Technology Partner Program

Integration Guide - Use Case Documentation

Author: Network Perception

Revision History	
1/19/2022	Baseline document
1/10/2024	Update to reflect support for Panorama and PAN-OS 11.x

Table 1: Partner information	
Date	1/10/2024
Partner Name	Network Perception
Website	www.network-perception.com
Product Name	NP-View
Partner Contact	info@network-perception.com
Support Contact	support@network-perception.com
Product Description	NP-View protects your critical assets by providing: • **Firewall Auditing:** Analysis of the rules that dictate access to ensure sufficient justification is provided. • **Segmentation Verification:** Enables visibility of zone-to-zone paths and shows the segmentation of the network. • **Network Visibility:** Intakes configuration information from firewalls, routers, switches and creates an easy-to-read map to provide rapid understanding of the network.

Table 2: Palo Alto Networks Products for Integration			
Palo Alto Networks Product	**Integration Status**	**Palo Alto Networks Versions Tested**	**Network Perception Versions Tested**
AutoFocus			
Cortex Data Lake			
Cortex XDR			
GlobalProtect			
IoT Security			
Prisma Access			
Prisma Cloud			
Prisma SaaS			
MineMeld			
Next-Generation Firewall	Validated	10.2.4, 11.0.1	NP-View 5.0
Panorama	Validated	10.2.4, 11.1.0	NP-View 5.0
VM-Series			
WildFire			
Other			

Use Cases for Integration with Palo Alto Networks

Use Case 1 – Firewall Auditing

NP-View provides in-depth Policy Review capabilities that automate the collection of access rules and object groups from Palo Alto Networks devices to separate monitoring from control. NP-View analyzes the data to identify changes and review the impacts of these changes, highlighting those that are a potential risk. Additionally, NP-View automates configuration review using the Network Perception audit assistant to help audit teams easily document evidence for compliance reviews.

Use Case 2 – Segmentation Verification

NP-View provides in-depth segmentation verification that automatically establishes a network baseline and generates an accurate network topology map for review. With this information the Security and Compliance teams can perform a network risk assessment, analyze vulnerability, and visualize the adoption of best practices.

Use Case 3 – Network Visibility

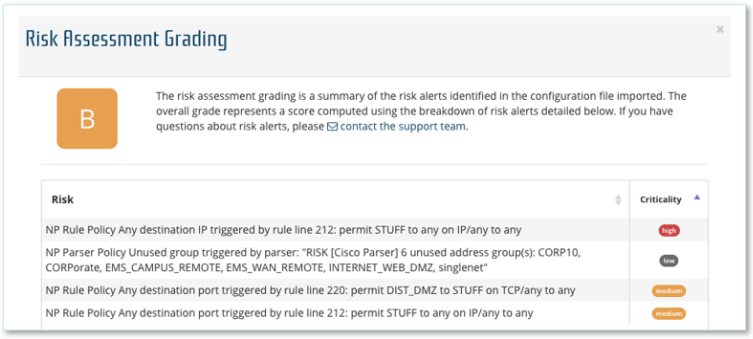
NP-View provides Continuous Configuration Monitoring that helps strengthen your cyber resiliency while simultaneously reducing your risk profile. NP-View helps with incident response preparation, by decreasing your response times and costs. In one comprehensive view, you can review network changes to track and identify improper changes made across your network.

Integration Benefits

NP-View connects with your Palo Alto devices to automatically retrieve configuration files to report change detection and risk identification. Benefits of the integration with Panorama and the Palo Alto Networks ML-Powered NGFW include:

