paloalto TECHDOCS

NGFW AIOps

docs.paloaltonetworks.com

Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About the Documentation

- For the most recent version of this guide or for access to related documentation, visit the Technical Documentation portal docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Palo Alto Networks, Inc.
www.paloaltonetworks.com

Last Revised

May 17, 2024

Table of Contents

AIOps for NGFW

Drawing on data collected through PAN-OS device telemetry, AIOps for NGFW gives you an overview of the health and security of your next-generation firewall deployment to help you identify areas of improvement and close security gaps. AIOps for NGFW derives health information from device telemetry metrics related to the operational status of your devices. For security information, AIOps for NGFW analyzes the configuration of your devices against Palo Alto Networks best practices to point out any potential gaps in your security posture.

AIOps for NGFW Premium & Strata Cloud Manager

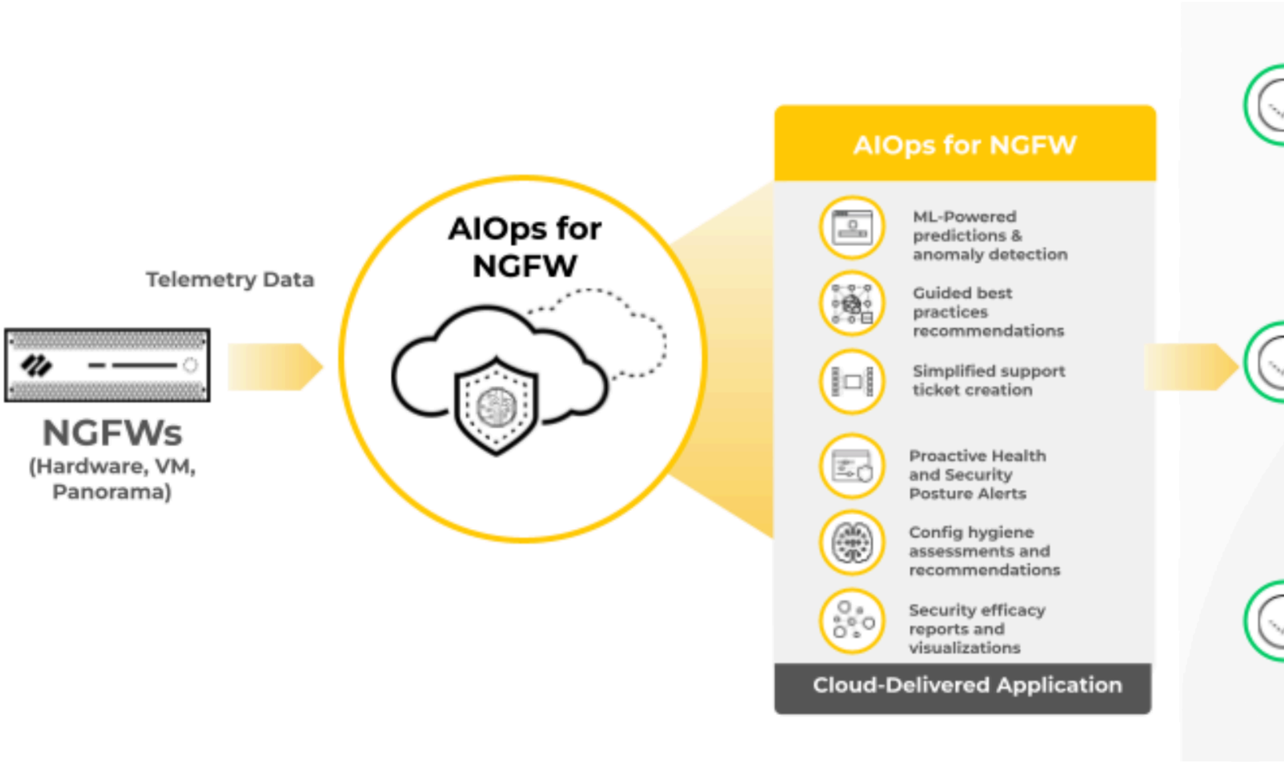
Strata Cloud Manager provides unified management and operations only for NGFWs using the AIOps for NGFW Premium license.

- ***NGFWs (PAN-OS and Panorama Managed)*** *→ For PAN-OS and Panorama Managed NGFWs with an AIOps for NGFW Premium license, use Strata Cloud Manager to oversee your deployment health and security posture.*
- ***NGFWs (Cloud Managed)*** *→ With an AIOps for NGFW license, you can also use Strata Cloud Manager for cloud management for NGFWs.*

The application tile name on the hub for AIOps for NGFW (the premium app only) is now changed to Strata Cloud Manager. With this update, the application URL has also changed to stratacloudmanager.paloaltonetworks.com, and you'll also now see the Strata Cloud Manager logo on the left navigation pane. Continue to use the AIOps for NGFW Free app for the NGFWs onboarded to AIOps for NGFW Free.

Get started:

- Free and Premium AIOps for NGFW
- Activate AIOps for NGFW
- Start sending device telemetry to AIOps for NGFW
- New Features
- On-Demand BPA Report
- AIOps for NGFW Incidents and Alerts


Telemetry Data
NGFWs
(Hardware, VM, Panorama)
AIOps for NGFW
AIOps for NGFW
ML-Powered predictions & anomaly detection
Guided best practices recommendations
Simplified support ticket creation
Proactive Health and Security Posture Alerts
Config hygiene assessments and recommendations
Security efficacy reports and visualizations
Cloud-Delivered Application

Regions for AIOps for NGFW

Where Can I Use This?	What Do I Need?
• NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series, funded with Software NGFW Credits	• AIOps for NGFW Free (use the AIOps for NGFW Free ap or • AIOps for NGFW Premium license (use the Strata Cloud

The region that you select when you activate AIOps for NGFW determines the physical location in which AIOps processes your data.

AIOps for NGFW is not offered in all the regions where the Strata Logging Service (SLS) infrastructure is supported. AIOps for NGFW deployment will expand to additional regions soon to match the telemetry data destinations. Currently, if you send your telemetry data to a region where the AIOps application is not supported, your data will be processed by an AIOps for NGFW instance in the United States-Americas region.

When you activate AIOps for NGFW, these restrictions are applied automatically. For example, if you select Germany as the region to activate an instance of AIOps for NGFW, only Germany-based SLS tenants can be attached to that instance.

Refer to the following table to understand the AIOps data processing for the various telemetry destination regions.

Strata Logging Service Region	Supported Region for an AIOps for NGFW Instance to Process Data
Germany	Germany
United Kingdom	United Kingdom
Netherlands - Europe	Netherlands - Europe
Italy - Europe	Italy - Europe
Spain - Europe	Spain - Europe
Switzerland - Europe	Switzerland - Europe
France - Europe	France - Europe
Poland - Europe	Poland - Europe
Korea	Korea
Indonesia	Indonesia

Strata Logging Service Region	Supported Region for an AIOps for NGFW Instance to Process Data
Israel	Israel
Taiwan	Taiwan
Qatar	Qatar
Singapore	Singapore
Australia	Australia
India	India
Japan	Japan
Canada	Canada
Remaining SLS Regions	United States-Americas

Free and Premium Features

Where Can I Use This?	What Do I Need?
• NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series, funded with Software NGFW Credits	• AIOps for NGFW Free (use the AIOps for NGFW Free ap or • AIOps for NGFW Premium license (use the Strata Cloud

AIOps for NGFW comes in two license tiers: free and premium.

Free AIOps for NGFW features enrich your understanding of your firewall deployment.

Free features:

- assess the firewall's configuration and identify areas for improvement
- provide easy access to runtime and historical telemetry data from firewalls
- detect system issues (independent of the detection method)
- reduce time to resolution through alert/notification workflows
- provide dynamic dashboards and visualizations for several security subscriptions

With a premium tier license, you have access to both free and premium features. Premium features focus on ensuring full utilization and maximal security outcome from your firewalls.

Premium features:

- Cloud management for NGFWs

  Contact your account team to enable Cloud Management for NGFWs using Strata Cloud Manager.

- use advanced ML techniques to promote an always-optimal security posture that responds to the changing threat and network landscapes, thereby reducing the attack surface
- provide dynamic dashboards and visualizations for WildFire and IOC Search
- interact with data and visualize the relationships between events on the network in the Strata Cloud Manager Command Center to uncover anomalies or find ways to enhance your network security

Strata Cloud Manager provides unified management and operations only for NGFWs using the AIOps for NGFW Premium license. The application tile name on the hub for AIOps for NGFW (the premium app only) is now changed to Strata Cloud Manager. With this update, the application URL has also changed to stratacloudmanager.paloaltonetworks.com, and you'll also now see the Strata Cloud Manager logo on the left navigation pane. Continue to use the AIOps for NGFW Free app for the NGFWs onboarded to AIOps for NGFW Free.

Feature Set	Free	Premium (use Strata Cloud Manager)
Strengthen Security Posture	**Partial**	**Yes**
- Security Posture Insights	Yes	Yes
- Feature Adoption	Yes	Yes
- Security Posture Settings	No	Yes
- Software Upgrade Recommendations	No	Yes
- CDSS Adoption	Yes	Yes
- Policy Analyzer	No	Yes
- On-Demand BPA Report	Yes	Yes
- Panorama CloudConnector Plugin	No	Yes
- Capacity Analyzer	No	Yes
- NGFW SDWAN Dashboard	No	Yes
- Compliance Summary Dashboard	No	Yes
Proactively Resolve Firewall Disruptions	**Partial**	**Yes**
- Alerts and Incidents	Partial	Yes
- PAN-OS CVEs dashboard	Yes	Yes
- Probable Cause Analysis for Alerts	No	Yes
Troubleshoot with Logs	**Yes**	**Yes**
- View, query and export logs in Log Viewer Check *licenses and other requirements to use Log Viewer.*	Yes	Yes
- Export Metadata for Troubleshooting	Yes	Yes
- View audit log	Yes	Yes
Optimize Your Security Investment	**Partial**	**Yes**

Feature Set	Free	Premium (use Strata Cloud Manager)
• Device ranking based on health and security posture	Yes	Yes
• All dashboards and reports except Threat Insights dashboard	Yes	Yes
• Threat Insights dashboard and report	No	Yes
• Search for security artifacts	No	Yes
• Build custom dashboard	No	Yes
• Strata Cloud Manager Command Center	No	Yes
Notifications	**Partial**	**Yes**
• Email Notifications	Yes	Yes
• ServiceNow Integration	No	Yes
Engagement and Support	**No**	**Yes**
• In-product support ticket creation capability for operational issues *requires Platinum Tier Support on the firewall (except for Power Supply Failure alerts)*	No	Yes

New capabilities in the product, across all feature categories, will be assigned to the Free and Premium tiers based solely on the discretion of Palo Alto Networks.

How to Activate AIOps for NGFW

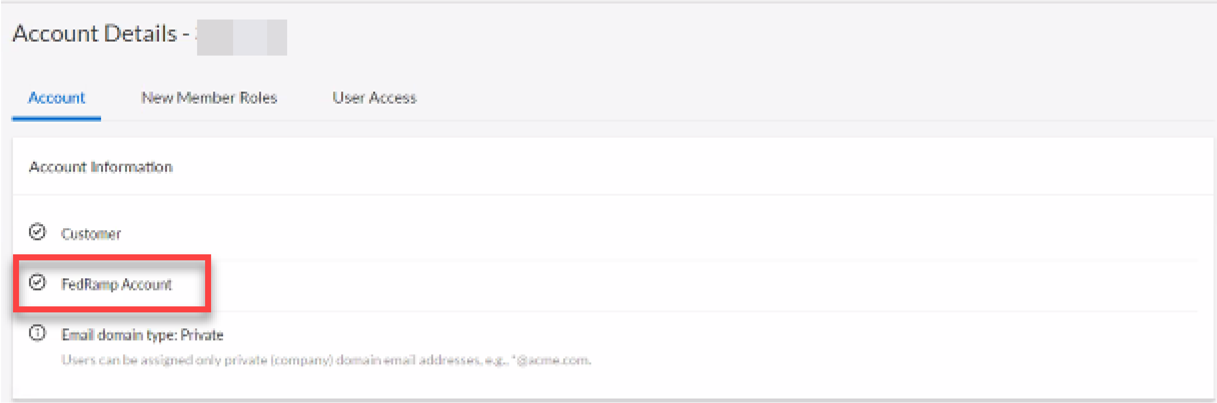
Where Can I Use This?	What Do I Need?
• NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series, funded with Software NGFW Credits	• AIOps for NGFW Free (use the AIOps for NGFW Free ap or • AIOps for NGFW Premium license (use the Strata Cloud

Here are the different scenarios for activating AIOps for NGFW:

Scenario	Plan
Activating AIOps for NGFW Free	Activate AIOps for NGFW (Free)
Activating AIOps for NGFW Premium (use Strata Cloud Manager app)	Activate AIOps for NGFW Through Common Services
Onboarding new devices to the activated AIOps for NGFW Free instance	Associate devices to a tenant Enable Telemetry on Devices
Onboarding new devices to the activated AIOps for NGFW Premium (use Strata Cloud Manager app)	Associate devices to a tenant Associate devices in tenant to app Enable Telemetry on Devices
Activating ELA AIOps for NGFW Premium	Activate Enterprise License Agreement (ELA) AIOps for NGFW Premium
Using Strata Cloud Manager (AIOps for NGFW Premium) to manage VM-Series	Activate a Software NGFW Credits License Agreement
Using Strata Cloud Manager (AIOps for NGFW Premium) for Panorama Managed VM-Series	Activate a Software NGFW Credits License for Panorama Managed VM-Series
Converting AIOps for NGFW Premium trial license to production	Convert Trial License to Production

Strata Cloud Manager provides unified management and operations only for NGFWs using the AIOps for NGFW Premium license. The application tile name on the hub for AIOps for NGFW (the premium app only) is now changed to Strata Cloud Manager. With this update, the application URL has also changed to stratacloudmanager.paloaltonetworks.com, and you'll also now see the Strata Cloud Manager logo on the left navigation pane. Continue to use the AIOps for NGFW Free app for the NGFWs onboarded to AIOps for NGFW Free.

*FedRAMP accounts can't use AIOps for NGFW. To check if this applies to you, sign in to your Customer Support Portal account and select **Account Management** > **Account Details**. If you see a **FedRamp Account** listed, then you cannot use AIOps for NGFW.*



Account Details - [redacted]

Account Information

Customer

FedRamp Account

Email domain type: Private

Users can be assigned only private (company) domain email addresses, e.g., *@acme.com.

Activate AIOps for NGFW (Free)

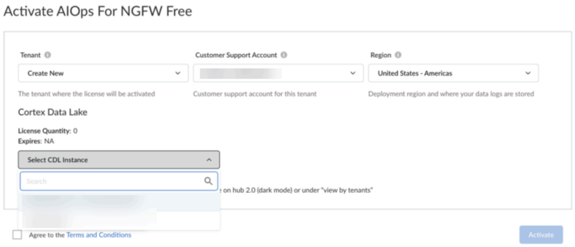
Activation requires the Account Administrator or App Administrator role.

1. Log in to the hub with the tenant-centric view.

   Toggle **View by Support Account** off if you're in the Support Account view.

   If you don't have an existing tenant, login to the hub with the support account view.

2. Find AIOps for NGFW Free and select **Activate**.
3. Complete the form.



Activate AIOps For NGFW Free

Tenant: Create New
The tenant where the license will be activated

Customer Support Account: [redacted]
Customer support account for this tenant

Region: United States - Americas
Deployment region and where your data logs are stored

Cortex Data Lake

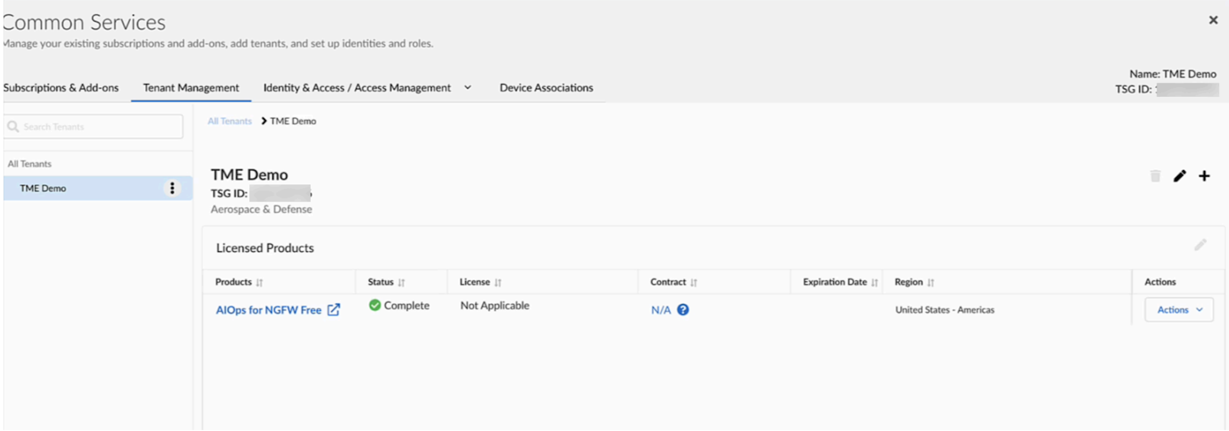
License Quantity: 0
Expires: NA

□ Agree to the Terms and Conditions

Tenant	Select the tenant where you will activate the AIOps for NGFW Free instance. If you don't have an existing tenant, select **Create New**.
Customer Support Account	Your Customer Support Portal account ID.
Region	The deployment region and the region where your data logs are stored. See Regions for AIOps for NGFW.
Strata Logging Service	The Strata Logging Service from which you want to send data to AIOps for NGFW Free. If you have a logging SLS, you can associate it

	with AIOps for NGFW Free. Otherwise, you can skip it.

4. **Agree to the Terms and Conditions** and **Activate**.
5. AIOps for NGFW Free is ready after **Status** shows **Complete**.



Common Services

Manage your existing subscriptions and add-ons, add tenants, and set up identities and roles.

Name: TME Demo
TSG ID: [redacted]

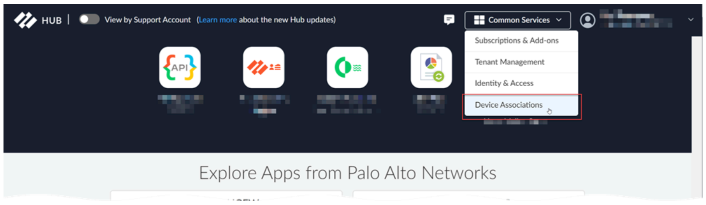
All Tenants > TME Demo

TME Demo
TSG ID: [redacted]
Aerospace & Defense

Licensed Products

Products	Status	License	Contract	Expiration Date	Region	Actions
AIOps for NGFW Free	✓ Complete	Not Applicable	N/A		United States - Americas	Actions

6. Associate devices to a tenant containing your AIOps for NGFW Free instance.
    1. Log in to the hub.
    2. Select **Common Services** > **Device Associations**.

        
        HUB
View by Support Account (Learn more about the new Hub updates)
Common Services
Subscriptions & Add-ons
Tenant Management
Identity & Access
Device Associations
Explore Apps from Palo Alto Networks

    3. Select **Add Device**.
    4. Select one or more firewalls or Panorama appliances and **Save**.

    You need to associate Panorama to the tenant containing AIOps for NGFW Free if you're onboarding Panorama-managed deployments. Make sure to individually associate all the firewalls managed by Panorama to the tenant.

    The devices that you associated with the tenant will be automatically added to AIOps for NGFW Free. For more information, see Associate devices to a tenant.

