Technical Overview

SysLog Custom SD-WAN Integrations

QOS NETWORKS

Business Need

Enterprises today are subject to more and more security and protocol requirements than ever before. As a result, implementing new solutions into their IT ecosystem can be cumbersome, time-consuming, and overall difficult to undertake. We see this often with compliance-based industries like finance, insurance, retail, manufacturing, etc. and come up often when considering new network solutions.

Strict audit requirements often precede these compliance certifications and the ability to perform and provide crucial information is the difference between passing or failing compliance. One such example are customers that are required to log and maintain lists of IP addresses that are identified as potentially malicious, including alerts to identify when these malicious actors are active.

VeloCloud Integration

Integrating with a VeloCloud solution, one of the integrations QOS has written includes an automated logging and alerting solution that triggers whenever a bad agent from the black listed IPs tries to access their site via the VeloCloud edge.

The VeloCloud edge contains an internal stateful firewall that blocks all incoming requests by default, unless they are explicitly allowed via the VeloCloud orchestrator. To facilitate these security logging requirements, QOS developed a solution that looks for incoming requests from these specific IP addresses, logs these requests in a specific format and streams them to the customer's syslog environment. The request is blocked by the VeloCloud edge and the customer is alerted via their existing environment. The VCO also doesn't have a native way to log incoming requests; just outbound or sources that are specifically NAT'd to an internal destination. There is also not a native way to manage a blacklist of IP addresses. They block everything incoming by default and let you white list specifics. Customers who need a more flexible way to log incoming requests can benefit from the custom integrations QOS has written.

This solution can integrate with any other integrated firewall platform. Other integratable platforms include offsite syslog servers or other managed security platforms. QOS can ship these log events to syslog on the customer side with the custom integrations into a customer's specified platform.

QOS NETWORKS

Learn more at qosnet.com/management-and-monitoring