filter table below by time. Currently showing full range.

Figure 1: Example detail view

Navigating to a report page carries the existing filter and value selections. (For example, clicking in the area of the denied traffic in the firewall traffic chart of the Adaptive Network Security dashboard navigates to the traffic report with the status preset to Denied.)

Note: Only filters from the Basic filter set are passed on to a report from a dashboard. When a detail view opens a new page (replacing the current report page), many existing filter criteria from the header are passed to the new page as well.

Access to the reporting application

The Adaptive Network Security Reports Application is available to customers with Lumen Managed Security Services. To access the feature, open the **Reports** > **Security Solutions Analytics** page, then click the **Lumen Security Solutions Reporting** link at the top of the page.

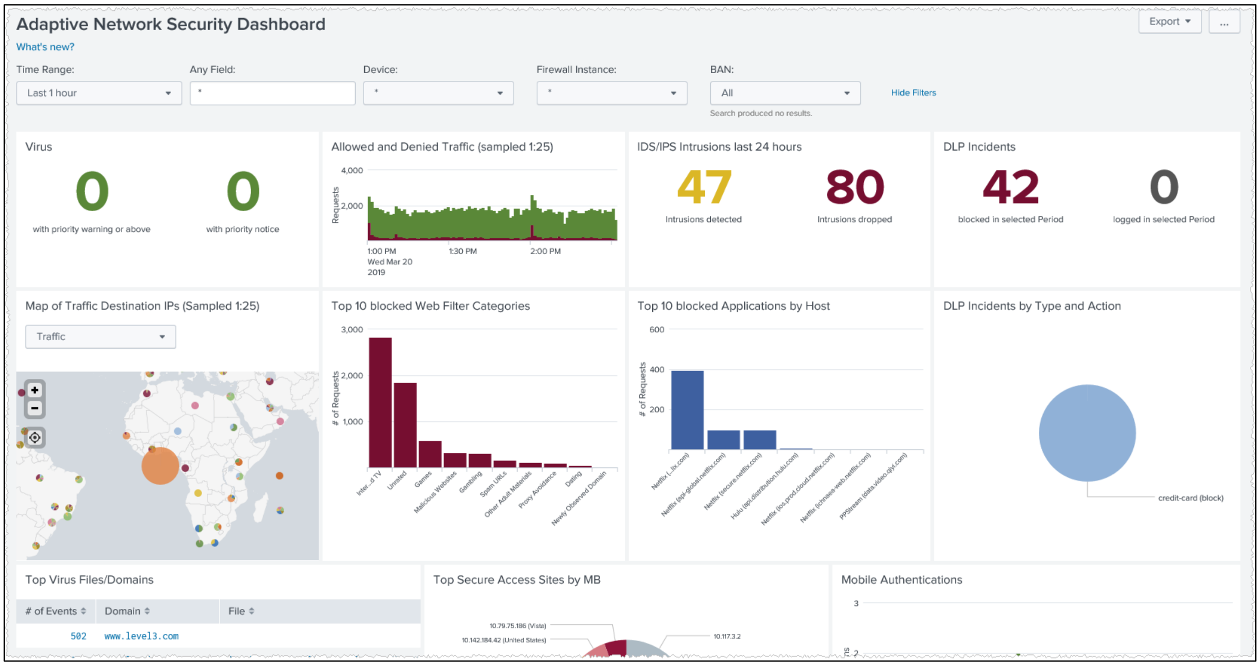
Note: Only users who have been set up with the managed security services permission and two-factor authentication can access the security reports.

Please note that, with the exception of the Access, DLP, Application Control, and Malware reports, the Adaptive Network Security Reporting Application is also applicable to the MSS Cloud and CPE services that so far have been covered by the Firewall & UTM reporting application.

Adaptive Network Security dashboard

The Adaptive Network Security Dashboard is the landing page of the reporting application (and is also available under the Lumen menu item). The dashboard dynamically combines important metrics from all service features in distinct panels: inclusion of a feature-specific panel indicates only if a customer has opted for the respective feature.

> **Note:** If no results are found in the selected range, the panel is hidden (even if the feature has been purchased).



Adaptive Network Security Dashboard

What's new?

Time Range: Last 1 hour

Any Field: *

Device: *

Firewall Instance: *

BAN: All

Search produced no results.

Top Virus Files/Domains

# of Events	Domain	File
502	www.level3.com	

Export
...
Hide Filters
Virus
0
with priority warning or above
0
with priority notice
Allowed and Denied Traffic (sampled 1:25)
4,000
2,000
Requests
1:00 PM
Wed Mar 20
2019
1:30 PM
2:00 PM
IDS/IPS Intrusions last 24 hours
47
Intrusions detected
80
Intrusions dropped
DLP Incidents
42
blocked in selected Period
0
logged in selected Period
Map of Traffic Destination IPs (Sampled 1:25)
Traffic
Top 10 blocked Web Filter Categories
3,000
2,000
1,000
# of Requests
Inter...d TV
Unrated
Games
Malicious Websites
Gambling
Spam URLs
Other Adult Materials
Proxy Avoidance
Dating
Newly Observed Domain
Top 10 blocked Applications by Host
600
400
200
# of Requests
Netflix (...lix.com)
Netflix (api-global.netflix.com)
Netflix (secure.netflix.com)
Hulu (api.distribution.hulu.com)
Netflix (ios.prod.cloud.netflix.com)
Netflix (ichnaea-web.netflix.com)
PPStream (data.video.qiyi.com)
DLP Incidents by Type and Action
credit-card (block)
Top Secure Access Sites by MB
10.79.75.186 (Vista)
10.142.184.42 (United States)
10.117.3.2
Mobile Authentications
3
2

Figure 2: Adaptive Network Security dashboard for a customer with all Adaptive Network Security services

In a full configuration, the following panels appear:

- The number of virus attacks of priority warning or higher for the last 24 hours (Anti-Virus) as well as the number of attacks with priority notice.
- A time chart of traffic volume in MB for allowed and denied firewall traffic for the selected range (Firewall Traffic).
- The number of dropped and detected IPS/IDS incidents for the last 24 hours (IDS/IPS).
- The number of blocked and logged DLP incidents for the selected range (DLP).
- A map showing the location of destination IPs for either denied or allowed traffic for the selected range (Firewall Traffic). Alternatively, the map can be changed to show the destination IPs for Virus and source IPs for IDS/IPS records.
- A column chart of the top 10 blocked web filter categories for the selected range (Webfilter).
- A column chart of the top 10 blocked application and host combinations for the selected range (Application Control).
- A pie chart showing the type of data detected or block (DLP).
- A list of the most frequently detected virus files for the last 24 hours (Virus).

Services not available everywhere. Business customers only. Lumen may change, cancel, or substitute products and services, or vary them by service area at its sole discretion without notice.

- A pie chart of the top secure access by volume in MB.
- A time chart of the number of failed and successful mobile access authentications.
- A time chart for scanning activity by rating (Malware Sandboxing).

Filters and customization

The main dashboard offers only limited filter controls as an overview across all services. However, the **Any Field** can be used for general purpose filtering against most attributes. In general, the Any Field matches only data that was in the raw log and not any additional decoration, such as location or IP address.

Due to the high variance in event counts for the different services, different time ranges are applied. Some panels show values for the last 24 hours or last 30 days. Other panels are aligned with the selected range of the Time Range picker. Note that 24 hours and 30 days panel do not change when the value of the Time Range picker is updated. Please use the service specific dashboard or report pages for those instead.

Detailed views

Clicking in a panel opens the corresponding report page, preserving selected values for the Any Field, Device, VDM, and BAN filter controls. Also, for some panels, the specific item that was clicked on is set on the report page filter as follows:

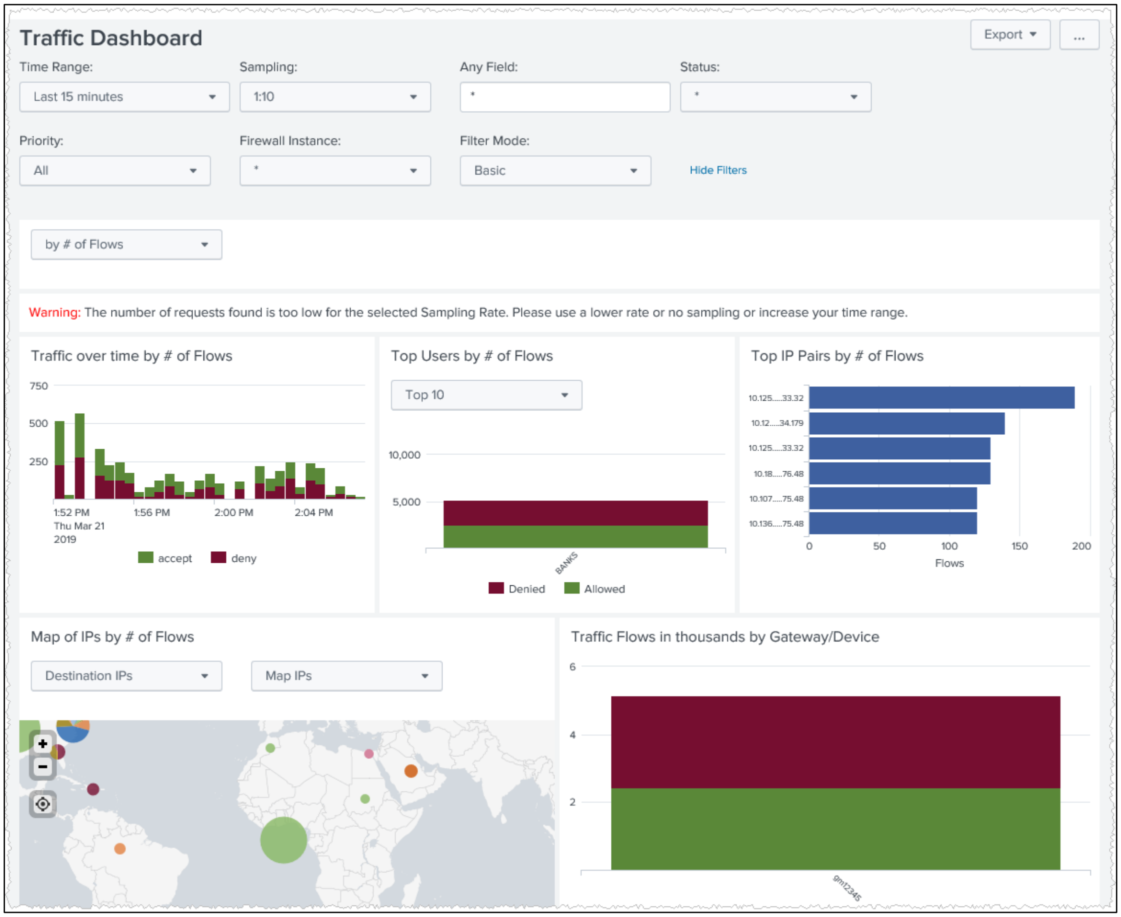
- Clicking on the number of Intrusions Detected or Intrusions Dropped opens the IDS/IPS report with status filter set to detected or dropped.
- Clicking on the number of Allowed and Denied Traffic opens the traffic report.
- Clicking on a column of the *Top 10 blocked Web Filter Categories* chart opens the Webfilter report with action set to Blocked and category set to the value of the selected column.
- Clicking on a column of the *Top 10 blocked Applications by Host* chart opens the Application Control report with action set to Block and application set to the application of the selected column.
- Clicking on a row of the *Virus last 24 ho*urs opens the Virus report with the file filter set. This automatically expands the filter section of the Virus report to *All Options*.

Traffic

The Traffic pages report on allowed and denied traffic traversing your firewall and are available under the Traffic menu item of the Adaptive Network Security Reports application. As for any feature, a summary dashboard and a report page are available. Report pages follow the same layout and pattern for each Adaptive Network Security feature and this is only described in detail in this Firewall Traffic section.

