Radiflow

CASE STUDY

Securing a Midwestern G&T Power Utility

THE CHALLENGE

Several requirements needed to be met to support the network project:

- Mechanism to control and monitor access to sub-station assets, according to NERC CIP v6 requirements
- Mechanism for creating specific firewall rules at BES Asset Boundaries for a variety of substation topologies, as per new CIP requirements
- Compliance with upcoming NERC CIP requirements for transient assets
- Serial connectivity, which is still required at several substations for legacy applications
- Environmental hardening was an imperative, as the power supply to hundreds of thousands of customers would be controlled and monitored by this technology
- User-friendly configuration and management

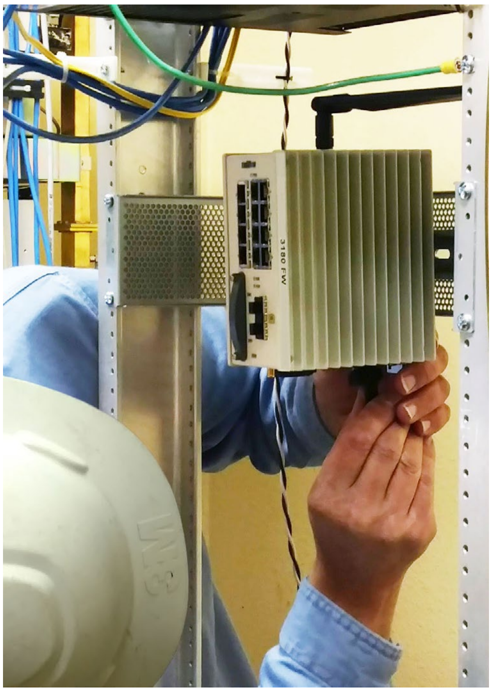
THE SOLUTION

For this project the utility chose Radiflow's 3180 Ruggedized Security Gateway. It has the capability to monitor traffic and send syslog connection data messages back to a central server. This allows the operator to examine traffic patterns and create specific firewall rules that can be loaded back into the 3180.

For secure remote access the 3180 offers a unique, highly granular feature called APA (Authentication Proxy Access). APA allows the operator to define specific date/time/user/device/protocol parameters for remote IED access. Once a technician has successfully authenticated into a 3180, a PCAP record is generated and stored for future network forensics.

The 3180's DIN-rail mounting and compact size make it perfect for small enclosures, while supporting a variety of interfaces – Copper and Fiber Ethernet, serial and even dual-cellular ports. Support for multiple 3G/4G networks ensures continuous connectivity without overloading the limited microwave links. The 3180 can be ordered with serial RS232 or RS485 interfaces to support legacy applications via terminal server application.

The 3180 Gateway meets and exceeds the rigorous requirements for IEEE1613 and IEC61850-3 certifications, which define the benchmark standards for communication devices within power utility environments.



Installing the Radiflow 3180 Ruggedized Gateway

In addition to the 3180 Gateway, the project included Radiflow's iSIM management tool, as well as the iSID Industrial Cybersecurity & Intrusion Detection System.

Radiflow's iSIM is a powerful centralized management tool for all of the 3180's features, including ACL management. It presents a network topology map in both logical tree structure and graphical map. In addition, iSIM supports pre-scheduled software updates and database backups.

Radiflow's iSID Industrial Cyber Security & Intrusion Detection System enables mapping application flows in substations, which in turn allows writing more accurate and more secure firewall rules, in preparation for firewall deployment.

Furthermore, used as a passive monitoring tool, iSID can further detect and alert on any anomalies in the sub-stations using its six security engines. It continuously checks for known vulnerabilities (signatures) and anomalies and is able to alert SIEM systems of potential attacks.

One of the Radiflow-equipped substations inlcuded in the project

FINAL DECISION

Factors that pushed Radiflow into the winner circle included:

- Numerous security features, all contained within one compact device (firewall, APA, VPN, etc.)
- Ability to monitor connections and provide relevant data back to a central site
- Radiflow Engineering and Technical Support Services
- A comprehensive cybersecurity solution and associated management capabilities

About Radiflow

Radiflow develops unique OT cybersecurity tools to protect and ensure organizations' digital resilience. The company closely collaborates with Managed Security Service Providers to oversee the discovery and management of all relevant data security points. Founded in 2009, Radiflow has offices and partners in Europe, USA and APAC. Its field-proven solutions are installed at over 6000 sites around the globe.

Radiflow