TECHNOLOGY PARTNER PROGRAM

USE CASE DOCUMENTATION

Author: Claroty

Contents

Partner Information

Partner information	
Date	January 9, 2020
Partner Name	Claroty
Web Site	http://www.claroty.com
Product Name	NGFW
Partner Contact	Lior Hammer Director, Product Management lior.h@claroty.com
Support Contact	Subjected to agreed SLA support@claroty.com or contact@claroty.com
Partner Product for Integration	Continuous Threat Detection (CTD)
Product Description	Claroty is an IT-OT-IoT product designed expressly to provide IT/SOC and even OT security personnel with extreme visibility into the OT environment. It passively monitors OT network and asset traffic, and delivers deep visibility, threat detection and alerts for earliest detection and resolution. With Palo Alto, our integration with NGFW and Panorama provides perimeter and policy support, even to the point of suggesting policy and configuration changes to the firewall when recommended given what's happening in the OT network. Unique to Palo Alto, Claroty can specify applications in use by AppID, helping responders figure out which specific application and protocols are in use and what to do when issues arise.

Palo Alto Networks Products for Integration

Palo Alto Networks Product	Integration Status	Palo Alto Networks versions supported	Claroty versions supported
AutoFocus			
Cortex XDR			
Cortex XDR Analytics			
Demisto			
GlobalProtect			
MineMeld			
NGFW	Validated	PAN-OS 8.0, PAN-OS 9.0	3.2 or above
Panorama	Validated	PAN-OS 8.0, PAN-OS 9.0	3.2 or above
Prisma Access			
Prisma Cloud			
Prisma Cloud Compute Edition			
Prisma SaaS			
Traps			

VM-Series			
Wildfire			
Other			

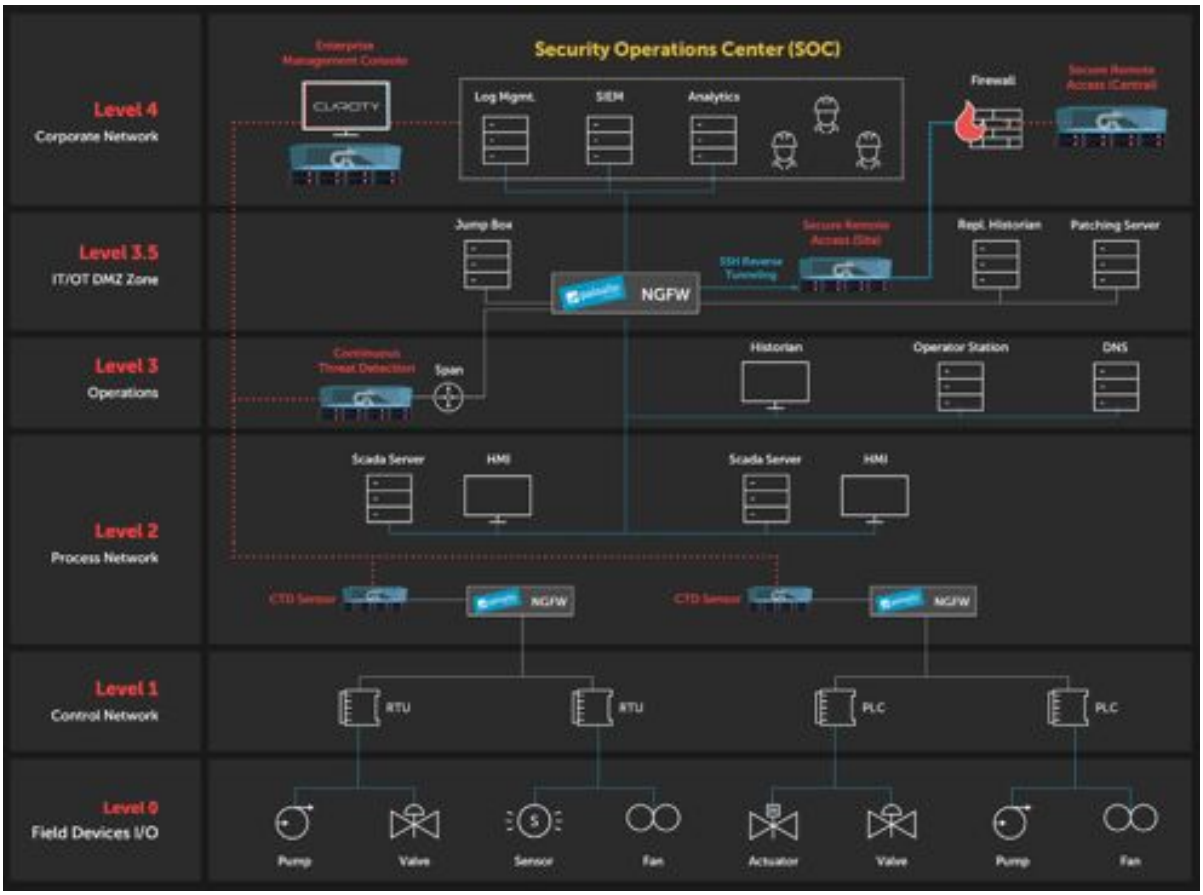
Use cases for integration into Palo Alto Networks Next Generation Security Operating Platform

