Technology Partner Program

Use Case Documentation

Author: AlgoSec

Revision History	
March 2023	Validated the integration on PAN-OS 11.0
September 2022	Validated the integration on PAN-OS 10.1

Table 1: Partner information	
Partner Name	AlgoSec
Website	https://www.algosec.com/
Product Name	AlgoSec Security Management Suite (ASMS)
Partner Contact	Doug Beasley, Director of Business Development doug.beasley@algosec.com Yarin Nahmani, Product Manager yarin.nahmani@algosec.com
Support Contact	support@algosec.com +1-888-358-3697
Product Description	The AlgoSec Security Management Suite (ASMS) empowers organizations to securely accelerate application delivery by automating application connectivity and security policy, anywhere. The AlgoSec platform enables organizations to gain visibility, reduce risk and process changes with zero-touch across the hybrid network. Over 1,800 of the world's leading organizations trust AlgoSec to help secure their most critical workloads across public clouds, private cloud, containers, and on-premise networks.

Use Cases for Integration with Palo Alto Networks

Use Cases

Unified Management for the Hybrid Environment

AlgoSec unifies security policy management across Palo Alto Networks next-generation firewalls deployed on-premise, and virtual appliances deployed on public and private clouds, alongside other network security solutions. AlgoSec provides a single pane of glass through which you can seamlessly manage your entire security policy, including change management, policy provisioning, network visualization, and traffic simulations, policy and risk analysis, auditing, and compliance reporting.

Application Connectivity Management:

AlgoSec automatically discovers and maps application connectivity requirements to the underlying network infrastructure and translates abstract change requests into networking terms that security and operations teams can understand, approve, and implement. With AlgoSec, organizations can accelerate application delivery, minimize outages, and enforce security and compliance across the enterprise network.

Security Policy Change Management:

Using intelligent, highly customizable workflows, AlgoSec automates the entire security policy change process—from planning and design through submission, proactive risk analysis, implementation on the device, validation, and auditing. With AlgoSec you can avoid guesswork and manual errors, reduce risk and enforce compliance.

Firewall Policy Optimization:

AlgoSec provides actionable recommendations to help you clean up and reduce risk across your environment.

o AlgoSec uncovers unused or duplicate rules, initiates a recertification process for expired rules, provides recommendations for how to consolidate or reorder rules for better performance, and tightens overly permissive “ANY” rules —without impacting business requirements.

Firewall Auditing and Compliance:

