TECHNOLOGY PARTNER PROGRAM

USE CASE DOCUMENTATION

Author: AlgoSec

Contents

Partner Information

Partner information	
Date	August 5th, 2019
Partner Name	AlgoSec
Web Site	www.algosec.com
Product Name	AlgoSec Security Management Suite (ASMS)
Partner Contact	Bruno Weinberger, VP Strategic Alliances bruno.weinberger@algosec.com Yoav Karnibad, Product Manager yoav.karnibad@algosec.com
Support Contact	support@algosec.com +1-888-358-3697
Partner Product for Integration	AlgoSec Security Management Suite (ASMS) Version - 2018.2
Product Description	The AlgoSec suite delivers a complete, integrated solution for managing complex network security policies -- from the business application layer to the network infrastructure. With powerful visibility across virtual, public and hybrid cloud and physical environments, the AlgoSec suite automates and simplifies the entire security change management process to accelerate application delivery while ensuring security and compliance.

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

- **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.

  - 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.

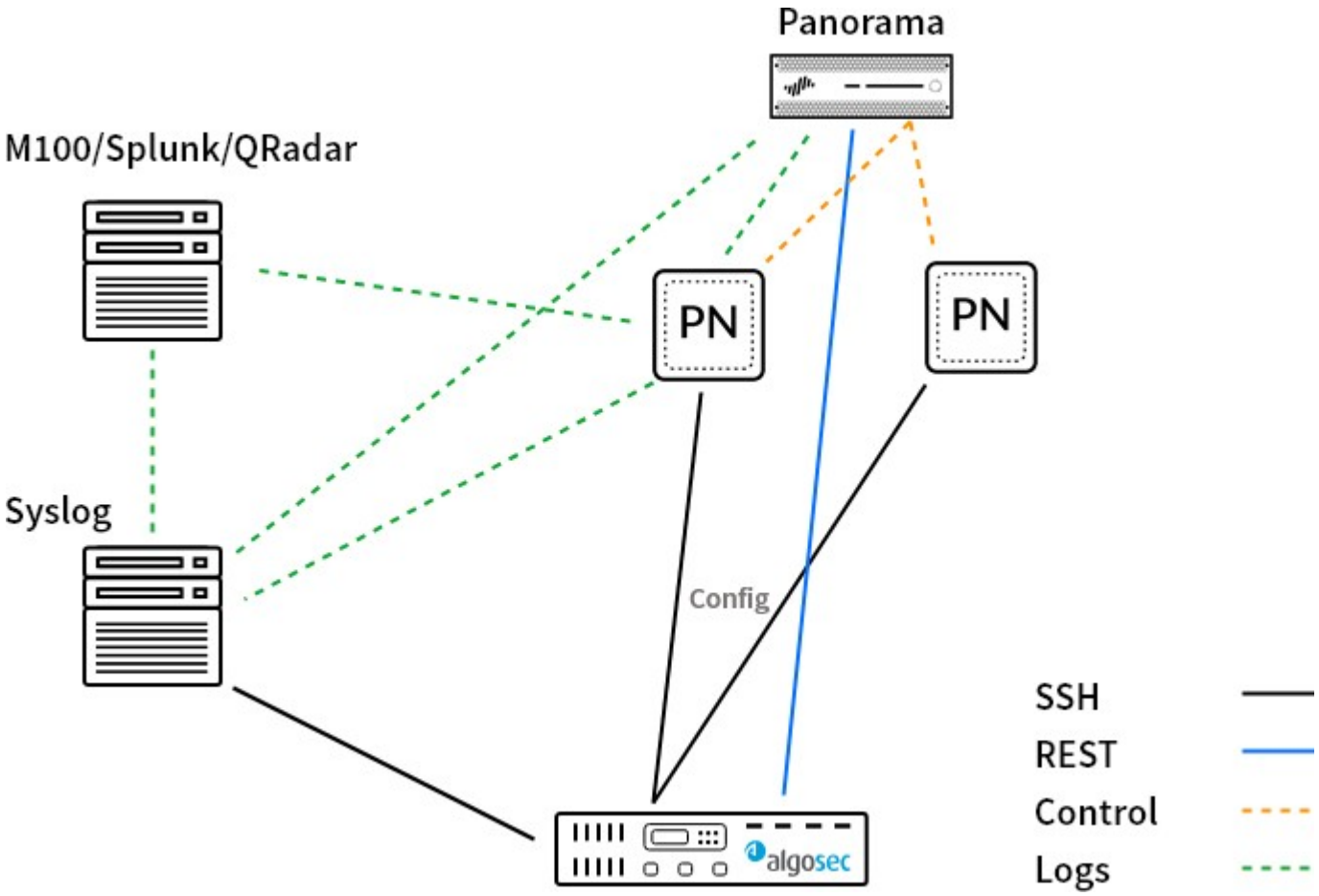
Palo Alto Networks Products for Integration

