Lumen® Managed Firewalls

Security Solutions portal (powered by Lumen)
User guide | February 2022

For Adaptive Network Security, Managed Premises Fortinet Firewalls, MSS Cloud, Secure Access

LUMEN®

Table of contents

Lumen Security Solutions Reporting

The Lumen Security Solutions Reporting (powered by Lumen) portal provides near real-time dashboard, reports of log events, analysis, threat-visualization, and rapid threat defense (Adaptive Network Security only) for the following Lumen managed firewall security services:

- Adaptive Network Security
- Managed Premises Firewalls (Fortinet)
- MSS Cloud
- Secure Access

Detailed firewall policies files are available on the Security Solutions Analytics landing page.

> **Note:** To access the Security Solutions Reporting (powered by Lumen) portal and firewall policies, sign in to Control Center using two-factor authentication.

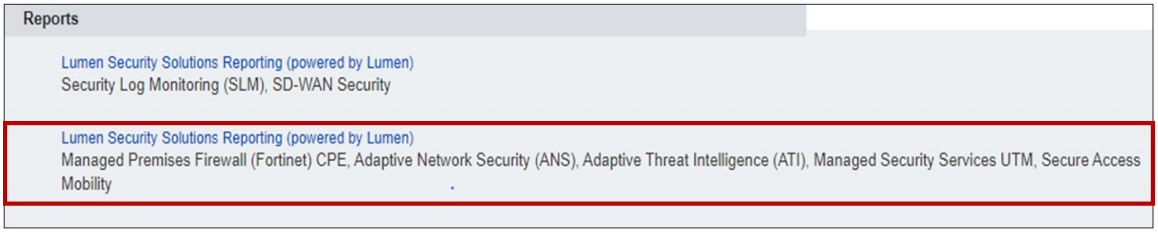
Support contacts

Please see https://www.lumen.com/help/en-us/security-solutions.html for more information.

Accessing the Lumen customer portal

Learn how to sign in to Control Center—the Lumen customer portal.

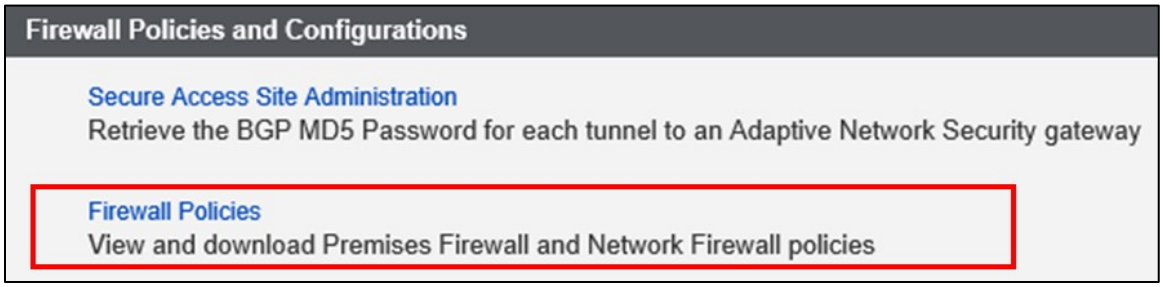
Select the second **Lumen Security Solutions Reporting (powered by Lumen)** link.



Viewing and downloading firewall policies

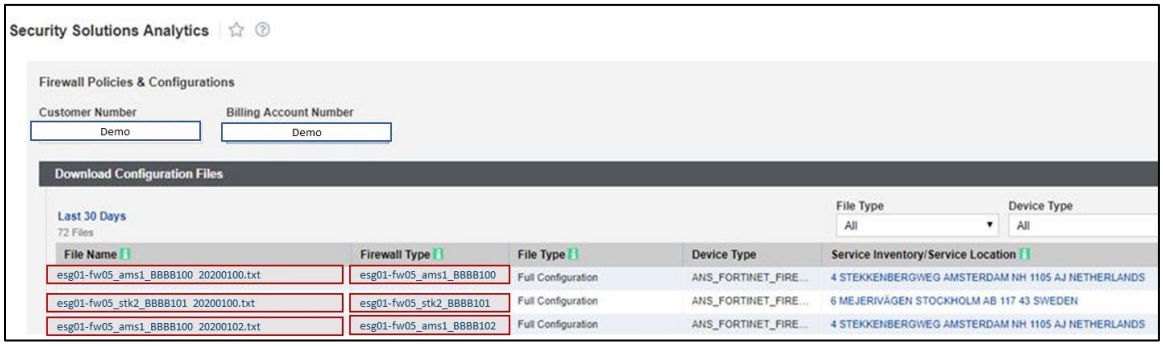
1. Sign in to Control Center.
2. Click **Monitoring**, then click **Security Solutions Analytics**.

3. To view and download Adaptive Network Security firewall policies files, scroll down to **Firewall Policies and Configurations** > **Firewall Policies**.



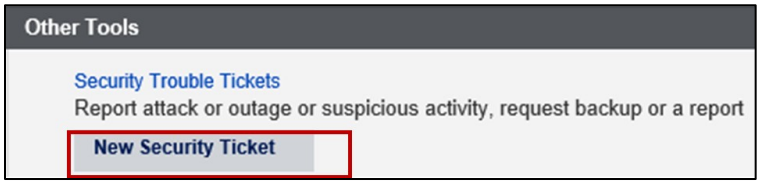
Adaptive Network Security and Managed Premises firewall policies

1. The Adaptive Network Security and Managed Premises 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 Reporting portal

The Lumen Security Solutions Reporting portal for Managed Firewall set of services includes:

- Adaptive Network Security
- Managed Premises Firewall (Fortinet)
- MSS Cloud
- Secure Access

The Lumen Security Solutions Reporting portal has a common layout and user interface for log events and capabilities represented in the Dashboard, Events, Security Posture (to set a security threat score with Rapid Threat Defense) on the left menu item tabs:

- **Dashboard**—Displays summary view of the set of critical indicators for service features. User can download reports based on dashboard.
- **Events**—Query capability to search logs based on a user defined set of filters
- **Incidents**—Displays set of interactions with malicious IP sites and domains based on near real-time threat intelligence indicators from Black Lotus Labs. User can view incident details and obtain automated analyst guidance. View enabled with Basic and Premium service levels.
- view incident details and to and obtain guidance on incidents identified on the Firewall service.
- **Reporting**—Enables user to create a report from a dashboard.
- **Security Posture**—Enables admin user to identify a security posture to set up automated deployment of countermeasures whenever new malicious entities are discovered by Black Lotus Labs™—the Lumen cyber threat intelligence team.

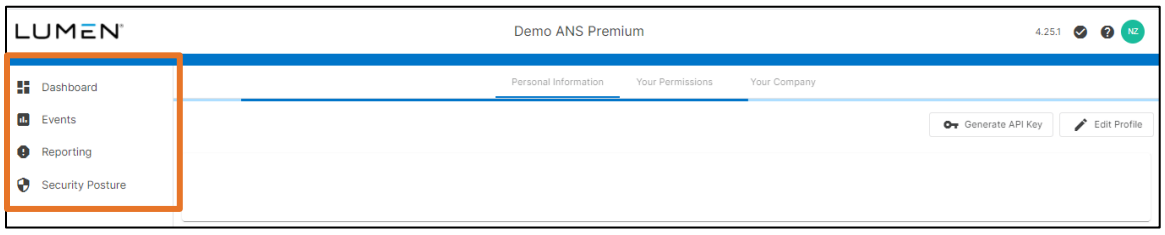
Key capabilities with top-right icons are

Release Notes

Incidents Assigned to you

Knowledge Base and Support

You will see a blank display and need to select a menu item on the left side.



Common filters and customization

Common controls across the Firewall dashboards are:

- **Date Range**—interval for viewing search results. Click the **Apply** button after selection.
- **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.
- **Firewall Type**—type of firewall, network firewall or premises firewall.
- **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.

Rapid Threat Defense (Security Posture)

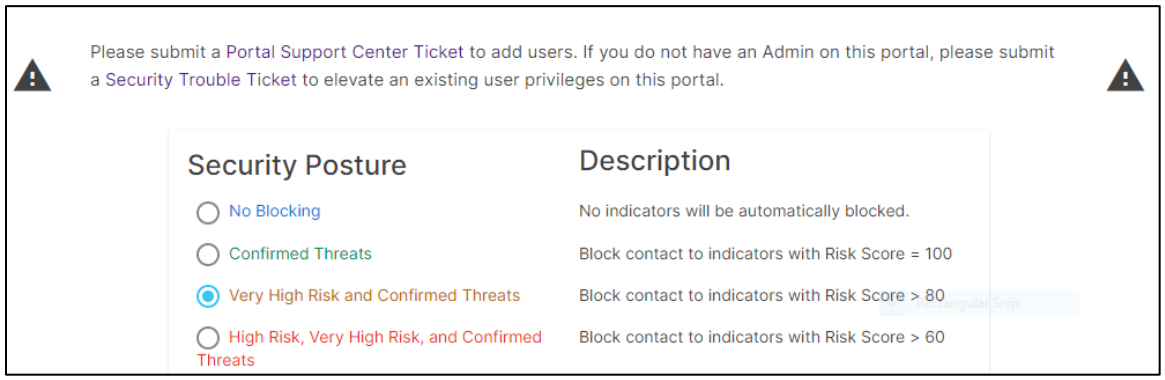
Rapid Threat Defense allows you to automatically detect and respond to threats for Adaptive Network Security Premium service only.

You 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.

To set security posture with Rapid Threat Defense, **Security Posture** menu item (left side).

> **Note:** You must have an admin role on the Lumen Security Solutions portal to set security posture or set Allow/Block IP v4 Address. If you need admin role privilege, submit a security trouble ticket to elevate your privileges to admin role.

The selected security posture risk score selections are:



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 (**Support** > **Security Repair 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 Firewall dashboards are a summary view of critical indicators with Adaptive Network Security, Managed Premises Firewall (Fortinet), MSS Cloud, Secure Access services. You can filter on Firewall Type and Firewall Device to determine the product offer:

- Adaptive Network Security → “esg” devices & “network firewall” type.
- MSS Cloud, Secure Access → “nsd” and “esg” devices & “network firewall” type.
- Managed Premises Firewall (Fortinet) → to “GM” devices & “premises firewall” type.

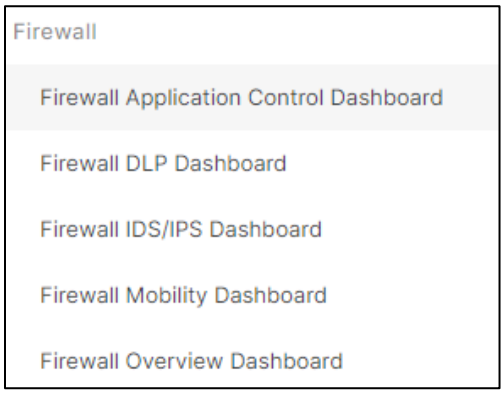
Default set of Adaptive Network Security service dashboards are:

- **Firewall Overview Dashboard**—displays the summary of important metrics from all features in distinct panels.
- **Firewall 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.
- **Firewall 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.
- **Firewall 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.
- **Firewall 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.
- **Firewall 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.
- **Firewall Traffic Dashboard**—displays summary of traffic allowed and denied by firewall policy. Reports show how traffic was managed in response to such policies.
- **Firewall 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.
- **Firewall 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

1. For initial set up, select **Create New Dashboard**.

   A list of Firewall Dashboard Templates appears.



2. Create the appropriate dashboards based on the features you have eanbled on the Firewall service. The minimum common firewall dashboards to create are:
   - Firewall Overview dashboard
   - Firewall IDS/IPS dashboard
   - Firewall Traffic dashboard

3. To adjust panel display, you can select the lock/unlock icon to adjust a widget display to fit your screen.

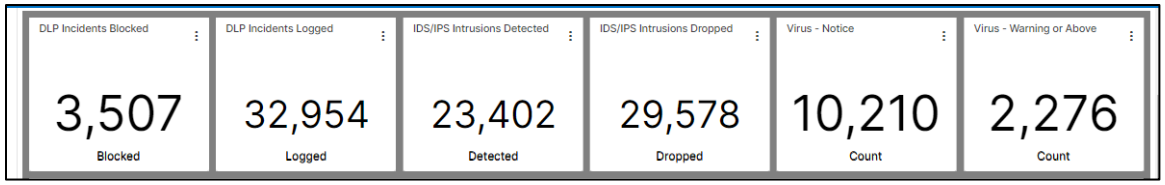
Firewall Overview Dashboard

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

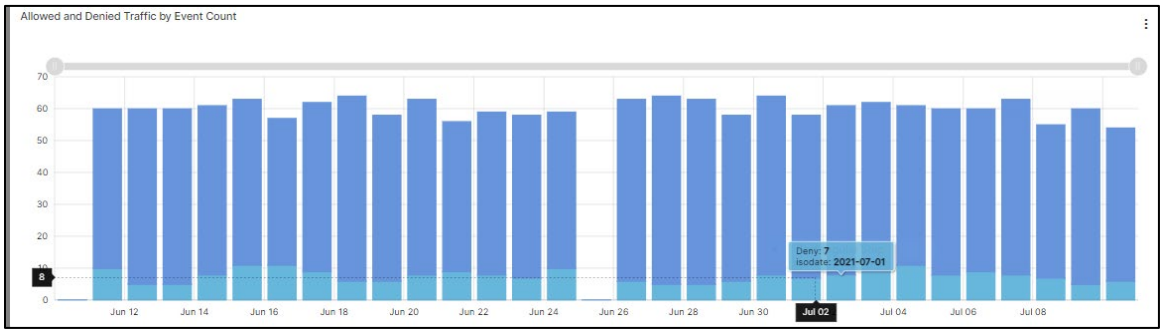
In full configuration, the following panels appear:

- **DLP Incidents Blocked and DLP Incidents Logged**: The number of blocked and logged DLP incidents for the selected date range
- **IDS/IPS Intrusion Detected and IDS/IPS Intrusions Dropped**: The number of detected and dropped IPS/IDS incidents for the selected date range.
- **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.

