cigre PARIS 2022

VTAN CONSULTING

PowerWater

Study Committee D2

Information Systems and Telecommunications

Paper 10588_2022

A METHOD IN EVALUATING THE EFFECTIVENESS OF SUBSTATION FIREWALLS AND A SUBSTATION PERIMETER ARCHITECTURE IN CONNECTING THIRD PARTY GENERATORS TO A TRANSMISSION SUBSTATION

Victor TAN[1], Brendan GRAHAM[2], Paolo TUAZON[2]

[1]VTan Consulting, [2]Power and Water Corporation

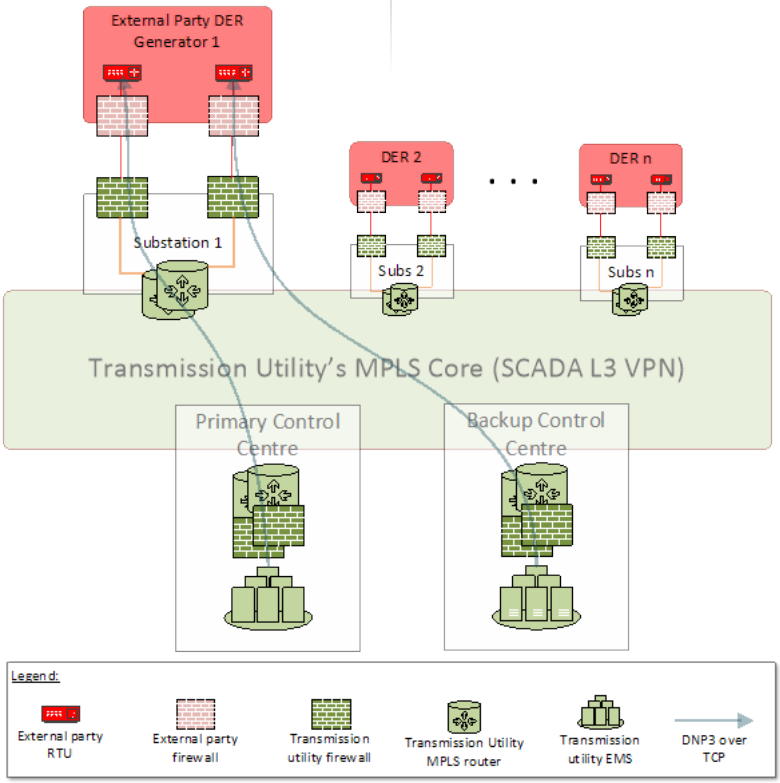
AUSTRALIA

Motivation

- Increasing demand in DER and renewables requiring external third parties to connect to the transmission utility in various locations.
- Increased SCADA data requiring a move from serial-based connections to DNP3.
- Third party generators are considered untrusted from cybersecurity perspective.
- New cybersecurity architecture was developed to securely connect third party SCADA links to the utility substations was developed.

Method/Approach

- Architecture and design consistent with Cybersecurity standards and best practices (IEC 62443, NIST SP 800-82, Australian AESCSF).
- Evaluation of suitable substation firewalls required prior to detailed design and proof-of-concept.
- Firewalls need to meet the cybersecurity requirements, utility's telecommunication requirements and internal design standards.



VTAN CONSULTING
PowerWater

Study Committee D2
Information Systems and Telecommunications

Paper 10588_2022

A METHOD IN EVALUATING THE EFFECTIVENESS OF SUBSTATION FIREWALLS AND A SUBSTATION PERIMETER ARCHITECTURE IN CONNECTING THIRD PARTY GENERATORS TO A TRANSMISSION SUBSTATION

