White Paper

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

Network Perception

June, 2018

Compliance with NERC[1] CIP Reliability Standards requires NERC entities to adopt precise procedures and to verify their implementation. This white paper describes the requirements under the standard CIP-005, the standard for Electronic Security Perimeters, and illustrates how a NERC 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. This set of standards is known as NERC CIP. There are currently 13 CIP standards either in effect, awaiting approval by FERC, or under development. These standards are numbered CIP-002 through CIP-014.

Important NERC CIP Concepts

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 and control electric power flows, usually under the supervision and direction of a control center.

The BES is monitored and controlled by many types of computing systems. The NERC CIP standards were developed 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 Asset – There are many types of systems that monitor and control the Bulk Electric System. Some of them are computers like those all of us are familiar with. Others are devices that look very different, and operate very differently, from "normal" computers. Since both types of devices have roles in controlling the BES, the NERC CIP standards introduced the fundamental concept of a Cyber Asset, defined as a "programmable electronic device". This means an electronic device whose operation can be controlled through a program, which can be revised or replaced in some way.

BES Cyber System (BCS) – While there are many Cyber Assets involved in monitoring and controlling the BES, not all of these are in scope for NERC CIP. There is a subset of these Cyber Assets whose loss or mis-operation (perhaps under the control of a virus or a hacker) could cause an "impact" on the BES within 15 minutes. These are called BES Cyber Systems[2]. Most of the

[2] 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.

requirements in the CIP standards apply to BES Cyber Systems, although these are divided into three groups based on their degree of impact on the BES: High, Medium and Low impact.

CIP-005 introduces the important concept of **Electronic Security Perimeter** (ESP). This is defined by NERC 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 is the "logical border" of a network that contains all of the BCS located at a BES asset (and used by that asset), when those BCS are connected to other Cyber Assets using IP. In some cases, there might be multiple ESPs located at one BES asset, such as a power plant that is spread over multiple buildings, each with its own IP network.

The ESP can contain Cyber Assets that aren't BES Cyber Systems – i.e. their loss or compromise won't impact the BES within 15 minutes. However, the former present as much of a risk as the latter. This is because, on a routable network, any device that has been compromised by a cyberattack can be used as a "jumping-off point" for attacks on other devices on the network. If just the BES Cyber Systems are protected by the CIP standards, they will still be vulnerable because they could still be compromised by an attack that "came through" one of the other systems on the network. For this reason, the CIP standards designate all other Cyber Assets connected to the ESP as **Protected Cyber Assets** (PCAs). Most of the CIP standards apply equally to BCS and PCAs.

Since the systems within most ESPs will need to communicate with the world outside the asset (including the control center that monitors and controls the asset), there needs to be provision for communications into and out of the ESP. Devices that control these communications, including firewalls, are referred to in CIP as Electronic Access Control and Monitoring Systems (EACMS).

