Lumen® Adaptive Network Security

Security Solutions portal (powered by Lumen) user guide for historical reporting (1st generation portal)

July 2021

LUMEN®

Table of contents

Adaptive Network Security: Lumen Security Solutions portal

The Adaptive Network Security (ANS) service near real-time dashboard, reports of log events, analysis, threat visualization and rapid threat defense are enabled on the Lumen Security Solutions portal. The Adaptive Network Security firewall policies files are available on the Security Solutions Analytics landing page. Access these features through Control Center.

Note: You must have both portal permissions for Managed Security Services and two-factor authentication to access the Lumen Security Solutions section of the portal.

Support contacts

Access security support contacts

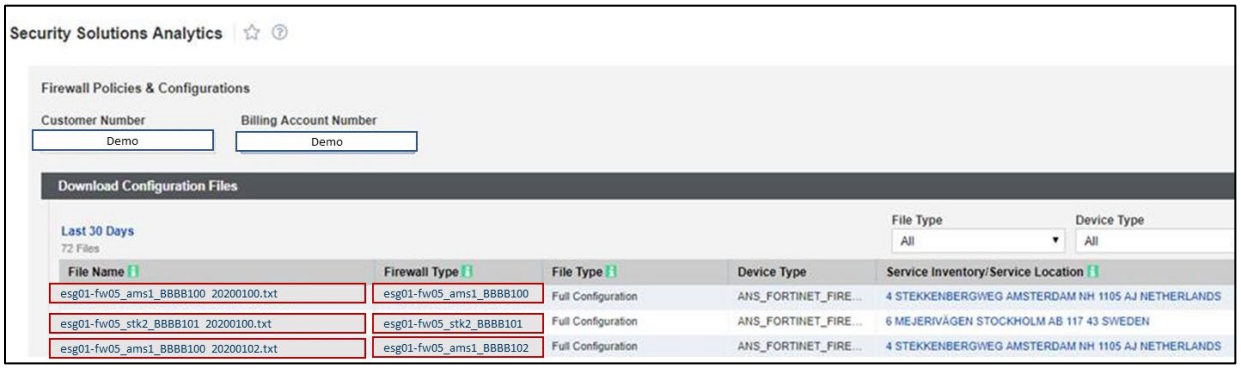
Accessing the Security Solutions portal

Note: Supported internet browsers are Chrome, Safari and Firefox. Use of unsupported browsers will likely result in reduced functionality.

Learn how to sign in to the Security Solutions portal

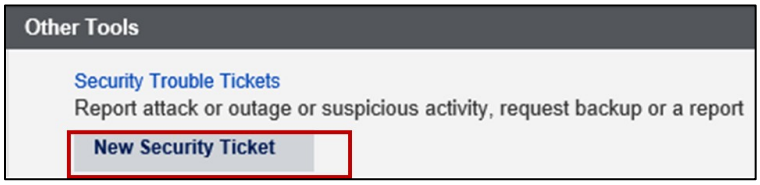
Adaptive Network Security firewall policies

1. The Adaptive Network Security firewall policies are formatted in a .txt file in JSON format.



2. Download, right-click, and select **Open with** > **WordPad** to better read the file.

3. If you have additional questions regarding Adaptive Network Security firewall policies, please submit a **Security Ticket** (Under **Other Tools**) to review with SOC personnel.

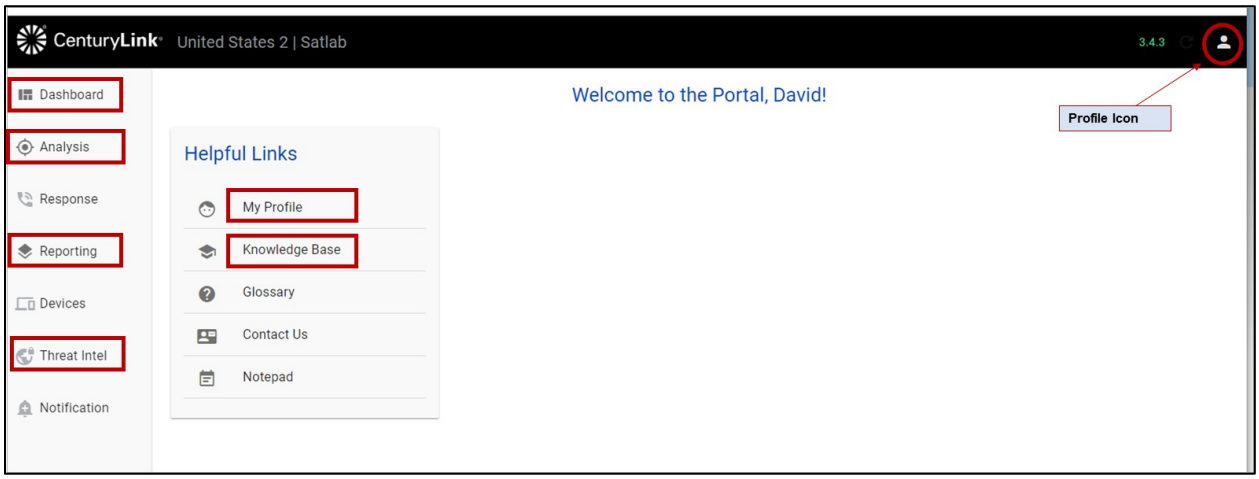


Lumen Security Solutions portal

The Lumen Security Solutions portal utilizes a single pane of glass across the Lumen Security Solutions portfolio with a common layout and user interface.

The Adaptive Network Security service includes a range of features and capabilities represented in the Dashboard, Analysis, Reporting, Threat Intel and the Profile – Administration - Security Policies (to set a security threat score with Rapid Threat Defense) menu items

- **Dashboard**—Displays summary view of the set of critical indicators for service features
- **Analysis**—Query capability to search logs based on a user defined set of filters
- **Reporting**—Displays set of default reports in a table view of underlying log events. These log events are inclusive of both Adaptive Network Security policies and Adaptive Network Security with augmented threat indicators with Rapid Threat Defense. User can create custom reports as well.
- **Threat Intel**—Displays set of interactions with malicious IP sites and domains based on near real-time threat intelligence indicators from Black Lotus Labs. View enabled with Basic and Premium service levels.
- **My Profile**—View and set access level, user preference, password.
- **Knowledge Base**—Online help for the Lumen Security Solution portal.
- **Profile Icon**—Further dropdown selections to Administration (to set Security Posture for Rapid Threat Defense), Glossary, Knowledge Base and Logout.



Common filters and customization

Common controls across the Adaptive Network Security dashboards are:

- **Date Range**—interval for viewing search results.
- **Query**—field to enable user to filer the data shown in the dashboard based a query they enter.
- **Device**—the firewall physical device host name that inspects traffic and enforces security compliance policies.

- **Firewall Instance**—customer virtual network firewall instance with customer configured policies on a device.
- **Company**—name of the customer

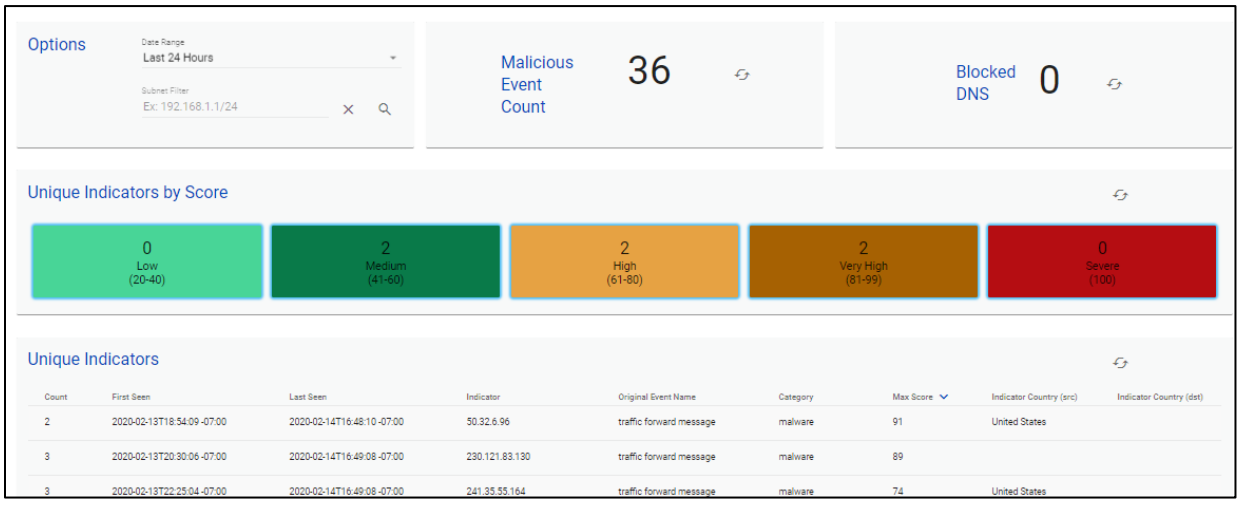
Wildcard—most filter controls are preset with the * wild card character that match any value, or you can select a value.

See Appendix A that describes the estimated event severity that caused a log event.

Threat Visualization

Threat Visualization displays a near real time view of the threat landscape in a single portal view, based on comprehensive threat intelligence data gathering and analytics from Lumen Black Lotus™ Labs. Customers can see interactions with single-selected malicious IP addresses including details such as its source, malware family, but no automated actions are taken. This capability is available with Adaptive Network Security Basic and Premium Service Level Packages.

- Select “Threat Intel” on the left menu.



The table of unique indicators column headings are described in the following table.

Column	Description
Count	Quantity of Interactions with this indicator
First Seen	The date and time this indicator was first reported. **Note:** For clarity, the time zone offset from GMT is included.
Last Seen	The date and time this indicator was last reported. Again, the time zone offset from GMT is included
Indicator	The IP address or domain that is hosting the malicious indicator
Original Event Name	Event as identified from the reporting source for this indicator. Some event names include: • Threatflow: The set of malicious indicators identified by IP address that has been collected and curated by Lumen Black Lotus Labs • Block DNS: Events that have been generated by users attempting to reach Domains that are malicious and meet the customer's criteria for blocking at DNS or that have been explicitly blocked by the customer administrator. • Allow DNS: Events that have been generated by users connecting with domains that have been explicitly allowed by the customer administrator.
Category	Threat category as explained above
Max Score	The highest risk score presented by this indicator. Note that any indicator may be participating in multiple threat campaigns and hence may have multiple risk core associated with it. The score in this column is the maximum value associated with this indicator
Indicator Country (src)	The geographic location from where this indicator is sourced
Indicator Country (dst)	The geographic location targeted by this indicator

A threat category is associated for each indicator listed. An indicator may be associated with multiple threat categories. The threat categories are described in the table below:

Category	Description
C2	C2 is shorthand for “Command and Control”. Each botnet has a C2 entities that manage the activities of the botnet.
Attack	These entities attempt to penetrate the peripheral defenses of an enterprise typically using “dictionary” attacks to crack passwords on publicly addressable assets.
Bot	Entities that have been compromised to participate in the activities a botnet.
Malware	Entities that distribute malware for the purpose of compromising assets to gain access to intellectual property.
Phish	Entities that proliferate communications for the purpose of collecting credentials to valuable assets. Phishing can use email, phone calls, text, IM and other vectors for this purpose.
Scan	Entities that probe the peripheral defenses of an enterprise for the purpose of discovering accessibility, typically pinholes in firewalls.
Spam	Entities that distribute communications for the purpose of attracting attention to services that are generally considered irrelevant to the business of the enterprise targeted.
Anonymous Proxy	Also known as “Proxy” or “TOR (The Onion Router).” Adversaries typically attempt to obfuscate their presence on The Internet by positioning behind an anonymous proxy service. Enterprises rarely have legitimate business associated with these entities, so communications with them is typically of interest.

The following indicators may also be present alongside the primary indicators.

Indicator	Description
Popular	Associated with IP addresses that are identified as malicious, but also have many services behind them, lowering the probability that the enterprise is communicating with the specific malicious entity. For instance, the IP address may belong to a hosting provider that has potentially thousands of domains behind it. The risk score associated with this indicator will be diminished to reflect the lower probability of direct interaction.
CDN	Associated with IP addresses that are identified as malicious but are also part of a CDN (content delivery network). This substantially lowers the probability that the enterprise is in direct contact with the malicious entity. The risk score associated with this indicator will be diminished to reflect the lower probability of direct interaction.

