Network Perception

Using NP-View to prepare for a NERC CIP-005 audit

Version 2

July, 2022

`

Key Summary

Compliance with NERC[1] CIP Reliability Standards requires NERC registered entities to adopt precise procedures and to verify their implementation. This white paper describes the requirements under CIP-005, the Standard for Electronic Security Perimeters. It illustrates how a NERC registered entity can utilize technological solutions such as NP-View to save time and resources assessing and managing its compliance with the primary parts of CIP-005.

[1] NERC is the acronym for the North American Electric Reliability Corporation. NERC is a non-profit organization tasked by the Federal Energy Regulatory Commission (part of the US Department of Energy) with ensuring the reliability of the North American electric power grid. Among its tasks are drafting and auditing standards for cybersecurity of the systems that monitor and control the grid. Known as NERC Critical Infrastructure Protection (CIP), this body of Standard number from CIP-002 through CIP-014.

Important NERC CIP Concepts

A general understanding of the terms employed within this whitepaper greatly enhances its meaning and application. These terms, defined below for convenience, in no way supercede the official NERC Glossary of Terms[2].

Bulk Electric System (BES)

The North American power grid consists of a huge network of fixed assets linked by transmission lines. The primary types of assets include:

- Control centers, where trained and experienced operators monitor and control electric power flows, using many types of computer systems;
- Generating assets, including traditional nuclear, coal, natural gas and other power plants, as well as renewable power assets such as wind and solar farms and hydroelectric dams;
- Low-power renewable generating assets, primarily solar panels, installed at homes and businesses; and
- Substations, where devices like transformers and circuit breakers control electric power flows, usually under the supervision and direction of a control center.

NERC entities use many types of computing systems to monitor the BES. Therefore NERC, under the direction of FERC[3], developed the Critical Infrastructure Protection (CIP) Standards to secure these systems against cyberattacks, whether targeted (as in individual hacking attempts), broadcast (e.g. computer viruses and worms), or inadvertent (a user clicks on a phishing email that installs ransomware and renders his system unusable).

Cyber Assets

Many types of systems monitor and control the BES. Many are recognizable as common-off-the-shelf information technology systems (computers) used throughout the modern business world. Other devices look and operate very differently from these “normal” IT systems. Often referred to as OT, or operational technology, these systems serve real-time critical reliability

[2] The current NERC Glossary may be found at https://www.nerc.com/files/glossary_of_terms.pdf.

[3] The Federal Energy Regulatory Commission (FERC) is the United States federal agency that regulates the transmission and wholesale sale of electricity and natural gas in interstate commerce and regulates the transportation of oil by pipeline in interstate commerce.

functions. However, since both types of devices have roles in controlling the BES, the NERC CIP standards introduced the fundamental concept of a Cyber Asset, defined in part as a "programmable electronic device".

While initially causing a great deal of argument, a Programmable Electronic Device (PED) has generally been recognized to follow the pseudo-formula below. A PED is any device that utilizes a digital Microprocessor and that contains field-updatable Logic, Software, or Firmware, and allows Field Updates, which includes flashable EEPROM and socketed ROM packages.

$$PED = M \text{ and } ((L \text{ or } S \text{ or } F) \text{ and } U)$$

BES Cyber Asset or System (BCA / BCS)

While entities may employ many cyber assets in monitoring and controlling the BES, not all may be included within the scope of NERC CIP compliance. When the loss, mis-operation, or degradation of a cyber asset could cause an impact on the BES within 15 minutes, they fall under the special NERC CIP category of BES Cyber Assets or BES Cyber Systems[4]. Most of the requirements in the CIP standards apply to BES Cyber Systems but may additionally divide into three groups based on their degree of impact on the BES: High, Medium and Low impact.

Electronic Security Perimeter (ESP)

CIP-005 introduces the important concept of Electronic Security Perimeter (ESP). NERC defined an ESP as "the logical border surrounding a network to which BES Cyber Systems are connected using a routable protocol" (almost all routable networks run the Internet Protocol, or IP). In other words, the ESP contains all of the BCS within a logical border. In some cases, multiple ESPs may exist at the location of one BES asset, such as a power plant that spreads between multiple buildings, each with its own IP network. An ESP may contain multiple networks, but a single network cannot contain multiple ESPs.

