Technology Partner Program Integration Guide

Author: Nozomi Networks

Revision History	
July 9, 2020	Validation of PAN-OS 8.1.0, 9.0.0, and 9.1.0. Added the Session Kill feature in Guardian to automatically terminate active sessions in the NGFW state table upon detecting anomalous behavior
August 25, 2020	Added more detail around API requests.

Partner Information	
Date	July 9, 2020
Partner Name	Nozomi Networks
Website	www.nozominetworks.com
Product Name	Guardian v20.0.1
Partner Contact	Phil Page Sales Engineering Manager – Partner Alliances Mobile: +1-443-534-7553 phillip.page@nozominetworks.com
Support Contact	support@nozominetworks.com
Product Description	Continuous monitoring anomaly-based IDS for Industrial Control Systems networks.

Palo Alto Networks Products for Integration

Table 1: Integration Details by Product			
Palo Alto Networks Product	Integration Status	Palo Alto Networks Versions Tested	Nozomi Networks Versions Tested
AutoFocus			
Cortex XDR Prevent			
Cortex XDR Pro			
Next-Generation Firewall	Validated	8.1.0 , 9.0.0, 9.1.0	17.1 – 20.0.1
Panorama			
Prisma Access			
Prisma Cloud Compute			
Prisma Cloud Enterprise			
Prisma SaaS			
VM-Series			
WildFire			
Other			

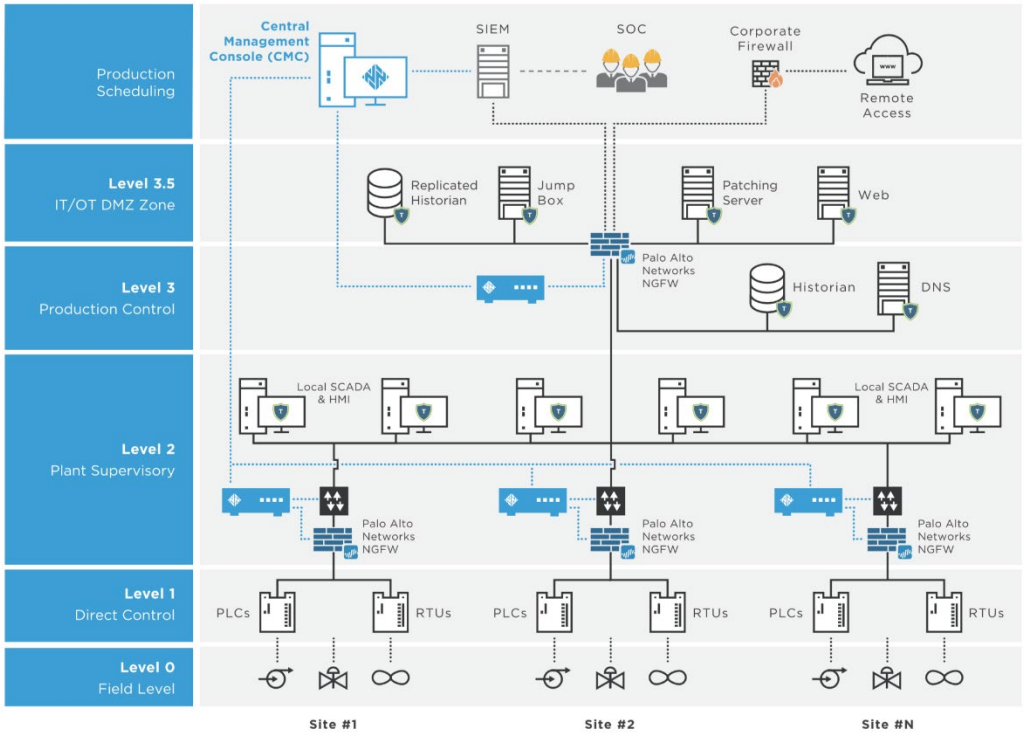
Use Cases for Integration with the Palo Alto Networks Security Operating Platform

- ACL modification
- Node Blocking: Upon detecting a new, previously unseen device on the network, Guardian instantiates a layer 3 ACL modification in the Palo Alto Networks Next-Generation Firewall (NGFW) to block any connections to or from that endpoint
- Link Blocking: Upon detecting a new, previously unseen connection (layer 3, 4, or 7) between two devices, Guardian instantiates a layer 4 ACL modification on the NGFW to block any connections between those devices on the detected source and destination address and destination port
- Session Kill: For PAN-OS 9.0 and 9.1, upon detecting a new, previously unseen session between two devices, Guardian sends an event to NGFW via the PAN-OS API to terminate any sessions between those devices based on the detected source and destination address and destination port and protocol