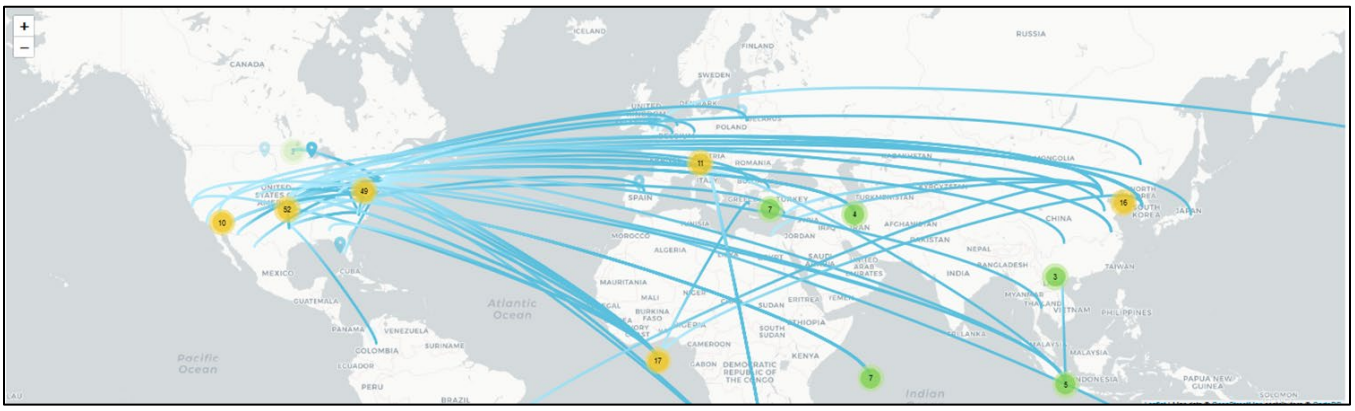
Each column can be sorted by ascending or descending with successive clicks. At the bottom of each table are selectors for:

- Tables that exceed the number of entries per page, display a “Page” selector is displayed. The default is 1, but clicking the down-arrow icon will list the pages that can be selected
- Number of table entries per page. The default is 5. Select the down-arrow icon to specify how many entries to see in a single display
- The specific entries of the total set are being displayed
- Previous and Next selectors

Note that all tables throughout the Adaptive Network Security reports have these capabilities.

Selecting any Unique Indicator will bring up the Indicator Reputation page for that selected indicator.

Scrolling down the dashboard page will display an interactive map that shows the geographic depiction of indicators (Figure 6). The color of the circle represents the highest risk score for all the indicators sourced in that location. The number inside the circle conveys the quantity of Unique Indicators in that location.



Selecting the +/- controls will cause the map to zoom in or out. Zooming can also be initiated from a mouse wheel. Selecting an indicator group (circle) displays the individual indicators with a presence indicator. Hovering over the presence indicator will display further information on the selected indicator.

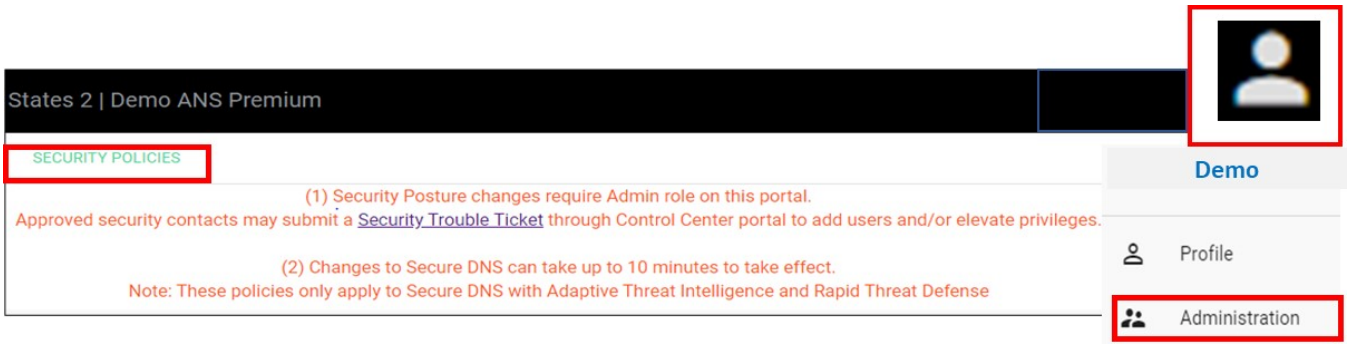
Rapid Threat Defense

Rapid Threat Defense allows customers to automatically detect and respond to threats.

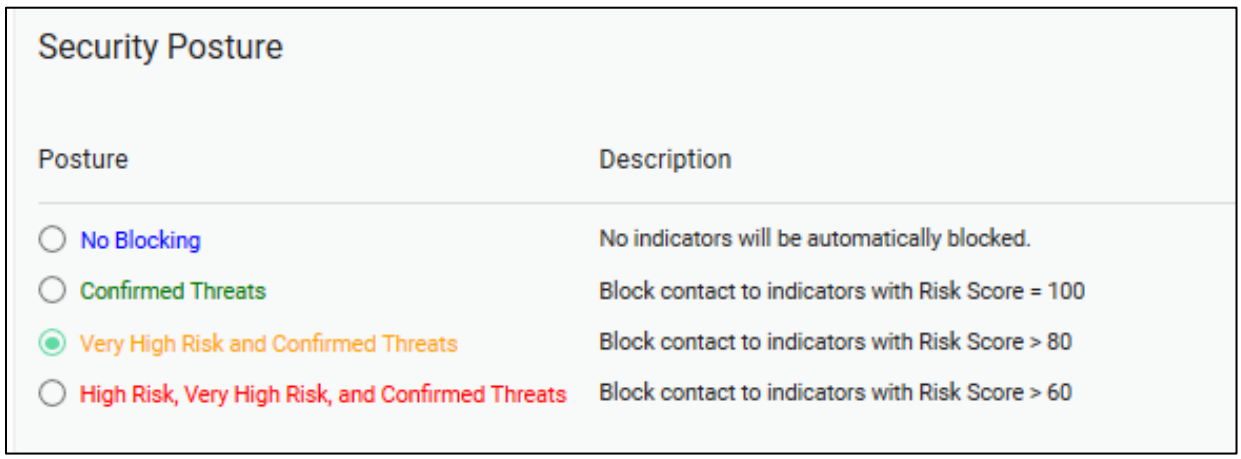
Customers specify a security posture which has an associated risk score. When malicious entities are discovered that have a risk score that meets or exceeds the risk score indicated in the security posture, countermeasures will be automatically deployed to block access to that malicious entity. Rapid Threat Defense is only available with Adaptive Network Security Premium service level.

To set security posture with Rapid Threat Defense, select the **Profile** icon (in the upper-right corner), scroll down to **Administration**, then click to **Security Policies**.

Note: Users must have an admin role to set security posture or set Allow/Block IP v4 Address on the Lumen Security Solutions portal. An approved security user on Control Center can submit a security trouble ticket to elevate their privileges to admin role, and/or add users on the Lumen Security Solutions portal.



The selected security posture risk score selections are as follows:



Selecting a security posture sets up automated deployment of countermeasures whenever new malicious entities are discovered by Black Lotus Labs™ – the Lumen cyber threat intelligence team. The Black Lotus Labs team has automated the discovery, classification and validation of new malicious entities to deploy countermeasures typically in under 30 minutes from discovery of the new malicious entity.

Adding global block or allow rules

In addition to selecting a security posture, customers can also select specific IPv4 address ranges to block or allow that are independent of security posture.

Block or allow list rules on specific IPv4 address ranges remain active, even if the security posture is set to “No Blocking”. These lists always take precedence to override or augment any countermeasures deployed by the security posture selection or any other Adaptive Network Security firewall policy if an IPv4 address match occurs.

- Allow IPv4 CIDR Address Range: Always allow access to this IPv4 CIDR address range, even if it is identified as malicious and has a risk score that meets or exceeds the risk score associated with the selected security posture.
- Block IPv4 CIDR Address Range: Always block access to the IPv4 CIDR address range in this entity, unless defined in the Allow list.

All IPv4 address countermeasures specified on this page are deployed globally. They apply to all Adaptive Network Security Firewall Instances, all users, all ports, all protocols and all services.

If a more specific policy is required, please submit a SOC security ticket (**Service Mgmt** > **Security Trouble Tickets**) where you can specify the following parameters per Adaptive Network Security Firewall Instance:

  - Source Interface (IPVPN is the default)
  - Source address (All is the default)
  - Schedule (e.g., limits hours, Always is the default)
  - Service (e.g., protocol, UDP, FTP, All is the default)
  - UTM Profile Sensors (e.g. WCF, IPS/IDS, Various is the default)

Dashboards

The Adaptive Network Security set of dashboards are a summary view of critical indicators with Adaptive Network Security Services.

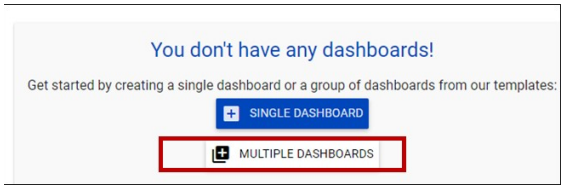
Default set of Adaptive Network Security service dashboards are:

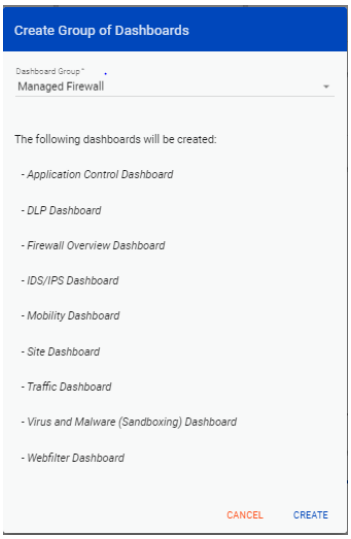
- **Firewall Overview Dashboard**—displays the summary of important metrics from all features in distinct panels.
- **Application Control Dashboard**—displays actions (pass or block) based on application usage. These setting are defined for a specific user, group, or IP address based on settings identified during service setup. Application Control identifies and enforces application use on the network.
- **DLP** (data loss protection) **Dashboard**—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.
- **IPS/IDS Dashboard** (Intrusion Prevention and Detection Services)—displays intrusion prevention (dropped) and intrusion detection (detected) events over time with view of top source IPs and common alerts. IPS/IDS provides management and monitoring, detection and prevention capabilities at your network edge. Traffic matching signatures of known attacks generate incident reports and may also be blocked on a per-signature basis.

- **Mobility Dashboard**—displays information of successful and unsuccessful mobility endpoint client authentication status and top client duration in hours. Mobility access is to a private network and/or the public Internet via Lumen internet access or third-party internet access.
- **Site Dashboard**—displays traffic and events from remote site access IPSec tunnels to a private network and/or the public Internet via Lumen internet access or third-party internet access.
- **Traffic Dashboard**—displays summary of traffic allowed and denied by firewall policy. Reports show how traffic was managed in response to such policies.
- **Virus and Malware (Sandboxing) Dashboard**—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.
- **Webfilter Dashboard**—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.

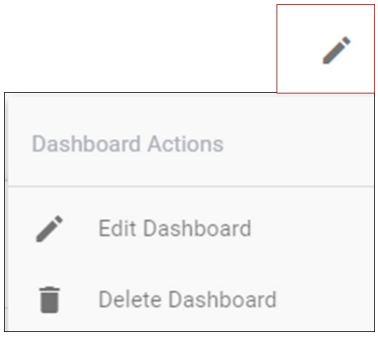
Dashboard displays

- For initial set up, select "Multiple Dashboards" and then Dashboard Group "Managed Firewall" to create the set of default Dashboards associated to the Adaptive Network Security service.





- To delete or edit a dashboard, click the edit button in the upper-right corner and select **Edit Dashboard** or **Delete Dashboard**.