The ESP can also contain Cyber Assets that do not meet the definition of BES Cyber Systems, meaning their loss or compromise will not impact the BES within 15 minutes. However, the former presents as much risk as the latter. Any device on a routable network compromised by a cyberattack may facilitate additional attacks on other devices and further penetration into systems. Protecting only the BES Cyber Systems and not other systems on the same network would introduce significant threat vectors. For this reason, the CIP standards designate all other Cyber Assets connected to the ESP as Protected Cyber Assets (PCA) and the vast majority of the

[4] BES Cyber Systems can be composed of one or many cyber assets. The individual cyber assets may or may not have a 15-minute BES impact, but the system as a whole does. Note that a BCS must be located at one of the six types of assets listed in CIP-002-5.1a R1.1, to be in scope for CIP.

CIP Requirements apply equally to both BCS and PCA. Often called ‘High-Water Marking’, this concept raises all devices within a control zone to the highest security level found within that zone.

Sometimes the systems within ESPs need communications with networks external to the ESP. The NERC Glossary calls this External Routable Communications (ERC), which needs provision for communications into and out of the ESP. The Standards refer to devices that control these communications, usually firewalls, as Electronic Access Control and Monitoring Systems (EACMS). All ERC must cross between networks at an EACMS interface identified and documented as an Electronic Access Point (EAP).

Audit Preparation Workflow

Successfully managing compliance means gaining a clear understanding of requirements and building a workflow that enables a team to coordinate while reviewing evidence and preparing reports. Used efficiently, technology can bring automation to this workflow, in order to save time and minimize the risk of human error. In the context of CIP-005, mis-identifying an asset or missing an access rule can lead to serious consequences, including fines. This white paper provides a step-by-step guidance towards building such a workflow for four important CIP-005 requirement parts.

The following sections explain how to use NP-View to manage compliance with four important CIP-005 requirement parts.

CIP-005 Requirement 1, Table 1.1

> *"All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP."*

As already mentioned, any other Cyber Assets attached to the same network will be Protected Cyber Assets and also subject to most of the CIP requirements, including all of the parts of CIP-005. To provide visual verification (for the organization or the auditors) that all BCS reside within an ESP:

1. Import the configuration file(s) of the firewall(s) protecting an ESP into NP-View.
2. Select the CIP-005 firewall(s) and mark their category as "CIP: EACMS" assets.
3. Select the EAP interface(s) connecting the BES Cyber Systems to the EACMS devices and use NP-View Zones to create a visual group called ESP (see figure 1 below).
4. If assets are missing from the topology map generated from the firewall configuration files alone, NP-View also supports secondary information such as network scans from Nmap or hostname files.
5. Right-click on BES Cyber Systems and mark their criticality as high or medium.
6. Verify that all BES Cyber Systems are within an identified ESP.

NP-View will identify and map out all of the networks at a location. Since the Standards define an ESP as any network that contains a BCS or BCA, NP-View provides the opportunity to confirm these populations within the platform. Also from the topology view, any BCS connected to a network external to an ESP should become obvious. Once satisfied that the ESP includes all BES Cyber Systems, flag any other cyber assets contained within as PCA hosts.

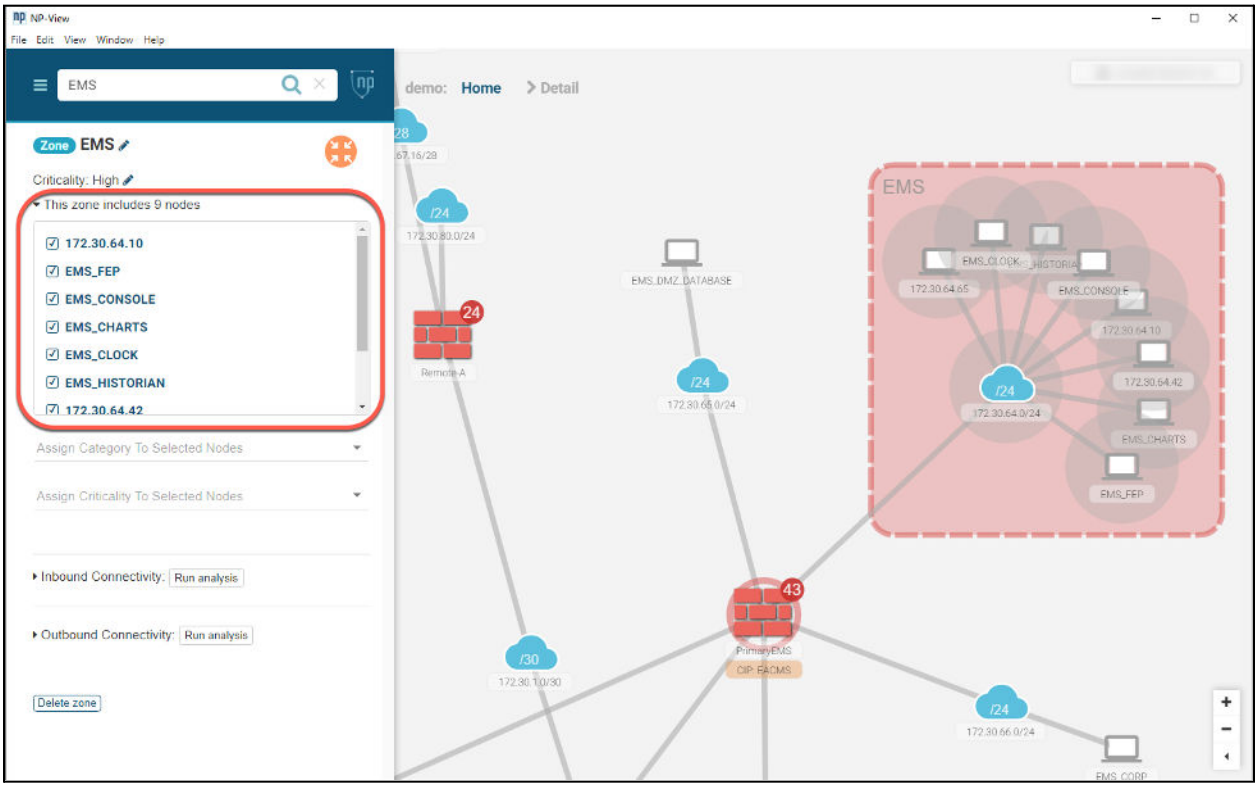

Figure 1: EMS Zone Created

CIP-005 Requirement 1, Table 1.2

> *"All External Routable Connectivity must be through an identified Electronic Access Point (EAP)."*

CIP-005 R1.2 introduces the concept of External Routable Connectivity (ERC). NERC defines this as "The ability to access a BES Cyber System from a Cyber Asset that is outside of its associated Electronic Security Perimeter via a bi-directional routable protocol connection." In other words, if a system outside of the ESP may transit the EAP over a routable protocol (and vice versa), then that ESP has ERC. The existence of ERC at an EAP naturally brings many additional compliance

requirements into scope. Note that the word “routable” includes any protocol that utilizes both network and host address spaces, expanding the possibilities well beyond only the TCP/IP suite.

CIP-005 R1.2 requires that all External Routable Connectivity communicate through an identified EAP. Each EACMS might have any number of hardware, software, or virtualized interfaces configured on the device. Entities will likely identify the closest interface to the ESP that allows routable communication. Compliance with CIP-005 R1.2 serves as good security practice. Without first Identifying, documenting, and robustly controlling an EAP, electronic access becomes far more difficult to understand and manage.

NP-View helps cybersecurity professionals determine whether any External Routable Connectivity enters or exits an ESP at any point other than the identified EAP. In other words, NP-View can identify undiscovered “holes” in an ESP, which lead to both network security and CIP compliance risk. To model your network access control with NP-View, simply:

1. Select the ESP subnet within the zone(s) created under the prior step.
2. Using the path analysis functions, review the incoming and outgoing paths reported by NP-View. Verify that all paths transit across an identified EAP.
3. Investigate any external paths that don’t come through an EACMS.

Figure 2 - Zone Path Analysis

CIP-005 Requirement 1, Table 1.3

> *"Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default."*

CIP-005 R1.3 requires that all inbound or outbound traffic flows at an EAP must be explicitly permitted and include a documented justification, or business reason, for each permission. Just as importantly, entities must periodically validate their justifications to ensure the need remains for each rule, as changes to systems often occur that may orphan rulesets.

Many entities document a rubric they use to make their justification statements consistent across the organization. Usually made up of three to five elements, the justification rubric creates strong audit-ready evidence. An example rubric might appear like this:

> Rubric Elements: <<ticket number>> <<system vendor>> <<approval owner>> <<original approval date>> <<detailed technical communication requirements>>
>
> Justification Example: 23422445 - Cisco - Sally Jones - 20181002 - Secure Shell required between jump host group and cisco routers for authorized remote access

Periodic review of rules supports cybersecurity best practice, even outside the reach of the NERC CIP Standards. For instance, an organization may decommission a database server that had access configured into a control network over a particular range of TCP ports. That organization would much rather discover unnecessary ports left open upon a quarterly or monthly review with NP-View versus during the forensics after a destructive breach has occurred!

Use NP-View to verify justifications and perform periodic validations with the following steps:

1. Click on any device and select Access Rules in the device's info panel (see figure 3).
2. Verify that all rules allowing traffic across an identified EAP have a valid justification. Flag any rule that does not have a justification.
3. For any open port or service flagged without a documented justification, either document the justification or close the port.

4. For ports and services with justifications, determine whether the justification is still valid. Document rule as “OK, Needs Review, or Needs Revision” using the drop-down box provided.

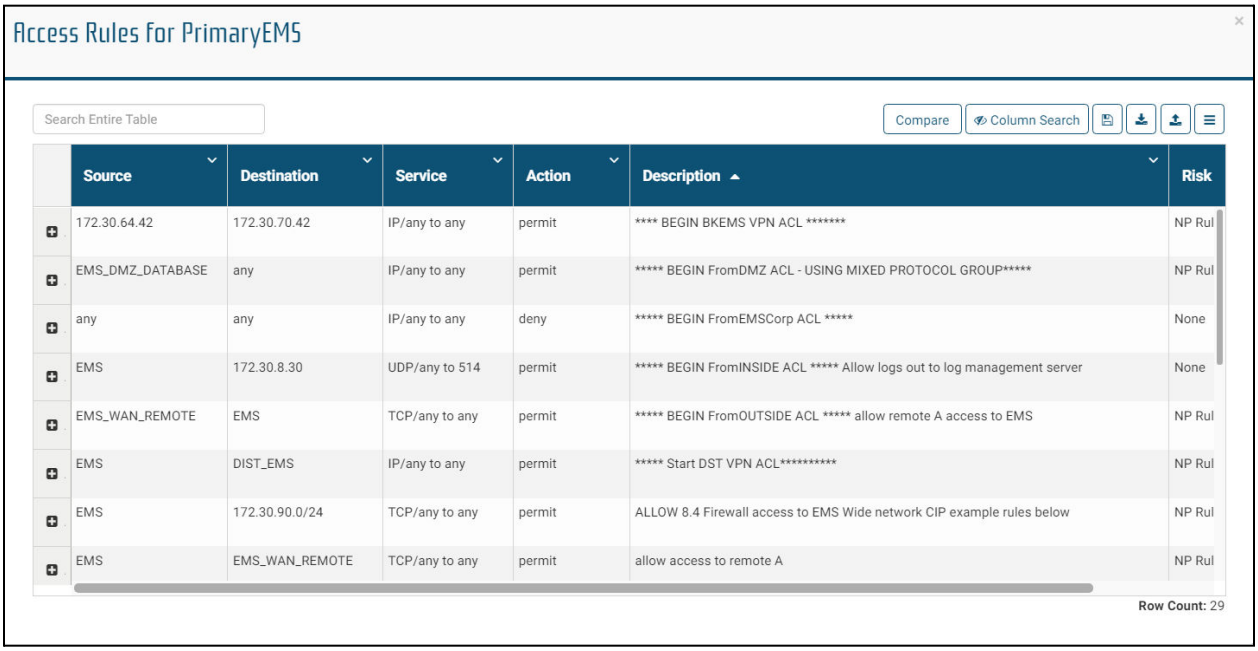

Figure 3 - Access Rule Table for Device

CIP-005 Requirement 2, Table 2.1

> *“Require inbound and outbound access permissions, including the reason for granting access, and deny all other access by default.”*

CIP-005 R2.1 introduces two more important concepts into the NERC CIP standards. First, NERC defines Interactive Remote Access (IRA) as “user-initiated access by a person employing a remote access client or other remote access technology using a routable protocol.” IRA places a person at the remote computer to interact in real-time with a BCS within an ESP. The definition goes on to say “Interactive remote access does not include system-to-system process communications.”