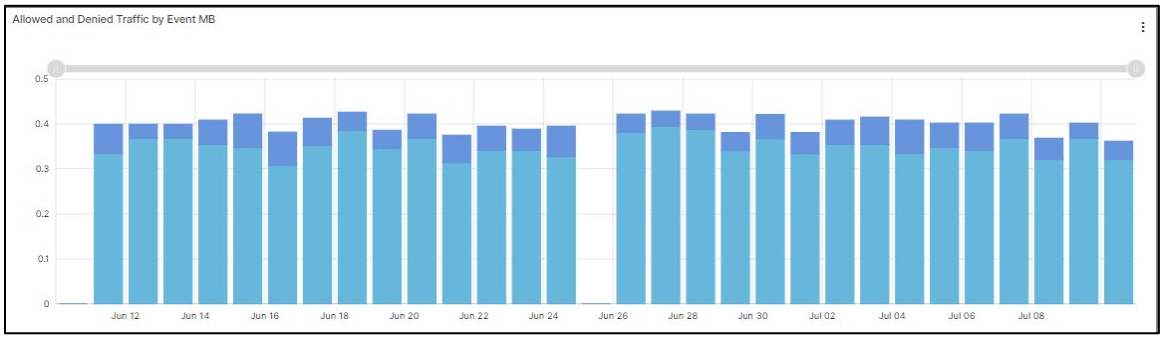
If you have not configured Data Leak/Loss Protection (DLP) or AntiMalware (Virus), these will appear with a “0” value.



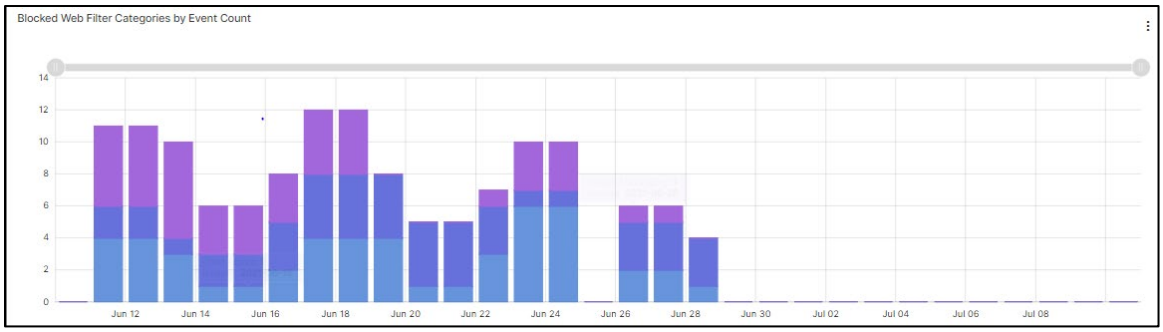
- **Allowed and Denied Traffic by Event Count**: A bar chart of the allowed and denied firewall traffic events for the selected date range.



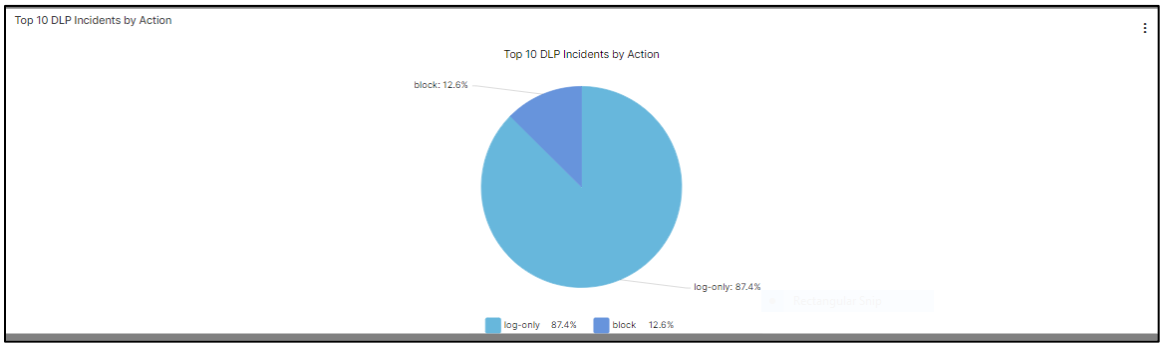
- **Allowed and Denied Traffic by MB**: A bar chart of the allowed and denied firewall traffic by volume (MB) for the selected date range.



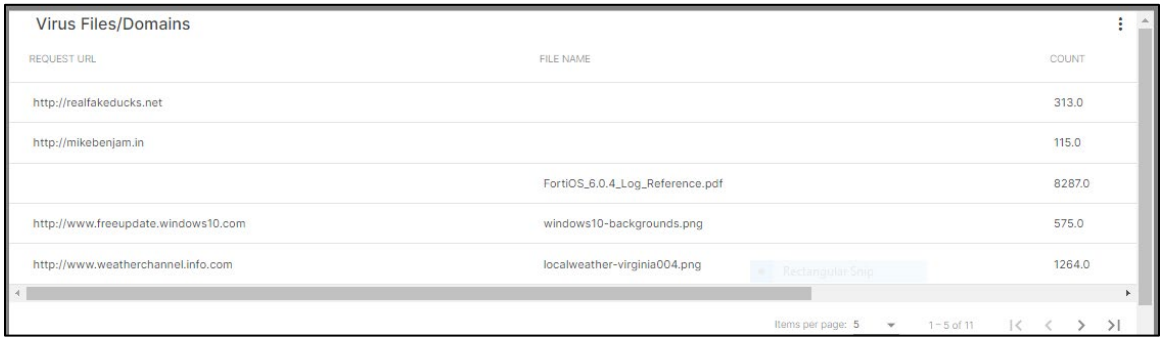
- **Blocked Web Filter Categories by Event Count**: A bar chart of the top 10 blocked web filter categories and count of the number of attempts to web sites that match the category for the selected date range.



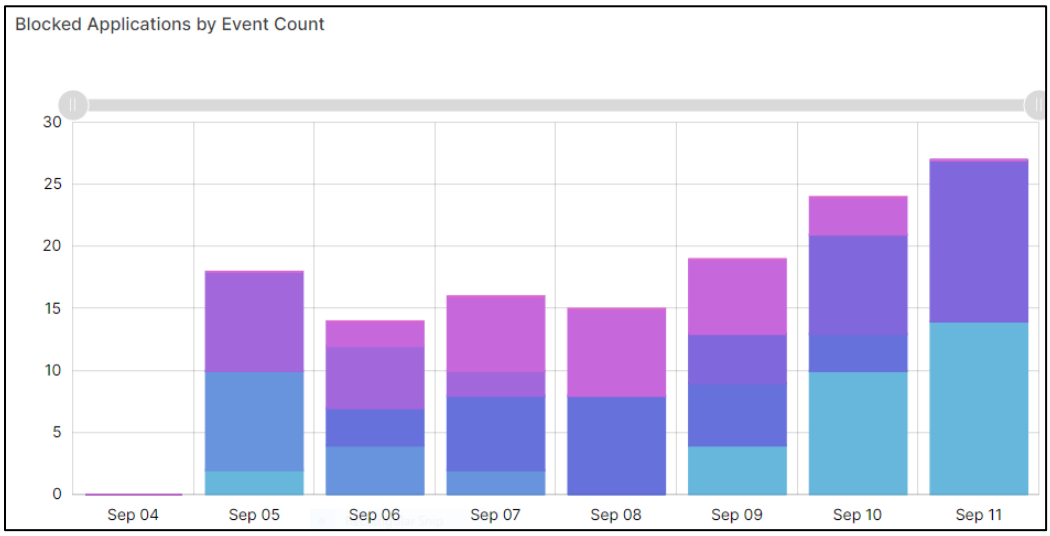
- **Top 10 DLP Incidents by Action**: A pie chart showing the type of data detected or block for selected date range.



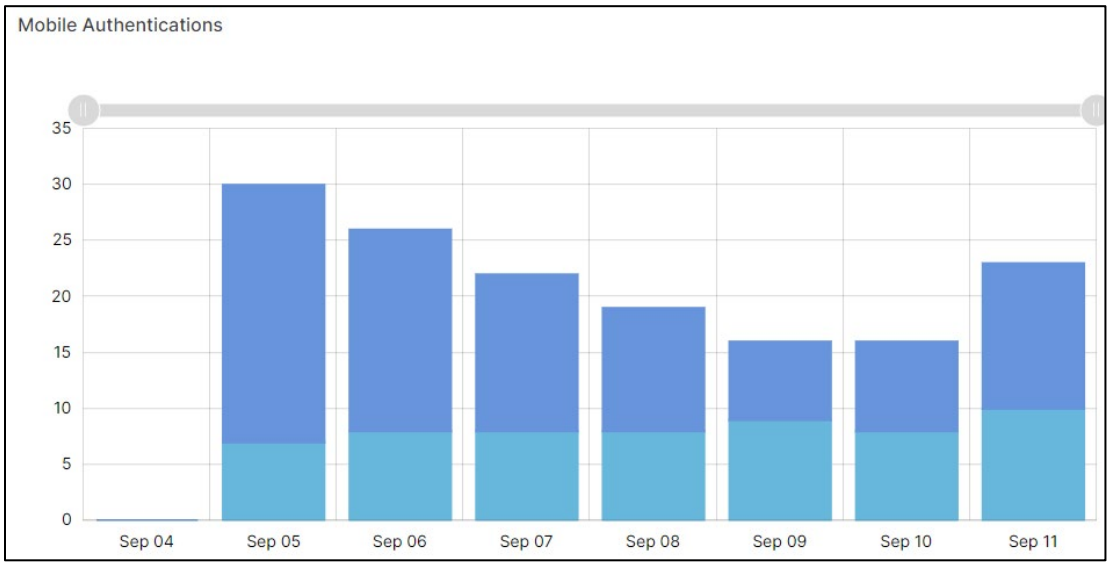
- **Top Virus Files/Domains**: A list of the most frequently detected virus files for the selected date range.



- **Blocked Applications by Event Count**: A bar chart of the top blocked and host combinations and count of attempts by application that match the category identified in the firewall policy for the selected date range.



- **Mobile Authentications**: A bar charge of the number of failed and successful mobility access authentication attempts fort the selected date range.

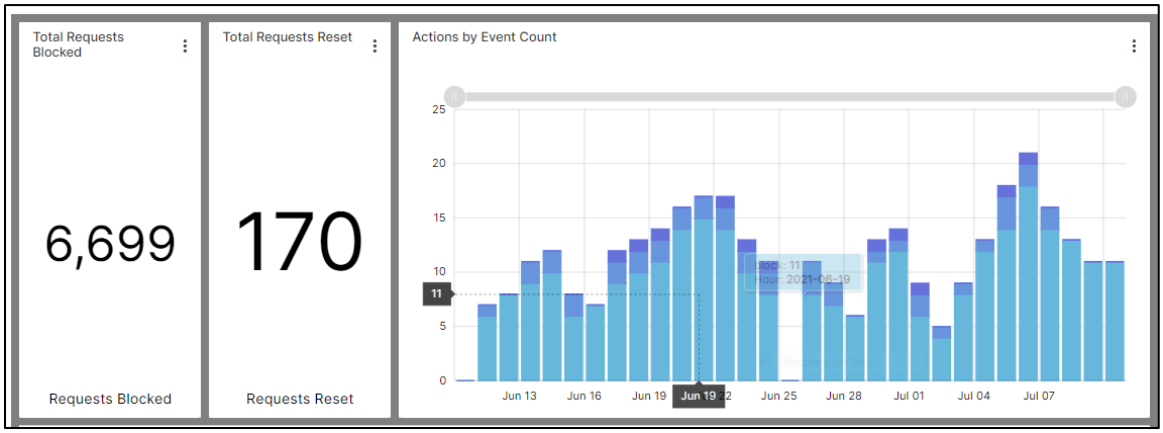


Firewall Application Control dashboard

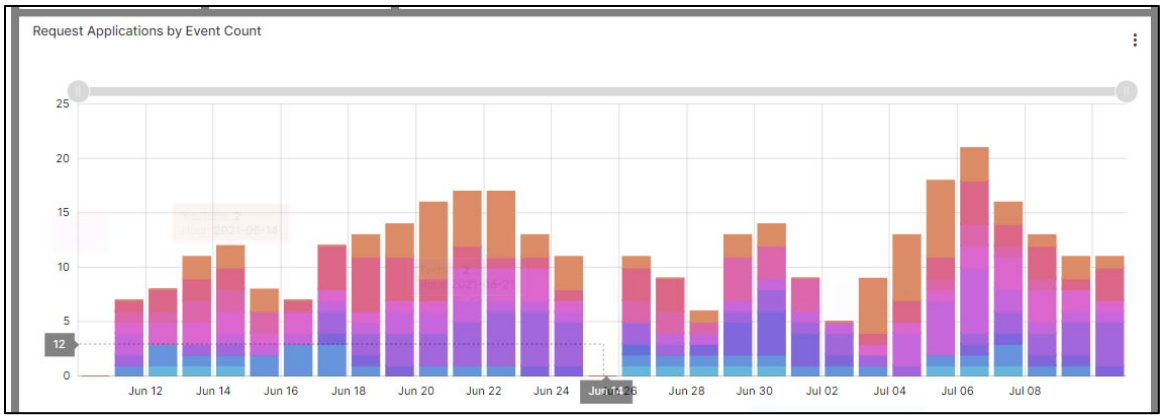
The Application Control dashboard presents logged events for application-based activities.