Integration Benefits

- Allows the customer to dynamically react to threats detected in their environment
- Bridges the “passive monitoring” and “active containment” approaches afforded by both Guardian and PANW NGFW

Integration Diagram



Before You Begin

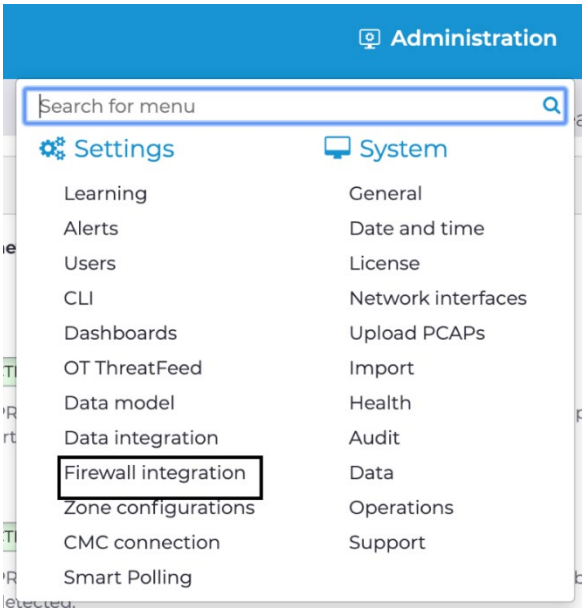
- Make sure the management interface of your Guardian appliance has connectivity to the NGFW management interface over TCP port 443 (TLS)

Palo Alto Networks Configuration

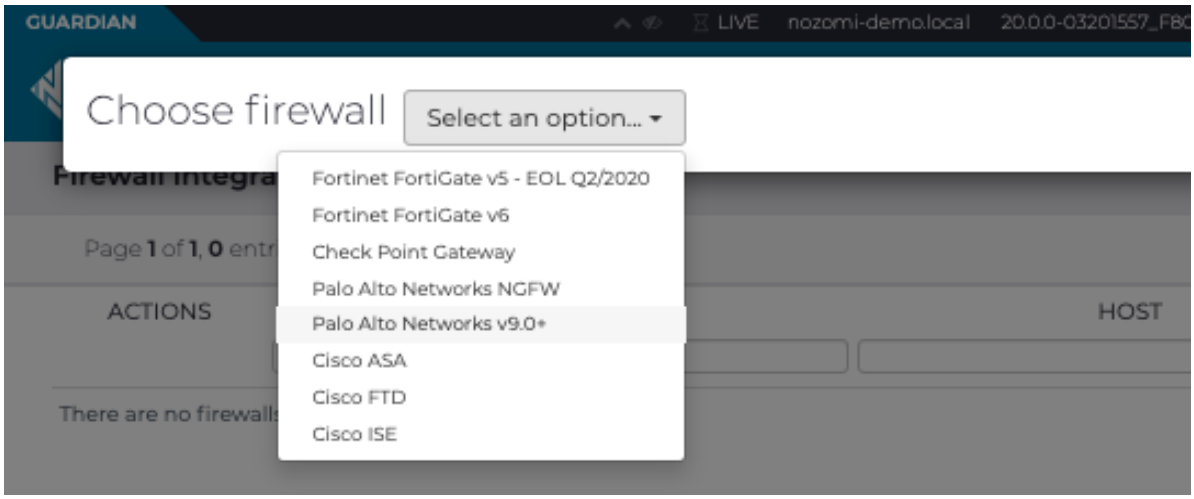
- Create a user with an admin role profile with XML or REST API permissions to modify the following:
  - Log
  - Configuration
  - Commit

