Lumen[®] Managed Security Services

User guide | February 2021



Table of contents

About the Adaptive Network Security application	4
Dashboards & reports by service feature	4
Filters and customization	5
Detailed views	7
Access to the reporting application	7
Adaptive Network Security dashboard	8
Filters and customization	9
Detailed views	9
Traffic	10
Traffic dashboard	10
Filters and customization	
Detailed views	11
Traffic report	12
Filters and customization	12
Traffic report data table field definitions	14
Webfilter	15
Webfilter dashboard	15
Filters and customization	15
Detailed views	16
Webfilter report	16
Webfilter report data table field definitions	18
Access	19
Site dashboard	19
Filters and customization	20
Detailed views	20
Mobility dashboard	20
Filters and customization	21
Detailed views	21
Access report	21
Filters and customization	
	23
	24
IDS/IPS dashboard	24
Filters and customization	25

Detailed views	25
IDS/IPS report	25
IDS/IPS report table data field definitions	26
DLP	27
DLP dashboard	27
Filters and customization	27
Detailed views	28
DLP report	28
DLP report data table field definitions	29
Application Control	30
Application Control dashboard	30
Filters and customization	30
Detailed views	31
Application Control report	31
Application control report data table field definitions	32
Virus and Malware (sandboxing)	33
Virus and Malware (sandboxing) dashboard	33
Filters and customization	34
Detailed views	34
Virus report	35
Virus report data table field definitions	35
Appendix A: priority levels table	37

About the Adaptive Network Security application

CenturyLink 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.

splunk>enterprise	App: ANS Demo 🔻			ans_demo	 Messages 	Settings 🔻	Activity -	Help 🔻	Find Q.
CenturyLink ▼ Traffic	▼ Webfilter▼	Access ▼ IDS	/IPS▼ DLP▼	Application Control	Virus and Mal	ware (Sandboxi	ng)▼ E	Development 🕶	ANS Demo
splunk>enterprise Apps ANS Reports AMS Reports Adaptive Timest Intelligence DDOS Proxy Managed Firewall &	₩ UTM								

Dashboards & reports by service feature

The CenturyLink 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 CenturyLink 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).



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 CenturyLink Managed Security Services. To access the feature, open the **Reports > Security Solutions Analytics** page, then click the **CenturyLink 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).

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).
- 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 hours 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.



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:

*	Map IPs	•
~	Map IPs	<u></u>
	Chart IPs	
	List IPs	

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										Export 🔻	
Time Range:	Any Field:		Status:		P	riority:		Gateway	or Device:		
Last 15 minutes	•		*		•	All		• *	-		
Firewall Instance:	Filter Mode:	•	Hide Filte	rs							
Event Distribution											
by # of Events	•										
200											
100											
2:05 PM 2:06 PM Thu Mar 21	2:07 PM 2:08	B PM 2:09 PM	2:10 PM	2:11 PM	2:12 PM	2:13 PM	2:14 PM	2:15 PM 2	2:16 PM 2:17 PM	2:18 PM 2:19 PM	
2:05 PM 2:06 PM Thu Mar 21 2019	2:07 PM 2:04	8 PM 2:09 PM	2:10 PM	2:11 PM	2:12 PM	2:13 PM	2:14 PM	2:15 PM 2	2:16 PM 2:17 PM	2:18 PM 2:19 PM	
2:05 PM 2:06 PM Thu Mar 21 2019	2:07 PM 2:00	8 PM 2:09 PM	2:10 PM	2:11 PM	2:12 PM	2:13 PM	2:14 PM	2:15 PM 2	filter table below by time.	2:18 PM 2:19 PM	range.
2:05 PM Thu Mer 21 2019	2:07 PM 2:00	2:09 PM	2:10 PM	2:11 PM	2:12 PM	2:13 PM	2:14 PM	2:15 PM 2	filter table below by time.	2:18 PM 2:19 PM	range.
2.05 PM Thu Mer 21 2019	2:07 PM 2:01	8 PM 2:09 PM	2:10 PM	2:11 PM	2:12 PM	2:13 PM	2:14 PM	2:15 PM 2	:16 PM 2:17 PM	2:18 PM 2:19 PM	range.
2:05 PM Thu Mar 21 2:019 All Requests	2:07 PM 2:01	8 FM 2:09 PM	2:10 PM	2:11 PM	2:12 PM	2:13 PM	2:14 PM	2:15 PM 2	filter table below by time.	2:18 PM 2:19 PM Currently showing full	range.
2:05 PM Tru Mar 21 2019 All Requests 2606 Rows	2:07 PM 2:01	8 FM 2:09 PM	2:10 PM	2:11 PM	2:12 PM accept ac	2:13 PM deny	2:14 PM	2:15 PM 2 Click in chart to stribution chart or	filter table below by time.	2:18 PM 2:19 PM Currently showing full n ** column to close it	range.
2:05 PM Tru Mar 21 2:019 2:06 PM 2:06	2.07 PM 2.01	*Firewall Instance \$	2:10 PM *User \$	2:11 PM *Group \$	2:12 PM accept Click on a va *Priority \$	2:13 PM deny lue of a ** co *Status \$	2:14 PM	2:15 PM 2 Click in chart to stribution chart or *Application \$	FIG PM 2:17 PM	2:18 PM 2:19 PM Currently showing full n *** column to close it *Destination IP \$	range. t again.
2:05 PM Thu Mar 21 2:019 2:05 PM 2:06 PM 2:07	2.07 PM 2.01	*Firewall Instance * ABC0467899	2:10 PM *User \$ BANKS	2:11 PM *Group \$ Level3_VPN	2:12 PM accept definition of the second seco	2:13 PM deny lue of a ⁺⁺⁺ Co *Status ¢ deny	2:14 PM	2:15 PM 2 Click in chart to stribution chart or *Application \$ N/A	FIG PM 2:17 PM filter table below by time, t map to the left, click on no *Application Category \$ N/A	2:18 PM 2:19 PM Currently showing full n *** column to close it *Destination IP \$ 10.109.71.76	range. t again. *Dest
2:05 PM Thu Mar 21 2:019 2:05 PM 2:06 PM 2:07	2:07 PM 2:01	*Firewall Instance * ABCD467899 ABCD467899	2:10 PM *User ¢ BANKS BANKS	2:11 PM *Group \$ Level3_VPN Level3_VPN	2.12 PM accept Click on a va *Priority \$ warning warning	2:13 PM deny lue of a *** co *Status \$ deny accept	2:14 PM 2:14 PM Uumn to see dl: *Service \$ 389/udp 123/udp	2:15 PM 2 Click in chart to stribution chart or *Application \$ N/A N/A	filter table below by time, f map to the left, click on no *Application Category \$ N/A N/A	2:18 PM 2:19 PM Currently showing full n *** column to close it *Destination IP \$ 10.109.71.76 10.18.29.184	range. t again. *Dest
2:05 PM Thu Mar 21 2:019 2:019 2:006 PM 2:006 PM 2:006 PM 2:006 PM 2:006 PM 2:007 PM	2:07 PM 2:01	*Firewall Instance * ABCD467899 ABCD467899 ABCD467899	2:10 PM *User * BANKS BANKS BANKS	2:11 PM *Group \$ Level3_VPN Level3_VPN Level3_VPN	2.12 PM accept Click on a va "Priority 2 warning warning warning	2:13 PM deny lue of a *** co *Status \$ deny accept accept	2:14 PM 2:14 PM Uumn to see dl: "Service \$ 389/udp 123/udp 389/udp	2:15 PM 2 Click in chart to stribution chart or *Application \$ N/A N/A N/A	filter table below by time. map to the left, click on no *Application Category * N/A N/A N/A	2:18 PM 2:19 PM Currently showing full "Destination IP \$ 10.109.71.76 10.18.29.184 10.0.195.236	range. t again. *Dest
2:05 PM Thu Mar 21 2:019 2:019 2:019 2:006 Rows 2:006 Rows 7 1/me ‡ 03/21/19 02:17:23 PM 03/21/19 02:17:23 PM 03/21/19 02:17:23 PM	2:07 PM 2:01 * * * Gateway/Device * gm12345 gm12345 gm12345	*Firewall Instance * ABCD467890 ABCD467890 ABCD467890 ABCD467890 ABCD467890	2:10 PM ¹ User ² BANKS BANKS BANKS BANKS	2:11 PM *Group \$ Level3_VPN Level3_VPN Level3_VPN Level3_VPN	2.12 PM accept Click on a va "Priority 2 warning warning warning warning	2:13 PM deny lue of a *** co *Status * deny accept accept deny	2:4 PM	2:15 PM 2 Click in chart to stribution chart or *Application \$ N/A N/A N/A	filter table below by time. map to the left, click on no *Application Category * N/A N/A N/A N/A	2:18 PM 2:19 PM Currently showing full "Destination IP \$ 10.109.71.76 10.18.29.184 10.0.195.236 10.5.41.209	range. t again. *Dest
2:05 PM Thu Mar 21 2:019 2:019 2:019 2:006 Rows 2:006 Rows 2:006 Rows 2:006 Rows 2:0119 02:17:23 PM 03/21/19 02:17:23 PM 03/21/19 02:17:23 PM 03/21/19 02:17:23 PM	2:07 PM 2:01 * * * Gateway/Device * gm12345 gm12345 gm12345 gm12345	*Firewall Instance * ABCD467890 ABCD467890 ABCD467890 ABCD467890 ABCD467890 ABCD467890	2:10 PM *User * BANKS BANKS BANKS BANKS BANKS	2:11 PM *Group \$ Level3_VPN Level3_VPN Level3_VPN Level3_VPN Level3_VPN	2.12 PM accept accept Click on a va "Priority ‡ warning warning warning warning	2:13 PM deny 'Status ¢ deny accept accept deny deny	2:4 PM	2:15 PM 2 Click in chart to stribution chart or *Application \$ N/A N/A N/A N/A N/A	filter table below by time. map to the left, click on no *Application Category = N/A N/A N/A N/A N/A	2:18 PM 2:19 PM Currently showing full *Destination IP \$ 10.109.71.76 10.18.29.184 10.0.195.236 10.5.41.209 10.1.1.6	range. t again. *Dest