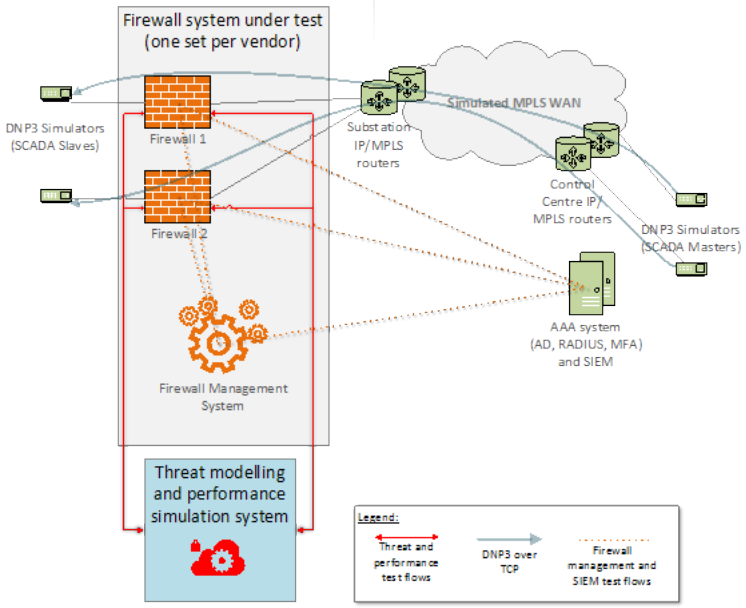
Continued

Test Requirements

- DNP3 protocol awareness (as per IEEE 1815-2012).
- Secure and efficient firewall management (as per IEC 62443, AESCSF, and utility's internal requirements).
- Physical and environmental attributes (as per IEC 61850-3, IEEE 1613, and utility's internal requirements).
- Cybersecurity certification (as per NIAP, Common Criteria, and utility's internal requirements).
- Telecommunications requirements – routing protocols, encryption, MPLS integration (as per utility's internal requirements).
- Security monitoring (as per IEC 62443, AESCSF).
- Firewall resilience – stateful failover, recovery times.
- Firewall effectiveness in stopping attacks based on CVSS criteria.
- Performance evaluation (as per RFC 2544 and Y.1564).

Firewall Evaluation Environment

- Cybersecurity threat modelling and vulnerability injection system.
- Network performance simulation system.
- DNP3 simulator.
- Substation MPLS routers and switches.
- SIEM logging and monitoring system.
- Authentication, Authorisation and Accounting (AAA) system.
- Virtualisation environment.
- Vendor A firewalls and firewall management system.
- Vendor B firewalls and firewall management system.



VTAN CONSULTING

PowerWater

Study Committee D2

Information Systems and Telecommunications

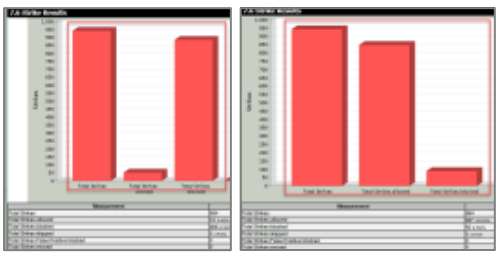
Paper 10588_2022

A METHOD IN EVALUATING THE EFFECTIVENESS OF SUBSTATION FIREWALLS AND A SUBSTATION PERIMETER ARCHITECTURE IN CONNECTING THIRD PARTY GENERATORS TO A TRANSMISSION SUBSTATION

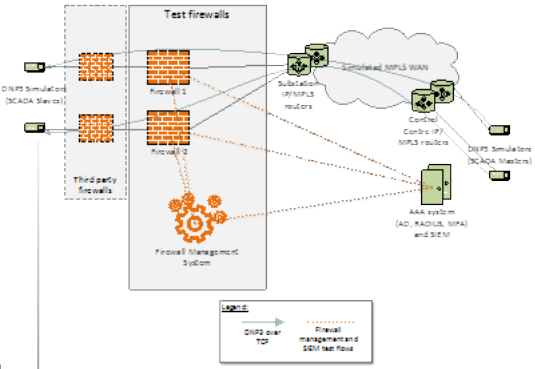
Continued

Test Results

- More than 40 test cases carried out covering the requirements on two sets of vendor devices.
- Differences observed between vendor devices in the results of the test cases, some insignificant, and some very significant ones.
- Vast differences in the DNP3 protocol awareness and capability, for example, ability to decode individual DNP3 operations, and protocol-level fault injection detection.
- Differences in scalability in management of a large number of firewalls in many substations.
- Differences between devices in efficacy in catching simulated network-based attacks:



Subsequent IPSEC Test Scenario



- Subsequent tests were carried specifically to test IPSEC compatibility, and stability impact on DNP3 on a back-to-back firewall.
- Impact of encryption (meeting the utility's cipher and strength requirement) was assessed.
- Impact of high-availability mode failover in the presence of physical firewall failover was assessed.
- Impact of large DNP3 over TCP packet (exceeding the MTU size in the presence of encryption overheads) was assessed.
- Main finding was that the firewall meets the utility's performance and cybersecurity criteria.

Summary of Findings

- Based on requirement evaluation and test results of the test cases, a normalised ranking of features, weighted against the importance of these features to the utility is produced between the firewalls tested: