CASE STUDY

SYSLOG ANALYZER

Syslog Analyzer helps Latin American cable operator improve network monitoring and performance

THE CUSTOMER

A large cable operator in Latin America uses Syslog records from core network elements to monitor and improve the network.

THE CHALLENGE

The cable operator needs the ability to monitor network data and generate alarms in real-time across a massively distributed network consisting of multiple Network Operations Centers located in far reaching geographies.

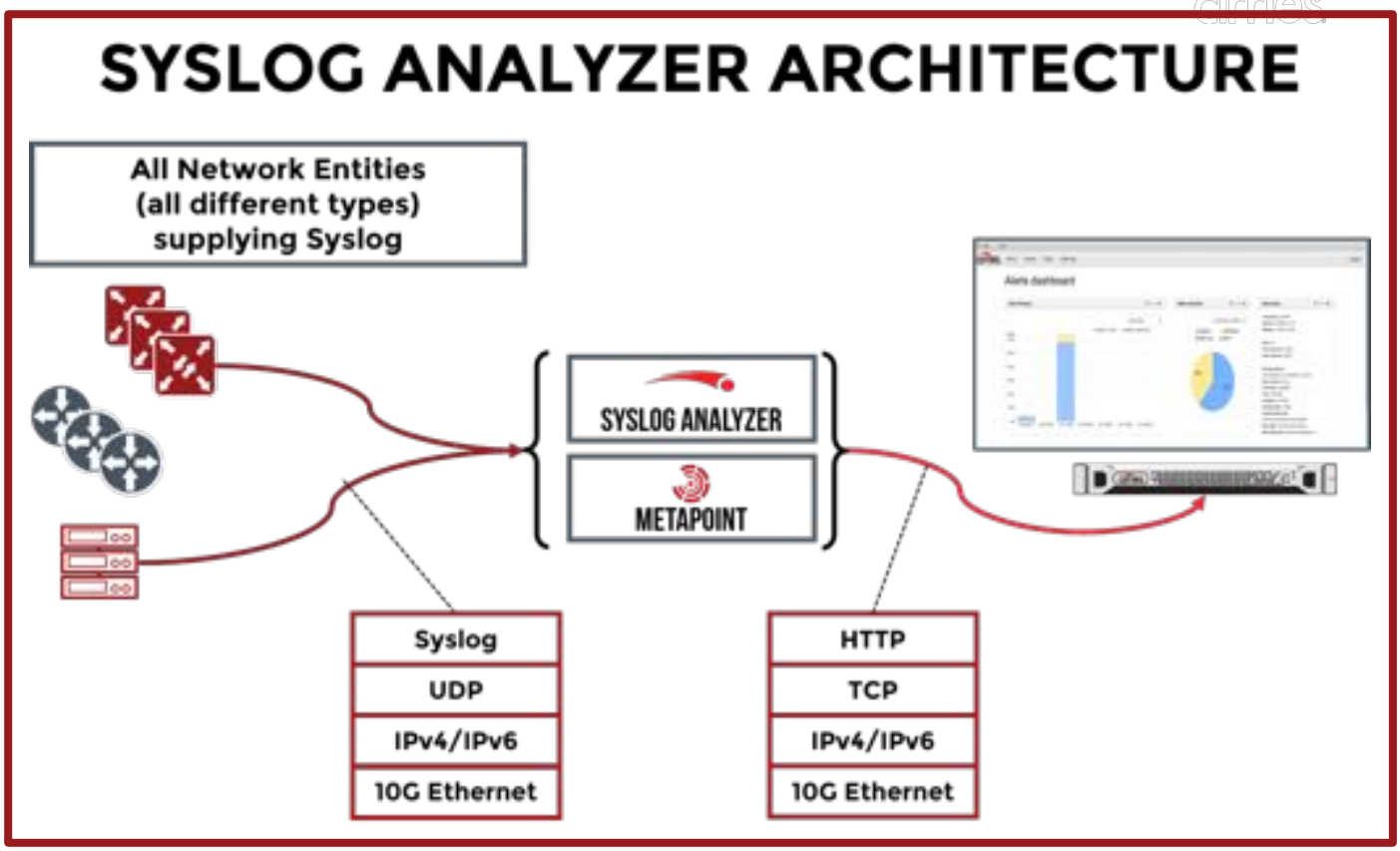
The operations team also needs better insight into network and element performance over time. Syslog records must be stored on a continual basis for an extended period to enable historical and predictive analysis.

THE ANSWER

The Syslog Analyzer, based on Cirries MetaPoint, collects syslog records from all network elements and stores them for an operator defined period, in this case six months. Alerting rules based on event severity and counter thresholds are configured to generate color-coded alarms to the Syslog Analyzer dashboard. The records are parsed and indexed, available for keyword and time-based searches from the dashboard.

HIGHLIGHTS

- Massive streaming of syslog messages
- Syslog Analyzer collects all syslog messages
- Big Data storage solution for long term trending and analysis
- Dashboard provides powerful analytic tools for intelligence mining. Allows keyword search for any specified time frame
- Real-time rule-based monitoring and alarm generation
- Operator programmable rule engine



SYSLOG ANALYZER BENEFITS

- Alarms – By collecting Syslog from all elements in the network, and allowing a rules-based policy to be defined, alarms can be reported for network-wide exceptions that could not be reported by a single element

- Troubleshooting – When a customer reports a problem or a response to an alarm is needed, troubleshooting a problem across multiple network elements is difficult. By collecting syslog from all elements and allowing flexible reports by selecting different types of data from different elements, problems can be identified more quickly

- Trends – By collecting the syslog from the network, storing them for multiple years and providing a flexible reporting capability, data from the network can be used to analyze trends and plan more effectively.

ABOUT CIRRIES

Cirries Technologies software empowers network operators and companies in the network visibility, fault isolation, performance and security industries. Cirries' products can digest data from multiple sources and reduce it to the right format for real-time notification, storage or application use to reveal real-time performance and security of any network. Cirries' software is highly scalable and easily deployed on COTS hardware, virtual machines or in the cloud.