Securing SCADA Protocols for NERC CIP

Connected Grid Network Architecture Services' custom signatures restrict access to substation devices for compliance.

Case Study

Industry: Power Utilities

Location: United States

Business Impact:

Benefits delivered by the Cisco solution include:

- Address NERC CIP requirements
- Prevent unauthorized traffic from reaching end devices
- Reduce amount of traffic over the network
- Increase reliability of the network and power grid

Business Challenge

Utilities must create a secure, reliable grid under the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards. As utilities seek to enable their grids with more sophisticated IP communication devices, cyber security threats become an increasingly important factor hindering the achievement of the reliability goal. Although NERC CIP helps utilities understand and address these security threats, its implementation poses a challenge for utilities due to the unclear mapping between traditional enterprise IT security features and the regulatory requirements.

Security concerns are increasing with the increased adoption of two-way communications to improve power system operation and asset management. For example, adequate security must be provided for all communications to voltage var control, remote device management, and intelligent distribution devices. Breaches in security on these communication links can lead to power system outages or instability. Securing the modern power grid requires in-depth knowledge of power systems engineering as well as advanced communications technology knowledge. In addition, the security solution must fit the existing IT/OT infrastructure used by the utility. This is a complex set of skills that is very difficult to find.

Solution and Results

Cisco brings together strong power system, communications technology, IT, and OT to provide the most comprehensive solutions to secure mission-critical Supervisory Control and Data Acquisition (SCADA). For example, Cisco was asked by a utility to:

- Analyze and model Modbus traffic
- Analyze network and SCADA communication traffic
- Characterize bandwidth and latency requirements
- Identify vulnerabilities

Cisco:

- Developed Modbus signatures
- Implemented standalone IPS device design at the control center between SCADA master and slave
- Delivered a modern design that met bandwidth and latency requirements
- Provided day one support to adjust signatures
- Reduced false positives

Cisco Connected Grid Services

Cisco® Connected Grid Network Architecture Services invites utilities to prepare for the smart grid future through its comprehensive planning services that assess current strengths and weaknesses of their networks and provides them with options for optimizing their investments. Cisco Connected Grid Services automates the entire energy chain and dramatically increases grid reliability and responsiveness while lowering costs.

"Together with Cisco, we determined and implemented solutions to best monitor, migrate threats, and protect grid facilities in our network for reliable and consistent delivery."

Director
Power Utilities Company

C36-693302-00 02/12