Quantalytics

Power Substation Network Architecture Review

Electric Power Substations are potentially, and paradoxically, both the weakest and strongest links in the power generation and distribution industry. Strongest, because their very well defined functionality makes it possible to lock down the activities that are allowed, and ban the rest. Weakest, because unless they have been hardened adequately against both physical intrusion and network intrusion, they offer multiple attack surfaces.

This is true even if the substations are using Modbus over a POTS phone line and modem. The same connection can potentially be subverted to carry other traffic, such as malware, as well as eavesdrop in order to perform reconnaissance. Our network security appliances can be configured to protect any substation using the most basic to the most advanced hardware and communications protocols.

In order to bring the benefits of TCP/IP remote access, monitoring and management to networks of far-flung power substations, it is necessary to deploy a complete and comprehensively secure network. Quantalytics has created a network security ecosystem to accomplish this.

Appliances at each Substation:

1. **Q-VPN®**. The Q-VPN allows for the creation of VPN-to-VPN networks with extreme granularity of control over the TCP/IP devices at the substation.

2. **Q-GridPot®** is a honeypot appliance specifically designed to mimic electric grids, including substations. The Q-GridPot is built on top of Conpot, and, again, is specifically for electric grids, including imitating operators' HIDs. In the event of a breech, this will help deny the attacker an accurate surveillance of the subsystem infrastructure, and serve as a tripwire if the hackers manage to bypass the other precautions. The number of attack surfaces is limited to the number of IP addresses available on each VLAN segment.

3. **Q-MBus®** The Q-MBus is a Quantalytics appliance that converts a serial Modbus connection to TCP/IP. This allows Modbus data to run over a VPN.

The Internet connection can be DSL, a cable modem, fiber optic, satellite, or Ethernet-over-Powerline.

All TCP devices connect to a managed switch that is managed via the VPN connection.

Appliances at The Control Room:

1. **Q-VPN®** creates VPN-to-VPN networks with extreme granularity of control over the TCP/IP devices at the substation. We recommend using 2 for failover and load balancing.

2. **Q-Box®** enables monitoring of all network devices and services via Nagios. The version of Nagios deployed in the Q-Box for monitoring includes the ability to monitor Modbus over TCP/IP. We recommend using 2 for failover and load balancing.

3. **Q-Vul®** is a vulnerability assessment and monitoring appliance built using OpenVAS to cover the substations. Even if no patch is available, or there is no time window available to deploy it, knowledge of security holes is still very valuable. The vulnerabilities, once known, can, at a minimum, be closely watched.

4. **Q-NAC®** (Network Access Control), built using PacketFence, provides full control over allowed devices and services. The Q-NAC can thwart a physical penetration of a substation, including providing protection against physical attack via plugbots.

5. **Q-Log®** is a log aggregation and analysis tool running the ELK Stack (Elasticsearch, Logstash, and Kirbana). The Q-Log processes log entries and issues alerts. The Q-Log works in conjunction with all Quantalytics appliances plus any device that has a log and can output it, as well as any SIEM system. (e.g. Q-OSSEC.)

6. **Q-IDS®** is an Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) built using Suricata. We recommend using 2 Q-IDS appliances for failover and load balancing. Suricata uses Snort definitions in addition to heuristics.

***Quantalytics** appliances are designed to be used individually, or can be combined as a synergistic ecosystem to maximize cybersecurity effectiveness.*