TECHNOLOGY PARTNER PROGRAM

USE CASE DOCUMENTATION

Author: AttackIQ

Contents

Partner Information

Partner information	
Date	August 30, 2019
Partner Name	AttackIQ
Web Site	www.AttackIQ.com
Product Name	AttackIQ Platform
Partner Contact	Andrea Swaney, andrea.swaney@attackiq.com, 973.580.6602
Support Contact	support@attackiq.com
Partner Product for Integration	AttackIQ Platform
Product Description	AttackIQ's distributed agent-cloud architecture launches real attacker behaviors on production systems – without impacting them -- to determine how effectively controls are working and configured.

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

- **Use case: Validate and Optimize Firewall Configuration**
  This use case is based on a scenario where you are using Panorama to manage multiple firewalls in your network.
- **How to Validate**: AttackIQ enables you to validate the configuration of each firewall across multiple network segments by emulating adversarial behavior, exercising each firewall against an assumed configuration policy you set within Panorama. This ensures you have consistent enforcement of policies across your firewalls.

  An example of this is the use of MITRE ATT&CK Framework, enabling you to select specific assessments that can be run to exercise your network security controls and provide efficacy metrics for prevention and detection against specific adversarial TTPs and attacker groups.

  This helps security analysts fully understand all components and features available so that once a real incident occurs, they can be prepared and respond quickly.

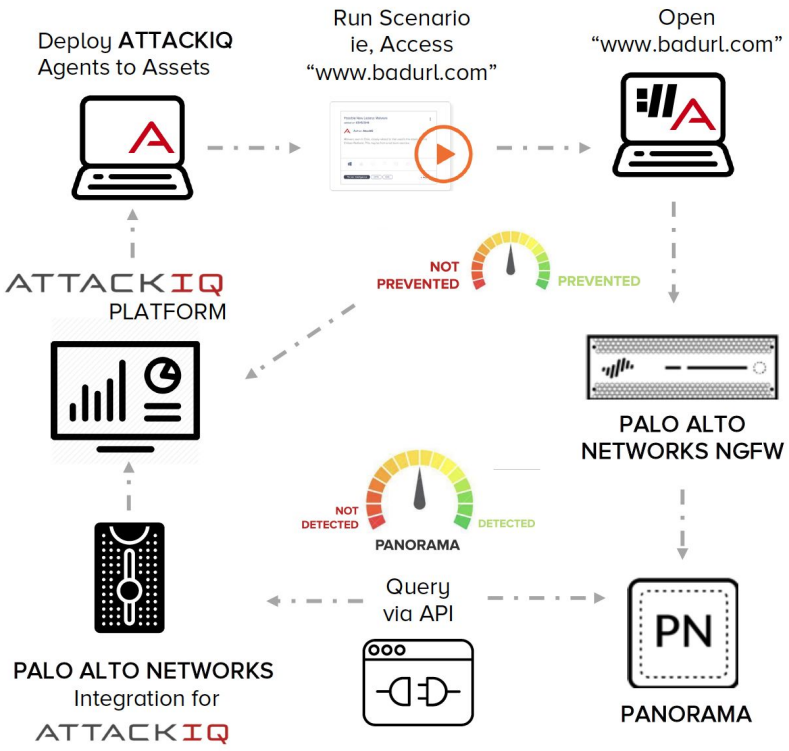
Palo Alto Networks Products for Integration

Palo Alto Networks Product	Integration Status	Palo Alto Networks versions supported	AttackIQ versions supported
AutoFocus			
Cortex XDR			
Cortex XDR - Analytics			
GlobalProtect			
MineMeld			
NGFW	Validated	PAN-OS v9.0.0	All current
Panorama	Validated	PAN-OS v9.0.0	All current
Prisma Access			
Prisma Cloud			
Prisma SaaS			
Traps			
VM-Series			
Wildfire			
Other			