Traffic dashboard

The dashboard summarizes traffic data via multiple graphics. Traffic data can be shown either by the number of logged events (traffic flows) or by the associated volume in megabytes (MB), selectable via the drop down on top.



Traffic Dashboard

Time Range: Last 15 minutes

Sampling: 1:10

Any Field: *

Status: *

Priority: All

Firewall Instance: *

Filter Mode: Basic

by # of Flows

Warning: The number of requests found is too low for the selected Sampling Rate. Please use a lower rate or no sampling or increase your time range.

Figure 3: Traffic dashboard

The dashboard includes the following panels:

- A time chart of traffic by detailed status (deny, accept, timeout, etc.).
- A column chart of the top 10 users stacked by status summary (denied or allowed, where allowed matches any status not equal to deny). If user data is not available, this chart does not appear. The drop down allows hiding the highest volume user, which is useful when high occurrences of N/A or guest cause others to be compressed.
- The top six IP Pairs with most flows or data volume.

- A map that shows the location of source or destination IPs (selectable via drop down). Using the second drop down, you can switch to a top 10 bar chart of IPs or a table of IPs by status, service, and user:

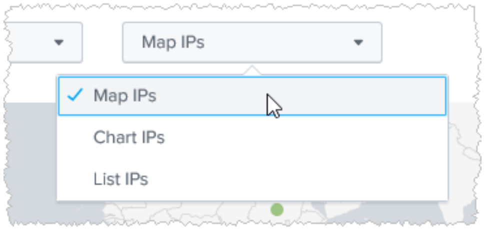


Figure 4: Top IP view options

- A stacked bar chart showing the top 10 Application Categories by performed action.
- A stacked column chart showing the top 10 Gateway Locations or Firewall Devices by requests and status (allowed or denied). The columns are sorted from left to right by denied requests.
- Two panels with top 10 bar charts that visualize the top source IPs or Users (for Active Directory integration) and top destination IPs or Locations (using IP geo lookup).

Filters and customization

The Traffic Dashboard offers a Basic filter set with the option to expand via the **Filter Type** drop down.

Traffic data can be shown either by the number of logged flows or by the associated volume in megabytes (MB), selectable via the drop down just below the filter section. This change applies to all panels in the dashboard.

> **Note:** Both the **Top Users** and **Top Applications** panels appear only if applicable data is found.

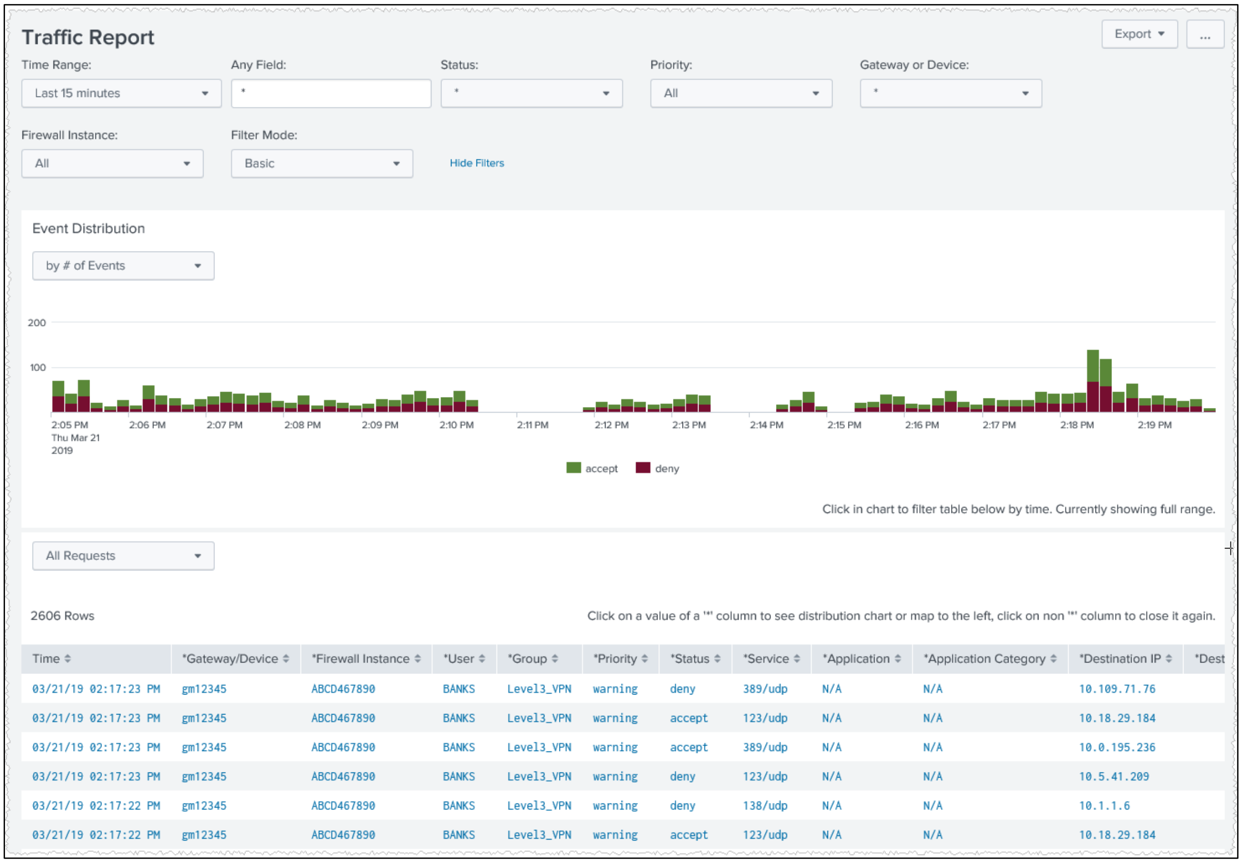
Detailed views

Clicking in a panel opens the traffic report page. Selected values for the **Any Field, Status** and **Firewall Instance** controls are passed on. Some of the special behavior for drill downs includes:

- Charts showing status **Denied** and **Allowed** do not pass the status value on a drill down. **Allowed** is a summary status (everything not equal to deny) with no matching status value in the report page.
- A drill down from the IP Pair chart passes the IP addresses to the **Any Field**, instead of the Source and Destination IP fields, to account for the bi-directional nature of the IP Pair counts.

Traffic report

The Traffic Report displays the logged events via a summarized graphical event distribution by time and listing with several summarized display options.



Traffic Report

Time Range: Last 15 minutes

Any Field: *

Status: *

Priority: All

Gateway or Device: *

Firewall Instance: All

Filter Mode: Basic

Event Distribution

by # of Events

Click in chart to filter table below by time. Currently showing full range.

All Requests

2606 Rows

Click on a value of a '*' column to see distribution chart or map to the left, click on non '*' column to close it again.

Time ⇕	*Gateway/Device ⇕	*Firewall Instance ⇕	*User ⇕	*Group ⇕	*Priority ⇕	*Status ⇕	*Service ⇕	*Application ⇕	*Application Category ⇕	*Destination IP ⇕	*Dest
03/21/19 02:17:23 PM	gm12345	ABCD467890	BANKS	Level3_VPN	warning	deny	389/udp	N/A	N/A	10.109.71.76	
03/21/19 02:17:23 PM	gm12345	ABCD467890	BANKS	Level3_VPN	warning	accept	123/udp	N/A	N/A	10.18.29.184	
03/21/19 02:17:23 PM	gm12345	ABCD467890	BANKS	Level3_VPN	warning	accept	389/udp	N/A	N/A	10.0.195.236	
03/21/19 02:17:23 PM	gm12345	ABCD467890	BANKS	Level3_VPN	warning	deny	123/udp	N/A	N/A	10.5.41.209	
03/21/19 02:17:22 PM	gm12345	ABCD467890	BANKS	Level3_VPN	warning	deny	138/udp	N/A	N/A	10.1.1.6	
03/21/19 02:17:22 PM	gm12345	ABCD467890	BANKS	Level3_VPN	warning	accept	123/udp	N/A	N/A	10.18.29.184	

Figure 5: Traffic Report

The Traffic Report page offers an extended set of filter controls available via the **All Options** of the Filter Type drop down. Figure 5 shows it with **All Options** selected. It also shows that for the Status filter, the accept value has been selected. Note that the number in parenthesis shows the amount of records for the selected time. It is obvious that the traffic data comes with a large number of events, which should be taken into account when selecting longer time frames. It is best to keep report windows to under four hours. The Report pages do not support sampling rates as this is the place where a user looks for the actual log data.

Filters and customization

The time chart above the table is optional and can be hidden via the Time Chart drop down. Depending on the drop-down selection above the chart, it plots data either by the number of logged traffic events or by the associated volume in MB. The time units are chosen automatically based on the length of the selected time range.

The table shows each logged traffic event, but also allows for summarization over time for IPs and Ports or just IPs via the drop down above the table. When summary aggregation is used, the Time value is dropped and instead, a Count column shows how many events with matching data have been combined in a given row.

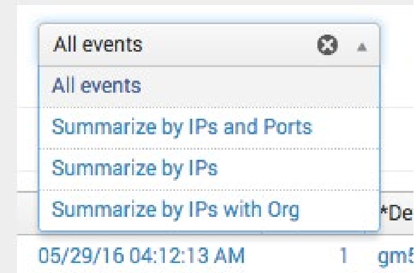


Figure 6: Summarize Events over Time

For summary by IPs, an additional option is to include the Organization for each IP via a best effort lookup. Note that this further impacts the load time for the table.

Click a value of a column that does not have the * character prefix, such as Time, to close the chart again and return to the regular table view.

Traffic report data table field definitions

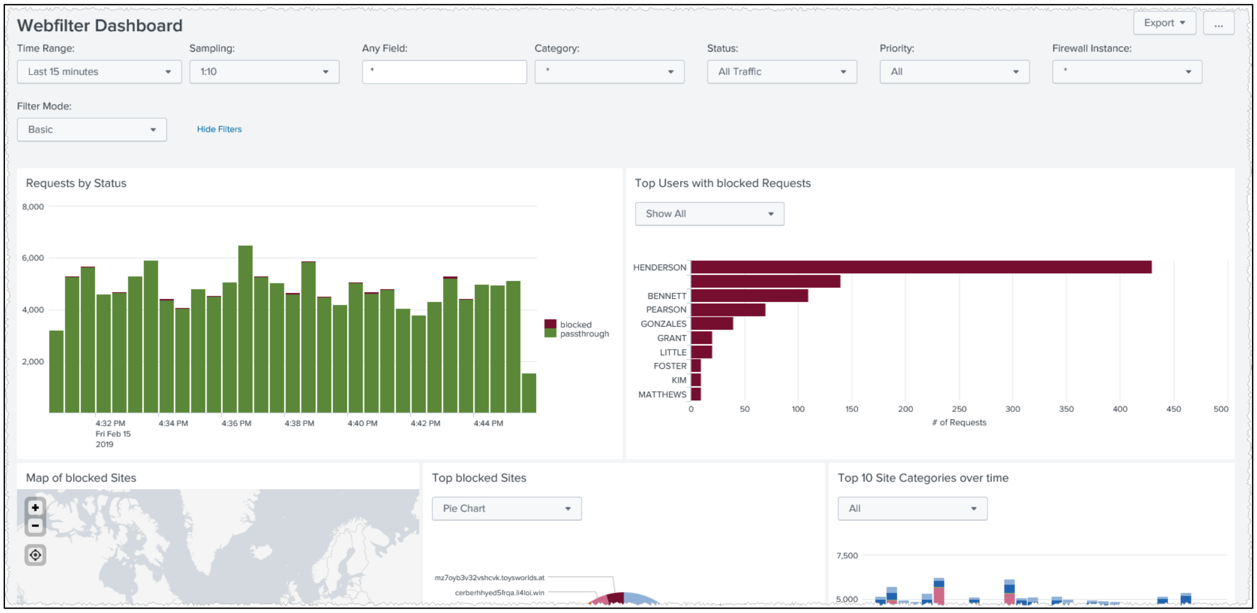
Item	Description
Time	Date/Time when log data was recorded
Gateway/Device	Adaptive Network Security Gateway location of Firewall Device
Firewall Instance	Virtual firewall identifier
User	Username (Active Directory Integration)
Group	Group name (Active Directory Integration)
Priority	Estimated Severity (See Appendix A – Priority Levels Table.)
Status	The status of the session: deny, start, close (allowed), timeout (allowed)
Service	The name of the application-layer protocol used by the traffic (http or https)
Application	Application name
Application Category	Application Category
Application Risk	Application Risk Level (low, medium, elevated, high, critical)
Application Action	The security action from app control (block, pass, reject, reset, monitor)
Source/Destination IP	IP address of traffic’s origin or destination
Source/Destination Port	Port number of traffic’s origin or destination
Source/Destination Location	City and country of source/destination IP (when available)
Duration	Duration of session
Megabytes Sent	Sent bytes in MB
Megabytes Received	Received bytes in MB
Total Megabytes	Sum of sent and received bytes (in MB)
Source Interface	The interface of the traffic's origin
Destination Interface	The interface of the traffic's destination
Policy ID	The name of the server policy governing the traffic causing the log message

Webfilter

Web Filtering classifies and blocks URLs and emails to help protect computers from infection. It controls the use of internet resources based on URL, content, and IP addresses blocking and inspecting downloaded content for malicious code before it reaches a user's device.

