Cloud Visibility: Industrial
Providing Visibility to Your Industrial SCADA Virtualization Environment

Industrial networks are looking to virtualize their environments to reduce hardware, infrastructure and facilitation costs as well as enabling better SCADA software integration into the existing virtualized IT environment.

With the growth in SCADA (Supervisory Control and Data Acquisition) deployments, a computer system for gathering and analyzing real-time data, virtualization has provided challenges to gaining 100% visibility of virtualized SCADA network traffic.

Challenge: Many of these challenges are tied to hardware and software infrastructure complexity. Current network designs deploy a multitude of servers, each server with a dedicated task, like one handling all Manufacturing Execution System (MES) data, one handling the Enterprise Resource Planning (ERP), and another server for the SCADA platform. All of this integrated to the IT infrastructure, such as WSUS server, Domain Controller (DC) server or Active Directory (AD) server, who each run different operating systems, like MES runs on Windows Server 2003, ERP runs on Windows Server 2008 and the SCADA solution runs on Linux.

If one of these servers were to go down, a failure in the power supply or CPU, leads to a cascading effect of the applications going down, leading to data loss and loss of functionality of the IT infrastructure.
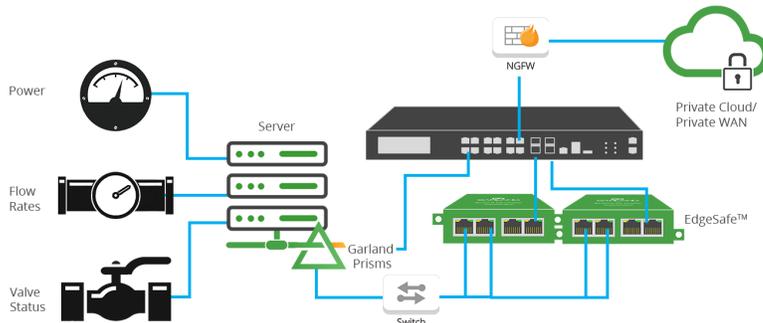
Goal: The concept with SCADA Virtualization would be to consolidate all of these servers and applications to run on one physical server, through a virtual environment. A comprehensive network virtualization strategy includes network visibility, network infrastructure, network redundancy, and disaster recovery. All with the goal of providing network continuity, process availability, while improving plant efficiency and reducing network complexity.

In these environments, the availability of data within industrial automation is critical. Optimized security and performance starts with 100% visibility into network traffic including both virtual and physical environments. And visibility starts with the packet. A network visibility fabric that includes network TAPs and packet brokers, provides complete network visibility and link optimization, can reduce network complexity, enable easier infrastructure upgrades, facilitate traffic growth and improve the effectiveness of SCADA tool performance.

Virtualized SCADA Substation Deployment

Solution: Migrating a utility substation design to a virtualized SCADA deployment offers many benefits including hardware server consolidation, high availability, migration capabilities, and easier backup and restore processes. However virtualizing a SCADA deployment leads to many challenges including having to reconfigure resource allocation, conflicts with network OS activities and reduced visibility into the substation.

Deploying Garland Prisms traffic mirroring with the substation server hypervisors, eliminates this data blind spot, providing the SCADA platform and any other connected system access and visibility. Integrating this virtual packet traffic with physical layer network TAPs and packet brokers provides a complete end-to-end visibility fabric.
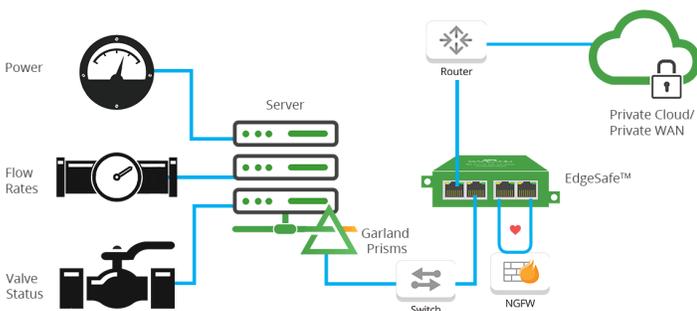

Benefits:
- Single-sensor for Public/Private cloud
- Private controller for air-gapped architectures
- Supports containers, Linux, and Windows Server
- TLS decryption including 1.3 and predecessors
- Integrates with Garland's physical network TAPs and packet brokers

Substation Firewall Optimization

Challenge: Another common utility challenge is firewall optimization within a substation. Updating firewall firmware can mean eliminating access to the substation during the firewall update cycle causing blind spots.

Solution: Deploying an external Bypass TAP in substation locations, offer the unique ability to implement inline lifecycle management, sandboxing firewall deployments, to easily taking out-of-band for updates, installing patches, performing maintenance or troubleshooting to optimize and validate before pushing back inline, without impacting the availability of the network. Both the bypass TAP and firewall can be remotely managed to automate the entire process.

Benefits:
- Scripting support or cloud orchestration
- Maintains control center visibility
- Remote accessibility
- Failover on loss of power
- Ease of configuration

With the constant change, all industrial processes are subject to, companies are taking the leap virtualizing SCADA environments with the ultimate goal to achieve reduced hardware, infrastructure and facilitation costs.

Garland Prism's cloud visibility with TLS decryption addresses this challenge with the industry's most flexible and feature-rich cloud traffic mirror providing complete visibility into tough to reach encrypted virtual traffic. Looking to learn how to provide visibility into your environment? Contact us for a free Design-IT session with our engineer team today!

Network TAPs + Packet Brokers + Inline Edge + Cloud Visibility | GarlandTechnology.com | +1 (716) 242.8500 | sales@garlandtechnology.com

072220