TECHNOLOGY PARTNER PROGRAM

USE CASE DOCUMENTATION

Author: Indeni

Contents

Partner Information 3

Use cases for integration into Palo Alto Networks Next Generation Security Operating Platform 3

Palo Alto Networks Products for Integration 4

Integration Benefits 5

Integration Diagram 5

Before you begin 5

Palo Alto Networks Configuration 6

Partner Product Configuration 6

Troubleshooting 6

Technical Details 7

Partner Information

Partner information	
Date	October 1, 2019
Partner Name	Indeni
Web Site	https://indeni.com
Product Name	Indeni Platform
Partner Contact	Yoni Leitersdorf, CEO & Founder, y@indeni.com
Support Contact	support@Indeni.com +1-877-778-8991
Partner Product for Integration	Indeni Platform
Product Description	Security infrastructure stability automation

Use cases for integration into Palo Alto Networks Next Generation Security Operating Platform

Automate Health and High Availability Readiness

- Deep knowledge of Palo Alto Networks NGFW & Panorama from crowd-sourced learnings
- Fully aware of hardware and virtual appliance deployments
- Indeni Rules for PAN-OS and Panorama are updated frequently
- Continuous monitoring for issues in following categories:
    - Detect state or config changes that would cause HA to fail or mis-handle traffic
    - Detect hidden situations that may require administrative maintenance
    - Detect indications of reduced system health
- Actionable information and flexible notification for detected Issues:
    - Description, Remediation Steps, and links to relevant Palo Alto Networks Support Portal articles
    - Flexible notification via northbound integration with ServiceNow, SNMP, syslog, and email

Reduce Administrative Overhead and Operational Impact

- Self-tuning based on device and version for low noise, high signal
- Issue self-closes if problem is resolved, re-opens if it recurs, and appends automated analysis notes
- Continuous monitoring for issues including, but not limited to, the following categories:
    - Validate use of Palo Alto Networks Best Practices
    - Validate compliance with site-local standards
    - System performance

    - SSL certificates
    - Dynamic Updates
    - Network Interfaces
    - High Availability
    - Routing Protocols
- Actionable information and flexible notification for detected Issues:
    - Description, Remediation Steps, and links to relevant Palo Alto Networks Support Portal articles
    - Flexible notification via northbound integration with ServiceNow, SNMP traps, syslog, and email

Palo Alto Networks Products for Integration

Palo Alto Networks Product	Integration Status	Palo Alto Networks versions supported	Indeni versions supported
Aperture			
Application Framework			
Autofocus			
Evident.io			
GlobalProtect			
GlobalProtect Cloud Service			
Logging Service			
MineMeld			
NGFW	Tested	PAN-OS 7.1, 8.0, 8.1, 9.0	Indeni 6.x and higher
Panorama	Tested	PAN-OS 7.1, 8.0, 8.1, 9.0	Indeni 6.x and higher
Traps			
VM-Series		PAN-OS 7.1, 8.0, 8.1, 9.0	Indeni 6.x and higher
Wildfire			
Other			

Integration Benefits

Find: Automated Palo Alto Networks expertise for customers

- Detection based on Knowledge of proper functioning per device, not generic thresholds.
- Per-alert description, recommended remediation, and links to any relevant Palo Alto Networks KB articles.
- Alerts self-clear if the situation resolves, with a Cooldown to prevent alert floods from flapping.

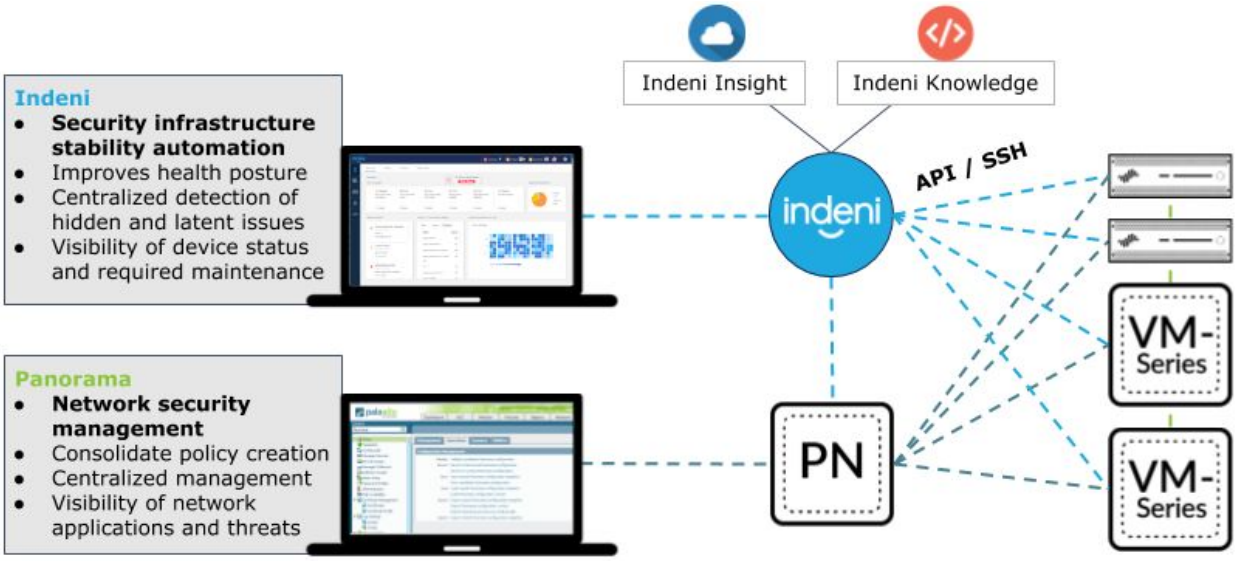
Analyze: Improved Palo Alto Networks and Panorama health posture