    - *For AIOps for NGFW Free activation, associating apps with devices isn't required.*
    - *You can associate devices to a tenant at the beginning of activation if you already have an existing tenant.*
    - *You can* remove device associations *if, for example, you are retiring or returning a firewall or Panorama appliance, or if you want to associate it with another tenant service group (TSG).*

7. Enable telemetry on devices.
    1. Confirm the device is registered in the Customer Support Portal by logging in to support.paloaltonetworks.com, switch to your account (if necessary), and identify your device in **Assets** > **Devices**.
    2. Install a device certificate on the devices you want to onboard.
    3. Enable telemetry sharing on the devices.

    After you onboard the devices and enable telemetry, it takes around a couple of hours for the first set of insights to be visible on the AIOps for NGFW dashboard. The process of generating and sending telemetry on the device's side is done in batches, with each metric being sampled and collected at a frequency optimized for the use cases the metric is used for. This batch process can result in a delay between onboarding the firewall and the availability of insights. It might take several hours for all insights associated with a newly onboarded device to appear on the AIOps for NGFW dashboard.

8. Log in to AIOps for NGFW Free by clicking on its icon in the hub.

Where Are My AIOps for NGFW Features?

This content is for the cloud management of Next-Generation Firewalls with AIOps for NGFW and Strata Cloud Manager. To get started managing Next-Generation Firewalls with PAN-OS, click here.

Where Can I Use This?	What Do I Need?
• NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series, funded with Software NGFW Credits	• AIOps for NGFW Free (use the AIOps for NGFW Free ap or • AIOps for NGFW Premium license (use the Strata Cloud

Palo Alto Networks Strata Cloud Manager is a new AI-Powered, unified network security management platform. Now, you can use Strata Cloud Manager to interact with and manage AIOps for NGFW together with your other Palo Alto Networks products and subscriptions.

To launch Strata Cloud Manager:

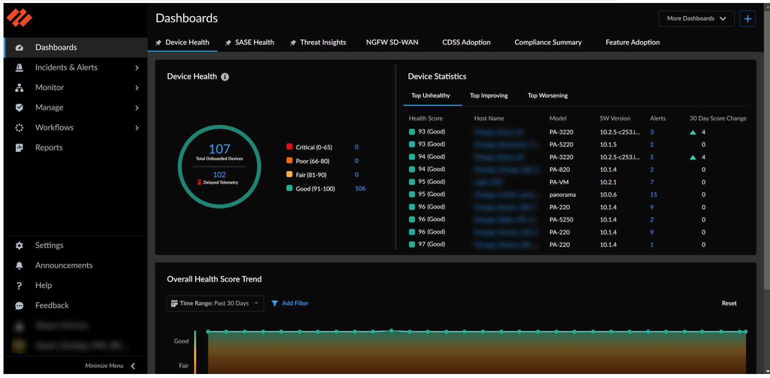
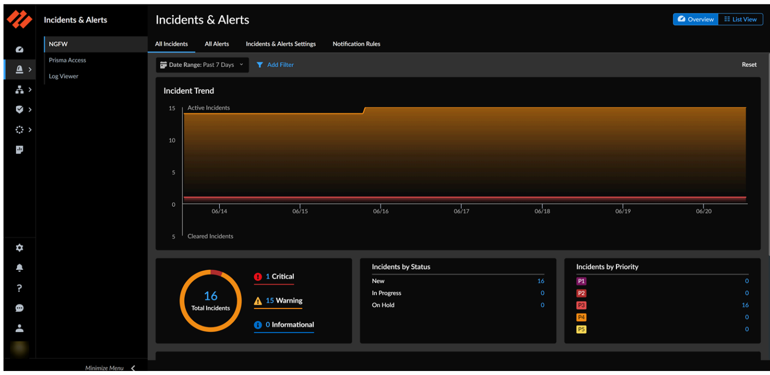
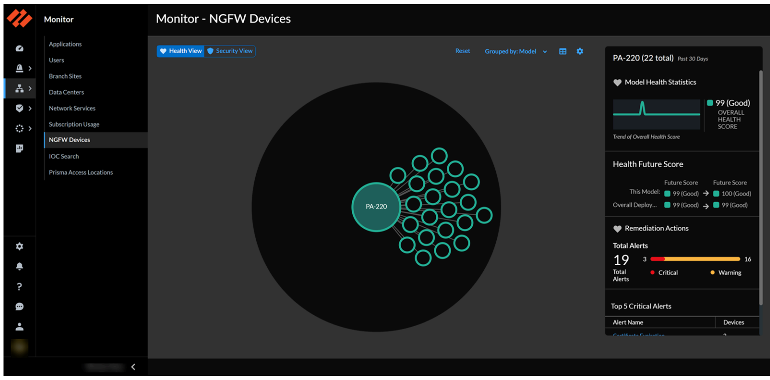
- Go to the hub and launch the Strata Cloud Manager app
- Go directly to the Strata Cloud Manager URL

- Strata Cloud Manager *provides unified management and operations only for NGFWs using the AIOps for NGFW Premium license. The application tile name on the* hub *for AIOps for NGFW (the premium app only) is now changed to Strata Cloud Manager. With this update, the application URL has also changed to* stratacloudmanager.paloaltonetworks.com*, and you'll also now see the Strata Cloud Manager logo on the left navigation pane. Continue to use the AIOps for NGFW Free app for the NGFWs onboarded to AIOps for NGFW Free.*
- *Contact your account team to enable* Cloud Management for NGFWs *using Strata Cloud Manager.*

If you've previously used the AIOps for NGFW app, here's where you can find your features in Strata Cloud Manager:

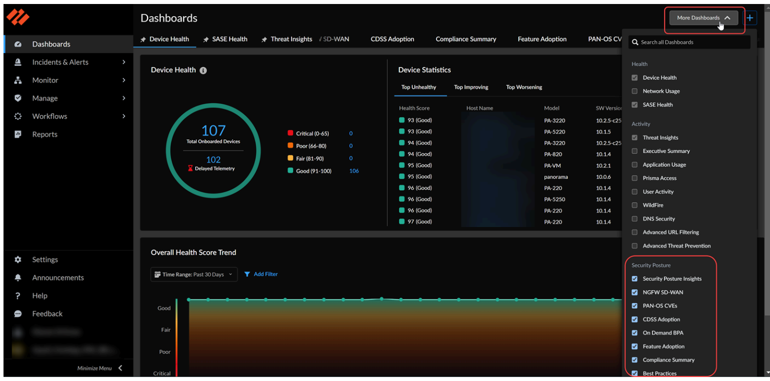
Table 1:

AIOps for NGFW App	Where to find these same features in Strata Cloud Manager:
Dashboards	→ Go to →Dashboards →Device Health

AIOps for NGFW App	Where to find these same features in Strata Cloud Manager:
	 Dashboards More Dashboards Device Health SASE Health Threat Insights NGFW SD-WAN CDSS Adoption Compliance Summary Feature Adoption Incidents & Alerts Monitor Manage Workflows Reports Settings Announcements Help Feedback Minimize Menu Device Health 107 Total Onboarded Devices 102 Delayed Telemetry Critical (0-65) 0 Poor (66-80) 0 Fair (81-90) 0 Good (91-100) 106 Device Statistics Top Unhealthy Top Improving Top Worsening Health Score / Host Name / Model / SW Version / Alerts / 30 Day Score Change 93 (Good) / [redacted] / PA-3220 / 10.2.5-c253.i... / 3 / ▲ 4 93 (Good) / [redacted] / PA-5220 / 10.1.5 / 2 / 0 94 (Good) / [redacted] / PA-3220 / 10.2.5-c253.i... / 5 / ▲ 4 94 (Good) / [redacted] / PA-820 / 10.1.4 / 2 / 0 95 (Good) / [redacted] / PA-VM / 10.2.1 / 7 / 0 95 (Good) / [redacted] / panorama / 10.0.6 / 15 / 0 96 (Good) / [redacted] / PA-220 / 10.1.4 / 9 / 0 96 (Good) / [redacted] / PA-5250 / 10.1.4 / 2 / 0 96 (Good) / [redacted] / PA-220 / 10.1.4 / 9 / 0 97 (Good) / [redacted] / PA-220 / 10.1.4 / 1 / 0 Overall Health Score Trend Time Range: Past 30 Days Add Filter Reset Good Fair
Alerts	→ Go to →Incidents & Alerts →NGFW  Incidents & Alerts NGFW Prisma Access Log Viewer Overview List View All Incidents All Alerts Incidents & Alerts Settings Notification Rules Date Range: Past 7 Days Add Filter Reset Incident Trend Active Incidents 15 10 5 0 06/14 06/15 06/16 06/17 06/18 06/19 06/20 Cleared Incidents 16 Total Incidents 1 Critical 15 Warning 0 Informational Incidents by Status New 16 In Progress 0 On Hold 0 Incidents by Priority P1 0 P2 0 P3 16 P4 0 P5 0 Minimize Menu
Monitor	→ Go to →Monitor →Devices →NGFW  Monitor Applications Users Branch Sites Data Centers Network Services Subscription Usage NGFW Devices IOC Search Prisma Access Locations Monitor - NGFW Devices Health View Security View Reset Grouped by: Model PA-220 PA-220 (22 total) Past 30 Days Model Health Statistics 99 (Good) OVERALL HEALTH SCORE Trend of Overall Health Score Health Future Score Future Score Future Score This Model: 99 (Good) → 100 (Good) Overall Deploy... 99 (Good) → 99 (Good) Remediation Actions Total Alerts 19 Total Alerts 3 16 Critical Warning Top 5 Critical Alerts Alert Name Devices
Posture	→ Go to Dashboards to see: • Best Practices dashboard • Security Posture Insights dashboard • NGFW SD-WAN dashboard • Security Advisory dashboard (PAN-OS CVEs) • CDSS Adoption dashboard

<table>
<tr><th>AIOps for NGFW App</th><th>Where to find these same features in Strata Cloud Manager:</th></tr>
<tr><td></td><td>

- On-Demand BPA dashboard
- Feature Adoption dashboard
- Compliance Summary dashboard



Dashboards

Device Health

107 Total Onboarded Devices

102 Delayed Telemetry

<table>
<tr><td>🟥 Critical (0-65)</td><td>0</td></tr>
<tr><td>🟧 Poor (66-80)</td><td>0</td></tr>
<tr><td>🟨 Fair (81-90)</td><td>0</td></tr>
<tr><td>🟩 Good (91-100)</td><td>106</td></tr>
</table>

Device Statistics

Top Unhealthy | Top Improving | Top Worsening

<table>
<tr><th>Health Score</th><th>Host Name</th><th>Model</th><th>SW Versio</th></tr>
<tr><td>93 (Good)</td><td>[redacted]</td><td>PA-3220</td><td>10.2.5-c25</td></tr>
<tr><td>93 (Good)</td><td>[redacted]</td><td>PA-5220</td><td>10.1.5</td></tr>
<tr><td>94 (Good)</td><td>[redacted]</td><td>PA-3220</td><td>10.2.5-c25</td></tr>
<tr><td>94 (Good)</td><td>[redacted]</td><td>PA-820</td><td>10.1.4</td></tr>
<tr><td>95 (Good)</td><td>[redacted]</td><td>PA-VM</td><td>10.2.1</td></tr>
<tr><td>95 (Good)</td><td>[redacted]</td><td>panorama</td><td>10.0.6</td></tr>
<tr><td>96 (Good)</td><td>[redacted]</td><td>PA-220</td><td>10.1.4</td></tr>
<tr><td>96 (Good)</td><td>[redacted]</td><td>PA-5250</td><td>10.1.4</td></tr>
<tr><td>96 (Good)</td><td>[redacted]</td><td>PA-220</td><td>10.1.4</td></tr>
<tr><td>97 (Good)</td><td>[redacted]</td><td>PA-220</td><td>10.1.4</td></tr>
</table>

Overall Health Score Trend

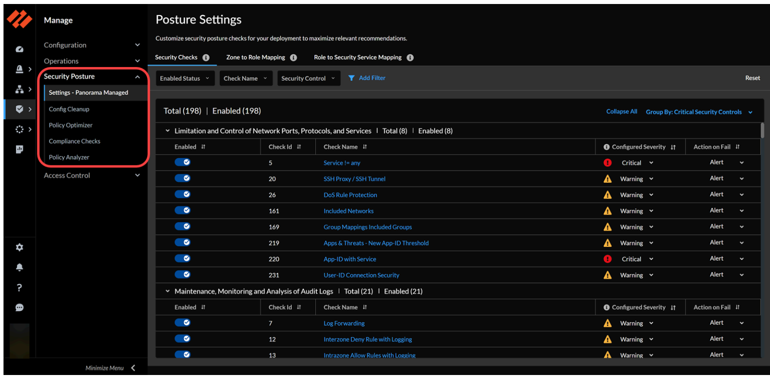
Health
☑ Device Health
☐ Network Usage
☑ SASE Health

Activity
☑ Threat Insights
☐ Executive Summary
☐ Application Usage
☐ Prisma Access
☐ User Activity
☐ WildFire
☐ DNS Security
☐ Advanced URL Filtering
☐ Advanced Threat Prevention

Security Posture
☑ Security Posture Insights
☑ NGFW SD-WAN
☑ PAN-OS CVEs
☑ CDSS Adoption
☑ On Demand BPA
☑ Feature Adoption
☑ Compliance Summary
☑ Best Practices

→ Go to →Manage →Security Posture to find:

- Settings - Panorama Managed
- Config Cleanup
- Policy Optimizer
- Compliance Checks
- Policy Analyzer



Posture Settings

Customize security posture checks for your deployment to maximize relevant recommendations.

Total (198) | Enabled (198)

Limitation and Control of Network Ports, Protocols, and Services | Total (8) | Enabled (8)

<table>
<tr><th>Enabled</th><th>Check Id</th><th>Check Name</th><th>Configured Severity</th><th>Action on Fail</th></tr>
<tr><td>✓</td><td>5</td><td>Service != any</td><td>Critical</td><td>Alert</td></tr>
<tr><td>✓</td><td>20</td><td>SSH Proxy / SSH Tunnel</td><td>Warning</td><td>Alert</td></tr>
<tr><td>✓</td><td>26</td><td>DoS Rule Protection</td><td>Warning</td><td>Alert</td></tr>
<tr><td>✓</td><td>161</td><td>Included Networks</td><td>Warning</td><td>Alert</td></tr>
<tr><td>✓</td><td>169</td><td>Group Mappings Included Groups</td><td>Warning</td><td>Alert</td></tr>
<tr><td>✓</td><td>219</td><td>Apps & Threats - New App-ID Threshold</td><td>Warning</td><td>Alert</td></tr>
<tr><td>✓</td><td>220</td><td>App-ID with Service</td><td>Critical</td><td>Alert</td></tr>
<tr><td>✓</td><td>231</td><td>User-ID Connection Security</td><td>Warning</td><td>Alert</td></tr>
</table>

Maintenance, Monitoring and Analysis of Audit Logs | Total (21) | Enabled (21)

<table>
<tr><th>Enabled</th><th>Check Id</th><th>Check Name</th><th>Configured Severity</th><th>Action on Fail</th></tr>
<tr><td>✓</td><td>7</td><td>Log Forwarding</td><td>Warning</td><td>Alert</td></tr>
<tr><td>✓</td><td>12</td><td>Interzone Deny Rule with Logging</td><td>Warning</td><td>Alert</td></tr>
<tr><td>✓</td><td>13</td><td>Intrazone Allow Rules with Logging</td><td>Warning</td><td>Alert</td></tr>
</table>

</td></tr>
<tr><td>

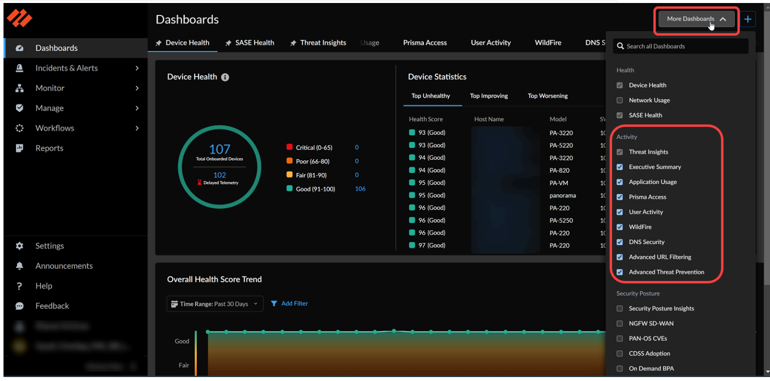
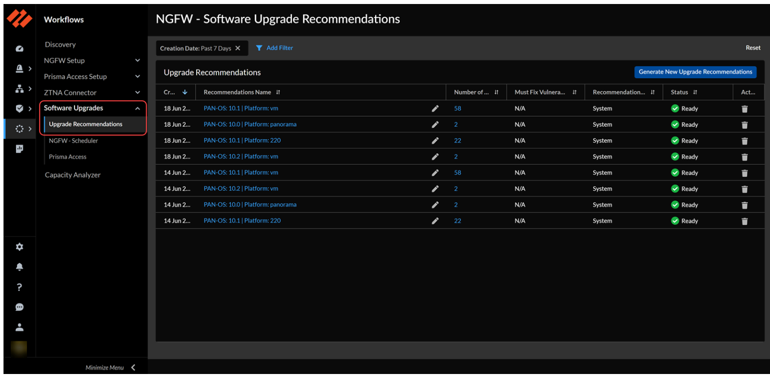
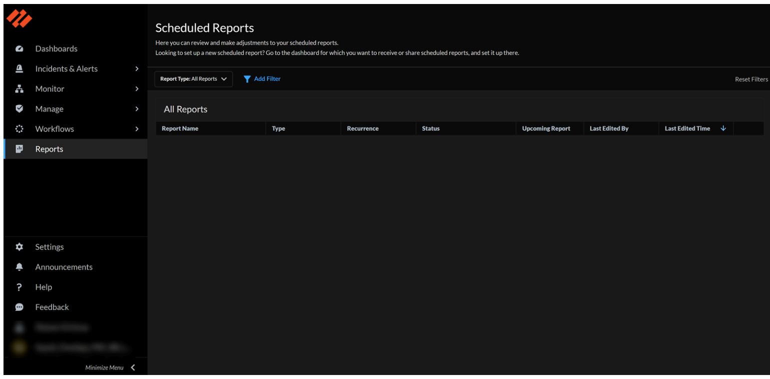
Activity

</td><td>

→ Go to Dashboards to see:

- Network Usage
- Threat Insights
- Application Usage
- Advanced WildFire
- DNS Security
- Executive Summary
- User Activity

</td></tr>
</table>

AIOps for NGFW App	Where to find these same features in Strata Cloud Manager:
	 → Go to **Reports** to generate reports for supported dashboards. → Go to **Incidents & Alerts** for **Log Viewer**.
Workflows	→ Go to **Workflows** > **Software Upgrades** to use the **Upgrade Recommendations**. 
Reports	→ Go to **Reports** to schedule reports for supported dashboards. 
Search	→ Go to **Monitor** for the **IoC Search**.

