Technology Partner Program

Integration Guide - Use Case Documentation

Author: NETSCOUT Systems, Inc.

Revision History	
October 13, 2021	Revalidating the Omnis Cyber Intelligence integration on PAN-OS 10.1
January 22, 2024	Revalidating the Omnis Cyber Intelligence integration on PAN-OS 11.1

Table 1: Partner information	
Date	January 24, 2024
Partner Name	NETSCOUT Systems, Inc.
Website	https://www.netscout.com/
Product Name	Omnis Cyber Intelligence (OCI)
Partner Contact	Michael.Segal@netscout.com
Support Contact	Amin.Abdulghani@netscout.com
Product Description	Advanced NDR platform that helps security teams easily detect, validate, investigate, and respond to cybersecurity incidents. At the core of this comprehensive platform lies deep packet inspection (DPI), offering enterprises unparalleled security visibility to accurately identify vulnerabilities and threats.

Use Cases for Integration with Palo Alto Networks

Use Case

- Omnis Cyber Intelligence detects Indicators of Compromise (IOCs). The security analyst investigates the violation in Omnis Cyber Intelligence. If deemed necessary, the security analyst can then send the IOC details to Panorama to be applied on the Palo Alto Networks NGFW for blocking. The IOC details that are sent to Panorama for blocking mitigation include hosts, IP Addresses, and URLs.

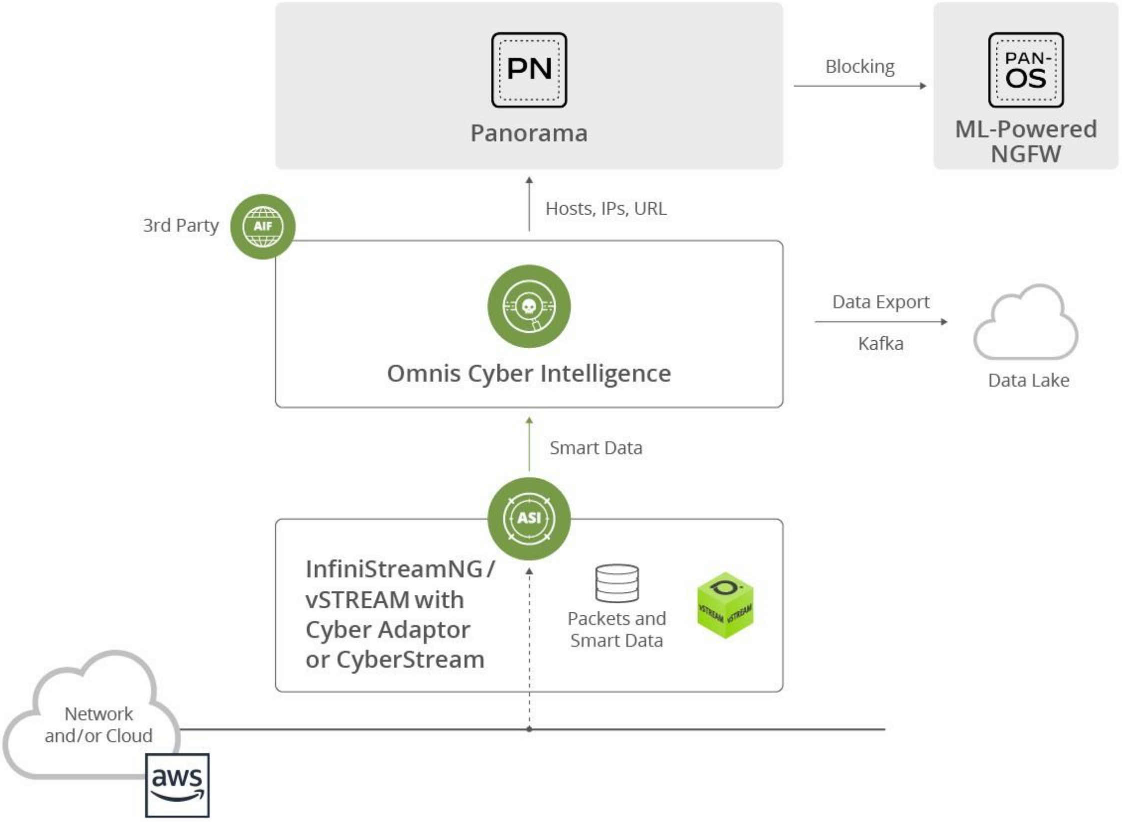
Table 2: Palo Alto Networks Products for Integration