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.

All events	© .
All events	
Summarize by IPs and P	Ports
Summarize by IPs	
Summarize by IPs with (Drg *De
5/29/16 04:12:13 AM	1 gm

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.



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 inpage 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.

ime Range:													Exhou .
0.23350.2007.200	Any Field:	Ci	tegory:		Status:			Priority:		User:		Gateway or De	vice:
Last 15 minutes	•		•	7	All Treff	fic .		All			*	1	*
irewall Instance:	Filter Mode:												
•	• Basic	•											
tide Filters													
Event Distribution													
10.000													
5.000							_		_				
													blocked
All Requests	•									Click in che	rt to filter table t	below by time. Curre	ntly showing full rang
All Requests	*							Click on a v	value of a ^{***} column to se	Click in che	it to filter table t	below by time. Curre Ieft, click on non ''' c	ntly showing full range olumin to close it agai
All Requests D Rows	* "Gateway/Device 5	*Firewall Instance #	*User ‡	"Group =	*Priority ©	*Action ©	"Status ©	Click on a v	value of a ^{***} column to se	Click in che e distribution cha "Service #	nt to filter table t nt or map to the l "Direction =	below by time. Curre left, click on non ** c "Destination IP =	ntly showing full range olumn to close it again "Destination Port ©
All Requests Rows lime = \$2/15/19_04:42:44_PM	* "Gateway/Device 5 Charlotte, USA	*Firewall Instance : A0CD51538	*User \$	*Group = Level3_VPN	*Priority © warning	*Action © 1 blocked I	*Status © blocked	Click on a v "Filter = webfilter	value of a "" column to ser "Casegory = Spart LRLs	Click in che e distribution che "Service 5 HTTPS	rt to filter table b rt or map to the l "Direction = outgoing	teft, click on non ^w c *Destination IP = 10.53.67.177	ntly showing full range olumin to close it again "Destination Port 4 443
All Requests Rows Time 0 12/15/19 04:42:44 PH 12/15/19 04:42:44 PH	* "Gateway/Device 5 Charlotte, USA Charlotte, USA	*Firewall Instance # ADCD51538 ABCD51538	"Oper ©	"Group = Level3_VPN Level3_VPN	*Priority 3 warning warning	*Action © 4 blocked 4 blocked 4	Status = blocked blocked	Click on a v "Fitter : webfilter webfilter	*Category 5 Spar LRLs Spar LRLs	Click in che e distribution che "Service 5 HTTPS HTTPS	rt to filter table t rt or map to the l "Direction = outgoing outgoing	left, click on non ¹⁴¹ c "Destination IP = 10.53.67.177 10.53.67.177	ntiy showing full rang olumn to close it agai "Destination Port = 443 443
All Requests Rows Ime 0 2/15/19 04:42:44 PM 2/15/19 04:42:42 PM	* "Gateway/Device : Charlotte, USA Charlotte, USA Charlotte, USA	*Firewall Instance 2 ABCD51538 ABCD51538 ABCD51538	*User \$	"Group = Level3_VPN Level3_VPN Level3_VPN	*Priority = warning warning warning	*Action © 1 blocked 1 blocked 1 blocked 4	"Status 0 blocked blocked blocked	Click on a v "Fistor : webfilter webfilter	*Category 2 *Category 2 Spart LRLs Spart LRLs Spart LRLs	Click in che e distribution cha service s HTTPS HTTPS HTTPS	rt to filter table b rt or map to the l "Direction = outgoing outgoing outgoing	teft, click on non ¹¹ c ¹ Destination IP = 10.53.67.177 10.53.67.177	ntly showing full range olumn to close it again "Destination Port = 443 443
All Requests) Rows Prime © \$22/15/19 04:42:44 PM \$22/15/19 04:42:42 PM \$22/15/19 04:42:42 PM \$22/15/19 04:39:34 PM	* "Gateway/Device 5 Charlotte, USA Charlotte, USA Charlotte, USA Washington, D.C., USA	*Firewall Instance 2 ACC651538 ADC051538 ABC051538 ABC051538 ABC015615	"User 2	"Group 2 Level3_VPN Level3_VPN Level3_VPN Level3_VPN Level3_VPN	*Priority 0 warning warning warning warning	*Action = 4 blocked 4 blocked 4 blocked 4	Status © blocked blocked blocked	Click on a v "Fittor : webfilter webfilter webfilter	value of a ^{mil} column to ser *Category s \$part LRLs \$part LRLs \$part LRLs \$part LRLs	Click in che e distribution cha "Service a HTTPS HTTPS HTTPS HTTPS	rt to filter table t tt or map to the l "Direction 2 outgoing outgoing outgoing outgoing	below by time. Curre reft, click on non ** c *Destination IP = 10.53.67.177 10.53.67.177 10.33.3.10	ntly showing full range olumn to close it again "Destination Port 5 443 443 443
All Requests D Rows 22/15/19 04:42:44 PH 02/15/19 04:42:44 PH 02/15/19 04:42:42 PH 02/15/19 04:39:34 PH 02/15/19 04:39:34 PH	* "Gateway/Device 5 Charlotte, USA Charlotte, USA Charlotte, USA Washington, 0.C., USA	*Pirewall Instance E ARC051518 ARC051518 ARC051518 ARC051518 ARC019615 ARC019615	"User : Gutterrez	"Group : Level3_VPN Level3_VPN Level3_VPN Level3_VPN Level3_VPN Level3_VPN	"Priority 2 warning warning warning warning warning	*Action 2 7 blocked 8 blocked 8 blocked 8 blocked 8	"Status © blocked blocked blocked blocked blocked	Click on a v "Feter : webfilter webfilter webfilter webfilter	volue of a "" column to ser "Category 2 Spare LRLs Spare LRLs Spare LRLs Spare LRLs Intermet Radio and T	Click in che e distribution cha *Service 2 HTTPS HTTPS HTTPS HTTPS Y HTTPS	rt to filter table t tt or map to the l "Direction 2 outgoing outgoing outgoing outgoing	below by time. Curre reft, click on non ** c *Destination IP = 10.53.67.177 10.53.67.177 10.30.3.10 10.226.177.55	ntly showing full range olumn to close it again "Destination Port = 443 443 443 443
All Requests D Rows 02/15/19 04:42:44 PH 02/15/19 04:42:42 PH 02/15/19 04:42:42 PH 02/15/19 04:42:42 PH 02/15/19 04:39:34 PH 02/15/15 04:37:43 PH	'Gateway/Device = Charlotte, USA Charlotte, USA Charlotte, USA Charlotte, USA Chicago, USA Chicago, USA	*Pirewall Instance © AdcDs1538 AdcDs1538 AdcD5538 AdcD5538 AdcD558 AdcD558 AdcD558 AdcD55145	"User 5 GUTLERREZ HENDERSON	"Group 5 Level3_VPN Level3_VPN Level3_VPN Level3_VPN Level3_VPN Level3_VPN	"Priority 2 warning warning warning warning warning warning	*Action 5 1 blocked 1 blocked 1 blocked 1 blocked 1 blocked 1 blocked 1	"Status © blocked blocked blocked blocked blocked	Click on a v "Føtor : webfilter webfilter webfilter webfilter	*Category = *Category = \$par LRLs \$par URLS \$par URLS \$par URLS Internet Radio and T Unrated	Click in che e distribution che service a HTTPS HTTPS HTTPS HTTPS HTTPS HTTPS HTTPS	rt to filter table t rt or map to the l "Direction 2 outgoing outgoing outgoing outgoing outgoing outgoing	left, click on non ^{**} c "Destination IP ∈ 10.53.67.177 10.53.67.177 10.33.3.10 10.326.177.55 10.169.214.153	ntly showing full range olumn to close it again "Destination Port © 443 443 443 443 443 443