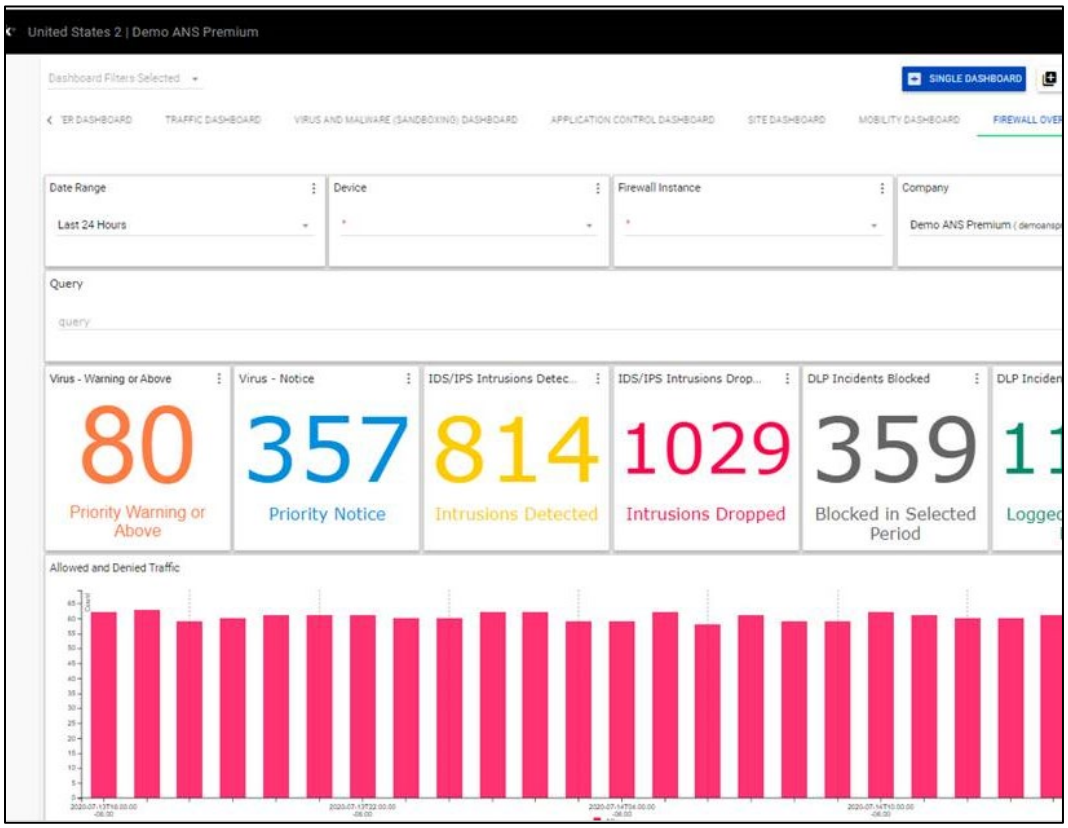


Firewall Overview Dashboard

The Firewall Overview Dashboard dynamically combines important metrics from all service features in distinct panels

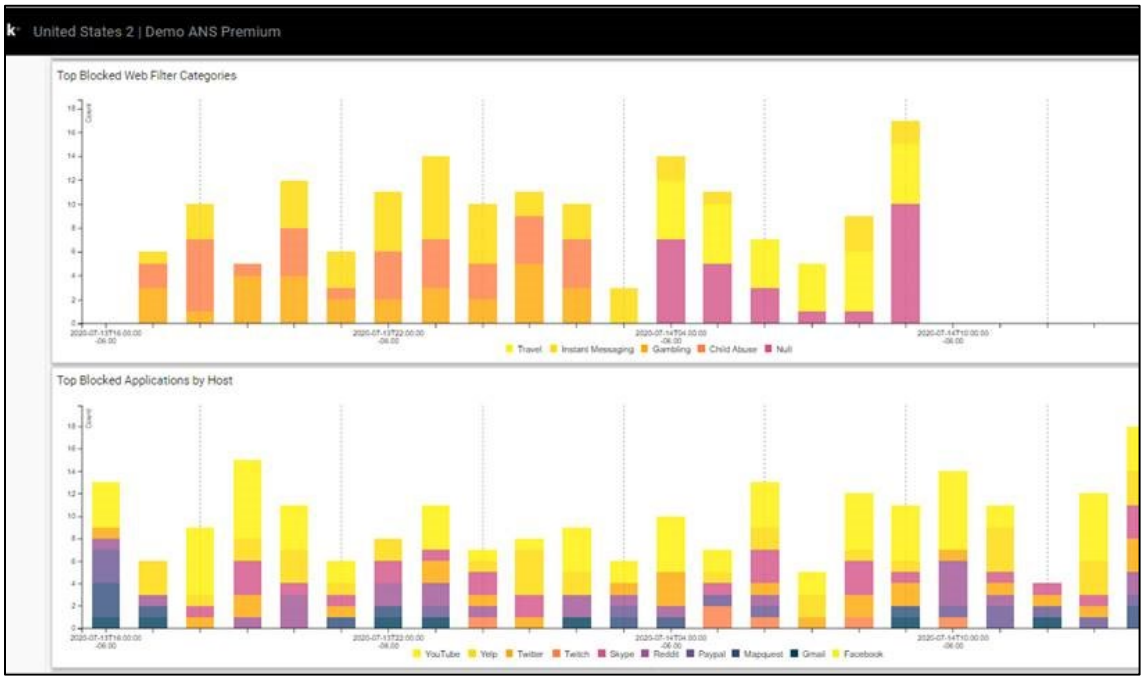
In full configuration, the following panels appear:

- **Virus – Warning or Above** and **Virus – Notice** - The number of virus attacks of priority warning or higher for the selected date rand and the number of virus attacks with priority notice.
- **IDS/IPS Intrusion Detected and IDS/IPS Intrusions Dropped** - The number of detected and dropped IPS/IDS incidents for the selected date range.
- **DLP Incidents Blocked and DLP Incidents Logged** - The number of blocked and logged DLP incidents for the selected date range.

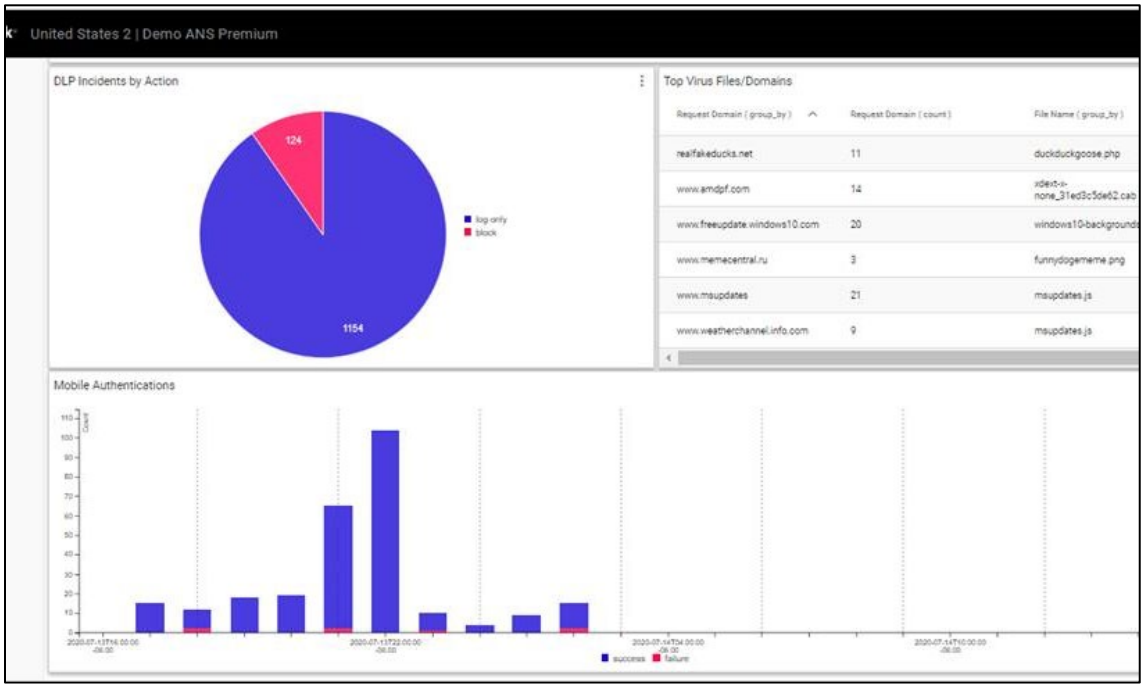


- **Allowed and Denied Traffic** - A bar chart of the allowed and denied firewall traffic events for the selected date range.
- **Top Blocked Web Filter Categories** - A bar chart of the top 10 blocked web filter categories and count of the number of attempts to web sites that match the category for the selected date range.
- **Top Blocked Applications by Host** - A bar chart of the top 10 blocked application and host combinations and count of the number of attempts by application that match the category for the

selected date range.



- **DLP Incidents by Action** - A pie chart showing the type of data detected or block for selected date range.
- **Top Files/Domains** - A list of the most frequently detected virus files for the selected date range
- **Mobile Authentications** - A bar chart of the number of failed and successful mobile access authentication attempts for the selected date range.