The following panels appear:

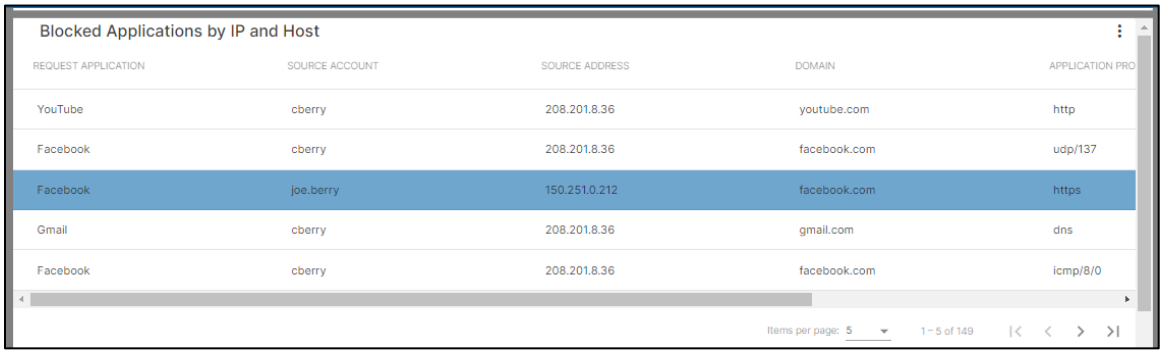
- **Total Requests Blocked**: The number of requests blocked for the selected date range.
- **Total Requests Reset**: The number of requests where the firewall terminated the connection with a reset signal for the selected date range
- **Actions by Event Count**: A bar chart of requests by action (block/pass/reset) for the selected date range.



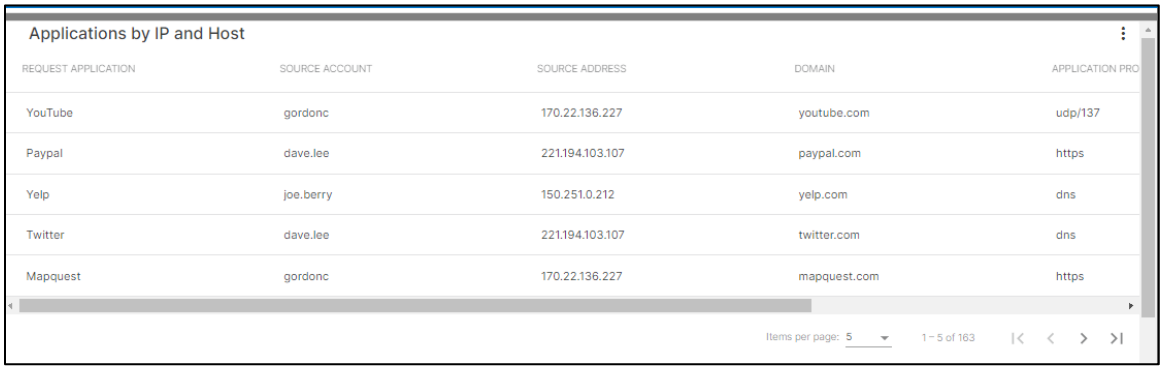
- **Request Applications by Event Count**: A bar chart of top 10 applications by the number of requests for the selected date range.



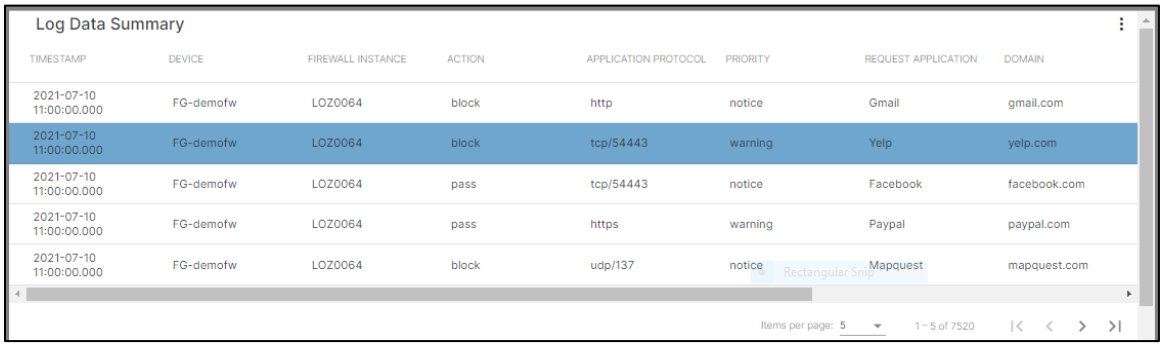
- **Blocked Applications by IP and Host**: Listing of the top blocked applications by IP and host (source and # requests).



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



- **Log Summary Data**: List of logs by action.

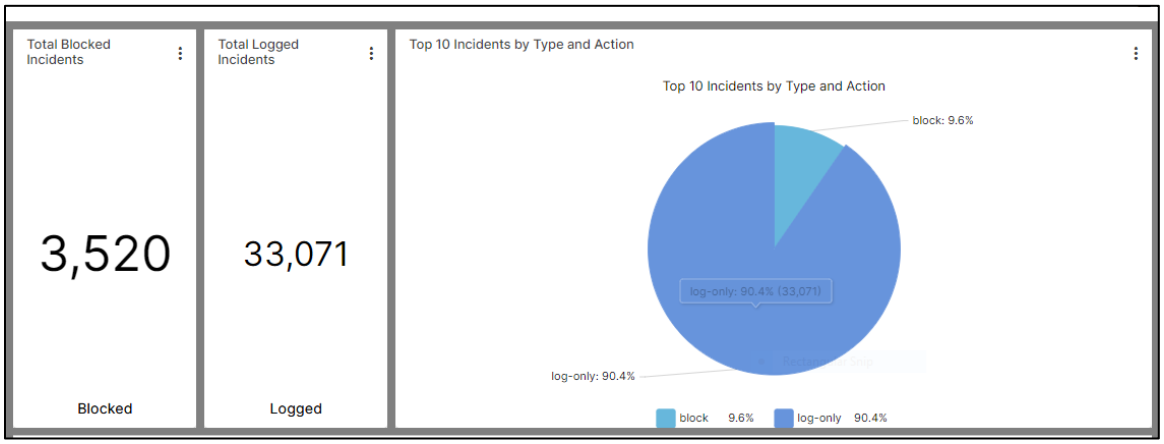


Firewall DLP dashboard

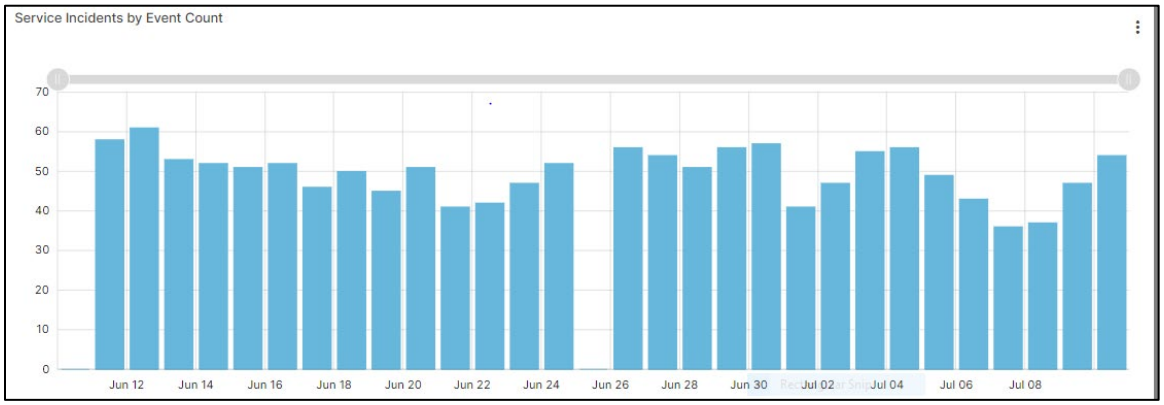
Data Leak/Loss Protection (DLP) monitors, prevents, and reports on attempts to send sensitive data outside a customer's organization.

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:

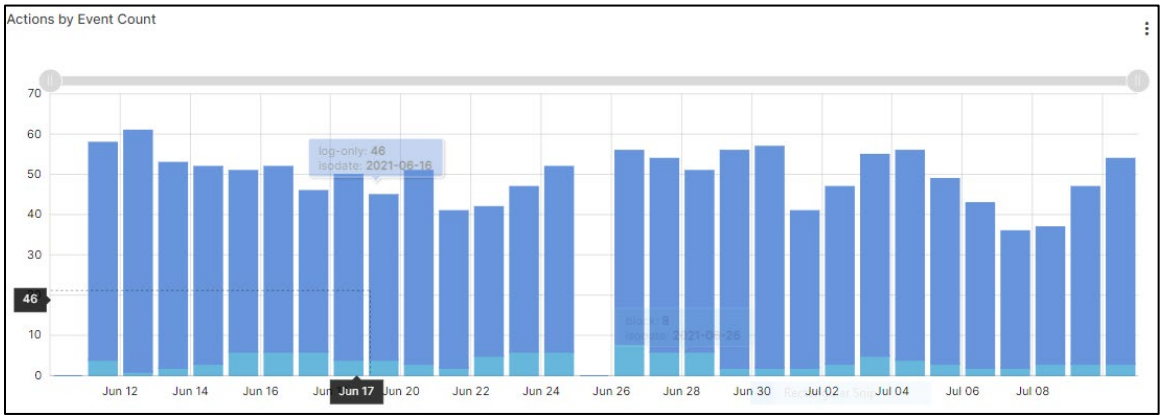
- **Total Blocked Incidents**: The total numbers of blocked DLP incidents.
- **Total Logged Incidents**: The total numbers of logged DLP incidents.
- **Top 10 Incidents by Type and Action**: A pie chart of incidents by type and status (log-only or blocked) for the selected date range.



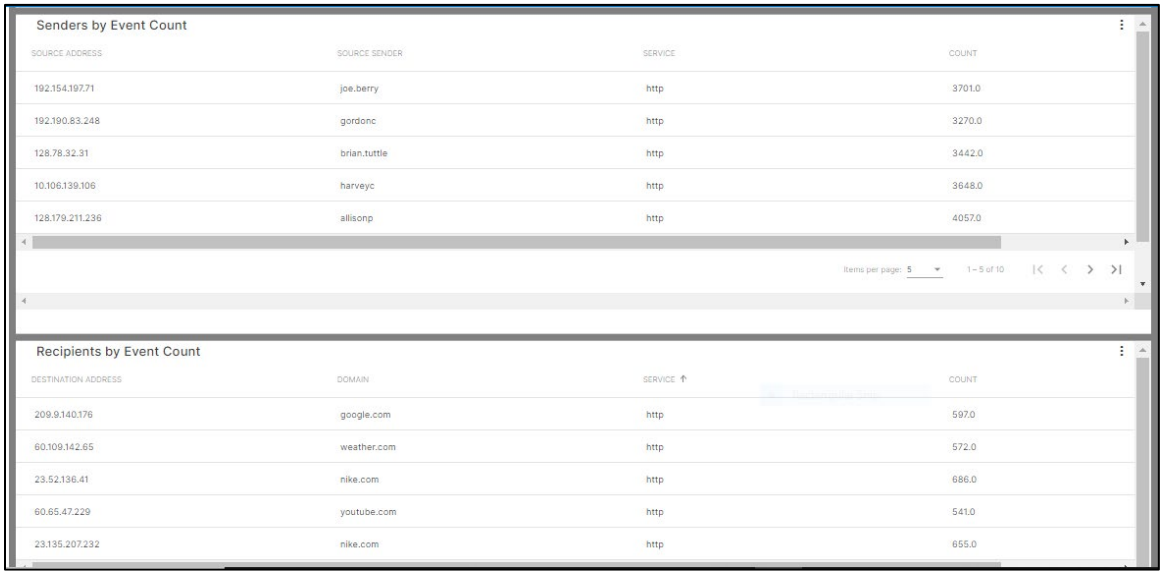
- **Service Incidents by Event Count**: A bar chart showing incidents by service (http or https) for the selected date range.



- **Actions by Event Count**: A bar chart of incidents by action (blocked/logged) for the selected date range.