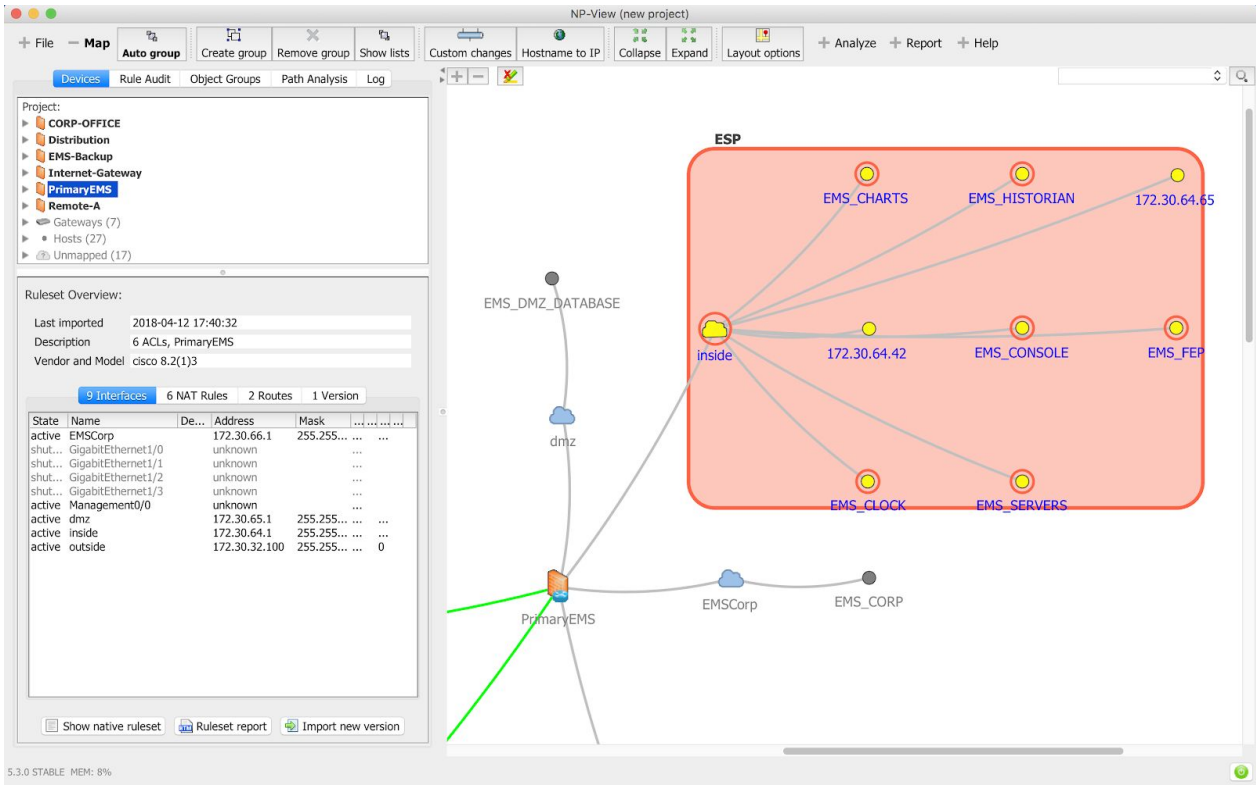
About NP-View

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 user interface of NP-View was designed to easily identify and keep track of overly permissive network access policies, as well as recording justification for rules, ports and services. The following sections explain how to use NP-View to manage compliance with four important CIP-005 requirement parts.

CIP-005 R1.1 All applicable Cyber Assets connected to a network via a routable protocol shall reside within a defined ESP.

CIP-005 R1.1 requires that High- and Medium-impact BES Cyber Systems reside within an 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 your 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 interface(s) connecting the BES Cyber Systems to the firewall(s) and create a visual group called ESP
3. If assets are missing from the topology map generated by NP-View, one can also import a network scan report from NMAP or a hostname file to add missing assets to the map
4. Right-click on BES Cyber Systems and mark their criticality as high or medium
5. Verify that all your BES Cyber Systems are within an ESP



Since NP-View will identify and map out all of the networks at a location, any network that contains a BCS is an ESP. It is important to confirm that all of your BCS (meaning all of the Cyber Assets that comprise each BCS) are contained within an ESP[3], and at the same time that no BCS is attached to a network that isn't an ESP. Once you are satisfied that your Electronic Security Perimeter includes all of your BES Cyber Systems, you also need to identify all of the other Cyber Assets that are connected within the ESP – these will all be Protected Cyber Assets.

CIP-005 R1.2 All External Routable Connectivity must be through an identified Electronic Access Point (EAP).