Integration Benefits

- Measure and continuously validate your firewall policies and controls
- Works with Panorama and NGFW, or standalone NGFW

Integration Diagram



- Data shared between products: AttackIQ queries the logs of Panorama to determine whether an attack was detected or not detected
- Data is shared via API
- Security analysts can use the data provided to prioritize remediation of missed detections or misconfigurations

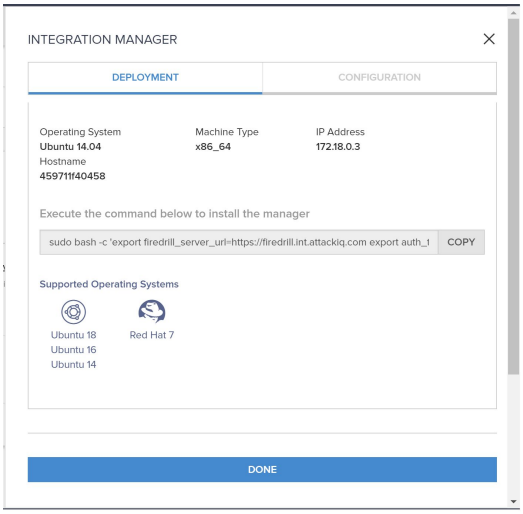
Before you begin

- On NGFW, enable pushing device monitoring data/logs to Panorama
- Have your AttackIQ Admin account credentials on hand
- Ensure you have deployed AttackIQ agents to assets in your environment

Install AttackIQ Integration Manager

If you haven’t installed AttackIQ Integration Manager already, follow these steps:

1. Deploy Ubuntu (14.x, 16.x, 18.x) or RedHat Server (7.x) for AIQ Integration Manager on-premise
    a. The Integration Manager should be deployed on a machine that is able to communicate via https/443 with Panorama/NGFW and AIQ Platform
2. Install Integration Manager on Ubuntu or RedHat Server
    a. Browse to AIQ Platform Tenant URL ⟶ Menu ⟶ Technologies ⟶ Integration Configuration ⟶ Integration Manager
    b. Copy and execute the installation command on the target machine to install the Integration Manager



Palo Alto Networks Configuration

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

  Step1) Select an Admin Role profile.
  Go to **Panorama>Admin Roles** and select or create an admin role.

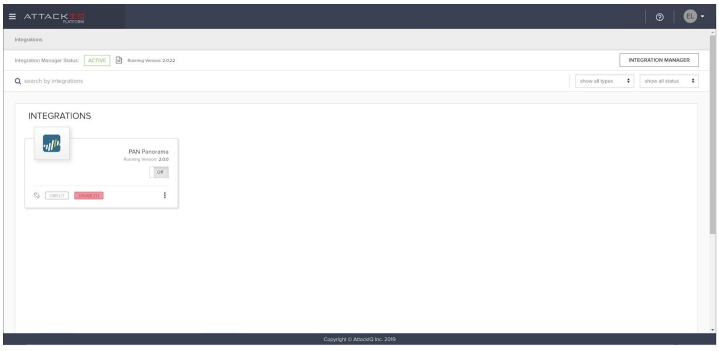
  Step2) Select features available to the admin role.

  1. Select the **XML API** tab.
  2. Enable or disable XML API features from the list, such as **Report**, **Log**, and **Configuration**.
  3. Select **OK** to confirm your change.

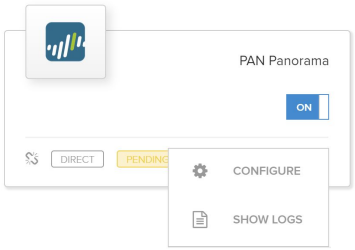
  Step3) Assign the admin role to an administrator account.