Any number of IRA protocols exist, but commonly recognized examples include SSH (TCP/22), RDP (TCP/3389), HTTPS (TCP/443), and SecureVNC (TCP/5900).

The other new concept NERC defines as “A Cyber Asset or collection of Cyber Assets performing access control to restrict Interactive Remote Access to only authorized users.” Officially called Intermediate Systems (IS), most people simply call these “jump hosts". Placed inside a DMZ network, jump hosts authenticate remote users, who may then open up a new session from the jump host to a BCS inside the ESP.

A session break of this fashion helps enforce electronic access control, with the additional benefits of slowing the propagation of malware, as well as adding layers of defense against malicious attackers. Complying with CIP-005 R2.1 requires entities to verify that all possible Interactive Remote Access paths terminate at the Intermediate System, not at a BCS inside the ESP. Similarly to CIP-005 R1.2, NP-View can identify possible IRA paths using the Path Analysis and Object Groups:

1. Select a network that exists within the ESP zone defined in earlier steps.
    a. Using the Inbound Connectivity analysis to filter for each method of suspected IRA that transits the EAP into the ESP. Upon discovery of any IRA into the ESP, document using the comment field provided.
    b. Ensure that all IRA that transits an EAP originates at a designated IS (or jump host) and document accordingly. **Flag for immediate compliance review any IRA that enters the ESP from any other source than an identified IS.**
    c. Repeat for each network that exists within an ESP zone.
2. Select an IS from the topology.
    a. Using the Inbound Connectivity tool, ensure that all IRA originates from an authorized source system or network.
    b. Using the Outbound Connectivity tool, double-check the existence of documentation of all IRA from the IS transiting the EAP into an identified ESP.
    c. Repeat for each IS (or DMZ network, as applicable).
3. For a quick listing of all documented IRA paths, use the Workspace Report and uncheck all options except Connectivity Paths (see figure 5). Additionally, the NERC CIP Report (discussed in steps below) also includes all path comments.

