network perception

NP-VIEW
Use Cases

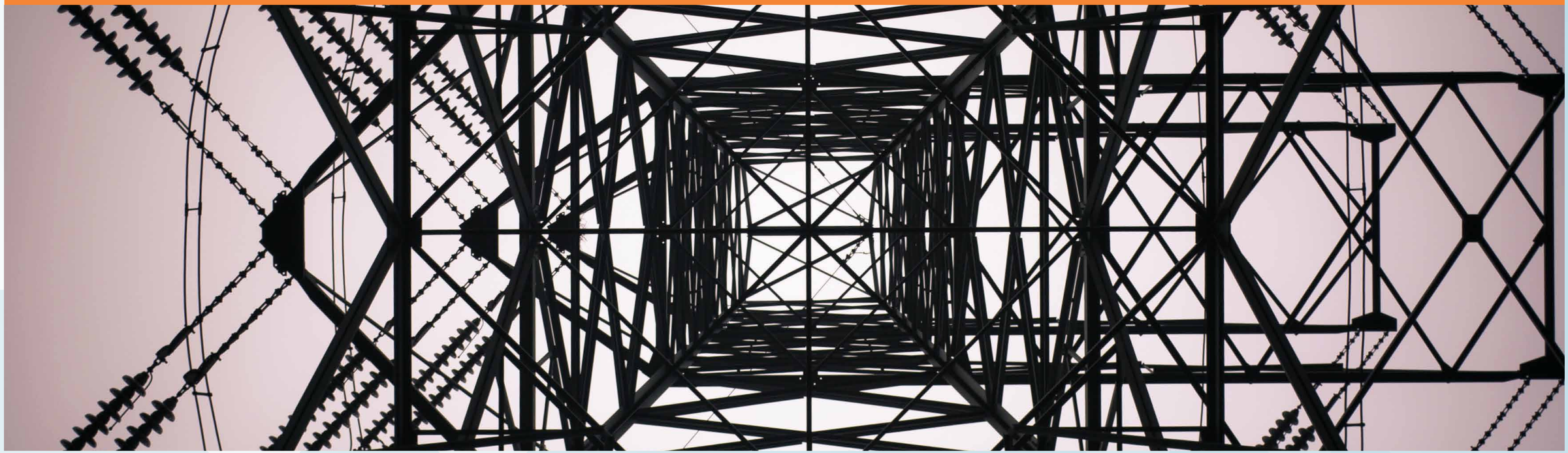


Table of Contents

Introduction

Since its inception, Network Perception has supported the needs of the North American Electrical Reliability Corporation (NERC) industry. Electric utilities in the US that are connected to the bulk electric system must comply with NERC regulations which include cybersecurity requirements under the Critical Infrastructure Protection (CIP) program. Our mission to strengthen cyber resiliency is well-aligned with NERC's mission to assure the effective and efficient reduction of risks to the reliability and security of the grid. Indeed, NERC has developed a risk-based approach to develop standards and the NERC auditors have been using NP-View since 2016 to conduct audits in a consistent manner.

Within the NERC industry, our primary end users have been compliance teams who must prepare for CIP audits and are motivated to see their network the same way NERC auditors would. This unique position has made Network Perception a central resource to bring transparency to network configuration and access policies for all stakeholders. We currently focus on CIP-005 which is the most complex and important standard for utilities with high-impact cyber assets.

The Path to Cyber Resiliency

Compliance Verification
Verify configurations and network segmentation

#1: Policy Review
- Separate monitoring from control
- Review impact of policy changes
- Leverage network sandbox solution

#2: Audit Assistance
- Automate tedious configuration review
- Empower and modernize audit team
- Document evidence of compliance easily

Cybersecurity Visibility
Visualize vulnerability and risk exposure

#3: Architecture Review
- Establish your baseline instantly
- Generate accurate network topology
- Document your network configuration

#4: Network Risk Assessment
- Automatically contextualize network risks
- Prioritize vulnerability mitigation
- Visualize adoption of best practices

Operational Velocity
Accelerate risk mitigation and recover faster

#5: Continuous Configuration Monitoring
- Strengthen your cyber resiliency
- Reduce your risk profile
- Transitioning to 24x7x365 monitoring

#6: Incident Response Preparation
- Decrease response time and cost
- Single pane of glass to provide context
- Provide complete network change history

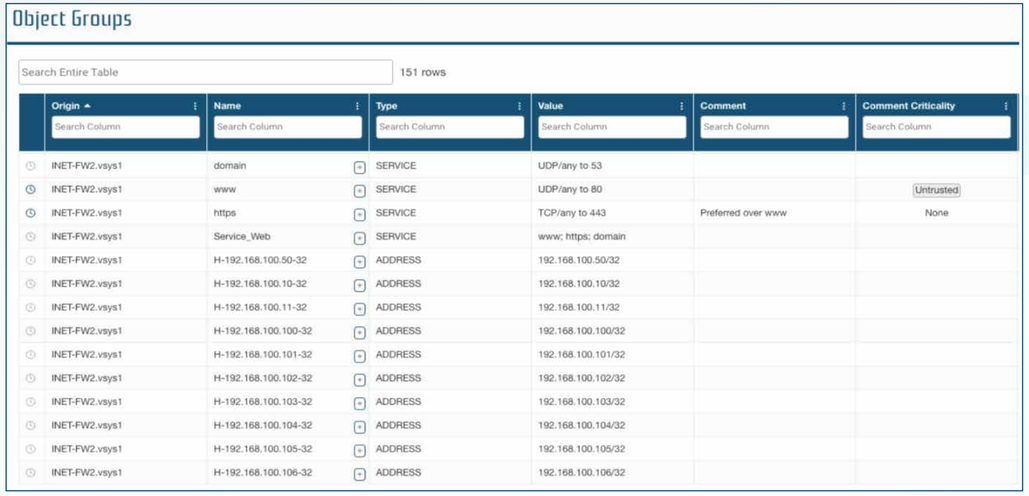
Compliance Verification

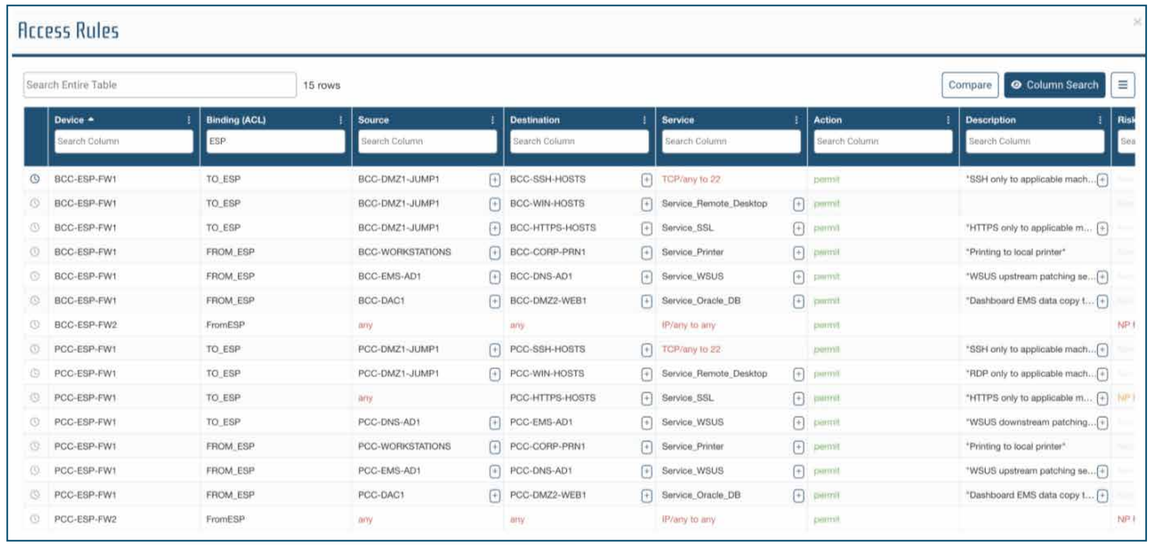
Policy Review

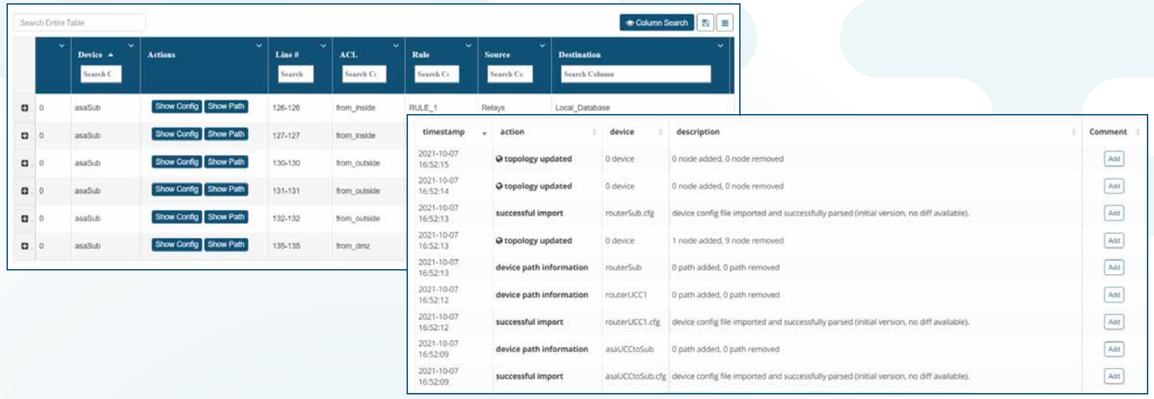
Compliance Verification: Prioritizing risk-based compliance verification can assist stakeholders in validating the accurate segmentation of their network and enhancing their cybersecurity and resilience strategies amidst emerging threats. To safeguard mission-critical assets, industrial control systems require cyber resiliency as their foundation. Achieving network visibility and adopting a risk-based compliance approach are crucial elements in establishing cyber resiliency.

