The Importance of Protecting MISSION-CRITICAL ASSETS on the Path to Cyber Resiliency

Benefits of the Integration

- Retrieve configuration files from Cisco IOS, ASA, FTD devices or Firepower Management Center (FMC).
- Analyze firewall configurations to identify potential configuration risks and vulnerabilities.
- Alert key users of potential risk situations in near-real time.
- Review an interactive visual representation of the network topology and cyber risks.

Customer Challenge

Your cyber resiliency journey starts with establishing a clear baseline. Then you can verify if your risk mitigation controls align with what you'd expect. To do this, you will need an accurate view of the network architecture and cybersecurity posture. This information can then be used to set up continuous monitoring so you can decrease your response time and adapt quickly to disruptions. While performing regular reviews of your compliance metrics is important for your organization, accessing that data and analyzing it can be time-consuming, tedious, and limited depending on where you are looking. As cybersecurity risks grow, reviews need to become more comprehensive and frequent and need to be managed in a way that will not overburden security and audit teams. Network assessment automation is a foundation of cyber resiliency that enables security and audit teams to transition from point-in-time spot-checking to real-time verification.

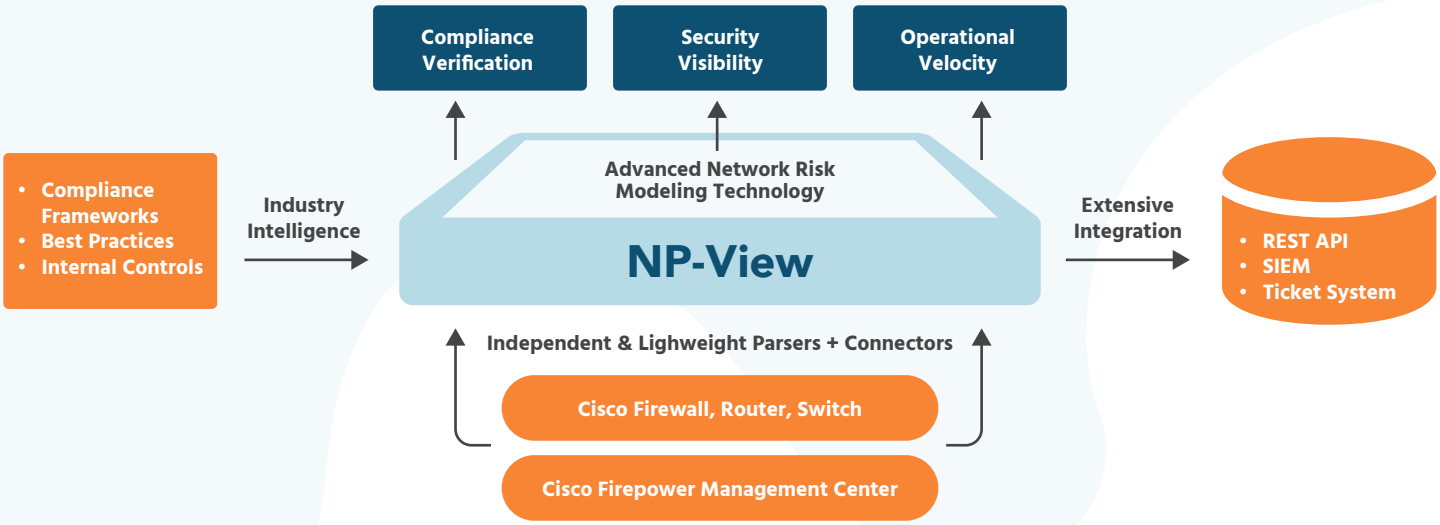
Network Perception NP-View

NP-View, combined with Cisco IOS, ASA or FTD network devices provides a comprehensive, independent audit platform to track and verify system changes and provide network visibility. NP-View provides auditors with assessment reports and network engineers with proactive alerts to help identify potential network risk. NP-View's read-only approach isolates the assessment team from the management systems, providing a secure barrier to prevent accidental system changes. NP-View's comprehensive connectivity path analysis allows for the assessment of each network path and visibility into the nearest neighbors with steppingstone analysis to identify system vulnerabilities.

Cisco and Network Perception

The integration between Cisco IOS, ASA or FTD devices and Network Perception NP-View provides network engineers, network security and compliance analysts with an easy review of firewall access rules and object groups. The integration provides automatic identification of configuration risks and the information needed to establish a configuration change review process. NP-View's audit assistants allow the compliance team to verify cybersecurity regulations, best practices and prepare audit-ready artifacts. For visual learners, NP-View provides the networking team with a topology map of their architecture. The topology can be used to identify and label critical cyber assets, critical network zones and review which devices are protecting which network zones.

The NP-View and Cisco Integration



USE CASES

Verify Configurations for Compliance

Challenge

A mission-critical OT application has a network of 175 high-availability Cisco FTD firewalls connected to a Firepower Management Center (FMC). The internal audit team needs to collect information to perform a compliance review.

Solution

NP-View policy review provides compliance analysts with automated capabilities to easily collect and review cyber assets with their firewall access rules and object groups. Audit assistants provide automatic identification and reporting of configuration risks and remediation recommendations.

Network Architecture Review

Challenge

A mission-critical IT facility is replacing its legacy ASA network with 50 FTD firewalls connected to a Firepower Management Center (FMC). The network architecture team wants to evaluate the network rules for potential risks before going live.

Solution

NP-View architecture review provides the networking team with capabilities for easy creation and visualization of an accurate topology of the network architecture. The topology can be used for evaluating the architecture for potential risks before the configurations are pushed into production by the Firepower Management Center (FMC).

ABOUT Network Perception

Network Perception protects industrial control systems by ensuring network access security as the first line of perimeter defense. Our monitoring software provides complete network transparency and continuous mapping to better support cybersecurity compliance and enable greater cyber resiliency. For more information, visit www.network-perception.com.

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