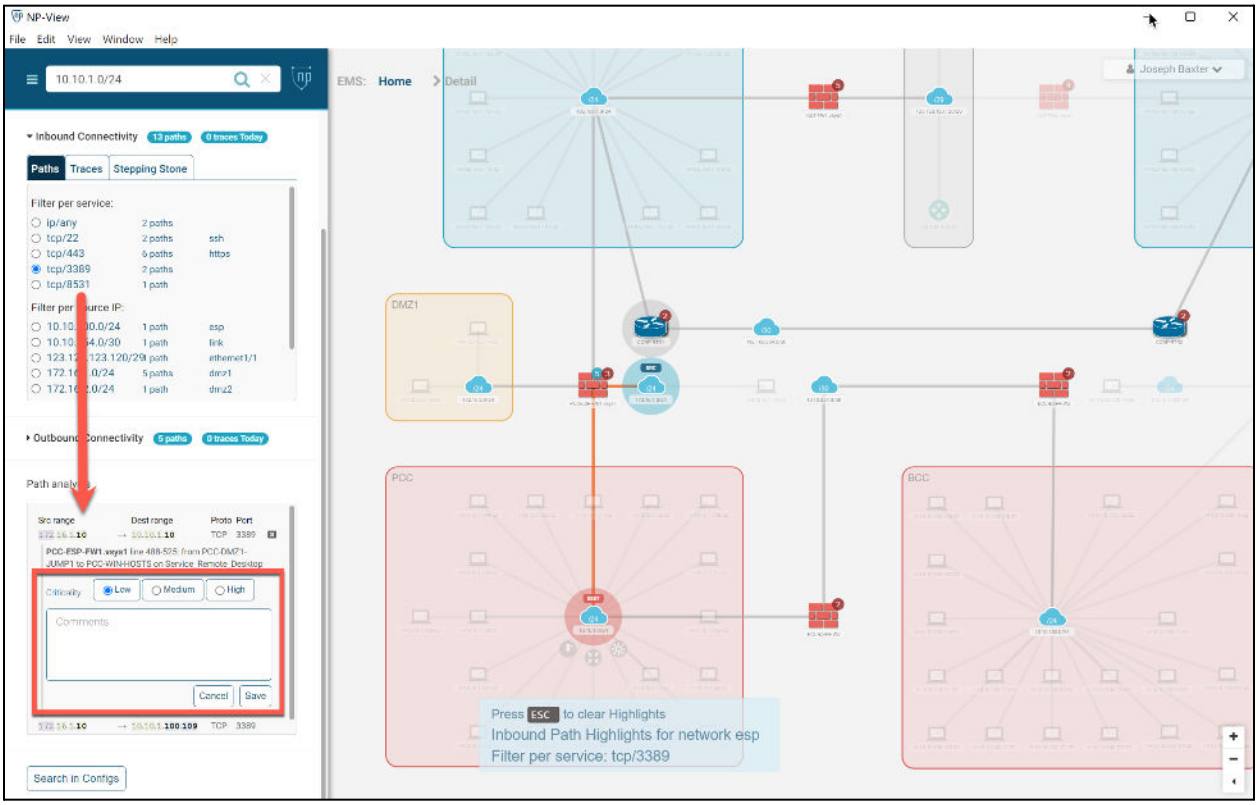

Figure 4 - Network Incoming Path Analysis

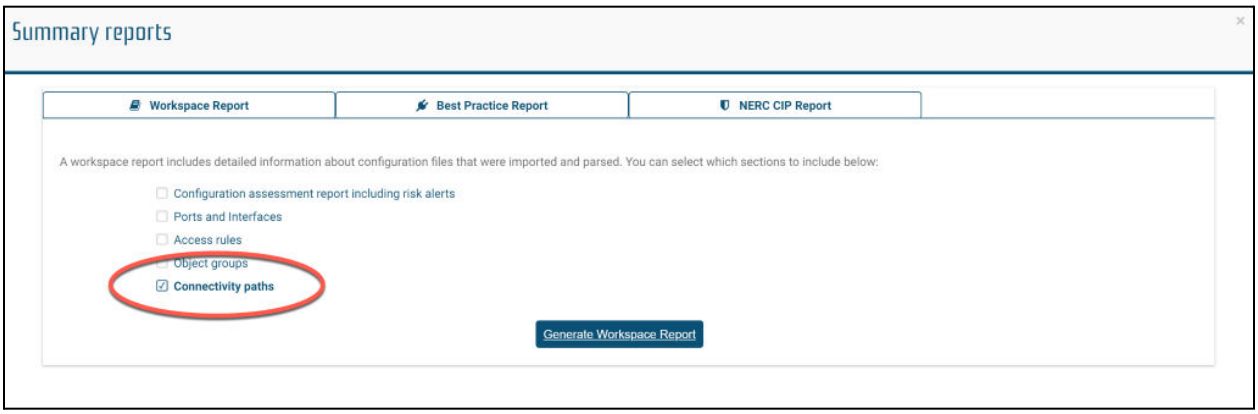

Figure 5 - Best Practice Report: Connectivity Paths

Reporting from NP-View

After building their evidence and documentation in preparation of an audit, NP-View provides entities several reporting and export options.

Data Export

Many tables within the NP-View interface will possess the ability to export data for further manipulation in other applications (see figure 6), principally Microsoft Excel (XLSX) and simple comma separated values (CSV).

