Firewall Configuration and Path Analysis for SmartGrid Networks

Conference Paper · May 2020

DOI: 10.1109/CQR47547.2020.9101400

5 authors, including:

Abhijeet Sahu
Texas A&M University
35 PUBLICATIONS **125** CITATIONS
SEE PROFILE

Ana Elisa P. Goulart
Texas A&M University
53 PUBLICATIONS **233** CITATIONS
SEE PROFILE

Edmond Rogers
University of Illinois, Urbana-Champaign
10 PUBLICATIONS **91** CITATIONS
SEE PROFILE

Firewall Configuration and Path Analysis for Smart Grid Networks

Nastassja Gaudet[1], Abhijeet Sahu[1], Ana Goulart[1], Edmond Rogers[2], Kate Davis[1]
[1]Texas A&M University, [2]University of Illinois
{[1]tgaudet7, abhijeet_ntpc, goulart, katedavis}@tamu.edu, [2]ejrogers@illinois.edu

***Abstract*—Firewalls are needed in electrical utility companies to protect their substations, control centers and their communication with the balancing authorities. Firewalls also allow the creation of demilitarized zones (DMZ's) in the utilities, where information about the utility's operation can be accessed by the corporate network and outside contractors. As an additional step in creating a cyber topology for a synthetic power system, in this paper we model an electrical utility and the main data flows in and out of its control center. This allows the creation of use cases and firewall rules for each case. The path of selected use cases are analyzed in terms of open ports and risk level.**

***Index Terms*—Smart grid network, Cyber-physical system, Network topology, Firewall rules, ACL, DMZ**

I. Introduction

Firewalls are network devices created to monitor and inspect incoming and outgoing traffic. They provide a layer of defense between networks. A set of rules, or access control lists (ACL's), can be established to allow or block certain packets between those networks. For this research, Cisco firewalls were used, which have a special configuration called a security level. Each interface can be set to have a numerical level from 0-100 that determines its hierarchy in the network. Incoming packets cannot pass from lower security zones to higher security zones without special rules. Typically, the inside of a network is set to a security level of 100, and the outside is set to a level of 0. Furthermore, DMZ's can be created with a typical security level of 50. This means that the main network can access the DMZ to push or pull data from a server since they are going from a high to a low security zone. Specified users from another network with a high security zone may also be able to access the data in that DMZ. However, any user accessing the DMZ will not be able to access the main network, since that would be from a low to a high security zone. Firewalls also use routing commands so that they can forward or discard packets after comparing them to the established rules.

How are firewalls configured to support critical infrastructure such as the electric grid? Is it possible to audit these firewalls to identify vulnerabilities or assess risk in an electric utility's operations technology (OT) network? What type of data flows and DMZ's are typically used in OT networks? To be compliant with the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) NERC-CIP-005 [1], an *electronic system perimeter* is needed. These security perimeters are implemented using firewalls that are carefully configured to protect the utilities' data flows, which are predictable and deterministic, in comparison with traditional data flows.

In our research to develop a communications model of the Texas 2000-bus synthetic model [2], this paper addresses the configuration of firewalls in electrical utility companies, from the substation level, to utility control center (UCC), and balancing authority (BA). This work extends the communications model presented in [3] to include firewall configurations. These allow us to perform risk assessments, simulate different firewall configurations, and perform training to the existing and future workforce. Our ultimate goal is to optimize the firewall rules to minimize vulnerabilities in a utilities' OT network, following the approach used in [4] in which an attack tree model is used to quantify the vulnerabilities in supervisory control and data acquisition (SCADA) systems.

The network policies for the model use the concept of least-privileges in that access to resources is limited to single hosts on a predetermined Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) port based on the requirements of the operation of the power system. Only ports and services necessary for operation are allowed. The control system is used as a central point. The control system initiates connections out to field devices, processes data in real time, then pushes results in real time out to servers in DMZ zones toward corporate and partner operations. Connections towards the control network are not allowed and this helps to reduce the network attack surface of the control system.

The remainder of this paper is organized as follows. The tools for modelling firewall are described in Section II, followed by the main data flows between substations, UCC, and BA. An implementation of the data flows is presented in Section IV, and the paths and risk analysis are presented in Section V.