Utility companies employ various technologies, processes, and personnel to protect their critical assets. The verification principle plays a vital role in assessing the utility's existing defenses, identifying vulnerabilities, and addressing them.

Commonly, utilities have different brands of firewalls and routers within their networks, resulting in inconsistent or inadequate permissions and alert rules. Through thorough verification analysis, these vulnerabilities can be detected and resolved. Compliance issues related to existing rules are also identified and rectified by capturing metadata, such as who, when, and why the rule changes were made. Often, this information is stored in Excel files, leading to discrepancies between the spreadsheet and the firewall. To address these gaps and inconsistencies, Network Perception offers utilities a standardized approach for storing metadata, ensuring consistent change management.







Compliance Verification

Audit Assistance

Performing a regular review of your compliance metrics is important for your organization. Performing the review manually is time consuming and tedious. Audit assistance provides the Compliance Team (Auditor, Compliance Officer, Compliance Analyst, and Consultants) with capabilities that allow users to easily prepare compliance reports using Audit Assistants.

Workspace Report (Standard)
The Workspace Report assistant is available within each workspace and will generate a report for a specific view that includes detailed information about configuration files that were imported and parsed including:

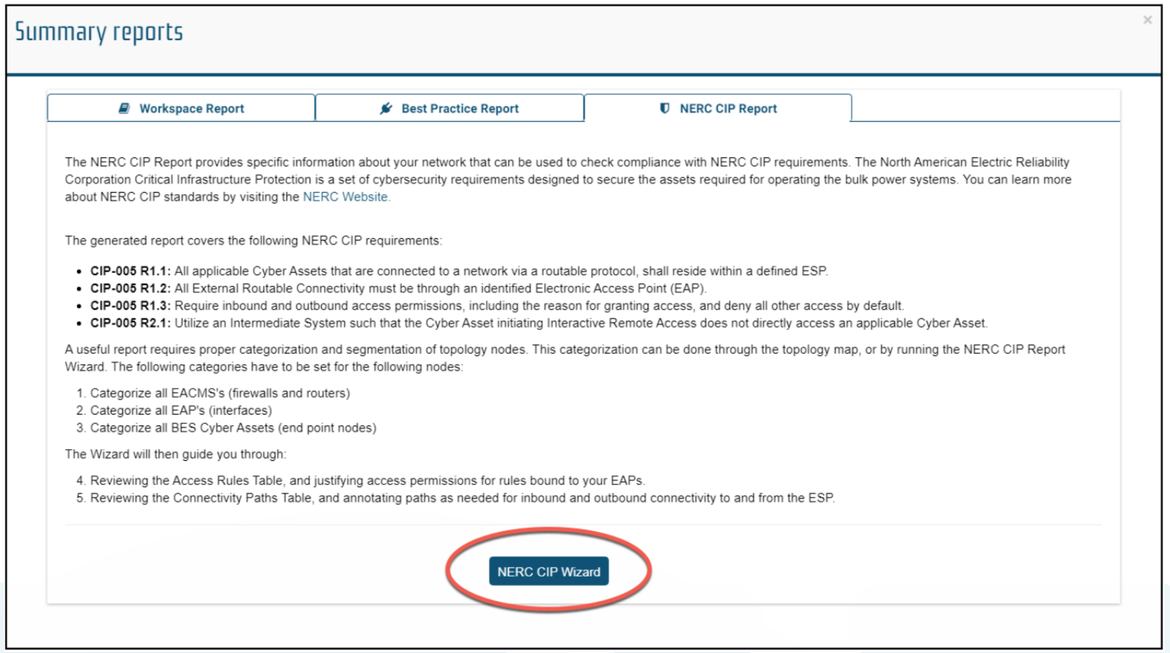
- Configuration assessment report including risk alerts
- Ports and Interfaces
- Access rules
- Object groups
- Path analysis

Industry Best Practice (Premium)
The Best Practice assistant requires a license to activate. This report is available within each workspace to generate a report for a specific view that includes the following topics:

- Parser Warnings and potential misconfigurations
- Unused Object Groups
- Access Rules missing a justification
- Unnamed nodes
- NP Best Practice Policies on access rules and CiS
- Benchmarks that have identified potential risks
- ACL's with no explicit deny by default rule

NERC CIP Compliance (Premium)
The NERC CIP assistant requires a license to activate this function and guides the user through the steps required to create a report covering CIP-005 requirements. The NERC CIP audit assistant is only available within a NERC-CIP workspace and allows audit teams to classify BES cyber assets as High, Medium, and Low based on the standards. We have added a category for untrusted (Internet, Corp, etc.) to tag non BES assets. NP-View allows compliance teams to collect and report evidence related to the following requirements:

- CIP-002 – BES Cyber System Categorization; impact rating and 15-month review
- CIP-003 – Security Management Control; cyber security policy
- CIP-005 – Electronic Security Perimeter; remote access management
- CIP-007 – System Security Management; ports and services
- CIP-010 – Change Management and Vulnerability; configuration change management, configuration monitoring, vulnerability assessment



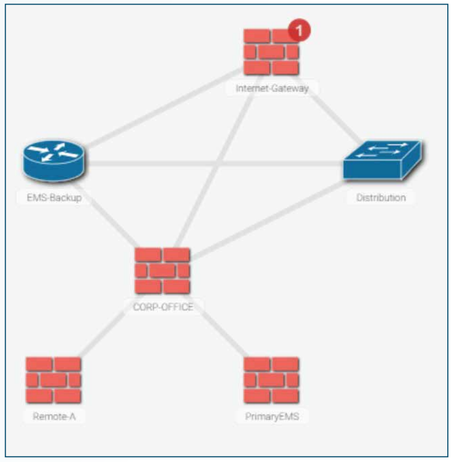
Visualization

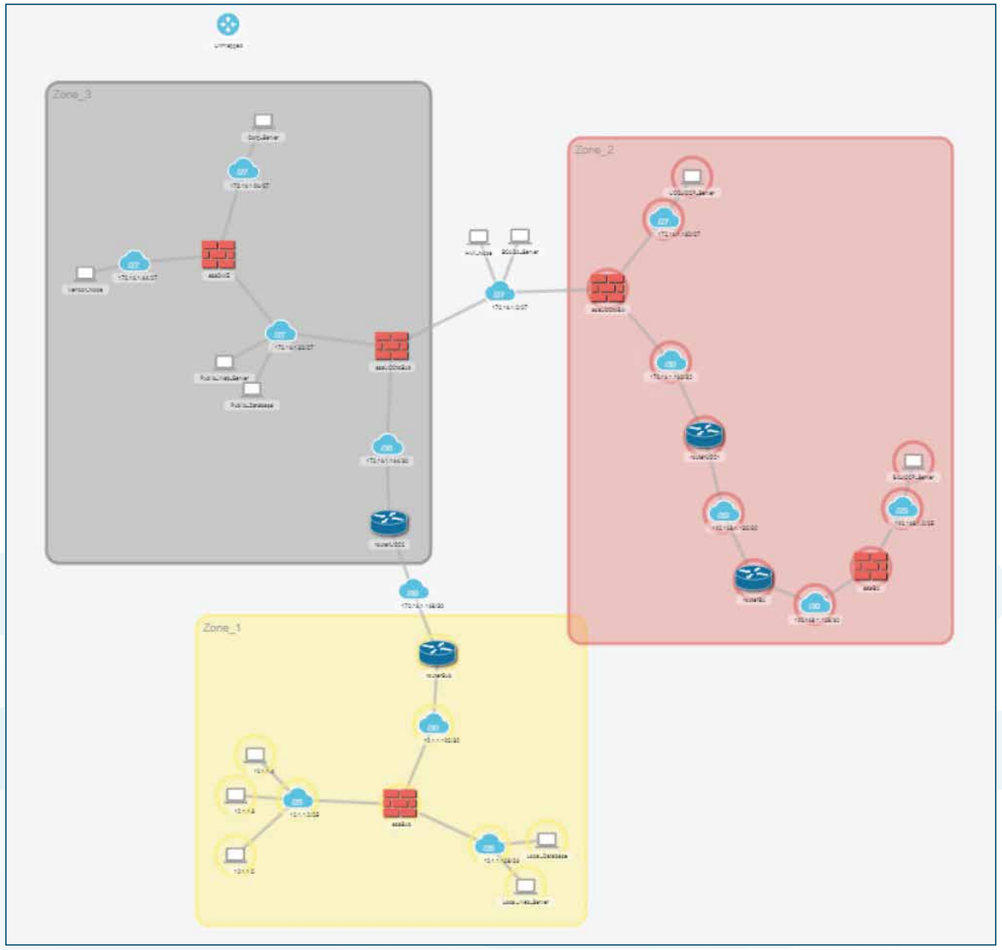
Visibility

The need for a common and easily understood language regarding a utility's network segmentation and the protection of critical assets is crucial for cyber resilience. Visibility plays a vital role in achieving this goal. Various factors contribute to visibility, and one criticality aspect is having a clear understanding of the importance of servers, workstations, and equipment within a network.