Webfilter dashboard

The Webfilter dashboard is available under the Webfilter menu item of the Adaptive Network Security reports application and presents logged events for URL and content based web traffic control.



Webfilter Dashboard

Time Range: Last 15 minutes
Sampling: 1:10
Any Field: *
Category: *
Status: All Traffic
Priority: All
Firewall Instance: *
Filter Mode: Basic

Figure 7: Webfilter dashboard

The dashboard includes the following panels:

- A time chart of requests by status.
- A bar chart of the top 10 users by blocked requests, if available.
- A map of the blocked sites.
- A top 10 blocked sites pie or bar chart.
- A time chart of either all or only the blocked requests by site categories.

Filters and customization

The Webfilter dashboard offers a Basic filter set with the option to expand via the Filter Type drop-down.

The Top Users panel allows excluding the user with the most requests via the drop down above, resulting in less compression for other users. The Top Blocked Sites panel supports a pie and bar chart visualization, while the Site Categories time chart can bet set to include all or just blocked requests.

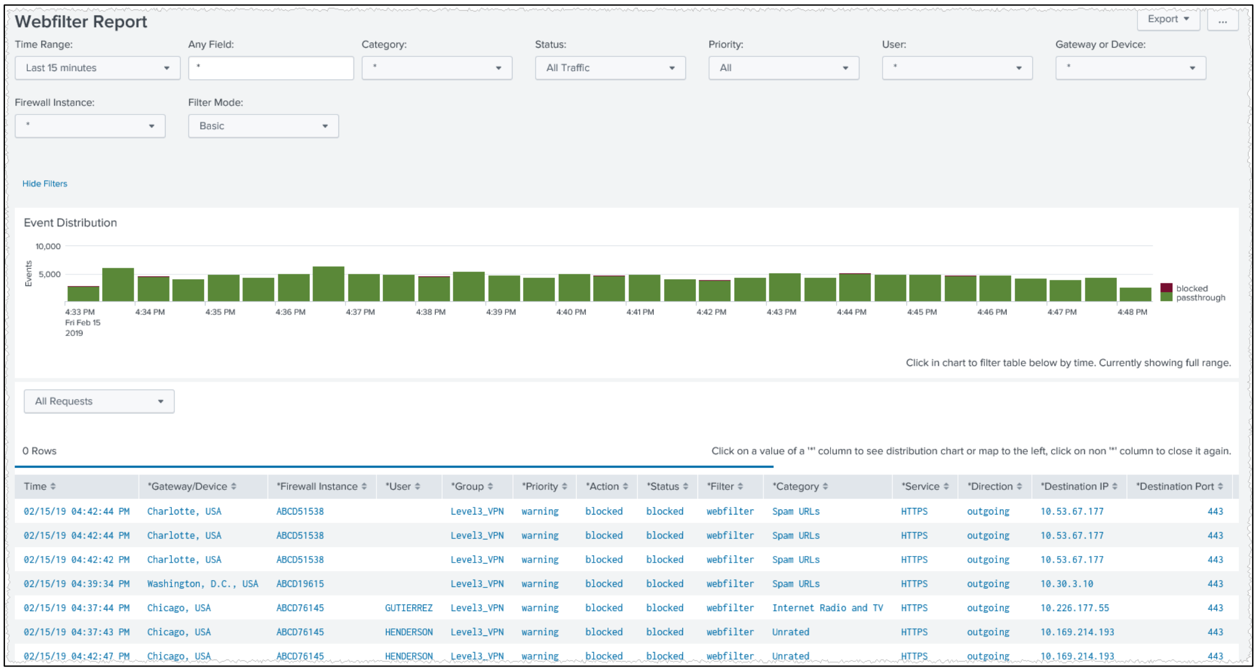
Detailed views

Clicking in a panel opens the Webfilter report page, preserving selected values for the **Any Field, Category, Status**, and **Firewall Instance** filter controls.

- Clicking on the *Request by Status* chart, opens the Webfilter report with status filter set to either blocked or passthrough, depending on what the user clicked on.
- The *Top Users with blocked Requests* does not support drill downs, but toggles between a bar chart and table presentation of top users.
- Clicking on the *Map of blocked Sites* opens the report page with status set to *blocked*.
- The *Top Blocked Sites* pie or bar chart (depending on drop down selection) supports an in-page drill down by setting the clicked-on site name to the Any Field filter of the Webfilter Dashboard.
- Drill down for the *Site Categories over time* chart sets the category filter in the report page, but does not set the Status field.

Webfilter report

The Webfilter report displays the logged events via a summarized graphical event distribution by time and listing with several summarized display options. Webfilter blocked, warning and monitor events are logged as standard.



Webfilter Report

Time Range: Last 15 minutes
Any Field: *
Category: *
Status: All Traffic
Priority: All
User: *
Gateway or Device: *
Firewall Instance: *
Filter Mode: Basic

Click in chart to filter table below by time. Currently showing full range.

All Requests

0 Rows

Click on a value of a '*' column to see distribution chart or map to the left, click on non '*' column to close it again.

Time	*Gateway/Device	*Firewall Instance	*User	*Group	*Priority	*Action	*Status	*Filter	*Category	*Service	*Direction	*Destination IP	*Destination Port
02/15/19 04:42:44 PM	Charlotte, USA	ABCD51538		Level3_VPN	warning	blocked	blocked	webfilter	Spam URLs	HTTPS	outgoing	10.53.67.177	443
02/15/19 04:42:44 PM	Charlotte, USA	ABCD51538		Level3_VPN	warning	blocked	blocked	webfilter	Spam URLs	HTTPS	outgoing	10.53.67.177	443
02/15/19 04:42:42 PM	Charlotte, USA	ABCD51538		Level3_VPN	warning	blocked	blocked	webfilter	Spam URLs	HTTPS	outgoing	10.53.67.177	443
02/15/19 04:39:34 PM	Washington, D.C., USA	ABCD19615		Level3_VPN	warning	blocked	blocked	webfilter	Spam URLs	HTTPS	outgoing	10.30.3.10	443
02/15/19 04:37:44 PM	Chicago, USA	ABCD76145	GUTIERREZ	Level3_VPN	warning	blocked	blocked	webfilter	Internet Radio and TV	HTTPS	outgoing	10.226.177.55	443
02/15/19 04:37:43 PM	Chicago, USA	ABCD76145	HENDERSON	Level3_VPN	warning	blocked	blocked	webfilter	Unrated	HTTPS	outgoing	10.169.214.193	443
02/15/19 04:42:47 PM	Chicago, USA	ABCD76145	HENDERSON	Level3_VPN	warning	blocked	blocked	webfilter	Unrated	HTTPS	outgoing	10.169.214.193	443

Figure 8: Webfilter report

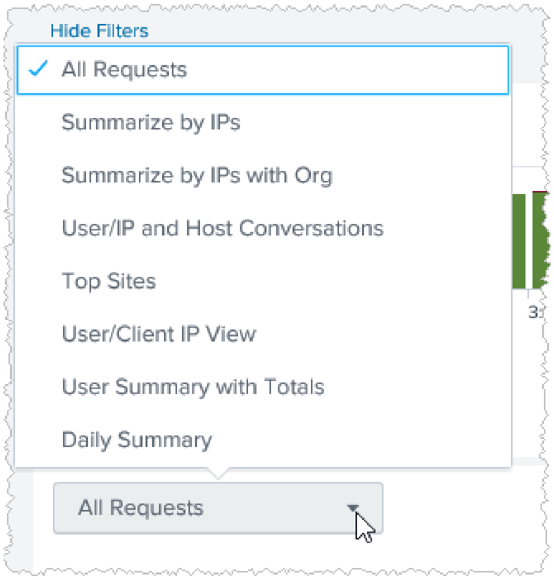


Figure 9: Webfilter aggregation options

The **All Requests** option, which is also the default, shows all individual requests. This can result in a large number of rows, even for fairly short reporting windows. In some cases, a report user is not interested in the individual requests, but in a general overview that summarizes requests by the targeted host and originating user (if available) or source IP. This can be done via the **Summarize by User/IP and Host** option.

Using the **User/IP and Host Conversations** option you get an additional breakdown by time, where only matching requests that occurred in close proximity are combined. Each record includes a start and end time as well as duration.

Webfilter report data table field definitions

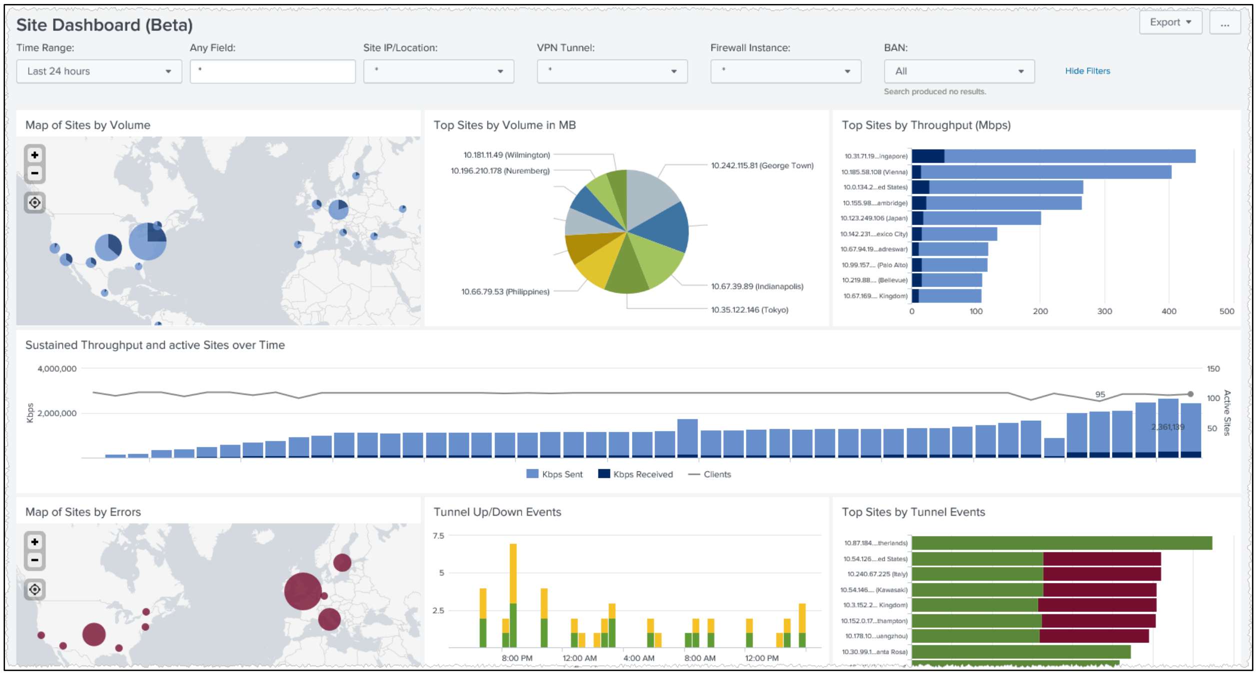
Attribute	Description
Time	Date/Time when log data was recorded
Gateway/Device	Adaptive Network Security Gateway location of Firewall Device
Firewall Instance	Virtual firewall identifier
User	Username (Active Directory Integration)
Group	Group name (Active Directory Integration)
Priority	Estimated Severity (See Appendix A – Priority Levels Table.)
Action	Security action performed, including pass, block, reject, reset, monitor
Status	Status based on security action performed (passthrough, blocked)
Filter	The Webfilter type
Category	Web category description
Service	Service name
Direction	Outgoing to the Internet.
Source/Destination IP	IP address of traffic's origin or destination
Source/Destination Port	Port number of traffic's origin or destination
Source/Destination Location	City and country of source/destination IP (when available)
Host	Host name of URL
URL	URL address
Bytes Sent	Sent Bytes
Bytes Rcvd.	Received Bytes

Access

The Access feature menu includes three items: a Site dashboard, a Mobility dashboard, and an access report, which includes the log records for both site and mobility data.