Palo Alto Networks Product	Integration Status	Palo Alto Networks Versions Tested	<PARTNER NAME> Versions Tested
Cortex XDR			
Xpanse			
GlobalProtect			
IoT Security			
Prisma Access			
Prisma Cloud			
Prisma SaaS			
Prisma SD-WAN			
Next-Generation Firewall	Validated	10.2.x, 11.1.x	NETSCOUT Omnis Cyber Intelligence 6.3.5
Panorama	Validated	10.2.x, 11.1.x	NETSCOUT Omnis Cyber Intelligence 6.3.5
VM-Series			
WildFire			
Other			

Integration Benefits

The NETSCOUT Omnis Cyber Intelligence (OCI) platform identifies IOCs detected in the network and on hosts. All Palo Alto Networks ML-Powered Next-Generation Firewalls (NGFWs) can also run [Cloud Delivered Security Service (CDSS) subscriptions](#) (*optional*). Additionally Palo Alto Networks NGFWs use a Single Pass Parallel Processing (SP3) Architecture where the ML and DL algorithms are embedded directly within the core of the NGFW, allowing the Palo Alto Networks NGFWs to make traffic classification decisions at "line speed". This integration provides environments that utilize both the NetScout OCI platform and Panorama to centrally manage their Palo Alto Networks NGFWs, a complementary and synergistic solution to allow operators to immediately send discovered threat information from the OCI platform directly to Panorama for rapid and precise mitigation.

Integration Diagram



NETSCOUT products use the following data:

Data shared between our products:

- Omnis Cyber Intelligence identifies IOCs detected in the network and on hosts.
  - The IOC host, IP or URL can be marked for blocking.
  - Optionally, the host on which it was received can be blocked.
  - Omnis Cyber Intelligence sends the marked entity to Panorama.

The security analyst sends the applicable IOC entry details to Panorama which can then push these entries to the Palo Alto Networks NGFW for enforcement.

- This data is shared through the PANW RESTful APIs that were tested as part of the integration.
- The action taken because of this data sharing is IOC blocking by Panorama through the NGFW.

Before You Begin

- Ensure that the Palo Alto Networks Panorama initial setup is complete. The below links may be helpful:
    - Panorama Administrative Access Best Practices
    - Set Up the Panorama Virtual Appliance
    - Planning Your Panorama Deployment
    - Installing the Panorama Virtual Appliance
    - How to Install Panorama Plugins
    - Performing Initial NGFW Configuration
    - Best Practices for Managing Firewalls with Panorama

- Complete the Omnis Cyber Intelligence installation:
    - IOC feed setup is complete (NETSCOUT AIF and / or 3rd party)
    - Configure link to Panorama on Omnis Cyber Intelligence (see remediation screenshot below)
    - Additional requirements for successful integration: None
    - PAN-OS 11.1.x and NETSCOUT Omnis Cyber Intelligence 6.3.5
    - API key(s) requirements: Not applicable

- Other applicable dependencies:
    - **NOTE**: If the system has device groups, Omnis Cyber Intelligence entities will be created and sent to the first 2 device groups returned by the PAN-OS API. The entries created in PAN-OS include Omnis Cyber Intelligence Address Group (OmnisSecurity ManualAddress), Omnis Cyber Intelligence URL Group (OmnisSecurity Manual URL) as well as Policy security rules related to Omnis Cyber Intelligence (OmnisSecurity-SRC rule, OmnisSecurity-DEST rule, OmnisSecurity URL Entries).

    - The device group list can optionally be defined using the property security.mediation.device.group.list

    - Drilldowns to Omnis Cyber Intelligence is through **ports 8443 or 8080 (configurable)**