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



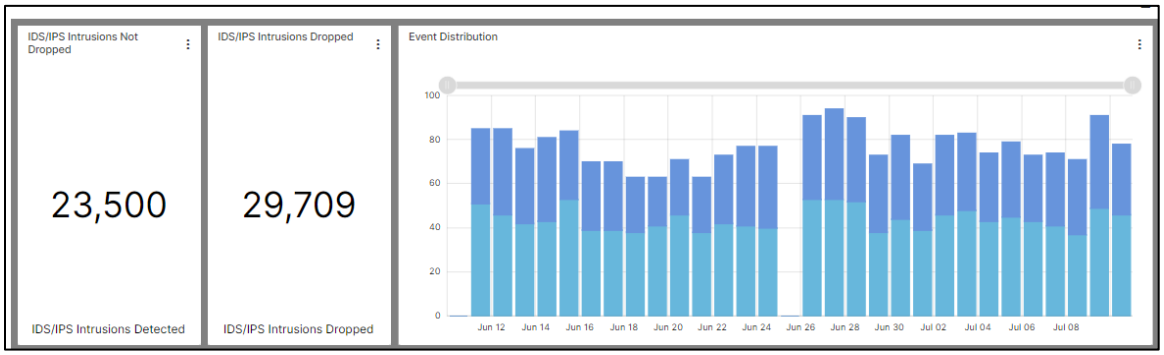
- **Log Data Summary**: List of log data by action.

Firewall IDS/IPS dashboard

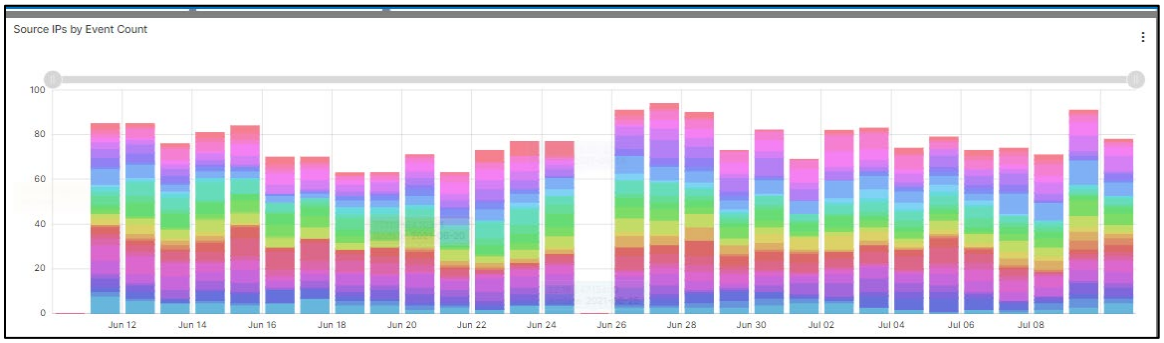
IDS/IPS prevents vulnerability exploits by examining packet content as it passes through the firewall against known signatures to detect, report and block intrusive behavior directed by your firewall policy.

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

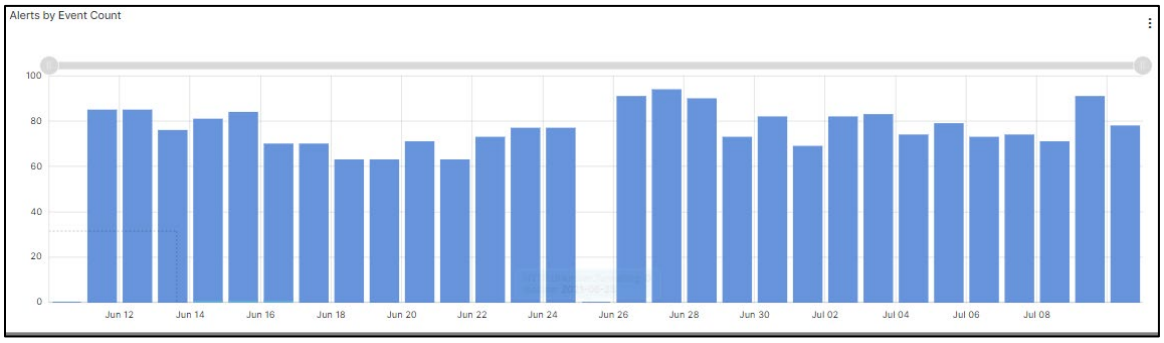
- **IDS/IPS Intrusion Detected and IDS/IPS Intrusions Dropped**: The number of detected and dropped IPS/IDS incidents for the selected date range.
- **Event Distribution**: A bar chart of alerts by status (detected/dropped) for the selected date range.



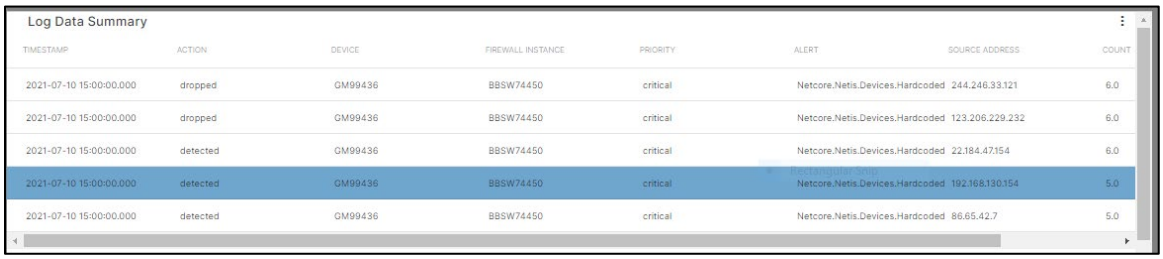
- **Source IPs by Event Count**: A bar chart of the top 20 IP pairs by number of incidents for the selected date range.



- **Alerts by Event Count**: A bar chart of the most common alerts for the selected date range.



- **Log Data Summary**: List of log data by action.

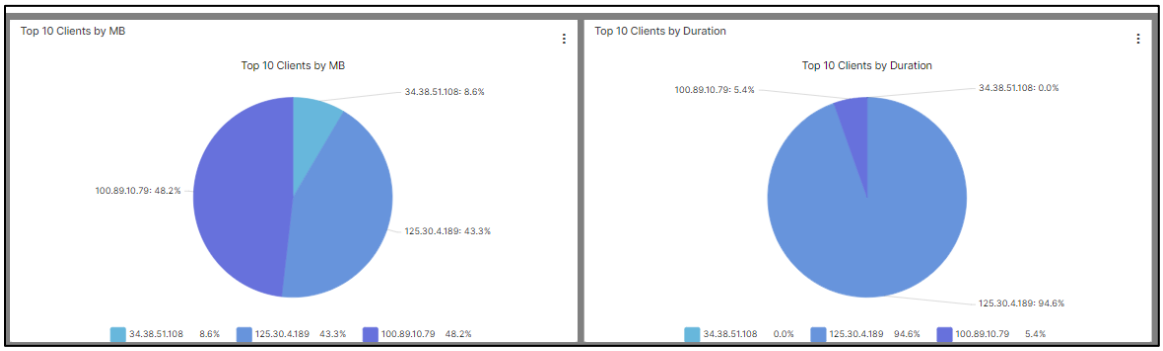


Firewall Mobility dashboard

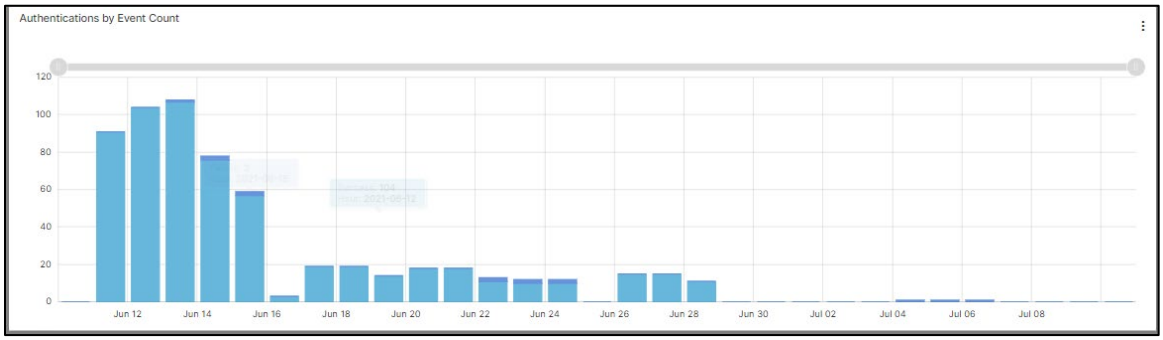
The mobility dashboard summarizes mobility client activity, focusing on logins as well as data volume and session durations. Mobility clients are identified by usernames (with active-directory integration) and geo location (based on remote IP lookup).

The following panels appear:

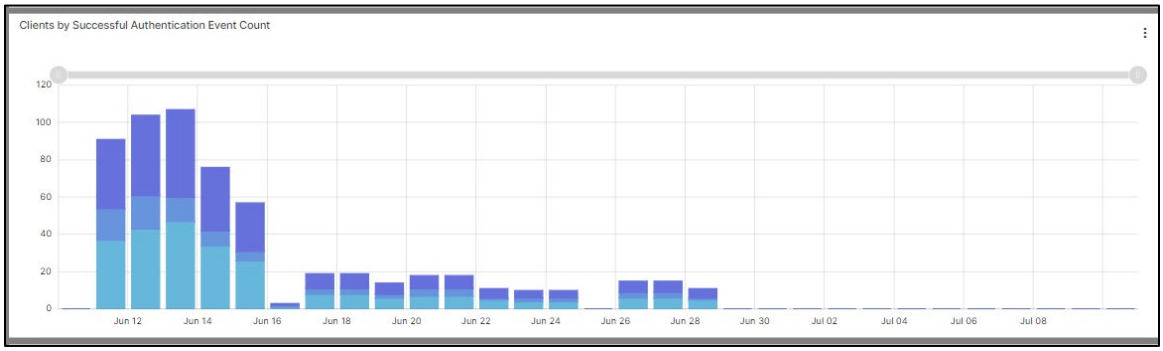
- **Top 10 Clients by MB**: A pie bar chart showing the top 10 clients by total number of authentication connections made by volume (MB) for the selected date range.
- **Top 10 Clients by Duration**: A pie bar chart showing the top 20 clients by total number of authentication connections made by duration for the selected date range.



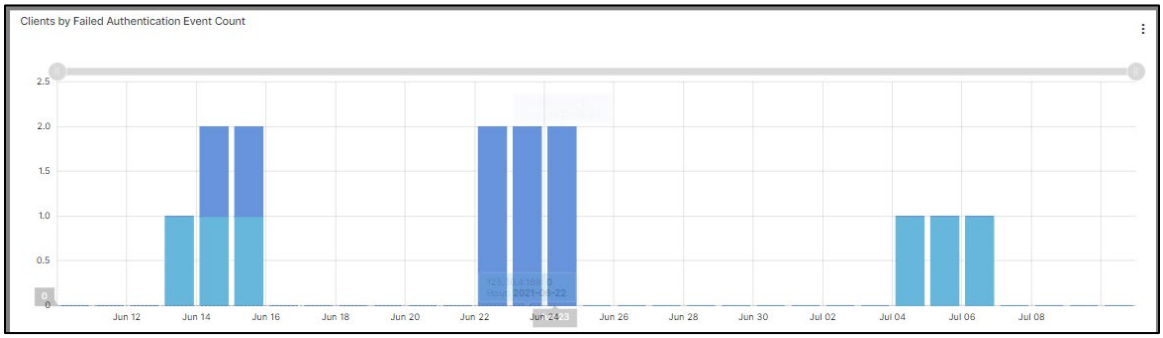
- **Authentications by Event Count**: A bar chart with the top 10 clients by number of authentication connections made by success and failure for the selected date range.



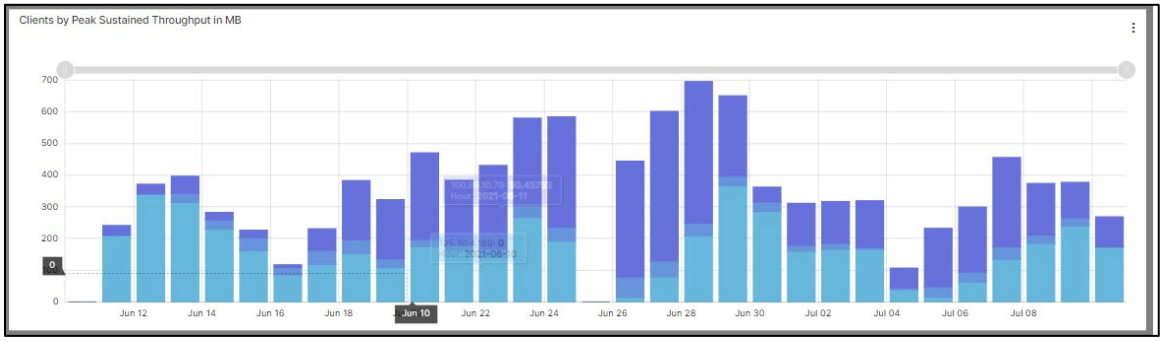
- **Clients by Successful Authentication Event Count**: A bar chart of the top 10 clients by successful authentications for the selected date range.



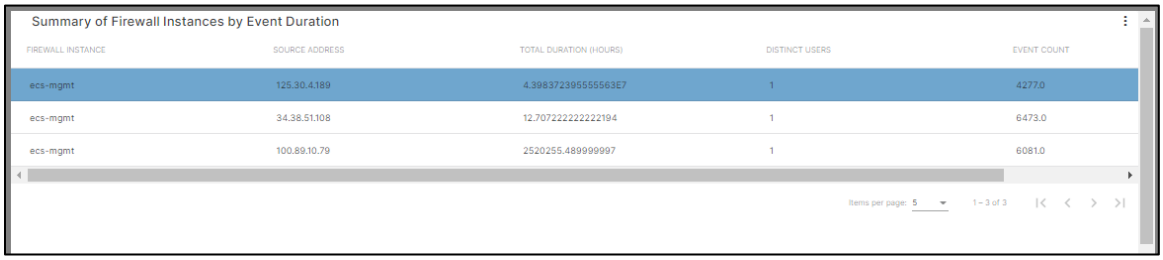
- **Clients by Failed Authentication Count**: A bar chart of the top 10 clients by failed authentications for the selected date range.