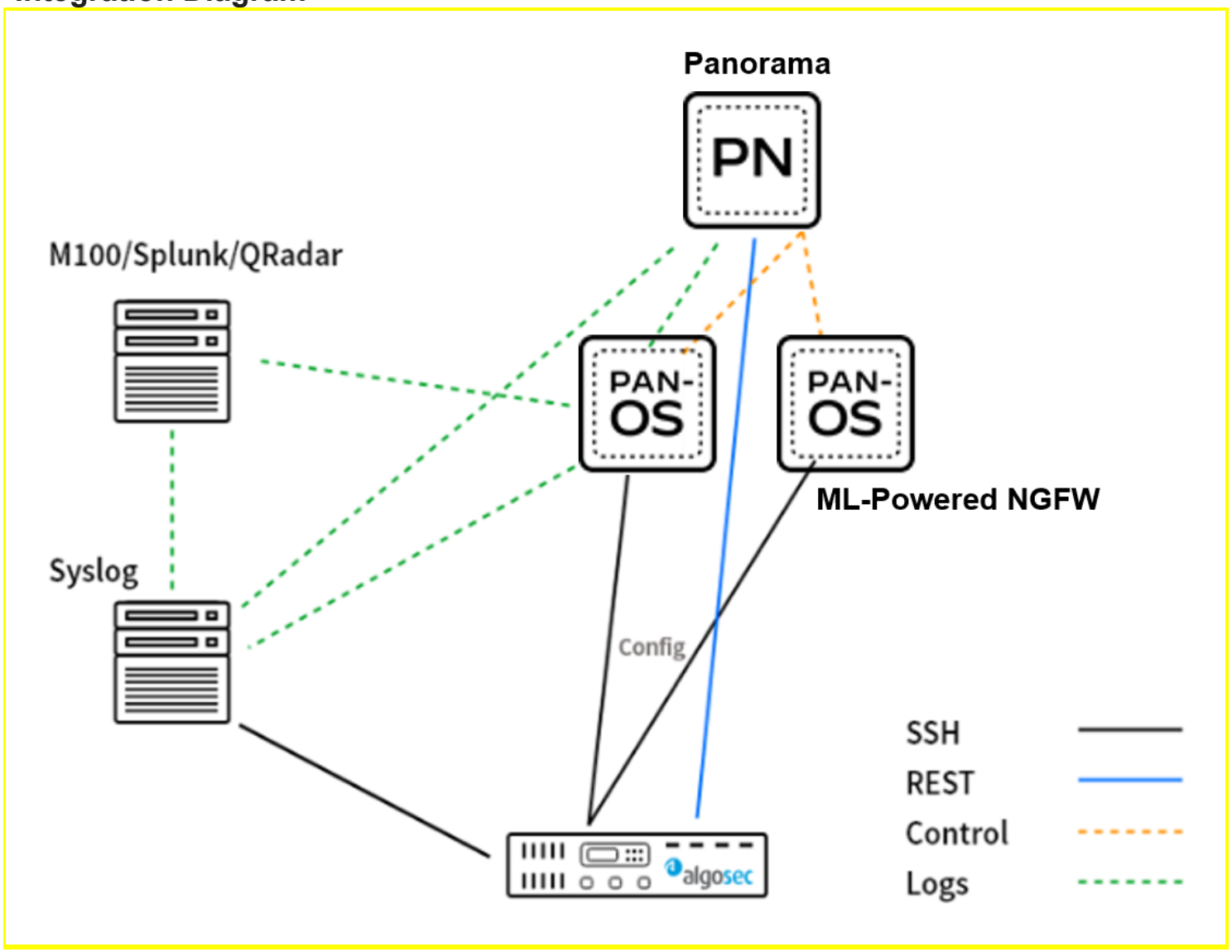
AlgoSec automatically generates pre-populated, audit-ready compliance reports for most industry regulations, as well as customized corporate policies — which help reduce audit preparation efforts and costs by as much as 80%. AlgoSec also uncovers gaps in your compliance posture and proactively checks all changes for compliance violations so you can remediate problems before an audit, and ensure continuous compliance.

Table 2: Palo Alto Networks Products for Integration			
Palo Alto Networks Product	**Integration Status**	**Palo Alto Networks Versions Tested**	**<PARTNER NAME> Versions Tested**
AutoFocus			
Cortex Data Lake			
Cortex XDR			
GlobalProtect			
IoT Security			
Prisma Access			
Prisma Cloud			
Prisma SaaS			
MineMeld			
Next-Generation Firewall	Validated	PAN-OS 10.1.x 10.2.x & 11.0.x	**ASMS A32.10** & above
Panorama	Validated	Panorama 10.1.x, 10.2..x & 11.0.x	**ASMS A32.10** & above
VM-Series	Validated	PAN-OS 10.1.x, 10.2.x & 11.0.x	**ASMS A32.10** & above
WildFire			
Other			

Integration Benefits

- Policy visibility
- Change monitoring
- Manage traffic change requests
- Discover and manage applications flows
- Risk analysis
- Perform policy optimization
- Process an object change request
- Regulatory compliance
- Baseline configuration compliance
- Network connectivity
- Topology visualization
- Traffic simulation

Integration Diagram



AlgoSec products use the following data:

- Policy Rules, Information Objects, NATRules, Routing Data, Traffic Logs, software and hardware configuration, including platform and operating system configurations.
- Data flows are marked in the diagram.
- AlgoSec collects information from Panorama using the REST API.
- AlgoSec collects information from the devices using SSH
- The devices or the M-100 forwards the Traffic logs and the Audit Logs to a Syslog-NG server which are collected by AlgoSec.
- The information is stored on the local AlgoSec server and is used for security and policy management.
- If ***Active Change*** is enabled, AlgoSec deploys changes of rules and objects on the devices

Before You Begin

- If traffic log collection is required (for policy optimization) and the NGFWs don't send the logs to a syslog server (e.g. just send to M-100) the customer needs to configure, so that logs will be forwarded to a standard Syslog-NG server.
- **Requirements for successful integration**:
  - XML API connection from AlgoSec to the Panorama.
  - SSH access from the AlgoSec Server to NGFW devices (when not managed by Panorama or if Baseline Compliance is enabled)
  - **When the NGFWs are managed by Panorama**, forward Traffic Logs and Audit Logs from Panorama or from M-100 to an external syslog server(**recommended**)
  - **When the NGFWs are not managed by Panorama**, forward Traffic and Audit Logs from the NGFW instances to an external syslog server(**recommended**)

Default ports HTTP-REST (TCP/443) and Syslog (UDP/514) for communication.