II. Tools for Modelling Firewalls

There are several tools to model computer networks and firewall configurations. For instance, Cisco Packet Tracer is an educational network simulation tool that allows users to simulate and test network architectures that they create [5]. The model presented in this paper began with a network in Cisco Packet Tracer to show the basic topology including a UCC, substation, BA, and a few DMZ's.

Next, we used NP-View [6] to analyze several firewall and router configuration files and run a path analysis for a risk assessment. NP-View was developed to determine if a company's current or proposed network security is optimal and meets both regulatory standards and best practices [7]. It is a tool that has been tied to this research for over a decade finding its roots in the Trustworthy Cyber Infrastructure for the Power grid (TCIP) research program, and then the Cyber-Physical Security Assessment (CyPSA) project [8]. In addition, NP-View is the standard tool used by NERC CIP auditors to measure network attack surface for Critical Assets in CIP 005 [1].

NP-View uses a path analysis approach to determine a full risk assessment based on the firewall and router configurations submitted to the software. It reads the IP addresses set on each interface and the object-groups [9] created in the file to determine the total number of networks known to each device. NP-View is able to determine every path into and out of a network, and give a warning for the risk level of that particular path. This path includes both the source and destination addresses, as well as the protocol and port used to access the network, which was useful in optimizing our configurations.

III. Data Flows for Smart Grid Network

Before developing the network topology and configuring firewalls using Cisco Packet Tracer to be analyzed in NP-view, we focused on listing these data flows:

- telemetry data requests from control center to substation,
- data from control center to corporate and other DMZ's,
- data from control center to balancing authority.

Figure 1 shows an overview of each of the data flows, color-coded by the protocol used. The firewalls are configured so that only certain traffic is allowed between specified devices with all other applications and users blocked for security. Using Figure 1 as a reference, the data flows are explained next beginning from the substation at the bottom of the figure.

A. DNP3 Protocol

Distributed Network Protocol 3 (DNP3) is a protocol used to control a remote network from a central network. This is mainly used in utility networks with SCADA systems. In industry, port 20000 is used over TCP for DNP3. This creates the SCADA object-group, which is used between the DNP3 Master in the UCC and the relays in the bay level at the substation. This is how the SCADA server is able to control the relays and get telemetry data at any given time. The DNP3 Master in the UCC will initiate the connection and access the DNP3 Outstation (DNP3 O/S) in the substation. The DNP3 O/S will have the current data sent from the Remote Terminal Unit (RTU) that the UCC needs to monitor. A Remote Terminal Access Controller (RTAC) is also found at the substation, which can control the relays locally. The relays can for instance trip a circuit breaker to isolate a faulty circuit. Other devices shown at the substation process level are transformers and switches.

B. Web-based Protocols

The next data flow between the substation and UCC is derived from Web-based protocols. They are used to access data in the smart grid network over HyperText Transfer Protocol (HTTP) and HTTP over Transport Layer Security (HTTPS). These two protocols run over TCP, and use ports 80 or 8080 for HTTP, and ports 443 or 8443 for HTTPS. In the UCC, these protocols are used by the Human Machine Interface (HMI) node to access the local substation data. Within the UCC, vendors will also need to access the web server located in the public DMZ from their own vendor DMZ.

C. Remote Access Protocols

Contractors or vendors access the UCC from an outside node in the global Internet to the vendor DMZ, which includes a dedicated machine for vendors to access. Secure Shell (SSH) and Remote Desktop (RDP) protocols are used for vendors to remotely access the Vendor DMZ, and from there obtain information from the Public DMZ.

D. Database Protocol

In this model, Structured Query Language (SQL) is the database protocol used by the UCC to upload or retrieve data from PI servers [10], also known as historian servers, which archive organized data from the substations and allow operators to perform data analytics. In the substation, the DNP3 O/S pushes the current data received from the RTU to a local database in the substation. The purpose of this is to store a backup of the recent data, which can be accessed by the UCC to see a history of data from the relays. The main database is located in the UCC, as the PI server in the SCADA DMZ. A copy of this database is also available at the Public DMZ, for vendors and corporate users to access.