Palo Alto Networks Product	Integration Status	Palo Alto Networks versions tested	AlgoSec versions tested
AutoFocus			
Cortex XDR			
Cortex XDR Analytics			
MineMeld			
NGFW	Supported	PAN-OS 4.x, 5.x, 6.x, 7.x, 8.x, 9.x	AlgoSec 6.2 (2011) and above
Panorama	Supported	PAN-OS 5.x, 6.x, 7.x, 8.x, 9.x	AlgoSec 6.9 (2015) and above
Prisma Access			
Prisma Public Cloud			
Prisma SaaS			
Traps			
VM-Series	Supported	PAN-OS 7.x, 8.x, 9.x	AlgoSec 2018.1 (2018) and 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



- **Data shared between products:**
  - Policy Rules, Information Objects, NAT Rules, Routing Data, Traffic Logs and software and hardware configuration, including platform and operating system configurations.
  - Data flows are marked in the diagram.
  - AlgoSec collects information from Panorama using REST API.
  - AlgoSec collects information from the devices using SS
  - 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 individual's firewalls don't send their 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 Firewalls are managed by Panorama, forward Traffic Logs and Audit Logs from Panorama or from M-100 to an external syslog server (recommended)
  - When Firewalls are not managed by Panorama, forward Traffic and Audit Logs from NGFW instances to an external syslog server (recommended)
- Note: AlgoSec supports connection to Panorama or to the NGFW 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 & 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.

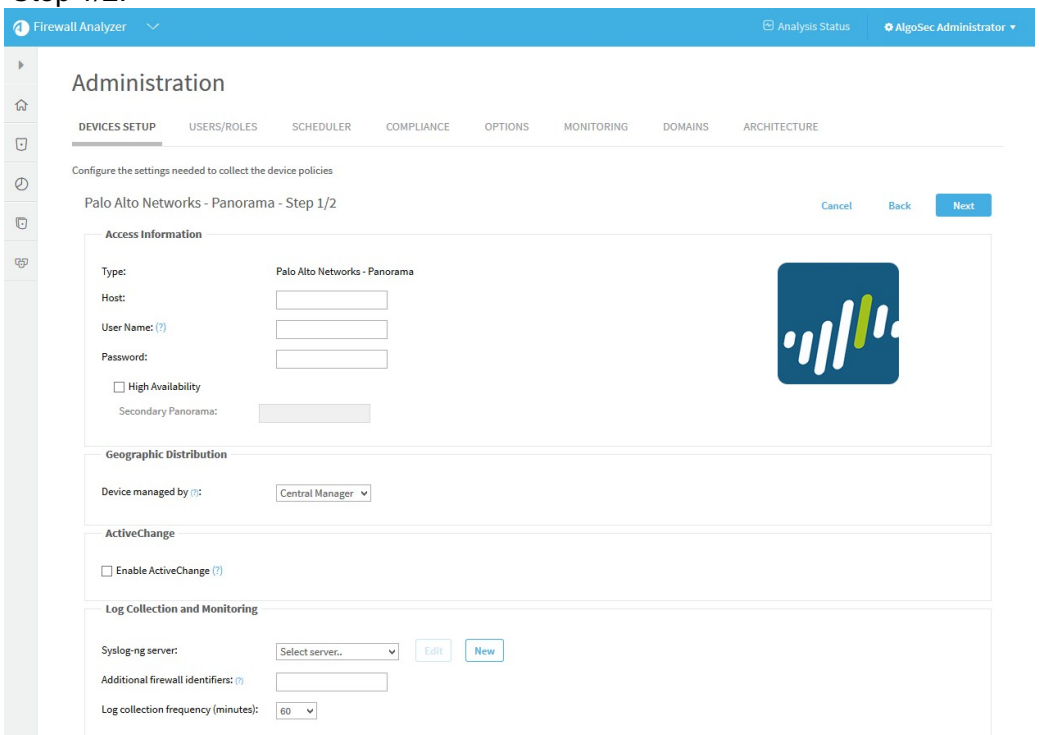
- Create a user with the required permissions for AlgoSec, as shown in the table above.
- Panorama – Set Up Administrative Access to Panorama
  - https://docs.paloaltonetworks.com/panorama/9-0/panorama-admin/set-up-panorama/set-up-administrative-access-to-panorama.html#
- PAN-OS – Manage Firewall Administrators
  - https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/firewall-administration/manage-firewall-administrators.html#