- Forthcoming expiration of certificates, licenses, contracts, and support
- Hardware redundancy loss from missing PS, RAID degradation, or LACP partial outage
- HA unreadiness from config skew, route mismatch, and sync failure
- Network problems indicated by VPN drops, route protocol errors, FIB next-hop resolution failures, or interface-level packet errors

Up-to-date automated expertise:

- New checks are released on a monthly basis, updated for new versions, emerging situations, support announcements such as EoS and EoL dates, and other recent developments

Integration Diagram



Before you begin

1. Create a Service Account on each Palo Alto Networks device.
    a. Best practice is to use a dedicated account for auditing and permission purposes.
2. Assign a role to the Service Account.
    a. The Service Account will work best with the Dynamic role of “Superuser (read-only)”.
    b. If tighter controls are required, use the following settings for a Custom role:
        i. WebUI - none. (Disable all)
        ii. XML API - Operational Requests
        iii. Command Line - “devicereader”
3. Full documentation is available at https://indeni.com/docs/user-guide/part-2-getting-started/2-1-adding-user/pan/

Palo Alto Networks Configuration

- Assure that the Indeni server can connect to the Palo Alto device(s) on the following ports:
    - 443: XML-API
    - 22: SSH (CLI)

Partner Product Configuration

1. Create a new Credential Set using the Service Account username(s) and password(s).
    a. Click on the Devices icon in the left menu bar: 
    b. Click on the Credential Sets tab.
    c. Click on the New icon.
    d. Add the Service Account credentials for HTTPS and SSH
        i. In the Credentials panel, click on New.
        ii. Add the Username and Password.
        iii. Select both HTTPS and SSH.
    e. Add the Subnet(s) for the credentials.
        i. The wildcard value to match everything is “0.0.0.0/0”
        ii. Apply to individual hosts with “1.2.3.4/32” (where 1.2.3.4 is the IP address of the management interface)
    f. Full documentation: https://indeni.com/docs/user-guide/part-5-adding-devices/5-1-credential-sets/
2. Add the device.
    a. Click on the Devices icon in the left menu bar: 
    b. Click on the Add new device icon: 
    c. In the Add Device dialog, click the New icon to add a single device, or click the Import icon to upload a list of devices.
    d. Enter the **IP address** for the device and the **name** that will be used for the device in the Indeni UI.
    e. Optional, but recommended: click the **Labels** icon to assign one or more labels to the device, for use in filters or groups elsewhere in the UI.
    f. Click the **Interrogate** button. Indeni will connect to the device with the Credential Set based on the subnet, and will auto-detect the device type, model, and version.
    g. Click the **Save** button.
    h. Full documentation: https://indeni.com/docs/user-guide/part-5-adding-devices/5-2-devices/
3. Indeni automatically starts executing health checks on the new device.

Troubleshooting

- If the device Interrogation fails, full details will be displayed in the dialog panel. The most common issues are failure to connect to port 22 and incorrect credentials.
- Common issues and troubleshooting steps are available here: https://indeni.com/docs/support/
- Support is available at support@Indeni.com or +1-877-778-8991
- Full documentation: https://indeni.com/docs/user-guide/

Technical Details

- Indeni scripts use a combination of XML-API (over https) and CLI commands (over SSH) to query device configuration and state.
- All health checks are available for view on the Indeni Knowledge Explorer: https://community.indeni.com/c/knowledge