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

Export • ... Site Dashboard (Beta) Last 24 hour A Map of Sites by Volum Top Sites by Volume in MB Top Sites by Throughput (Mbps -0.242 115 81 196.210.178 (N ٢ Sustained Throughput and active Sites over Time 8 2,000,00 Map of Sites by Errors Tunnel Up/Down Events Top Sites by Tunnel Events Ð 10.54.125 ed ٢

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

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 Dashbo	bard	distant and a second			2-11-01-0					Export *	
Last 24 hours	Any Field.	User or XAuth Oser.	when turner.		*		Al	-	Hoe Filters		
							Search produced	na remailte.			
Authentications	No results found.	Top Client	s by Successful Authento	cations dis fount.		Top C	lients by Fallec	Authentications two iesuits	found.		
Map of Clients by Aut	nentication And States	Top Clent	10547189 10547189 1034818246 101858238 101850344			Top C 10 10138 10.5 10.55 10.552	Fents by Durat 19.32 19.34 19.34 19.37 19.32 19.32 19.32	ion in Hours			
\.	Anaco Dusternala		5.37.198 105434.55 10:03.2		0.242.05.0	10.17 10.178.2 10.249	74219 27.194 162.46 0 1	,000 2,000	8,008 K.0 Hisurs	05 K.550	4,04
Peak Sustained Throu 270:040 2430:395 2430:395 350:054 3130:055 3130:055 310000000000000000000000000000000000	gt put and Clients over Time									2.345,94	100

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.

