SOPHOS

What's in the Central Firewall Reporting EAP

What's in the Central Firewall Reporting Early Access Program (EAP)

With Central Firewall Reporting (CFR), we're excited to share our new, built from the ground up, cloud-architected reporting platform in Sophos Central. CFR is the first service to leverage this modern data platform. As we continue to execute on the Sophos Darwin strategy, you can expect to see additional services leveraging this new platform in the future. Exciting times are ahead for the value we can provide you with a Sophos Central data platform. But for now, let's talk about what we're doing with CFR.

Increasing visibility into network activity through analytics has become vital as organizations strive to gain a deeper understanding of user activities, applications, network events, performance, risks and more in their security environment. Using that knowledge, organizations can implement policy changes to drive efficiencies that enhance productivity while also protecting against cyber threats.
Organizations often need the following capabilities:

- Deep insight into user activity, application usage and security threats on the network
- Tools to report and identify trends that require an actionable response
- Pre-defined, out-of-the-box reports to streamline the report creation process
- Flexibility to create hundreds of customized report views, tailored to specific needs
- An intuitive user interface that makes report creation fast and easy

Solution
An integral service of Sophos Central, Central Firewall Reporting is a cloud-based reporting platform that provides organizations with a powerful set of options to capture network logs through a Sophos Central account and their XG Firewall running v18 firmware. Using the interactive reports and report dashboard, administrators can drill down into the syslog data for a granular view that is presented in a visual format for easy understanding. The data can then be analyzed for trends that could identify gaps in the security posture and illuminate the need for potential policy change. A key theme with CFR is that we want to put the control for what goes into the report in your hands. As is often the case, there are many different reporting scenarios requiring countless variations of data from a given a report. Rather than bombard you with a multitude of alternatives for every given report type,

we're empowering you with tools to configure chart options, table, filters, and time ranges so that you can get a report that best suits your specific use cases.

Key Features (CFR initial launch)

Rich, granular data organized into easy-to-understand reports

Sophos CFR provides administrators with the ability to configure flexible reports with a high degree of customization. Each report table, containing dozens of column choices, allows administrators to add or remove columns of data, thereby making a report more granular, compressed, or enriched as desired. This flexibility enables administrators to define the data fields they need in their report and to see correlated data together. To illustrate this flexibility, take the application bandwidth report that shows bandwidth usage by application and risk. The application and risk columns can be removed and replaced with source IP to provide a bandwidth usage report broken out by IP address. Further, the v18 log data model has been standardized and updated with over a hundred enhancements to provide more data in the reports and log fields.

Flexible out-of-the-box reports

Reports are structured around specific modules such as Application Usage, Web Usage, and so forth. Each of the reports can be further customized by changing data fields in the table and charts and applying filters to the hundreds of data fields. The flexible report table and charts allow users to customize each report and create a library of hundreds of variations from any report. Each report provides multiple charting options, enabling administrators to visualize data and trends for their specific use case. For example, the Application Bandwidth report uses a stacked area chart showing bandwidth consumption over a defined period. The administrator can switch from a stacked area chart to a bar chart, as it would allow provide a better understanding of application usage relative to other applications.

Customizable chart options

Have you ever wished you could change a chart type for a report because it better represented the 'story' of the data? We did, so that's why you can select between a bar, pie, stacked area, and line chart for any report. What's more, the X and Y dimensions are configurable in the chart, providing a high degree of choice for what you want to represent in a report. And yes, there's also a geographical view so that you can understand where security threats are originating from around the globe.

Syslog search and view

As Sophos CFR ingests and indexes the firewall log data, it also stores all the logs sent to Sophos Central. You can pivot from a report with specific filters directly into the log data should you need a more detailed look at what drove the data in the report view. The log viewer provides a tabular view and a 'raw' view of the logs. Columns of data can be configured, and filters can be applied to retrieve logs of interest.

As a preemptive notice, CFR will not function as a log forwarder. Organizations that need to store their log data in a third-party SIEM or log collector in addition to Sophos Central can configure their XG firewall to send data to multiple locations in parallel (e.g. a local SIEM and Sophos Central).

Report dashboard

The report dashboard is an at-a-glance view from the XG Firewall for network operational health, policy control events, and all security-driven events. Sometimes administrators just need to get the quick glance of the last 24 hours of events without having to dive into a more detailed report. The report dashboard surfaces the top network, security, and policy-driven events. From the report dashboard, administrators can quickly pivot into a full report for a more detailed analysis.

Licensing

Collecting, storing, and aggregating firewall logs naturally requires compute and storage resources in the data platform. For the EAP, we are providing administrators with a rolling seven days of log retention and reporting data per firewall, at no cost. Additional details will be made available later regarding the licensing options for CFR, which will include both free and premium licensed capabilities.

The power of the cloud and incremental updates

Unlike monolithic releases that you may see with firewall firmware, the Sophos Central cloud platform allows us to deliver incremental features and value to you more quickly. What that means is that you can expect to see new features on a more frequent basis. The best analogy for this is that a train leaves the station roughly every six weeks carrying small amount of cargo with Sophos Central. Contrast that with firewall releases, and that train leaves the station only a few times a year carrying larger cargo. After CFR enters General Availability (GA), expect to see smaller incremental updates more frequently. Here are examples of things coming soon after General Availability:

- Create reports that aggregate data from multiple XG Firewalls
- Save and export reports in multiple file formats to share with others
- Report scheduling
- Additional reports
- And much more!