- New asset discovery - assets discovered by CTD are automatically synced into Palo Alto Networks NGFW platform.
- Network Segmentation - Virtual zones segmentation for OT networks - as analyzed by CTD are synced into Palo Alto Networks Platform and created as security groups, enabling creation and enforcement of security policies based on Claroty's discovery and segmentation capabilities.
- Existing and new assets (all assets discovered by CTD) are in a 'security group' defined by their 'virtual zone' in CTD.
- New security policies with OT relevant applications in use (**AppIDs)** are synced into Palo Alto Networks Platform, where granular policies for OT networks are enforced.

Integration Benefits

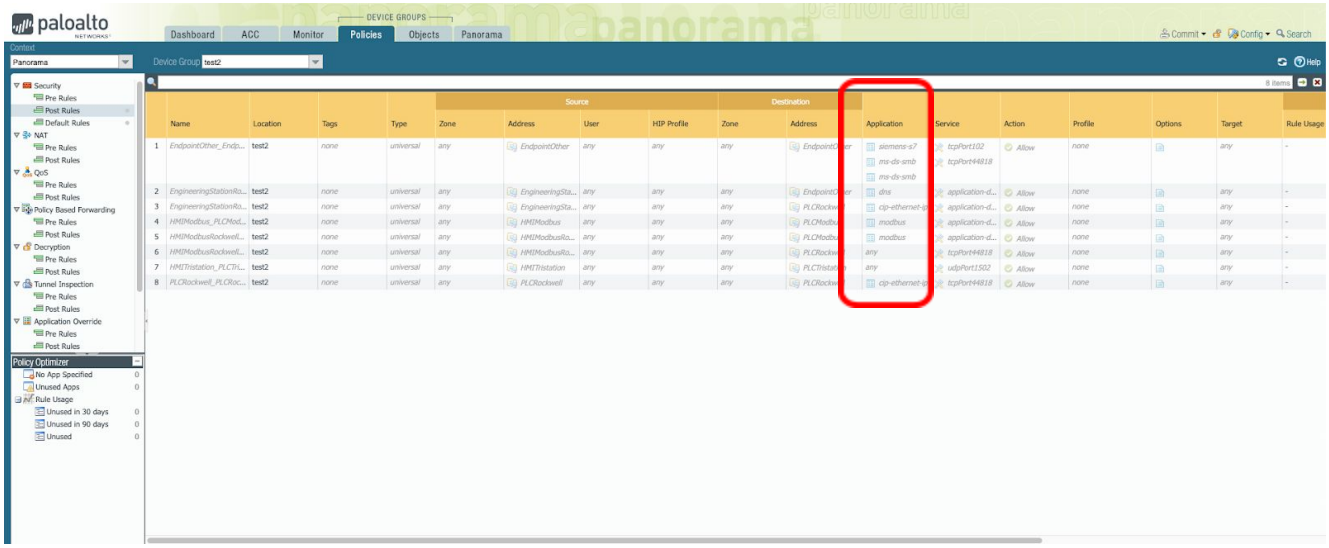
- Extreme Visibility of industrial control system networks allows critical infrastructure organizations to assess, monitor and mitigate potential threats
- Accelerated Incident Response capabilities with automated detection and blocking actions to cyber threats
- Improved Threat Hunting via real-time contextual alerting and immediate implications on process integrity and cyber resiliency

Integration Diagram



Palo Alto Networks NGFW asset data and policy are being determined by Claroty's CTD server by pushing data into Palo Alto Networks NGFW using its designated set of XML API's.

Data from CTD is shared in a way which creates new object and policies in Palo Alto Networks platform that enables both visibility of OT assets, and enforcement of security policies derived from CTD segmentation features. The security policies in the screen below also shows APPIDs which map to relevant OT protocols and applications for the concerned traffic. This visibility gives SOCs and security personnel granular policy control, and potentially a faster way to find and resolve when applications are in use that violate policy or need refinement.