Network Perception addresses the need for a common language and the concept of criticality by visualizing a utility's network topology. This visualization allows utilities to assign labels indicating assets' criticality and corresponding defenses. This approach facilitates comprehension for both technical and non-technical audiences.

To adequately protect critical assets, it is essential to have multiple layers of defense. However, before implementing such defenses, it is crucial to identify the critical assets and understand the various layers of defense involved. Questions such as whether there are multiple zones or if the network is correctly segmented can be addressed by utilizing the topology map and associated reports provided by Network Perception. These tools enable utilities to verify the effectiveness of their network defenses and ensure proper protection for critical assets.





Visualization

Network Risk Assessment

Network risk assessment offers essential capabilities to the Networking Team and Audit Team. It helps assess network segmentation, identify risky connectivity paths, and understand asset vulnerability. By leveraging these capabilities, organizations can effectively enhance their cybersecurity posture and protect their network infrastructure.

Identifying Risky Connectivity Paths
Using industry best practices, Network Perception automatically identifies potential risks related to network configurations. Using the Network Perception Connectivity Path analysis, the user can review each of the highlighted risks and make a judgment on action.

Exposure of Vulnerable Assets – Vulnerability Analytics
NP-View provides your security team with a single pane of glass for reviewing network vulnerability exposure. With the addition of scanner data or data from a vulnerability data service, vulnerabilities can be tracked across your network. In NP-View vulnerabilities are displayed in a few places

Topology Display of Vulnerabilities
When scanned data has been added to a workspace, and a topology view is built that also includes that scan data, nodes on the topology of that view will be marked with a shield indicating the presence of vulnerabilities. These shields can be toggled on and off using the topology settings menu.

Device Panel Display of Vulnerabilities
Firewalls, Gateways, and Hosts may contain vulnerability and service information imported from scans. Clicking on any of these nodes in a View that contains vulnerability information, will display it in the info panel that opens over the main menu.

Identifying Risky Connectivity Paths

Source	Destination	Protocol	Port	Rule Sequence
10.1.1.192:10.1.1.195	172.16.1.168:172.16.1.171	ip	any	
10.1.1.192:10.1.1.195	172.16.1.164:172.16.1.167	ip	any	
10.1.1.2:10.1.1.4	10.1.1.130:10.1.1.130	tcp	1433	asaSub: line 126: from Relays to Local_Database on SQL
172.16.1.0:172.16.1.31	172.16.1.128:172.16.1.159	ip	any	
172.16.1.0:172.16.1.31	172.16.1.160:172.16.1.163	ip	any	
172.16.1.130:172.16.1.130	172.16.1.35:172.16.1.35	tcp	1433	asaUCCtoBA: line 126: from UCC_ICCP_Server to Public_Database on SQL
172.16.1.160:172.16.1.163	192.168.1.132:192.168.1.135	ip	any	
172.16.1.160:172.16.1.163	192.168.1.128:192.168.1.131	ip	any	
172.16.1.164:172.16.1.167	172.16.1.168:172.16.1.171	ip	any	
172.16.1.164:172.16.1.167	10.1.1.192:10.1.1.195	ip	any	
172.16.1.168:172.16.1.171	10.1.1.192:10.1.1.195	ip	any	
172.16.1.168:172.16.1.171	172.16.1.164:172.16.1.167	ip	any	
172.16.1.3:172.16.1.3	10.1.1.2:10.1.1.4	tcp	20000	asaUCCtoSub: line 122: from SCADA_Server to Relays on SCADA
172.16.1.3:172.16.1.3	172.16.1.35:172.16.1.35	tcp	1433	asaUCCtoSub: line 125: from SCADA_Server to Public_Database on SQL
172.16.1.4:172.16.1.4	10.1.1.131:10.1.1.131	tcp	80	asaUCCtoSub: line 123: from HMI_Node to Local_Web_Server on HTTP
172.16.1.4:172.16.1.4	10.1.1.131:10.1.1.131	tcp	443	asaUCCtoSub: line 123: from HMI_Node to Local_Web_Server on HTTP
172.16.1.4:172.16.1.4	10.1.1.131:10.1.1.131	tcp	8080	asaUCCtoSub: line 123: from HMI_Node to Local_Web_Server on HTTP
172.16.1.4:172.16.1.4	10.1.1.131:10.1.1.131	tcp	8443	asaUCCtoSub: line 123: from HMI_Node to Local_Web_Server on HTTP
				asaDMZ: line 126: from Vendor_Node to Public_Database on SQL
				e to Public_Web_Server on HTTP
				e to Public_Web_Server on HTTP