- **Clients by Peak Sustained Throughput in MB**: 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.



- **Summary of Firewall Instances by Event Duration**: List event count with total duration by firewall instance.



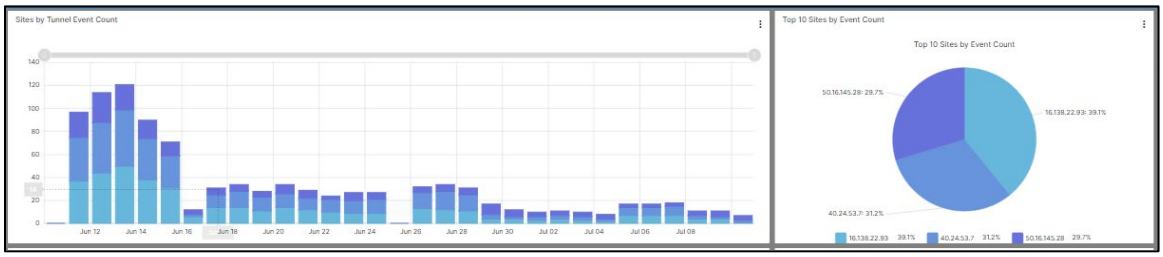
- **Log Data Summary**: List of log data by action.

Firewall Site dashboard

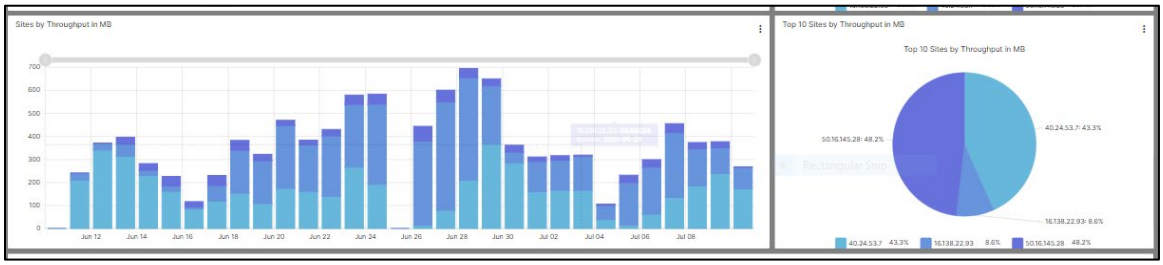
The Firewall Site dashboard summarizes traffic from remote access site encrypted tunnels.

The following panels appear:

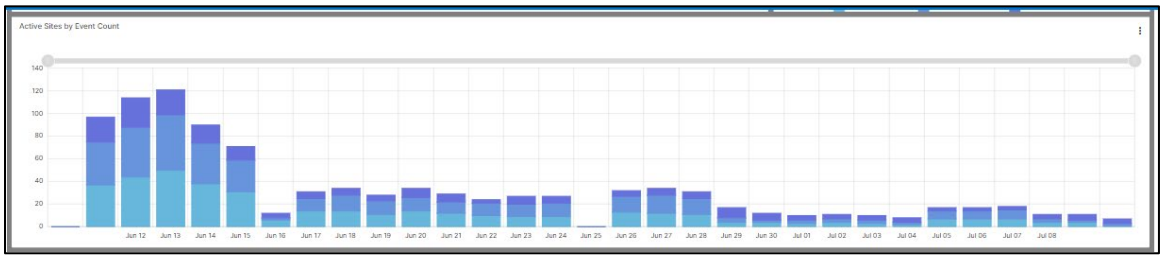
- **Top 10 Sites by Tunnel Events**: A bar chart with the top 10 sites by number of tunnel events (distinct connections) for selected date range.
- **Sites by Tunnel Event Count**: A pie chart with the top sites (up to 20 sites) by number of tunnel events (distinct connections) seen for the given IP address.



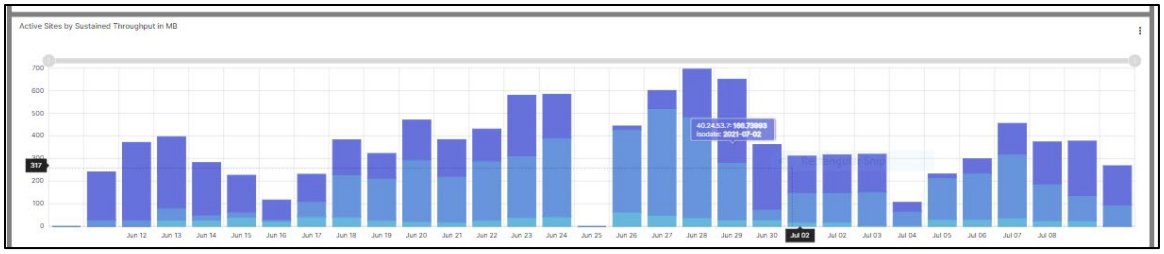
- **Top 10 Sites by Throughput in MB**: A bar chart with the top 10 sites by volume (in MB) for selected date range.
- **Sites by Throughput in MB**: A pie chart with the top sites (up to 20 sites) by volume (in MB) seen for the given IP address.



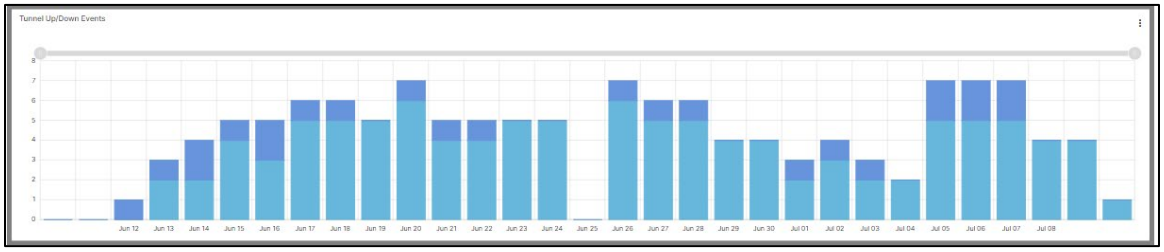
- **Active Sites by Event Count**: A bar chart with top sites by the sustained bi-directional throughput (the sum of the number of bytes sent from active sites) for the selected date range. Note that throughput is an approximate value based on 10+ minute volume updates.



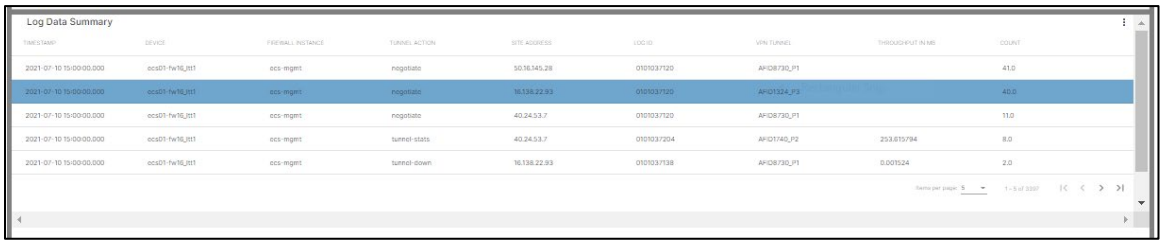
- **Active Sites by Sustained Throughput in MB**: A bar chart with top sites by the sustained bi-directional throughput (the sum of the number of bytes sent from active sites) for the selected date range. Note that throughput is an approximate value based on 10+ minute volume updates.



- **Tunnel Up/Down Events**: A bar chart with top sites showing tunnel up and down events for the selected date range.



- **Log Data Summary**: List of log data by action.

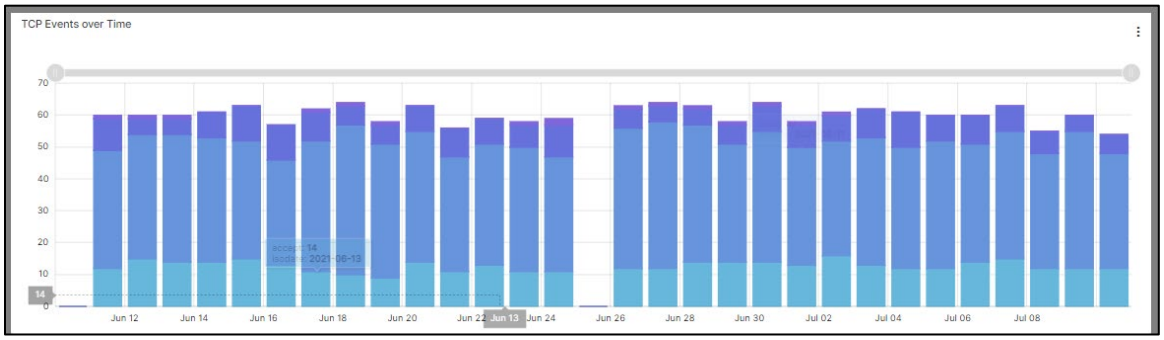


Firewall Traffic dashboard

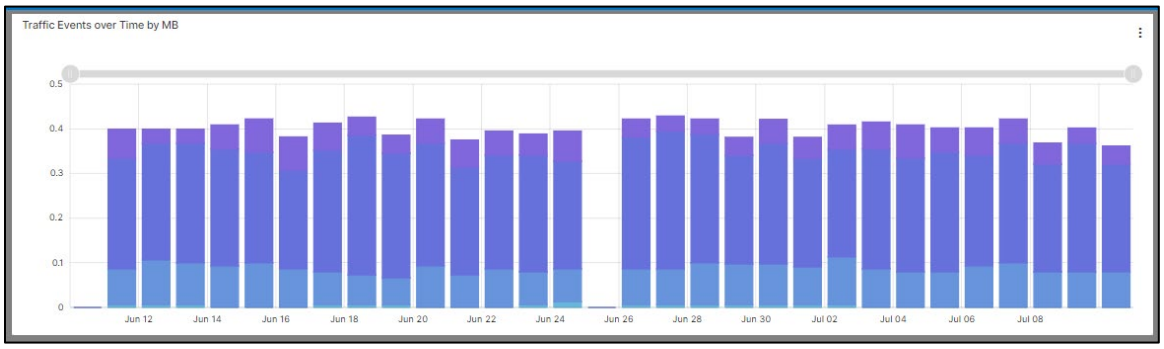
The Firewall traffic dashboard summarizes traffic traversing users firewall via multiple graphics. Traffic data is shown by the number of logged events (traffic flows) and by volume (by MB).

The following panels appear:

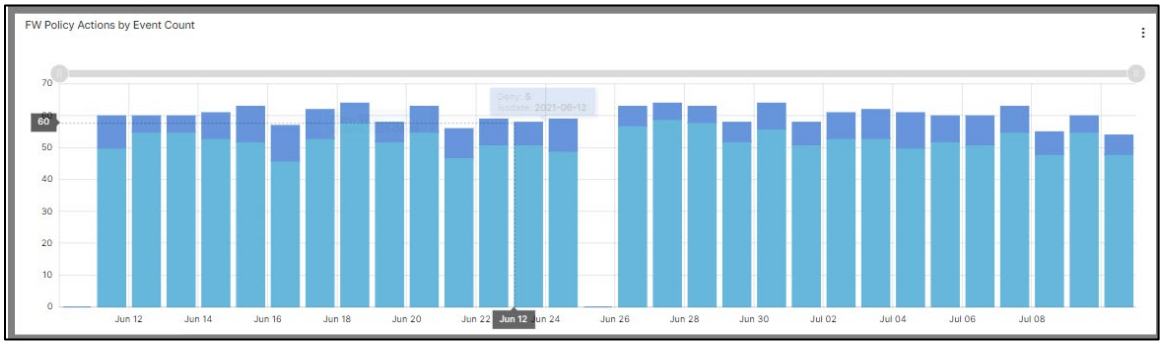
- **TCP Events over Time**: A bar chart of the total firewall traffic events by action type (accept, close, deny, timeout) for the selected date range.



- **TCP Events over Time by MB**: A bar chart of the total firewall traffic events by action type (accept, close, deny, timeout) for the selected date range.

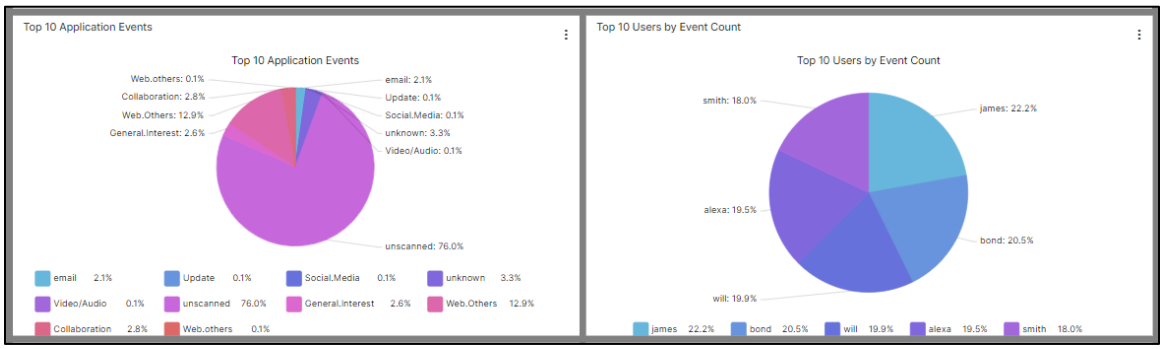


- **FW Policy Actions by Event Count**: A bar chart of the allowed and denied firewall traffic events for the selected date range.