Sample OT-Specific AppIDs that may be in use *(not a full list of what may be detected)*

Protocol / Application	Protocol / Application	Protocol / Application	Protocol / Application
DNP3	Modbus	Siemens S7	ABB Network Manager
IEC 60870-5-104	CIP EtherNet IP	Siemens FactoryLink	Schneider OaSys
ICCP (IEC 60870-6 / TASE.2)	BACnet	Siemens Profinet IO	Rockwell FactoryTalk
Synchrophasor (IEEE C.37.118)	Foundation Fieldbus	OPC UA	GE iFIX
Elcom 90	MQTT	Matrikon OPC Tunneller	GE EGD
DLMS / COSEM / IEC 62056	RTCM (GPS/IP)	OSIsoft PI Systems	Cygnet SCADA

Before you begin

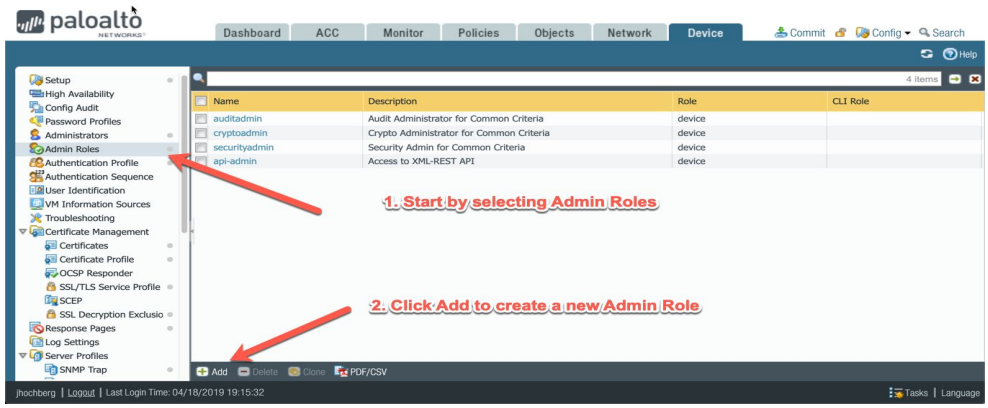
- Make sure CTD Server is of version 3.2 or above
- Make sure Panorama or PAN-OS version 8 or above
- Make sure you have admin credentials for PAN-OS /Panorama with API access.

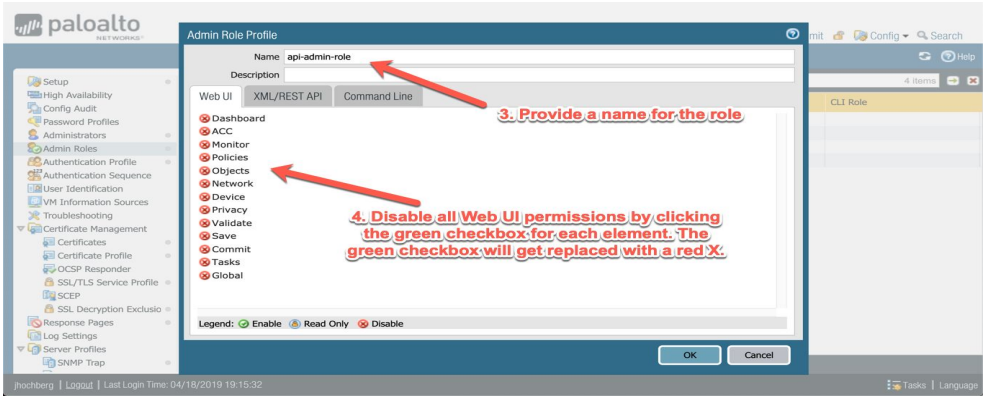
Palo Alto Networks Configuration

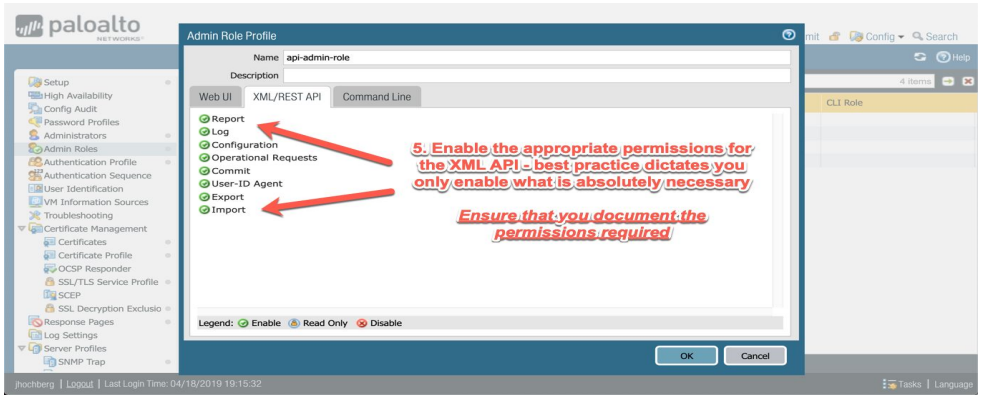
- As a best practice, set up a separate admin account for XML API access to NGFW or Panorama, following the steps here:-

