OWL Cyber Defense

CASE STUDY

Improving the Security Posture of a Consolidated Utilities Energy Management System

Summary

ABOUT THE CUSTOMER

A leading U.S. competitive energy provider, the company incorporates 6 power and gas utilities, power generation, transmission, and delivery, and competitive energy sales, and serves over 10 million end customers in the United States and Canada.

CASE SUMMARY

To improve the security posture of its NERC CIP-compliant consolidated utility interfaces, the company aimed to implement a number of new security tools and techniques, including data diodes. This project involved the unidirectional and bidirectional transfer of ICCP, SFTP, HTTPS, and PI System historian data between 8 Production and 4 Test high availability (HA) clusters on two geographically separated instances to a power system balancing authority and neighboring utilities. After a review of proposals, the company chose Owl Cyber Defense data diodes for their capabilities in handling multiple data types and data flows, and both unidirectional and bidirectional transfers, with fewer devices, a lower overall cost, and a simpler architecture.

Cybersecurity Challenge

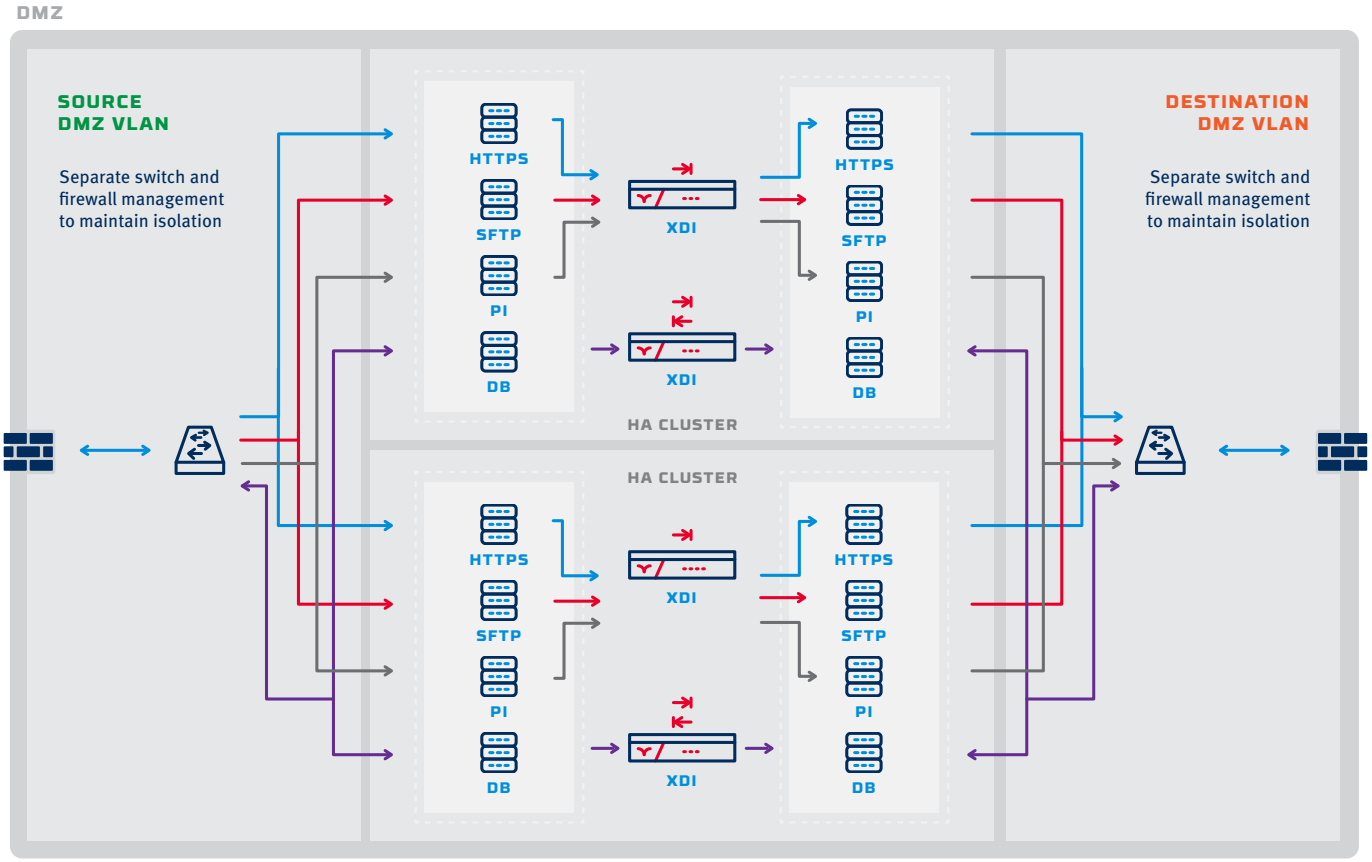
As a part of the company's project to update and harden their power transmission systems, the company was focused on improving the security posture of its fully NERC CIP-compliant consolidated utility interfaces through improved security tools and techniques, including the acquisition and implementation of data diodes. This project involved the unidirectional and bidirectional transfer of ICCP, SFTP, HTTPS, SQL database, and PI System historian data between 8 Production and 4 Test high availability (HA) clusters on two geographically separated instances to a power system balancing authority and neighboring utilities.