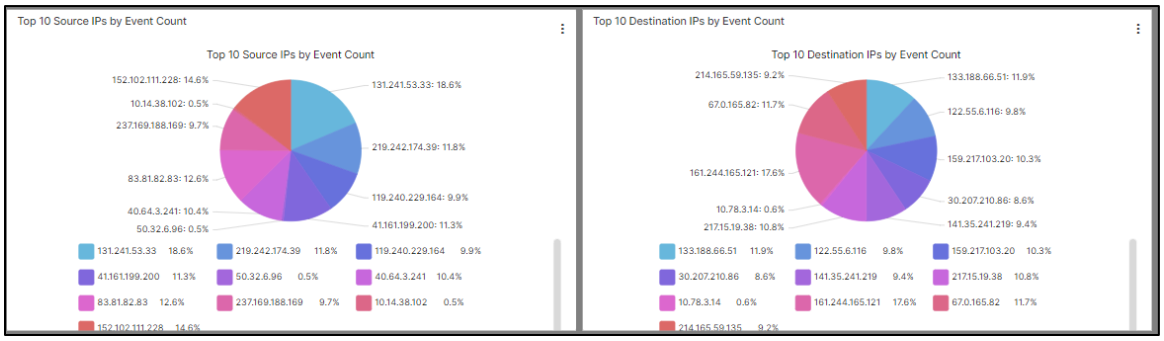


- **Top 10 Application Events**: A pie chart of the number of connections by top 10 application categories by IP address.

- **Top 10 Users by Event Count (**with active-directory integration**)**: A pie charge of the top 10 IP source users for traffic events



- **Top 10 Source IPs by Event Count**: A pie charge of the top 10 IP Source users for traffic events.
- **Top Destination IPs by Event Count**: A pie charge of the top 10 Destination IPS for traffic events.



- **Log Data Summary**: List of log data by action.

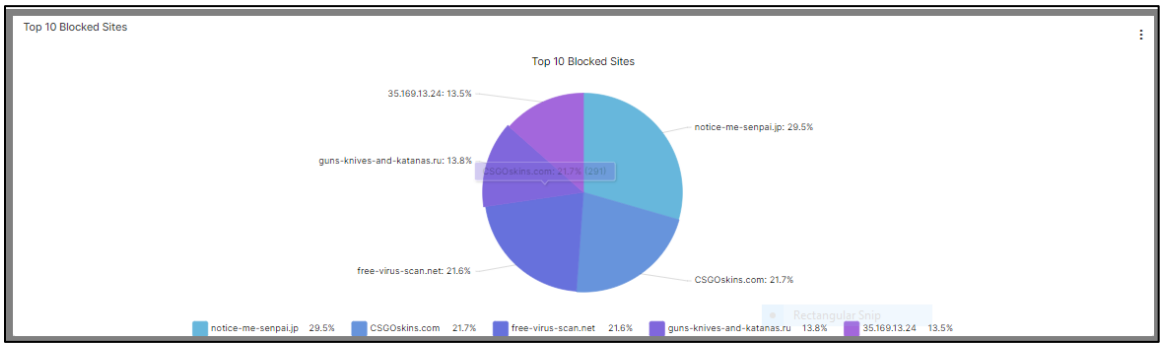
Firewall Webfilter dashboard

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

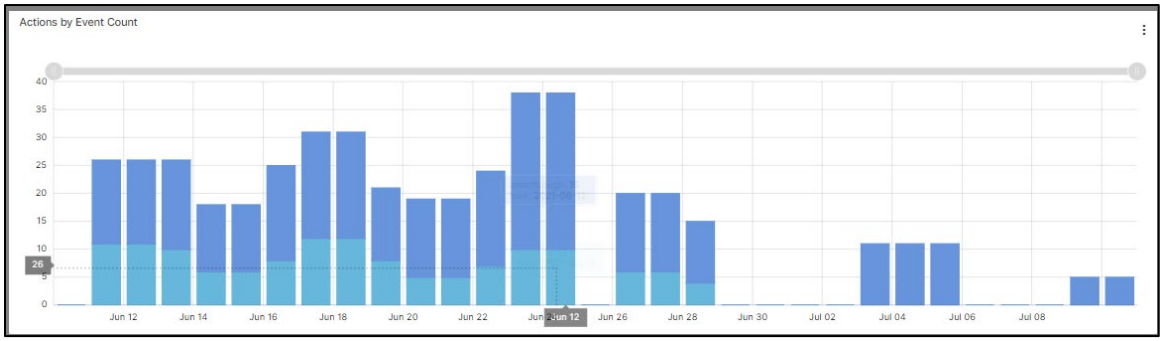
The Firewall Webfilter dashboard presents logged events for URL and content-based web-traffic control.

The following panels appear:

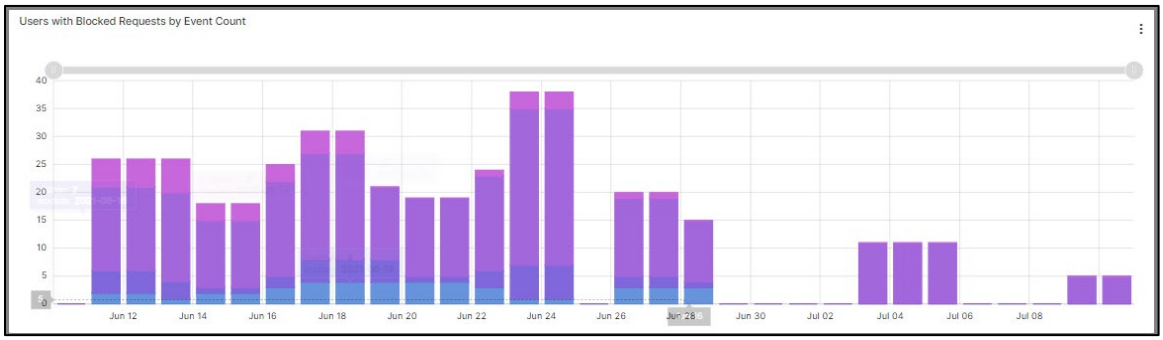
- **Top 10 Blocked Sites**: A pie chart showing the top blocked web sites for selected date range.



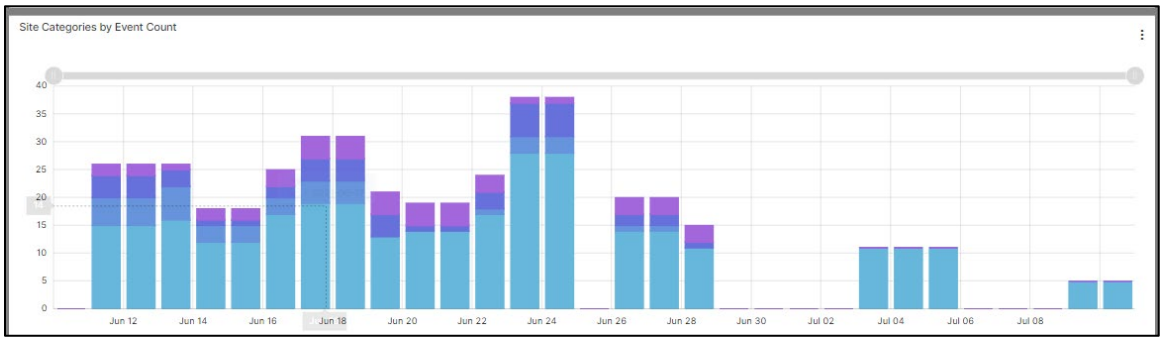
- **Actions by Event Count**: A bar chart of the number of attempts to websites by action (passthrough, blocked) for selected date range.



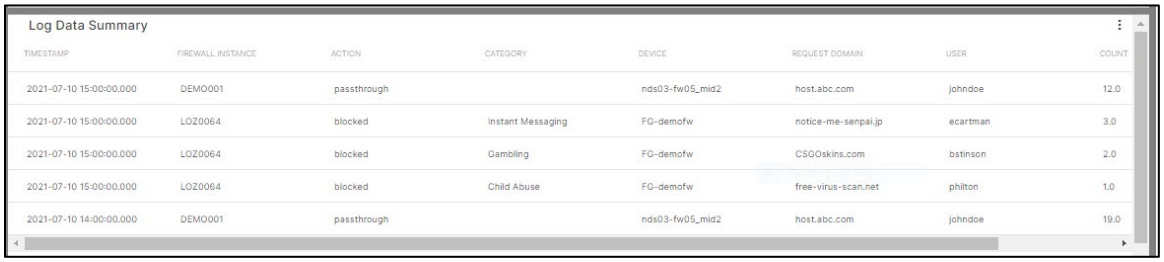
- **Users with Blocked Requests by Event Count**: A bar chart of the top 10 users (with active-directory integration) by blocked requests for selected date range.



- **Site Categories by Event Count**: A bar chart of the top web site categories by blocked and passthrough attempts for selected date range.



- **Log Data Summary**: List of log data by action.



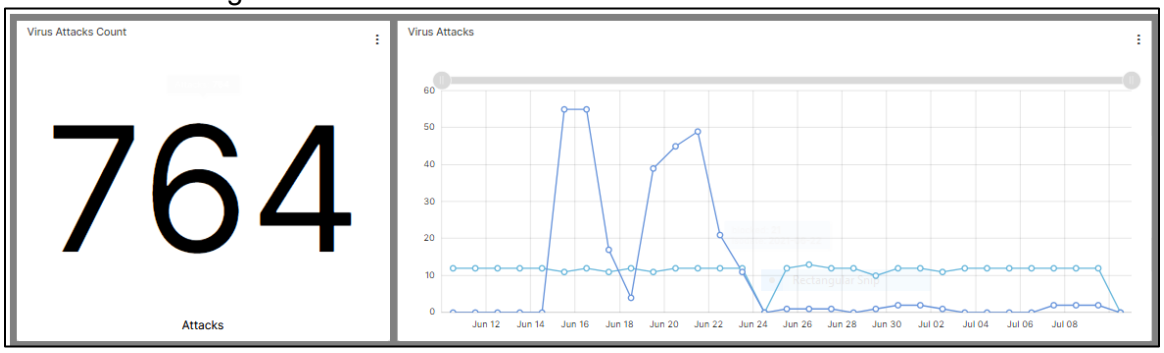
Firewall Virus and malware (sandboxing) dashboard

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

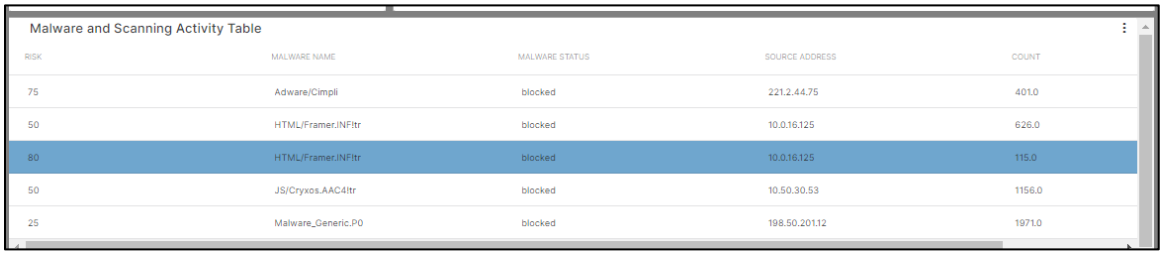
The Virus and Malware (sandboxing) feature displays potential infections based on signatures and actions taken (analytics (sent to the sandbox for analysis), monitored, passthrough, blocked). This service operates in conjunction with the anti-malware feature. Anti-malware sandboxing scans and blocks 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:

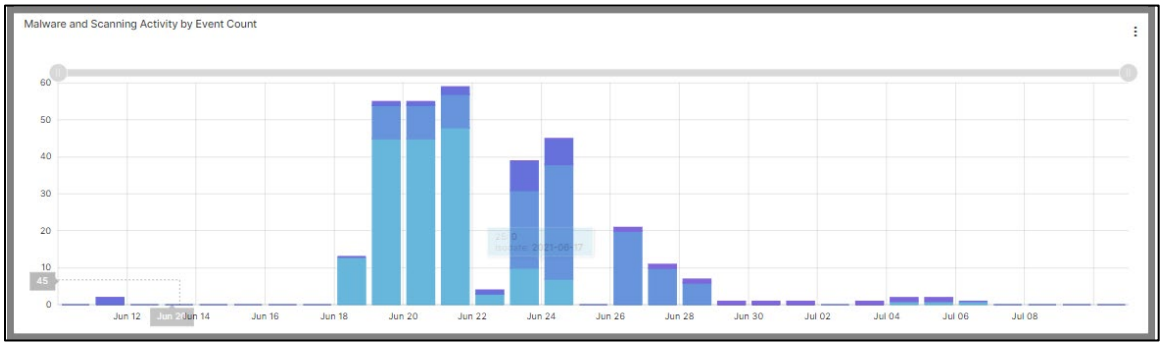
- **Virus Attack Counts**: The number of virus attacks with a priority of warning or higher.
- **Virus Attacks**: A time chart showing virus attacks by status (blocked/analytics) over the selected date range.