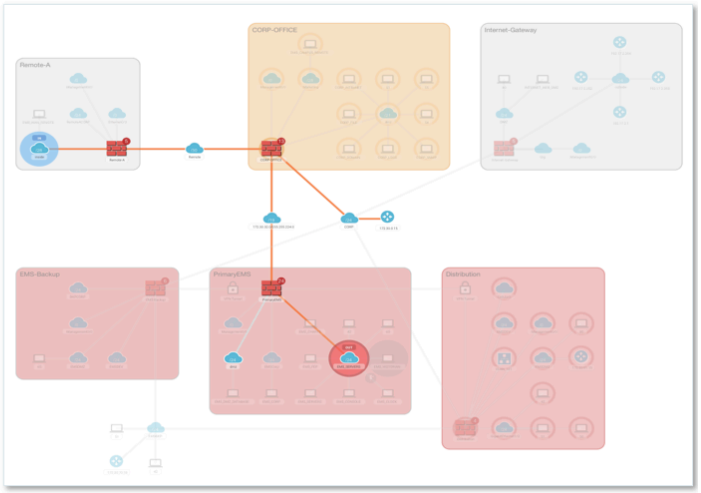
- Automatically retrieve configuration files from Palo Alto Networks NGFWs or Panorama Network Management Systems (Panorama) devices.
- Automatically analyze NGFW configurations to identify potential configuration risks and vulnerabilities.
- Automatically alert key users of potential risk situations in near real-time.
- Provide an interactive visual representation of network topology and cyber risk areas.

- **Automated Risk Scoring**
  - *Risk alerts*
  - *Access rule review*
  - *Misconfigurations*
- **Compliance Modules**
  - *Best practices*
  - *NERC CIP*
- **Instant Reports**
  - *Change tracking*
  - *Asset inventory & device info*
  - *Object groups*
  - *Access rule table*
  - *Network zones*
  - *Path analysis & path history*



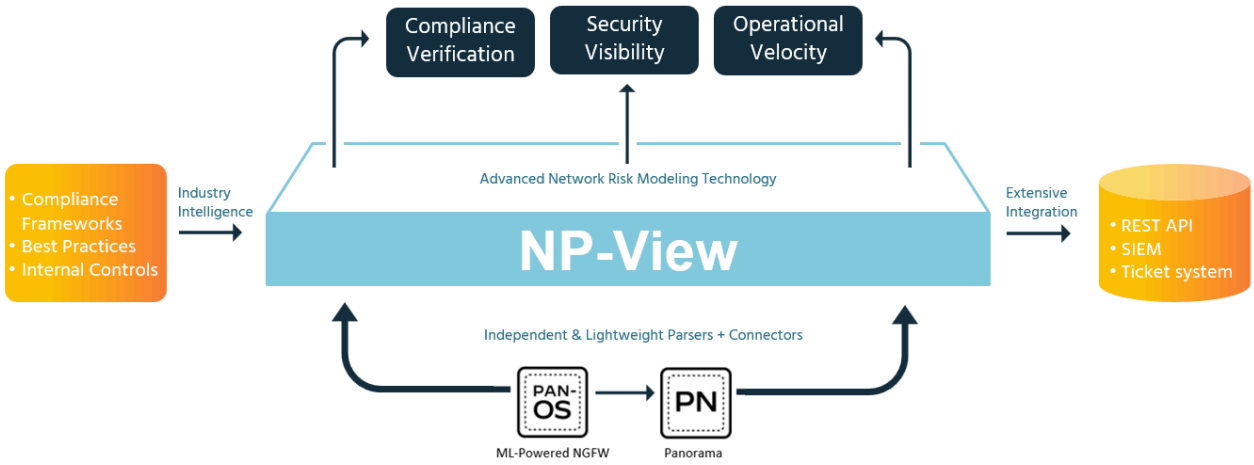
#1: Policy Review **#2: Audit Assistance**

- **Intelligent Network Topology**
  - *Uses only device configuration*
  - *Easy navigation & customization*
  - *Designed for both technical and non-technical users*
- **Visual Path Analysis**
  - *End-to-end connectivity*
  - *Ports and services review*
  - *Stepping-stone attack map*
- **Single Pane of Glass**
  - *Import scanner reports*
  - *Visualize vulnerability exposure*
  - *Import ARP tables and hostname files*



#3: Architecture Review **#4: Network Risk Assessment**

Integration Diagram



Network Perception & Data

The data used by NP-View consists of Palo Alto Networks NGFW and/or Panorama files containing device and system configuration information. The data is shared over HTTPS for real time analysis or through a manual device export / import into NP-View. NP-View is a read-only system and does not write back to the NGFW or Panorama. Configuration changes are recorded, data is analyzed, potential risks are identified, logged, and notifications of risks can be sent by email, syslog, STIX/TAXII or Service Now.

Before you begin, you will need to install and configure NP-View.