Site dashboard

This dashboard summarizes traffic from secure access site tunnels via multiple graphics.



Site Dashboard (Beta)

Time Range: Last 24 hours

Any Field: *

Site IP/Location: *

VPN Tunnel: *

Firewall Instance: *

BAN: All

Search produced no results.

Figure 10: Site dashboard

The dashboard includes the following panels:

- A map view plotting sites by geo location with their total volume in MB.
- A pie chart with the top 10 sites by volume in MB.
- A bar chart with the top 10 sites by throughput in Mbps. Note that throughput is an approximate value based on 10+ minute volume updates.
- A time chart showing bi-directional data throughput in Kbps and number of active sites. Throughput values are approximate, based on 10+ minute volume updates.
- A map view plotting each site by total volume.
- A time chart showing tunnel up and down events.
- A bar chart with the top 10 sites by logged tunnel events, breaking out error status.

Filters and customization

The Site dashboard offers only a Basic filter set, the User and VPN Tunnel fields being specific to the Mobility data.

Traffic data can be shown either by the number of logged flows or by the associated volume in megabytes (MB), selectable via the drop down just below the filter section. This change applies to all panels in the dashboard.

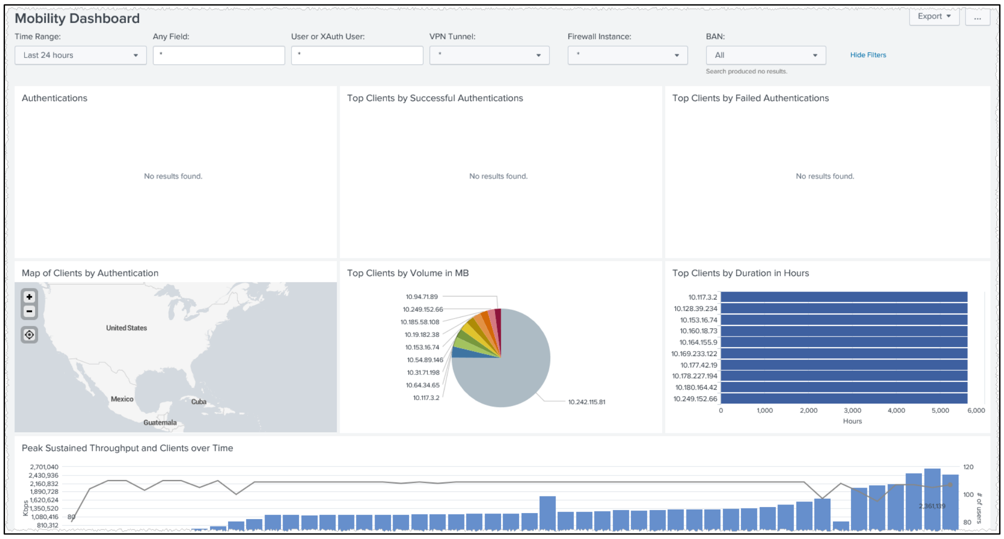
Both the **Top Users** and **Top Applications** panels appear only if applicable data is found.

Detailed views

Clicking in a panel opens the Access Report page with the Access Type control set to Mobility (see Access Report). Selected values for the **Any Field, Site IP/Location, VPN Tunnel, Firewall Instance**, and **BAN** controls are passed on.

Mobility dashboard

This dashboard offers an overview of mobility client activity, focusing on logins as well as data volume and session durations. Mobility clients are identified by user names and geo location (based on remote IP lookup).



Mobility Dashboard

Time Range: Last 24 hours

Any Field: *

User or XAuth User: *

VPN Tunnel: *

Firewall Instance: *

BAN: All

Search produced no results.

Authentications

No results found.

Top Clients by Successful Authentications

No results found.

Top Clients by Failed Authentications

No results found.

Figure 11: Mobility dashboard

The dashboard includes the following panels:

- A time chart of successful and failed authentication attempts.
- A bar chart of the top 10 clients by successful authentications.
- A bar chart of the top 10 clients by failed authentications.
- A map that shows the location of remote IPs by successful and failed authentications.
- A pie bar chart showing the top 10 clients by total data volume in MB.
- A bar chart with the top 10 clients by duration of sessions.
- A time chart showing bi-directional data throughput in Kbps. Values are approximate based on

10+ minute volume updates.

Filters and customization

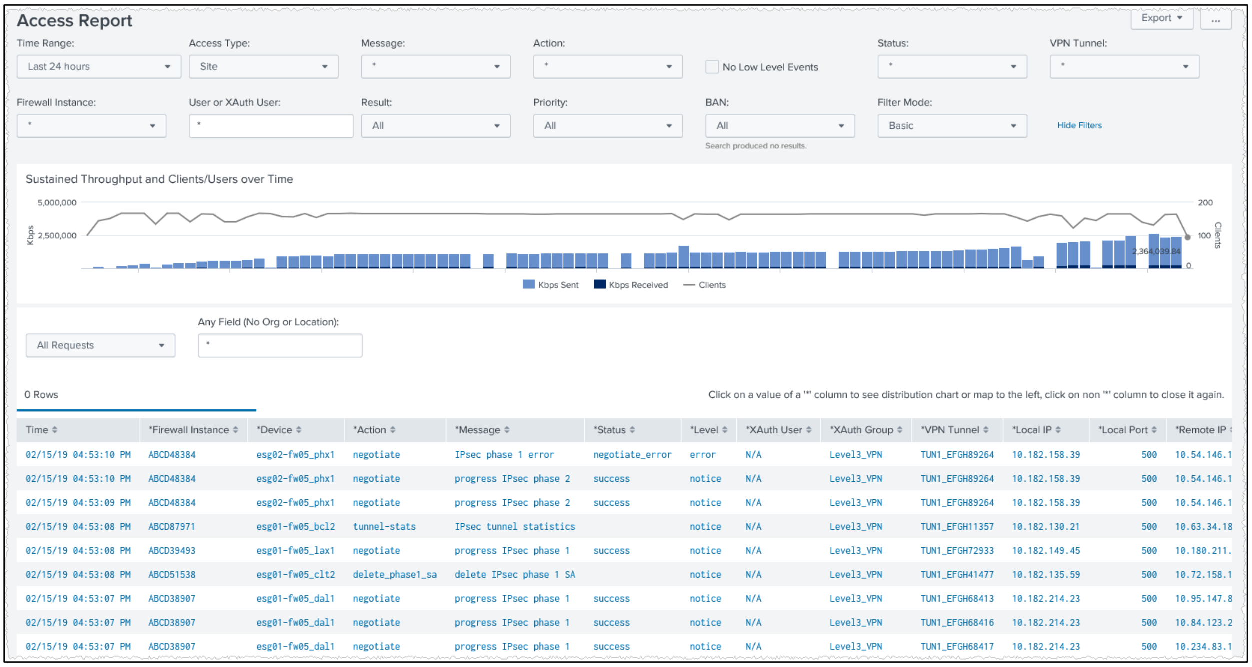
The Mobility dashboard offers only a Basic filter set, with User and VPN Tunnel fields being specific to the Mobility data.

Detailed views

Clicking in a panel opens the Access Report page with the Access Type control set to Site (see Access report). Selected values for the **Any Field, Site IP/Location, VPN Tunnel,** and **Firewall Instance** controls are passed on.

Access report

The Access report displays a summarized graphical distribution of sustained tunnel throughput over time and listing of each tunnel listing with several summarized display options. The access report supports both the Site and Mobility Access logs and can be specified via the Access Type control.



Access Report

Time Range: Last 24 hours
Access Type: Site
Message: *
Action: *
□ No Low Level Events
Status: *
VPN Tunnel: *
Firewall Instance: *
User or XAuth User: *
Result: All
Priority: All
BAN: All
Search produced no results.
Filter Mode: Basic

Any Field (No Org or Location): *

0 Rows

Click on a value of a '*' column to see distribution chart or map to the left, click on non '*' column to close it again.

Time	*Firewall Instance	*Device	*Action	*Message	*Status	*Level	*XAuth User	*XAuth Group	*VPN Tunnel	*Local IP	*Local Port	*Remote IP
02/15/19 04:53:10 PM	ABCD48384	esg02-fw05_phx1	negotiate	IPsec phase 1 error	negotiate_error	error	N/A	Level3_VPN	TUN1_EFGH89264	10.182.158.39	500	10.54.146.1
02/15/19 04:53:10 PM	ABCD48384	esg02-fw05_phx1	negotiate	progress IPsec phase 2	success	notice	N/A	Level3_VPN	TUN1_EFGH89264	10.182.158.39	500	10.54.146.1
02/15/19 04:53:09 PM	ABCD48384	esg02-fw05_phx1	negotiate	progress IPsec phase 2	success	notice	N/A	Level3_VPN	TUN1_EFGH89264	10.182.158.39	500	10.54.146.1
02/15/19 04:53:08 PM	ABCD87971	esg01-fw05_bcl2	tunnel-stats	IPsec tunnel statistics		notice	N/A	Level3_VPN	TUN1_EFGH11357	10.182.130.21	500	10.63.34.18
02/15/19 04:53:08 PM	ABCD39493	esg01-fw05_lax1	negotiate	progress IPsec phase 1	success	notice	N/A	Level3_VPN	TUN1_EFGH72933	10.182.149.45	500	10.180.211.
02/15/19 04:53:08 PM	ABCD51538	esg01-fw05_clt2	delete_phase1_sa	delete IPsec phase 1 SA		notice	N/A	Level3_VPN	TUN1_EFGH41477	10.182.135.59	500	10.72.158.1
02/15/19 04:53:07 PM	ABCD38907	esg01-fw05_dal1	negotiate	progress IPsec phase 1	success	notice	N/A	Level3_VPN	TUN1_EFGH68413	10.182.214.23	500	10.95.147.8
02/15/19 04:53:07 PM	ABCD38907	esg01-fw05_dal1	negotiate	progress IPsec phase 1	success	notice	N/A	Level3_VPN	TUN1_EFGH68416	10.182.214.23	500	10.84.123.2
02/15/19 04:53:07 PM	ABCD38907	esg01-fw05_dal1	negotiate	progress IPsec phase 1	success	notice	N/A	Level3_VPN	TUN1_EFGH68417	10.182.214.23	500	10.234.83.1

Figure 12: Access report

The report includes events of different log IDs, with additional type information shown under the Message column. Use the **No Low Level Events** check box to only include messages of type “IPsec tunnel statistics” and “IPsec connection status change”. The “IPsec tunnel statistics” events track accumulating counters for bytes sent and received as well as the length of sessions. Typically, updates are received about every 10 minutes. In addition to the throughput time chart, for Mobility an event time chart stacked by Action is also shown.