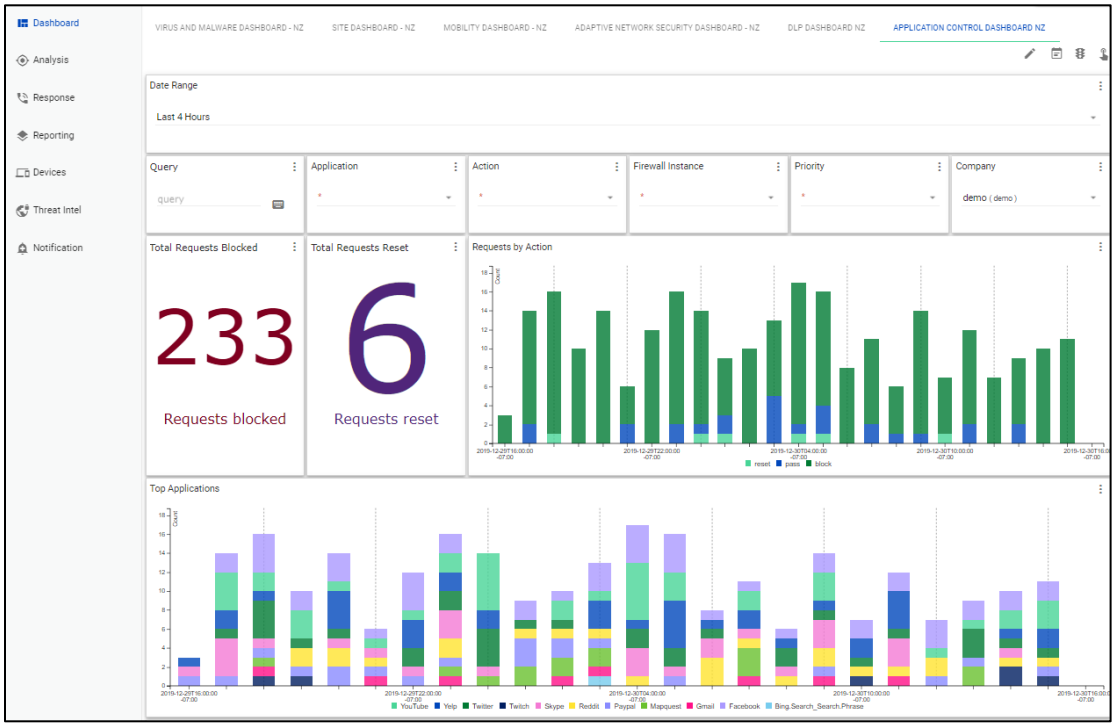


Application Control dashboard

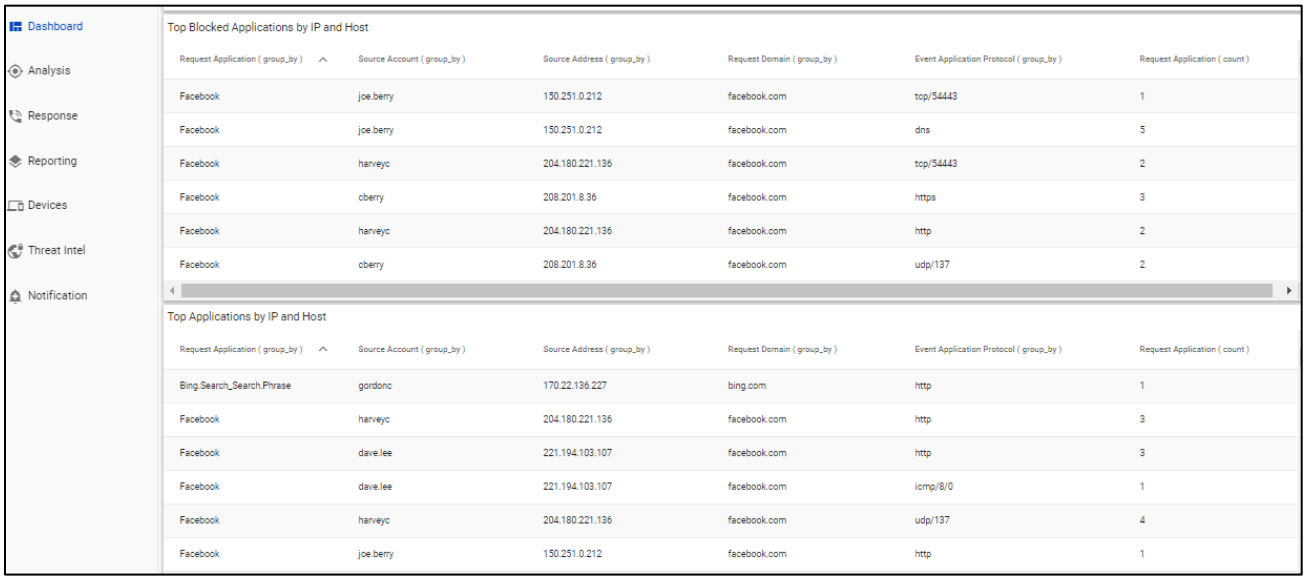
The Application Control dashboard presents logged events for application-based activities.

The following panels appear:

- **Total Requests Blocked -** The number of requests blocked for the selected date range.
- **Total Requests Reset** - The number of requests where the firewall terminated the connection with a reset signal for the selected date range
- **Requests by Action** - A bar chart of requests by action (block/pass/reset) for the selected date range.
- **Top Applications** - A bar chart of top 10 applications by the number of requests for the selected date range.



- **Top Blocked Applications by IP and Host** - Listing of the top blocked applications by IP and host (source and # requests).
- **Top Applications by IP and Host** - Listing of the top applications by IP and host (source and # requests).

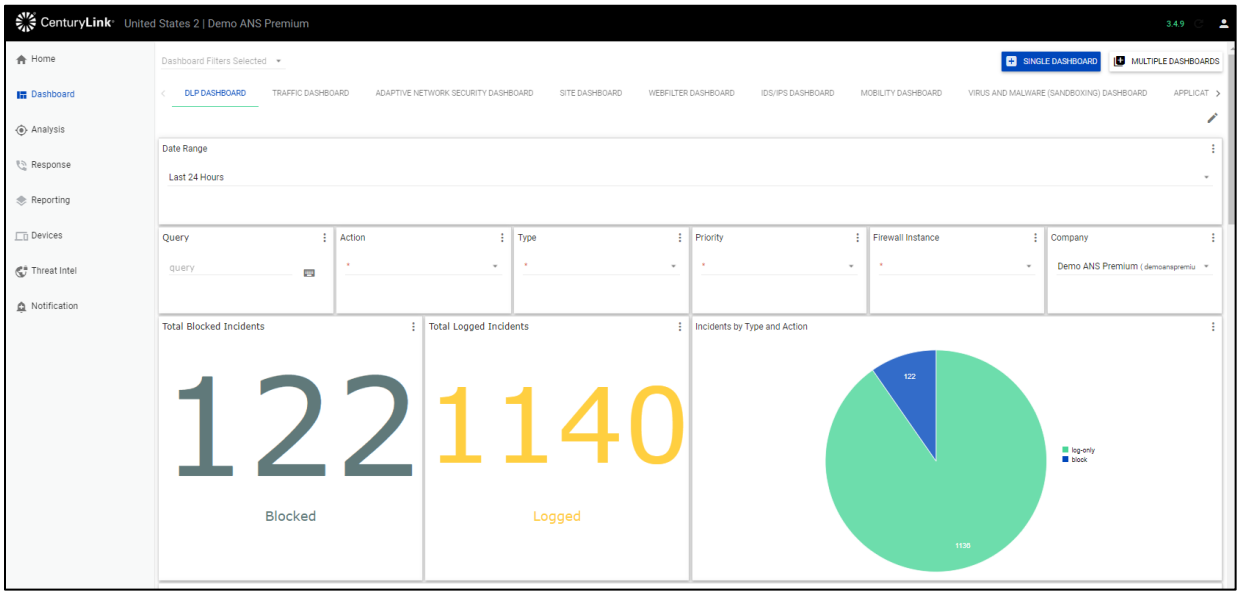


DLP dashboard

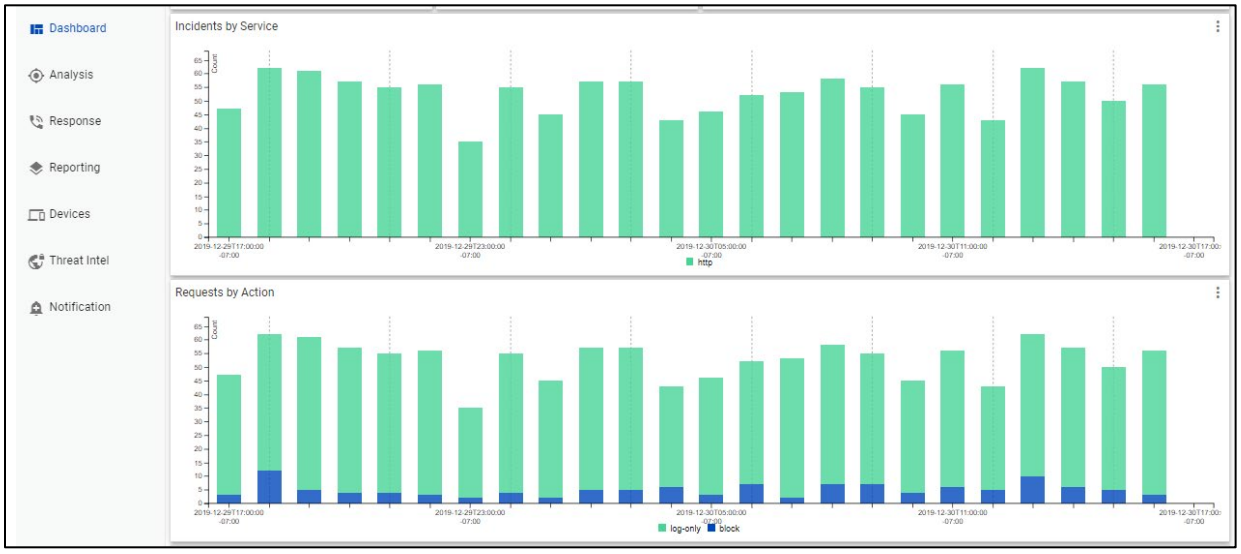
Data Loss Protection (DLP) monitors, prevents, and reports on attempts to send sensitive data outside a customer's organization.

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. The following panels appear:

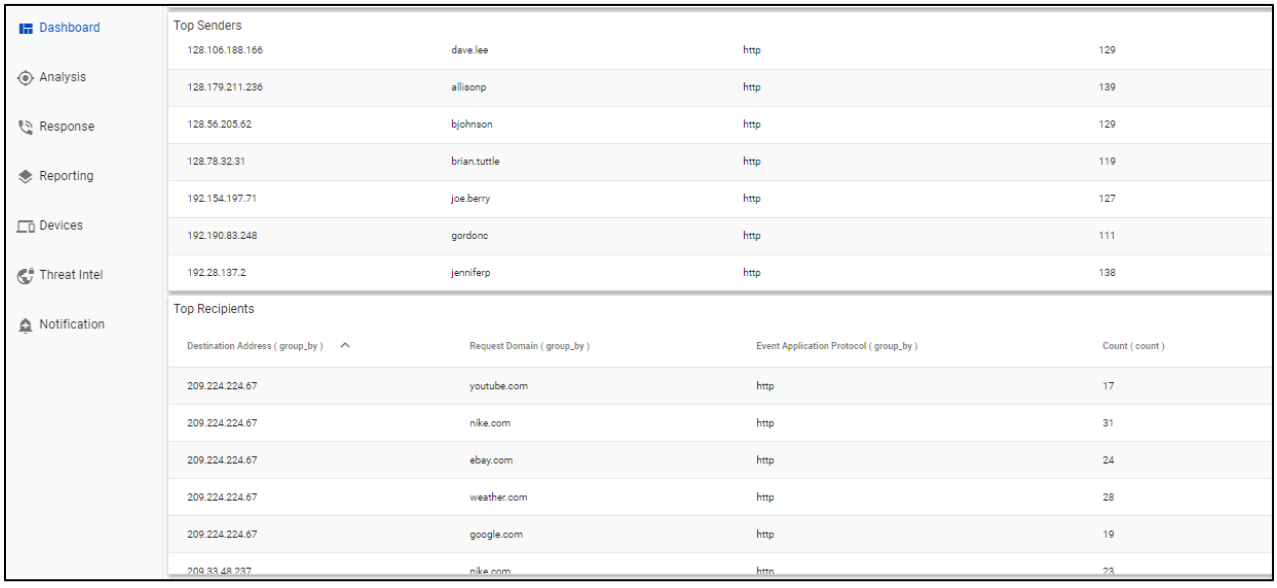
- **Total Blocked Incidents** - The total numbers of blocked DLP incidents.
- **Total Logged Incidents** – The total numbers of logged DLP incidents.
- **Incidents by Type and Action** - A pie chart of incidents by type and status (log-only or blocked) for the selected date range.



- **Incidents by Service** - A bar chart showing incidents by service (http or https) for the selected date range.
- **Requests by Action** - A bar chart of incidents by action (blocked/logged) for the selected date range.



- **Top Senders** - List of top senders of files by source address, source account (user with active-directory integration), event application protocol (http or https), and count.
- **Top Recipient** - List of top recipients by destination address, request domain, event application protocol (http or https), and count.

