Electric Transmission Data Networks and NERC CIP

Summary

Industry

Electric Utilities

Overview

This use case provides a high-level reference design for network security in electric transmission data networks. It is based on real-world deployments that use Palo Alto Networks Next-Generation Firewall and have been implemented in North American electrical utilities subject to NERC CIP compliance. These utilities have taken their implementations through audits with NERC's regional entities and security reviews performed by the US Department of Homeland Security and the Idaho National Laboratory.

Using this design as a foundation, transmission data network security professionals will have a security subsystem that:

- Makes anomalous/malicious traffic easier to detect.
- Makes security policies easier to manage and maintain.
- Makes logs easier to read and filter to get to useful information.
- Simplifies documentation required for compliance reporting purposes.
- Provides a solid foundation to support evolving compliance requirements.

Some important notes about this use case:

- Although entities can pass audits by implementing minimum controls, that is not the focus here. Rather, this paper's focus is on helping utilities exceed the minimum by implementing better segmentation and more advanced capabilities that allow them to detect and prevent advanced cyberattacks.
- Much of this paper's discussion focuses on NERC CIP compliance, but the concepts are very much applicable to unregulated environments in North America, such as distribution data networks; T&D networks in countries outside NERC jurisdiction that may still be subject to local laws; or countries that are simply looking for best practice references.

Business Drivers and Challenges

As backdrop, it is useful to have a brief discussion on the different business drivers for improving grid cybersecurity and related business problems.

Business Drivers

NERC CIP Regulations

Electric utilities with assets that are subject to the cybersecurity regulations under NERC CIP need to implement the necessary controls and processes to meet their regulatory obligations. Tremendous costs are involved in these compliance activities in terms of capex and opex, and even bigger costs could be involved if organizations are deemed to be in violation of the standards. Thus, it is in the interest of these organizations to find the solutions that allow them to meet their compliance obligations and run their compliance activities in the most cost-effective manner. While not subject to regulations, other organizations—for best practice reference as well as in anticipation of future regulations—are using elements of the NERC CIP standard as part of their own cybersecurity policies.

Business Continuity

The concern over securing the grid from advanced attacks deployed by various threat actors, such as nation-states and well-resourced cybercriminals, is increasing. There are now multiple publicly disclosed incidents that demonstrate that the threats are legitimate. For example, the December 2015 and 2016 attacks on the Ukrainian power grid showed that remote cyberattacks to electric substations with the intention to cause a mass outage are possible.[1] Similarly, although there was no reported service outage, ransomware proved effective in compromising the Lansing Board of Water and Light in the state of Michigan in the United States.[2]

Grid Modernization

Aging electric grid infrastructures are being modernized to "smart" and Industrial Internet of Things (IIoT) models to increase operational efficiency and reduce costs. This update includes increased connectivity to extraneous ecosystem networks, migration to a common Internet Protocol-based network, increased use of the cloud, and wider use of mobility. We see more smart grid, substation automation, and cloud-based analytics projects coming online, supporting this trend. The increased modernization has also caused many organizations to think about the new cyberattack vectors that come with this modernization and to include this factor in their planning for OT modernization.

Business Challenges

Organizations are trying to address the following common business problems:

- **Stiff penalties for compliance violations:** Entities subject to NERC CIP regulations must meet the requirements or face stiff penalties. Organizations need to ensure they have the proper tools and systems that allow them to achieve and maintain compliance.
- **High cost of compliance activities:** The cost of running compliance activities is very high. Organizations are constantly looking for ways to streamline their compliance activities and reduce capital and operational expenditures.
- **High potential economic impact of an outage:** There may be tremendous negative consequences to economies should critical electricity services be compromised for an extended period.
- **High potential compromise to people/environmental safety:** Similarly, there could be severe compromise to the safety of people and the environment during extended downtime or if equipment were destroyed in a cyberattack, whether intentionally or by accident.
- **Risk of lawsuits**: Should the aforementioned incidents occur due to a successful cyberattack, utilities could be subject to financially

1. "'Crash Override': The Malware That Took Down a Power Grid," Wired Magazine, June 12, 2017, https://www.wired.com/story/crash-override-malware.
2. "Michigan Power and Water Utility Hit by Ransomware Attack," SecurityWeek, May 3, 2016, https://www.securityweek.com/michigan-power-and-water-utility-hit-ransomware-attack.

Table 2: NERC CIP Standards Relevant to Palo Alto Networks Next-Generation Firewall		
Standard	**Title**	**Requirements Directly Provided (P) or Supported (S)**
CIP-002-5.1	Cybersecurity – BES Cyber System Categorization	Not applicable
CIP-003-8	Cybersecurity – Security Management Controls	S: 1.1.2, 1.1.4, 1.1.5, 1.1.7, 1.2.3, 1.2.4, 2 A-3, 2 A-4
CIP-004-6	Cybersecurity – Personnel & Training	Not applicable
CIP-005-6	Cybersecurity – Electronic Security Perimeter(s)	P: 1.1, 1.2, 1.3, 1.5, 2.1, 2.2, 2.3, S: 2.2
CIP-006-6	Cybersecurity – Physical Security of BES Cyber Systems	Not applicable
CIP-007-6	Cybersecurity – System Security Management	P: 1.1, 1.2, 3.1-3.3, 4.1, 4.2, 4.3, 5.1, 5.2, 5.4, 5.5, 5.6, 5.7, S: 2.1, 2.2, 2.3, 2.4, 4.4
CIP-008-6	Cybersecurity – Incident Reporting & Response Planning	S: 1.1, 1.2, 2.3
CIP-009-6	Cybersecurity – Recovery Plans for BES Cyber Systems	P: 1.5 S: 1.3, 1.4, 2.1, 2.2, 2.3
CIP-010-3	Cybersecurity – Configuration Change Management & Vulnerability Assessments	P: 1.1, 1.2, 2.1 S: 1.3
CIP-011-2	Cybersecurity – Information Protection	P: 1.2, 2.1, 2.2

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

parent_ds_electric-transmission-nerc-cip_011824