E. ICCP Protocol

At the top of Figure 1, we have the BA which oversees several utilities connected to the power grid and manages the deregulated energy market. The Inter-Control Center Protocol (ICCP) is a protocol that has been developed internationally for use in energy networks to transfer various types of data including both historical and current data. The BA uses the ICCP protocol to communicate with the UCC via an ICCP server in the BA that accesses an ICCP node in the UCC to pull data.

IV. Basic Network Topology

The network topology used for this project is shown in Figure 2. This network was created using Cisco Packet Tracer, to test if the network included all necessary components and to test the firewall rules that Cisco Packet Tracer is able to test. It includes our model of the UCC connected to the BA through a serial link, and the UCC connected to the substation through another serial link.

Following the data flows in Figure 1, the UCC houses five DMZ's for: SCADA, the corporate network, the BA, the public, and for the vendors to access the public network. The

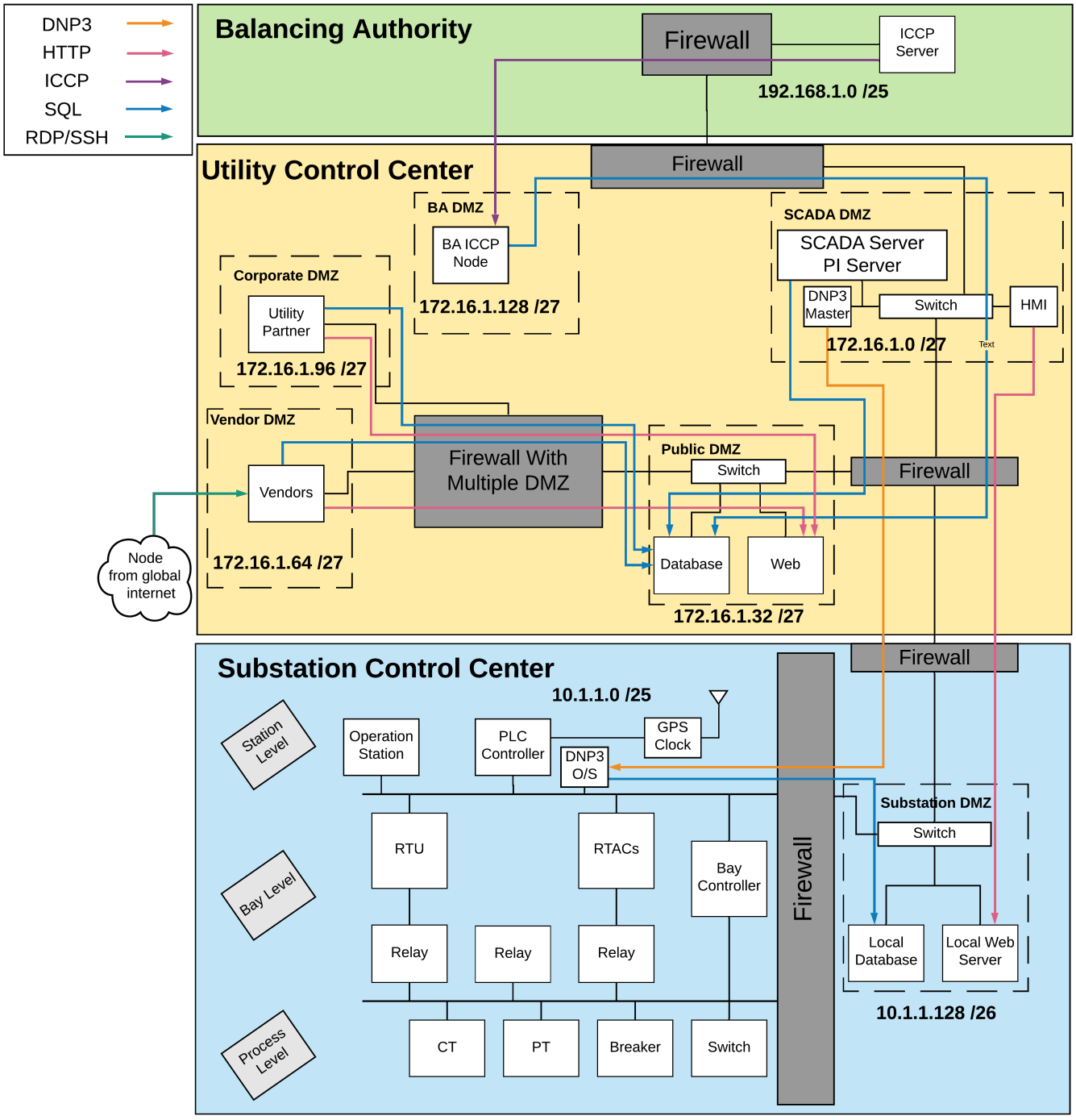

Fig. 1: Data flows between substation, utility control center and balancing authority.

corporate and vendor DMZ's are protected by two different interfaces of a shared firewall, and that same firewall is connected to one end of the public DMZ. This ensures that the main control center can access the public DMZ from one side and both vendors and corporate can access it from the other side. On the other side of the public DMZ is a firewall also connected to the inside of UCC and the substation. The ICCP DMZ is behind a firewall connected to the BA, where it only communicates with the BA's ICCP server. The BA network only has one firewall, which protects their ICCP Server.

The substation network includes one firewall which divides it into two subnets, both with a high security level. One subnet is for the relay network which sends all power information back to the UCC, and the other is for the substation DMZ, which includes a local database and web server, which the

