WATERFALL®
Stronger Than Firewalls

WATERFALL FOR SYSLOG

SAFE EVENT NOTIFICATIONS

The Syslog protocol is widely deployed to transport and relay messages, from originators to collectors, over UDP, TCP and TLS. In Industrial Control System (ICS) networks, originators are typically industrial devices and severs, while syslog collectors and relays can be deployed on enterprise WANs or over the Internet as cloud services. Connecting enterprise networks to industrial Syslog sources through a firewall, however, is high risk. All firewalls that permit data to leave an industrial system also permit attacks to enter that system.

The Waterfall for Syslog connector is part of the Waterfall Unidirectional Security Gateway family of products. The Syslog replicas provide Syslog collectors with the data that SOCs need to analyze, diagnose, and respond to OT events, such as security incidents, predictive failure warnings, or fault conditions. The connector replicates Syslog alerts and sources unidirectionally and in real-time, from industrial networks to IT networks, without the risks that always accompany firewalls.

The Waterfall for Syslog connector is simple to install, with powerful web-based configuration and monitoring tools. Comprehensive diagnostics include real-time alarms via Syslog, Windows logs, email, SNMP traps, log files, and Waterfall's monitoring console.

BENEFITS OF USING WATERFALL FOR SECURITY MONITORING

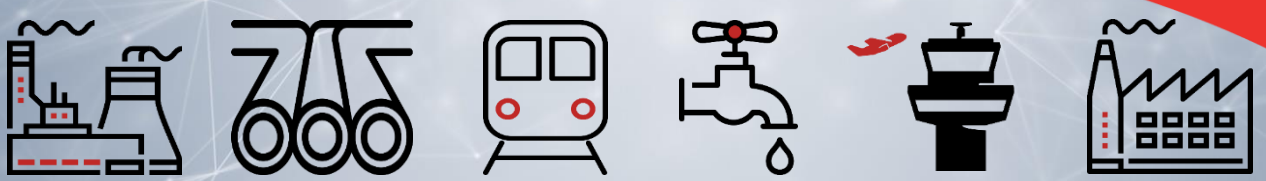
Secure replication of Syslog transport messages

Simple deployment – connector runs entirely in the Unidirectional Gateway with simple web user interface

Not physically able to transmit any remote attacks or malware propagation from external networks into protected networks

Facilitates compliance with NERC CIP, NIST 800-82, ANSSI, IEC 62443 and more

Safe visibility into industrial control system networks and systems from central and cloud-based SOCs



WATERFALL®
Stronger Than Firewalls

WATERFALL FOR SYSLOG

Central security monitoring is focused on events and alerts encoded as Syslog messages. Waterfall for Syslog is a standard Syslog server on a protected industrial network, gathering Syslog messages from that network. Syslog alert content and metadata are forwarded through Unidirectional Gateway hardware. On the external network, new Syslog alerts are formulated and sent to a central enterprise or cloud-based SIEM or SOC installations without risk to operations.

Waterfall for Syslog can gather data from an unlimited number of Syslog-capable hosts, network devices, industrial devices or other sources. There are no limits on data sources or throughput other than hardware limitations. Waterfall hardware supports standard 1Gbps and 10Gbps connectivity options, and so scales to even the largest of industrial installations.

FULLY-FEATURED & ROBUST SUPPORT:

- Replicates Syslog relays and collectors to enterprise or cloud-connected networks
- Flexible configurations don't require new hosts or software
- Gathers Syslog data from an unlimited number of sources / hosts / devices
- Enables secure, real-time monitoring of critical assets across the organization
- Standard 1-10Gbps connectivity
- Supports an unlimited number of Syslog events
- Supports TCP, UDP and TLS message transport protocols

INFO@WATERFALL-SECURITY.COM | WWW.WATERFALL-SECURITY.COM

ABOUT WATERFALL

Waterfall Security Solutions' unbreachable OT cybersecurity technologies keep the world running. For more than 15 years, the most important industries and infrastructure have trusted Waterfall to guarantee safe, secure, and reliable operations. The company's growing list of global customers includes national infrastructures, power plants, nuclear generators, onshore and offshore oil and gas facilities, refineries, manufacturing plants, utility companies, and more. Waterfall's patented Unidirectional Gateways and other solutions combine the benefits of impenetrable hardware with unlimited software-based connectivity, enabling 100% safe visibility into industrial operations and automation systems.