NP-View System Documentation

- Installation guide for NP-View
- Configuration guide for NP-View

Dependencies

The server version of NP-View is a Linux only application that will run on most editions of Linux and has been tested on CENTOS 7, RedHat, Ubuntu, and Debian. Alternatively, the .OVF can be downloaded and installed on most virtual machines that accept a .OVF and has been tested on VMWare and Virtual Box. System sizing can be accessed through the NP-View Installation Guide.

Palo Alto Networks Configuration

- NP-View is a lightweight application designed to make integration as simple as possible. Simply create a connector in NP-View using standard user credentials. NP-View is a real-time application so we recommend creating a Superuser (read-only) account on the Panorama instance that can be used by NP-View.

  Also see:

  Performing Initial Configuration on the Palo Alto Networks NGFW

  Setting Up the Panorama Virtual Appliance

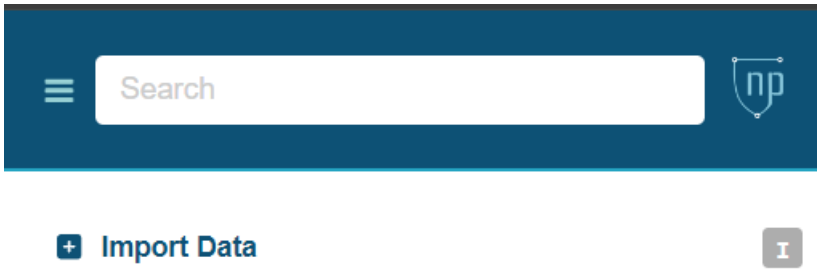
  Administrative Access Best Practices

- Palo Alto Networks PAN-OS API access must be enabled for NP-View to have access to the data through the Superuser account. Enable PAN-OS API Access

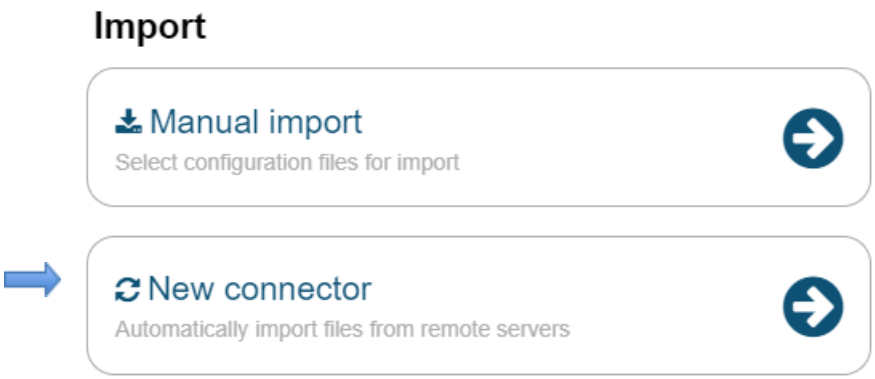
Partner Product Configuration

Use the below steps to configure NP-View connectors.

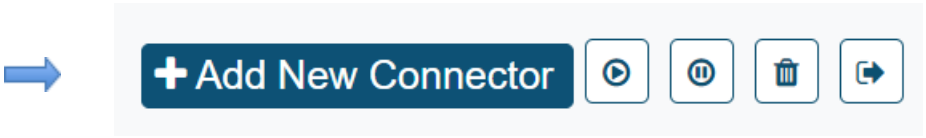
- Select and import data from the main menu.