Connectivity Matrix

From/To	OUTSIDE	INSIDE	DMZ
OUTSIDE		Denied	Denied
INSIDE	Denied		TCP/1433
DMZ	Denied	Denied	

Velocity

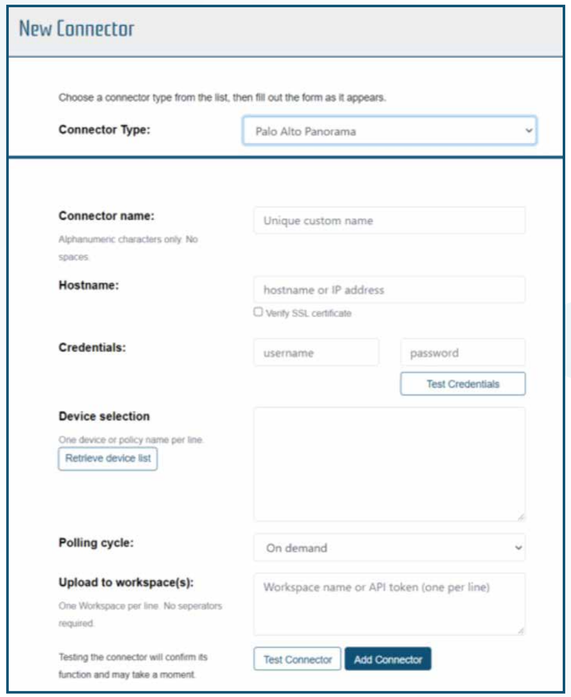
Continuous Monitoring

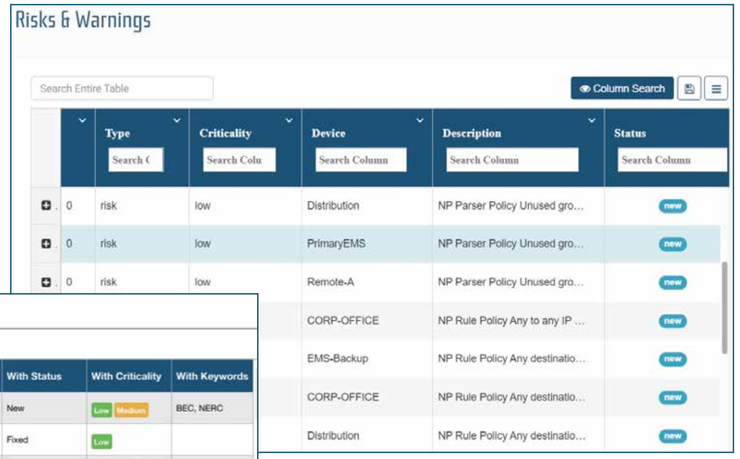
Achieving and maintaining utility cyber resilience presents a formidable challenge due to the relentless adaptability and evolution of cybercriminal attacks, far outpacing the capacity of security measures to respond effectively. This challenge is compounded when utilities fail to assess and address risks and attacks in real-time.

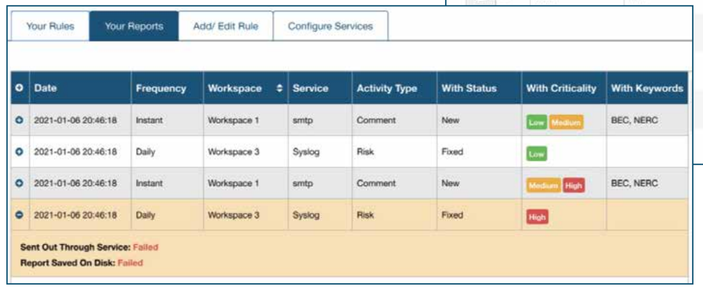
The solution lies in embracing velocity—a fundamental principle that guards against the risk profile spiraling out of control by continuously verifying and visualizing risks. Simply checking the network for vulnerabilities once a year leaves room for exponential risk growth over the course of twelve months. To counter this, a velocity-driven approach advocates for real-time risk assessment and monitoring.