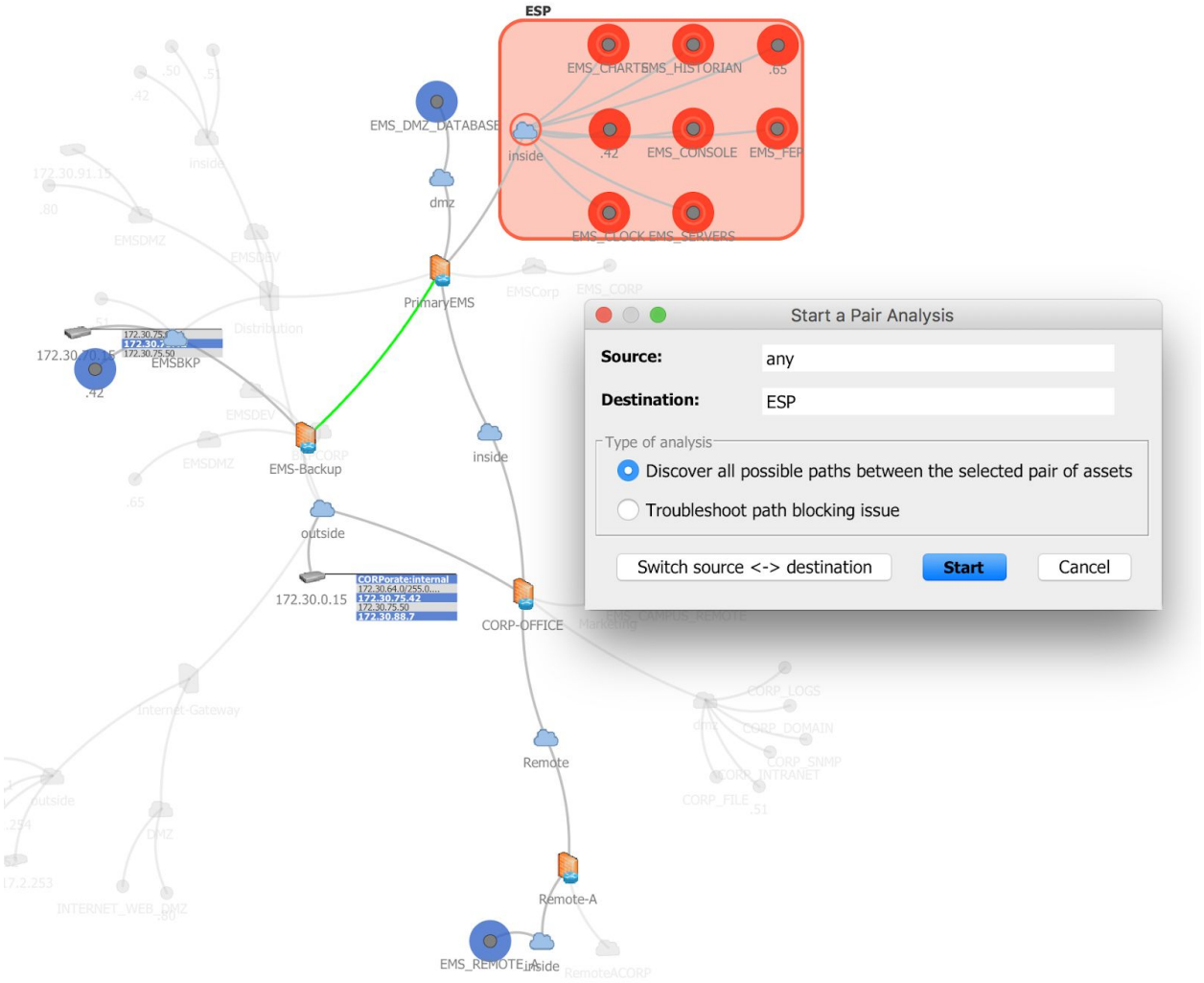
CIP-005 R1.2 introduces the concept of External Routable Connectivity (ERC). This is defined by NERC as "The ability to access a BES Cyber System from a Cyber Asset that is outside of its associated Electronic Security Perimeter via a bi-directional routable protocol connection." In other words, if a BES Cyber System can be accessed by a system outside of the ESP using a routable protocol (usually IP), then that BCS is said to have ERC. Note that, even though there may be a firewall blocking access to the Cyber Asset from devices outside the ESP, as long as the Cyber Asset is routably connected to a network that has access to the outside world, it still has ERC. In fact, if one device connected to an ESP has ERC (whether or not it's a BCS), all of the other devices connected to the ESP are assumed to have ERC as well.

CIP-005 R1.2 requires that all External Routable Connectivity come through an Electronic Access Point (EAP). This is a port on an Electronic Access Control and Monitoring System (typically a firewall or router) that allows routable communication between Cyber Assets outside and inside the Electronic Security Perimeter. Compliance with CIP-005 R1.2 – as well as good network security practice – requires there should be no route for a computer outside the ESP to access a BES Cyber System within the ESP, unless that route goes through an EAP.

You can use NP-View to determine whether there is any External Routable Connectivity coming into a BCS, that doesn't enter the ESP through an EAP. In other words, NP-View can identify "holes" in your ESP that you may not know about; these can lead to both network security and CIP compliance risk. You just have to:

[3] While all BCS components have to be contained within *an* ESP, it is possible for the components of a single BCS to be contained within multiple ESPs. For example, a utility may decide to classify all of their relays in all Medium impact BES substations as a single BCS, meaning they would most likely be contained within many ESPs. The individual relays would be BES Cyber Assets. Each of these would need to be contained within an ESP, but they would be separate ESPs, presumably one for each Medium impact substation.