Health Score	Host Name	Model
93 (Good)		PA-3220
93 (Good)		PA-5220
94 (Good)		PA-3220
94 (Good)		PA-820
95 (Good)		PA-VM
95 (Good)		panorama
96 (Good)		PA-220
96 (Good)		PA-5250
96 (Good)		PA-220
97 (Good)		PA-220

Health
- ☑ Device Health
- ☐ Network Usage
- ☑ SASE Health

Activity
- ☑ Threat Insights
- ☑ Executive Summary
- ☑ Application Usage
- ☑ Prisma Access
- ☑ User Activity
- ☑ WildFire
- ☑ DNS Security
- ☑ Advanced URL Filtering
- ☑ Advanced Threat Prevention

Security Posture
- ☐ Security Posture Insights
- ☐ NGFW SD-WAN
- ☐ PAN-OS CVEs
- ☐ CDSS Adoption
- ☐ On Demand BPA

Upgrade Recommendations

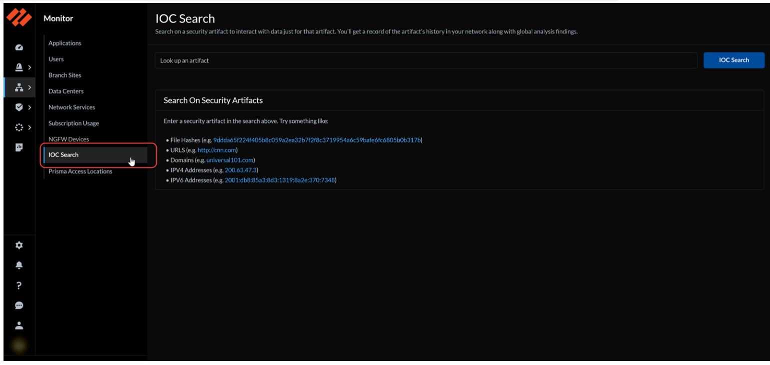
Cr...	Recommendations Name	Number of ...	Must Fix Vulnera...	Recommendation...	Status	Act...
18 Jun 2...	PAN-OS: 10.1 | Platform: vm	58	N/A	System	Ready	
18 Jun 2...	PAN-OS: 10.0 | Platform: panorama	2	N/A	System	Ready	
18 Jun 2...	PAN-OS: 10.1 | Platform: 220	22	N/A	System	Ready	
18 Jun 2...	PAN-OS: 10.2 | Platform: vm	2	N/A	System	Ready	
14 Jun 2...	PAN-OS: 10.1 | Platform: vm	58	N/A	System	Ready	
14 Jun 2...	PAN-OS: 10.2 | Platform: vm	2	N/A	System	Ready	
14 Jun 2...	PAN-OS: 10.0 | Platform: panorama	2	N/A	System	Ready	
14 Jun 2...	PAN-OS: 10.1 | Platform: 220	22	N/A	System	Ready	

Scheduled Reports

Here you can review and make adjustments to your scheduled reports.
Looking to set up a new scheduled report? Go to the dashboard for which you want to receive or share scheduled reports, and set it up there.

All Reports

Report Name	Type	Recurrence	Status	Upcoming Report	Last Edited By	Last Edited Time

<table>
<tr><th>AIOps for NGFW App</th><th>Where to find these same features in Strata Cloud Manager:</th></tr>
<tr><td></td><td>


IOC Search

Search on a security artifact to interact with data just for that artifact. You'll get a record of the artifact's history in your network along with global analysis findings.

Search On Security Artifacts

Enter a security artifact in the search above. Try something like:

• File Hashes (e.g. 9ddda65f224f405b8c059a2ea32b7f2f8c3719954a6c59bafe6fc6805b0b317b)
• URLS (e.g. http://cnn.com)
• Domains (e.g. universal101.com)
• IPV4 Addresses (e.g. 200.63.47.3)
• IPV6 Addresses (e.g. 2001:db8:85a3:8d3:1319:8a2e:370:7348)
</td></tr>
<tr><td>

Settings

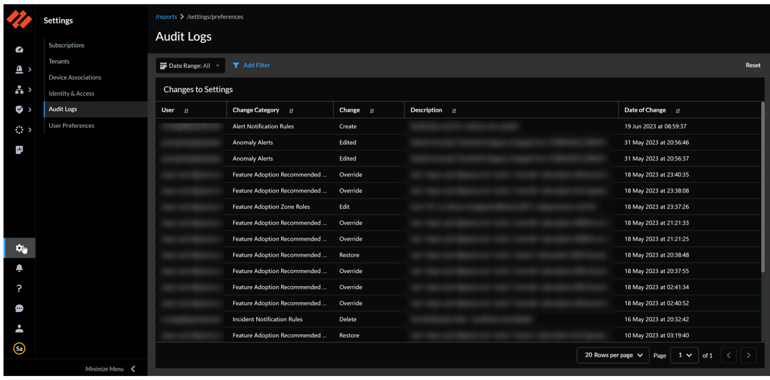
</td><td>

→ Go to **Incidents & Alerts** > **NGFW** > **Incidents & Alerts Settings** to see Forecast and Anomaly Incidents & Alerts.

→ Go to **Incidents & Alerts** > **NGFW** to set Notification Rules.

→ Go to **Settings** to see:

- Audit Logs
- User Preferences



/reports > /settings/preferences

Audit Logs

Changes to Settings

<table>
<tr><th>User</th><th>Change Category</th><th>Change</th><th>Description</th><th>Date of Change</th></tr>
<tr><td>[redacted]</td><td>Alert Notification Rules</td><td>Create</td><td>[redacted]</td><td>19 Jun 2023 at 08:59:37</td></tr>
<tr><td>[redacted]</td><td>Anomaly Alerts</td><td>Edited</td><td>[redacted]</td><td>31 May 2023 at 20:56:46</td></tr>
<tr><td>[redacted]</td><td>Anomaly Alerts</td><td>Edited</td><td>[redacted]</td><td>31 May 2023 at 20:56:37</td></tr>
<tr><td>[redacted]</td><td>Feature Adoption Recommended ...</td><td>Override</td><td>[redacted]</td><td>18 May 2023 at 23:40:35</td></tr>
<tr><td>[redacted]</td><td>Feature Adoption Recommended ...</td><td>Override</td><td>[redacted]</td><td>18 May 2023 at 23:38:08</td></tr>
<tr><td>[redacted]</td><td>Feature Adoption Zone Roles</td><td>Edit</td><td>[redacted]</td><td>18 May 2023 at 23:37:26</td></tr>
<tr><td>[redacted]</td><td>Feature Adoption Recommended ...</td><td>Override</td><td>[redacted]</td><td>18 May 2023 at 21:21:33</td></tr>
<tr><td>[redacted]</td><td>Feature Adoption Recommended ...</td><td>Override</td><td>[redacted]</td><td>18 May 2023 at 21:21:25</td></tr>
<tr><td>[redacted]</td><td>Feature Adoption Recommended ...</td><td>Restore</td><td>[redacted]</td><td>18 May 2023 at 20:38:48</td></tr>
<tr><td>[redacted]</td><td>Feature Adoption Recommended ...</td><td>Override</td><td>[redacted]</td><td>18 May 2023 at 20:37:55</td></tr>
<tr><td>[redacted]</td><td>Feature Adoption Recommended ...</td><td>Override</td><td>[redacted]</td><td>18 May 2023 at 02:41:34</td></tr>
<tr><td>[redacted]</td><td>Feature Adoption Recommended ...</td><td>Override</td><td>[redacted]</td><td>18 May 2023 at 02:40:52</td></tr>
<tr><td>[redacted]</td><td>Incident Notification Rules</td><td>Delete</td><td>[redacted]</td><td>16 May 2023 at 20:32:42</td></tr>
<tr><td>[redacted]</td><td>Feature Adoption Recommended ...</td><td>Restore</td><td>[redacted]</td><td>10 May 2023 at 03:19:40</td></tr>
</table>

→ Go to **Manage** > **Security Posture** to customize Settings - Panorama Managed.

→ Go to **Help** →Export Tenant Metadata.

</td></tr>
<tr><td>

–

</td><td>

Looking for how to manage NGFWs with Strata Cloud Manager?

This is supported only with Strata Cloud Manager with AIOps for NGFW Premium, and is not available in the AIOps for NGFW app.

→ Go to **Manage** > **Configuration** > **NGFWs and Prisma Access** and **Workflows** > **NGFW Setup**.

</td></tr>
</table>

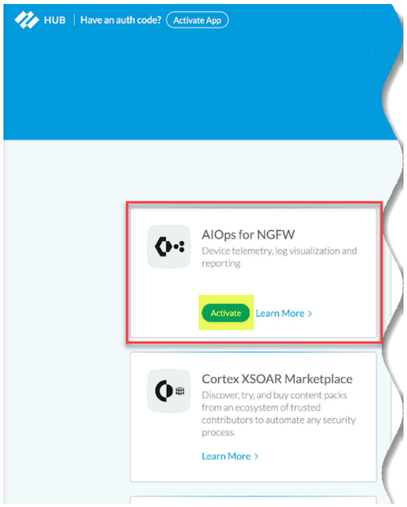
Panorama CloudConnector Plugin

Where Can I Use This?	What Do I Need?
• NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series, funded with Software NGFW Credits	□ AIOps for NGFW Premium license (use the Strata Cloud

Want to proactively check your policies for adherence to best practices? You shouldn't have to wait to get an alert and then fix a problem after you've pushed your policies. Connect AIOps for NGFW to your Panorama to evaluate your configuration against certain best practice checks before pushing it to your managed firewalls.

You'll need these things to connect AIOps for NGFW to your Panorama:

- An activated Premium instance.



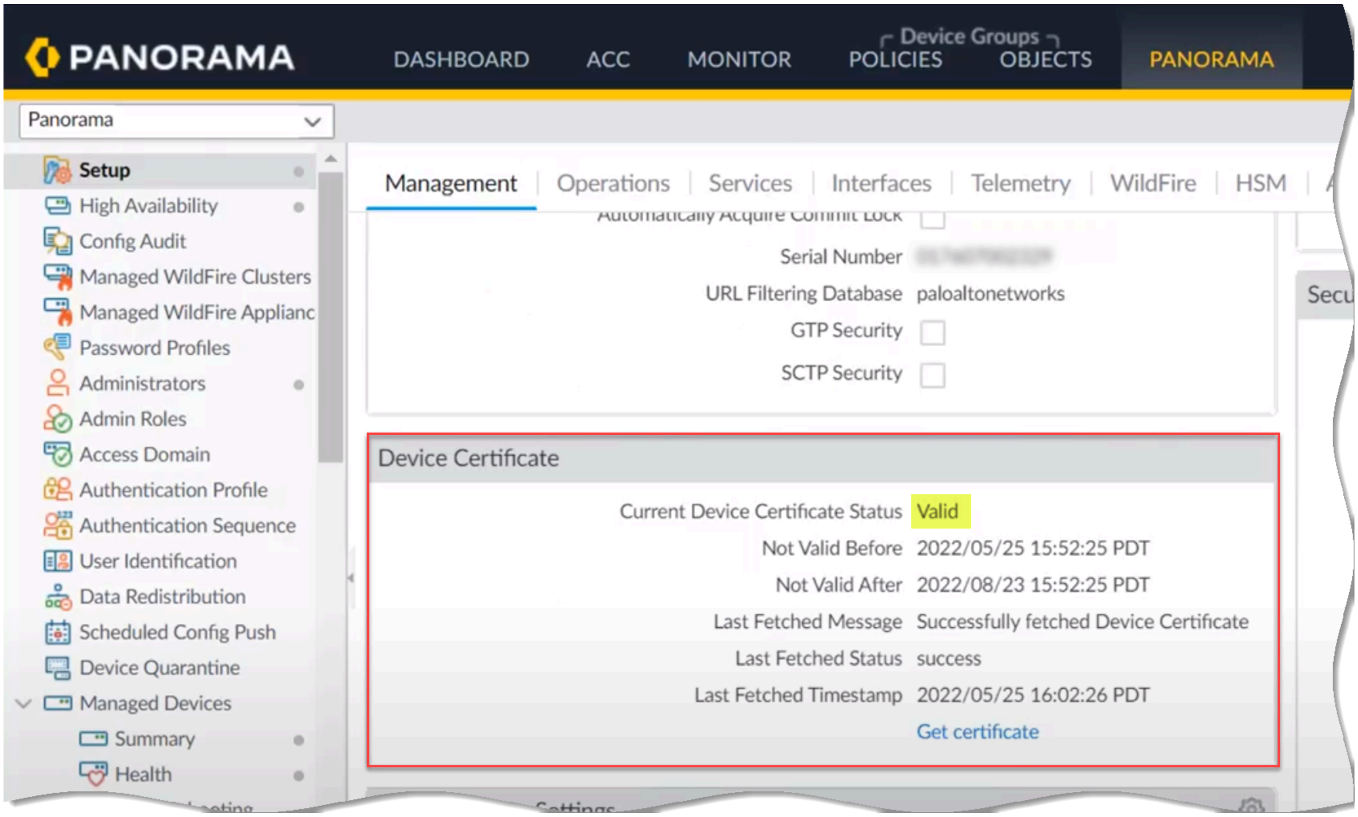
AIOps for NGFW

Device telemetry, log visualization and reporting

Cortex XSOAR Marketplace

Discover, try, and buy content packs from an ecosystem of trusted contributors to automate any security process.

- A Panorama with a device certificate installed.



Automatically Acquire Commit Lock □

Serial Number [redacted]

URL Filtering Database paloaltonetworks

GTP Security □

SCTP Security □

Device Certificate

Current Device Certificate Status Valid

Not Valid Before 2022/05/25 15:52:25 PDT

Not Valid After 2022/08/23 15:52:25 PDT

Last Fetched Message Successfully fetched Device Certificate

Last Fetched Status success

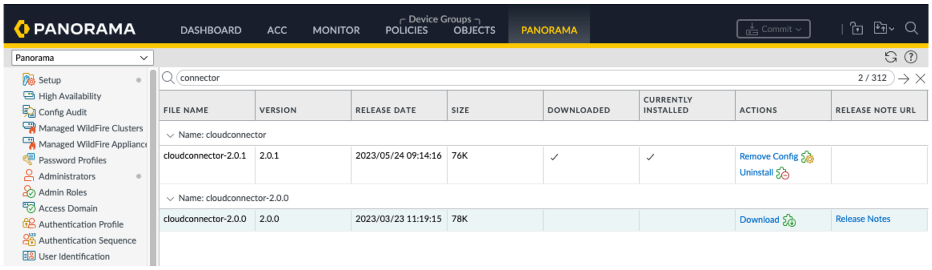
Last Fetched Timestamp 2022/05/25 16:02:26 PDT

Get certificate

Settings

- The Panorama CloudConnector Plugin installed on your Panorama running PAN OS 10.2.1 and above.

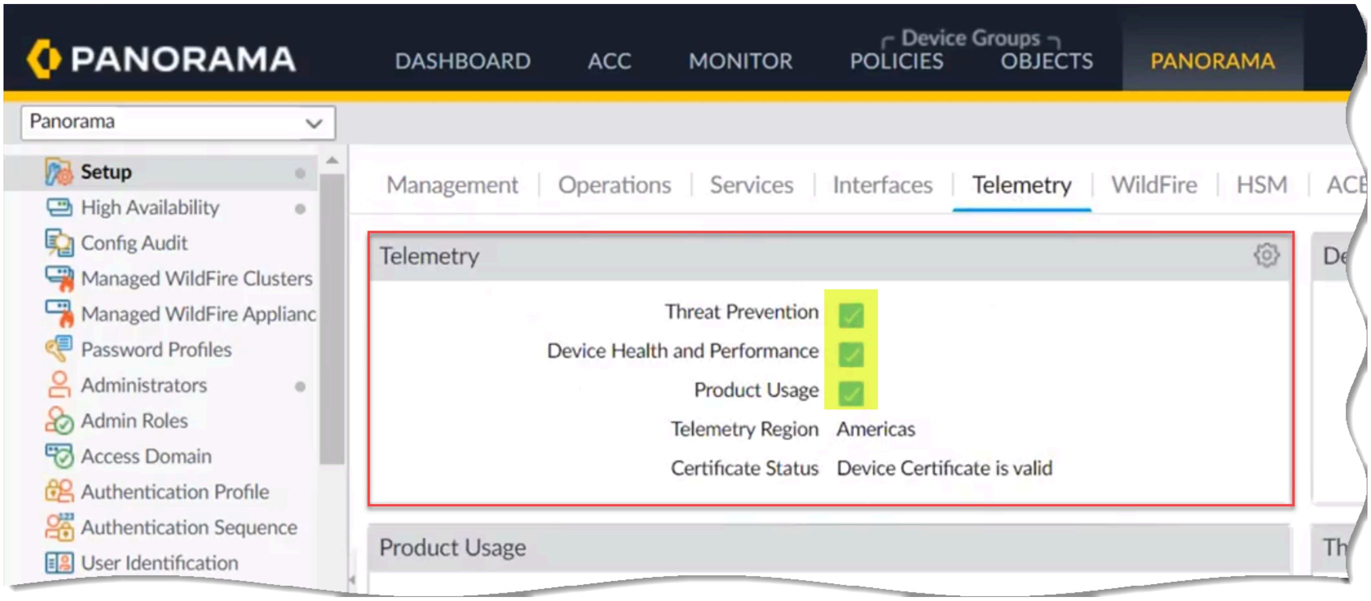
> *To help customers, we have pre-installed this plugin with newer Panorama versions (11.0.1 and above)*



connector 2 / 312

FILE NAME	VERSION	RELEASE DATE	SIZE	DOWNLOADED	CURRENTLY INSTALLED	ACTIONS	RELEASE NOTE URL
Name: cloudconnector							
cloudconnector-2.0.1	2.0.1	2023/05/24 09:14:16	76K	✓	✓	Remove Config Uninstall	
Name: cloudconnector-2.0.0							
cloudconnector-2.0.0	2.0.0	2023/03/23 11:19:15	78K			Download	Release Notes

- Device telemetry enabled on your Panorama.



Telemetry

Threat Prevention	☑
Device Health and Performance	☑
Product Usage	☑
Telemetry Region	Americas
Certificate Status	Device Certificate is valid

Product Usage

- A security policy rule that allows communication between Panorama and the FQDN that corresponds to your Strata Logging Service host region:

Americas (americas)	https://prod.us.secure-policy.cloudmgmt.paloaltonetworks.com/
Australia (au)	https://prod.au.secure-policy.cloudmgmt.paloaltonetworks.com/
Canada (ca)	https://prod.ca.secure-policy.cloudmgmt.paloaltonetworks.com/
Europe (europe)	https://prod.eu.secure-policy.cloudmgmt.paloaltonetworks.com/
FedRAMP (gov)	https://prod.gov.secure-policy.cloudmgmt.paloaltonetworks.com/
Germany (de)	https://prod.de.secure-policy.cloudmgmt.paloaltonetworks.com/
India (in)	https://prod.in.secure-policy.cloudmgmt.paloaltonetworks.com/
Japan (jp)	https://prod.jp.secure-policy.cloudmgmt.paloaltonetworks.com/
Singapore (sg)	https://prod.sg.secure-policy.cloudmgmt.paloaltonetworks.com/
United Kingdom (uk)	https://prod.uk.secure-policy.cloudmgmt.paloaltonetworks.com/

Get Alert Notifications

Where Can I Use This?	What Do I Need?
• NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series, funded with Software NGFW Credits	• AIOps for NGFW Free (use the AIOps for NGFW Free ap or • AIOps for NGFW Premium license (use the Strata Cloud

STEP 1 | Select **Incidents & Alerts** > **NGFW** > **Notification Rules** > **+ Add Notification Rule**

STEP 2 | Enter a `Name` and `Description`

STEP 3 | Specify the `Rule Conditions` that will trigger the notification.

STEP 4 | Choose the `Notification Type and Recipients` of the notification.

1. If choosing **Email**, select an email group, which is a group of users that will receive the email notifications, or **Create a New Email Group**.

    1. If creating a new email group, enter an Email Group Name and begin typing the Email Addresses of those you want to add to the group. Press the Return key after completing each email address.
    2. Select **Next**.
    3. Select the frequency with which you want to send these notifications:

    - Immediately
    - Grouped and sent every 4 hours
    - Grouped and sent once a day

2. If choosing **ServiceNow**, enter the `ServiceNow URL`, client credentials, ServiceNow credentials, and the `ServiceNow API Version`.