											Expo	6. T
lime Range:	Access Type	ē	Message:	Action:				Status:		VPN Tu	nnet:	
Last 24 hours	* Site	7		* 4	•	No	Low Level Events	14		•		
irewall instance:	User or XAu	th User:	Result	Priority:		BAN:		Filter M	ode:			
4	4 (B)		All	- All		All		- Bosi		+ Hide Fi	ners	
						Search p	enduced on results					
g 2,500,000		n BRUUNI		Kbps Serv	t. Kbps Received	- Clients				I.s 11	2.364.03	100 g
All Requests	Any Field (No Org or Location):										
All Requests	Any Field (No Org or Location):				Click	on a value of a ''' ci	olumn to see distrib	ution chart or map to	the left, click on r	non *** column to e	:lose it again.
All Requests 0 Rows Time 0	Any Field	No Org or Location):	*Action #	"Message 1	*Status 0	Click o	on a value of a ^{re} ci "XAuth User +	olumn to see distrib "XAuth Group #	ution chart or map to	the left, click on r *Local IP ©	non ** column to r *Local Port #	close it again. *Remote IP
All Requests O Rows Time 9 92/15/19 94:53:10 PM	Any Field	No Org or Location): "Device 0 esg02-fn05_ptx1	*Action * negotiate	"Message % IPsec phase 1 error	*Status # negotiate_error	Click o *Level # error	on a value of a ^{rec} o "XAuth User # N/A	olumn to see distrib "XAuth Group # Level3_VPN	ution chart or map to "VPN Tunnel 9 TUN1_EFGH59264	*Local IP 9 10, 182, 158, 39	non ** column to (*Local Port # 508	Slosé it again. ''Remote IP 19,54,146.
All Requests 0 Rows Time 0 02/15/15 04:53:10 PM 02/15/15 04:53:10 PM	Any Field	No Org or Location): "Device 0 esg02-fw05_phx1 esg02-fw05_phx1	*Action 0 negotiate negotiate	"Messege 9 IPsec phase 1 error progress IPsec phase 2	*Status € negotiate_error success	Click of "Level # error notice	on a value of a ^{see} cr "XAuth User & N/A N/A	Summ to see distrib "XAuth Group # Level3_VPN Level3_VPN	ution chart or map to "VPN Tunnel 8 TUNT_EFGH89264 TUNT_EFGH89264	*Local IP 6 10, 182, 158, 39 10, 182, 158, 39	non ** column to (*Local Port † 500 500	Close it again. *Remote IP 10.54.146. 10.54.146.
All Requests 0 Rows Time 0 02/15/15 04:53:10 PM 02/15/15 04:53:10 PM 02/15/19 04:53:09 PM	Any Field * Firewall Instance * ABCD45354 ABCD45354 ABCD45354	No Org or Location): *Device + esg82-fn05_phx1 esg82-fn05_phx1 esg82-fn05_phx1	"Action 0 negotiate negotiate negotiate	"Message 1 : IPsoc phase 1 error progress IPsec phase 2 : progress IPsec phase 2 :	*Status * negotiate_error success success	Click o "Level # error notice notice	on a value of a ^{re} ci "XAuth User & N/A N/A N/A	*KAuth Group # Level3_VPN Level3_VPN Level3_VPN	ution chart or map to "VPN Tunnel 0 TUR1_EFGH89264 TUN1_EFGH89264 TUN1_EFGH89264	the left, click on r *Local IP 0 10, 182, 158, 39 10, 182, 158, 30 10, 182, 158, 39	non ¹⁴¹ column to r "Local Port # 598 598	10.54,146, 10.54,146, 10.54,146, 10.54,146,
All Requests O Rows Time 0 02/15/19 04:53:10 PH 02/15/19 04:53:00 PH 02/15/19 04:53:06 PH	Any Field (* * * * * * * * * * * * * * * * * * *	No Org or Location): "Device # esg82-fx85_phx1 esg82-fx85_phx1 esg82-fx85_phx1 esg82-fx85_phx1	"Action 0 negotiate negotiate negotiate tunnel-stats	"Message 0 . IPsec plase 1 error progress IPsec plase 2 IPsec tunel statistics	*Status * negotiate_error success success	Click of "Level # error notice notice	on a value of a ^{sec} or "XAuth User & N/A N/A N/A N/A	*XAuth Group # Level3_VPN Level3_VPN Level3_VPN Level3_VPN Level3_VPN	Ution chart or map to "VPN Tunnel ® TUHT_EFG485264 TUHT_EFG485264 TUHT_EFG485264 TUHT_EFG41357	the left, click on r *Local IP 0 10, 152, 158, 39 10, 152, 158, 39 10, 152, 150, 39 10, 152, 150, 39	non ^{III} column to r "Local Port # 500 500 500 500	Close it again. "Remote IP 10.54.146. 10.54.146. 10.54.146. 10.63.34.1
All Requests. O Rows Time 0 02/15/19 04:53:10 PM 02/15/19 04:53:00 PM 02/15/19 04:53:06 PM 02/15/19 04:53:06 PM 02/15/19 04:53:08 PM	Any Field • • • • • • • • • • • • • • • • • • •	No Org or Location): "Device # esg82=fn45_phx1 esg82=fn45_phx1 esg82=fn45_phx1 esg81=fn45_phx1 esg81=fn45_phx1	*Action 8 megotiate megotiate megotiate tunnel-stats megotiate	"Message 8 IPsec phase 1 error progress IPsec phase 2 IPsec tunnel statistics progress IPsec phase 1	"Status # negotiate_error success success	Click c "Level # error notice notice notice	nn a value of a ^{ser} cr "XAuth User & N/A N/A N/A N/A N/A	"XAuth Group @ Level3_VPN Level3_VPN Level3_VPN Level3_VPN Level3_VPN Level3_VPN	TVPN Tunnel ® TVPN Tunnel ® TUHT_EFG485264 TUHT_EFG485264 TUHT_EFG485264 TUHT_EFG411357 TUHT_EFG411357	the left, click on r *Local IP 6 10.182.158.39 10.182.158.39 10.182.158.39 10.182.159.39 10.182.130.21 10.182.149.45	non ** column to / *Local Port # 588 589 588 588	"Remote IP 10,54,146, 10,54,146, 10,54,146, 10,54,146, 10,63,34,1 10,188,211
All Requests 0 Rows Time 0 02/15/19 04:53:10 PM 02/15/19 04:53:00 PM 02/15/19 04:53:08 PM 02/15/19 04:53:08 PM 02/15/19 04:53:08 PM	Any Field *Firewall Instance * Accu43384 Accu43384 Accu43384 Accu43384 Accu43384 Accu54538	*Device * *Device * esg82-fx45_phx1 esg82-fx45_phx1 esg82-fx45_phx1 esg82-fx45_phx1 esg81-fx45_b212 esg81-fx45_c122	"Action 8	*Message 1 IPsec phase 1 error progress IPsec phase 2 progress IPsec phase 1 IPsec tunnel statistics progress IPsec phase 1 delete IPsec phase 1 SA	"Status 9 negotiate_error success success success	Click of "Level 0 error notice notice notice notice	nn a value of a ** cr *XAuth User & N/A N/A N/A N/A N/A N/A	VKAuth Group # Level3_VPN Level3_VPN Level3_VPN Level3_VPN Level3_VPN Level3_VPN	VEN Tunnel * TVRN Tunnel * TURT_EFG485264 TURT_EFG485264 TURT_EFG485264 TURT_EFG485264 TURT_EFG485263 TURT_EFG485263 TURT_EFG441477	the left, click on r "Local IP 6 10, 182, 158, 39 10, 182, 158, 39 10, 182, 158, 39 10, 182, 158, 39 10, 182, 149, 45 10, 182, 135, 59	non ** column to / *Local Port # 588 588 588 588 588 588	llose it ogoin. *Remote IP 10, 54, 146. 10, 54, 146. 10, 54, 146. 10, 63, 34, 1 10, 180, 211 10, 72, 156.
All Requests. O Rows Time 0 02/15/19 04:53:10 PH 02/15/19 04:53:00 PH 02/15/19 04:53:00 PH 02/15/19 04:53:00 PH 02/15/19 04:53:00 PH	Any Field *Firewall Instance 6 ACD4334 ACD45384 ACD45384 ACD45384 ACD51535 ACD51535 ACC05897	*Device 9 *Device 9 esg82-fw85_phx1 esg82-fw85_phx1 esg82-fw85_phx1 esg81-fw85_eb12 esg81-fw85_eb12 esg81-fw85_eb12 esg81-fw85_eb12	"Action 8 mepotiate mepotiate negotiate tunnel-stats mepotiate delete_pheet_se megotiate	"Message 1 IPsec phase 1 error progress IPsec phase 2 progress IPsec phase 2 IPsec tunnel statistics progress IPsec phase 1 SA progress IPsec phase 1 SA	"Status 9 negotiate.error success success success	Click of "Level # notice notice notice notice notice	nn o value of a ** cr *XAuth User 0 8/A 8/A 8/A 8/A 8/A 8/A 8/A 8/A	VKAuth Group # Level3_VPN Level3_VPN Level3_VPN Level3_VPN Level3_VPN Level3_VPN Level3_VPN Level3_VPN	TVPN Tunnel 3 TVRN_EPO455264 TUR1_EPO455264 TUR1_EPO455264 TUR1_EPO45535 TUR1_EPO475353 TUR1_EPO41477 TUR1_EPO44477	the left, click on r "Local IP 6 10, 182, 158, 39 10, 182, 134, 39 10, 182, 145, 59 10, 182, 214, 23	non *** column to r *Local Port # 598 598 598 598 598 598 598 598 598	Llosé It again. "Remote IP 10, 54, 146. 10, 54, 146. 10, 54, 146. 10, 63, 34, 1 10, 180, 211 10, 72, 156. 10, 95, 147.
All Requests O Rows Time 0 02/15/19 04:53:10 PH 02/15/19 04:53:00 PH 02/15/19 04:53:00 PH 02/15/19 04:53:08 PH 02/15/19 04:53:07 PH 02/15/19 04:53:07 PH	Any Field * Frewall Instance * AcCL4334 AcCL4334 AcCL4334 AcCL4334 AcCL4334 AcCL33493 AcCL33493 AcCL34997 AcCL34997 AcCL34997	*Device # *222-fx85_phx1 esg82-fx85_phx1 esg82-fx85_phx1 esg81-fx85_phx1 esg81-fx85_phx1 esg81-fx85_phx1 esg81-fx85_phx1 esg81-fx85_phx1 esg81-fx85_phx1 esg81-fx85_phx1	*Action 8 negotiate negotiate negotiate tunnel-stats negotiate delete_jame_jame negotiate negotiate	*Message 1 IPsec phase 1 error progress IPsec phase 2 progress IPsec phase 2 IPsec tunnel statistics progress IPsec phase 1 progress IPsec phase 1 progress IPsec phase 1 progress IPsec phase 1	"Status 9 negotiate.error success success success success success	Click of "Level # error notice notice notice notice notice	N/A N/A N/A N/A N/A N/A N/A N/A N/A N/A	*XAuth Group # *XAuth Group # Level3_VPN Level3_VPN Level3_VPN Level3_VPN Level3_VPN Level3_VPN Level3_VPN Level3_VPN Level3_VPN	TVPN Tunnel 3 TVPN Tunnel 3 TUHT_EFOR85264 TUHT_EFOR85264 TUHT_EFOR85264 TUHT_EFOR85264 TUHT_EFOR8533 TUHT_EFOR85413 TUHT_EFOR86416	the left, click on r *Local IP 9 10, 152, 155, 39 10, 152, 155, 55 10, 152, 114, 25 10, 152, 214, 23 10, 152, 214, 23	*Local Port # 500 500 500 500 500 500 500 500 500	Llose it egain. "Remote IP 10, 54, 146, 10, 54, 146, 10, 54, 146, 10, 63, 34, 11 10, 180, 211 10, 180, 211 10, 72, 158, 10, 95, 147, 1 10, 84, 123, 2

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.



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.



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	Any Field:		Action		Туре:		Priority:	Firewall	Instance: Fit	er Mode:	Export •
Last 24 hours					-	.T	All •		•] [1	Basic	•
Hide Filters											
Total Incidents 15,918 Bicked	(D	Requests by Action			Incidents by T	ype and Action		Incidents by Service		
Top Senders			5:00 PM Thu Feb 14 2019	too AM Pri Reb 15	9:00 AM	Top Recipient	s cred	t card (plock)	0 2,500 8,000	7,500 10,000 12 # of incidents	500 18,000
List Senders 🔹						List Recipient	s •				
ip e	User #	From #	Service #		# of incidents *	IP ¢	Host #	To *	Location #	Service #	# of incidents
10.52.145.106			HTTP		15455	10.69.6.201	xhrnfffaixawpuob.pw		Fort Huachuca, United Stat	es HTTP	12771
10.52.5.171			HTTP		275	10.214.245.55	xhrnfffaixawpuob.pw		Curitiba, Brazil	HTTP	295
10.20.10.15			нттр		16	18.48.32.75	mz?oyb3v32vshcvk.torlongor.1	11	Castelli, Argentina	HTTP	1
10.52.32.115			HTTP		15	10.79.197.223	u0003321.cp.regruhosting.ru		United States	HTTP	1
10.52.5.120			NTTP		8	10.48.32.67	mz?oyb3v32vshcvk.torlongor.l	11	Monterrey, Mexico	HTTP	3
10.52.32.105			HITP		8	10.63.245.67	mz7oyb3v32vshcvk.torlongor.1	11	Presidente Medici, Brazil	HTTP	3
10.52.32.111			HTTP		8	10.48.32.59	mz7oyb3v32vshcvk.torlongor.l	11	Port Louis, Mauritius	HTTP	

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.