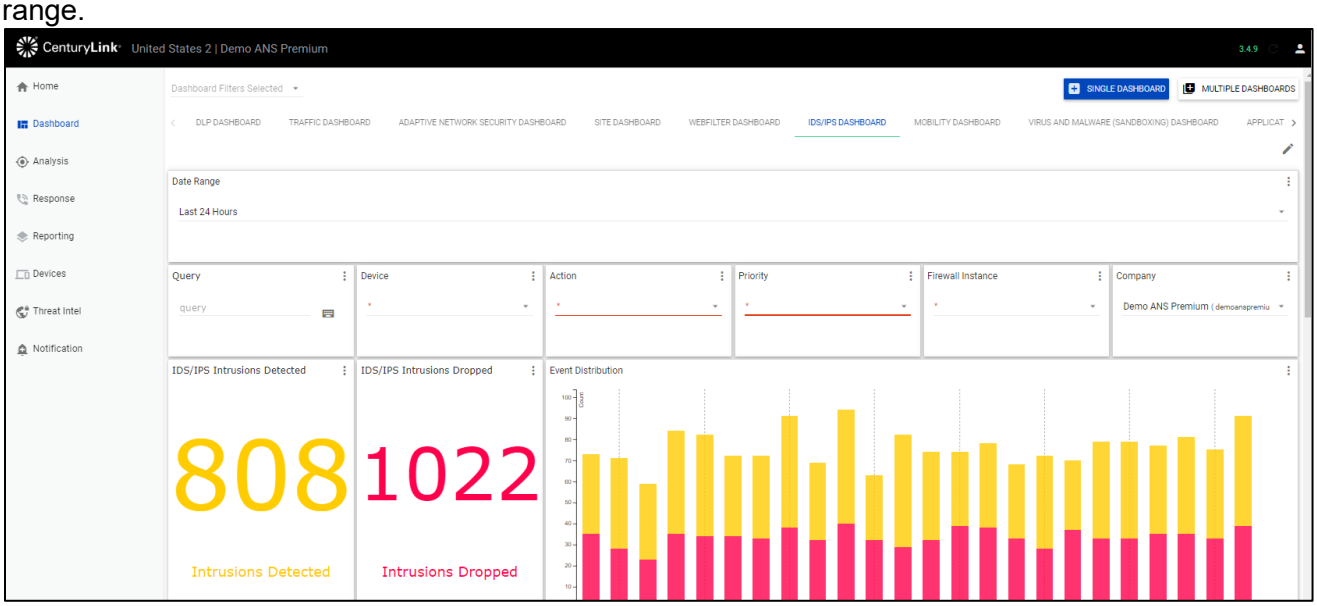


IDS/IPS dashboard

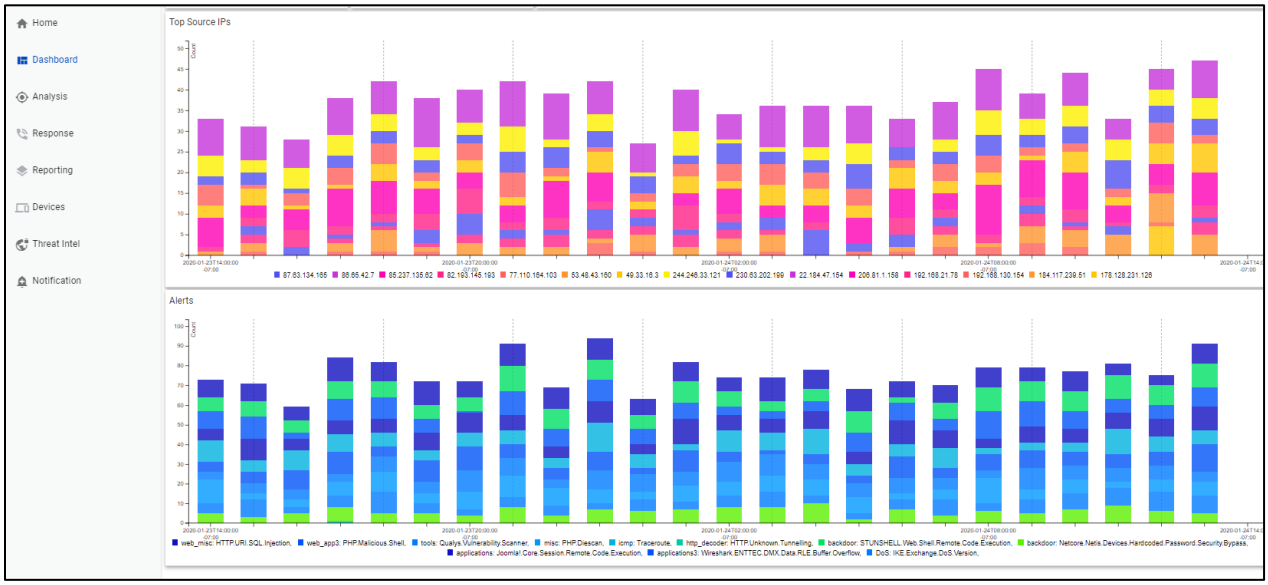
IDS/IPS prevents vulnerability exploits by examining packet content as it passes through the firewall against known signatures to detect, report and block intrusive behavior directed by your firewall policy.

The IDS/IPS dashboard displays logged alerts for intrusion detection and prevention incidents. The following panels appear:

- **IDS/IPS Intrusion Detected and IDS/IPS Intrusions Dropped** - The number of detected and dropped IPS/IDS incidents for the selected date range.
- **Event Distribution** - A bar chart of alerts by status (detected/dropped) for the selected date range.



- **Top Source IPs** - A bar chart of the top 20 IP pairs by number of incidents for the selected date range.
- **Alerts** – A bar chart of the most common alerts for the selected date range.

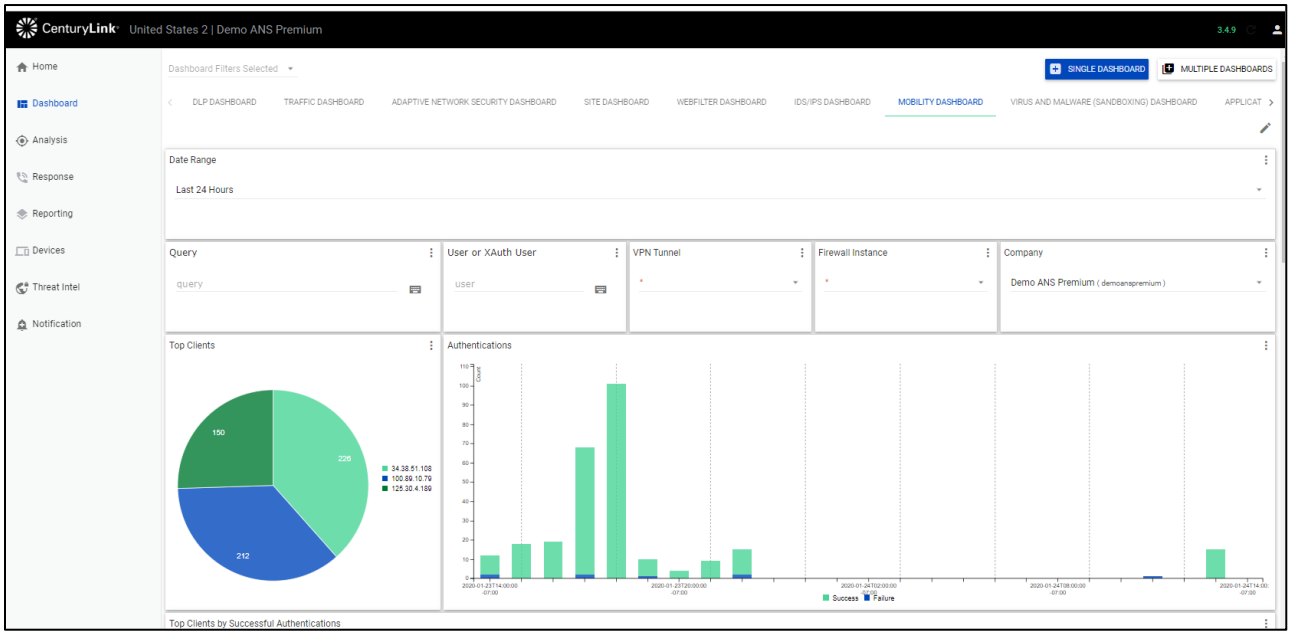


Mobility dashboard

The mobility dashboard summarizes mobility client activity, focusing on logins as well as data volume and session durations. Mobility clients are identified by usernames (with active-directory integration) and geo location (based on remote IP lookup).

The following panels appear:

- **Top Clients** - A pie bar chart showing the top 20 clients by total number of authentication connections made for the selected date range.
- **Authentications** - A bar chart with the top 20 clients by number of authentication connections made by success and failure for the selected date range.



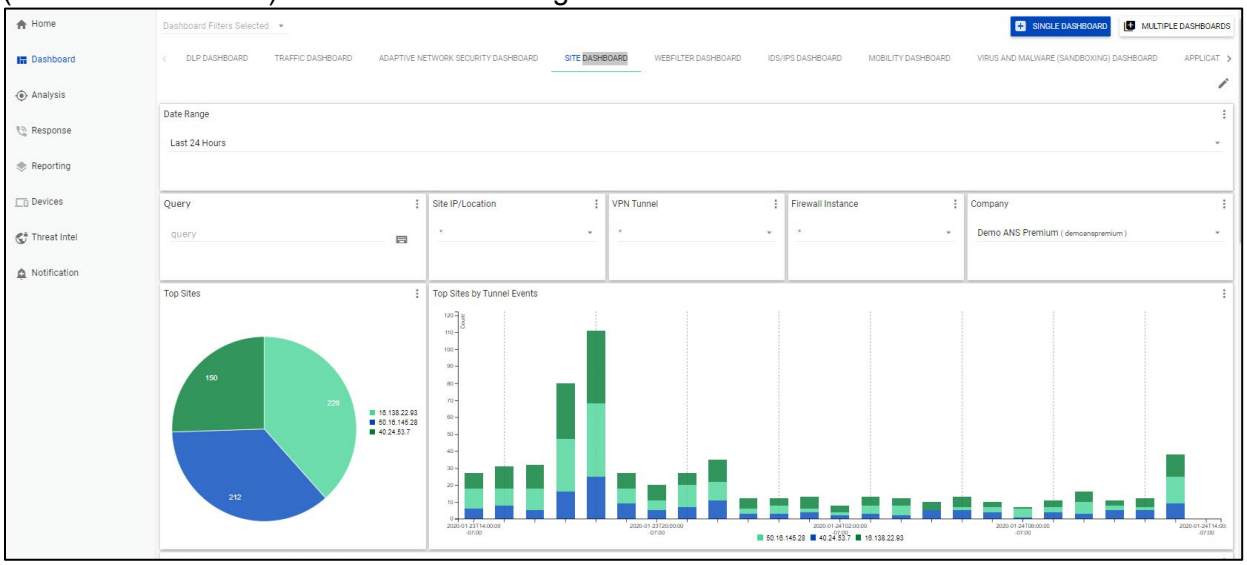
- **Top Clients by Successful Authentications:** A bar chart of the top 20 clients by successful authentications for the selected date range.
- **Top Clients by Failed Authentications:** A bar chart of the top 20 clients by failed authentications for the selected date range.
- **Peak Sustained Throughput of Clients over Time:** A bar chart of the top clients by the sustained bi-directional throughput (the sum of the number of bytes sent from active clients) for both success and failures for the selected date range. Note that throughput is an approximate value based on 10+ minute volume updates.

Site dashboard

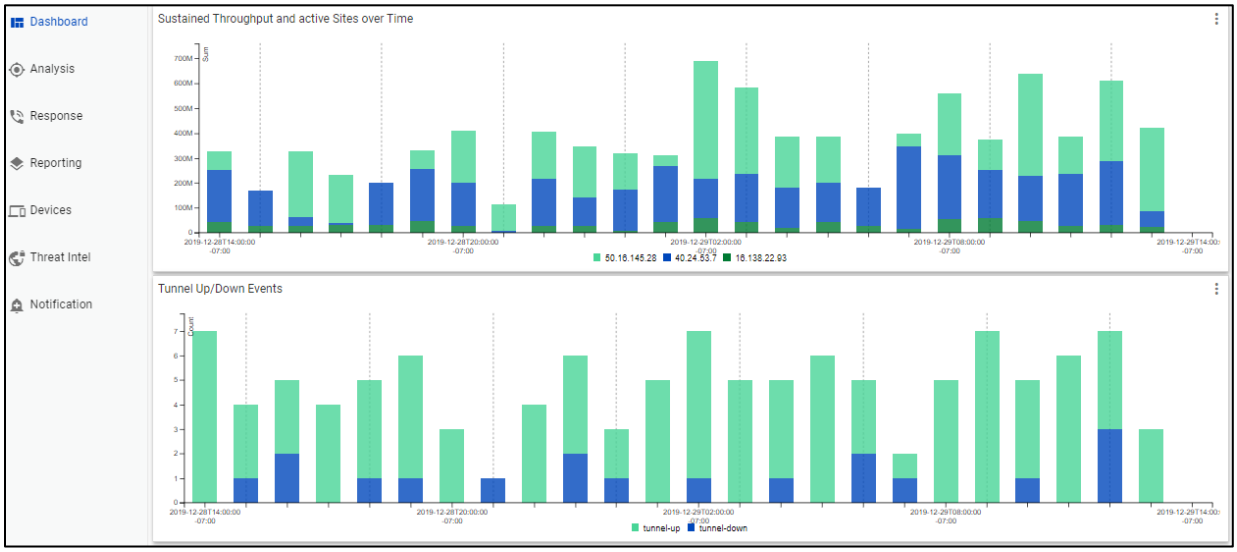
The Site dashboard summarizes traffic from remote access site tunnels.