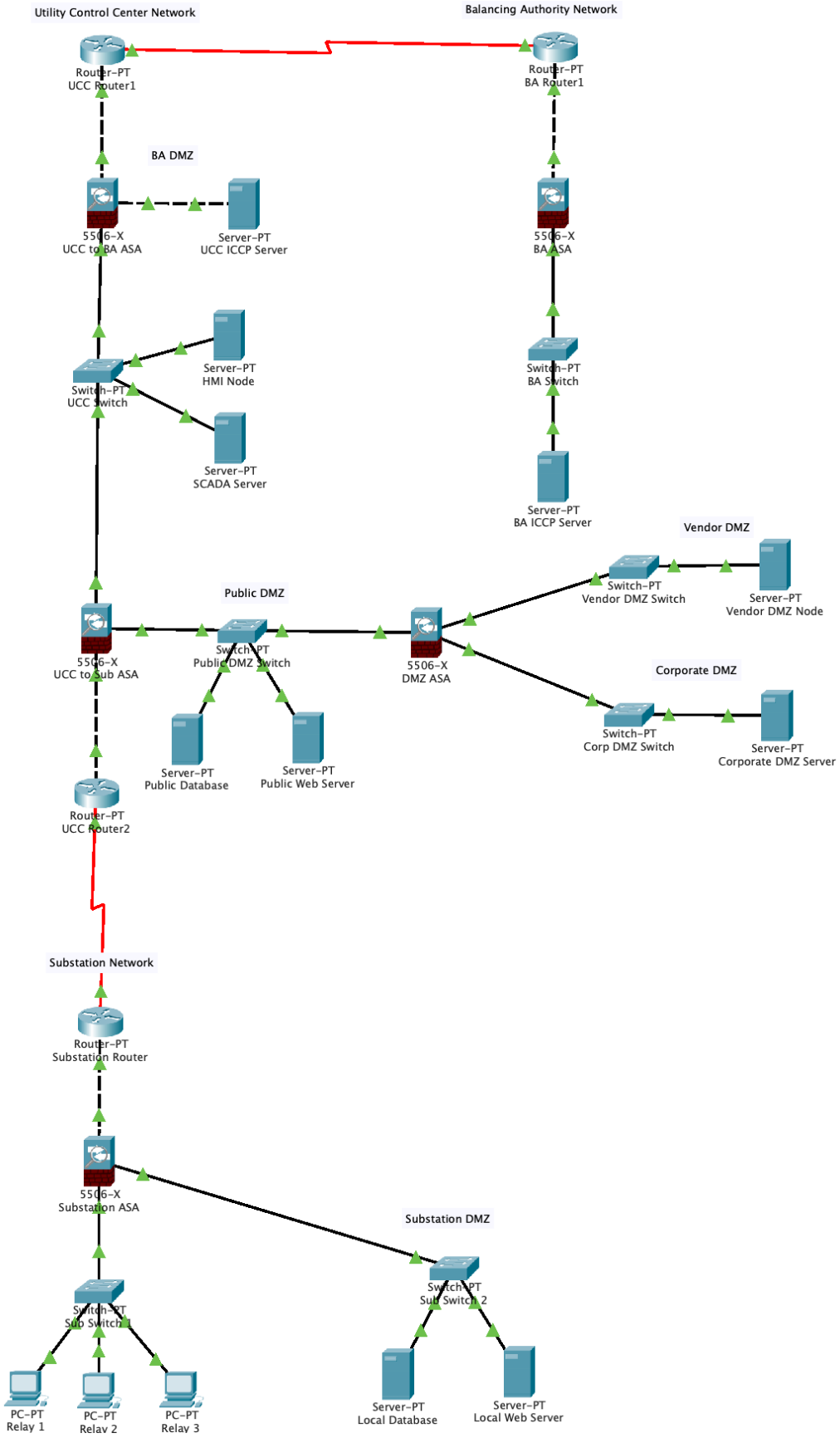

Fig. 2: Comprehensive network topology in the substation, utility control center, and the balancing authority.

UCC can access to pull a data history.

The IP addresses assigned to this model network are shown below in Tables I, II, and III. To be more concise, the point-to-point links in the UCC are not shown, only the major subnets. For the Texas 2000 model, each substation will have the address space of 10.1.X.0, with X representing the substation number. Since there are about 300 substations in the Texas 2000 model, some will begin with 10.2.X.0. Each UCC will have the address space of 172.16.X.0, with X representing the UCC number. Finally, each BA will have the address space of 192.168.X.0, with X representing the UCC it is connected to. Although in Texas there is only one BA (e.g., ERCOT, or Electric Reliability Council of Texas), other locations may have more than one BA.

TABLE I: IP Allocation in Substation

Subnet	Mask	Description
10.1.1.0	/25	Relay Network
10.1.1.128	/26	Substation DMZ Network
10.1.1.192	/30	Firewall to Router Link

TABLE II: IP Allocation in Utility Control Center

Subnet	Mask	Description
172.16.1.0	/27	Control Center Servers
172.16.1.32	/27	Public DMZ
172.16.1.64	/27	Vendor DMZ
172.16.1.96	/27	Corporate DMZ
172.16.1.128	/27	ICCP DMZ for BA

TABLE III: IP Allocation in Balancing Authority

Subnet	Mask	Description
192.168.1.0	/25	ICCP Server Network
192.168.1.128	/30	Firewall to Router Link
192.168.1.132	/30	BA Router to UCC Router Link

V. Experiments and Results

To implement and test this model, firewalls and routers were first configured in Cisco Packet Tracer then tested in NP-View. The model has five firewalls and four routers.

A. Firewall File Configuration

To begin, IP addresses were first configured on each device, including all servers. Then security-levels were configured on each interface of each firewall. The interfaces protecting the inside the network of the firewall were assigned 100, the outside interfaces were assigned 0, and the DMZ interfaces were assigned 50.

Next, object-groups were created for each network host that needed to be accessed, and for each application and protocol that needed to be used. Network object-groups allow a specific host or set of hosts to be called by one keyword when creating the rules for network access. Service object-groups allow specific port numbers to be grouped and named for easier access. For this model, eleven network-objects were created, and five service-object groups were created for the different data flows defined in Figure 1.

The next step was to configure the rulesets to define who can access each device and how, using ACL's [11]. Extended ACL's match both the source and destination addresses on the packet, as well as the protocol and application port number. At the end of each ACL, a deny all statement must be written [1] to ensure that all other packets attempting to access the network are discarded. Table IV shows the properties of the ACL's configured on the five Cisco Adaptive Security Appliance (ASA) firewalls.