DLP Report												Exp	···· • troc
Time Range:	Any Field:		Action:		Тур	101		Gatewa	y or Device:	Firewall Instan	be: Filte	r Mode:	
Last 24 hours	× 1		1		×. 12		. •	275		이 말	• 8	esiq	
Hide Filters													
Event Distribution													
													1
E 2,000													- 3
	and the second second	-											block
6.00 PM Thu Feb 1	8:00 PM	10:00 PM	12:00 AM Fit Feb 15	2.00	AM	4:00 AM	6:00 A	м	8:00 AM	0.00 AM 12.0	00 PM 2.00 PM	4:00 PM	
2019													
										Click in cl	sart to filter table below by	time. Currently sho	wing full range.
AB available													
AR EVENIS	•												5
15918 Rows								Click or	n a value of a '" colum	n to see distribution ch	ert or map to the left, click	on non ** column to	o close it again.
Time t	*Gateway/Device *	*Firewall Instance *	*User ©	"Group 0	*Priority ©	*Action ©	*Service 0	*Severity *	*Destination IP *	*Destination Port +	*Destination Location \$	*Source IP t	*Source Port t
02/15/19 04:39:38 PM	Chicago, USA	ABC076145	HENDERSON	Level3_VPN	warning	block	нтте	medium	10.63.71.203	50		18.95.0.45	6111:
02/14/19 08:39:06 PM	Chicago, USA	ABCD76145	HENDERSON	Level3_VPN	warning	block	HTTP	medium	10.21.81.240	88		10.55.0.45	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	57996
02/14/19 07:57:30 PM	Los Angeles, USA	ABC089217		Level3_VPN	warning	block	нттр	nedium	10.63.74.42	80		10.20.100.133	5121/
02/14/19 07:57:22 PH	Los Angeles, USA	ABCD89217		Level3_VPN	warning	block	HTTP	medium	10.22.150.241	80		10.20.100.133	51281
02/14/19 07:42:34 PM	Los Angeles, USA	ABC089217		Level3_VPN	warning	block	HTTP	medium	10.27.140.227	80		10.20.109.139	4986
02/15/19 02:38:49 PM	esg01-fw05_dal1	ABCD38907		Level3_VPN	warning	block	HTTP	medium	10,249,229,254	88		10.52.86.111	59401
02/14/19 08:03:59 PM	esg01-fw05_dal1	A0CD38307		Level3_VPN	warning	block	нттр	medium	10.63.245.67	50		10.52.86.151	56451

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 Con	trol Dashb	oard	20220	275572	10.00				Export •
Time Range:	Sampling	F.)	Any Field:	Application	Action		Firewall	Instance: Prior	ity:
Last 24 hours	• 1:10	•	1		•		· ·	• AJ	•
Filter Mode:									
Basic	• Hide Fit	80							
Total Requests			Requests by	Action			Top 5 Applicati	lons	
200	0	0	80,000				HTTPLEROWSER		
3.65	<i>J</i> U	0					Merhank. CHile 365		
Requests droop	ed	Requests reset		III Baa		block pass	Microsoft, Jonationa		
			6:00 Thu 8	PM 12.00 AM Feb 14 Fri Feb 15	6.00 AM 12.00 PM		Googie Services		
							0	500,000 1,000,0 # of Reg	00 1,500,000 2,000,000 uests
Top Blocked Application	ons by IP and Ho	st			Top Applications by	IP and Host			
Ust Application IPs	•				List Applications IPs				
Application © User ©	IP t	Host 0		Location #	Application #	User ‡	IP ¢	Host #	Location #
Netflix	10.38.109.135	g4dhhg53jsdjnnkjwjr1	fyiouh3o4u4th.vinerteen.com	Gwangju, Republic of K	Microsoft.SharePoint		10.107.136.5	panel.vargakragard.se	
Netflix	10.224.92.128	rzss2zfue73dfvmj.on	linerpgame.ch	Washington, United Sta	HTTPS.BROWSER		19.229.210.181	axpoium.echange.su	Dryden, United States
Notflix	10.38.109.206	danislenefc.info		Rex, United States	Skype.Portals		10.107.3.128	hui-ain-apparel.tk	Ithaca, United States
Netflix	10.32.83.161	bbwscimanuk.pdsda.nr	et -	Antalya, Turkey	Skype.For.Business		18,112,65,175	fapet.ipb.ac.id	Drammen, Norway
Netflix	10.7.159.18	rzss2zfue73dfvmj.oni	Linerpgame.ch		Citrix.Receiver		10.29,105.232	pmenboeahyrpvoma, 5b1s82, top	Lewisburg, United States
Netflix	10.48.204.31	bbwsclmanuk.pdsda.ne	et		HTTP. BROWSER		18.69.6.201	xhrnfffaixawpuob.pw	Fort Huachuca, United St.
8-101-				Balland Blackas	MP-ML states lightle			an index to be and	Delard Paster

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.