The following panels appear:

- **Top Sites** - A pie chart with the top sites (up to 20 sites) by volume of tunnel events (distinct connections) seen for the given IP address.
- **Top Sites by Tunnel Events** - A bar chart with the top sites by number of tunnel events (distinct connections) for selected date range.



- **Sustained Throughput and active Sites over Time** - A bar chart with top sites by the sustained bi-directional throughput (the sum of the number of bytes sent from active sites) for the selected date range. Note that throughput is an approximate value based on 10+ minute volume updates.
- **Tunnel Up/Down Events** - A bar chart with top sites showing tunnel up and down events for the selected date range.

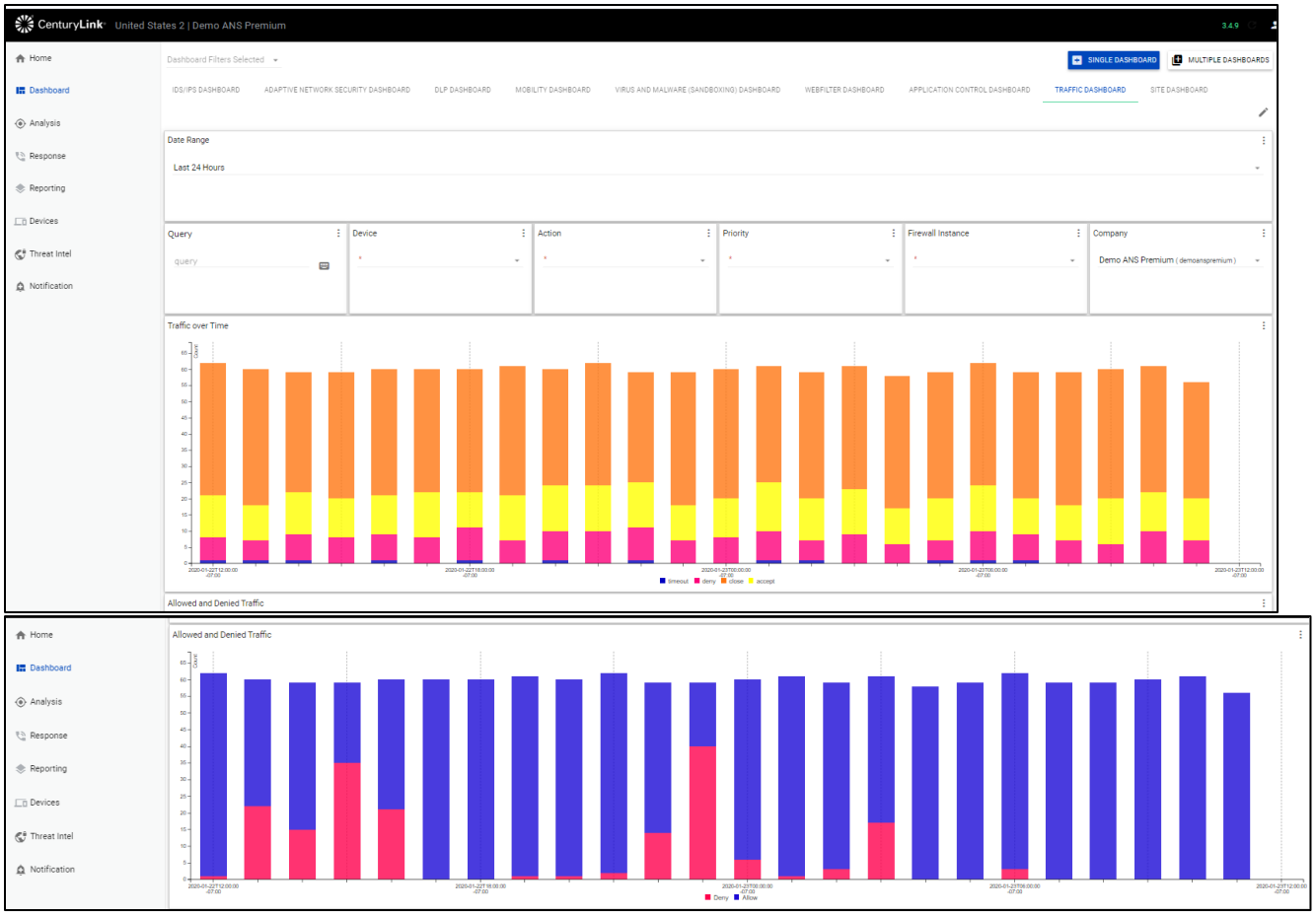


Traffic dashboard

The Traffic dashboard summarizes traffic traversing users firewall via multiple graphics. Traffic data is shown by the number of logged events (traffic flows).

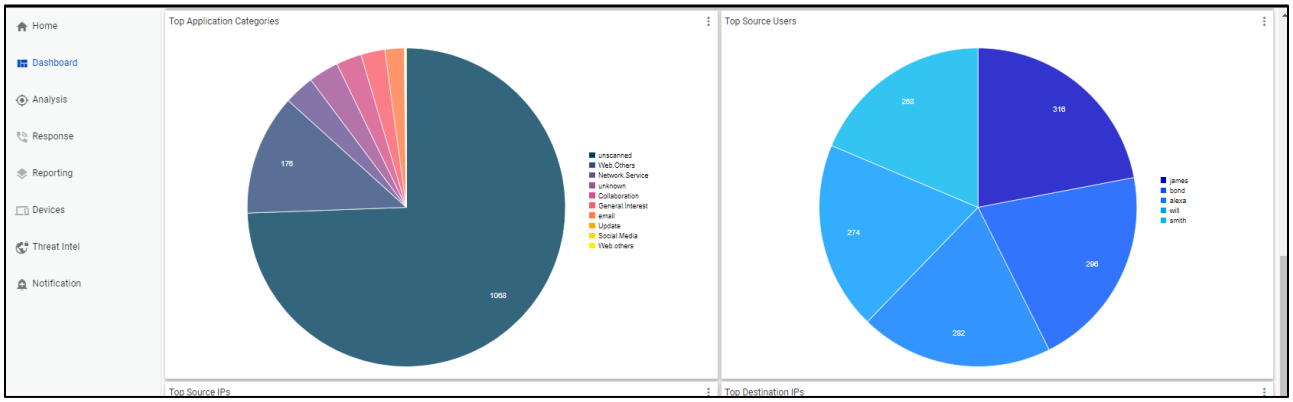
The following panels appear:

- **Traffic over Time –** A bar chart of the total firewall traffic events by action type (accept, close, deny, timeout) for the selected date range
- **Allowed and Denied Traffic** - A bar chart of the allowed and denied firewall traffic events for the selected date range

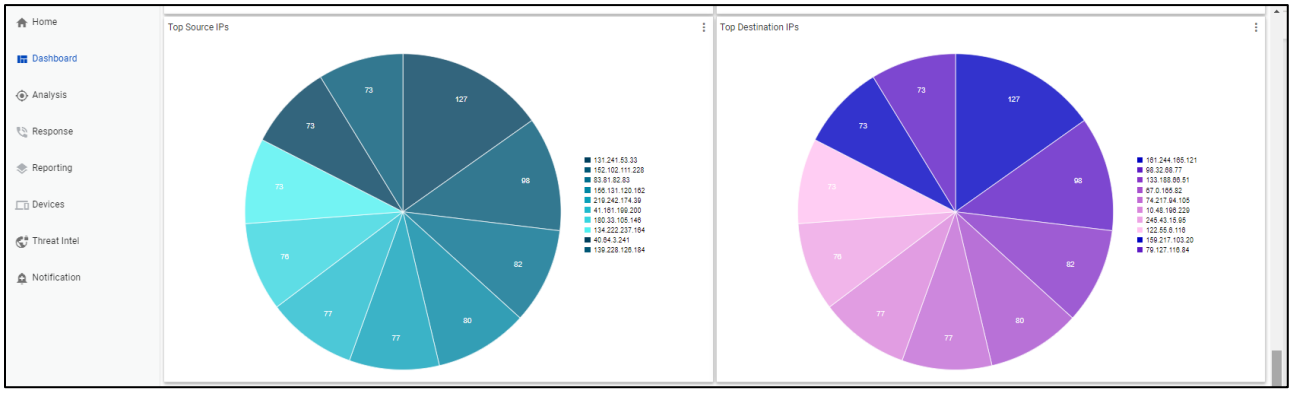


- **Top Application Categories** – A pie chart of the number of connections by top 10 application categories.

- **Top Source Users (**with active-directory integration**)** – A pie charge of the top 10 IP source users for traffic events



- **Top Source IPs** – A pie chart of the number of connections by top 10 application categories by IP address.
- **Top Destination IPs** – A pie charge of the top 10 IP Source users for traffic events.



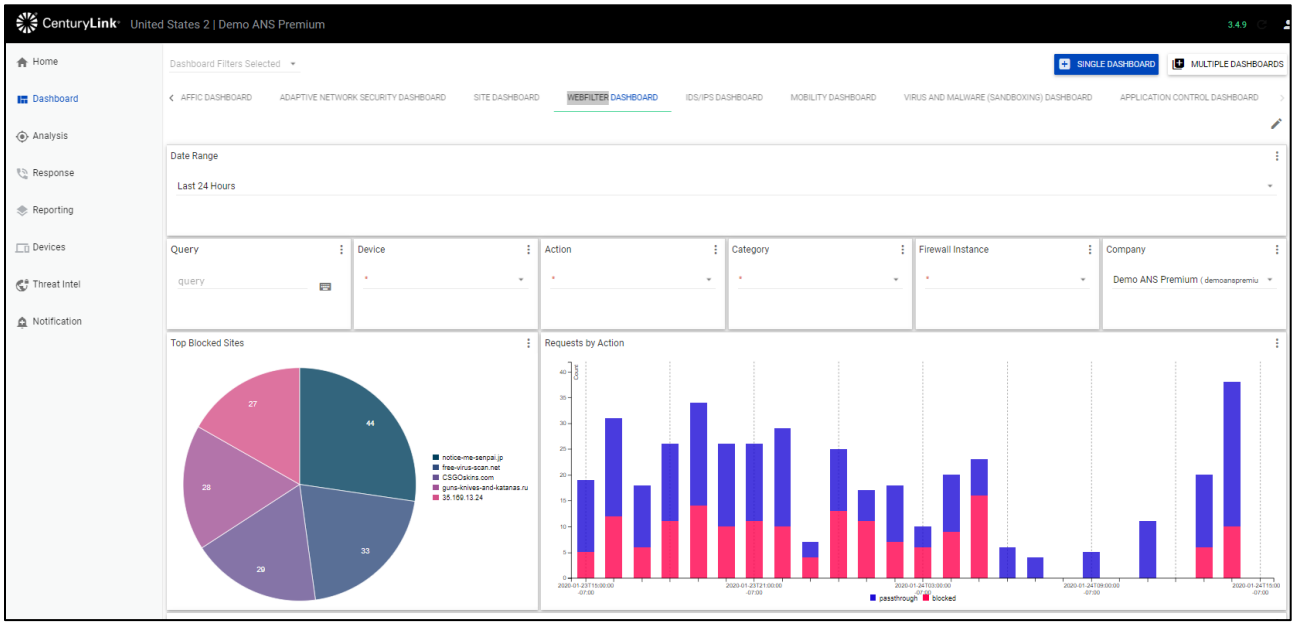
Webfilter dashboard

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

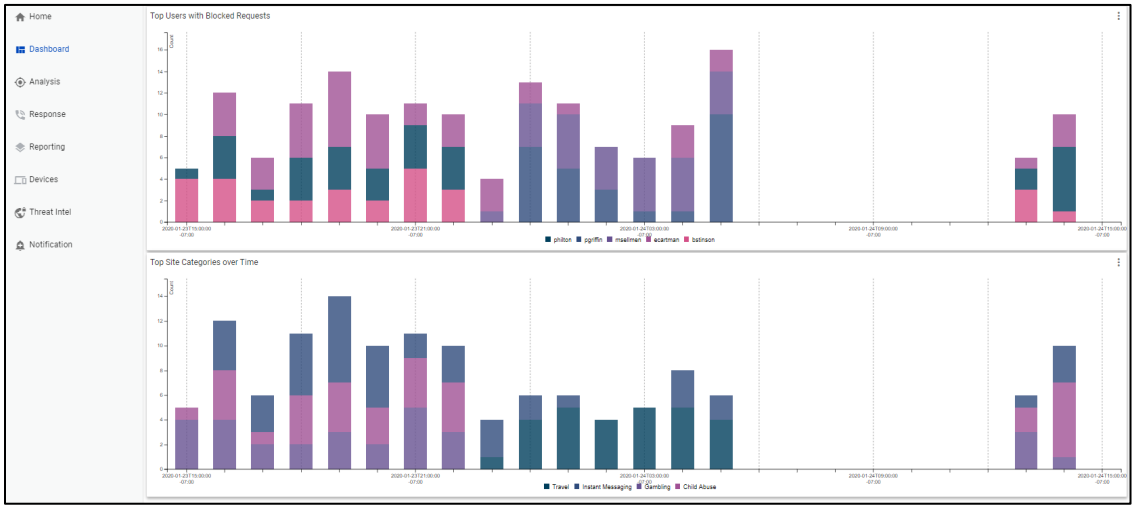
The Webfilter dashboard presents logged events for URL and content-based web-traffic control.