    1. **Test** your connection to ensure the integration is working.
    2. Select **Next**.

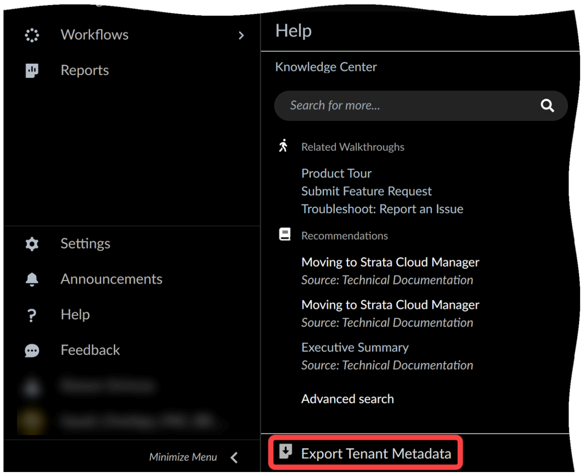
STEP 5 | **Save Rule**.

Export Metadata for Troubleshooting

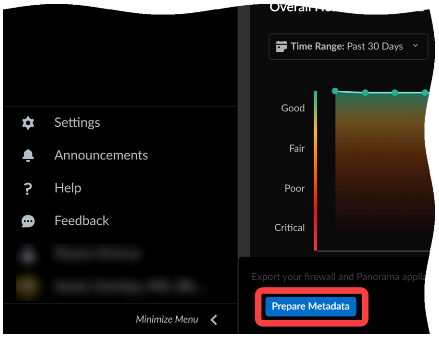
Where Can I Use This?	What Do I Need?
• NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series, funded with Software NGFW Credits	• AIOps for NGFW Free (use the AIOps for NGFW Free ap or • AIOps for NGFW Premium license (use the Strata Cloud

To provide technical support with the information they need to better assist you, AIOps for NGFW enables you to export your deployment data to your local machine. This data arrives in JSON files that are compressed in the gzip format.

STEP 1 | Select **Help** > **Export Tenant Metadata**.



STEP 2 | Click **Prepare Metadata**.



STEP 3 | **Download** your metadata file.

The metadata file name contains your Customer Support Portal (CSP) ID, your AIOps for NGFW tenant ID, and the timestamp for the export: <*csp-tenant-timestamp*>.gzip.

Troubleshoot NGFW Connectivity and Policy Enforcement Anomalies

Where Can I Use This?	What Do I Need?
• NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series, funded with Software NGFW Credits	• AIOps for NGFW Premium license (use the Strata Clo is required for Cloud Management for NGFWs • Strata Logging Service license is required for logging • If you have a Prisma Access license, you can use **Folder Management** to view your predefined folders and enable Web Security for a folder

Troubleshoot your NGFWs from Strata Cloud Manager without having to move between various firewall interfaces. If you experience connectivity issues after deploying and configuring your NGFWs, you can get an aggregate view of your routing and tunnel states, and drill down to specifics to find anomalies and problematic configurations.

Troubleshoot your identity-based policy rules and dynamically defined endpoints. You can check the status of specific NGFWs and expose possible mismatches between how you expect a policy to work and its actual enforcement behavior.

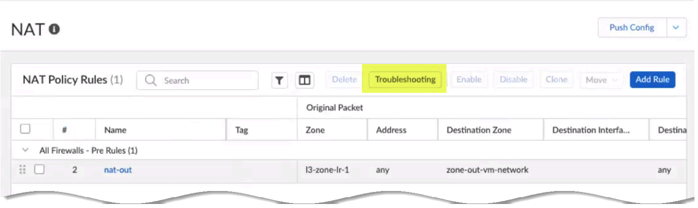
Troubleshooting lets you drill down on issue that might arise within these networking and identity features–track down and resolve connectivity issues or policy enforcement anomalies:

Network Troubleshooting

- NAT
- DNS Proxy

Identity and Policy Troubleshooting

- User Groups
- Dynamic Address Groups
- Dynamic User Groups
- User ID



				Original Packet				
☐	#	Name	Tag	Zone	Address	Destination Zone	Destination Interfa...	Destina
All Firewalls - Pre Rules (1)								
☐	2	nat-out		l3-zone-lr-1	any	zone-out-vm-network		any

Go to the feature you want to troubleshoot and select the **Troubleshooting** button to get started.

View and sort troubleshooting jobs you've run by Status, Action, Search Target, and Timestamp.

Feature	Feature Location	Available Actions	Action Scope	Job Output Organized By:
DNS Proxy (Network)	**Manage Configuration > NGFW and Prisma Access > Device Settings > DNS Proxy**	• Show DNS Proxy Cache • Search the DNS Proxy Cache	Firewalls you specify	• Domain Name • IP Address • Type–IPv4 Address Record (A), IPv6 Address Record (AAAA), Canonical Name Record (CNAME), Mail Exchange Record (MX), and Pointer to a canonical name (PTR) • Class: Internet (IN TCP/IP), Chaos (CH), and Hesiod (HS) • Time-to-live (TTL) in seconds • Hits–Number of times the record was requested since the last reboot
NAT (Network)	**Manage Configuration > NGFW and Prisma Access > Network Policies > NAT**	Show the NAT Rule IP Pool	Firewalls you specify	• Rule • Type • Used • Available • Memory Size Ratio
User Groups (Identity)	**Manage Configuration**	• Show User Group	Firewalls you specify	• Username

Feature	Feature Location	Available Actions	Action Scope	Job Output Organized By:
	> **NGFW and Prisma Access** > **Identity Services** > **Cloud Identity Engine**	- Search User Group		- Group
Dynamic Address Groups (Identity)	**Manage Configuration** > **NGFW and Prisma Access** > **Objects** > **Address** > **Address Groups**	- Show All Dynamic Address Groups - Search for a Dynamic Address Group (Chosen from a list)	Firewalls you specify	- Name - Filter - Members
Dynamic User Groups (Identity)	**Manage Configuration** > **NGFW and Prisma Access** > **Objects** > **Dynamic User Groups**	- Search by Dynamic User Group - Search by Username	Firewalls you specify	- Members (Username) and / or Dynamic User Group
User ID (Identity)	**Manage Configuration** > **NGFW and Prisma Access** > **Identity Services** > **Identity Redistribution**	- Show All User IP Mapping - Search For User IP Mapping	Firewalls you specify	- IP - User - From - Idle Timeout - Max Timeout

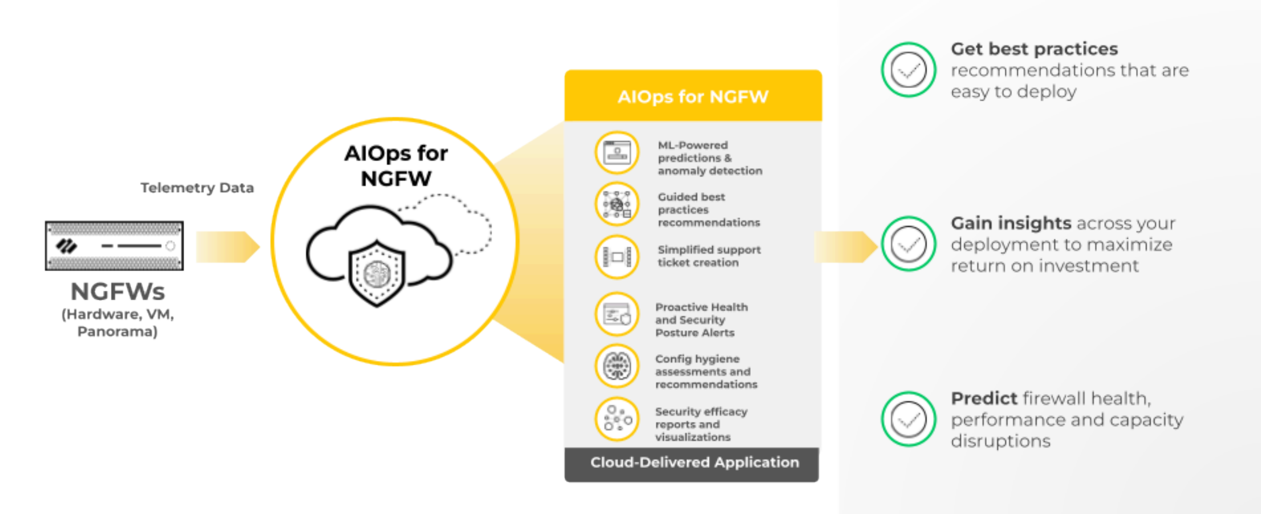
Device Telemetry for AIOps for NGFW

Where Can I Use This?	What Do I Need?
• NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series, funded with Software NGFW Credits	• AIOps for NGFW Free (use the AIOps for NGFW Free ap or • AIOps for NGFW Premium license (use the Strata Cloud

AIOps for NGFW assesses the health of the firewalls in your deployment by analyzing telemetry data that your PAN-OS devices send to Strata Logging Service. To send this data, you must have enabled device telemetry on your devices.

Once telemetry is configured, your next-generation firewalls send raw telemetry data to Strata Logging Service at fixed intervals. Strata Logging Service parses and translates this raw data so that AIOps for NGFW can provide you with device status, visualizations, and alerts.

Onboard your devices to begin sending device telemetry to AIOps for NGFW.


Telemetry Data
NGFWs
(Hardware, VM, Panorama)
AIOps for NGFW
AIOps for NGFW
ML-Powered predictions & anomaly detection
Guided best practices recommendations
Simplified support ticket creation
Proactive Health and Security Posture Alerts
Config hygiene assessments and recommendations
Security efficacy reports and visualizations
Cloud-Delivered Application
Get best practices recommendations that are easy to deploy
Gain insights across your deployment to maximize return on investment
Predict firewall health, performance and capacity disruptions

Enable Telemetry on Devices

Where Can I Use This?	What Do I Need?
• NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series, funded with Software NGFW Credits	• AIOps for NGFW Free (use the AIOps for NGFW Free ap or • AIOps for NGFW Premium license (use the Strata Cloud

Follow the steps below to use AIOps for NGFW with your PAN-OS devices.

If your outbound traffic passes through a proxy, ensure that you have allowed the Domains Required for AIOps for NGFW.

You need to onboard Panorama on AIOps for NGFW if you are onboarding Panorama-managed deployments.

STEP 1 | Confirm the device is registered in the Customer Support Portal by logging in to support.paloaltonetworks.com, switch to your account (if necessary), and identify your device in **Assets** > **Devices**.

STEP 2 | Install a device certificate on the devices you want to onboard.

STEP 3 | Enable telemetry sharing on the devices.

After you onboard the devices and enable telemetry, it takes around couple of hours for the first set of insights to be visible on the AIOps for NGFW dashboard. The process of generating and sending telemetry on the device's side is done in batches, with each metric being sampled and collected at a frequency optimized for the use-cases the metric is used for. This batch process can result in a delay between onboarding the firewall and the availability of insights. It might take several hours for all insights associated with a newly onboarded device to appear on the AIOps for NGFW dashboard.

Domains Required for AIOps for NGFW

Where Can I Use This?	What Do I Need?
- NGFW (Managed by Strata Cloud Manager) - NGFW (Managed by PAN-OS or Panorama) - VM-Series, funded with Software NGFW Credits	- AIOps for NGFW Free (use the AIOps for NGFW Free ap or - AIOps for NGFW Premium license (use the Strata Cloud

If outbound traffic from your devices passes through a proxy, ensure that you have allowed the following FQDNs in order to successfully use AIOps for NGFW.

Domains to Access AIOps for NGFW

Allow these domains in order to access the AIOps for NGFW application, regardless of your geographic region.

- *.prod.di.paloaltonetworks.cloud
- *.paloaltonetworks.com
- *.prod.di.paloaltonetworks.com
- *.prod.reporting.paloaltonetworks.com
- *.receiver.telemetry.paloaltonetworks.com
- https://storage.googleapis.com

App-IDs and Domains to Send Telemetry

See TCP Ports and FQDNs Required for Strata Logging Service for the App-IDs and ports that you must allow on your Palo Alto Networks firewalls to successfully send telemetry data to AIOps for NGFW.

On your proxy server, in addition to allowing the required ports and FQDNs, allow the domain that corresponds to your geographic region so that your devices can send telemetry data to AIOps for NGFW.

Region	Domain
US	http://br-prd1.us.cdl.paloaltonetworks.com/
Europe	http://br-prd1.nl.cdl.paloaltonetworks.com/
UK	http://br-prd1.uk.cdl.paloaltonetworks.com/
Canada	http://br-prd1.ca1.ne1.cdl.paloaltonetworks.com/
Singapore	http://br-prd1.sg1.se1.cdl.paloaltonetworks.com/

Region	Domain
Japan	http://br-prd1.jp1.ne1.cdl.paloaltonetworks.com/
Australia	http://br-prd1.au1.se1.cdl.paloaltonetworks.com/
Germany	http://br-prd1.de1.ew3.cdl.paloaltonetworks.com/
India	http://br-prd1.in1.as1.cdl.paloaltonetworks.com/

Utilize Activity Dashboards

AIOps for NGFW provides interactive dashboards that helps you to know how Palo Alto Networks security services are protecting your network. You can interact with data on the applications, threats, users, and security subscriptions at work in your network.

- View Executive Summary - View how your Palo Alto Networks security subscriptions are protecting you.
- Monitor WildFire - Shows how WildFire safeguards against newly emerging malware concealed within files, executables, and email links.
- Monitor DNS Security - Shows how your DNS Security subscription is shielding you from sophisticated threats and malware leveraging DNS.
- Monitor Advanced Threat Prevention - Shows a comprehensive view of detected threats in your network and highlights opportunities to enhance your overall security posture.
- Check the Strata Cloud Manager Command Center - Get a consolidated view of the Palo Alto Networks Network security platform and highlights areas where you can take direct actions to improve the health of your network.

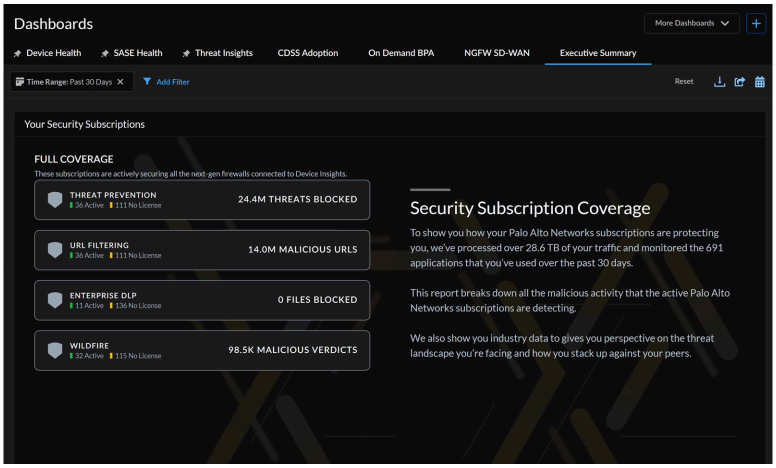
View Executive Summary

Where Can I Use This?	What Do I Need?
• NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series, funded with Software NGFW Credits This dashboard is supported for both AIOps for NGFW and Prisma Access.	□ AIOps for NGFW Free (use the AIOps for NGFW Free ap or AIOps for NGFW Premium license (use the Strata Cloud □ Strata Logging Service license □ A role that has permission to view the dashboard □ Licenses to unlock certain widgets and view data from supported product in the dashboard: Enterprise DLP, Advanced URL Filtering, Advanced Threat Prevention, Advanced WildFire, Prisma Access

The **Executive Summary** dashboard shows you how your Palo Alto Networks security subscriptions are protecting you. This report breaks down malicious activity in your network that these subscriptions are detecting: WildFire, Advanced Threat Prevention, Advanced URL Filtering, and Enterprise DLP. The dashboard shows data for each of these service with links to security services dashboards to dive deeper for further investigation.

You can use this dashboard to:

- Review all the malicious activity that the active Palo Alto Networks subscriptions are detecting. See if you need to refine the subscription settings or security rule settings to close any security gaps.
- Shows you industry data to gives you perspective on the threat landscape you're facing and how you stack up against your peer.



Time Range: Past 30 Days

Your Security Subscriptions

FULL COVERAGE

These subscriptions are actively securing all the next-gen firewalls connected to Device Insights.

THREAT PREVENTION 36 Active 111 No License	24.4M THREATS BLOCKED
URL FILTERING 36 Active 111 No License	14.0M MALICIOUS URLS
ENTERPRISE DLP 11 Active 136 No License	0 FILES BLOCKED
WILDFIRE 32 Active 115 No License	98.5K MALICIOUS VERDICTS

Security Subscription Coverage

To show you how your Palo Alto Networks subscriptions are protecting you, we've processed over 28.6 TB of your traffic and monitored the 691 applications that you've used over the past 30 days.

This report breaks down all the malicious activity that the active Palo Alto Networks subscriptions are detecting.

We also show you industry data to gives you perspective on the threat landscape you're facing and how you stack up against your peers.

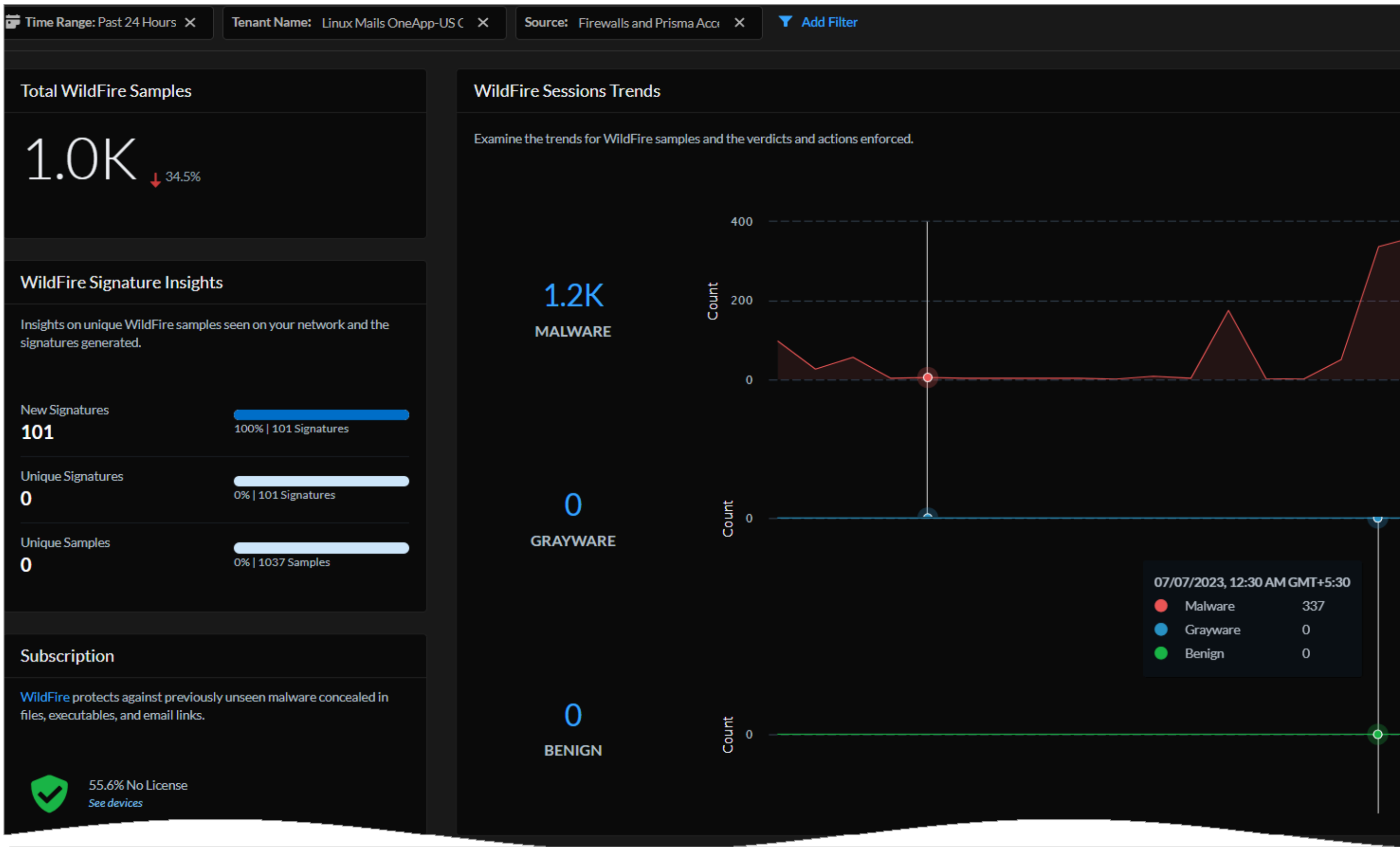
For more information, see Dashboard: Executive Summary.