TABLE IV: Firewall ACL Properties

Firewall Location	Number of Rules	Number of Interfaces
Substation ASA	6	3
UCC to Sub ASA	7	3
UCC DMZ ASA	7	3
UCC to BA ASA	5	3
BA ASA	3	2

The ACL's were created using applications over TCP, and are state-aware. This means that each rule only needs to be defined on one interface, as the firewall will allow the return packet through without another rule on the opposite interface.

B. Path Analysis and Vulnerability Assessment

After creating these files, they were input into a project in NP-View where a path analysis was completed. Figure 3 shows the network model that NP-View built based on only these configuration files. The lower half beneath the router named "routerSub" represents the substation network, the upper part of the network directly connected underneath the router named "routerBA" represents the BA, and the rest of the network represents the UCC. The cloud shapes in the figure that are named "inside," "outside," or "dmz," represent the border gateway interface for each firewall in Figure 3. The nodes are then shown within each of the interfaces represented by the gray dots in the model. For instance, the three nodes inside of the inside interface on "asaSub" named ".2," ".3," and ".4," represent the three relays of the substation. This model is beneficial to see how each node can be accessed, and through which interfaces on each firewall.

A path analysis can then be run on the network, and the software determines every possible way to access every node in the network, and the criticality level of each path. In this model, thirty-three possible paths were found, which were then reviewed and marked to be okay, low-risk, or high-risk. The path analysis can also be filtered to only show every incoming or outgoing traffic to a specific node in the network. For instance, the SCADA Server shows only two outgoing paths which are to the public database in the public DMZ over SQL, and to the relays in the substation over DNP3. There are no incoming paths however, so this verifies that our rulesets in the model network are secure.