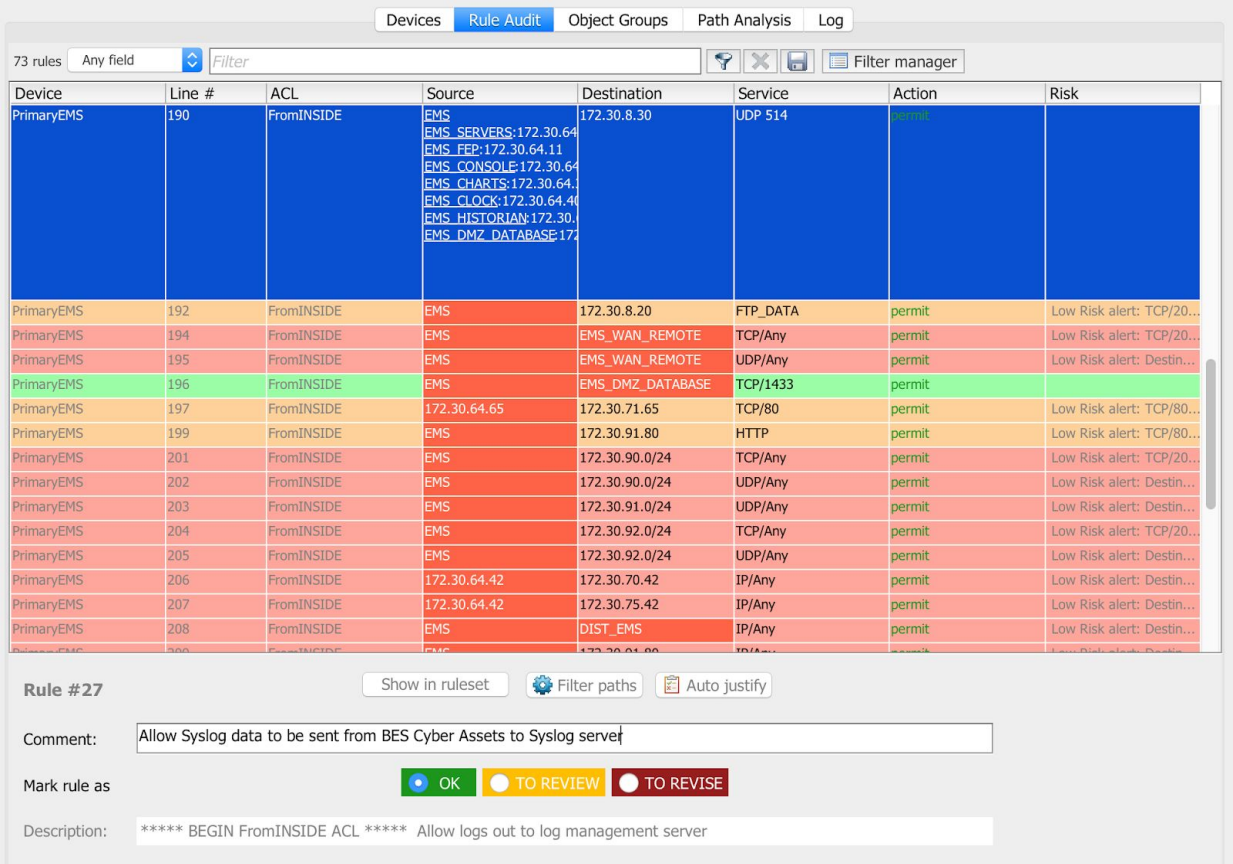
1. Save the project first and then go the Analyze toolbar and select Pair analysis to launch a path analysis from “any” to the group “ESP” that was created in the previous step
2. Review the path results being reported by NP-View in the Path Analysis table to verify that all paths originating outside of the ESP come through an Electronic Access Point on an Electronic Access Control and Monitoring System (usually a firewall).
3. Investigate any external paths that don’t come through an EACMS.



CIP-005 R1.3 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 there must be a justification for each permission; just as importantly, these permissions need to be regularly evaluated to make sure they are still needed and that the justifications remain correct. This requires regular review of firewall rule sets to make sure all permissions have documented justifications, and that these justifications remain valid. You can use NP-View to verify your compliance with CIP-005 R1.3 as follows:

1. Go through the Rule Audit tab to review Risk Alerts and Justifications.
2. Use the Rule Marker to mark rules that need to be examined more closely.
3. For any open port or service that doesn't have 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.