Filters and customization

The table shows each logged traffic event, but also allows for summarization over time for IPs and Ports via the drop down above the table. When summarization is used, the Time column is replaced by a Start, End Time, and Duration column; an additional Count column shows how many events with matching data have been combined in a single row.

For each column prefixed with the * character, clicking on a value displays a distribution bar chart on the left, showing the top 20 values of the selected column. By selecting an option in the drop-down, you can change the chart to a pie chart and suppress the top value or plot to only the bottom 20 percent. Clicking on a bar or pie slice sets the corresponding value from the bar to the filter section of the page (using the **Any Field**) and refreshes the search.

Access report data table field definitions

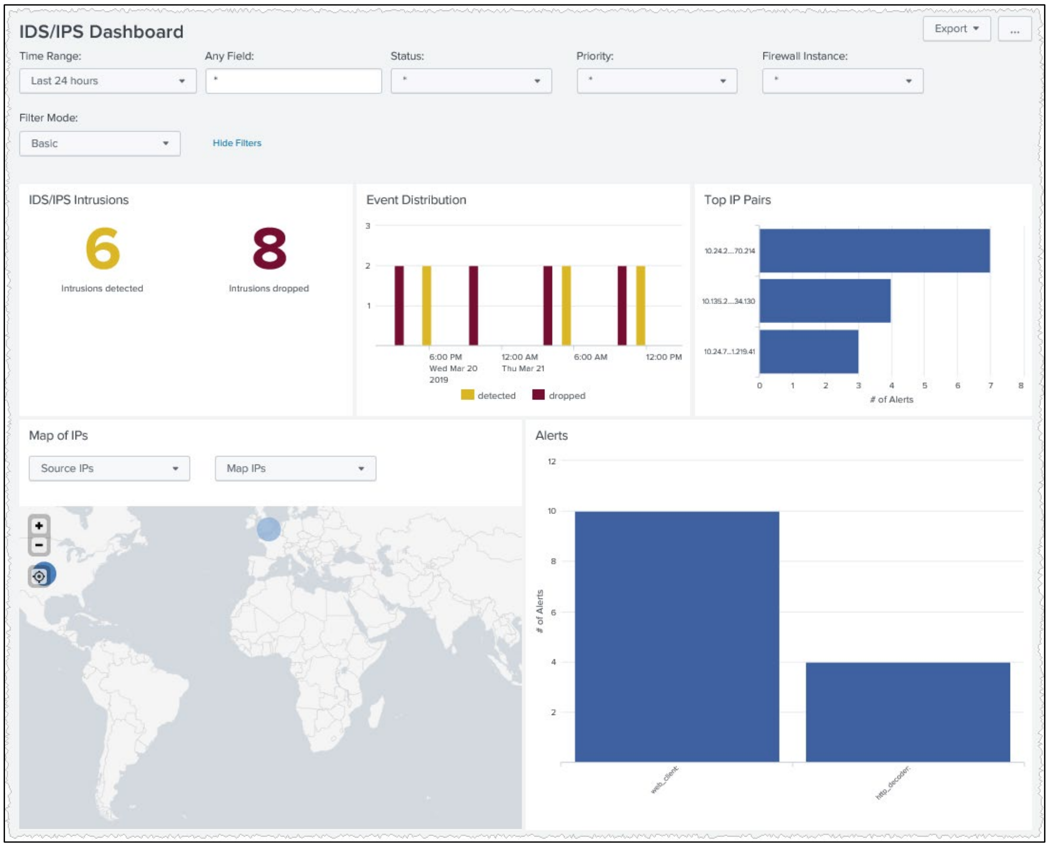
Attribute	Description
Time	Date/Time when log data was recorded
Firewall Instance	Virtual firewall identifier
Device	Adaptive Network Security Gateway location of Firewall Device
Action	Status of the session.
Message	Log Message
Status	Outcome of the log event action - Success or failure
Level	Log level
XAuth User	XAuth Username(Active Directory Integration)
XAuth Group	Xauth Group name(Active Directory Integration)
VPN Tunnel	IPsec VPN Tunnel Name
Local/Remote IP	IP address of traffic’s origin or destination
Local/Remote Port	Port number of traffic’s origin or destination
City	City of source/destination IP (when available)
Country	Country of source/destination IP (when available)
Assigned IP	Assigned IP Address
Duration (sec)	Duration of the current session in seconds
Sent bytes	Bytes sent from firewall instance to remote site across the VPN tunnel
Rcvd. Bytes	Bytes received at firewall instance from remote site across the VPN tunnel
Role	Role
Initiator	Initiator
Result	Result
Log Id	10-digit log identifier, starting with 0101

IDS/IPS

IDS/IPS prevents vulnerability exploits by examining packet content as it passes through the firewall against known signatures to detect, report and block intrusive behavior directed by your firewall policy.

IDS/IPS dashboard

The IDS/IPS dashboard (and report) is available under the IDS/IPS menu item of the Adaptive Network Security Reports application and presents logged alerts for intrusion detection and prevention incidents.



IDS/IPS Dashboard

Time Range: Last 24 hours

Any Field: *

Status: *

Priority: *

Firewall Instance: *

Filter Mode: Basic

Figure 13: IDS/IPS dashboard

The dashboard includes the following panels:

- The total numbers of detected and dropped intrusions.
- A time chart of alerts by status (detected/dropped).
- A bar chart of the top 6 IP Pairs by number of incidents.
- A map of source or destination IPs, selectable by drop down. Can also render a bar chart or table of IPs.
- A top 10 bar chart of the most common alerts.

Filters and customization

The IDS/IPS dashboard offers a Basic filter set with the option to expand via the **Filter Mode** drop down. Source and Destination IPs can either be plotted in a map (default), as a bar chart based on the number of alerts, or as a table.

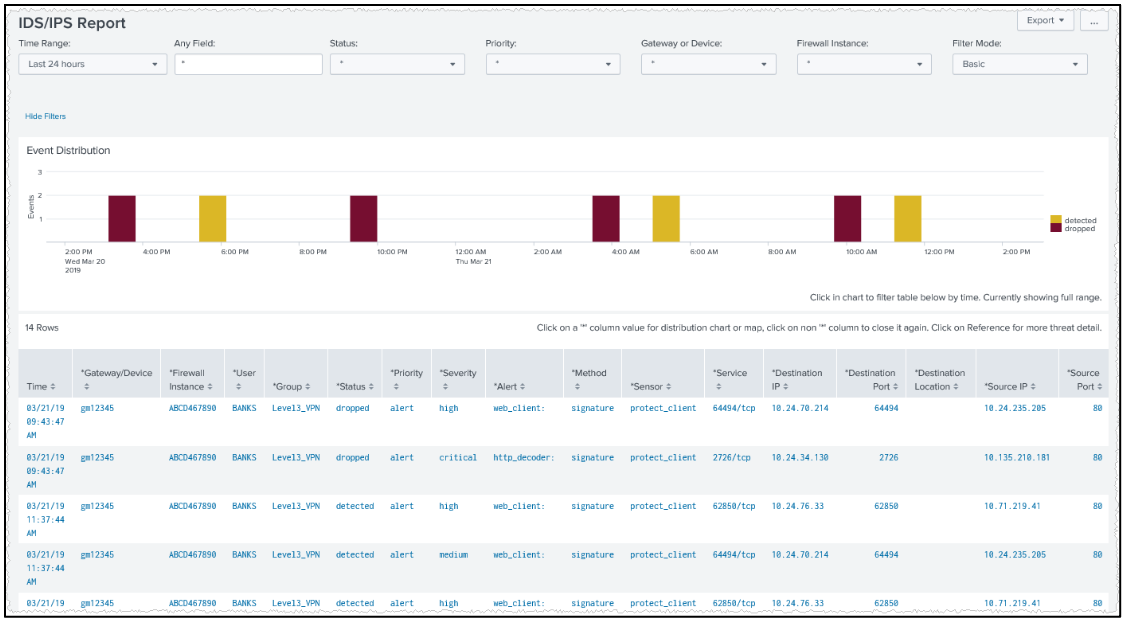
Detailed views

Clicking in a panel opens the IDS/IPS report page, preserving selected values for the **Any Field, Status, Firewall Instance**, and **BAN** filter controls.

- Clicking on the number, the *Detected or Dropped IDS/IPS Intrusions* or on the Alert Distribution chart opens the IDS/IPS report with status filter set to either detected or dropped, depending on what the user clicked on.
- Drill down from a bar of the Top IP Pairs chart sets the IP addresses to the Any Field filter of the reports page to only show alerts for such pairs.
- The Map of IPs opens the IDS/IPS report page without filtering, while a drill down from the alternate chart or table view sets the IP address of the selected bar or row to the respective Source or Destination IP filter field. In this case, the Filter Mode automatically expands to *All Options* to show the IP filter fields.
- The top Alerts column chart toggles between a column chart and table view.

IDS/IPS report

The IDS/IPS report displays the logged events via a summarized graphical event distribution by time and listing with several summarized display options.



IDS/IPS Report

Time Range: Last 24 hours

Any Field: *

Status: *

Priority: *

Gateway or Device: *

Firewall Instance: *

Filter Mode: Basic

Click in chart to filter table below by time. Currently showing full range.

14 Rows

Click on a '*' column value for distribution chart or map, click on non '*' column to close it again. Click on Reference for more threat detail.

Time	*Gateway/Device	*Firewall Instance	*User	*Group	*Status	*Priority	*Severity	*Alert	*Method	*Sensor	*Service	*Destination IP	*Destination Port	*Destination Location	*Source IP	*Source Port
03/21/19 09:43:47 AM	gm12345	ABCD467890	BANKS	Level3_VPN	dropped	alert	high	web_client:	signature	protect_client	64494/tcp	10.24.70.214	64494		10.24.235.205	80
03/21/19 09:43:47 AM	gm12345	ABCD467890	BANKS	Level3_VPN	dropped	alert	critical	http_decoder:	signature	protect_client	2726/tcp	10.24.34.130	2726		10.135.210.181	80
03/21/19 11:37:44 AM	gm12345	ABCD467890	BANKS	Level3_VPN	detected	alert	high	web_client:	signature	protect_client	62850/tcp	10.24.76.33	62850		10.71.219.41	80
03/21/19 11:37:44 AM	gm12345	ABCD467890	BANKS	Level3_VPN	detected	alert	medium	web_client:	signature	protect_client	64494/tcp	10.24.70.214	64494		10.24.235.205	80
03/21/19	gm12345	ABCD467890	BANKS	Level3_VPN	detected	alert	high	web_client:	signature	protect_client	62850/tcp	10.24.76.33	62850		10.71.219.41	80