Palo Alto Networks Configuration

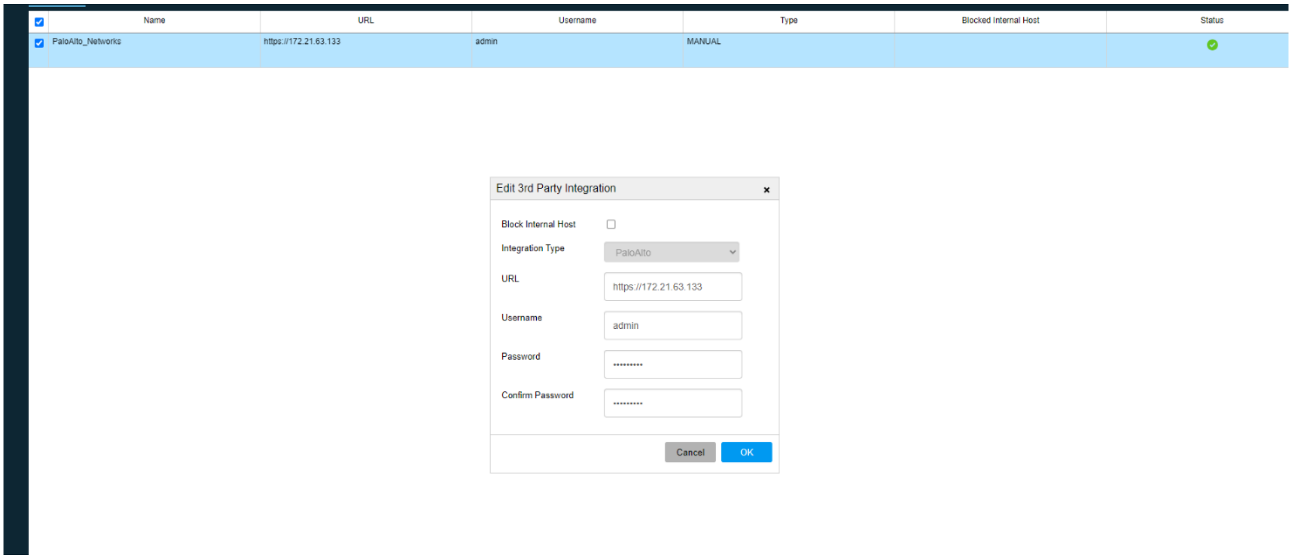
After the Panorama initial setup is completed, no additional customer configuration on Panorama is required.

- The following objects are created in Panorama as part of the linking from Omnis Cyber Intelligence:
    - OmnisSecurity Manual Address (Address Group)
    - OmnisSecurityManual URL (URL Category)
- The following policies are pushed to Panorama:
    - When IOCs are identified, the IOC details for hosts /IP are included as part of " Addresses" and "Address Groups".
    - The IOC details for URLs are included as part of URL Category.

Omnis Cyber Intelligence Product Configuration

- This section covers the process required to configure Omnis Cyber Intelligence for the Palo Alto Networks Panorama environment.

- For adding Palo Alto Networks credentials to Omnis Cyber Intelligence:



☑	Name	URL	Username	Type	Blocked Internal Host	Status
☑	PaloAlto_Networks	https://172.21.63.133	admin	MANUAL		✓