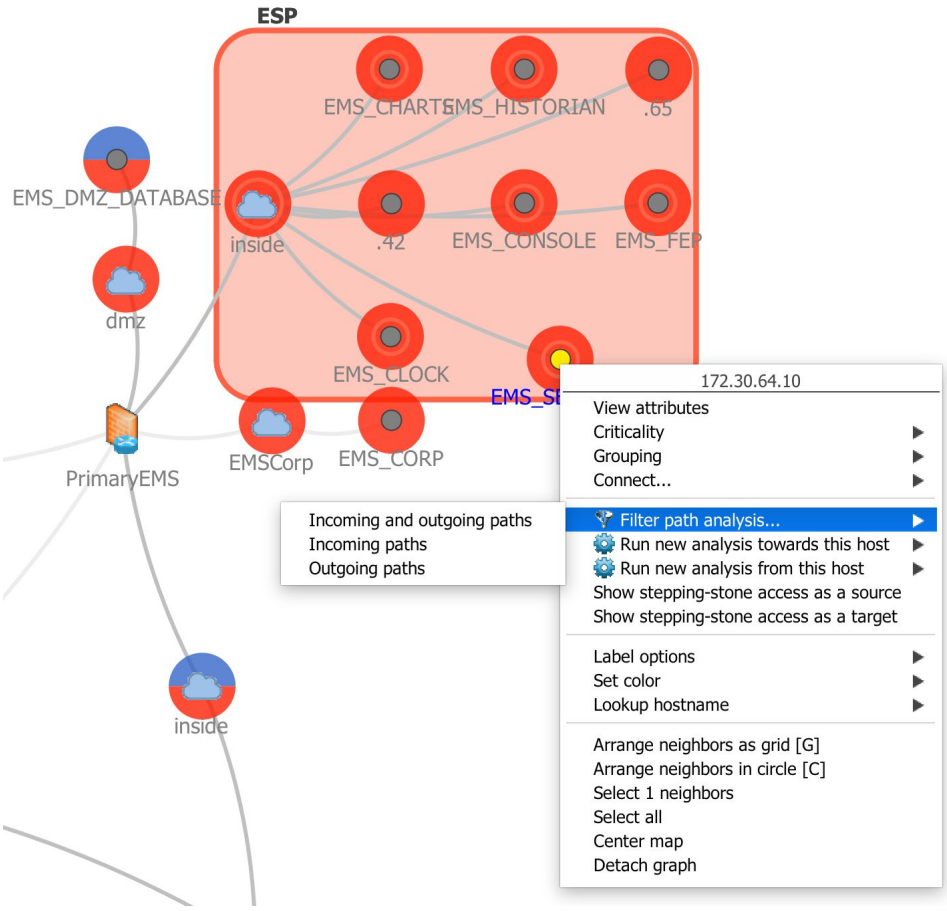
CIP-005 R2.1 For all Interactive Remote Access, utilize an Intermediate System such that the Cyber Asset initiating Interactive Remote Access does not directly access an applicable Cyber Asset.

CIP-005 R2.1 introduces two more important concepts into the NERC CIP standards. The first of these is Interactive Remote Access (IRA). NERC's definition of IRA begins with this sentence: "User-initiated access by a person employing a remote access client or other remote access technology using a routable protocol." Note that the most important feature of IRA is that there is a person sitting at the remote computer and interacting with a BES Cyber System within an ESP. The definition goes on to say "Interactive remote access does not include system-to-system[4] process communications."

The other new concept is Intermediate System (IS), which NERC defines as "A Cyber Asset or collection of Cyber Assets performing access control to restrict Interactive Remote Access to only authorized users." This is what is often called a "jump host" – a server that authenticates remote users, then opens up a new session to connect them to a system on the protected network, which in this case is the ESP. Because the IS opens up a new session, malware on the remote system can't spread into the ESP. The IS needs to be installed in a DMZ, not on the ESP itself. Complying with CIP-005 R2.1 requires you to confirm that all possible Interactive Remote Access paths terminate at the Intermediate System, not at a BES Cyber System in the ESP. Similarly to CIP-005 R1.2, you can identify possible IRA paths using the Path Analysis feature of NP-View:

1. Launch a Full Path Analysis
2. Right click on each component of a BES Cyber System and select "Filter path analysis…" > "Incoming paths"
3. Verify that the paths that use an interactive remote access protocol and that terminate at the selected BES Cyber System component originate from a valid jump host
4. Right click on the jump host and select "Filter path analysis…" > "Incoming and outgoing paths" to review which interactive remote access protocols are permitted to go through the jump host

[4] System-to-system remote access by vendors is addressed in two new requirement parts, CIP-005 R2.4 and R2.5. These two parts are awaiting approval by FERC along with CIP-013, the new standard for supply chain cyber security risk management. CIP-013 and these two requirement parts, as well as another new requirement part, CIP-010 R1.6, will most likely come into effect in later 2019.



Conclusion: Building a 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. This is especially important in the context of CIP-005, since mis-identifying an asset or missing an access rule can lead to serious consequences. This white paper provided a step-by-step guidance towards building such a workflow for four important CIP-005 requirement parts. If you have questions or would like to know more about NP-View, you can contact the Network Perception team at:

(773) 830-4061
info@network-perception.com
https://portal.network-perception.com