The following panels appear:

- **Top Blocked Sites** – A pie chart showing the top blocked web sites for selected date range.
- **Request by Action** – A bar chart of the number of attempts to websites by action (passthrough, blocked) for selected date range.



- **Top Users with Blocked Requests** - A bar chart of the top 10 users (with active-directory integration) by blocked requests for selected date range.
- **Top Site Categories over Time** – A bar chart of the top web site categories by blocked and passthrough attempts for selected date range.



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.

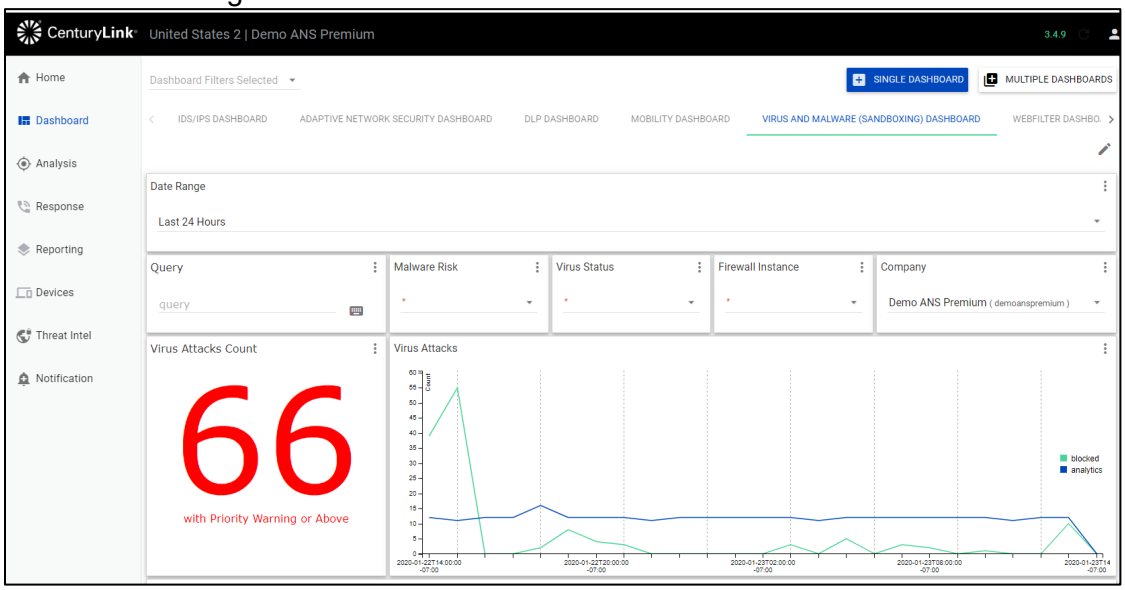
Virus and malware (sandboxing) dashboard

The Virus and Malware dashboard presents logged events for managing files attempting to enter the customers network via HTTP, FTP, IMAP, POP3, SMTP, or NNTP protocols, including known viruses as well as new, yet to be classified threats.

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). 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. Files can be blocked based on both file attachment type or filename suffix, as well as for matching known virus signature patterns.

The following panels appear:

- **Virus Attack Counts** - The number of virus attacks with a priority of warning or higher.
- **Virus Attacks** - A time chart showing virus attacks by status (blocked/analytics) over the selected date range.

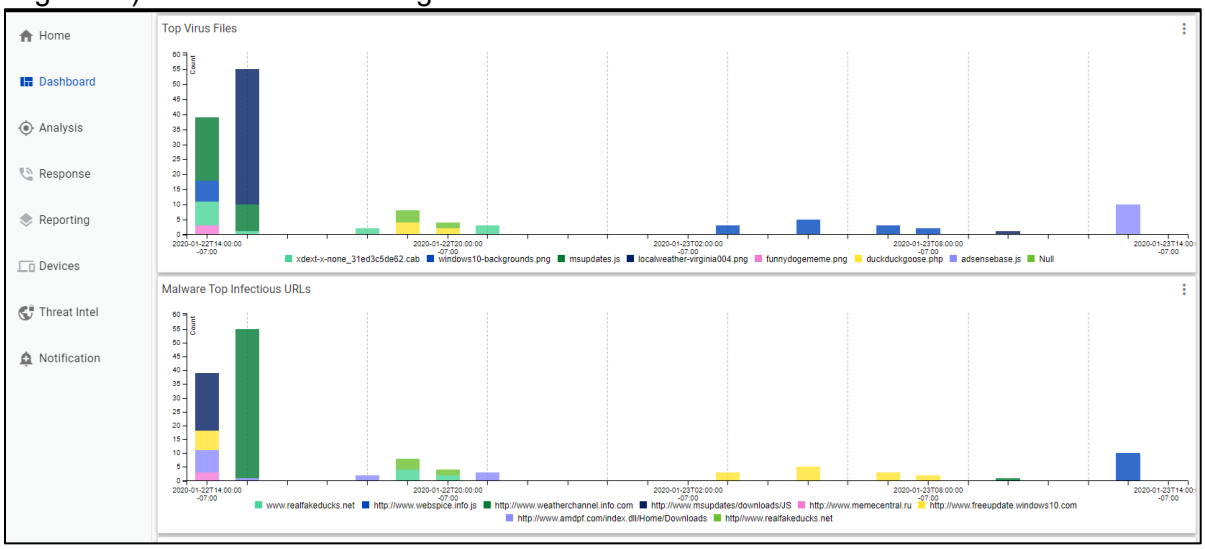


1. **Malware and Scanning Activity Table** - A table listing of virus attacks by virus name, virus status (blocked/analytics), source address, count for the selected date range.

2. **Malware and Scanning Activity** - A bar chart of malware or scanning activity by malware risk for the selected date range.

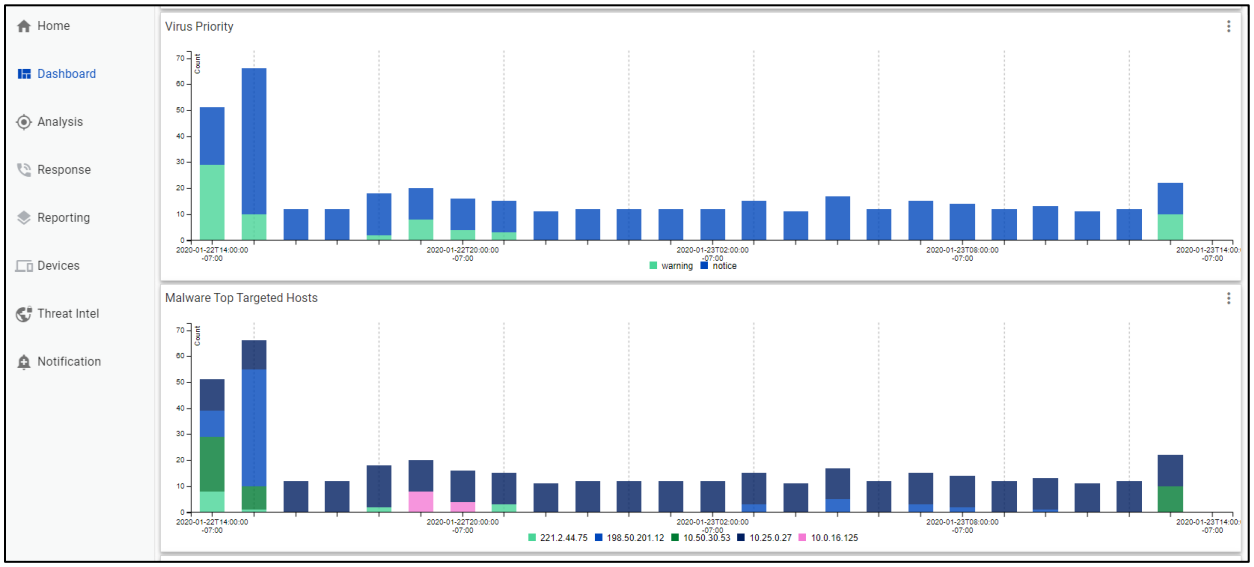
3. **Top Virus Files** - A bar chart of the top 10 virus files for the selected date range.

4. **Malware Top Infectious URLs** - A bar chart of the top infected URLs (from which malware originated) for selected date range.

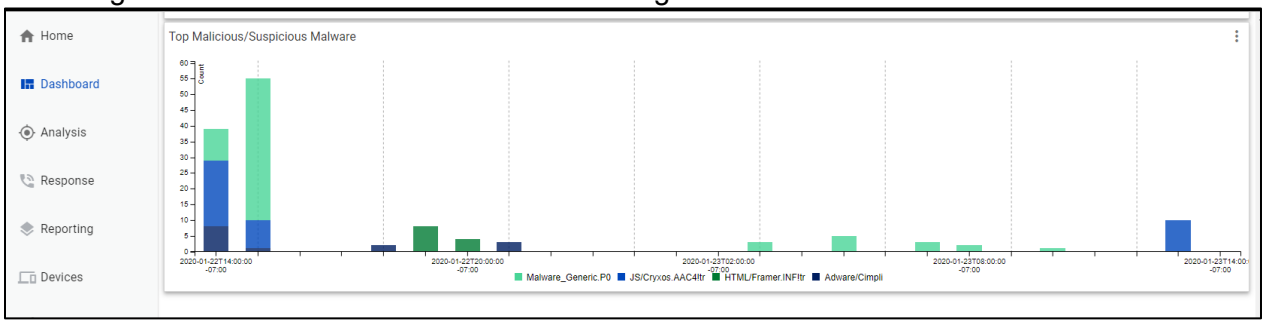


5. **Virus Priority** - A bar chart of the virus priority rating for selected date range.

6. **Malware Top Targeted Hosts** - A bar chart of the top malware hosts (from which malware originated) for selected date range.



7. **Top Malicious/Suspicious Malware** - A bar chart of the top malware files (based on the name Fortinet gives to the malware for selected date range.

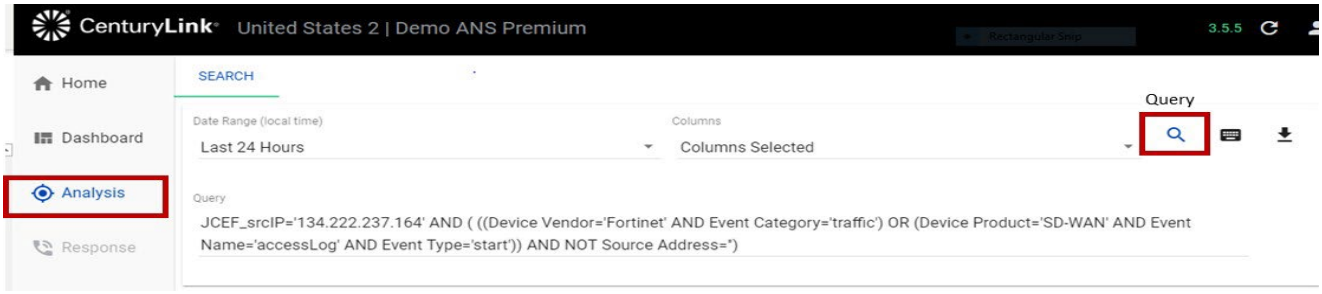


Analysis

The Analysis menu item enables users the ability to view logs by flexible query filters.