	пиогкероп										Export	· …
TimeRange:	Any Field:		Application	Action	к.	Gatewa	y or Device: Fire	wall Instance:		Priority:		
Last 60 minutes			P.				•			All		
iter Mode:												
Basic	Hide Filters											
Event Distribution												
10,000												
ta						و و و و م						
												block pass
4:05 PM	4:10 PM	4.15 PM 4:20	PM 4:25 PM	4:30 PM	4:35 Ph	4.40 PM	445 PM 45	O PM	4.55 PM	5.00 PM		
2019												
								Click in shart	to fitat table bal	Incumultime Com	in with a science day.	All months
								Click in chart	to filter table be	low by time. Cur	rently showin	g full range.
All events								Click in chart	to filter table be	low by time. Cur	rently showin	g full range.
All events	•							Click in chart	to filter table be	low by time. Curr	rently showin	g full range.
All events	*							Click in chart	to filter table be	low by time. Cur	rently showin	g full range.
All events O Rows	×					Click o	n a value of a ^{set} column to see dis	Click in chart tribution chart	to filter table bei or map to the lef	iow by time. Cur ft, click on non **	column to cir	g full range. ose it again.
All events O Rows Time #	• "Gateway/Device =	*Firewall Instance #	*App List =	*App Category #	*App Risk =	Click o	n a value of a th column to see dis 'Host =	Click in chart tribution chart	to filter table be or map to the lef "Group \$	fow by time. Cur ft, click on non ** *Priority 3	column to cli *Action ©	g full range, ose it again. "Service =
All events 0 Rows Time # 02/15/19 04:32:40 PH	* "Gateway/Device = Chicago, USA	*Firewall Instance # ADCD76145	*App List = LEVEL3-DEFAULT-AC	*App Category = Web.Client	*App Risk = medium	Click o "Application = HTTPS. DROWSER	n a value of a ^{su} column to see dis 'Host © allfortune???.biz	Click in chart tribution chart *User = JORDAN	to filter table be or map to the lef 'Group 0 Level3_VPN	low by time. Cur ft, click on non ** 'Priority = information	column to cli *Action © pass	g full range, ose it again. "Service = HTTPS
All events O Rows Time = e2/15/19 04:32:40 PH e2/15/19 04:32:40 PH	* "Gateway/Device = Chicago, USA Chicago, USA	"Firewall Instance 5 ARCD76145 ABCD76145	*App List = LEVEL3-DEFAULT-AC LEVEL3-DEFAULT-AC	*App Category = Web.Client Web.Client	"App Risk = medium medium	Click o *Application = HTTP5. DROKSER HTTPS. UROKSER	n a value of a ^w column to see dis 'Host © allfortune???.biz xclones.in.net	Click in chart tribution chart "User 1 JORDAN HAVES	to filter table bei or map to the lef "Group 0 Level3_VPN Level3_VPN	tow by time. Cur ft, click on non ** *Priority * information information	column to cli *Action 5 pass	a full range, ose it again, "Service = HTTPS HTTPS
All events 0 Rows 7/mie * 02/15/15 04:32:40 PH 02/15/19 04:32:40 PH 02/15/19 04:32:40 PH	* *Gateway/Device 5 Chicago, USA Chicago, USA Chicago, USA	"Firewall Instance 5 ABC076145 ABC076145 ABC076145	*App List = LEVEL3-DEFAULT-AC LEVEL3-DEFAULT-AC LEVEL3-DEFAULT-AC	'App Category = Neb.Client Neb.Client Meb.Client	"App Risk 2 medium medium medium	Click o *Application = HTTPS_BROKSER HTTPS_BROKSER HTTPS_BROKSER	n a value of a ^w column to see dis 'Host i allfortune???.biz xclones.in.net dlauten.bplaced.net	Click in chart tribution chart "User = JORDAN HAYES HARVEY	to filter table bei or map to the lef "Group = Level3_VPN Level3_VPN Level3_VPN	for by time. Cur ft, click on non " "Priority = information information	column to cli "Action 0 pass pass pass	a full range. ose it again. "Service : HTTPS HTTPS HTTPS
All events O Rows Timie 9 82/15/19 04:32:40 PH 92/15/19 04:32:40 PH 92/15/19 04:32:40 PH 92/15/19 04:32:40 PH	* "Gateway/Device = Chicago, USA Chicago, USA Chicago, USA	"Firewall Instance 5 ABC076145 ABC076145 ABC076145 ABC076145	*App List = LEVEL3-DEFAULT-AC LEVEL3-DEFAULT-AC LEVEL3-DEFAULT-AC LEVEL3-DEFAULT-AC	'App Category : web.client web.client web.client General.Interest	"App Risk = medium medium medium elevated	Сіск о "Application s нттря, веожея нттря, веожея нттря, веожея своде, Ассоинта	n a value of a ^{sul} column to see dis 'Host i allfortune777.biz xclones.in.net dlauten.bjaced.net. penbogdhyrpvong.cm158.top	Click in chart tribution chart "User = JORDAN HAYES HARVEY DUNN	to filter table bel or map to the lef "Group 0 Level3_VPN Level3_VPN Level3_VPN Level3_VPN	iow by time. Cur ft, click on non ** *Priority = information information information	column to cli "Action = pass pass pass pass	a full range. ose it again. "Service : HTTPS HTTPS HTTPS HTTPS
All events 0 Rows Dimo = 02/15/19 04:32:40 PH 02/15/19 04:32:40 PH 02/15/19 04:32:40 PH 02/15/19 04:32:40 PH 02/15/19 04:32:40 PH	* Sateway/Device F Chicago, USA Chicago, USA Chicago, USA Chicago, USA	"Firewall Instance 5 ABCD76145 ABCD76145 ABCD76145 ABCD76145 ABCD76145	*App List = LEVEL3-05FAULT-AC LEVEL3-05FAULT-AC LEVEL3-05FAULT-AC LEVEL3-05FAULT-AC LEVEL3-05FAULT-AC	'App Category : Web.Client Web.Client Web.Client General.Interest Web.Client	"App Risk = nedius nedius nedius elevated nedius	Click o "Application = HTTPS.BROKER HTTPS.BROKER HTTPS.BROKER HTTPS.BROKER	n a value of a ^{sec} column to see dis 'Hoot : allfortune???.biz xclones.in.net dlauten.bplaced.net perbbedyrpromq.cm158.top shadowraze.pe	Click in chart tribution chart "User = JORDAN HARES HARVEY DUNN HARVEY	to filter table bel or map to the lef "Group © Level3_VPN Level3_VPN Level3_VPN Level3_VPN Level3_VPN	iow by time. Cur ft, click on non ** *Priority = information information information information	column to cli "Action = pass pass pass pass pass	a fuil range. ose it again. "Service : HTTPS HTTPS HTTPS HTTPS HTTPS
All events O Rows Time = 02/15/19 04:32:40 PH 02/15/19 04:32:40 PH 02/15/19 04:32:40 PH 02/15/19 04:32:40 PH 02/15/19 04:32:40 PH	* Chicago, USA Chicago, USA Chicago, USA Chicago, USA Chicago, USA	"Firewall Instance 5 AbC076145 ABC076145 ABC076145 ABC076145 ABC076145 ABC076145 ABC076145	"App List = LEVEL3-OFAULT-AC LEVEL3-OFAULT-AC LEVEL3-OFAULT-AC LEVEL3-OFAULT-AC LEVEL3-OFAULT-AC LEVEL3-OFAULT-AC	'App Category = web.client web.client General.interest General.interest	"App Risk = nedius nedius nedius elevated nedius elevated	Click o "Application := HTTPs. DROWSER HTTPs. DROWSER HTTPs. DROWSER GogeLe. Accounts HTTPs. DROWSER GoogLe. Services	n a value of a ^{set} column to see dis 'Host © allfortune777.biz xclones.in.net dlautes.in.net dlautes.bplaced.net pmetbeedpyrpvong.cmr158.top shadowrze.pw doratopelase.pw	Click in chart tribution chart "User © JORAN HAVES HARVEY KELCH	to filter table bel or map to the left 'Group = Level3_VPN Level3_VPN Level3_VPN Level3_VPN Level3_VPN Level3_VPN	iow by time. Cur ft, click on non " 'Priority : information information information information	column to cli *Action 2 pass pass pass pass pass pass pass pas	a full range. ose it again. "Service : HTTPS HTTPS HTTPS HTTPS HTTPS HTTPS HTTPS
All events O Rows Time 1 02/15/19 04:32:40 PH 02/15/19 04:32:40 PH 02/15/19 04:32:40 PH 02/15/19 04:32:40 PH 02/15/19 04:32:40 PH 02/15/19 04:32:40 PH	Gateway/Device = Chicago, USA Chicago, USA	*Firewall Instance 5 Anco?6145 Abco?6145 Abco?6145 Abco?6145 Abco?6145 Abco?6145 Abco?6145	*App List = LEVEL3-027AULT-AC LEVEL3-027AULT-AC LEVEL3-027AULT-AC LEVEL3-027AULT-AC LEVEL3-027AULT-AC LEVEL3-027AULT-AC LEVEL3-027AULT-AC	'App Category € Web.Client Web.Client Web.Client General.Interest Web.Client General.Interest Web.Client	"App Risk 2 medius medius medius medius medius medius medius medius	Click o "Application : HTTPS.DROMER HTTPS.DROMER Google.Accounts HTTPS.DROMER Google.Accounts HTTPS.DROMER Google.Srvices HTTP.DROMER	n a value of a ^{sec} column to see dis "Host E allfortune???.biz xclones.in.net dlauten.bplaced.net pmenbeedyrproved.emf58.top shadowraze.pw doratopelase.pw dobservers.pw	Click in chart tribution chart "User © JORDAN HAYES HARVEY NARVEY KELCH KELCH	to filter table bel or map to the left "Group 5 Level3_YFN Level3_YFN Level3_YFN Level3_YFN Level3_YFN Level3_YFN Level3_YFN	iow by time. Cur ft; click on non ** *Priority = information information information information information	column to cir *Action 2 pass pass pass pass pass pass pass pass pass pass pass pass	a full range. ose it again. "Service : HTTPS HTTPS HTTPS HTTPS HTTPS HTTPS HTTPS
All events O Rows Tritic 1 02/15/19 04:32:40 PH 02/15/19 04:32:40 PH 02/15/19 04:32:40 PH 02/15/19 04:32:40 PH 02/15/19 04:32:40 PH	Gateway/Device = Chicage, USA Chicage, USA	Firewall Instance 2 ARCD76145 ABCD76145 ABCD76145 ABCD76145 ABCD76145 ABCD76145 ABCD76145 ABCD76145	*App List = LEVEL3-CEFAULT-AC LEVEL3-CEFAULT-AC LEVEL3-CEFAULT-AC LEVEL3-CEFAULT-AC LEVEL3-CEFAULT-AC LEVEL3-CEFAULT-AC LEVEL3-CEFAULT-AC LEVEL3-CEFAULT-AC	<pre>'App Category 0 web.Client web.Client web.Client General.Interest web.Client General.Interest web.Client Collaboration</pre>	TApp Risk 2 medius medius medius elevated elevated elevated	Click o "Application 5 HTTPS, DROWER HTTPS, DROWER HTTPS, DROWER Google, Accounts HTTPS, DROWER Google, Services HTTP, BROWER HTTP, BROWER HTTP, BROWER	n a value of a ^{sur} column to see dis "Host i allfortune???.biz xclones.in.net dlauten.bplaced.net. peenboedyrpronq.cm:158.top shadowraze.pw doratopelase.pw debservers.pw dilecome.hotmail.ru	Click in chart tribution chart "User 9 JOROAN HAYES HARVEY NELCH HARVES HARVEY NELCH HARVES	to filter table bei or map to the lef "Group ¢ Level3_VPN Level3_VPN Level3_VPN Level3_VPN Level3_VPN Level3_VPN Level3_VPN Level3_VPN Level3_VPN	Iow by time. Cur t, click on non "" "Phonty : Information Information Information Information Information Information Information	column to cir *Action 2 pass pass pass pass pass pass pass pass pass pass pass pass pass pass pass pass	a full range. ose it again. "Service : HTTPS HTTPS HTTPS HTTPS HTTPS HTTPS HTTPS HTTP HTTP

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. ©2021 Lumen Technologies. All Rights Reserved.