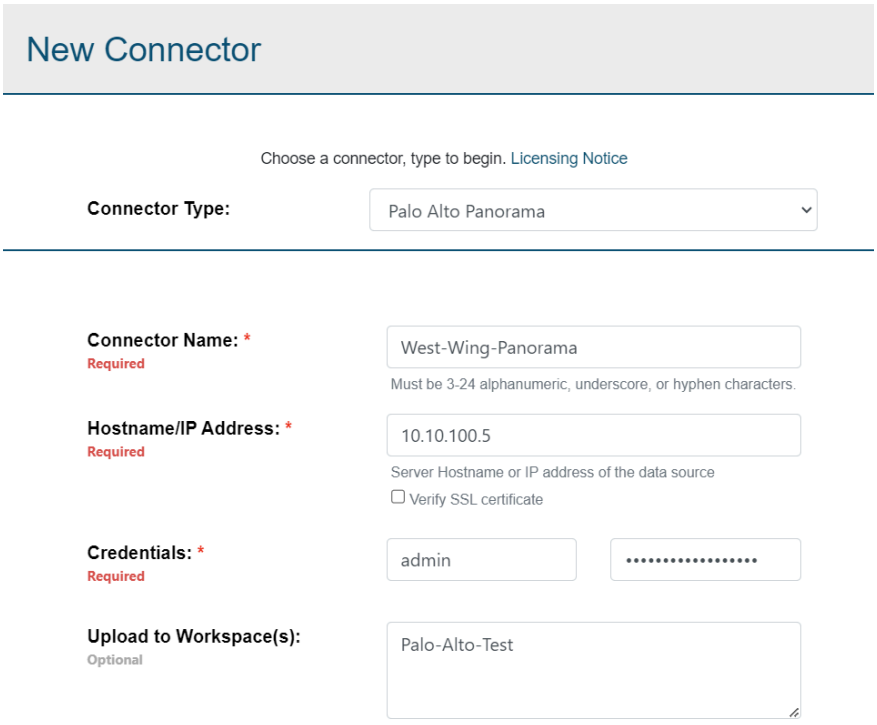
- Select New Connector



- Select 'Add New Connector'

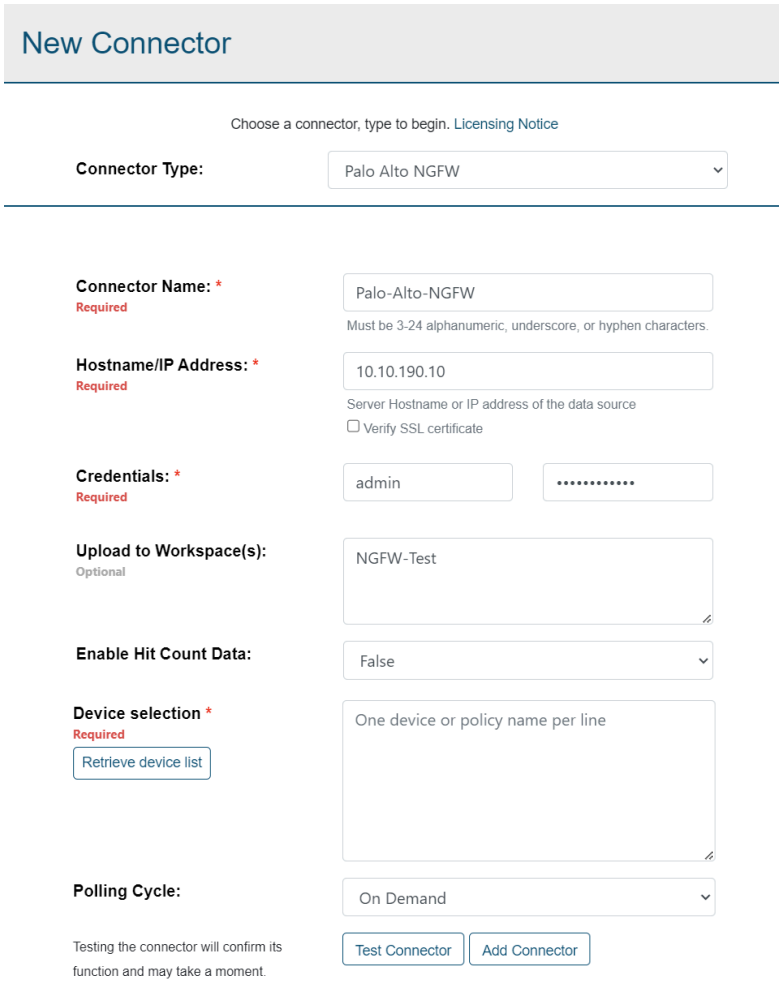


- Select the required connector type from the dropdown.
  - Option A - Panorama Connector:
    - Name the connector and fill in the connection credentials.
    - After successful authentication, add a list of NGFWs to import (one per line) or select ‘Retrieve device list’ to be presented with a list of devices to select from.
    - Then add the workspaces where the chosen device data is to be delivered.
    - Select a polling cycle
    - Select Add Connector