REQUIREMENTS

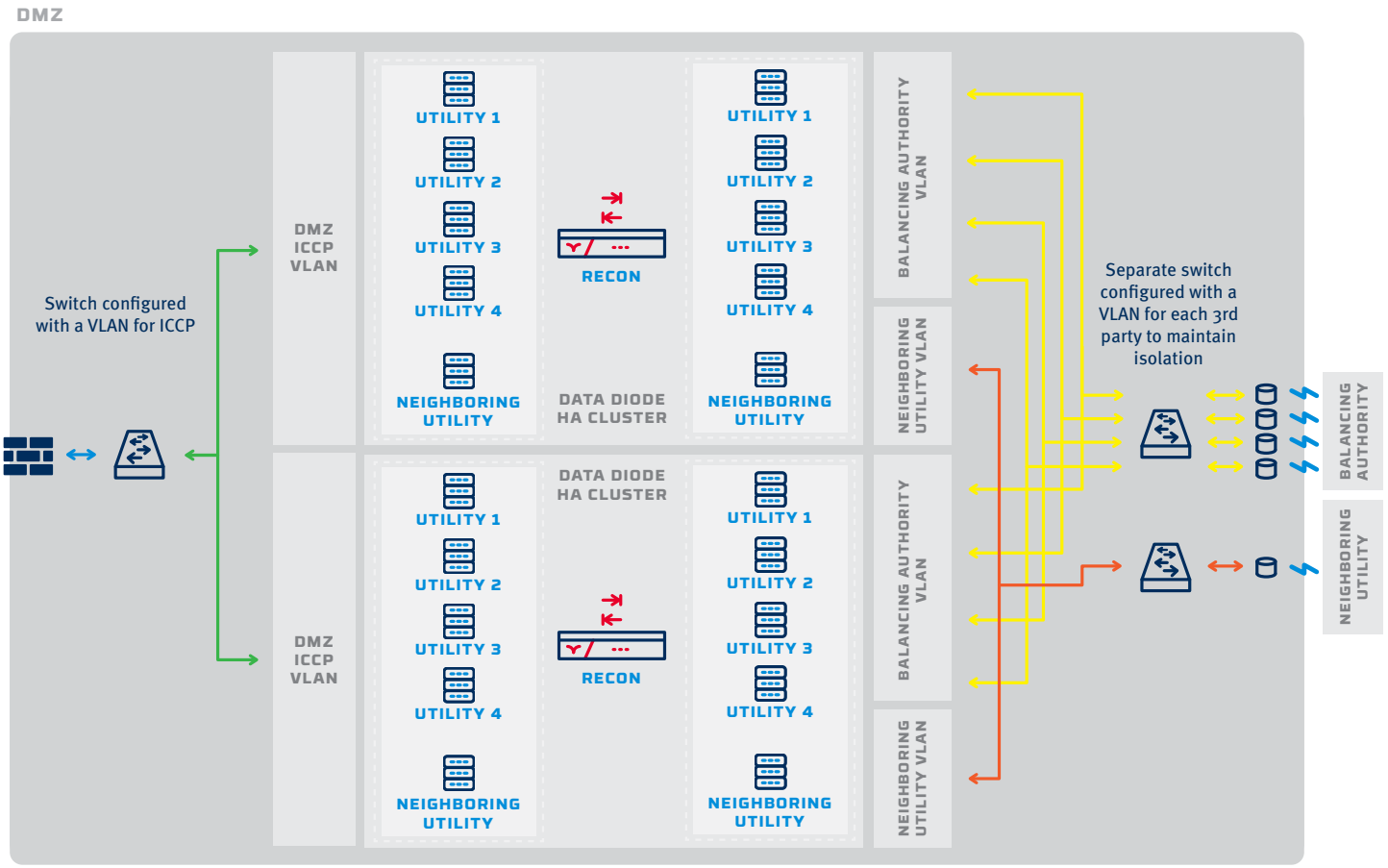
- Securely connect bidirectional ICCP data flow for 4 production DMZ and 2 test DMZ data flows with high availability redundant pairs for each connection
- Securely connect bidirectional DB synchronization data flow for 4 production DMZ and 2 test DMZ data flows with high availability redundant pairs for each connection
- Securely connect unidirectional data flow for SFTP, HTTPS, and PI System historian data for 4 production DMZ and 2 test DMZ data flows with high availability redundant pairs for each connection
- Best in class capabilities, including low latency, high throughput capacity, and ability to handle multiple data flows and data types
- Provides broad support for application integration
- Enable data flow content inspection and filtering to further reduce cyber risk
- Provide enterprise-grade scalability and redundancy to meet mission critical resiliency
- Adheres to architecture security requirements, including NIST Cybersecurity Framework and DHS industrial control systems security guidance