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.



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.

														Export •	
ime Range:	An	y Field:	s	itatus:		Priori	ty:		Gateway or I	Device:	Firewall Inst	tance:	Filter Mode:		
Last 24 hours	•			•		Al		*	270		•	•	Basic	*	
Hide Filters															
Event Distribution															
10.000															
500.8 L	-			inde.											
2:00 PM Wed Mer 20 2019	4,00 PM	6:00 PM	8:00 PM	10)	DO I'M	12:00 AM Thu Mar 21	2:00 AM	4:0	0 AM	5.00 AM	8.00 AM	10:00 AM	12:00 PM 2:00 PM	pasta	roogn
											ci	ick in chart to filter tab	le below by time. Currently	r showing full r	rangi
											to see distribution d	had or man to the laft	station and the second Phil		anali
86167 Rows									click on a valu	e or a - column	to see outroutorie	hart of map to bie reit.	click on non column (1)	ne) to close it i	ogui
86167 Rows Time 9	gw_dev =	*Firewall Instance ©	*User *	*Group =	"Service =	*Agent =	*Status =	*Priority =	"Method ©	*Message =	*Destination IP =	"Destination Port =	*Destination Location =	"Source IF	e e
36167 Rows Time 9 83/21/19 82:43:85 PM	gw_dev = gn12345	*Firewall Instance © ABC0467898	*User # BANKS	"Group = Level3_VPN	"Service #	*Agent = N/A	"Status = passthrough	*Priority = notice	"Method = filename	"Message ©	*Destination IP = 18.125.228.92	*Destination Port #	*Destination Location #	"Source IF 18.24.40.	e e . 81
86167 Rows Time 0 03/21/19 02:43:05 PH 03/21/19 02:43:04 PH	gw_dev = gn12345 gn12345	*Firewall Instance = ABCD467898 ABCD467898	*User * DANKS BANKS	"Group = Level3_VPN Level3_VPN	"Service = http http	*Agent = N/A N/A	*Status © passthrough passthrough	*Priority * notice notice	"Method © filename	"Message ÷ File File	*Destination IP = 10, 125, 228, 92 10, 125, 228, 92	*Destination Port # 80	*Destination Location #	"Source IF 10.24.40. 10.24.40.	2 e .81 .81
Time 0 03/21/19 02:43:05 PH 03/21/19 02:43:04 PH 03/21/19 02:43:04 PH	gw_dev = gm12345 gm12345 gm12345	*Firewall Instance + ABCD467890 ABCD467890 ABCD467890	"Usor * DANKS BANKS BANKS	*Group = Level3_VPN Level3_VPN Level3_VPN	"Service * http http http	*Agent = N/A N/A N/A	*Status = passthrough passthrough	*Priority * notice notice notice	"Method © filename filename filename	"Message ÷ File File File	*Destination IP = 10.125.228.92 10.125.228.92 10.125.228.91	"Destination Port = 80 80	"Destination Location 4	"Source IF 18.24.40. 18.24.40. 19.24.40.	9 e .81 .81 .81
Time 0 a0/21/19 02:43:05 PH 03/21/19 02:43:04 PH 03/21/19 02:43:04 PH 03/21/19 02:43:04 PH	gw_dev = gm12345 gm12345 gm12345 gm12345	*Firewall Instance © ABC0467890 ABC0467890 ABC0467890 ABC0467890 ABC0467890	*User * DANKS BANKS BANKS BANKS	*Group # Level3_VPN Level3_VPN Level3_VPN Level3_VPN	"Service # http http http http	*Agent = N/A N/A N/A N/A	"Status = passthrough passthrough passthrough	"Priority = notice notice notice	"Method = filename filename filename filename	"Message © File File File File	"Destination IP = 19, 125, 228, 92 18, 125, 228, 92 19, 125, 228, 91 10, 125, 228, 91	"Destination Port = 80 80 80 80 80	"Destination Location #	"Source IF 10.24.40. 10.24.40. 10.24.40. 10.24.40.	9 c .81 .81 .81 .81
86167 Rows Time 0 83/21/19 02:43:05 PH 83/21/19 02:43:04 PH 83/21/19 02:43:04 PH 83/21/19 02:43:04 PH 83/21/19 02:43:04 PH	gw_dev = gn12345 gn12345 gn12345 gn12345 gn12345	"Firewall Instance * Abc0467890 ABC0467890 ABC0467890 ABC0467890 ABC0467890	*User = DANKS BANKS BANKS BANKS QANKS	"Group = Level3_VPN Level3_VPN Level3_VPN Level3_VPN Level3_VPN	"Service = http http http http http	*Agent = N/A N/A N/A N/A	"Status = passthrough passthrough passthrough passthrough	"Priority = notice notice notice notice	"Method = filename filename filename filename filename	"Message 0 File File File File File	"Destination IP = 10.125.228.92 10.125.228.92 10.125.228.91 10.125.228.91 10.125.228.90 10.125.228.77	"Destination Port # 80 80 80 80 80 80 80 80 80 80 80 80 80	"Destination Location 1	"Source IF 10.24.40. 10.24.40. 10.24.40. 10.24.40. 10.24.40.	9 ¢ .81 .81 .81 .81 .81
10167 Rows Time = 83/21/19 82:43:65 PH 83/21/19 82:43:64 PH 83/21/19 82:43:64 PH 83/21/19 82:43:64 PH 83/21/19 82:43:64 PH 83/21/19 82:43:64 PH	gw_dev = gn12345 gn12345 gn12345 gn12345 gn12345 gn12345	"Firewall Instance 5 ADC0467839 ABC0467839 ABC0467899 ABC0467890 ABC0467890 ABC0467890	*User ÷ DANKS BANKS BANKS BANKS DANKS BANKS	"Group = Level3_VPN Level3_VPN Level3_VPN Level3_VPN Level3_VPN Level3_VPN	"Service # http http http http http http http	*Agent = N/A N/A N/A N/A N/A N/A	"Status ÷ passthrough passthrough passthrough passthrough passthrough	"Priority = notice notice notice notice notice	"Method = filename filename filename filename filename	"Message = File File File File File File File	"Destination IP = 10.125.228.92 10.125.228.92 10.125.228.91 10.125.228.91 10.125.228.90 10.125.228.77 10.12.68.35	"Destination Port # 80 80 80 80 80 80 80 80 80 80 80 80 80	"Destination Location 1	"Source IF 10.24.40. 10.24.40. 10.24.40. 10.24.40. 10.24.40. 10.24.40. 10.24.40.	9 ¢ .81 .81 .81 .81 .81 .81 .81
1007 Rows Time 0 83/21/19 82:43:65 PH 83/21/19 82:43:64 PH 83/21/19 82:43:64 PH 83/21/19 82:43:64 PH 83/21/19 82:43:64 PH 83/21/19 82:43:64 PH 83/21/19 82:43:64 PH	gw_dev * gn12345 gn12345 gn12345 gn12345 gn12345 gn12345 gn12345	"Firewall Instance 5 ADC0467839 ABC0467839 ABC0467899 ABC0467890 ABC0467890 ABC0467890 ABC0467890	*User * DANKS BANKS BANKS BANKS DANKS DANKS	*Group = Level3_VPN Level3_VPN Level3_VPN Level3_VPN Level3_VPN Level3_VPN Level3_VPN	"Service # http http http http http http http	*Agent = N/A N/A N/A N/A N/A N/A	"Status © passthrough passthrough passthrough passthrough passthrough passthrough	"Priority = notice notice notice notice notice notice	"Method : filename filename filename filename filename filename filename	"Message = File File File File File File File File	*Destination IP = 10.125.220.92 10.125.228.92 10.125.228.91 10.125.228.90 10.125.228.77 10.12.68.35 10.12.68.35	*Destination Port # 80 80 80 80 80 80 80 80 80 80 80 80 80	"Destination Location 1	"Source IF 16.24.40. 10.24.40. 10.24.40. 10.24.40. 10.24.40. 10.24.40. 10.24.40. 10.24.40.	9 0 81 81 81 81 81 81 81 81 81 81