Partner Product Configuration

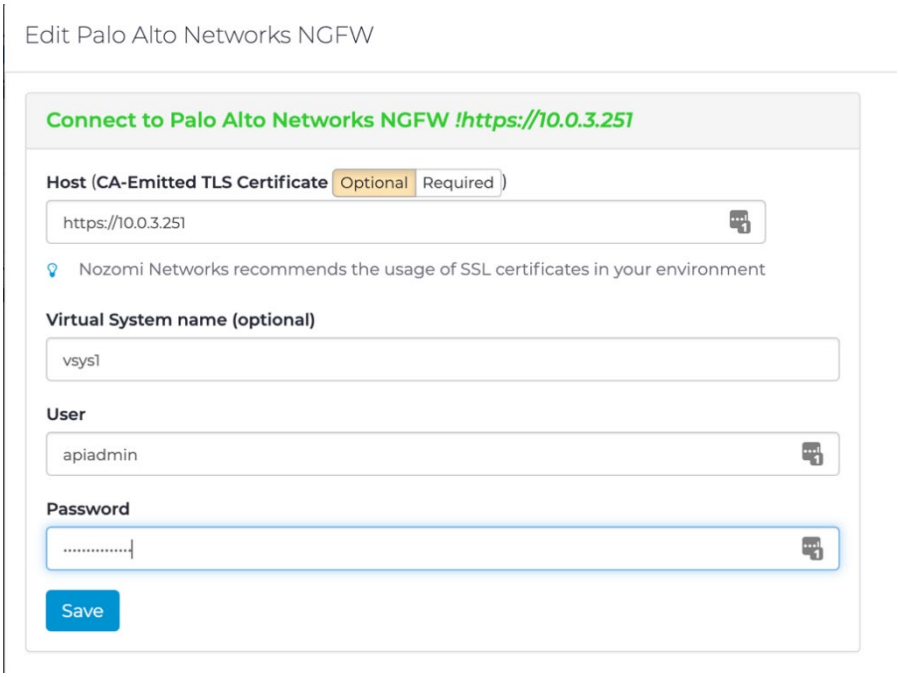
- Ensure your Guardian is fully licensed and configured for management access
- Log in with an admin user
- Go to Administration -> Firewall Integration



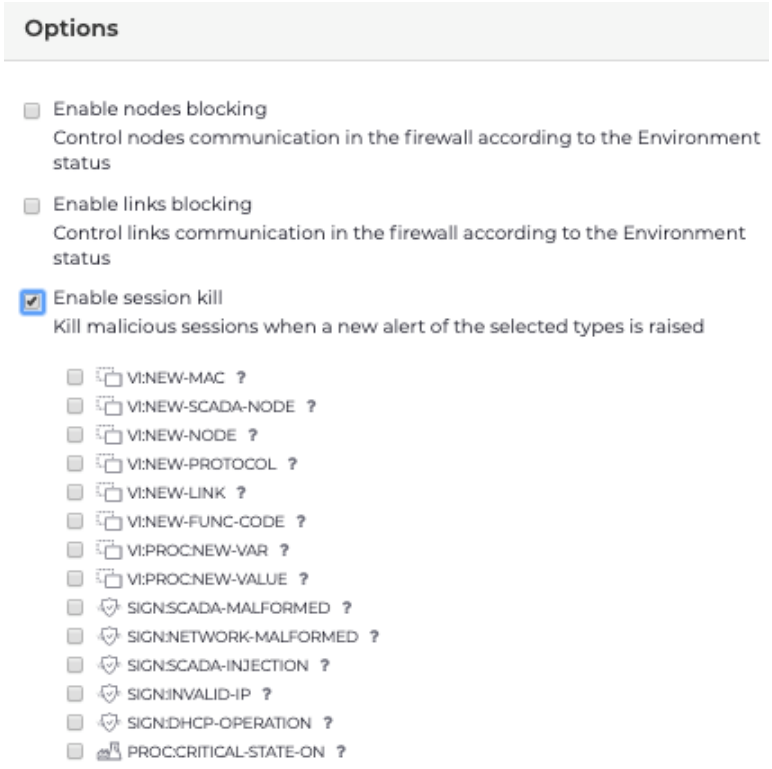
- Click the + in the top right corner to add a new Firewall. Select "Palo Alto NGFW" or Palo Alto Networks v90+ from the dropdown menu.



- Enter the hostname/IP, vsys (if applicable), username, and password. Note: if your PA-NGFW and Guardian are not configured with CA-signed certificates, select "Optional" for "CA-Emitted TLS Certificate").