Edit 3rd Party Integration

Block Internal Host □

Integration Type: PaloAlto

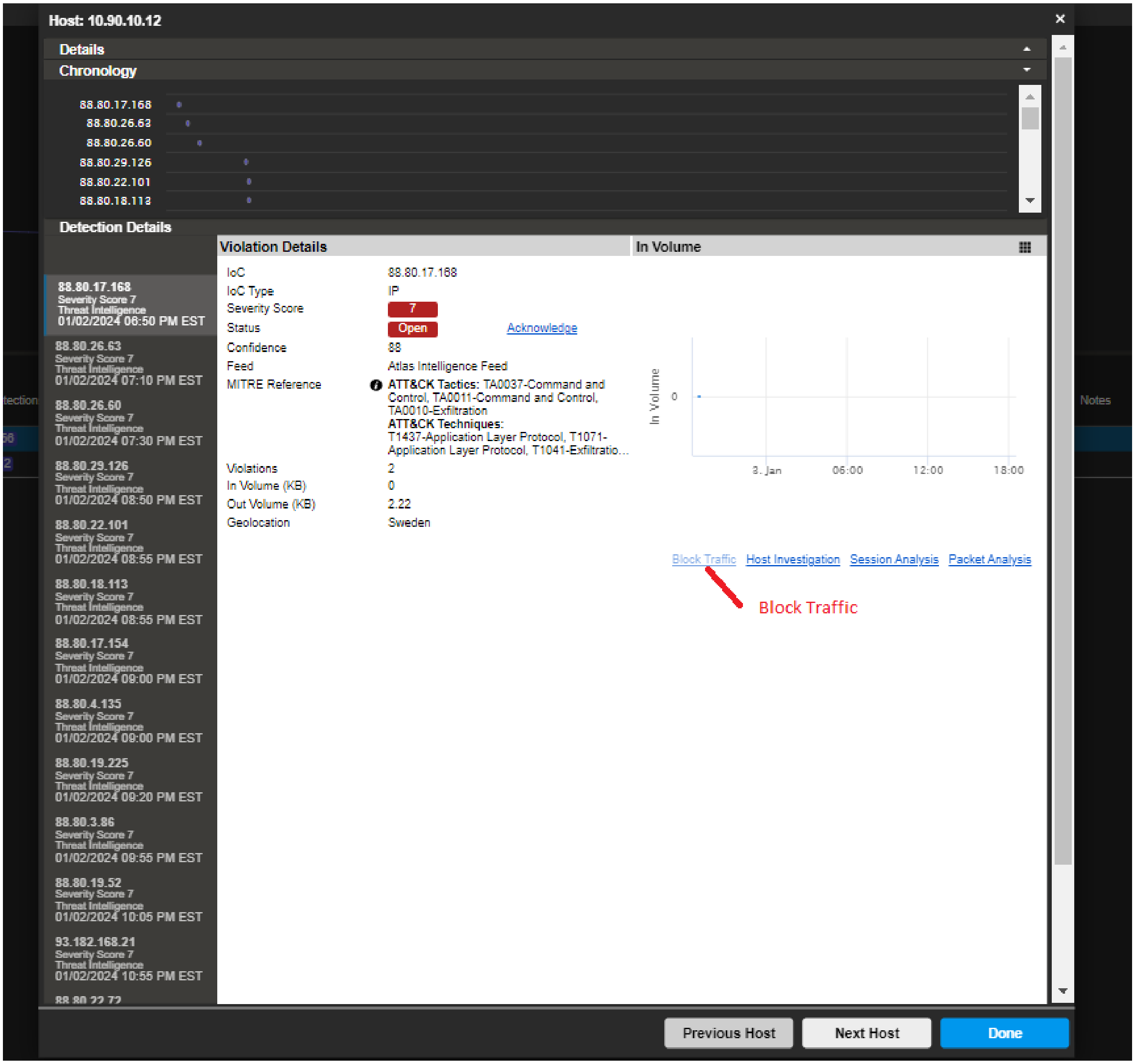
URL: https://172.21.63.133

Username: admin

Password: *********

Confirm Password: *********

- For blocking:
    - From the Security Event Center filter on the hosts getting Threat intelligence events.
    - Click on the host which is getting the traffic that needs to be blocked
    - From the detail screen, clicking on the “block traffic” icon sends the IOC to Panorama so that it can be applied to the NGFWs.
    - Selecting the IOC and then clicking on the block icon sends the IOC to Panorama so that it can be applied to the NGFWs.
    - The following example shows an example of an IOC from the detail screen that is an IP address.