Monitor WildFire

Where Can I Use This?	What Do I Need?
• NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series, funded with Software NGFW Credits	• Minimum requirement: □ AIOps for NGFW Free (use the AIOps for NGFW Free or AIOps for NGFW Premium license (use the Strata Clou □ Advanced WildFire license □ A role that has permission to view the dashboard • License to view data from supported product in the dashboard: Prisma Access

The WildFire dashboard shows you how WildFire is protecting you from net new malware that's concealed in files, executables, and email links. Use this dashboard to-

- monitor WildFire submissions and get details of WildFire samples submitted to WildFire cloud for analysis.
- view details of targeted users, the applications that delivered the files, the firewalls that submitted the samples for analysis, and all URLs involved in the command-and-control activity of the files.
- view WildFire logs and analysis report and refine the WildFire settings for your deployment based on the report.



Time Range: Past 24 Hours ✕ | Tenant Name: Linux Mails OneApp-US C ✕ | Source: Firewalls and Prisma Acc ✕ | Add Filter

Total WildFire Samples

1.0K ↓ 34.5%

WildFire Signature Insights

Insights on unique WildFire samples seen on your network and the signatures generated.

New Signatures	101	100% | 101 Signatures
Unique Signatures	0	0% | 101 Signatures
Unique Samples	0	0% | 1037 Samples

Subscription

WildFire protects against previously unseen malware concealed in files, executables, and email links.

55.6% No License
See devices

WildFire Sessions Trends

Examine the trends for WildFire samples and the verdicts and actions enforced.

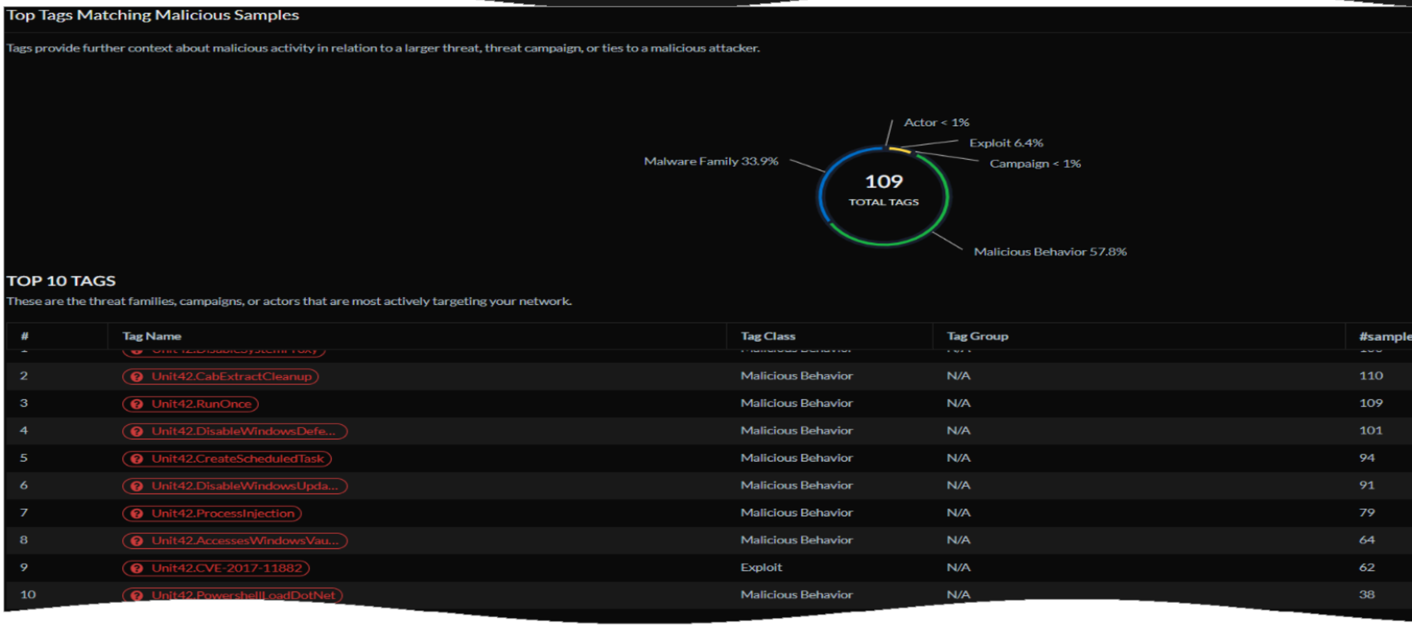
1.2K MALWARE

0 GRAYWARE

0 BENIGN

07/07/2023, 12:30 AM GMT+5:30

🔴 Malware	337
🔵 Grayware	0
🟢 Benign	0



Top Tags Matching Malicious Samples

Tags provide further context about malicious activity in relation to a larger threat, threat campaign, or ties to a malicious attacker.

TOP 10 TAGS

These are the threat families, campaigns, or actors that are most actively targeting your network.

#	Tag Name	Tag Class	Tag Group	#sample
1	[illegible]	Malicious Behavior	N/A	[illegible]
2	Unit42.CabExtractCleanup	Malicious Behavior	N/A	110
3	Unit42.RunOnce	Malicious Behavior	N/A	109
4	Unit42.DisableWindowsDefe...	Malicious Behavior	N/A	101
5	Unit42.CreateScheduledTask	Malicious Behavior	N/A	94
6	Unit42.DisableWindowsUpda...	Malicious Behavior	N/A	91
7	Unit42.ProcessInjection	Malicious Behavior	N/A	79
8	Unit42.AccessesWindowsVau...	Malicious Behavior	N/A	64
9	Unit42.CVE-2017-11882	Exploit	N/A	62
10	Unit42.PowershellLoadDotNet	Malicious Behavior	N/A	38

AIOps Premium customers can also view WildFire data in the Strata Cloud Manager Command Center. For more information, see Dashboard: WildFire.

Monitor DNS Security

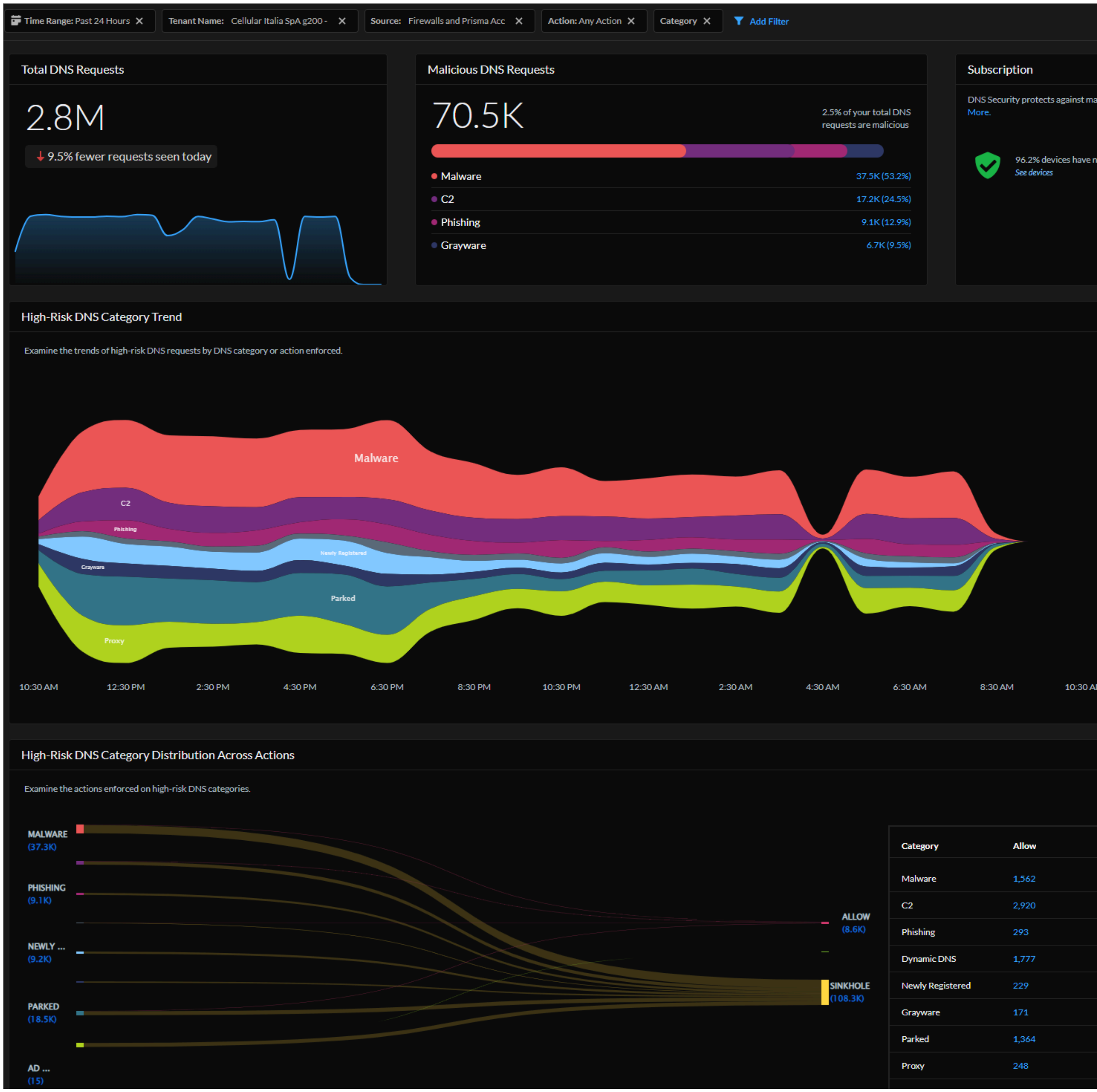
Where Can I Use This?	What Do I Need?
• NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series, funded with Software NGFW Credits	• Minimum requirement: □ AIOps for NGFW Free (use the AIOps for NGFW Free or AIOps for NGFW Premium license (use the Strata Clou □ DNS Security license □ A role that has permission to view the dashboard • License to view data from supported product in the dashboard: Prisma Access

The **DNS Security** dashboard shows you how your DNS Security subscription is protecting you from advanced threats and malware that use DNS. You can also filter the information displayed on the dashboard by time range, action taken, domain, resolver IP, and DNS category. The source and tenant name for which the data is displayed on the dashboard are shown in the Tenant Name and Source filters. You can view:

- DNS request statistics and trends
- number of devices with a DNS Security license)
- DNS activity associated with malicious domains
- breakdown of DNS-based malware and request types

This dashboard helps you to:

- examine how DNS requests are processed and categorized
- get insight into the DNS based threats



Time Range: Past 24 Hours ✕ | Tenant Name: Cellular Italia SpA g200 - ✕ | Source: Firewalls and Prisma Acc ✕ | Action: Any Action ✕ | Category ✕ | Add Filter

Total DNS Requests

2.8M

↓ 9.5% fewer requests seen today

Malicious DNS Requests

70.5K

2.5% of your total DNS requests are malicious

● Malware	37.5K (53.2%)
● C2	17.2K (24.5%)
● Phishing	9.1K (12.9%)
● Grayware	6.7K (9.5%)

Subscription

DNS Security protects against ma
More.

96.2% devices have n
See devices

High-Risk DNS Category Trend

Examine the trends of high-risk DNS requests by DNS category or action enforced.

High-Risk DNS Category Distribution Across Actions

Examine the actions enforced on high-risk DNS categories.

Category	Allow
Malware	1,562
C2	2,920
Phishing	293
Dynamic DNS	1,777
Newly Registered	229
Grayware	171
Parked	1,364
Proxy	248

AIOps Premium customers can also view DNS Security data in the Strata Cloud Manager Command Center. For more information, see Dashboard: DNS Security.

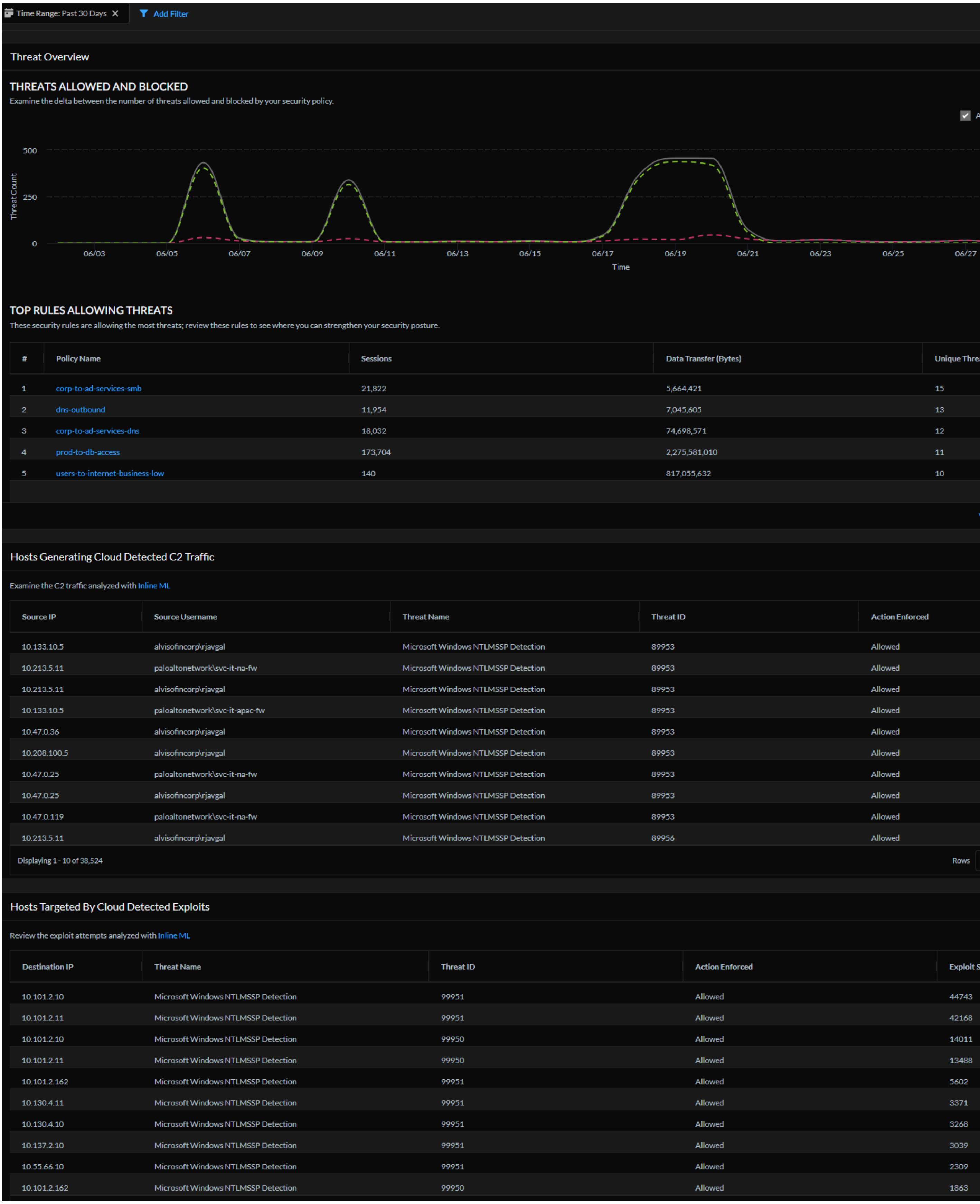
Monitor Advanced Threat Prevention

Where Can I Use This?	What Do I Need?
• NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series, funded with Software NGFW Credits	Minimum requirement: □ AIOps for NGFW Free (use the AIOps for NGFW Free ap or AIOps for NGFW Premium license (use the Strata Cloud □ Strata Logging Service license □ A role that has permission to view the dashboard

The Advanced Threat Prevention dashboard gives insight into threats detected in your network and identifies opportunities to strengthen your security posture. Threats are detected using inline cloud analysis models and threat signatures generated from malicious traffic data collected from various Palo Alto Networks services. This dashboard provides a timeline view of threats allowed and blocked and a list of hosts generating cloud-detected C2 traffic and hosts targeted by cloud-detected exploits.

Use this dashboard to:

- get threat visibility in your network traffic
- analyze threat sessions to improve the accuracy of your policy rules
- gain insight into the real-time threat detected by inline cloud analysis
- get context around the threat from logs and cloud reports and use this data to improve your incident response process.



Threat Overview

THREATS ALLOWED AND BLOCKED

Examine the delta between the number of threats allowed and blocked by your security policy.

TOP RULES ALLOWING THREATS

These security rules are allowing the most threats; review these rules to see where you can strengthen your security posture.

#	Policy Name	Sessions	Data Transfer (Bytes)	Unique Threa
1	corp-to-ad-services-smb	21,822	5,664,421	15
2	dns-outbound	11,954	7,045,605	13
3	corp-to-ad-services-dns	18,032	74,698,571	12
4	prod-to-db-access	173,704	2,275,581,010	11
5	users-to-internet-business-low	140	817,055,632	10

Hosts Generating Cloud Detected C2 Traffic

Examine the C2 traffic analyzed with Inline ML

Source IP	Source Username	Threat Name	Threat ID	Action Enforced
10.133.10.5	alvisofincorp\rjavgal	Microsoft Windows NTLMSSP Detection	89953	Allowed
10.213.5.11	paloaltonetwork\svc-it-na-fw	Microsoft Windows NTLMSSP Detection	89953	Allowed
10.213.5.11	alvisofincorp\rjavgal	Microsoft Windows NTLMSSP Detection	89953	Allowed
10.133.10.5	paloaltonetwork\svc-it-apac-fw	Microsoft Windows NTLMSSP Detection	89953	Allowed
10.47.0.36	alvisofincorp\rjavgal	Microsoft Windows NTLMSSP Detection	89953	Allowed
10.208.100.5	alvisofincorp\rjavgal	Microsoft Windows NTLMSSP Detection	89953	Allowed
10.47.0.25	paloaltonetwork\svc-it-na-fw	Microsoft Windows NTLMSSP Detection	89953	Allowed
10.47.0.25	alvisofincorp\rjavgal	Microsoft Windows NTLMSSP Detection	89953	Allowed
10.47.0.119	paloaltonetwork\svc-it-na-fw	Microsoft Windows NTLMSSP Detection	89953	Allowed
10.213.5.11	alvisofincorp\rjavgal	Microsoft Windows NTLMSSP Detection	89956	Allowed

Displaying 1 - 10 of 38,524

Rows

Hosts Targeted By Cloud Detected Exploits

Review the exploit attempts analyzed with Inline ML

Destination IP	Threat Name	Threat ID	Action Enforced	Exploit S
10.101.2.10	Microsoft Windows NTLMSSP Detection	99951	Allowed	44743
10.101.2.11	Microsoft Windows NTLMSSP Detection	99951	Allowed	42168
10.101.2.10	Microsoft Windows NTLMSSP Detection	99950	Allowed	14011
10.101.2.11	Microsoft Windows NTLMSSP Detection	99950	Allowed	13488
10.101.2.162	Microsoft Windows NTLMSSP Detection	99951	Allowed	5602
10.130.4.11	Microsoft Windows NTLMSSP Detection	99951	Allowed	3371
10.130.4.10	Microsoft Windows NTLMSSP Detection	99951	Allowed	3268
10.137.2.10	Microsoft Windows NTLMSSP Detection	99951	Allowed	3039
10.55.66.10	Microsoft Windows NTLMSSP Detection	99951	Allowed	2309
10.101.2.162	Microsoft Windows NTLMSSP Detection	99950	Allowed	1863

AIOps Premium customers can also view Advanced Threat Prevention data in the Strata Cloud Manager Command Center. For more information, see Dashboard: Advanced Threat Prevention.