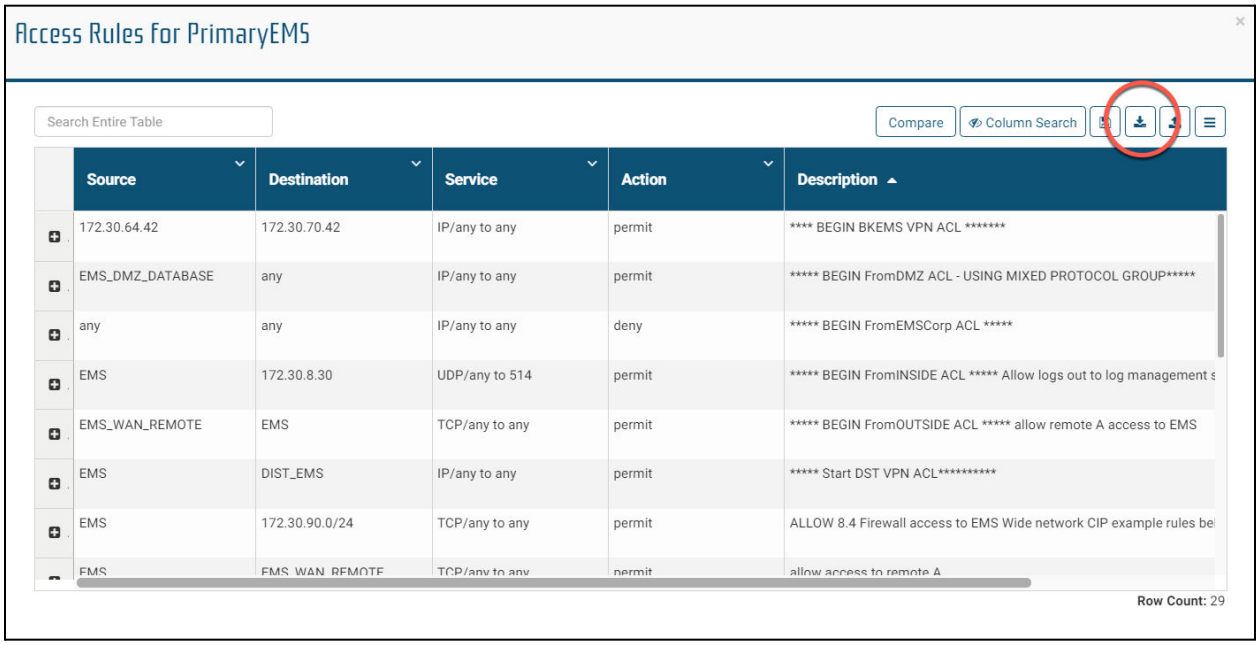

Figure 6 - Export Feature

NP-View CIP Report

Among the pre-built reports (see figure 7) standard in NP-View, entities may use the NERC CIP Report as a snapshot of their compliance evidence. This report uses a wizard-based approach to select the ESP, EACMS, EAP, and all BCS devices. Upon completion of the wizard, NP-View provides the user with an effective report, formatted to match the order of the Requirements of CIP-005 itself.

One common approach to audit readiness centers upon the creation of a new audit scope workspace that contains only devices on the audit sample list. Doing so limits possible confusion

with out-of-scope devices. From the audit scope workspace, the entity may then create new reports and print to PDF to submit as supplementary evidence. The audit scope workspace may be deleted after the audit closes.

The NP-View Best Practice report serves as a checklist to bring each device up to meet the highest level of cybersecurity possible. It provides a very device-centric view and offers highlights on common risks and misconfigurations. Entities not facing a near-term audit may also decide to maintain a PDF Workspace report once each month as a network history.

Export a workspace for later retrieval from the initial screen (see figure 8). These archives support audit and evidence requests from a historical perspective.