Figure 14: IDS/IPS report

IDS/IPS report table data field definitions

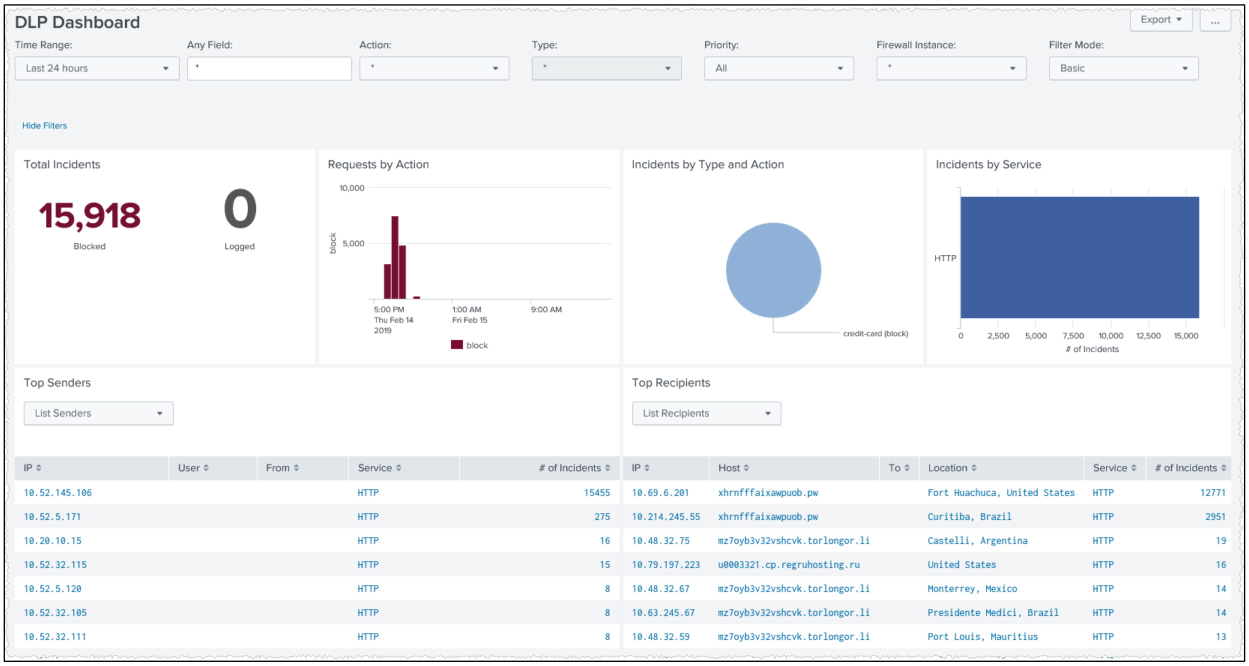
Attribute	Description
Time	Date/Time when log data was recorded
Gateway/Device	Adaptive Network Security Gateway location of Firewall Device
Firewall Instance	Virtual firewall identifier
User	Username (Active Directory Integration)
Group	Group name (Active Directory Integration)
Status	Status based on security action performed (dropped, detected)
Priority	Estimated Severity of the event that caused the log message (See Appendix A – Priority Levels Table.)
Severity	Severity of the attack (info, low, medium, high, critical)
Alert	Message description
Host	Host name of URL
Method	Sub type for message description
Service	Service name
Source/Destination IP	IP address of traffic's origin or destination
Source/Destination Port	Port number of traffic's origin or destination
Source/Destination Location	City and country of source/destination IP (when available)
Reference	References the known threat used to log the event

DLP

Data Loss Protection (DLP) monitors, prevents, and reports on attempts to send sensitive data outside a customer's organization.

DLP dashboard

The DLP dashboard presents a summary of the total number of incidents, requests by action, incidents by type and action, incidents by service, top senders, and top recipients.



DLP Dashboard

Time Range: Last 24 hours
Any Field: *
Action: *
Type: *
Priority: All
Firewall Instance: *
Filter Mode: Basic

Top Senders

IP	User	From	Service	# of Incidents
10.52.145.106			HTTP	15455
10.52.5.171			HTTP	275
10.20.10.15			HTTP	16
10.52.32.115			HTTP	15
10.52.5.120			HTTP	8
10.52.32.105			HTTP	8
10.52.32.111			HTTP	8

Top Recipients

IP	Host	To	Location	Service	# of Incidents
10.69.6.201	xhrnfffaixawpuob.pw		Fort Huachuca, United States	HTTP	12771
10.214.245.55	xhrnfffaixawpuob.pw		Curitiba, Brazil	HTTP	2951
10.48.32.75	mz7oyb3v32vshcvk.torlongor.li		Castelli, Argentina	HTTP	19
10.79.197.223	u0003321.cp.regruhosting.ru		United States	HTTP	16
10.48.32.67	mz7oyb3v32vshcvk.torlongor.li		Monterrey, Mexico	HTTP	14
10.63.245.67	mz7oyb3v32vshcvk.torlongor.li		Presidente Medici, Brazil	HTTP	14
10.48.32.59	mz7oyb3v32vshcvk.torlongor.li		Port Louis, Mauritius	HTTP	13

Figure 15: DLP dashboard

The dashboard includes the following panels:

- The total numbers of blocked and logged DLP incidents.
- A time chart of incidents by action (blocked/logged).
- A pie chart of incidents by type and status for the selected period.
- A bar chart showing incidents by service.
- Two panels that visualize the top senders and recipients of requests with identified DLP incidents. By default, they appear in a table format but can be altered to a map and chart view via drop downs.

Filters and customization

The DLP dashboard offers a Basic filter set with the option to expand via the **Filter Type** drop down.

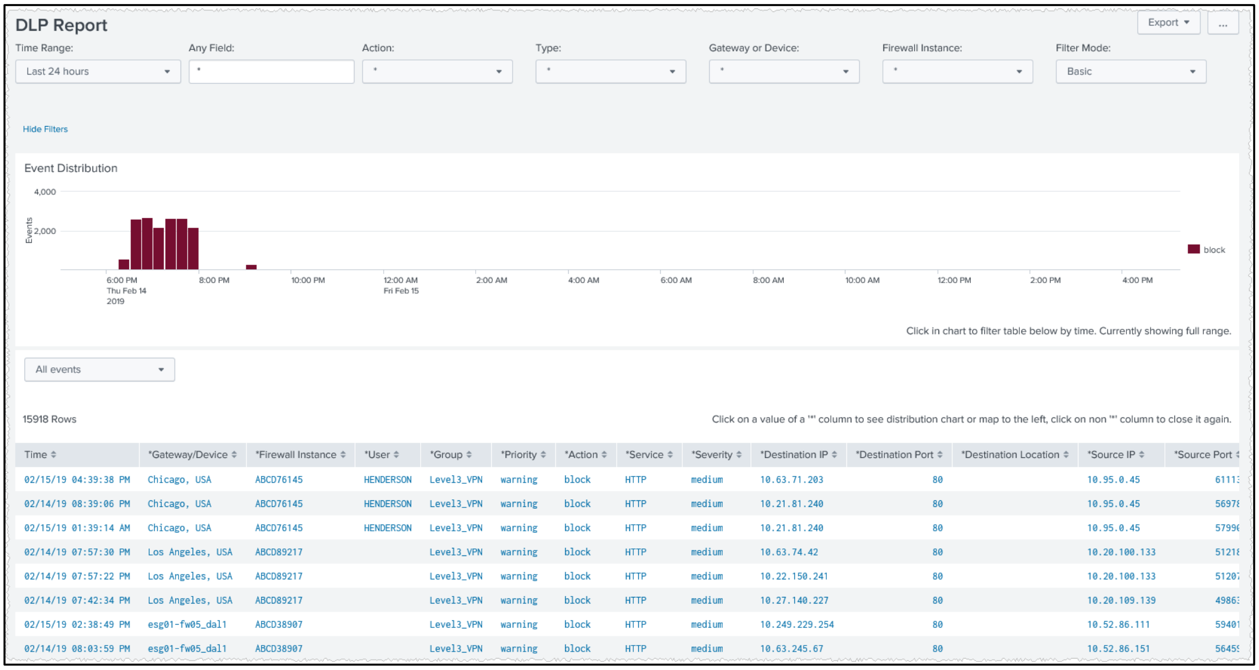
Detailed views

Clicking in a panel opens the DLP report page, preserving selected values for the **Any Field, Action, Type (such as Credit Card or SSN), and Firewall Instance** filter controls.

- Clicking on the number the *Blocked or Logged DLP incidents* or on the *Request by Action* chart, opens the DLP report with action filter set to either blocked or logged, depending on what the user clicked on.
- Drill down from the *Incidents by Type and Action* pie chart opens the report page with both file type and action preset to the selected values.
- Clicking on a row or bar for the Top Senders or Top Recipients panels sets the respective source or destination IP filter of the report page with the selected IP. The alternate map view does not support additional filtering on drill down.

DLP report

The DLP report displays the logged events via a summarized graphical event distribution by time and listing with several summarized display options.



Time Range: Last 24 hours

Any Field: *

Action: *

Type: *

Gateway or Device: *

Firewall Instance: *

Filter Mode: Basic

Click in chart to filter table below by time. Currently showing full range.

All events

15918 Rows

Click on a value of a '*' column to see distribution chart or map to the left, click on non '*' column to close it again.

Time	*Gateway/Device	*Firewall Instance	*User	*Group	*Priority	*Action	*Service	*Severity	*Destination IP	*Destination Port	*Destination Location	*Source IP	*Source Port
02/15/19 04:39:38 PM	Chicago, USA	ABCD76145	HENDERSON	Level3_VPN	warning	block	HTTP	medium	10.63.71.203	80		10.95.0.45	61113
02/14/19 08:39:06 PM	Chicago, USA	ABCD76145	HENDERSON	Level3_VPN	warning	block	HTTP	medium	10.21.81.240	80		10.95.0.45	56978
02/15/19 01:39:14 AM	Chicago, USA	ABCD76145	HENDERSON	Level3_VPN	warning	block	HTTP	medium	10.21.81.240	80		10.95.0.45	57990
02/14/19 07:57:30 PM	Los Angeles, USA	ABCD89217		Level3_VPN	warning	block	HTTP	medium	10.63.74.42	80		10.20.100.133	51218
02/14/19 07:57:22 PM	Los Angeles, USA	ABCD89217		Level3_VPN	warning	block	HTTP	medium	10.22.150.241	80		10.20.100.133	51207
02/14/19 07:42:34 PM	Los Angeles, USA	ABCD89217		Level3_VPN	warning	block	HTTP	medium	10.27.140.227	80		10.20.109.139	49863
02/15/19 02:38:49 PM	esg01-fw05_dal1	ABCD38907		Level3_VPN	warning	block	HTTP	medium	10.249.229.254	80		10.52.86.111	59401
02/14/19 08:03:59 PM	esg01-fw05_dal1	ABCD38907		Level3_VPN	warning	block	HTTP	medium	10.63.245.67	80		10.52.86.151	56459

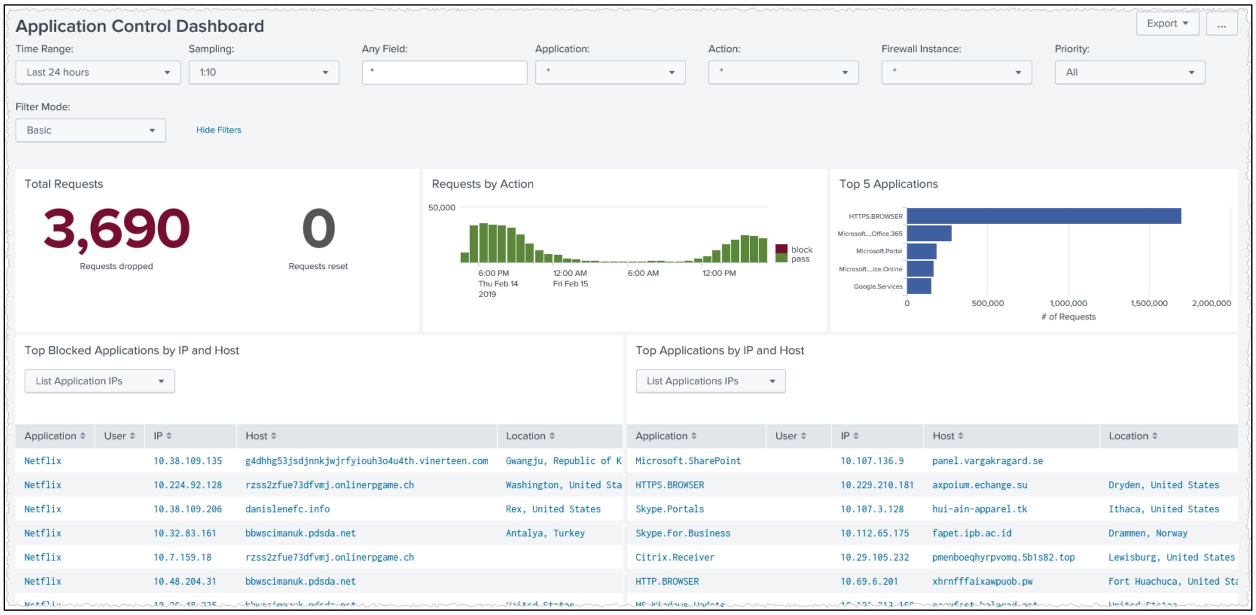
DLP report data table field definitions

Attribute	Description
Time	Date/Time when log data was recorded
Gateway/Device	Adaptive Network Security Gateway location of Firewall Device
Firewall Instance	Virtual firewall identifier
User	Username (Active Directory Integration)
Group	Group name (Active Directory Integration)
Priority	Estimated Severity of the event that caused the log message (See Appendix A – Priority Levels Table.)
Action	Security action performed
Service	Service name
Severity	Severity level of DLP rule
Destination / Source IP	IP address of traffic's origin or destination
Destination / Source Port	Port number of traffic's origin or destination
Destination / Source Location	City and country of source/destination IP (when available)
File Type	File type
Filter Category	DLP Filter Category
File Name	File name
File Size	File size in bytes
Filter Type	DLP Filter Type (credit card, SSN)
Message	Log Message
Host	Host name of URL
URL	URL address
KB Sent	Sent Bytes
KB Rcvd.	Received Bytes