Optimize Security Posture

Where Can I Use This?	What Do I Need?
• NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series, funded with Software NGFW Credits	• AIOps for NGFW Free (use the AIOps for NGFW Free ap or • AIOps for NGFW Premium license (use the Strata Cloud

In addition to helping you keep your firewalls functionally healthy, AIOps for NGFW aids in verifying that they are providing you with effective protection against security threats.

Security posture assessments currently don't support multiple virtual systems; only the default virtual system (vsys1) is considered during configuration processing.

- Monitor Security Posture Insights: Get visibility into the security status and trend of your deployment based on the security postures of the onboarded NGFW devices.
- Monitor Feature Adoption: View the security features that you're using in your deployment.
- Monitor Feature Configuration: View whether your security features are configured according to Palo Alto Networks best practices.
- Monitor Security Advisories: View the number of devices impacted by a specific vulnerability based on the features that have been enabled on the devices.
- Monitor Security Subscriptions: View the recommended Cloud-Delivered Security Services (CDSS) subscriptions and their usage in your devices.
- Assess Vulnerabilities: View the vulnerabilities impacting a specific firewall and PAN-OS version, aiding in your decision-making process regarding whether an upgrade is necessary.
- Build a Custom Dashboard: Create custom dashboards to get visibility into areas of your interest in your network using widgets.
- Monitor Compliance Summary: View a history of changes to the security checks made up to 12 months in the past, grouped together by the Center for Internet Security (CIS) and the National Institute of Standards and Technology (NIST) frameworks.
- Configure Security Checks And Other Posture Settings: Customize security posture checks for your deployment to maximize relevant recommendations.
- Proactively Enforce Security Checks: Take proactive measures against suboptimal configurations by blocking commits that don't pass particular best practice checks.
- Policy Analyzer: Get analysis and suggestions for possible consolidation or removal of specific policy rules to meet your intended Security posture, as well as checks for anomalies, such as shadows, redundancies, generalizations, correlations, and consolidations in your rulebase.

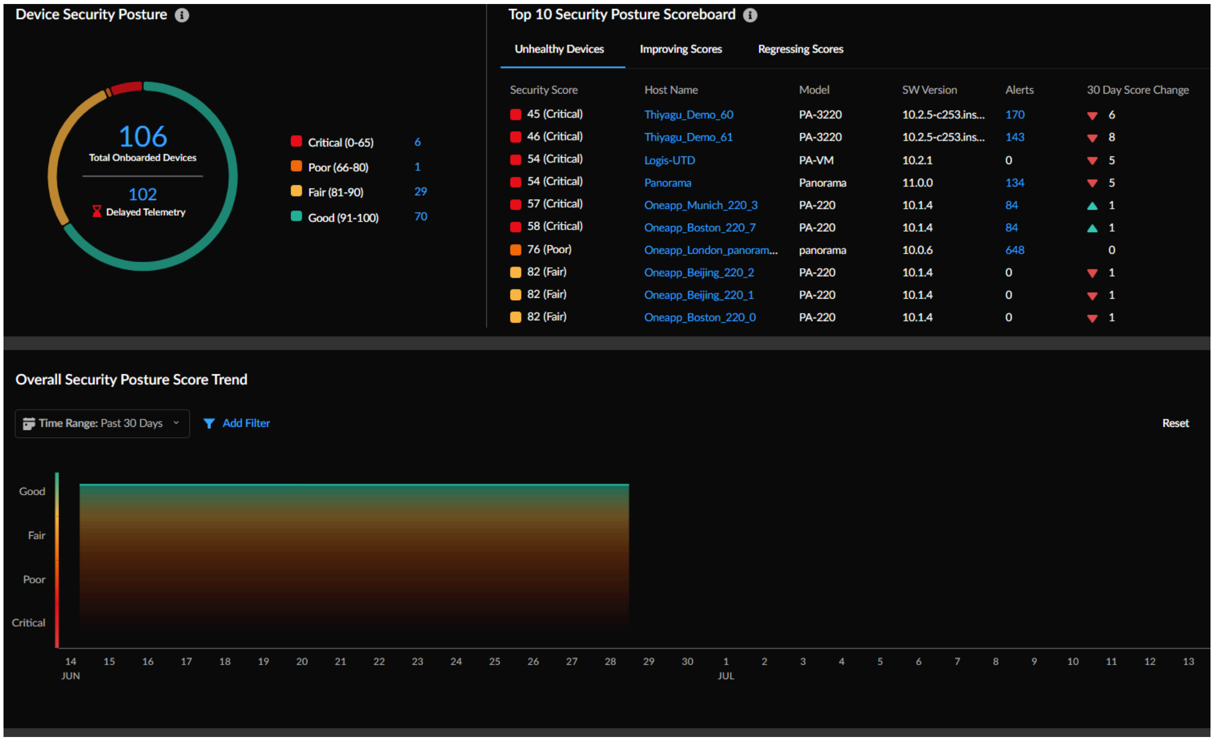
Monitor Security Posture Insights

Where Can I Use This?	What Do I Need?
• NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series, funded with Software NGFW Credits	□ AIOps for NGFW Free (use the AIOps for NGFW Free ap or AIOps for NGFW Premium license (use the Strata Cloud □ A role that has permission to view the dashboard

You can use the **Security Posture Insights** dashboard to get visibility into the security status and trend of your deployment based on the security postures of the onboarded NGFW devices. The severity of the security score (0-100) and its corresponding security grade (good, fair, poor, critical) determine the security posture of a device. The security score is calculated based on the priority, quantity, type, and status of the open alerts.

Use this dashboard to:

- Know the trend of issues that impact the security posture of your deployment.
- Understand the security improvements that you have made in your deployment by looking at the historical security score data.
- Narrow down devices where there is an opportunity to improve the security posture and prioritize the issues to resolve them.



🟥 Critical (0-65)	6
🟧 Poor (66-80)	1
🟨 Fair (81-90)	29
🟩 Good (91-100)	70

Security Score	Host Name	Model	SW Version	Alerts	30 Day Score Change
🟥 45 (Critical)	Thiyagu_Demo_60	PA-3220	10.2.5-c253.ins...	170	▼ 6
🟥 46 (Critical)	Thiyagu_Demo_61	PA-3220	10.2.5-c253.ins...	143	▼ 8
🟥 54 (Critical)	Logis-UTD	PA-VM	10.2.1	0	▼ 5
🟥 54 (Critical)	Panorama	Panorama	11.0.0	134	▼ 5
🟥 57 (Critical)	Oneapp_Munich_220_3	PA-220	10.1.4	84	▲ 1
🟥 58 (Critical)	Oneapp_Boston_220_7	PA-220	10.1.4	84	▲ 1
🟧 76 (Poor)	Oneapp_London_panoram...	panorama	10.0.6	648	0
🟨 82 (Fair)	Oneapp_Beijing_220_2	PA-220	10.1.4	0	▼ 1
🟨 82 (Fair)	Oneapp_Beijing_220_1	PA-220	10.1.4	0	▼ 1
🟨 82 (Fair)	Oneapp_Boston_220_0	PA-220	10.1.4	0	▼ 1

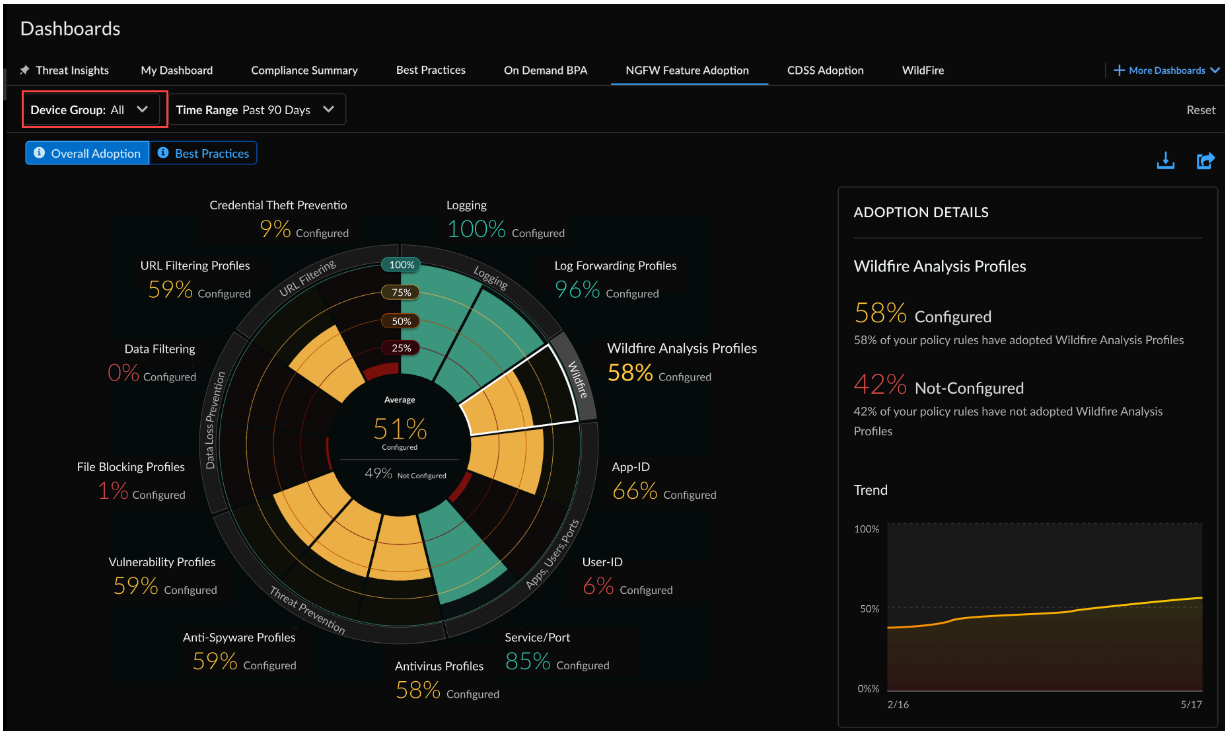
For more information, see Dashboard: Security Posture Insights.

Monitor Feature Adoption

Where Can I Use This?	What Do I Need?
• NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series, funded with Software NGFW Credits	□ AIOps for NGFW Free (use the AIOps for NGFW Free ap or AIOps for NGFW Premium license (use the Strata Cloud □ A role that has permission to view the dashboard

In **Dashboards** > **Feature Adoption**, you can view the security features that you are using in your deployment. This helps you make sure that you are getting the most out of your Palo Alto Networks security subscriptions and firewall features.

- To focus on the feature adoption for a specific set of firewalls, you can filter the chart based on device group, including Panorama-managed devices. You can also see historical adoption trend charts.



Device Group: All

Time Range Past 90 Days

ADOPTION DETAILS

Wildfire Analysis Profiles

58% Configured

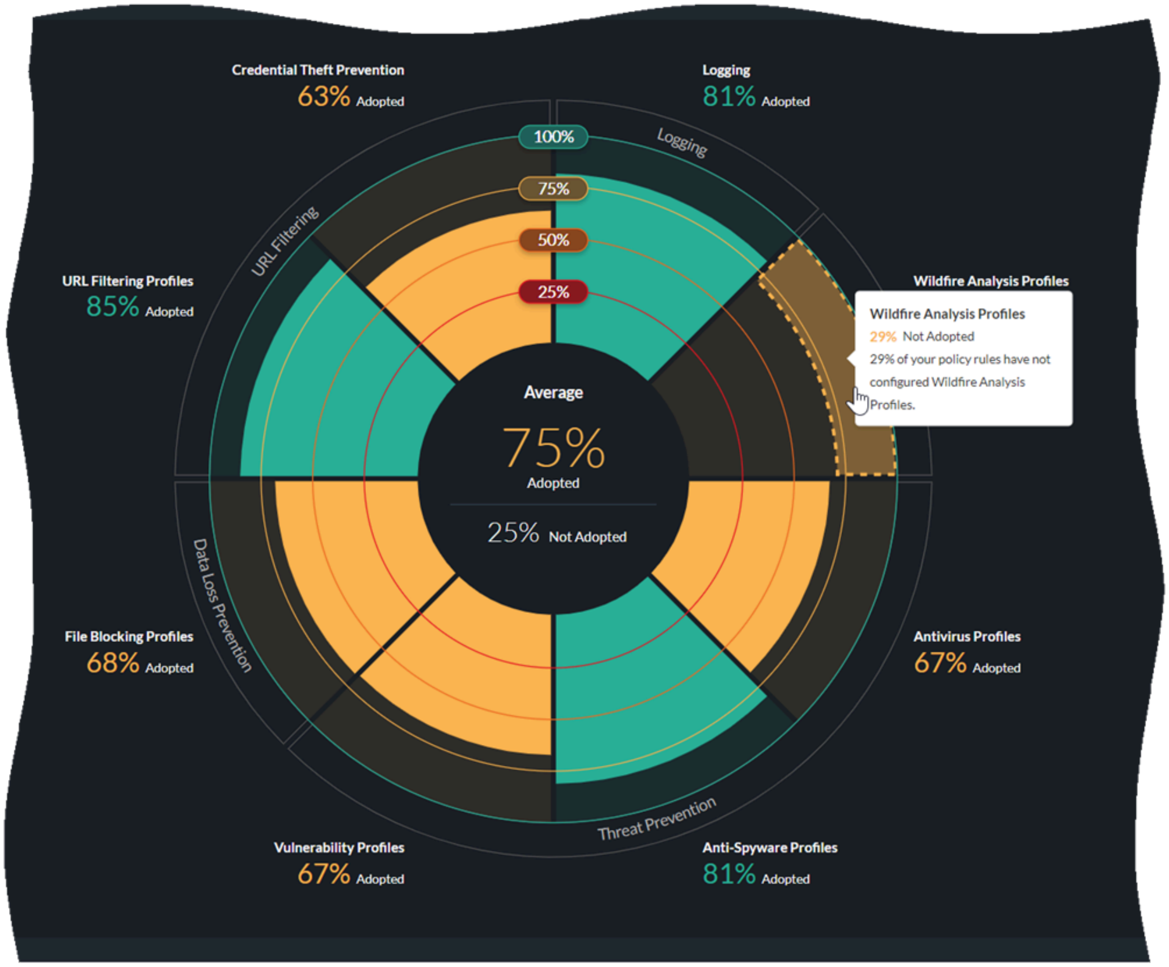
58% of your policy rules have adopted Wildfire Analysis Profiles

42% Not-Configured

42% of your policy rules have not adopted Wildfire Analysis Profiles

- *When you generate an On-Demand BPA report using a TSF, adoption information from your TSF is reflected on the Feature Adoption dashboard. (PAN-OS 9.1 and above TSFs)*
- *You can export adoption data in .csv format for use in third-party applications such as Microsoft Excel*

- Select the section for a feature on the chart to view which policy rules lack that feature.

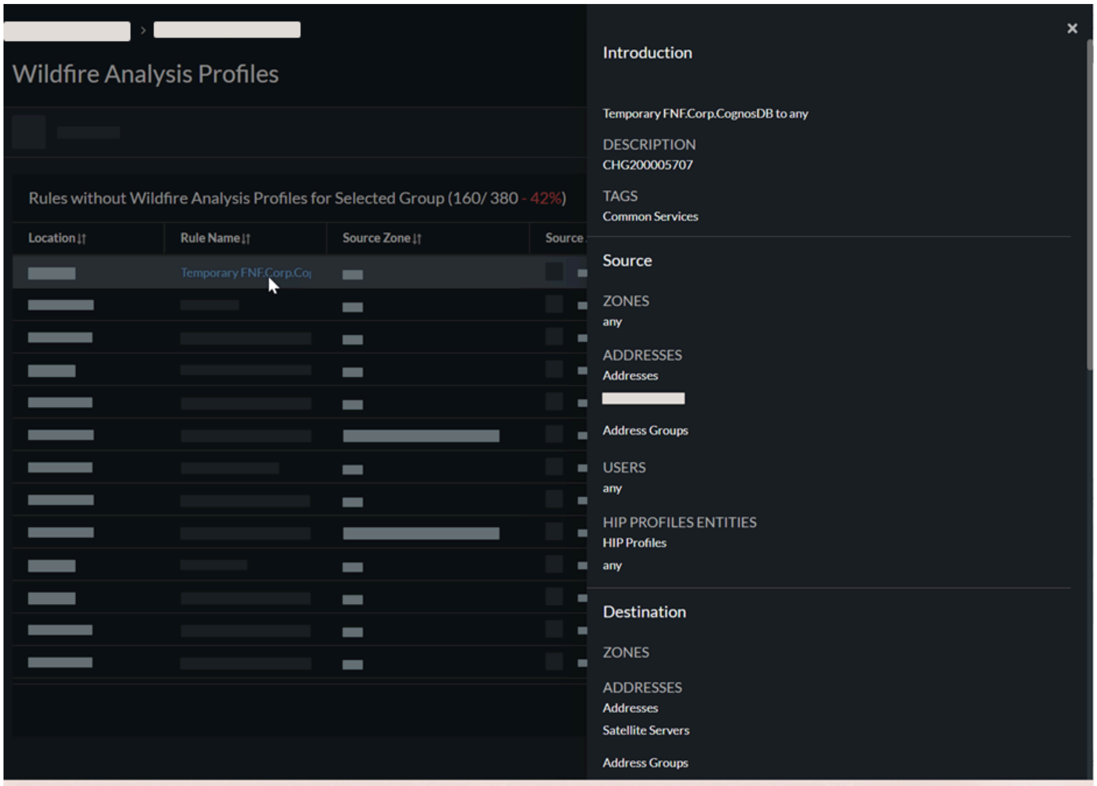


Wildfire Analysis Profiles

29% Not Adopted

29% of your policy rules have not configured Wildfire Analysis Profiles.

- Select a rule to view its details without needing to leave the app.