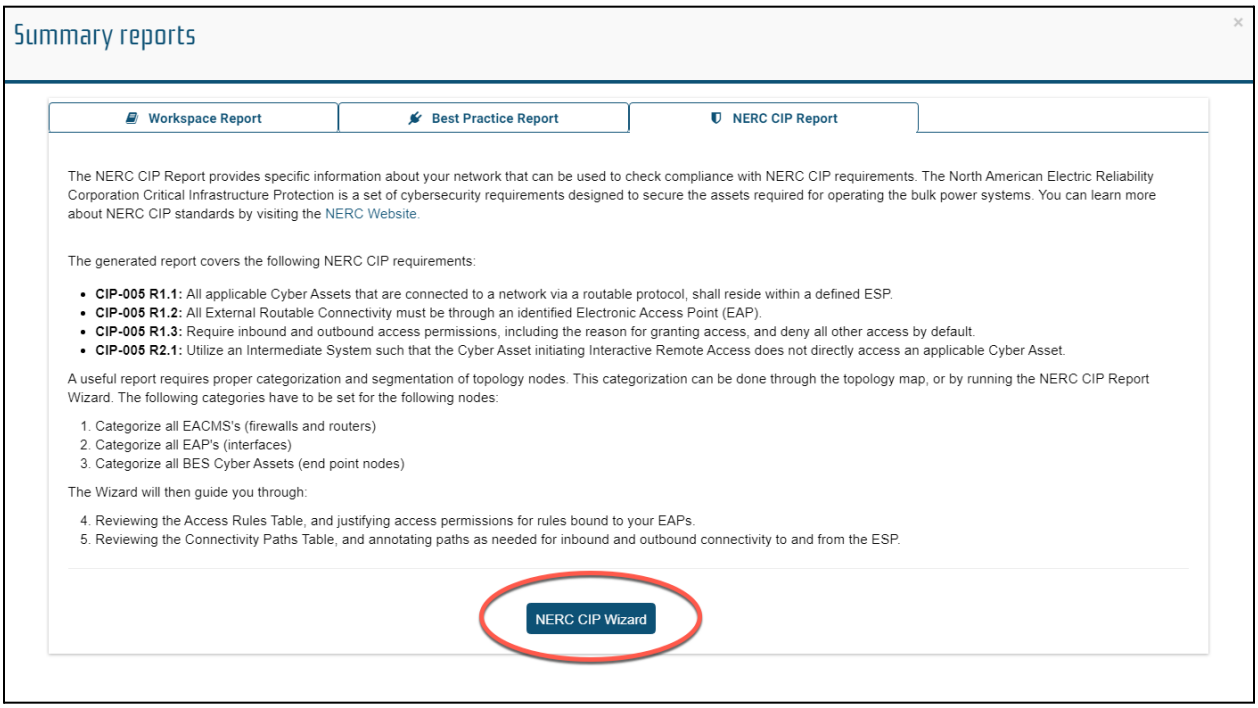

Figure 7 - NERC CIP Report

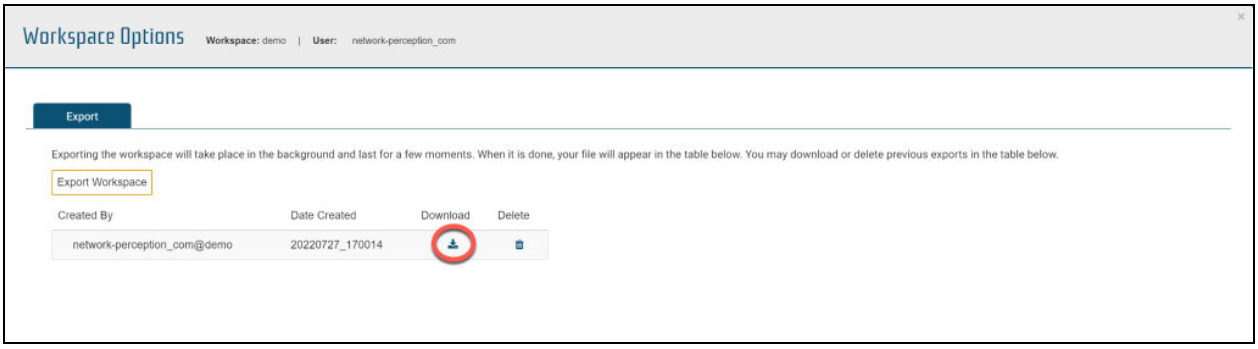

Figure 8 - Workspace Export

About NP-View

NP-View is a software product developed by a team of networking and security experts at Network Perception. It works offline and generates a network topology diagram by analyzing configuration files from firewalls, routers, and switches. The interface design of NP-View allows users to easily identify and track overly-permissive network access policies, as well as recording justifications for rules, ports and services. If you have questions or would like to know more about NP-View, please contact the Network Perception team at:

+1 (872) 245-4100 | info@network-perception.com | https://kb.network-perception.com