Optional SSH (TCP/22) for gathering hardware baseline compliance details.

NOTE: AlgoSec supports connection to Panorama or to the NGFWs directly when Panorama is not in use

Requirements for API keys

	User permissions required for most actions (Analysis, monitor, log collection etc.)	**User permissions required for *ActiveChange***
NGFW PA & VM-Series	**User must be one of the following:** **Superuser (read-only)** **Device Admin (read-only)**	
Panorama	**In Admin Role Profile choose in the XML API tab:** **Configuration** **Operational Requests**	**In Admin Role Profile choose in the XML API tab:** **Configuration** **Operational Requests** **Export**

Palo Alto Networks Configuration

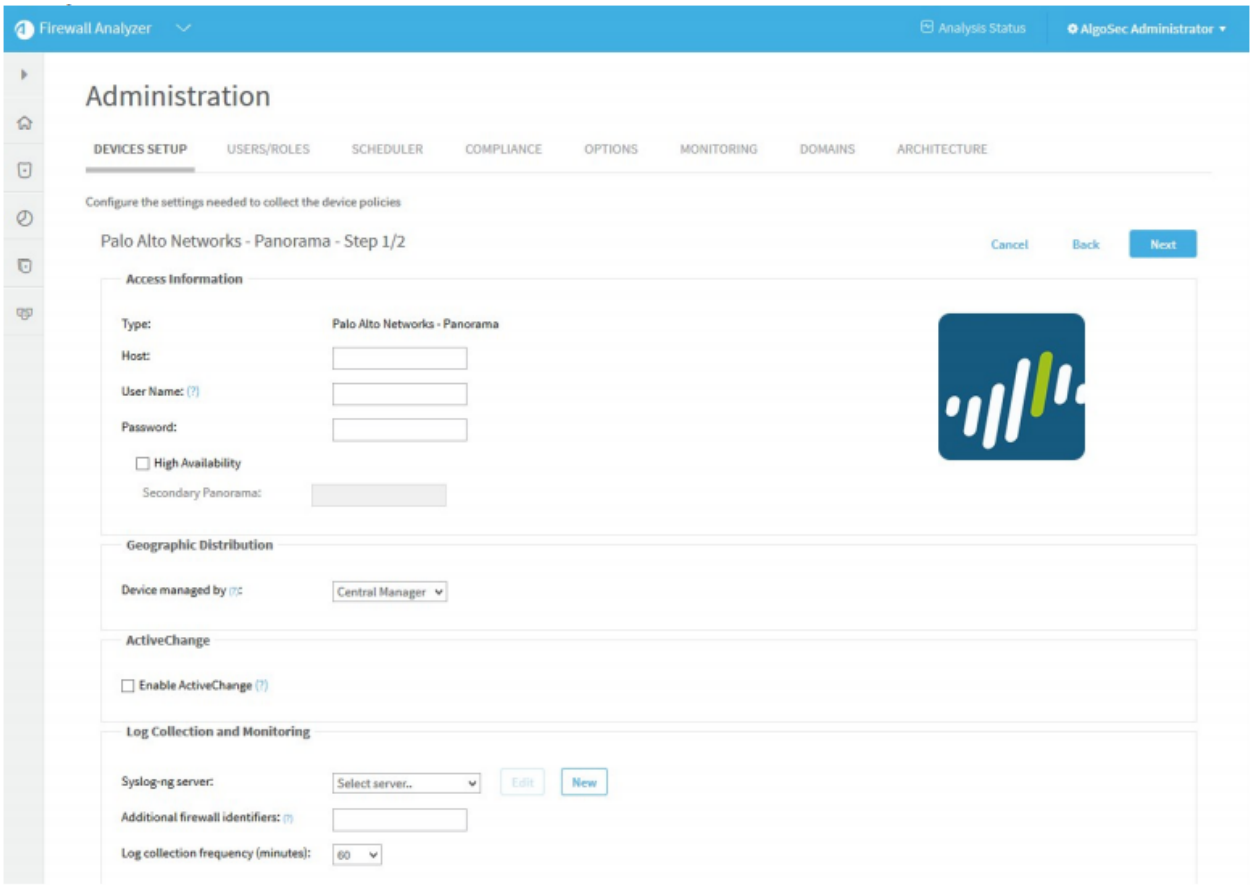
- Create a user with the required permissions for AlgoSec, as shown in the table above.