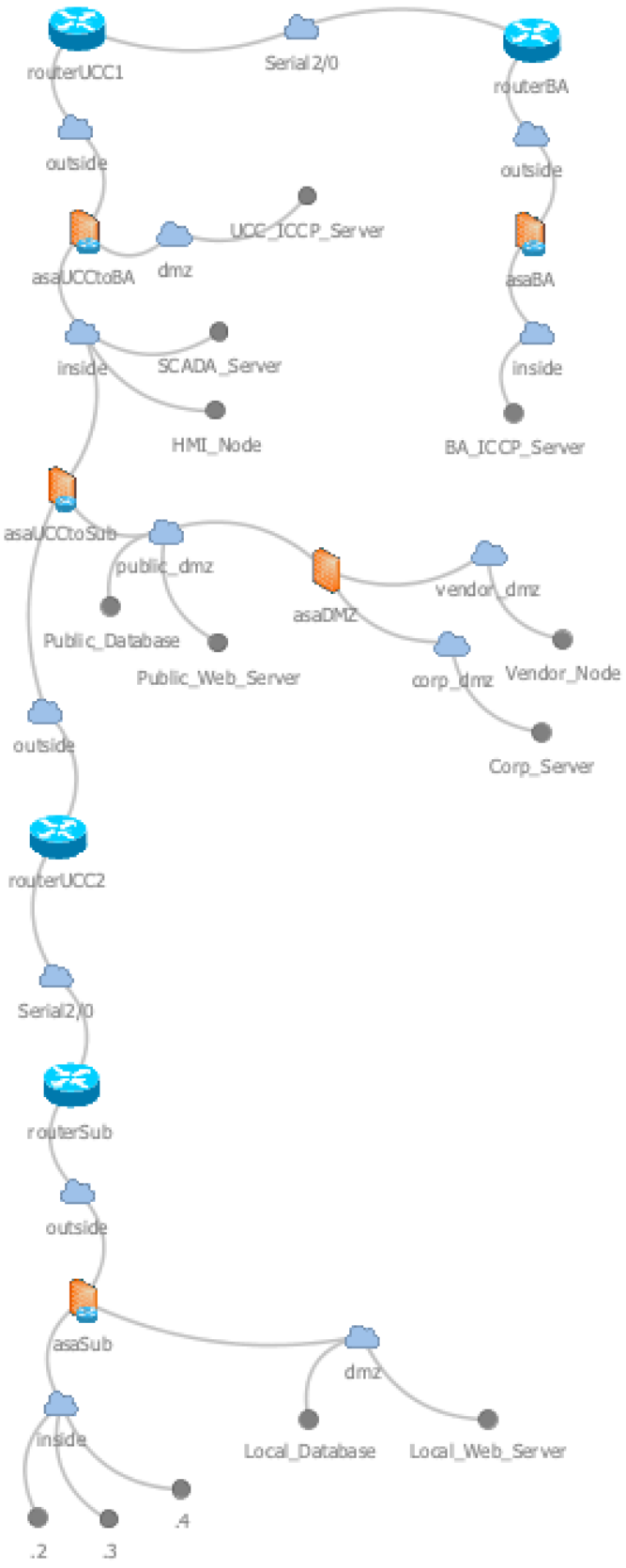

Fig. 3: NP-View diagram.

VI. Conclusion and Future Work

Firewall configuration files have been created and tested using Cisco Packet Tracer and NP-View, based on data flow models that represent the OT network traffic of an electric utility company, including substation, control center, balancing authority and several DMZ's.

Best practices in the industry mirror best practices for all industries. For industrial control systems, care needs to be taken to ensure that connections are only allowed to originate based on need to operate the system and data flows are only allowed to originate from the control system or instrument side. This practice is best summated in NERC-CIP-005. Challenges and pitfalls in design of the network involve insuring that data flows originate from control system only. Use of discrete DMZ zones allow for separation of business operations. Insights gained could include the possibility to template firewall configurations by producing an algorithm that can produce best practice based firewall configurations. NP-View does have some APIs that allow for ingestion of network traces. There has been some research done on building such an API but currently this is an unfunded feature request.

Acknowledgement

This research is supported by the US Department of Energy Cybersecurity for Energy Delivery Systems program under award DE-OE0000895.

References

[1] CIP-005-5. Cyber security electronic security perimeter(s). [Online]. Available: https://www.nerc.com/pa/Stand/Reliability\%20Standards/CIP-005-5.pdf

[2] A. B. Birchfield, T. Xu, K. M. Gegner, K. S. Shetye, and T. J. Overbye, "Grid structural characteristics as validation criteria for synthetic networks," *IEEE Transactions on power systems*, vol. 32, no. 4, pp. 3258–3265, 2016.