Device selection *
Required
Device state: Active
Retrieve device list
First, choose the state of the devices you wish to retrieve, then click Retrieve.
The retrieved items will appear here as one policy or device per line.
Polling Cycle:
Daily
Testing the connector will confirm its function and may take a moment.
Test Connector
Add Connector

- Option B - NGFW Connector:
  - Name the connector and fill in the connection credentials.
  - After successful authentication, add the workspaces where the data is to be delivered.
  - Select add connector



Troubleshooting & Support

Troubleshooting

NOTE: *Use cases that do not match the use case(s) as documented in this integration guide, using a major release of PAN-OS or a major release of the partner product not listed as tested and validated are* ***out of the scope*** *of the integration as documented by this integration guide. Any additional use cases or variation from those use cases documented in this integration guide are* ***out of the scope*** *of this integration guide document. It is not outside the realm of possibility that unanticipated issues (i.e. scalability, concurrent API session limits, interoperability, other incompatibilities, etc.) could be encountered if* ***out-of-scope*** *use cases for this integration guide document are deployed. Therefore, after familiarizing yourself with the use cases documented in this integration guide, if there are plans to deploy use cases that are* ***out-of-scope*** *for this integration guide, it is highly recommended that the initial deployment be performed in a pilot/proof-of-concept environment prior to deployment within production.*

Network Perception:

- The NP-View connectors communicate over HTTPS. The most common connection issues are caused by the NGFWs prohibiting HTTPS traffic from the NGFW or Panorama systems to NP-View.

Palo Alto Networks:

*****PAN-OS 11.0 Release Notes******
PAN-OS 11.0.0 Known and Addressed Issues

PAN-OS 11.1.0 Known and Addressed Issues

NOTE: Starting from PAN-OS 10.2 forward, it is required that all certificates meet the following minimum requirements:

- RSA 2048 bits or greater, or ECDSA 256 bits or greater
- Digest of SHA256 or greater

See Certificate Management or Setting Up Authentication Using Custom Certificates for more information on regenerating or re-importing your certificates.

NOTE: Ensure that the running version of PAN-OS and/ or Panorama is not EoL: End-of-Life Summary - Palo Alto Networks

Palo Alto Networks Customer Support does not provide support of any kind for system software that is EoL.

If you need to upgrade to a supported version please see: PAN-OS Upgrade Guide

HA Concepts

Palo Alto Networks NGFWs support stateful active/passive or active/active high availability with session and configuration synchronization with a few exceptions:

- The VM-Series NGFW on Azure and VM-Series NGFW on AWS support active/passive HA only. On AWS, when you deploy the NGFW with the Amazon Elastic Load Balancing (ELB) service, it does not support HA (in this case, ELB service provides the failover capabilities).
- The VM-Series NGFW on Google Cloud Platform does not support HA.

If you are going to configure HA clustering, begin by understanding the HA Concepts and the HA Clustering Overview .

Helpful Resources

Network Perception:

- Network Perception Knowledgebase

Palo Alto Networks:

- Palo Alto Networks TechDocs - Home
- Panorama Administrator's Guide
- PAN-OS® Administrator's Guide
- Get Started with PAN-OS
- Creating Security Policy Rules
- Security Policy Rule Optimization - PAN-OS
- Palo Alto Networks Best Practice Guides
- Configuring Various Authentication Methods
- The Best Practice Assessment (BPA) Tool
- Installing a Device Certificate (On Device Not Being Managed by Panorama)
- PAN-OS® and Panorama™API Usage Guide
- Palo Alto Networks Live Community
- End-of-Life Summary - Palo Alto Networks

Contact Information for Support

For Network Perception specific issues:

- support@network-perception.com

For Palo Alto Networks specific issues:

- Palo Alto Networks Customer Support
- How to set up a Palo Alto Networks Customer Support Account

Technical Details

The PAN-OS API calls being leveraged in this integration are listed below:

- GET API key
  https://<firewall>/api/?type=keygen&user=<username>&password=<password>

- GET current running config
  https://{{host}}/api/?type=config&action=show&xpath=

- GET a list of connected NGFWs
  https://<panorama>/api/?key=apikey&type=op&cmd=<show><devices><all></all></devices></show>