Solution Architecture

SFTP, HTTPS, PI SYSTEM, DB REPLICATION



ICCP TRANSFER



Solution Description

The solution was initially architected under the assumption that each data type would require its own secure data transfer solution – a total of 30 units across all connections. The proposed solution consolidated the FTP/SFTP, HTTPS, and PI System historian data flows into one XDI system per connection, reducing the overall number of required units by nearly half, to just 18 units, without impacting performance or reliability.

ICCP and database synchronization data flows from the production facility networks to the balancing authority and neighboring utilities were enabled through the ReCon data diode. This provided the capability to transmit data bidirectionally without exposing the operational network to unauthorized external access.

XDI

The world's first and only cross domain solution developed specifically for operational technology (OT) networks, protocols, and data types. XDI features 1 Gbps unidirectional or bidirectional throughput with advanced content filtering. Combined with hardware-enforced domain separation and protocol termination, XDI effectively eliminates network information data leakage.

ReCon

A specialized bidirectional data diode, designed to combine the same proven security benefits of a hardware-enforced data diode cybersecurity solution with the ability to provide secure round trip communication. Features single-side command and secure authentication capabilities in a compact, 1U form factor.

Results & Customer Benefits

Unlike competing unidirectional gateway technology, Owl network security and data transfer solutions supported multiple data types and formats simultaneously on a single 19" 1U appliance with no flanking servers, saving power, valuable rack space, and countless service hours. This premier capability enabled the utility company to be far more agile and provided the ability to adapt quickly in case of changing requirements without the need for additional purchases, change management, or significant downtime.

The company also benefited from compatibility with over 35 industrial applications, historians, and protocols, including PI System, ICCP, HTTPS, and SFTP as well as security intelligence, data loss prevention (DLP), and intrusion detection systems (IDS), such as LogRhythm, Splunk, Indegy, Claroty, and Morpho Detection.

Because it was based on proven, validated data diode architectures within previous deployments for electronic security perimeters, as well as NIST Cybersecurity Framework principles, the solution provided secure external data flows with hardware-enforced protection and did not alter the NERC-CIP compliance of the utility network.

KEY BENEFITS

- NERC-CIP compliant, hardware-enforced security on all external data flows
- Multiple unidirectional data flows consolidated into a single data diode unit for transfer
- Bidirectional support for non-unidirectional data types, including ICCP and database synchronization
- Built-in sophisticated content inspection and filtering based on military-grade technology
- Best-in-class capabilities provide high performance, low latency, and a wide array of supported protocols and data types in a low-SWaP form factor
- Scalable deployment allows for easy throughput upgrades and added data types

OWL Cyber Defense

Owl Cyber Defense cross domain, data diode, and portable media solutions provide hardened security checkpoints for absolute threat prevention and secure data availability. Certified by the U.S. government, independent testing authorities, and international standards bodies, Owl technologies and services help to secure the network edge and enable controlled unidirectional and bidirectional data transfers. For over 20 years, clients worldwide in defense, intelligence, and infrastructure have trusted Owl's unmatched expertise to protect networks, systems, and devices.

For more information on Owl, or to schedule a demo, visit www.owlcyberdefense.com

@OwlCyberDefense

203-894-9342 | Info@owlcyberdefense.com

C002 | V1 | 3-22-2021