Application Control

Application Control dashboard

The Application Control Dashboard is available under the Application Control menu item of the reports application and presents logged events for application-based activities.



Application Control Dashboard

Export ▾ ...

Time Range: Last 24 hours ▾

Sampling: 1:10 ▾

Any Field: *

Application: * ▾

Action: * ▾

Firewall Instance: * ▾

Priority: All ▾

Filter Mode: Basic ▾

Hide Filters

Total Requests

3,690 Requests dropped

0 Requests reset

Requests by Action

Top 5 Applications

Top Blocked Applications by IP and Host

List Application IPs ▾

Application ⇕	User ⇕	IP ⇕	Host ⇕	Location ⇕
Netflix		10.38.109.135	g4dhhg53jsdjnnkjwjrfyiouh3o4u4th.vinerteen.com	Gwangju, Republic of K
Netflix		10.224.92.128	rzss2zfue73dfvmj.onlinerpgame.ch	Washington, United Sta
Netflix		10.38.109.206	danislenefc.info	Rex, United States
Netflix		10.32.83.161	bbwscimanuk.pdsda.net	Antalya, Turkey
Netflix		10.7.159.18	rzss2zfue73dfvmj.onlinerpgame.ch	
Netflix		10.48.204.31	bbwscimanuk.pdsda.net	
Netflix		10.26.48.225	bbwscimanuk.pdsda.net	United States

Top Applications by IP and Host

List Applications IPs ▾

Application ⇕	User ⇕	IP ⇕	Host ⇕	Location ⇕
Microsoft.SharePoint		10.107.136.9	panel.vargakragard.se	
HTTPS.BROWSER		10.229.210.181	axpoium.echange.su	Dryden, United States
Skype.Portals		10.107.3.128	hui-ain-apparel.tk	Ithaca, United States
Skype.For.Business		10.112.65.175	fapet.ipb.ac.id	Drammen, Norway
Citrix.Receiver		10.29.105.232	pmenboeqhyrpvomq.5b1s82.top	Lewisburg, United States
HTTP.BROWSER		10.69.6.201	xhrnfffaixawpuob.pw	Fort Huachuca, United Sta
MS.Windows.Update		[illegible]	[illegible]	United States

Figure 16: Application Control dashboard

The dashboard includes the following panels:

- The total numbers of dropped and reset requests.
- A time chart of incidents by action (block/pass).
- A bar chart of top 10 applications by the number of requests for the selected period.
- Two panels that visualize the top blocked and overall applications by IP and Host. By default, they appear in a table format but can be altered to a map and chart view via drop downs.

Filters and customization

The Application Control dashboard offers a Basic filter set with the option to expand via the Filter Type drop down. A Sampling option defaults to 1:10 to accelerate load times, but can be turned off or set to a range of different rates.

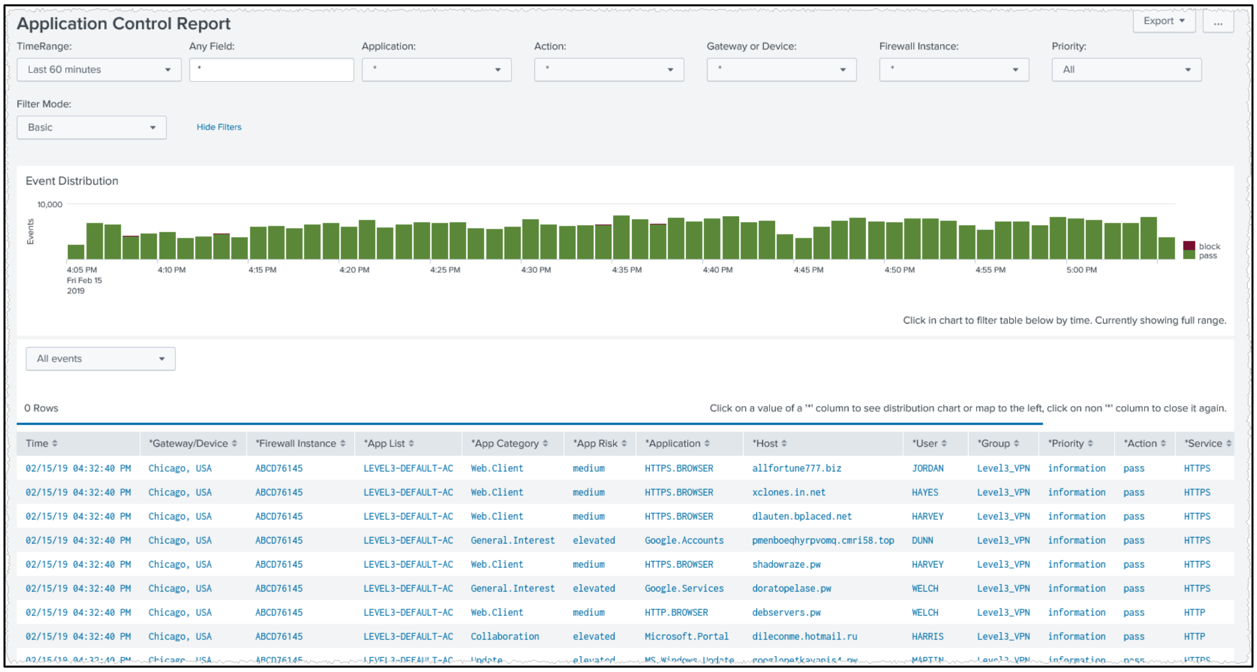
Detailed views

Clicking in a panel opens the Application Control report page, preserving selected values for the **Any Field, Application, Action, Firewall Instance**, and **Priority** filter controls.

- Clicking on the number the *Blocked or Reset Requests* or on the *Request by Action* chart, opens the Application Control report with action filter set to either blocked or reset, depending on what the user clicked on.
- Drill down from the *Top 5 Applications* bar chart sets the application to that of the selected bar.
- Clicking on either a row or bar of the *Top Applications by IP and Host* presets both the IP and host filters on the Report page. For the *Top Blocked Applications* panel, it also sets the action to blocked. The Map visualizations only sets the action for the *Top Blocked Applications* panel, but does not set the IP or host.

Application Control report

The Application Control report displays the logged events via a summarized graphical event distribution by time and listing with several summarized display options.



Application Control Report

TimeRange: Last 60 minutes
Any Field: *
Application: *
Action: *
Gateway or Device: *
Firewall Instance: *
Priority: All

Filter Mode: Basic

Click in chart to filter table below by time. Currently showing full range.

0 Rows

Click on a value of a '*' column to see distribution chart or map to the left, click on non '*' column to close it again.

Time	*Gateway/Device	*Firewall Instance	*App List	*App Category	*App Risk	*Application	*Host	*User	*Group	*Priority	*Action	*Service
02/15/19 04:32:40 PM	Chicago, USA	ABCD76145	LEVEL3-DEFAULT-AC	Web.Client	medium	HTTPS.BROWSER	allfortune777.biz	JORDAN	Level3_VPN	information	pass	HTTPS
02/15/19 04:32:40 PM	Chicago, USA	ABCD76145	LEVEL3-DEFAULT-AC	Web.Client	medium	HTTPS.BROWSER	xclones.in.net	HAYES	Level3_VPN	information	pass	HTTPS
02/15/19 04:32:40 PM	Chicago, USA	ABCD76145	LEVEL3-DEFAULT-AC	Web.Client	medium	HTTPS.BROWSER	dlauten.bplaced.net	HARVEY	Level3_VPN	information	pass	HTTPS
02/15/19 04:32:40 PM	Chicago, USA	ABCD76145	LEVEL3-DEFAULT-AC	General.Interest	elevated	Google.Accounts	pmenboeqhyrpvomq.cmri58.top	DUNN	Level3_VPN	information	pass	HTTPS
02/15/19 04:32:40 PM	Chicago, USA	ABCD76145	LEVEL3-DEFAULT-AC	Web.Client	medium	HTTPS.BROWSER	shadowraze.pw	HARVEY	Level3_VPN	information	pass	HTTPS
02/15/19 04:32:40 PM	Chicago, USA	ABCD76145	LEVEL3-DEFAULT-AC	General.Interest	elevated	Google.Services	doratopelase.pw	WELCH	Level3_VPN	information	pass	HTTPS
02/15/19 04:32:40 PM	Chicago, USA	ABCD76145	LEVEL3-DEFAULT-AC	Web.Client	medium	HTTP.BROWSER	debservers.pw	WELCH	Level3_VPN	information	pass	HTTP
02/15/19 04:32:40 PM	Chicago, USA	ABCD76145	LEVEL3-DEFAULT-AC	Collaboration	elevated	Microsoft.Portal	dileconme.hotmail.ru	HARRIS	Level3_VPN	information	pass	HTTP
02/15/19 04:32:40 PM	Chicago, USA	ABCD76145	LEVEL3-DEFAULT-AC	Update	elevated	MS.Windows.Update	googlonetkavanis4.pw	MARTIN	Level3_VPN	information	pass	HTTPS