Host: 10.90.10.12

Details

Chronology

Detection Details

88.80.17.168
Severity Score 7
Threat Intelligence
01/02/2024 06:50 PM EST

88.80.26.63
Severity Score 7
Threat Intelligence
01/02/2024 07:10 PM EST

88.80.26.60
Severity Score 7
Threat Intelligence
01/02/2024 07:30 PM EST

88.80.29.126
Severity Score 7
Threat Intelligence
01/02/2024 08:50 PM EST

88.80.22.101
Severity Score 7
Threat Intelligence
01/02/2024 08:55 PM EST

88.80.18.113
Severity Score 7
Threat Intelligence
01/02/2024 08:55 PM EST

88.80.17.154
Severity Score 7
Threat Intelligence
01/02/2024 09:00 PM EST

88.80.4.135
Severity Score 7
Threat Intelligence
01/02/2024 09:00 PM EST

88.80.19.225
Severity Score 7
Threat Intelligence
01/02/2024 09:20 PM EST

88.80.3.86
Severity Score 7
Threat Intelligence
01/02/2024 09:55 PM EST

88.80.19.52
Severity Score 7
Threat Intelligence
01/02/2024 10:05 PM EST

93.182.168.21
Severity Score 7
Threat Intelligence
01/02/2024 10:55 PM EST

88.80.22.72

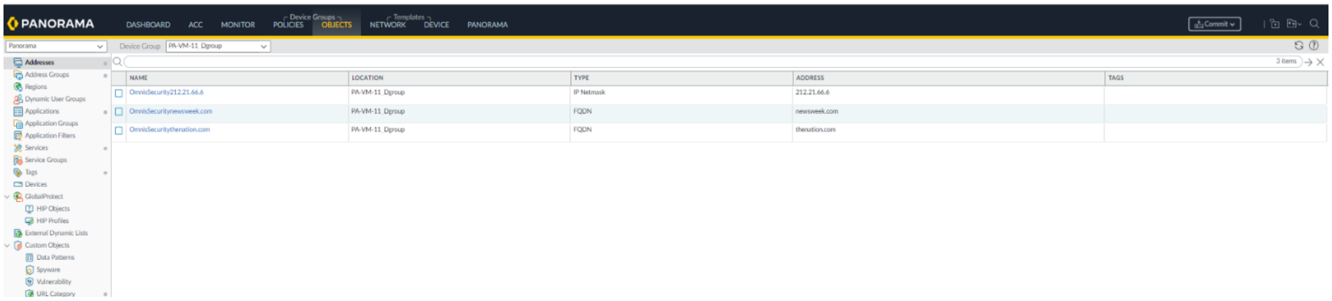
Violation Details

IoC	88.80.17.168
IoC Type	IP
Severity Score	7
Status	Open Acknowledge
Confidence	88
Feed	Atlas Intelligence Feed
MITRE Reference	**ATT&CK Tactics:** TA0037-Command and Control, TA0011-Command and Control, TA0010-Exfiltration **ATT&CK Techniques:** T1437-Application Layer Protocol, T1071-Application Layer Protocol, T1041-Exfiltratio...
Violations	2
In Volume (KB)	0
Out Volume (KB)	2.22
Geolocation	Sweden

In Volume

Panorama

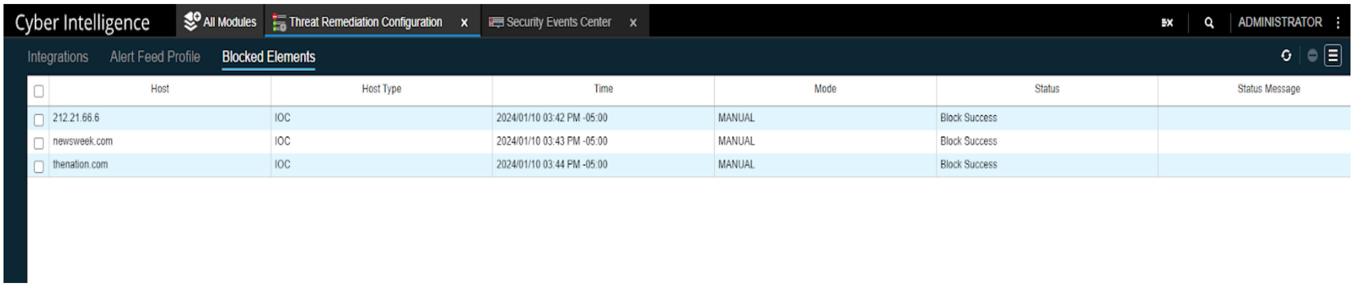
- In Panorama, the blocked address and URLs sent from Omnis Cyber Intelligence are listed:
- For Addresses:(Objects > Addresses)
- For URLS: (Object-> URL Category



NAME	LOCATION	TYPE	ADDRESS	TAGS
OmnisSecurity212.21.66.6	PA-VM-11_Dgroup	IP Netmask	212.21.66.6	
OmnisSecuritynewsweek.com	PA-VM-11_Dgroup	FQDN	newsweek.com	
OmnisSecuritythenation.com	PA-VM-11_Dgroup	FQDN	thenation.com	

- Blocked host lists

The block list is also shown in Omnis Cyber Intelligence



□	Host	Host Type	Time	Mode	Status	Status Message
□	212.21.66.6	IOC	2024/01/10 03:42 PM -05:00	MANUAL	Block Success	
□	newsweek.com	IOC	2024/01/10 03:43 PM -05:00	MANUAL	Block Success	
□	thenation.com	IOC	2024/01/10 03:44 PM -05:00	MANUAL	Block Success	

Configuring Threat Remediation

- **Note** : If you are not a SECADMIN user, ensure that you are assigned the OmnisCI - Security Configuration Admin privilege to modify the Threat Remediation Configuration page and to block IOCs.