Time 0 a3/21/19 02:43:05 PH 83/21/19 02:43:04 PH 83/21/19 02:43:04 PH 83/21/19 02:43:04 PH 83/21/19 02:43:04 PH 83/21/19 02:43:04 PH 83/21/19 02:43:04 PH	gw_dev * gn12345 gn12345 gn12345 gn12345 gn12345 gn12345 gn12345 gn12345	*Firewall Instance 5 ADC0467830 ABC0467830 ABC0467830 ABC0467830 ABC0467830 ABC0467830 ABC0467830 ABC0467830	*User * DANKS BANKS BANKS BANKS BANKS DANKS BANKS BANKS	*Group = Level3_VPN Level3_VPN Level3_VPN Level3_VPN Level3_VPN Level3_VPN Level3_VPN	"Service # http http http http http http http htt	*Agent 5 N/A N/A N/A N/A N/A N/A N/A N/A	*Status ÷ passthrough passthrough passthrough passthrough passthrough passthrough passthrough	"Priority = - notice notice notice notice notice notice notice	"Method = filename filename filename filename filename filename filename	"Message 0 File File File File File File File File	*Destination IP = 10, 125, 228, 92 10, 125, 228, 92 10, 125, 228, 92 10, 125, 228, 93 10, 125, 228, 90 10, 125, 228, 93 10, 125, 228, 77 10, 12, 68, 35 10, 12, 69, 35 10, 221, 229, 55	*Destnation Port 2 80 80 80 80 80 80 80 80 80 80 80 80 80	*Destination Location 1	"Source IF 10.24.40. 10.24.40. 10.24.40. 10.24.40. 10.24.40. 10.24.40. 10.24.40. 10.24.40. 10.24.40.	2 0 81 81 81 81 81 81 81 81 81 81
Time 5 83/21/19 02:43:05 PH 83/21/19 02:43:04 PH	gw_dev 5 ga12345 ga12345 ga12345 ga12345 ga12345 ga12345 ga12345 ga12345 ga12345	*Firewall Instance * AbCo467899 ABCo467899 ABCo467899 ABCo467899 ABCo467899 ABCo467899 ABCo467899 ABCo467899 ABCo467899	"User * DANKS BANKS BANKS BANKS BANKS BANKS BANKS BANKS BANKS	"Group = Level3_VPN Level3_VPN Level3_VPN Level3_VPN Level3_VPN Level3_VPN Level3_VPN	"Service 0 http http http http http http http htt	*Agent # N/A N/A N/A N/A N/A N/A N/A N/A N/A	*Status S passthrough passthrough passthrough passthrough passthrough passthrough passthrough	*Priority = notice notice notice notice notice notice notice notice notice	'Method 9 filename filename filename filename filename filename filename filename filename	"Message 0 File File File File File File File File	*Destination IP = 10.125.228.92 10.125.228.92 10.125.228.91 10.125.228.91 10.125.228.90 10.125.228.90 10.126.15 10.12.63.15 10.12.63.15 10.12.25.55 10.221.229.55	*Destination Port = *Destination Port = 80 80 80 80 80 80 80 80 80 80	*Destination Location t	"Source IP 10. 24.40. 10. 24.40. 10. 24.40. 10. 24.40. 10. 24.40. 10. 24.40. 10. 24.40. 10. 24.40. 10. 24.40. 10. 24.40.	81 81 81 81 81 81 81 81 81 81
Time 2 02/21/19 02:43:05 PH 02/21/19 02:43:04 PH	gw_dev 2 gn12345 gn12345 gn12345 gn12345 gn12345 gn12345 gn12345 gn12345 gn12345	*Firewall instance * ACC047399 ABC047399 ABC047399 ABC047399 ABC047399 ABC047399 ABC047399 ABC047399 ABC047399 ABC047399	"User = DANKS BANKS BANKS BANKS BANKS BANKS BANKS BANKS	"Group 2 Level3_V9N Level3_V9N Level3_V9N Level3_V9N Level3_V9N Level3_V9N Level3_V9N Level3_V9N Level3_V9N Level3_V9N	"Service 5 http http http http http http http htt	*Agent # N/A N/A N/A N/A N/A N/A N/A N/A N/A	*Status S passthrough passthrough passthrough passthrough passthrough passthrough passthrough passthrough	"Priority = notice notice notice notice notice notice notice notice notice	"Method 5 filename filename filename filename filename filename filename filename filename filename	"Message Country File File File File File File File File	*Destination IP = 10.125.228.92 10.125.228.92 10.125.228.91 10.125.228.91 10.125.228.90 10.125.63.15 10.12.63.15 10.21.229.55 10.221.229.55 10.221.229.55	*Destination Port = *Destination Port = 80 80 80 80 80 80 80 80 80 80	*Destination Location 1	*Source II *Source II 10, 24, 40, 10, 24,	2 ¢ 61 .81 .81 .81 .81 .81 .81 .81 .8
20007 Rows Time 0 80/21/19 82:43:65 PH 80/21/19 82:43:64 PH	gw_dev 2 gw12345 gw12345 gw12345 gw12345 gw12345 gw12345 gw12345 gw12345 gw12345 gw12345 gw12345	*Firewall Instance * ACC447399 ABC047399 ABC047399 ABC047399 ABC047399 ABC047399 ABC047399 ABC047399 ABC047399 ABC047399 ABC047399	"User + DANKS BANKS BANKS BANKS BANKS BANKS BANKS BANKS BANKS	"Group 5 Level3_VPN Level3_VPN Level3_VPN Level3_VPN Level3_VPN Level3_VPN Level3_VPN Level3_VPN Level3_VPN	"Service 5 http http http http http http http htt	*Agent # N/A N/A N/A N/A N/A N/A N/A N/A N/A N/A	"Status * passthrough passthrough passthrough passthrough passthrough passthrough passthrough passthrough	"Priority = notice notice notice notice notice notice notice notice notice notice	"Method 5 filename filename filename filename filename filename filename filename filename filename filename	"Message 2 File File File File File File File File	*Destination IP = 10.125.228.92 10.125.228.92 10.125.228.93 10.125.228.91 10.125.228.90 10.125.228.90 10.125.228.93 10.125.228.95 10.12.68.35 10.221.229.55 10.221.229.55 10.221.229.61 10.221.266.121	*Destination Port = *Destination Port = 80 80 80 80 80 80 80 80 80 80 80 80 80	*Destination Location 1	*Source II *Source II 10. 24. 40. 10. 24. 40.	2 c 61 81 81 81 81 81 81 81 81 81 8
B0067 Rows Time 0 B0/21/19 B2/21/19 B0/21/19 B2/43/40 B0/21/19 B2/43/40	9w_dev 5 p12345 p12345 p12345 p12345 p12345 p12345 p12345 p12345 p12345 p12345 p12345 p12345 p12345		"User * DANKS BANKS BANKS BANKS BANKS BANKS BANKS BANKS	"Group 5 Level3_VPN Level3_VPN Level3_VPN Level3_VPN Level3_VPN Level3_VPN Level3_VPN Level3_VPN Level3_VPN Level3_VPN	"Service 5 http http http http http http http htt	*Agent # N/A N/A N/A N/A N/A N/A N/A N/A N/A N/A	"Status * passthrough passthrough passthrough passthrough passthrough passthrough passthrough passthrough passthrough	*Priority = notice notice notice notice notice notice notice notice notice notice notice	"Method 3 filename filename filename filename filename filename filename filename filename filename filename	Message 2 File File File File File File File File	*Destination IP = 10.125.228.92 10.125.228.92 10.125.228.92 10.125.228.90 10.125.228.90 10.125.228.97 10.125.63.55 10.125.63.55 10.126.95 10.221.229.55 10.221.229.55 10.221.226.121 10.223.36.136 10.2.81.49	*Destination Port = *Destination Port = 80 80 80 80 80 80 80 80 80 80 80 80 80	*Destination Location 1	Source IF 18. 24. 40. 19. 24. 40.	81 81 81 81 81 81 81 81 81 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

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. ©2021 Lumen Technologies. All Rights Reserved.

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)
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.