[redacted] › [redacted]

Wildfire Analysis Profiles

Rules without Wildfire Analysis Profiles for Selected Group (160/ 380 - 42%)

Location	Rule Name	Source Zone	Source
[redacted]	Temporary FNF.Corp.Co	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

Introduction

Temporary FNF.Corp.CognosDB to any

DESCRIPTION
CHG200005707

TAGS
Common Services

Source

ZONES
any

ADDRESSES
Addresses
[redacted]

Address Groups

USERS
any

HIP PROFILES ENTITIES
HIP Profiles
any

Destination

ZONES

ADDRESSES
Addresses
Satellite Servers

Address Groups

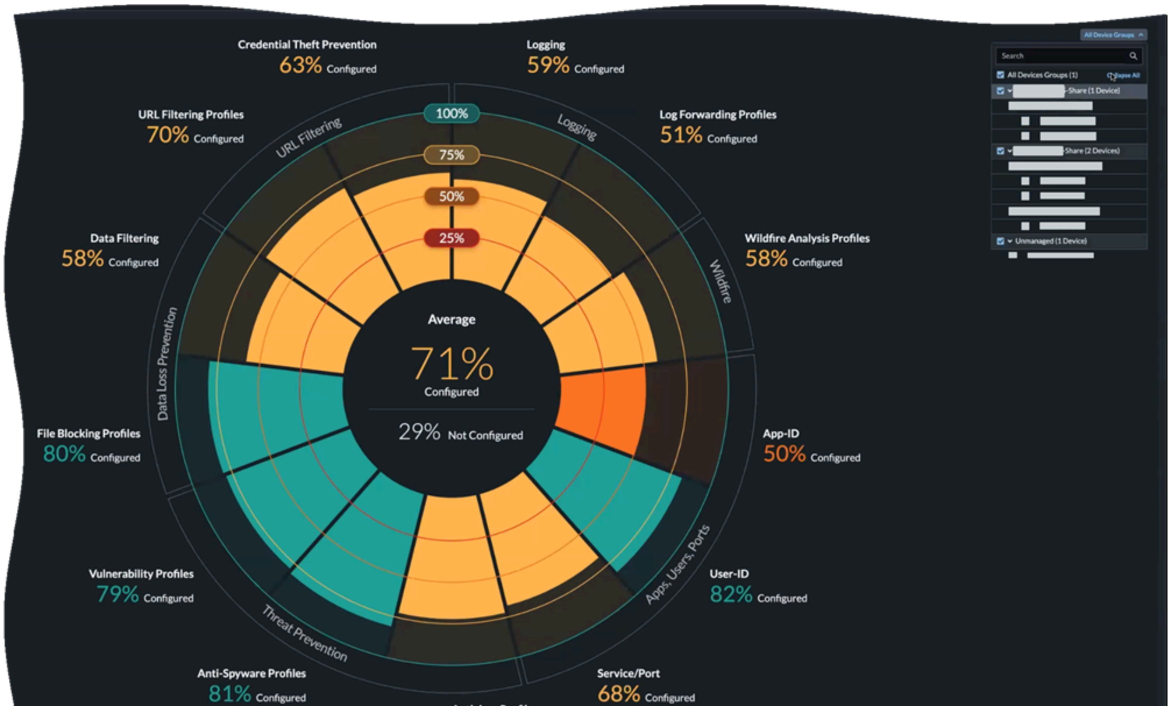
For more information, see Dashboard: Feature Adoption.

Monitor Feature Configuration

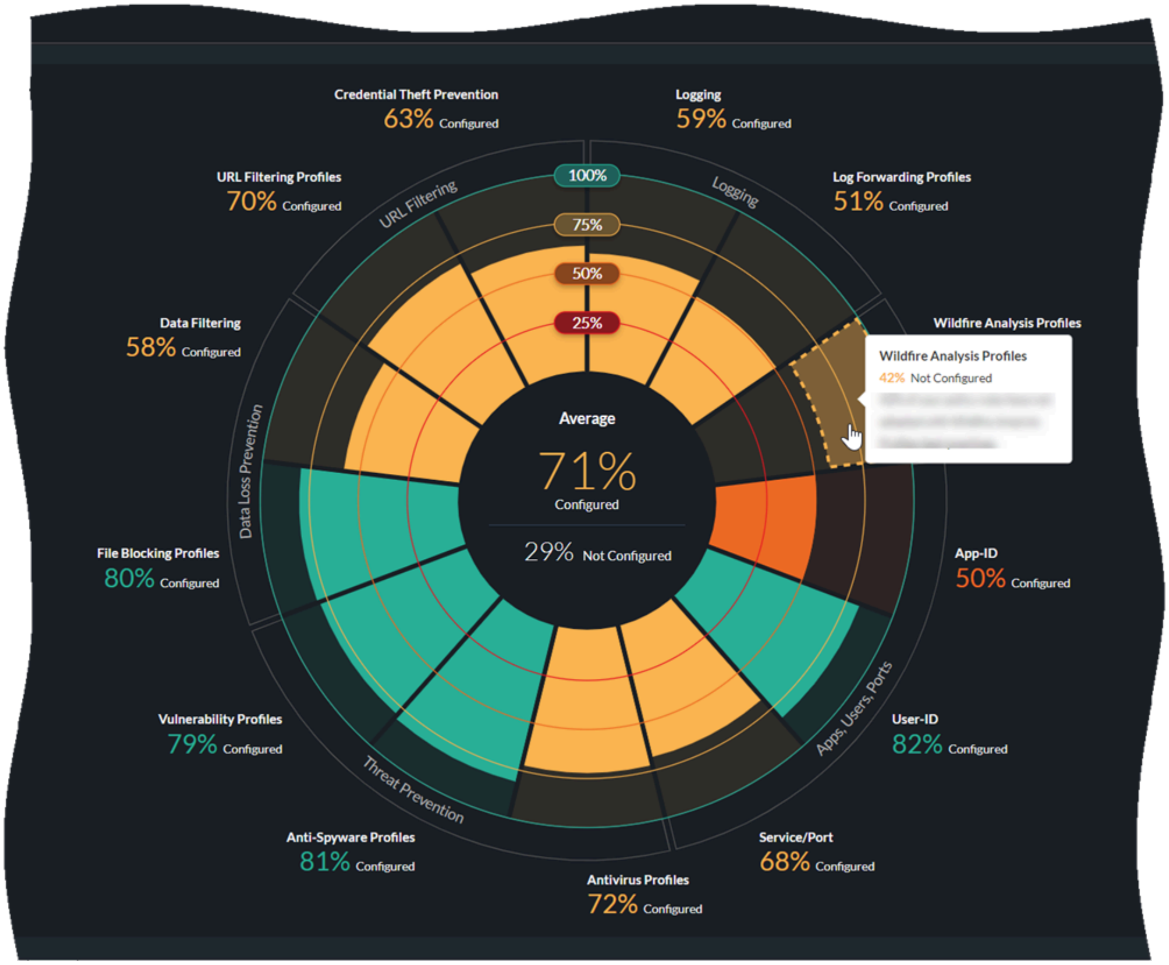
Where Can I Use This?	What Do I Need?
• NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series, funded with Software NGFW Credits	□ AIOps for NGFW Free (use the AIOps for NGFW Free ap or AIOps for NGFW Premium license (use the Strata Cloud □ A role that has permission to view the dashboard

In **Dashboard** > **Feature Adoption**, you can view whether your security features are configured according to Palo Alto Networks best practices by selecting **Best Practices**.

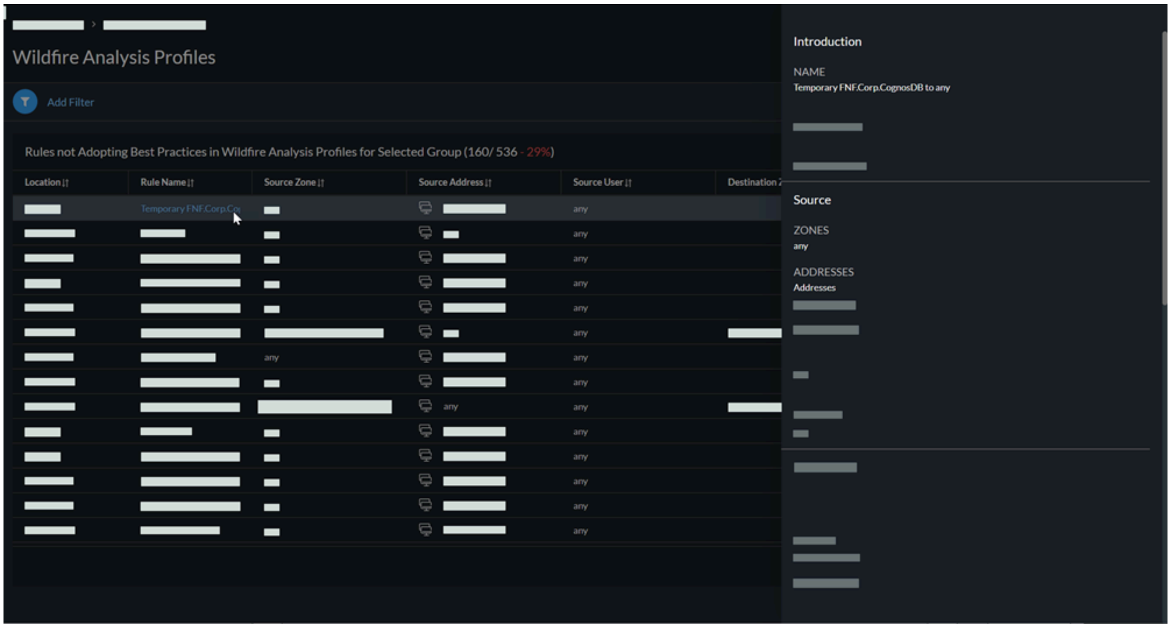
◉ To focus on best practice compliance for a specific set of firewalls, you can filter the chart based on device group.



- Select the section for a feature on the chart to view which policy rules can be improved.



- Select a rule to view its details without needing to leave the app.


[redacted] > [redacted]

Wildfire Analysis Profiles

Add Filter

Rules not Adopting Best Practices in Wildfire Analysis Profiles for Selected Group (160/ 536 - 29%)

Location	Rule Name	Source Zone	Source Address	Source User	Destination Z
[redacted]	Temporary FNF.Corp.Co	[redacted]	[redacted]	any	
[redacted]	[redacted]	[redacted]	[redacted]	any	
[redacted]	[redacted]	[redacted]	[redacted]	any	
[redacted]	[redacted]	[redacted]	[redacted]	any	
[redacted]	[redacted]	[redacted]	[redacted]	any	
[redacted]	[redacted]	[redacted]	[redacted]	any	[redacted]
[redacted]	[redacted]	any	[redacted]	any	
[redacted]	[redacted]	[redacted]	[redacted]	any	
[redacted]	[redacted]	[redacted]	any	any	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	any	
[redacted]	[redacted]	[redacted]	[redacted]	any	
[redacted]	[redacted]	[redacted]	[redacted]	any	
[redacted]	[redacted]	[redacted]	[redacted]	any	
[redacted]	[redacted]	[redacted]	[redacted]	any	

Introduction

NAME
Temporary FNF.Corp.CognosDB to any

[redacted]

Source

ZONES
any

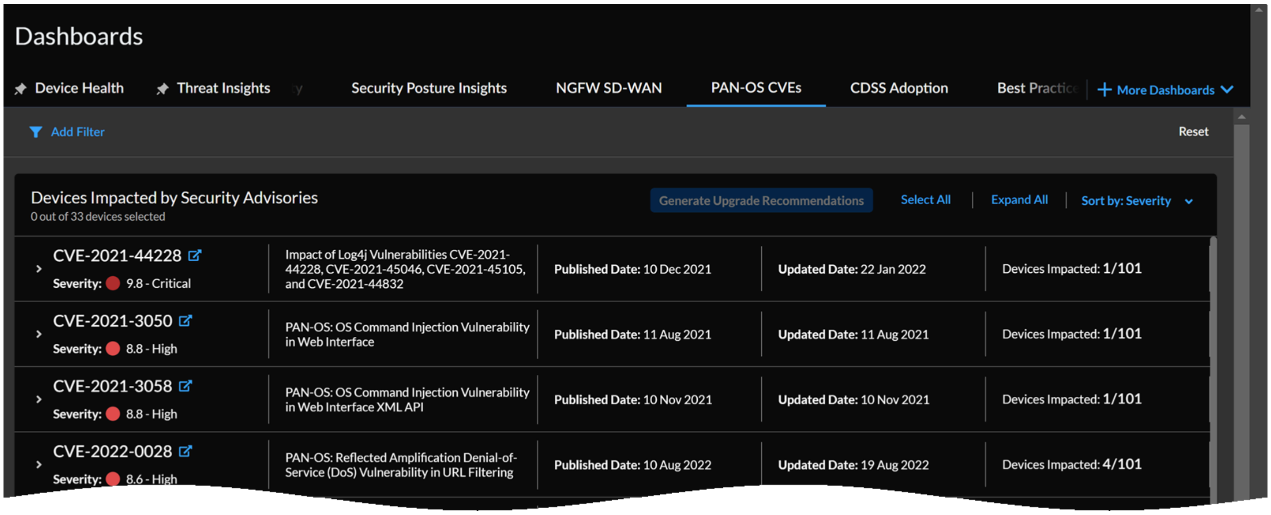
ADDRESSES
Addresses

[redacted]

Monitor Security Advisories

Where Can I Use This?	What Do I Need?
- NGFW (Managed by Strata Cloud Manager) - NGFW (Managed by PAN-OS or Panorama) - VM-Series, funded with Software NGFW Credits	□ AIOps for NGFW Free (use the AIOps for NGFW Free ap or AIOps for NGFW Premium license (use the Strata Cloud for generating upgrade recommendations. □ A role that has permission to view the dashboard

In **Dashboards** > **PAN-OS CVEs**, you can view the number of devices impacted by a specific vulnerability based on the features that have been enabled on devices. Strata Cloud Manager analyzes the features that have been enabled to determine the devices impacted by the CVE. This helps you decide which devices to upgrade to mitigate the vulnerability. Expand a CVE to view details about an impacted device such as Host Name, Model, Serial Number, SW Version, and Last Telemetry Update. You can filter CVEs by using these details and sort them further by **Severity** or **Devices Impacted**. You can click a CVE to view the advisory associated with it.



Devices Impacted by Security Advisories
0 out of 33 devices selected

CVE-2021-44228 Severity: ● 9.8 - Critical	Impact of Log4j Vulnerabilities CVE-2021-44228, CVE-2021-45046, CVE-2021-45105, and CVE-2021-44832	**Published Date:** 10 Dec 2021	**Updated Date:** 22 Jan 2022	Devices Impacted: **1/101**
CVE-2021-3050 Severity: ● 8.8 - High	PAN-OS: OS Command Injection Vulnerability in Web Interface	**Published Date:** 11 Aug 2021	**Updated Date:** 11 Aug 2021	Devices Impacted: **1/101**
CVE-2021-3058 Severity: ● 8.8 - High	PAN-OS: OS Command Injection Vulnerability in Web Interface XML API	**Published Date:** 10 Nov 2021	**Updated Date:** 10 Nov 2021	Devices Impacted: **1/101**
CVE-2022-0028 Severity: ● 8.6 - High	PAN-OS: Reflected Amplification Denial-of-Service (DoS) Vulnerability in URL Filtering	**Published Date:** 10 Aug 2022	**Updated Date:** 19 Aug 2022	Devices Impacted: **4/101**

After you understand the vulnerabilities for impacted devices, you can plan your patching using the Software Upgrade Recommendations feature. Expand the CVEs and select firewalls that you want to upgrade to fix the vulnerabilities, and click **Generate Upgrade Recommendations**. You are redirected to Software Upgrade Recommendations to view the generated report.

For more information, see Dashboard: PAN-OS CVEs.

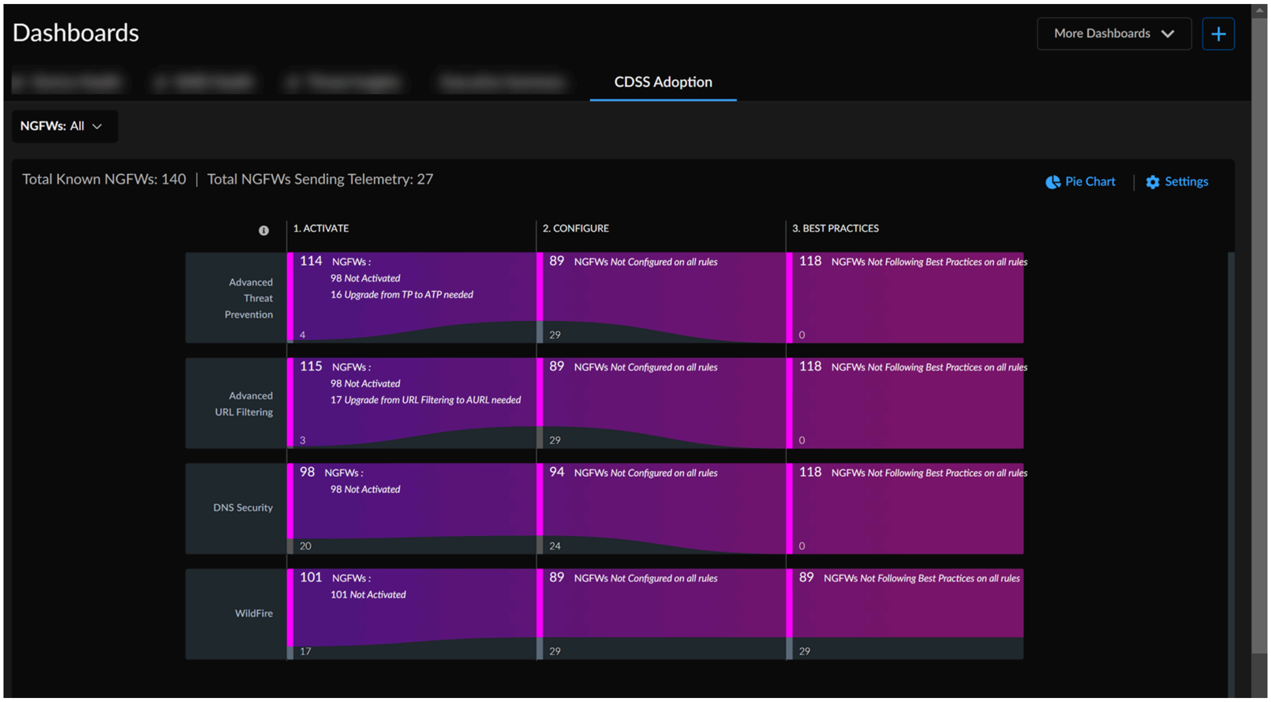
Monitor Security Subscriptions

Where Can I Use This?	What Do I Need?
- NGFW (Managed by Strata Cloud Manager) - NGFW (Managed by PAN-OS or Panorama) - VM-Series, funded with Software NGFW Credits	□ AIOps for NGFW Free (use the AIOps for NGFW Free ap or AIOps for NGFW Premium license (use the Strata Cloud □ A role that has permission to view the dashboard

In **Dashboard** > **Posture** > **CDSS Adoption**, you can view the recommended Cloud-Delivered Security Services (CDSS) subscriptions and their usage in your devices. This helps you to identify security gaps and harden the security posture of your enterprise. After you navigate to this page, you will see a pop-up asking you to confirm or update your zone roles in NGFWs to get accurate security services recommendations. You can follow the link in this pop-up window to map zones to roles.

Currently, this dashboard only supports four security subscriptions: Advanced Threat Prevention, Advanced URL Filtering, DNS Security and Wildfire.