AttackIQ Integration Configuration

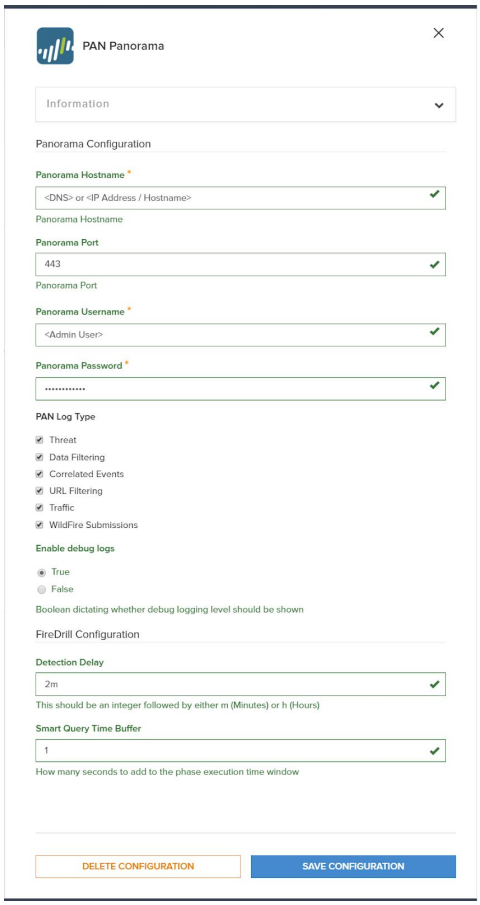
1. Click on Menu ⟶ Technologies ⟶ Integration Configuration
2. Locate Palo Alto Network Module, and slide radio button to turn “ON”



3. Click Menu ⋮ ⟶ Configure



4. Input the required information to configure Panorama integration



- Configure which logs you want (recommended: check all)
    - **Threat** - Displays an entry for each security alarm generated by the firewall. Each entry includes the date and time, a threat name or URL, the source and destination zones, addresses, and ports, the application name, and the alarm action (allow or block) and severity.
    - **Data Filtering** - Displays logs for the security policies with attached Data Filtering profiles, to help prevent sensitive information such as credit card or social security numbers from leaving the area protected by the firewall, and File Blocking profiles, that prevent certain file types from being uploaded or downloaded.
    - **Correlated Events** - Displays logs when the patterns and thresholds defined in a Correlation Object match the traffic patterns on your network.
    - **URL Filtering** - Displays logs for URL filters, which control access to websites and whether users can submit credentials to websites.

    - **Traffic** - Displays an entry for the start and end of each session. Each entry includes the date and time, source and destination zones, addresses and ports, application name, security rule name applied to the flow, rule action (allow, deny, or drop), ingress and egress interface, number of bytes, and session end reason.
    - **WildFire Submissions** - isplays logs for files and email links that the firewall forwarded for WildFire™ analysis. The WildFire cloud analyzes the sample and returns analysis results, which include the WildFire verdict assigned to the sample (benign, malware, grayware, or phishing).

Troubleshooting

- Contact information for support – support@attackiq.com
- Member of TSA Net

Technical Details

- AttackIQ Platform validates that Panorama and NGFW logs match those of the attack scenarios AttackIQ runs to validate the controls are working. We view the following logs: Traffic, data filtering, correlated events, wildfire, URL filtering.

Additional Administrator Role Web References

- Panorama Administrator Role Settings
    - https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-web-interface-help/panorama-web-interface/panorama-admin-roles.html
- Configure an Admin Role Profile – Panorama Administrators Guide 9.0
    - https://docs.paloaltonetworks.com/panorama/9-0/panorama-admin/set-up-panorama/set-up-administrative-access-to-panorama/configure-an-admin-role-profile.html
- Get Started with the XML API – PAN-OS and Panorama API Guide 9.0
    - https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-panorama-api/get-started-with-the-pan-os-xml-api.html
- Enable API Access – PAN-OS and Panorama API Guide 9.0
    - https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-panorama-api/get-started-with-the-pan-os-xml-api/enable-api-access.html#