To create a query from a Dashboard:

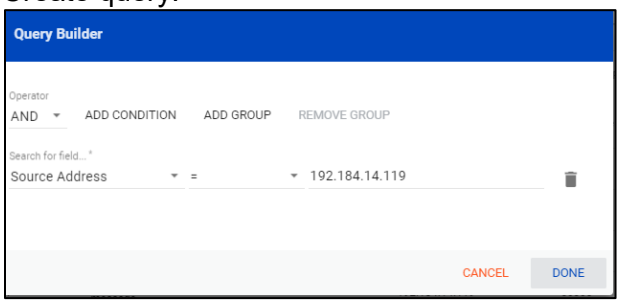
1. Double click on a Dashboard data item
2. This will bring you to the **Analysis** page with query detail auto-populated from the Dashboard
3. Click query search button.



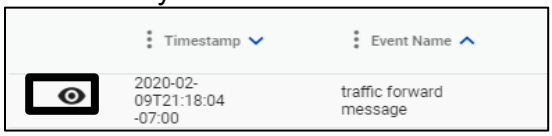
To create a custom query:

1. From the left menu, select **Analysis**.

2. Select the query builder icon on the top right.
3. See the Glossary section for query field definitions.
4. Create query.



5. Select the eyeball icon on the left to drill down on the query results



6. Select the download button on the top right to export query results.

Reporting

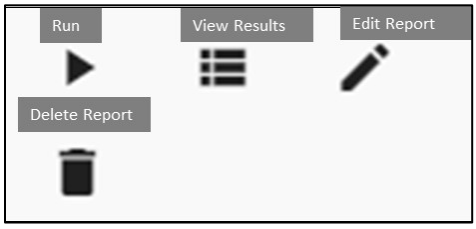
The Reporting section enables a user to create and export a standard default report or a custom report for Adaptive Network Security services.

The Adaptive Network Security default report templates include:

- **Firewall: Application Control Report**—provides details about the application protocols being used as reported by on FortiGate devices for the Firewall Services.
- **Firewall: DLP Report**—provides details about DLP detections including policies and files as reported on FortiGate devices for the Firewall Services.
- **Firewall: IDS/IPS Report**—provides details about intrusion detection and prevention events as reported on FortiGate devices for the Firewall Services.
- **Firewall: Mobility Report**—provides details about remote mobility access on FortiGate devices for the Firewall Services.
- **Firewall: Site Report**—provides details about remote site access on FortiGate devices for the Firewall Services.
- **Firewall: Traffic Report**—provides details about traffic and connection events as reported on FortiGate devices for the Firewall Services.
- **Firewall: Virus Report**—provides details about virus and malware events as reported on FortiGate devices for the Firewall Services.
- **Firewall: Webfilter Report**—provides details about web traffic and filtered web content as reported on FortiGate devices for the Firewall Services.

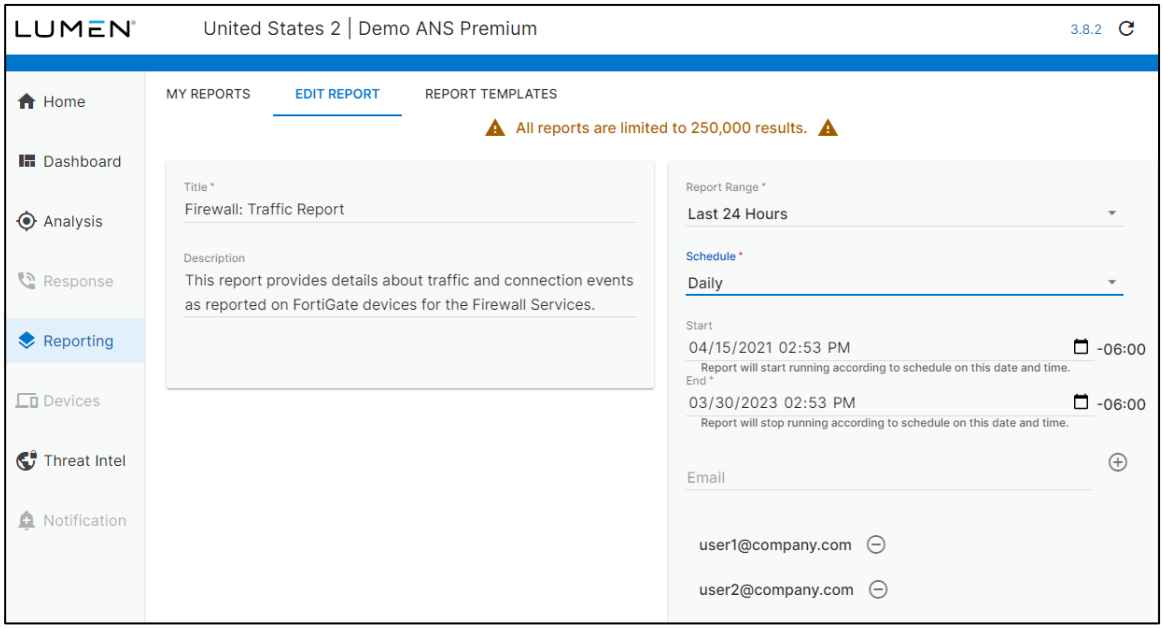
Reporting Tab Functions include:

- **My Reports**—listing of reports you've built
- **Build Reports**—allows you to create reports - either custom reports or from default standard report templates.
    - Full Page Table Report Layout & Standard Log Data are the pre-defined reports.
    - Summarized log data allows you to customize reports by Aggregate List, Average, Count, Group By, Maximum, Minimum or Sum values.
    - Scroll to the bottom and click Save Report
- **Report Templates**—list of available default standard templates. You must go to Build Reports to create the report.
- Icons are used to Run report, View Results, Edit report and Delete report.



Users can also schedule a report on the **My Reports** tab to send to other users:

1. Select report in the **My Reports** tab (e.g., Firewall: Traffic Report).
2. Select **Edit Report** (pencil icon).
3. Update report range, schedule, start and end date.
4. Identify emails where the report will be sent.
5. Scroll to the bottom.
6. Select **Save Report**.



7.

Mobility and Site Report Data field definitions

Column	Description
Event Receipt Time	Date/time when log data was recorded
Device Host	Virtual firewall instance identifier
Device Serial Number	Adaptive Network Security gateway location of firewall device
Device Action	Status of the session
Event Message	Log message
Custom String 6	Outcome of the log event action: success or failure
Event Severity	Estimated severity of the event that caused the log message See appendix A for definitions.
Custom String 2	XAuth username (active-directory integration) – If this is N/A this is a site
Custom String 3	XAuth group name (active-directory integration)
Custom String 1	IPsec VPN tunnel name
Source/Destination Address	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)
Source Translated Address	Translated IP address (when available)
Source Bytes	Bytes sent from firewall instance to remote site across the VPN tunnel
Destination Bytes	Bytes received at firewall instance from remote site across the VPN tunnel
Request Result	Result
Event Signature ID	10-digit log identifier, starting with 0101

Application Control Report Data field definitions

Column	Description
Event Receipt Time	Date/time when log data was recorded
Device Host	Virtual firewall instance identifier
Device Serial Number	Adaptive Network Security gateway location of firewall device
Custom String 1	Application control profile name
Request Category	Application category
Request Application	Application name
Request Domain	The host name of a URL
Source Account	Username (active-directory integration)
Source Group	Group name (active-directory integration)
Event Severity	Estimated severity of the event that caused the log message. See appendix A for definitions.
Device Action	Security action performed, including pass, block, reject, reset, monitor
Event Application Protocol	The name of the application-layer protocol used by the traffic (HTTP, HTTPS, DNS, TCP, UDP)
Source/Destination Address	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)
Event Name	Log message
Request URL	URL address

DLP Report Data field definitions

Column	Description
Event Receipt Time	Date/Time when log data was recorded
Device Host	Virtual firewall instance identifier
Device Serial Number	Adaptive Network Security gateway location of firewall device
Source Account	Username (active-directory integration)
Source Group	Group name (active-directory integration)
Device Action	Security action performed, including pass, block, reject, reset, monitor
Event Severity	Estimated severity of the event that caused the log message. See appendix A for definitions.
Source/Destination Address	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)
Device Action	Security action performed, including pass, block, reject, reset, monitor
Event Application Protocol	The name of the application-layer protocol used by the traffic (HTTP, HTTPS, DNS, TCP, UDP)
Source Email	Source email
Destination Email	Destination email
File Type	File type
File Name	File name
File Size	File size in bytes
Filter Type	DLP filter type (credit card, SSN)
Custom String 2	DLP filter category
Event Message	Log message
Request URL	URL address

IDS/IPS Report Data field definitions

Column	Description
Event Receipt Time	Date/time when log data was recorded
Device Serial Number	Adaptive Network Security gateway location of firewall device
Device Host	Virtual firewall instance identifier
Source Account	Username (active-directory integration)
Source Group	Group name (active-directory integration)
Custom String 6	Status based on security action performed (dropped, detected)
Event Severity	Estimated severity of the event that caused the log message. See appendix A for definitions.
Custom String 3	Severity of the attack (info, low, medium, high, critical)
Event Message	Log message
Request Domain	Host name of URL
Event Sub Type	Sub type for log message
Event Application Protocol	The name of the application-layer protocol used by the traffic (HTTP, HTTPS, DNS, TCP, UDP)
Source/Destination Address	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)
Custom String 7	References the known threat used to log the event

Traffic Report Data field definitions

The traffic data comes with many events, which should be considered when selecting longer time frames. It is best to keep report windows to under four hours. The report pages don't support sampling rates as this is the place where a user looks for the actual log data.

Column	Description
Event Receipt Time	Date/time when log data was recorded
Device Serial Number	Adaptive Network Security gateway location of firewall device
Device Host	Virtual firewall instance identifier
Source Account	Username (active-directory integration)
Source Group	Group name (active-directory integration)
Event Severity	Estimated severity of the event that caused the log message. See appendix A for definitions.
Custom String 6	The status of the session: deny, start, close (allowed), timeout (allowed)
Event Application Protocol	The name of the application-layer protocol used by the traffic (HTTP, HTTPS, DNS, TCP, UDP)
Request Application	Application name
Request Category	Application category
Source/Destination Address	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)
Source Bytes	Sent bytes in MB
Destination Bytes	Received bytes in MB
Event Bytes	Sum of sent and received bytes (in MB)
Event Session ID	The name of the server policy governing the traffic causing the log message

Virus Report Data field definitions

Column	Description
Event Receipt Time	Date/time when log data was recorded
Device Serial Number	Adaptive Network Security gateway location of firewall device
Device Host	Virtual firewall instance identifier
Source Account	Username (active-directory integration)
Source Group	Group name (active-directory integration)
Event Application Protocol	The name of the application-layer protocol used by the traffic (HTTP, HTTPS, DNS, TCP, UDP)
Request User Agent	User agent
Custom String 6	Status based on security action performed, including analytics, blocked, monitored, pass through
Event Severity	Estimated severity of the event that caused the log message. See appendix A for definitions.
Event Sub Type	Sub type of the log message
Event Message	Log message
Source/Destination Address	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)
Request URL	URL address
File Name	File name

Webfilter Report Data field definitions

Column	Description
Event Receipt Time	Date/time when log data was recorded
Device Serial Number	Adaptive Network Security gateway location of firewall device
Device Host	Virtual firewall instance identifier
Source Account	Username (active-directory integration)
Source Group	Group name (active-directory integration)
Event Severity	Estimated severity of the event that caused the log message. See appendix A for definitions.
Device Action	Security action performed, including pass, block, reject, reset, monitor
Custom String 6	Status based on security action performed (passthrough, blocked)
Event Sub Type	Sub type of the log message (webfilter type)
Request Category Description	Web category description
Event Application Protocol	The name of the application-layer protocol used by the traffic (HTTP, HTTPS, DNS, TCP, UDP)
Event Direction	Outgoing to the internet.
Source/Destination Address	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)
Request Domain	Host name of URL
Request URL	URL address
Source Bytes	Sent bytes
Destination Bytes	Received bytes

Appendix A: Event Severity definitions

The following table describes the event severity, which is the estimated severity causing 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.