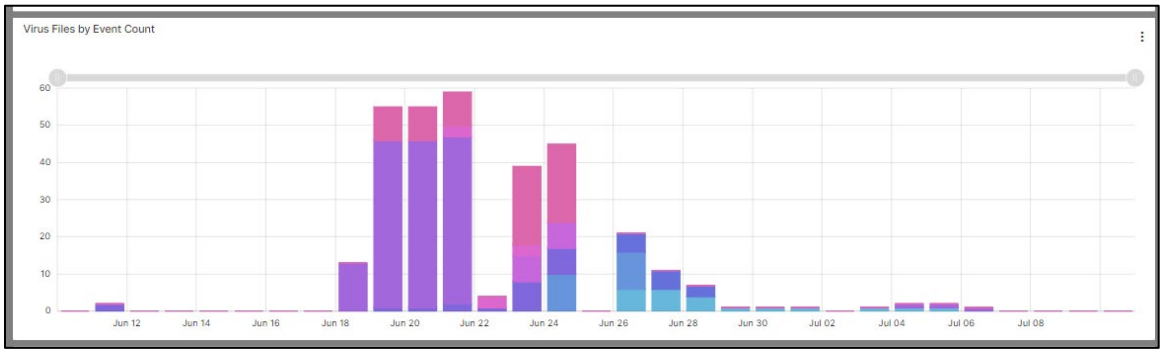
- **Malware and Scanning Activity Table**: A table listing of virus attacks by virus name, virus status (blocked/analytics), source address, count for the selected date range.



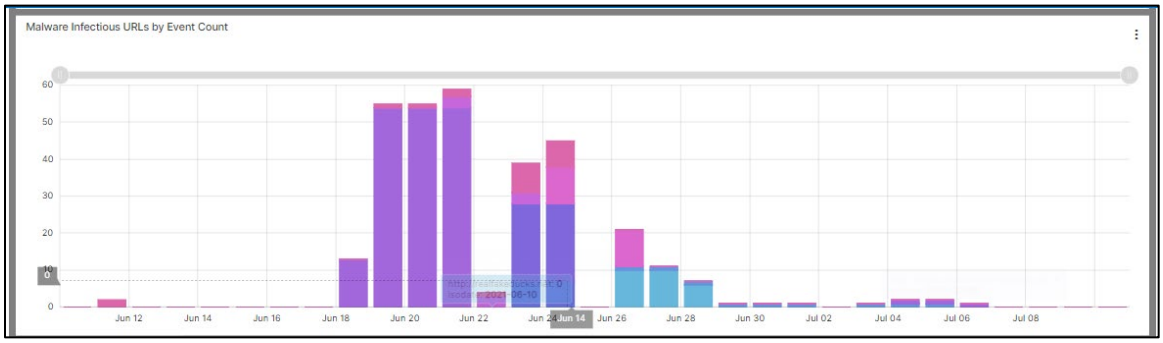
- **Malware and Scanning Activity by Event Count**: A bar chart of malware or scanning activity by malware risk for the selected date range.



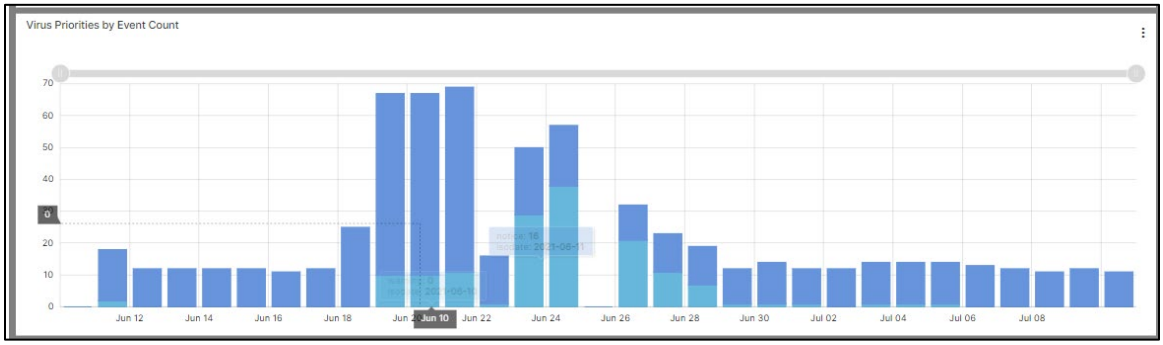
- **Virus Files by Event Count**: A bar chart of the top 10 virus files for the selected date range.



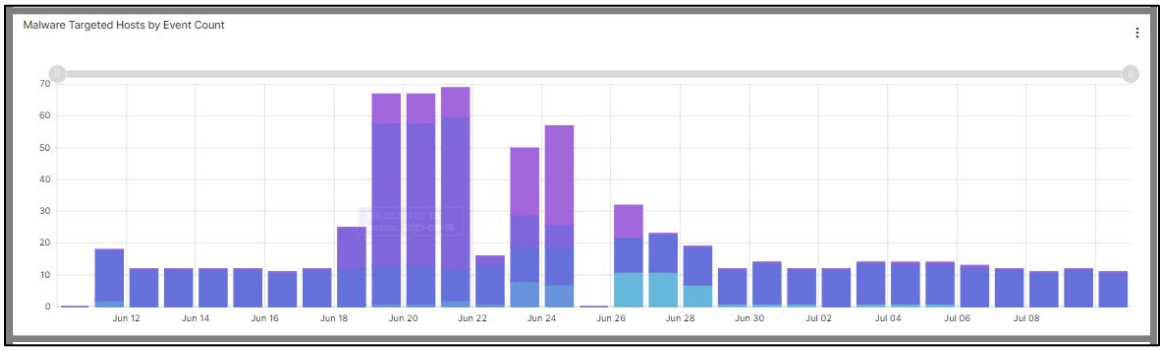
- **Malware Infectious URLs by Event Count**: A bar chart of the top infected URLs (from which malware originated) for selected date range.



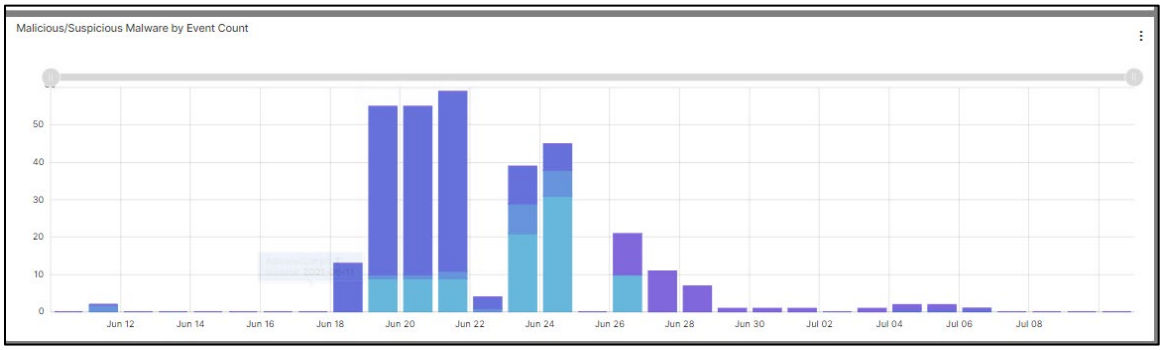
- **Virus Priority by Event Count**: A bar chart of the virus priority rating for selected date range.



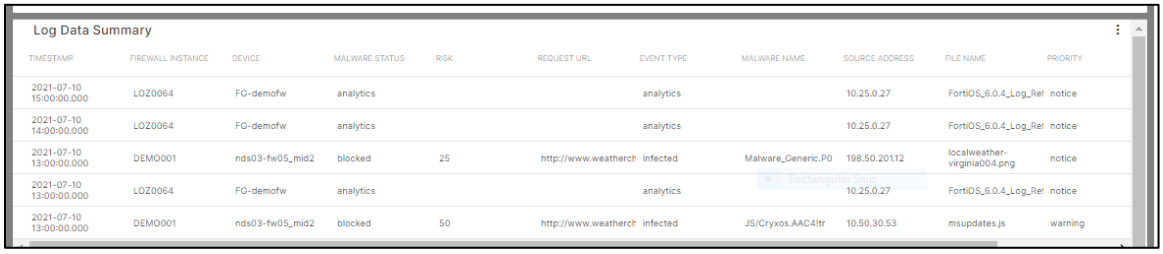
- **Malware Targeted Hosts by Event Count**: A bar chart of the top malware hosts (from which malware originated) for selected date range.



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



- **Log Data Summary**: List of log data by action.

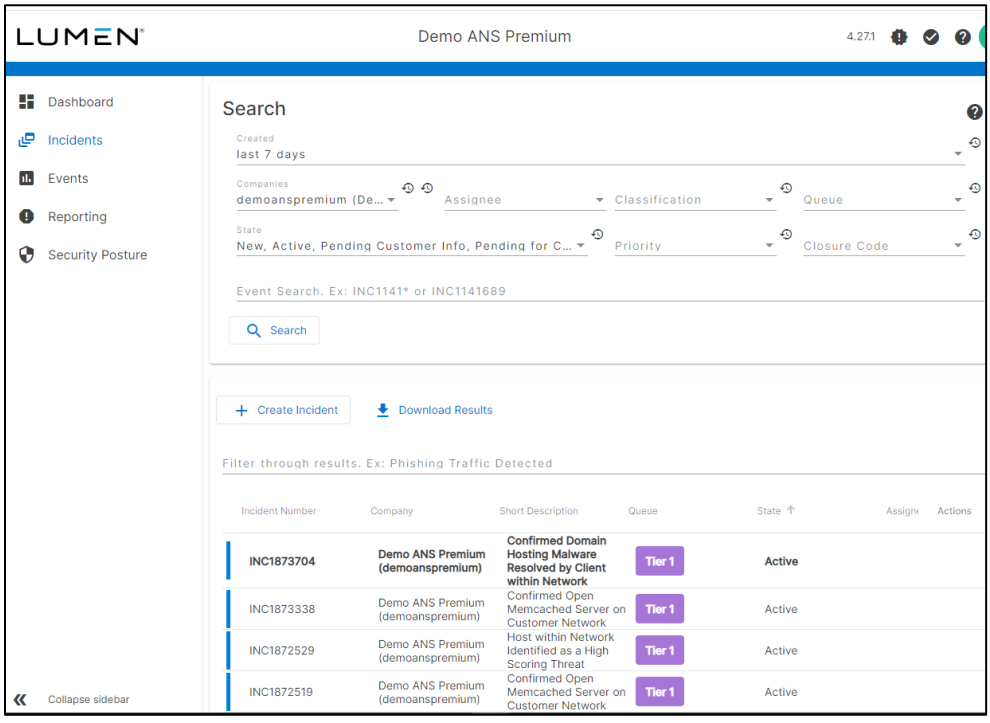


Incidents

Use the **Incidents** menu to view incident details and to obtain guidance on incidents identified on the Firewall service.

1. Enter a date range value in the **Created** field, then click **Search**.

   The following Incidents will be displayed with the option to download results.



2. To obtain details and guidance, double click a specific incident:
   - Automated Analyst Summary
   - Threat Profile detail
   - Additional Information of Attributes
   - Base Events for Alert
   - Firewall Connections Summary as Source Address
   - Firewall Connections Summary as Destination Address
   - Investigation Summary

Confirmed Domain Hosting Malware Resolved by Client within Network

A new investigation has been created for the company "demoanspremium" on the alert "Confirmed Domain Hosting Malware Resolved by Client within Network".

Timestamp	Event Severity	Event Type	Event Name	Event Signature Id	Event Direction	Event Message	Source Address	Source Network	
2021-09-11 12:30:45	0	Lead	Confirmed Domain Hosting Malware Resolved by Client within Network	ans-00010	Outbound	The malware hosting domain at windows.storageupgrade.net was resolved by the source IPv4 address 10.0.0.2 on the customer network. Investigate the host within the customer network that established the connection with the command and control server. This can be accomplished by doing things such as checking recent log entries and changes related to this host, looking for suspicious processes on the host, and checking common methods for persistence such as registry keys.	10.0.0.2	RFC-1918	w

Threat Profile

Notes

The source demo_malicious_domains has identified windows.storageupgrade[.]net as hosting malware.

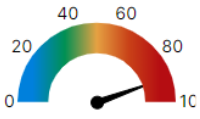
This threat is scored a very high risk level based on the activity observed. Very high risk indicators can be are ones that have been reported as suspected C2s, or are exhibiting multiple types of malicious behavior.