Application control report data table field definitions

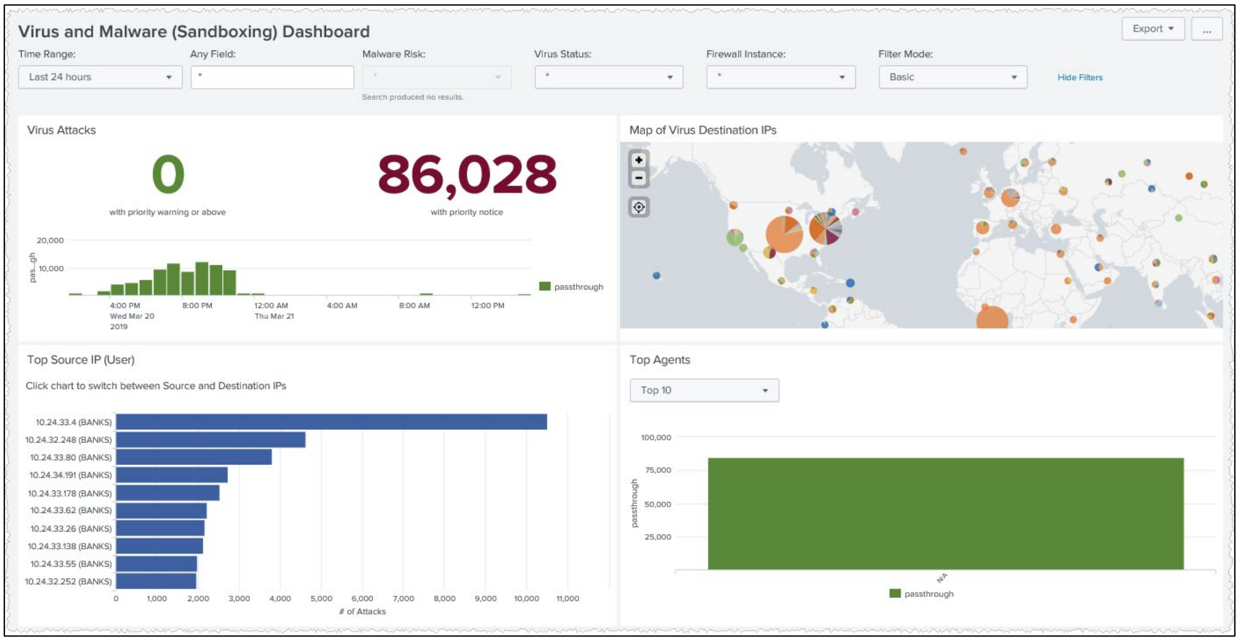
Attribute	Description
Time	Date/Time when log data was recorded
Gateway/Device	Adaptive Network Security Gateway location of Firewall Device
Firewall Instance	Virtual firewall identifier
App. List	Application Control Profile name
App. Category	Application Category
App. Risk	Application Risk Level (low, medium, elevated, high, critical)
Application	Application name
Host	The host name of a URL
User	Username (Active Directory Integration)
Group	Group name (Active Directory Integration)
Priority	Estimated Severity of the event that caused the log message (See Appendix A – Priority Levels Table.)
Action	Security action performed, including pass, block, reject, reset, monitor
Service	The name of the application-layer protocol used by the traffic (http or https)
Destination / Source IP	IP address of traffic’s origin or destination
Destination / Source Port	Port number of traffic’s origin or destination
Destination / Source Location	City and country of source/destination IP (when available)
Message	Log Message
URL	URL address

Virus and Malware (sandboxing)

The Virus and Malware (Sandboxing) feature displays potential infections based on signatures and actions taken: analytics (sent to the sandbox for analysis), monitored, passthrough, blocked. Summaries of Top IP address, Agents, URLs, Files, Targeted Hosts, Malware are displayed. Anti-Virus blocks unwanted files from entering the customer's network via HTTP, FTP, IMAP, POP3, SMTP, or NNTP protocols. Files can be blocked based on both file attachment type or filename suffix, as well as for matching known virus signature patterns. This service operates in conjunction with the Anti-malware feature. Anti-Malware Sandboxing scans and blocks malicious code found in the network traffic. Sandboxing places unknown anomalous payloads in a protected environment for execution. If the payload appears to be malicious, a signature is created to detect and mitigate future threats

Virus and Malware (sandboxing) dashboard

The Virus and Malware dashboard is available under the Anti-Virus and Malware (sandboxing) menu item of the Adaptive Network Security Reports application, and presents logged events for managing files attempting to enter the customers network, including known viruses as well as new, yet to be classified threats.



Virus and Malware (Sandboxing) Dashboard

Time Range: Last 24 hours

Any Field: *

Malware Risk: *

Search produced no results.

Virus Status: *

Firewall Instance: *

Filter Mode: Basic

Virus Attacks

0 with priority warning or above

86,028 with priority notice

Figure 17: Virus and Malware (sandboxing) dashboard

The dashboard includes the following panels showing virus and malware event data:

- An indicator listing the number of virus attacks with a priority of warning or higher.
- A time chart showing virus attacks by status over the selected time range.
- A bar chart of all virus attacks by priority.
- A map of the blocked Source IPs for virus files.
- A bar chart of the top 10 virus files, customizable to exclude to most frequent one.
- A table and time chart of the scanning activities with identified risk (clean, suspicious malicious) and – if applicable – the execution VM.
- A bar chart of the top infected hosts (from which malware originated) with the option to change to a table view.
- A top 10 bar chart of the targeted hosts.
- A bar chart of the top 10 malware files.

Filters and customization

The Virus and Malware dashboard offers a Basic filter set with the option to expand via the **Filter Type** drop down.

The Top Files panel allows excluding the virus file with the most requests via the drop down above, resulting in less compression for other files. Clicking on the bar chart changes to a table presentation with additional fields for user, status, and priority.

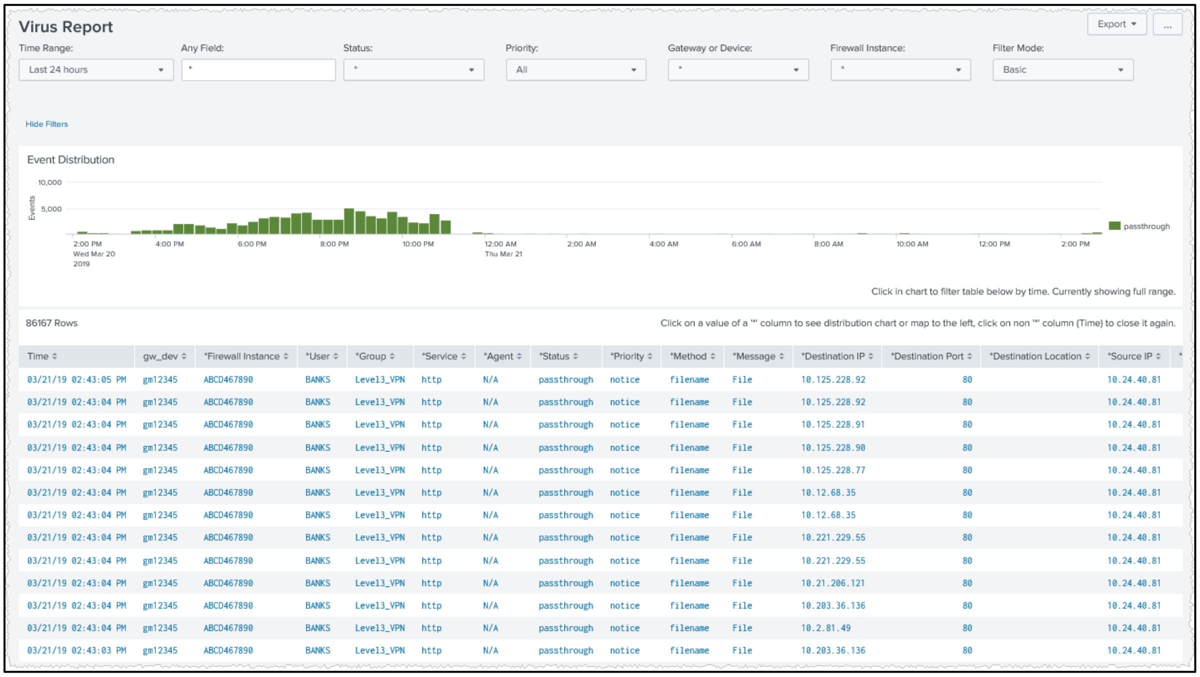
Detailed views

Clicking in a panel opens either the Virus or Malware report page, preserving selected values for the **Any Field, Status** (for virus panels), **Malware Risk (for malware panels)**, **Firewall Instance**, and **BAN** filter controls.

- Clicking on the *Virus Attacks* number or the bar chart for *Virus Attacks by priority* sets the priority filter on the report page to reflect the lower threshold instead of an exact match.

Virus report

The Virus report displays the logged events via a summarized graphical event distribution by time and listing with several summarized display options.



Time Range: Last 24 hours
Any Field: *
Status: *
Priority: All
Gateway or Device: *
Firewall Instance: *
Filter Mode: Basic

Click in chart to filter table below by time. Currently showing full range.

86167 Rows

Click on a value of a "*" column to see distribution chart or map to the left, click on non "*" column (Time) to close it again.

Time	gw_dev	*Firewall Instance	*User	*Group	*Service	*Agent	*Status	*Priority	*Method	*Message	*Destination IP	*Destination Port	*Destination Location	*Source IP	*
03/21/19 02:43:05 PM	gm12345	ABCD467890	BANKS	Level3_VPN	http	N/A	passthrough	notice	filename	File	10.125.228.92	80		10.24.40.81	
03/21/19 02:43:04 PM	gm12345	ABCD467890	BANKS	Level3_VPN	http	N/A	passthrough	notice	filename	File	10.125.228.92	80		10.24.40.81	
03/21/19 02:43:04 PM	gm12345	ABCD467890	BANKS	Level3_VPN	http	N/A	passthrough	notice	filename	File	10.125.228.91	80		10.24.40.81	
03/21/19 02:43:04 PM	gm12345	ABCD467890	BANKS	Level3_VPN	http	N/A	passthrough	notice	filename	File	10.125.228.90	80		10.24.40.81	
03/21/19 02:43:04 PM	gm12345	ABCD467890	BANKS	Level3_VPN	http	N/A	passthrough	notice	filename	File	10.125.228.77	80		10.24.40.81	
03/21/19 02:43:04 PM	gm12345	ABCD467890	BANKS	Level3_VPN	http	N/A	passthrough	notice	filename	File	10.12.68.35	80		10.24.40.81	
03/21/19 02:43:04 PM	gm12345	ABCD467890	BANKS	Level3_VPN	http	N/A	passthrough	notice	filename	File	10.12.68.35	80		10.24.40.81	
03/21/19 02:43:04 PM	gm12345	ABCD467890	BANKS	Level3_VPN	http	N/A	passthrough	notice	filename	File	10.221.229.55	80		10.24.40.81	
03/21/19 02:43:04 PM	gm12345	ABCD467890	BANKS	Level3_VPN	http	N/A	passthrough	notice	filename	File	10.221.229.55	80		10.24.40.81	
03/21/19 02:43:04 PM	gm12345	ABCD467890	BANKS	Level3_VPN	http	N/A	passthrough	notice	filename	File	10.21.206.121	80		10.24.40.81	
03/21/19 02:43:04 PM	gm12345	ABCD467890	BANKS	Level3_VPN	http	N/A	passthrough	notice	filename	File	10.203.36.136	80		10.24.40.81	
03/21/19 02:43:04 PM	gm12345	ABCD467890	BANKS	Level3_VPN	http	N/A	passthrough	notice	filename	File	10.2.81.49	80		10.24.40.81	
03/21/19 02:43:03 PM	gm12345	ABCD467890	BANKS	Level3_VPN	http	N/A	passthrough	notice	filename	File	10.203.36.136	80		10.24.40.81	

Virus report data table field definitions

Attribute	Description
Time	Date/Time when log data was recorded
Gateway/device	Adaptive Network Security Gateway location of Firewall Device
Firewall Instance	Virtual firewall identifier
User	Username (Active Directory Integration)
Group	Group name (Active Directory Integration)
Service	Proxy service that scanned the traffic
Agent	User agent
Status	Status based on security action performed, including analytics, blocked, monitored, pass through
Priority	Estimated Severity of the event that caused the log message (See Appendix A – Priority Levels Table.)
Method	Sub type of the log message
Message	Log Message
Destination / Source IP	IP address of traffic's origin or destination
Destination / Source Port	Port number of traffic's origin or destination
Destination / Source Location	City and country of source/destination IP (when available)

Services not available everywhere. Business customers only. Lumen may change, cancel, or substitute products and services, or vary them by service area at its sole discretion without notice.

URL	URL address
File	File type

Appendix A: priority levels table

The following table describes the priority, which is the estimated severity that caused a log event.

Name	Description
Alert	Immediate action required.
Critical	Functionality is affected.
Emergency	The system is unusable or not responding.
Error	An error exists and functionality could be affected
Information	General information about system operations.
Notification	Information about normal events
Warning	Functionality could be affected.