- 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
    - https://docs.paloaltonetworks.com/panorama/9-0/panorama-admin/manage-log-collection/configure-log-forwarding-from-panorama-to-external-destinations.html#
- PAN-OS – Configure Syslog Monitoring
    https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/monitoring/use-syslog-for-monitoring/configure-syslog-monitoring#

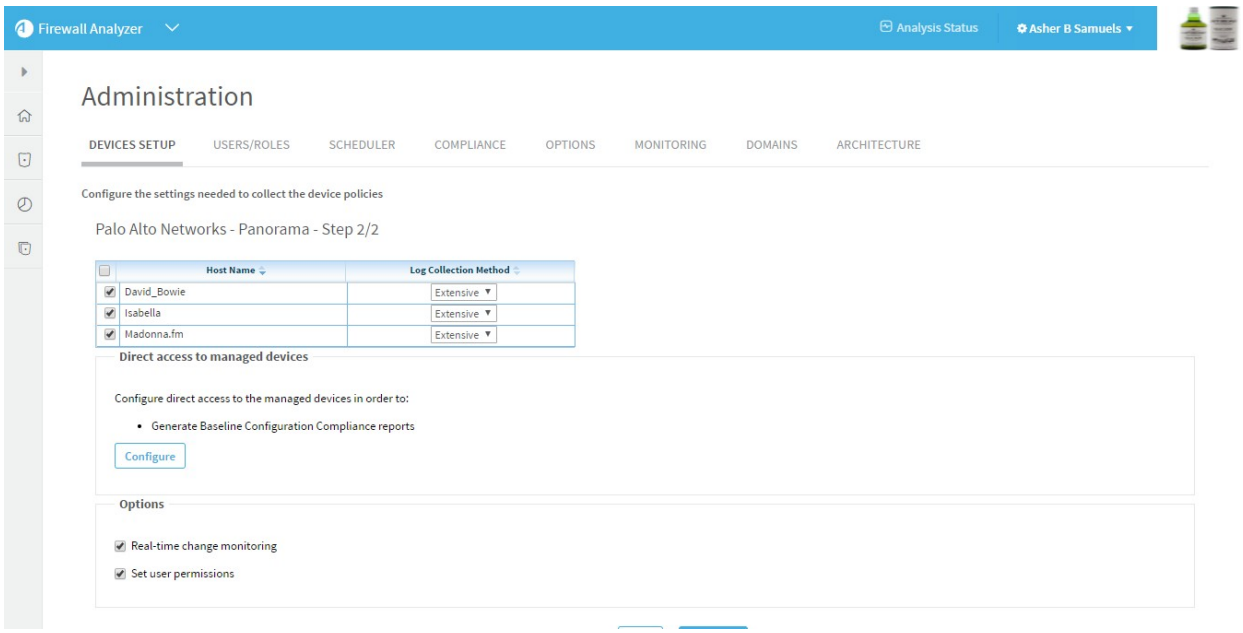
Partner Product Configuration

- See sections "Adding a Palo Alto Networks Panorama" and "Adding a Palo Alto Networks Firewall" in the AlgoSec Administration Guide: Firewall Analyzer v2018.2 Administrator Guide (https://portal.algosec.com/en/documentation/release_notes)
- The two screenshots below demonstrate the Palo Alto Networks – Panorama configuration dialog boxes.