[3] P. Wlazlo, K. Price, C. Veloz, A. Sahu, H. Huang, A. Goulart, K. Davis, and S. Zounouz, "A cyber topology model for the texas 2000 synthetic electric power grid," in *2019 Conference on Principles, Systems and Applications of IP Telecommunications (IPTComm)*. IEEE, October, 2019.

[4] C. Ten, C. Liu, and M. Govindarasu, "Vulnerability assessment of cybersecurity for scada systems using attack trees," in *2007 IEEE Power Engineering Society General Meeting*, June 2007, pp. 1–8.

[5] Z. Trabelsi and H. Saleous, "Exploring the opportunities of cisco packet tracer for hands-on security courses on firewalls," *2019 IEEE Global Engineering Education Conference (EDUCON)*, pp. 411–418, 2019.

[6] "Network Perception," 2020. [Online]. Available: https://www.network-perception.com/np-view//

[7] S. Singh, "Automatic verification of security policy implementations," Ph.D. dissertation, Univ. of Illinois at Urbana-Champaign, Urbana, 2012. [Online]. Available: https://tcipg.org/publications/automatic-verification-security-policy-implementations

[8] G. A. Weaver, K. Davis, C. M. Davis, E. J. Rogers, R. B. Bobba, S. Zonouz, R. Berthier, P. W. Sauer, and D. M. Nicol, "Cyber-physical models for power grid security analysis: 8-substation case," in *2016 IEEE International Conference on Smart Grid Communications (SmartGridComm)*. IEEE, 2016, pp. 140–146.

[9] J. Frahim and O. Santos, *Cisco ASA: All-in-One Firewall, IPS, Anti-X, and VPN Adaptive Security Appliance*. Cisco Press, 2010.

[10] The power behind the PI server. [Online]. Available: https://www.osisoft.com/pi-system/pi-capabilities/pi-server/

[11] F. Soldo, A. Markopoulou, and K. Argyraki, "Optimal filtering of source address prefixes: Models and algorithms," in *IEEE INFOCOM 2009*, April 2009, pp. 2446–2454.