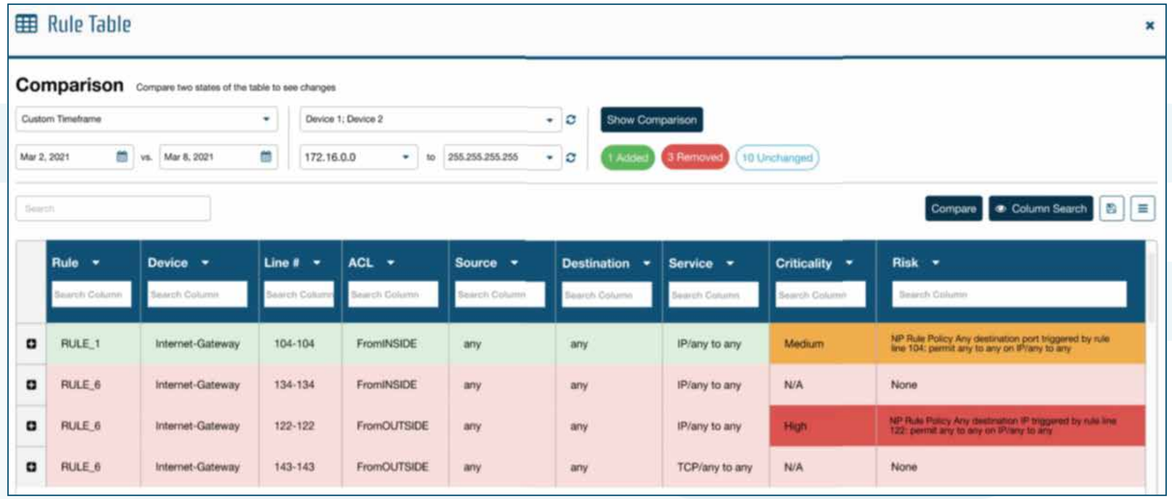
A solution like Network Perception empowers utilities to model their networks and visualize risks and vulnerabilities in real-time, injecting unparalleled velocity into their cyber resilience endeavors. By seamlessly integrating configuration files and data, this solution enables utilities to proactively identify and mitigate risks as they unfold. This fusion of asset criticality and an understanding of vulnerability pathways allows for informed decision-making regarding the prioritization of actions—such as promptly patching vulnerable assets, enhancing zone segmentation, and addressing access policy gaps with utmost urgency.

In essence, the passage underscores the criticality of real-time risk assessment and visualization in safeguarding the cyber resilience of utilities. It highlights the immense value of deploying a solution like Network Perception to unlock the power of velocity, effectively responding to the ever-evolving landscape of cyber threats.