- **Note**: If you manually unblock IP addresses or URL entries in PAN-OS, you must use the Threat Remediation module to unblock the same IP address(es)/URLs to ensure consistency on what is blocked.

NetScout Threat Remediation Configuration Help

This section describes the options available in Threat Remediation to integrate with Palo Alto Networks PAN-OS

Integration Toolbar Options

Option	Description
+	Add Integration
✎	Edit Integration
🗑	Remove Integration
⏻	Activate/Deactivate Integration
☰	Click to access the options above and the online help.

• Integrations List Options

Option	Description
Name	Name of the third party integration.
URL	URL of the associated integration server.
Username	User name associated with the associated integration server.
Type	Blocked trac type of the associated integration; for this release: Manual.
Blocked Internal Host	Identifies if the internal host if the associated integration is blocked; can be: l True l False
Status	Identifies the status of the associated integration; can be: l ✔ (ok) l ! (warning) l ✖ (critical)
^ / **v** Integration Operation Progress	Click **^** to show the integration configuration progress. Click **v** to hide the integration configuration progress.

Add/Modify Third-Party Feed Integration Options

Option	**Description** ◉
Block Preference Type	The default and only option is Manual.
Block Internal Host □	Check the check box to block the internal host and add it to the Blocked Elements listing page.
Integration Type	Use the drop down list to choose which third-party integration feed you want to add. Default = PaloAlto.
URL	hostname or IP address.
Username	User name for the associated host server.
Password	Password for the associated host server.
□ Show Password	Check the checkbox to display the password in the Password field, instead of masking characters.

• **NETSCOUT customers with GTAC** **support** have immediate access to the latest product and service information for assistance with setup and configuration of this integrated solution.

Troubleshooting

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

NETSCOUT:

Please **NOTE**: The user / security analyst, should do an explicit push from Panorama to the Palo Alto Networks NGFW to apply the IOC policy.

Beyond the above mentioned configuration, the integration should be seamless to the customer. In case of NETSCOUT specific issue(s), please contact NETSCOUT support.

Palo Alto Networks:

NOTE: Starting from PAN-OS 10.2.0 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 and/ or Panorama is not EoL: End-of-Life Summary - Palo Alto Networks

Palo Alto Networks Customer Support 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

HA Concepts

Palo Alto Networks NGFWs support stateful active/passive or active/active high availability with session and configuration synchronization with a few exceptions:

- The VM-Series NGFW on AWS supports active/passive HA only.
  On AWS, when you deploy the NGFW with the Amazon Elastic Load Balancing (ELB) service, it does not support HA (in this case, ELB service provides the failover capabilities).

If you are going to configure HA clustering, begin by understanding HA Concepts and the HA Clustering Overview .

Please also see:

- PAN-OS Release Notes - PAN-OS 11.1
- Changes to Default Behavior - PAN-OS 11.1

Helpful Resources

NETSCOUT:

- Learn more about Omnis Cyber Intelligence

Palo Alto Networks:

- PAN-OS Documentation
- Getting Started with the CLI
- Performing Initial Configuration on the Palo Alto Networks NGFW
- Installing a Device Certificate (On Device Not Being Managed by Panorama)
- PAN-OS Upgrade Guide
- Security Policy Rules
- PAN-OS ® New Features Guide - 11.1
- Optional Subscriptions You Can Use With the NGFW
- VM-Series Deployment Guide
- Panorama Administrator's Guide
- Panorama Templates
- PAN-OS® and Panorama™API Usage Guide
- Palo Alto Networks Best Practices
- PAN-OS End-of-Life Summary - Palo Alto Networks

Contact Information for Support

For NETSCOUT specific issues:

- https://www.netscout.com/support-services

NETSCOUT customers with GTAC support have immediate access to the latest product and service information for assistance with setup and configuration of this integrated solution.

For Palo Alto Networks specific issues:

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

Technical Details

Panorama XML and Xpath APIs leveraged in this integration:

- Xpath api for getting device groups
- Xpath api for creating/removing addresses
- Xpath api for adding/removing OmnisSecurity address group (OmnisSecurity Manual Address)
- Xpath api adding/removing OmniSecurity url group (OmnisSecurity Manual URL)
- Xpath api for adding/deleting address entries to OmnisSecurityAddressgroup
- Xpath api for adding/removing urls entries to/from OmnisSecurityManual URL
- Xpath api for adding/removing security rules