- Panorama- Set up Administrative Access to Panorama
  - Setting Up Administrative Access to Panorama
- PAN-OS – Manage Firewall Administrators
  - Manage Firewall Administrators
- Configure the system to forward the Traffic Logs and the Audit Logs to the syslog server.
- Panorama – Configure Log Forwarding from Panorama to External Destinations
  - Configure Log Forwarding from Panorama to External Destinations
- PAN-OS – Configure Syslog Monitoring
  - Configure Syslog Monitoring

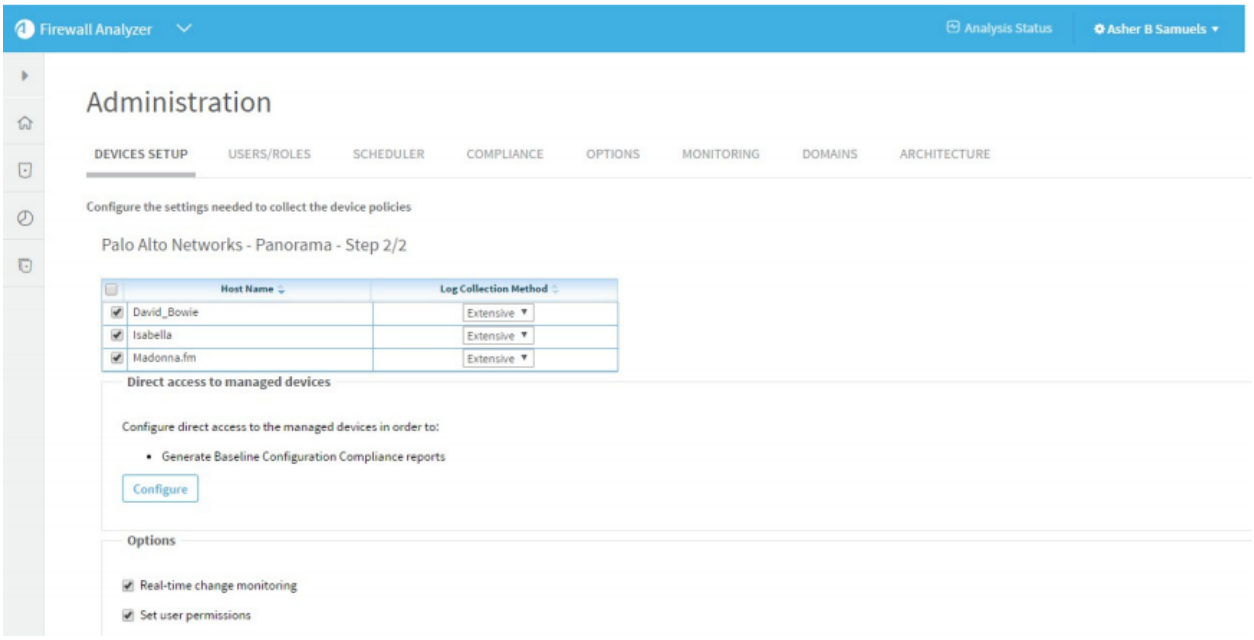
Partner Product Configuration

- See sections "Adding a Palo Alto Networks Panorama" and "Adding a Palo Alto Networks Firewall" in the AlgoSec Administration Guide ASMS Documentation (algosec.com)
- The two screenshots below demonstrate the Palo Alto Networks Panorama configuration dialog boxes:

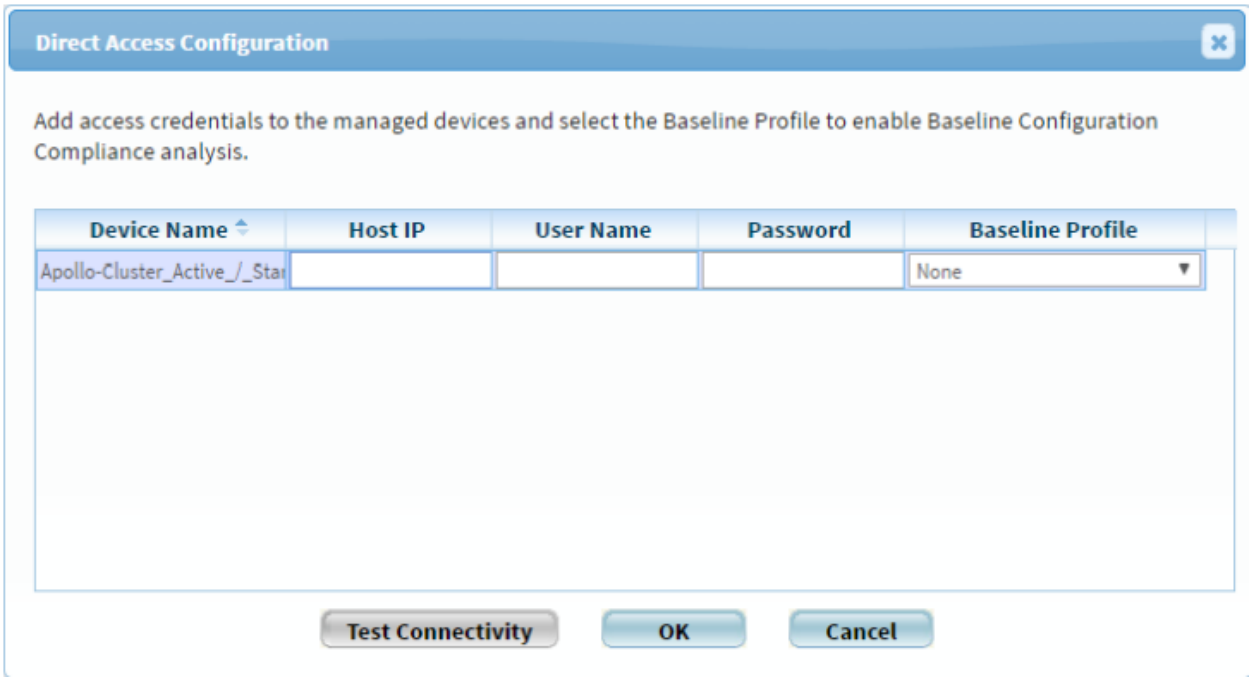
Step 1|2



Step2|2



The screenshot below demonstrates the Palo Alto Networks – direct device access configuration dialog box



Troubleshooting

NOTE: *Use cases that do not match the use case(s) as documented in this integration guide, using a major version of PAN-OS or a major version 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.*

Common troubleshooting steps

AlgoSec:

Common troubleshooting guidance can be found in the AlgoSec Portal:

AlgoSec Portal

Additional troubleshooting can be found in the AlgoPedia:

AlgoPedia

Palo Alto Networks:

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 or Panorama is not EOL: End-of-Life Summary - Palo Alto Networks

Palo Alto Networks 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

Helpful Resources

AlgoSec:

- AlgoSec-and-PAN-WEB.pdf

In case of performance degradation due to API load, caching can be applied. See more details in the following AlgoPedia KB: Performance Fixes for Scaling Palo Alto Networks NGFWs

Palo Alto Networks:

- Palo Alto Networks TechDocs Home
- Registering Panorama and Installing Licenses
- Panorama Administrator's Guide
- Setting Up the Panorama Virtual Appliance
- Everything Panorama
- Panorama Templates
- Templates and Template Stacks
- Managing Templates and Template Stacks
- Palo Alto Networks Solution Offerings: Best Practices
- Changes to Default Behavior in PAN-OS 11.0
- PAN-OS Release Notes - 11.0
- PAN-OS Upgrade Guide
- Creating and Managing Security Policies in PAN-OS
- Data Center Best Practice Security Policy
- Security Policy Best Practices
- Creating Best Practice Security Profiles for the Internet Gateway
- Security Policy Optimizer in PAN-OS
- Platform Support and Licensing for Virtual Systems
- Configure Syslog Monitoring
- Installing a Device Certificate (On Device Not Being Managed by Panorama)
- Subscriptions You Can Use With the NGFW
- End-of-Life Summary - Palo Alto Networks

Contact Information for Support

For AlgoSec specific issues:

- Email: support@algosec.com
- AlgoSec is a TSA Net member

For Palo Alto Networks specific issues:

- Palo Alto Networks Live Community
- Palo Alto Networks Customer Support

Technical Details

AlgoSec uses the PAN-OS XML API:

Get Started with the PAN-OS XML API

Use the CLI to Find XML API Syntax

For the integration with Panorama, AlgoSec uses the following PAN-OS CLI commands:

PAN-OS CLI Quick Start

Operational:

- show config candidate
- show system info
- show config pushed-template
- show routing fib
- show system info panorama
- show panorama dynamic address groups
- show device dynamic address groups
- show devices all
- show connected device
- show dg-hierarchy

Configuration:

- config shared
- config devices groups
- config virtual routers
- show interfaces
- get all vsys
- show predefined

When using ***Active Change*** AlgoSec also uses the following PAN-OS API calls:

Configuration commands:

- Add-rule
  - Device group pre/post:
    - /api/?type=config&action=set&xpath=/config/devices/entry/devicegroup/entry/pre-rulebase/security/rules/entry[@name='24142']
    - /api/?type=config&action=set&xpath=/config/devices/entry/devicegroup/entry/post-rulebase/security/rules/entry[@name='24142']
  - Shared pre/post:
    - /api/?type=config&action=set&xpath=/config/shared/pre-rulebase/security/rules/entry[@name='Test_123']
    - /api/?type=config&action=set&xpath=/config/shared/post-rulebase/security/rules/entry[@name='Test_123']
- Edit-rule:
  - Device group pre/post:
    - /api/?type=config&action=edit&xpath=/config/devices/entry/devicegroup/entry/pre-rulebase/security/rules/entry[@name='24142']
    - /api/?type=config&action=edit&xpath=/config/devices/entry/devicegroup/entry/post-rulebase/security/rules/entry[@name='24142']
  - Shared pre/post:
    - /api/?type=config&action=edit&xpath=/config/shared/pre-rulebase/security/rules/entry[@name='Test_123']
    - /api/?type=config&action=edit&xpath=/config/shared/post-rulebase/security/rules/entry[@name='Test_123']
- Delete-rule:
  - Device group pre/post:
    - /api/?type=config&action=delete&xpath=/config/devices/entry/devicegroup/entry/pre-rulebase/security/rules/entry[@name='24142']
    - /api/?type=config&action=delete&xpath=/config/devices/entry/devicegroup/entry/post-rulebase/security/rules/entry[@name='24142']
  - Shared pre/post:
    - /api/?type=config&action=delete&xpath=/config/shared/pre-rulebase/security/rules/entry[@name='Test_123']
    - /api/?type=config&action=delete&xpath=/config/shared/post-rulebase/security/rules/entry[@name='Test_123']
- Add address object:
  - Device group:
    - /api/?type=config&action=set&xpath=/config/devices/entry/device-group/entry[@name=]/address/entry[@name=]
  - Shared:
    - /api/?type=config&action=set&xpath =/config/shared/address/

      entry[@name=]
- Add service object:
  - Device group:
    - /api/?type=config&action=set&xpath=/config/devices/entry/device-group/entry[@name=]/service/entry[@name=]
  - Shared:
    - /api/?type=config&action=set&xpath=/config/shared/service/

      entry[@name=]

- Add object group(service/address/application):
  - Device group:
    - /api/?type=config&action=set&xpath=/config/devices/entry/devicegroup/entry[@name=]/ service-group/entry[@name=]
  - Shared:
    - /api/?type=config&action=set&xpath=/config/shared/ service-group/ entry[@name=]

Commit commands:

<commit></commit>

<commit><partial><admin><member>" + userName +

"</member></admin></partial></commit>

<commit-all><shared-policy><device-group><entry name='" + deviceGroup +

"'/></device-group></shared-policy></commit-all>

<commit-all><shared-policy><device-group><name>" + deviceGroup +

"</name></device-group></shared-policy></commit-all>

- For the integration with the Palo Alto Networks NGFW, AlgoSec uses the following PAN-OS CLI commands:

Operational:
- show system info
- show routing fib
- show config pushed-template
- show high-availability state
- show config running
- show configpushed-shared-policy
- show config pushed-shared-policy vsys [name]
- show config pushed vsys []name
- show vsys

- Configuration:
  - show predefined

Log types being used:
- In this integration traffic, audit, config, and system logs are being used.