Velocity

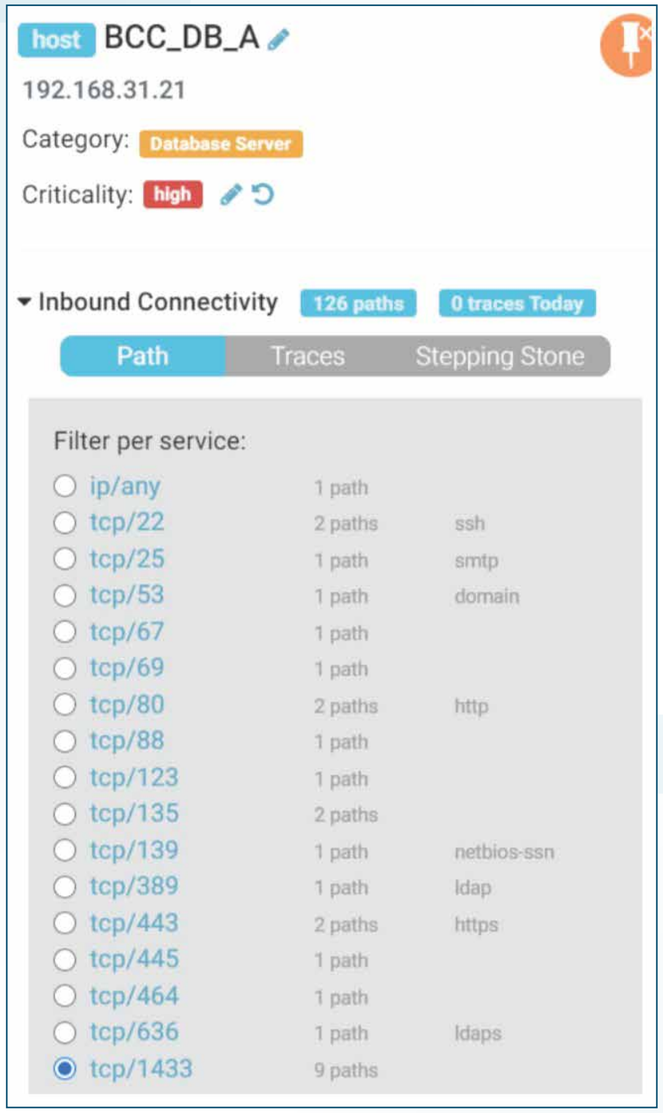
Incident Response Preparation

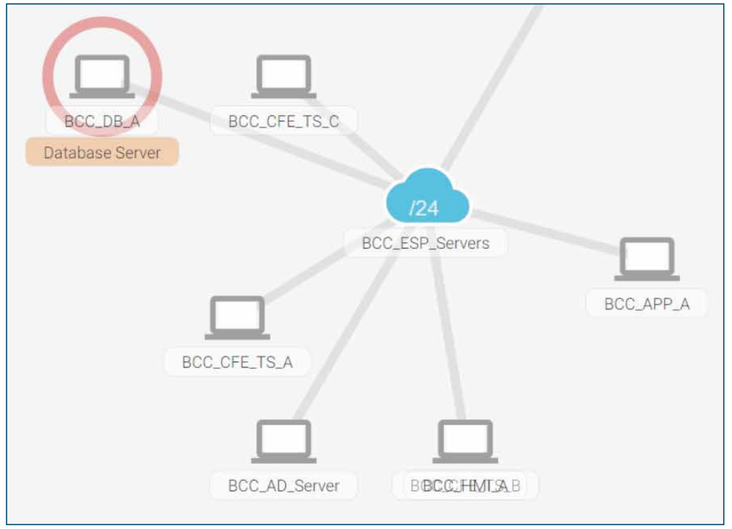
Incident Response Preparation provides the Network Security Team and Compliance Team with capabilities that allow users to:

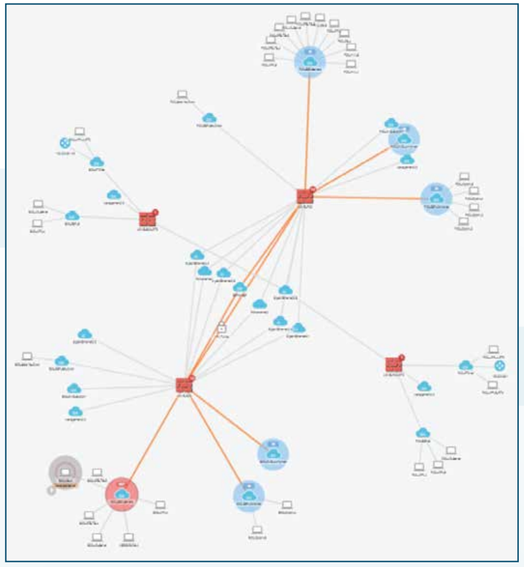
Align network architecture understanding and break silos through a single pane of glass
Monitoring for indicators of compromise allows organizations to better detect and respond to security compromises. When the security team discovers a potential compromise, NP-View can assist with incident response by quickly identifying critical paths to the compromised system.

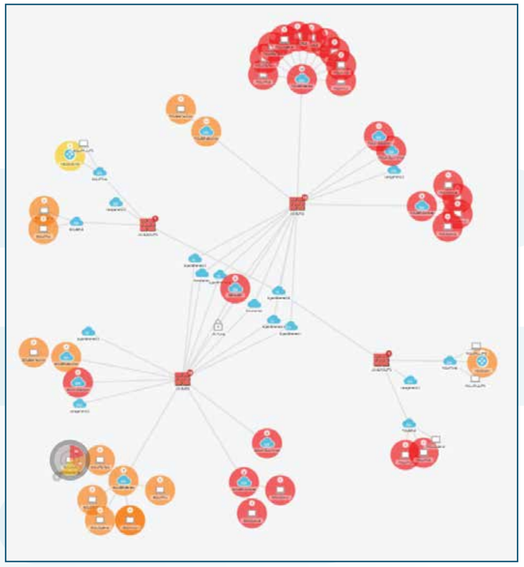
Train first responders and harden defenses via realistic attack scenario simulation
Users can be trained to use NP-View to quickly assess the situation. NP-View shows each host with the inbound and outbound paths. In this example, the inbound port, 1443, is the likely target for the increased database activity.

Prioritize vulnerability mitigation faster
Stepping stones are hosts in a network which could be compromised and used by malicious attackers to perform lateral movements. Attackers hop from one compromised host to another to form a chain of stepping stones before launching an attack on the actual target host.









network perception

Secure Today to Ensure Tomorrow:
Working Together to Protect Utilities and Critical Infrastructure.

Contact us today, we can help you.

+1 (872) 245-4100

info@network-perception.com

https://network-perception.com

Request a Demo