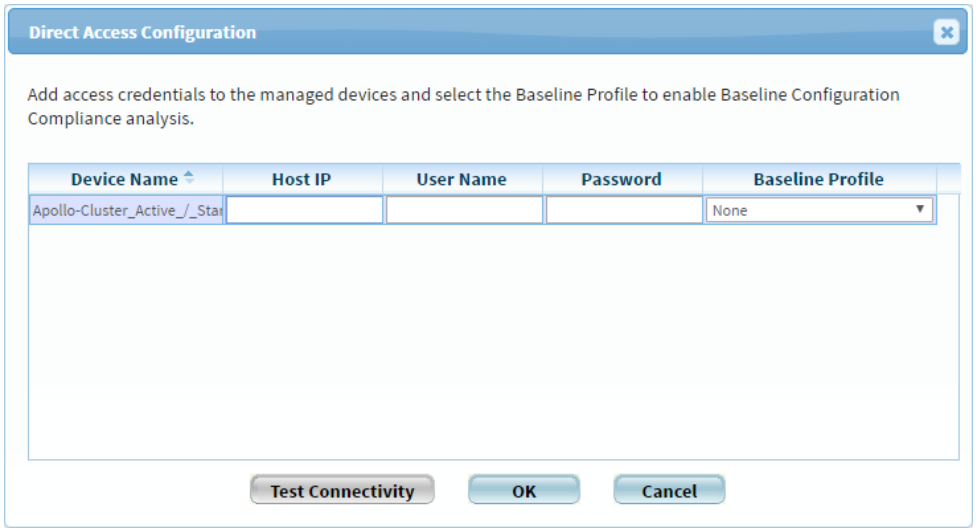
- Step 1/2:



Step 2/2:



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



Troubleshooting

- Common troubleshooting guidance can be found in the AlgoSec Portal:
  - https://portal.algosec.com/en/training_academy/online_courses#pTab-5
- Additional troubleshooting can be found in the AlgoPedia:
  - https://knowledge.algosec.com
- Contact information for support
  - support@algosec.com
- AlgoSec is a TSA Net member
- Helpful Resources:
  - *https://www.algosec.com/wp-content/uploads/2016/03/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: https://knowledge.algosec.com/skn/c6/AlgoPedia/e16068/Performance_Fixes_for_Scaling_Palo_Alto_Panorama_Firewalls_with_ASMS

Technical Details

- AlgoSec uses the XML API
- **For the integration with Panorama AlgoSec uses the following API calls:**

  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 uses also the following API calls:**

  Configuration commands:
  - Add-rule:

        - Device group pre/post:
            - /api/?type=config&action=set&xpath=/config/devices/entry/device-group/entry/pre-rulebase/security/rules/entry[@name='24142']
            - /api/?type=config&action=set&xpath=/config/devices/entry/device-group/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/device-group/entry/pre-rulebase/security/rules/entry[@name='24142']
            - /api/?type=config&action=edit&xpath=/config/devices/entry/device-group/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/device-group/entry/pre-rulebase/security/rules/entry[@name='24142']
            - /api/?type=config&action=delete&xpath=/config/devices/entry/device-group/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/device-group/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 a direct integration with the firewalls, AlgoSec uses the following API calls:**
    - Operational:
        - show system info
        - show routing fib
        - show config pushed-template
        - show high-availability state
        - show config running
        - show config pushed-shared-policy
        - show config pushed-shared-policy vsys [name]
        - show config pushed vsys []name
        - show vsys
    - Configuration:
        - show predefined
- **Log types being used:**
    - In the integration Traffic logs and Audit logs (Config & System logs) are used.