Risk Level

Very High

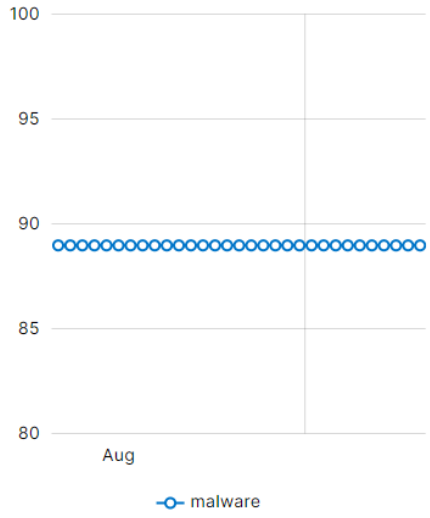
Risk Score

89



Observed Activity

Last 30 days



Additional Information

Attribute	Value(s)
Last Seen	2021-09-11 12:30:45
First Seen	2021-09-04 20:57:21
Source	Back Door
Entity Type	application control ips log (block)
Port	59727

Base Events for Alert

Below are the events that generated the alert Confirmed Domain Hosting Malware Resolved by Client within Network:

Timestamp	Device Vendor	Device Product	Device Hostname	Event Name	Event Application Protocol	Source Address	Source Port	Source Account	Destination Address
2021-09-11 12:25:30	Fortinet	FortiGate	GM239842	application control ips log (block)	https	10.0.0.2	59727	wrightnicole	208.85.248.173

Firewall Connections Summary as Source Address

Top 20 firewall connections for the IP address 10.0.0.2 as a source over the last 7 days:

Source Address	Destination Address	Destination Port	Event Name	Event Application Protocol	Count
10.0.0.2	208.85.248.173	443	application control ips log (block)	https	28
10.0.0.2	208.85.248.173	443	Confirmed Domain Hosting Malware Resolved by Client within Network		14
10.0.0.2	208.85.248.173	443	Outbound Interaction Observed with High/Very High Scoring Threat Indicator		1

Firewall Connections Summary as Destination Address

Top 20 firewall connections for the IP address 10.0.0.2 as a destination over the last 7 days:

Source Address	Destination Address	Destination Port	Event Name	Event Application Protocol	Count
80.147.44.211	10.0.0.2	11707	traffic forward message	tcp/11222	14
80.147.44.211	10.0.0.2	11707	Interaction Observed with a Severe Scoring Source IPv4 Address		13

Search Link

Investigation Summary

Below is the investigation summary:

- A new alert, Confirmed Domain Hosting Malware Resolved by Client within Network, was detected.
- The severity of alert that started this investigation was 0.
- Base events for the alert were found.

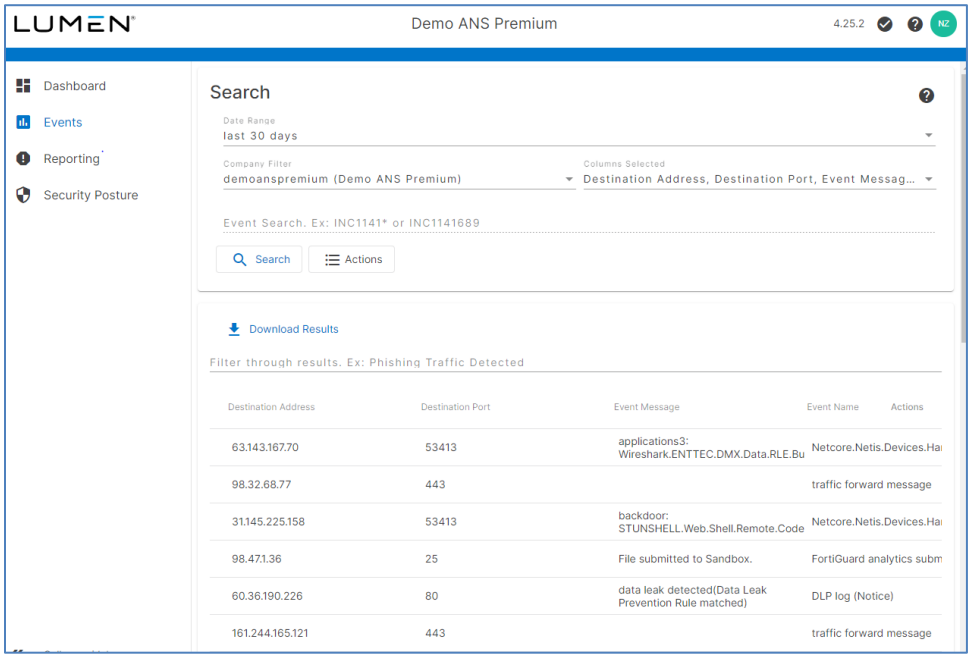
Events

Use the **Events** menu to view logs or create a flexible query filter.

To search and download events from a date range:

1. From the left menu, select **Events**.
2. Select the date range.
3. Select or change the defaults in the **Columns Selected** field.
4. Click the **Search** button.

   A list of events appears.



5. Select **Download Results** to export to a .csv file.
6. Double click on an event to obtain more information on the event.

Reporting

You can create reports two ways:

- **Dashboard** section: download to a firewall default report template associated to the dashboard. Selects the **DOWNLOAD REPORT** button, then select either .csv or .pdf format.
- **Reporting** section: enabling a user to create and export a standard report from a firewall default report template or a custom report.

The 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.

Creating a report

Below are common input values for generating reports.

- **Date range** – identifies how long you want the report to run for. There is a “Run Forever” option allowing you to run the report until you delete the report.
- **Report Run Frequency** – identifies how often you want this report to run(e.g. running it every day or once per week). This uses the cron expression with 5 possible values. The **Validate** button allows you to check whether your cron expression is correct and give you a visual text of when things will run
    a. The five possible values are the following:

Seconds	Minutes	Hours	Day of Month	Month	Day of the week	Year

        1) ***** <***all***> for example in the minute field will specify that it should happen every minute
        2) **?** <***any***> utilized for Day of the month and day of the week. Example if you pick a day of the week or of the month when you want your report to run, by adding ? you do not care which specific day of the week that day falls under.
        3) **/** <***increment***> specifies an incremental value. Example For example, a “5/15” in the minute field means at “5, 20, 35 and 50 minutes of an hour.”

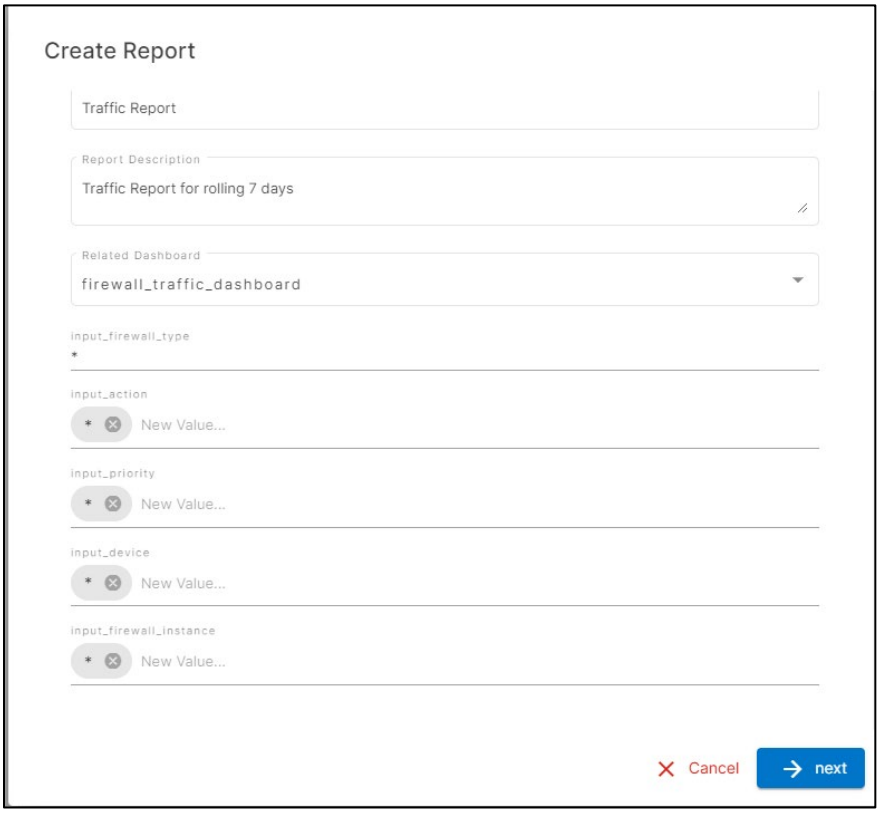
4) - <***range***> determines the value range. For example, 10-11 in the hour field means “10th and 11th hours.”
5) L <last> has different meanings when used in various fields. For example, if it's applied in the day-of-month field, it means last day of the month, i.e. “31st of January” and so on as per the calendar month. It can be used with an offset value, like “L-3”, which denotes the “third to last day of the calendar month.” In day-of-week, it specifies the “last day of a week.” It can also be used with another value in day-of-week like “6L”, which denotes the “last Friday.”
6) # specifies the “N-th” occurrence of a weekday of the month, for example, “third Friday of the month” can be indicated as “6#3”.
7) **,** <values> specifies multiple values. For example, “MON, WED, FRI“ in <day-of-week> field means on the days “Monday, Wednesday and Friday.”
8) **L** <last> has different meanings when used in various fields. For example, if it's applied in the <day-of-month> field, it means last day of the month, i.e. “31st of January” and so on as per the calendar month. It can be used with an offset value, like “L-3”, which denotes the “third to last day of the calendar month.” In <day-of-week>, it specifies the “last day of a week.” It can also be used with another value in <day-of-week>, like “6L”, which denotes the “last Friday.”

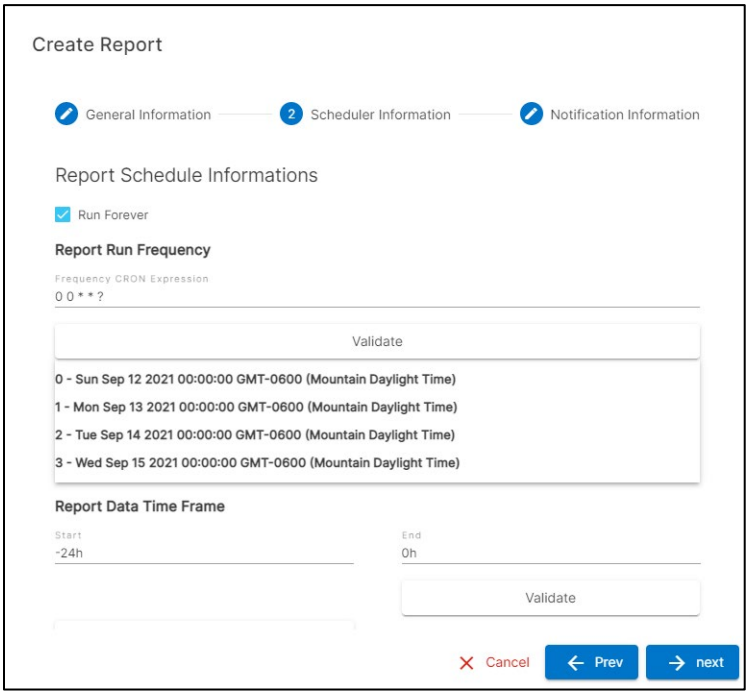
Typical scenarios are:

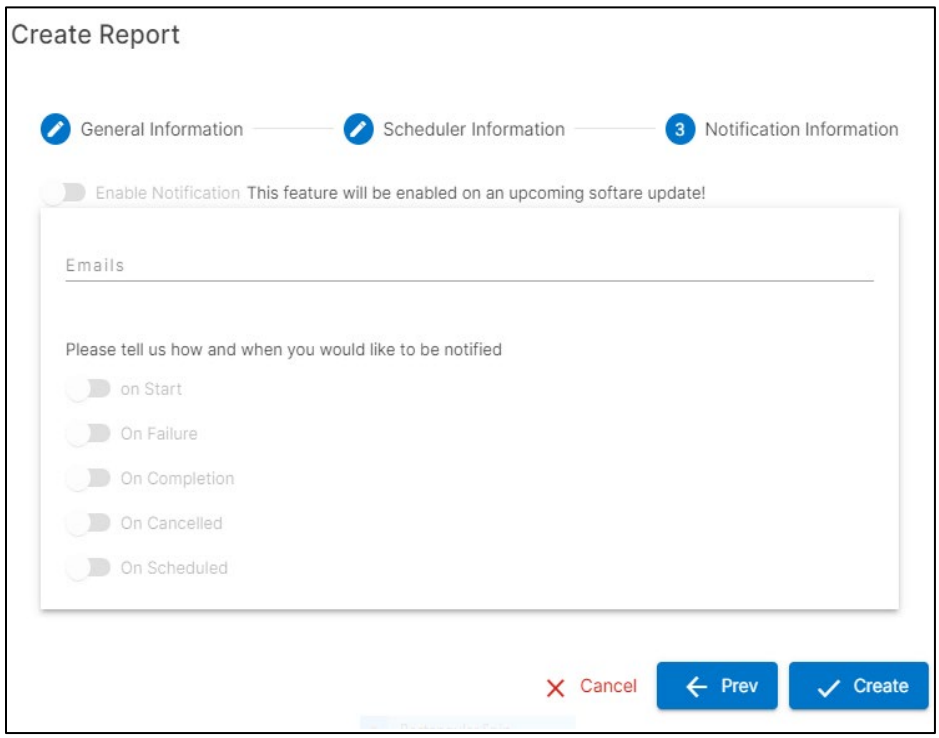
- **Once a day report for the last 24 hours of data**
  - The report will **run forever**
  - Cron expression → 0 0 * * ?
  - First maya expression → -24h | Second maya expression → 0h
- **Once a week for the last 7 days of data**
  - The report will **run forever**
  - Cron expression → 0 0 1 * *
  - First maya expression → -7d | Second maya expression → 0d
  -
- **Once a month for the last month of data**
  - The report will **run forever**
  - Cron expression → 0 0 0 ? * *
  - First maya expression → -30d | Second maya expression → 0d

Example – Once a day report for the last 24 hours of data.

Please enter the value then click **Enter** to ensure  is displayed and click → **next**.







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.