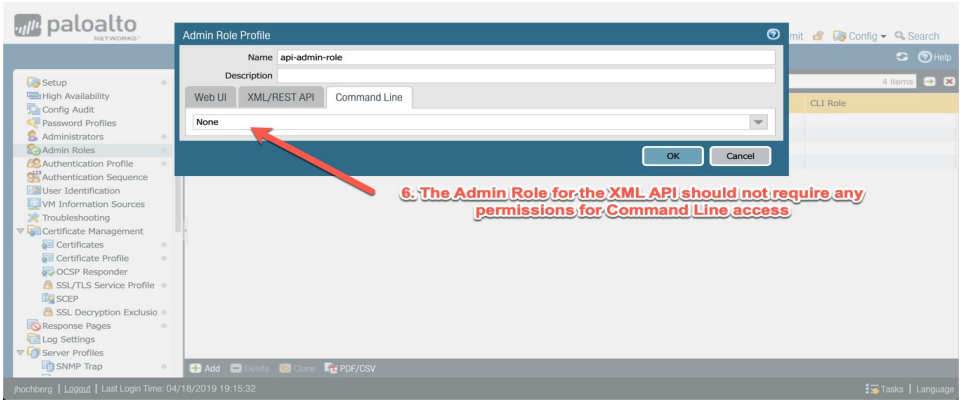
https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-panorama-api/get-started-with-the-pan-os-xml-api/enable-api-access.html

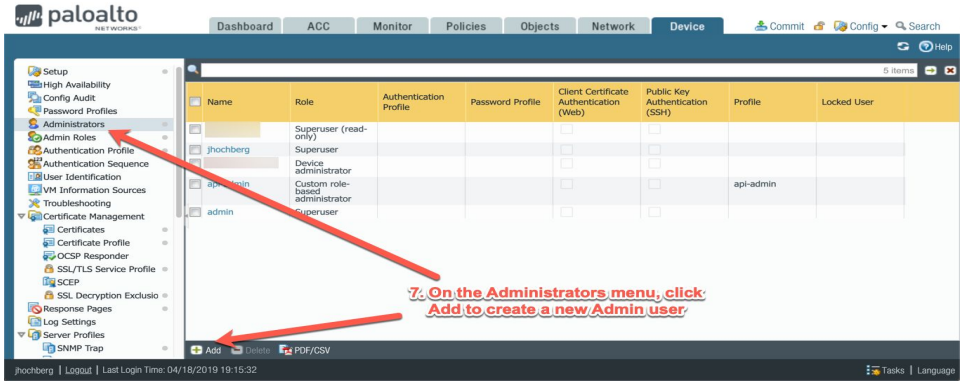
Below is an example of these steps for the NGFW.