- Click “Optional” to use a self-signed certificate
- On the right-hand side of the window, select the actions you want to take including which alert types you want terminate sessions for via Session Kill:



- Click “save”

Troubleshooting

- Verify connectivity is permitted from Guardian to the NGFW management interface over TCP port 443
- Ensure proper API user permissions on NGFW
- Verify n2osids process is running (from the CLI: "service n2osids restart")
- If using signed certificates, ensure both certificates are valid and trust the same CA
- Ensure time is synchronized on both Guardian and the NGFW
- Note that NGFW generates a new random Session ID for each session so only the first session will be killed even if you place a persistent kill command in the Nozomi configuration file
- Contact support@nozominetworks.com for further support (requires an active support contract)

Technical Details – REST API Requests

- keygen
  https://<ip>/api/?password=nozominetworks1&user=admin&type=keygen
- Show active sessions
  https://<ip>/api/?type=op&cmd=<show><session><all><filter></filter></all></session></show>&key=<key>
- Apply show session filter
  https://<ip>/api/?type=op&cmd=<show><session><all><filter><destination-port>53</destination-port></filter></all></session></show>&key=<key>
- Clear session by id
  https://<ip>/api/?type=op&cmd=<clear><session><id>15627</id></session></clear>&key=<key>
- Get Objects Tags
  https://<ip>/restapi/9.0/Objects/Tags?key=<key>&name=n2os-bn-tag-from&location=vsys&vsys=vsys1
- get Objects AddressGroup
  https://<ip>/restapi/9.0/Objects/AddressGroups?key=<key>&location=vsys&vsys=vsys1
- delete Objects AddressGroup
  https://<ip>/restapi/9.0/Objects/AddressGroups?key=<key>&name=ag1&location=vsys&vsys=vsys1
- delete Objects Address
  https://<ip>/restapi/9.0/Objects/Address?key=<key>&name=ag1&location=vsys&vsys=vsys1
- add Objects AddressGroup
  https://<ip>/restapi/9.0/Objects/AddressGroups?key=<key>&name=name&location=vsys&vsys=vsys1
- add Objects Address
  https://<ip>/restapi/9.0/Objects/Address?key=<key>&name=name&location=vsys&vsys=vsys1
- Get Objects Address
  https://<ip>/restapi/9.0/Objects/Address?key=<key>&name=name&location=vsys&vsys=vsys1
- get Objects Services
  https://<ip>/restapi/9.0/Objects/Services?key=<key>&name=name&location=vsys&vsys=vsys1
- add Objects Services
  https://<ip>/restapi/9.0/Objects/Services?key=<key>&name=service_name&location=vsys&vsys=vsys1
- add Objects ServicesGroups
  https://<ip>/restapi/9.0/Objects/Services?key=<key>&name=service_name&location=vsys&vsys=vsys1
- update Objects ServicesGroups
  https://<ip>/restapi/9.0/Objects/ServiceGroups?key=<key>&name=service_group_name&location=vsys&vsys=vsys1
- get Objects ServicesGroups
  https://<ip>/restapi/9.0/Objects/ServiceGroups?key=<key>&name=service_group_name&location=vsys&vsys=vsys1

- get Objects Services
  https://<ip>/restapi/9.0/Objects/Service?key=<key>&name=service_group_name&location=vsys&vsys=vsys1
- update Objects AddressGroup
  https://<ip>/restapi/9.0/Objects/AddressGroups?key=<key>&name=name&location=vsys&vsys=vsys1
- update Objects Address
  https://<ip>/restapi/9.0/Objects/Address?key=<key>&name=name&location=vsys&vsys=vsys1
- add Objects Tags
  https://<ip>/restapi/9.0/Objects/Tags?key=<key>&name=n2os-bn-tag-from&location=vsys&vsys=vsys1
- delete Objects Tags
  https://<ip>/restapi/9.0/Objects/Tags?key=<key>&name=n2os-bn-tag-from&location=vsys&vsys=vsys1
- add Rule
  https://<ip>/restapi/9.0/Objects/Policies/SecurityRules?key=<key>&location=vsys&vsys=vsys1&name=rule_name
- update Rule
  https://<ip>/restapi/9.0/Objects/Policies/SecurityRules?key=<key>&location=vsys&vsys=vsys1&name=rule_name
- delete Rule
  https://<ip>/restapi/9.0/Objects/Policies/SecurityRules?key=<key>&location=vsys&vsys=vsys1&name=rule_name
- move Rule on top
  https://<ip>/restapi/9.0/Objects/Policies/SecurityRules?key=<key>&location=vsys&vsys=vsys1&name=rule_name&where=top&action=move
- Commit/partial/admin/member
  https://<ip>/api/?type=commit&cmd=<commit><partial><admin><member></member></admin></partial></commit>