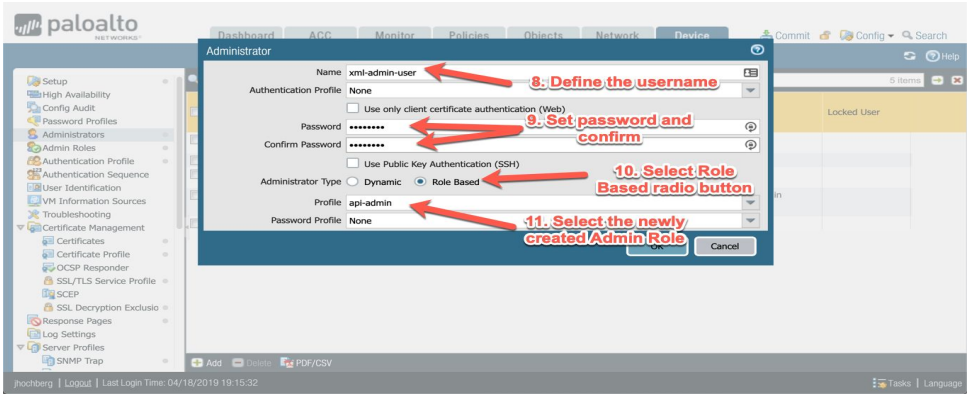

Dashboard
ACC
Monitor
Policies
Objects
Network
Device
Commit
Config
Search
Help
Setup
High Availability
Config Audit
Password Profiles
Administrators
Admin Roles
Authentication Profile
Authentication Sequence
User Identification
VM Information Sources
Troubleshooting
Certificate Management
Certificates
Certificate Profile
OCSP Responder
SSL/TLS Service Profile
SCEP
SSL Decryption Exclusio
Response Pages
Log Settings
Server Profiles
SNMP Trap
4 items
Name
Description
Role
CLI Role
auditadmin
Audit Administrator for Common Criteria
device
cryptoadmin
Crypto Administrator for Common Criteria
device
securityadmin
Security Admin for Common Criteria
device
api-admin
Access to XML-REST API
device
1. Start by selecting Admin Roles
2. Click Add to create a new Admin Role
Add
Delete
Clone
PDF/CSV
jhochberg | Logout | Last Login Time: 04/18/2019 19:15:32
Tasks | Language


Admin Role Profile
Name
api-admin-role
Description
Web UI
XML/REST API
Command Line
3. Provide a name for the role
Dashboard
ACC
Monitor
Policies
Objects
Network
Device
Privacy
Validate
Save
Commit
Tasks
Global
4. Disable all Web UI permissions by clicking the green checkbox for each element. The green checkbox will get replaced with a red X.
Legend: Enable Read Only Disable
OK
Cancel


Admin Role Profile
Name
api-admin-role
Description
Web UI
XML/REST API
Command Line
Report
Log
Configuration
Operational Requests
Commit
User-ID Agent
Export
Import
5. Enable the appropriate permissions for the XML API - best practice dictates you only enable what is absolutely necessary
Ensure that you document the permissions required
Legend: Enable Read Only Disable
OK
Cancel


Admin Role Profile
Name
api-admin-role
Description
Web UI
XML/REST API
Command Line
None
OK
Cancel
6. The Admin Role for the XML API should not require any permissions for Command Line access
Add
Delete
Clone
PDF/CSV



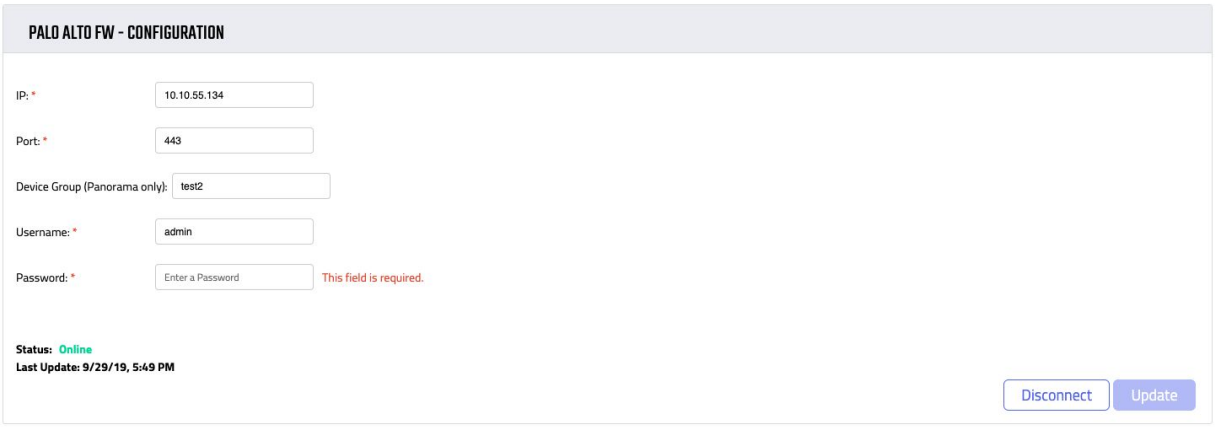


Record the login credentials of admin user for CTD Integration Configuration

Partner Product Configuration

After logging in into CTD administration, open configuration panel through the menu on the left pane. Select Integrations, Palo Alto FW, and enter the IP, Port, Username and Password of the desired device, and click on Connect.

Note: If integration is done with *Panorama,* a device group must be set.



Once connected, virtual zones and policies are automatically synced every 5 minutes.

To stop automatic sync, select “Disconnect” on CTD’s Palo Alto FW integration page.

When the system is properly configured, it will show a green “Online” status at the bottom part of the configuration pane.

Troubleshooting

Please refer to the Claroty CTD Administrator Guide and User Guide for further assistance and troubleshooting. Reference: https://www.claroty.com/continuous-threat-detection

- For further assistance please contact support@claroty.com or contact@claroty.com

Technical Details

CTD communicates with Palo Alto Networks NGFW using the PAN-OS XML-API interface.