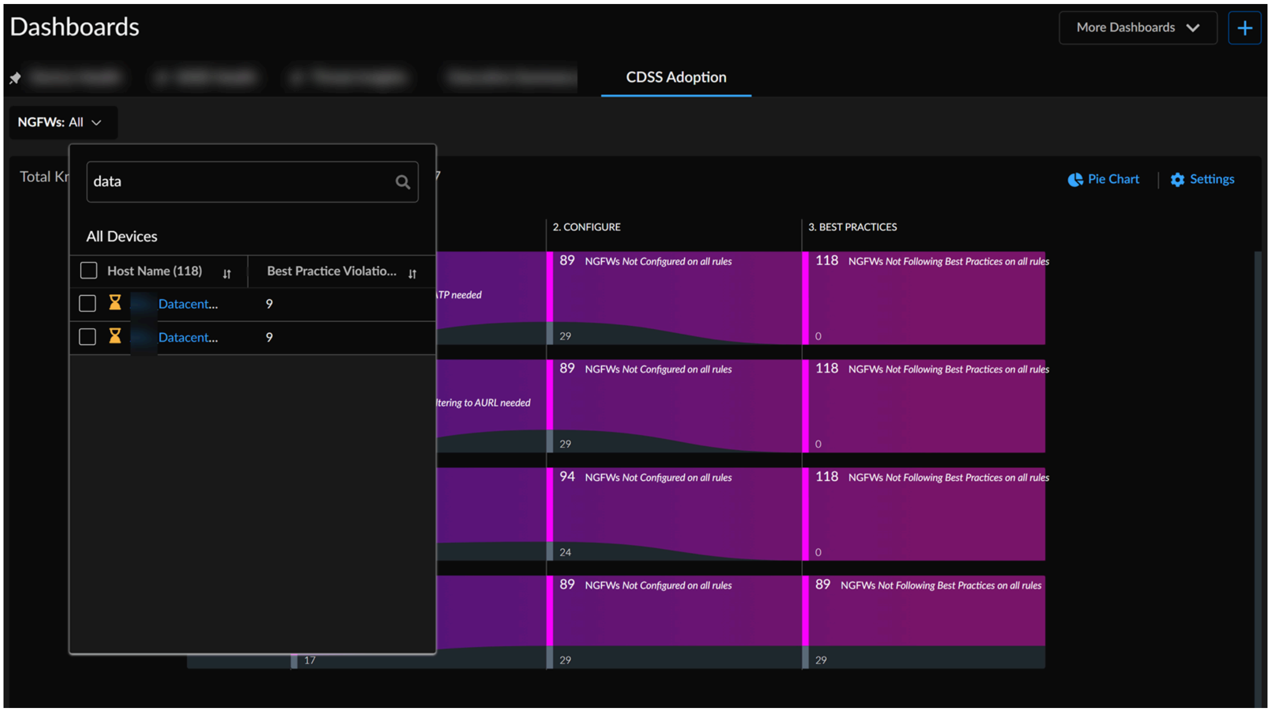
At the top of the Overview page, you can view the number of total known NGFWs and number of NGFWs sending telemetry in your AIOps for NGFW instance. The adoption of CDSS involves progressing through activation, configuration, and adherence to best practices. To track progress for each subscription, simply click on the numbers in the chart to view a list of devices that require updates along this journey. To use a security subscription license in a device, you need to activate it and then set up the service or feature accordingly.



Total Known NGFWs: 140 | Total NGFWs Sending Telemetry: 27

	1. ACTIVATE	2. CONFIGURE	3. BEST PRACTICES
Advanced Threat Prevention	114 NGFWs : 98 Not Activated 16 Upgrade from TP to ATP needed 4	89 NGFWs Not Configured on all rules 29	118 NGFWs Not Following Best Practices on all rules 0
Advanced URL Filtering	115 NGFWs : 98 Not Activated 17 Upgrade from URL Filtering to AURL needed 3	89 NGFWs Not Configured on all rules 29	118 NGFWs Not Following Best Practices on all rules 0
DNS Security	98 NGFWs : 98 Not Activated 20	94 NGFWs Not Configured on all rules 24	118 NGFWs Not Following Best Practices on all rules 0
WildFire	101 NGFWs : 101 Not Activated 17	89 NGFWs Not Configured on all rules 29	89 NGFWs Not Following Best Practices on all rules 29

To focus on the security services data for a specific NGFW, filter the chart based on it. You can also view the best practice violations for a device in this drop-down list.

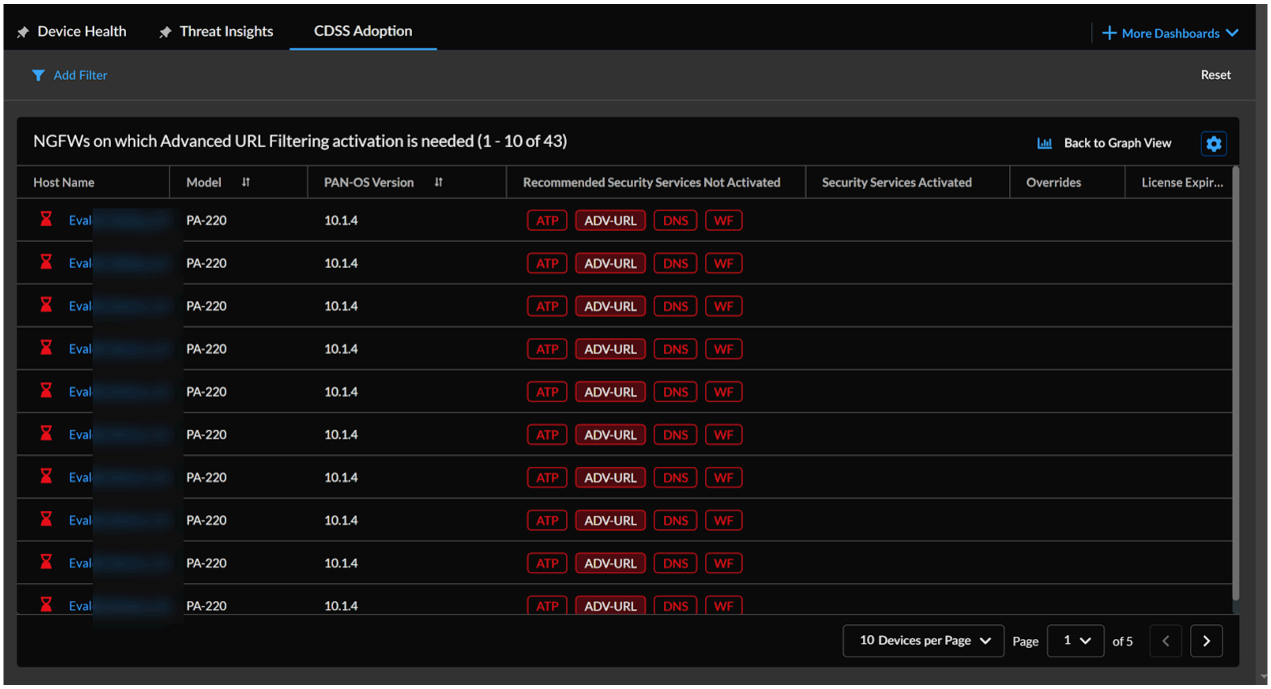

Dashboards
More Dashboards
+
CDSS Adoption
NGFWs: All
Total Kr
Pie Chart
Settings
2. CONFIGURE
3. BEST PRACTICES
TP needed
ltering to AURL needed
89 NGFWs Not Configured on all rules
29
118 NGFWs Not Following Best Practices on all rules
0
89 NGFWs Not Configured on all rules
29
118 NGFWs Not Following Best Practices on all rules
0
94 NGFWs Not Configured on all rules
24
118 NGFWs Not Following Best Practices on all rules
0
17
89 NGFWs Not Configured on all rules
29
89 NGFWs Not Following Best Practices on all rules
29

data

All Devices

☐ Host Name (118)	Best Practice Violatio...
☐ Datacent...	9
☐ Datacent...	9

You can click one of the values under **ACTIVATE**, **CONFIGURE**, or **BEST PRACTICES** to view details in a tabular format.

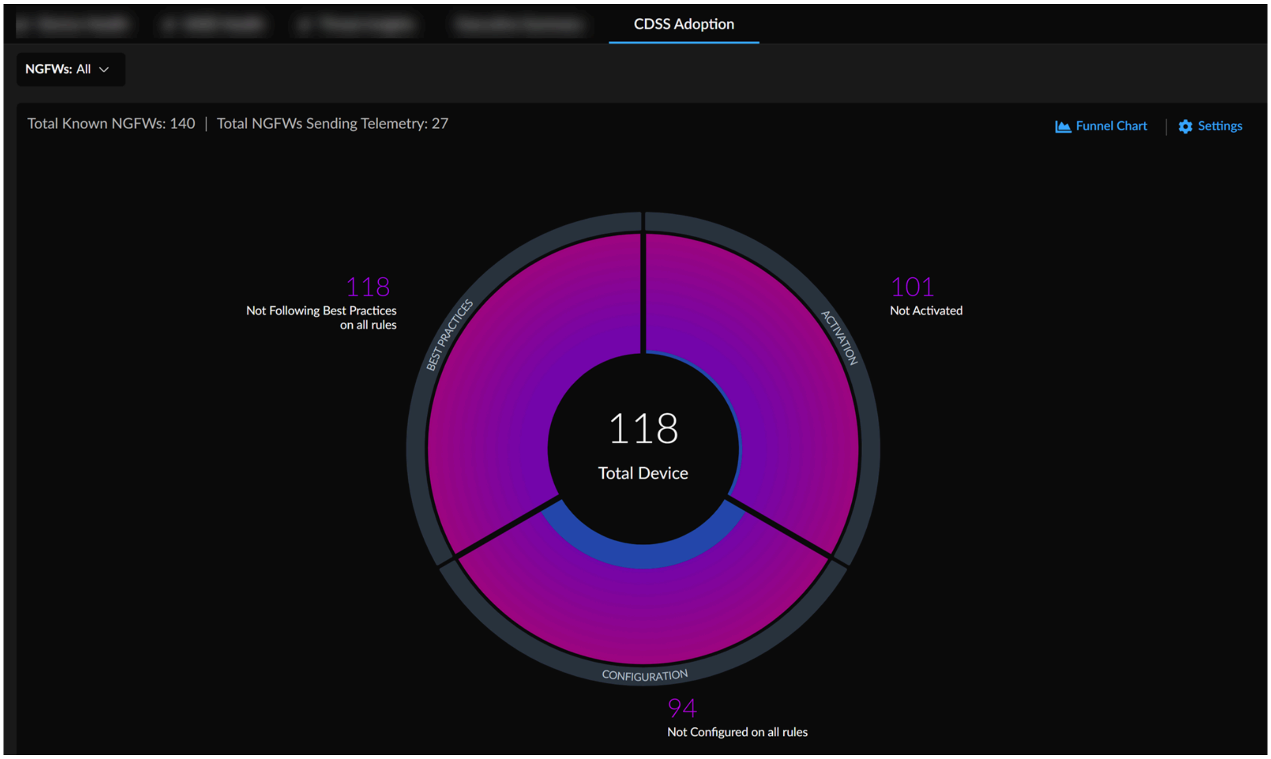


NGFWs on which Advanced URL Filtering activation is needed (1 - 10 of 43)

Host Name	Model	PAN-OS Version	Recommended Security Services Not Activated	Security Services Activated	Overrides	License Expir...
⌛ Eval[redacted]	PA-220	10.1.4	ATP ADV-URL DNS WF			
⌛ Eval[redacted]	PA-220	10.1.4	ATP ADV-URL DNS WF			
⌛ Eval[redacted]	PA-220	10.1.4	ATP ADV-URL DNS WF			
⌛ Eval[redacted]	PA-220	10.1.4	ATP ADV-URL DNS WF			
⌛ Eval[redacted]	PA-220	10.1.4	ATP ADV-URL DNS WF			
⌛ Eval[redacted]	PA-220	10.1.4	ATP ADV-URL DNS WF			
⌛ Eval[redacted]	PA-220	10.1.4	ATP ADV-URL DNS WF			
⌛ Eval[redacted]	PA-220	10.1.4	ATP ADV-URL DNS WF			
⌛ Eval[redacted]	PA-220	10.1.4	ATP ADV-URL DNS WF			
⌛ Eval[redacted]	PA-220	10.1.4	ATP ADV-URL DNS WF			

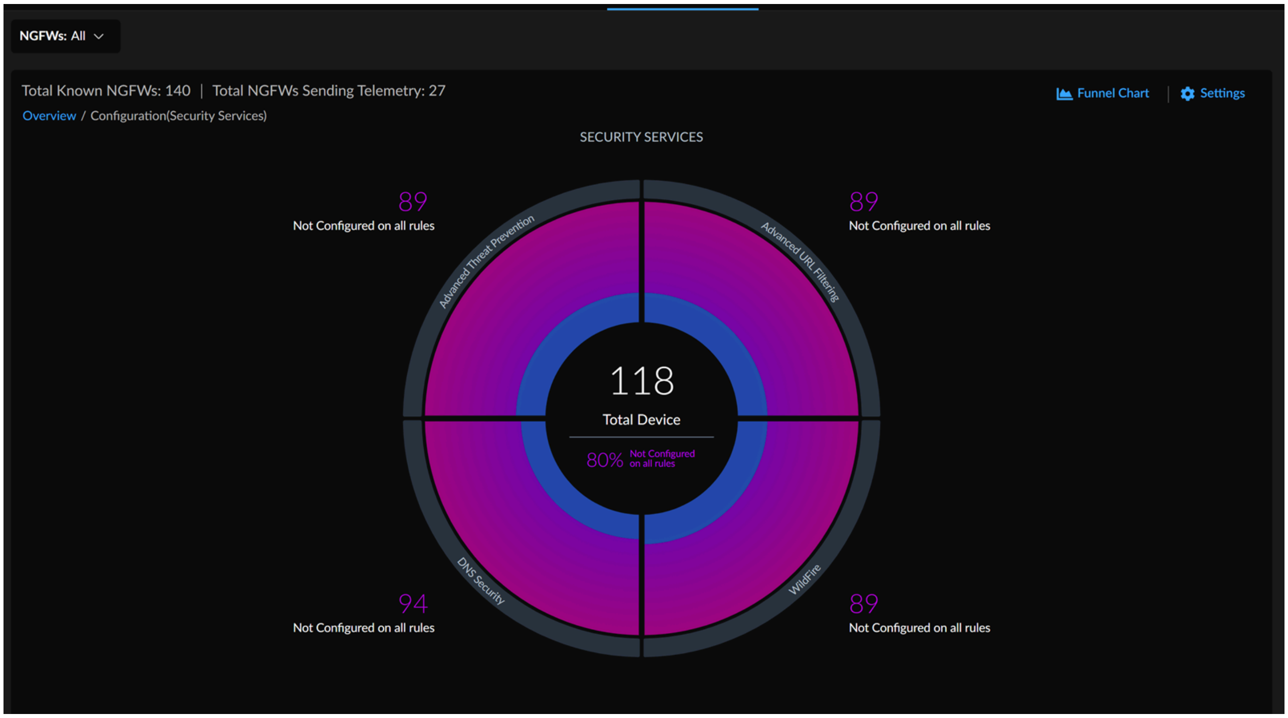
In this example, AIOps for NGFW recommends the activation of Advanced URL Filtering (ADV-URL) along with Advanced Threat Protection (ATP), Domain Name System (DNS), and WildFire (WF) security services for NGFWs. You can click **Back to Graph View** to navigate to the Overview page.

You can also view the same security posture data in a pie chart format. Click the pie-chart icon to view the information about recommended security services in a pie-chart format.



Total Known NGFWs: 140 | Total NGFWs Sending Telemetry: 27

You can click the sections of the pie-chart to view the information about the individual security service.



NGFWs: All

Total Known NGFWs: 140 | Total NGFWs Sending Telemetry: 27

Overview / Configuration(Security Services)

Funnel Chart
Settings
SECURITY SERVICES
89
Not Configured on all rules
Advanced Threat Prevention
89
Not Configured on all rules
Advanced URL Filtering
118
Total Device
80% Not Configured on all rules
94
Not Configured on all rules
DNS Security
89
Not Configured on all rules
WildFire

In this example, to view the NGFW where DNS Security is not configured, you can either click the value above the **DNS Security** section of a pie chart or click the **DNS Security** section of a pie chart.

For more information, see Dashboard: CDSS Adoption.

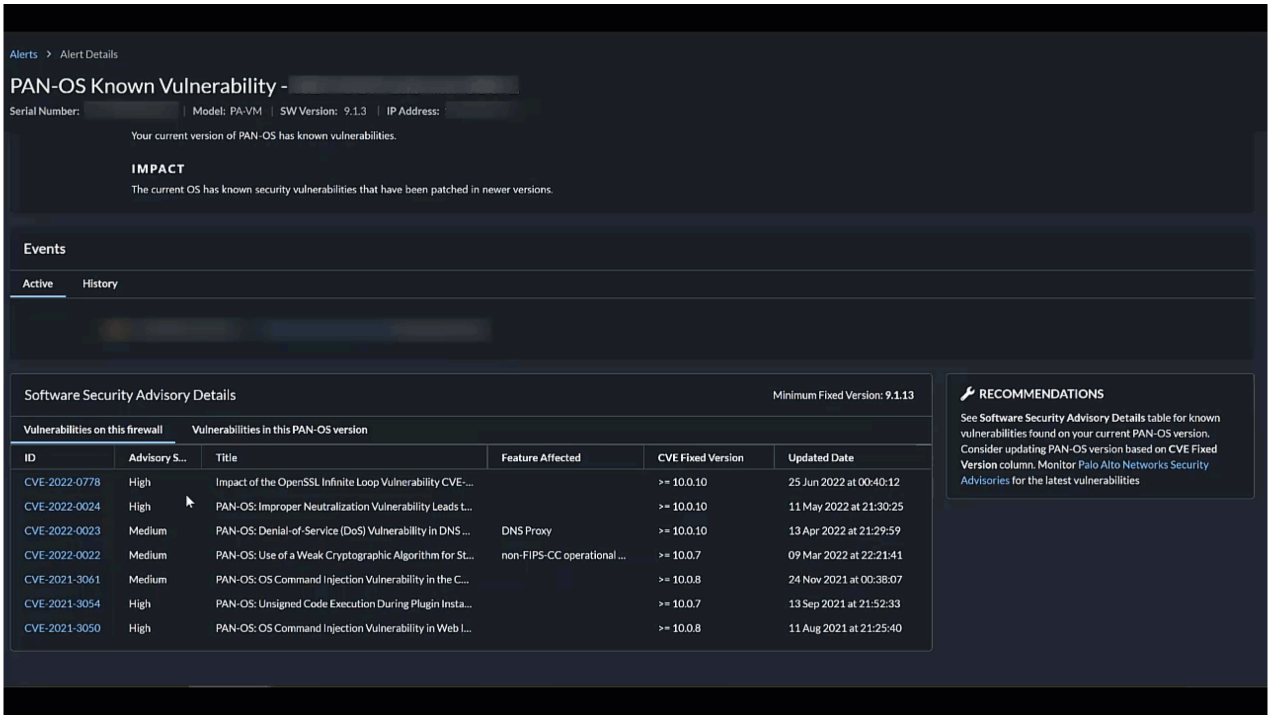
Assess Vulnerabilities

Where Can I Use This?	What Do I Need?
• NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series, funded with Software NGFW Credits	• AIOps for NGFW Free (use the AIOps for NGFW Free ap or • AIOps for NGFW Premium license (use the Strata Cloud

AIOps for NGFW shows you which vulnerabilities affect a given firewall and PAN-OS version to help you decide whether you should upgrade. Select the **PAN-OS Known Vulnerability** alert to see the latest security advisories impacting the firewall that raised the alert.

Select **Vulnerabilities in this PAN-OS version** to view the affected feature for a vulnerability in the **Feature Affected** column. This helps you to decide whether to upgrade a firewall based on the vulnerability and its impact on your enabled feature. If a CVE is not associated with a feature, then the value under **Feature Affected** is blank. This type of CVE affects the firewall with the specified model or version.

By default, the **PAN-OS Known Vulnerability** alert shows all of the vulnerabilities in the PAN-OS version on the device. However, if you enabled Product Usage telemetry on the firewall, you can choose to view only the vulnerabilities that affect the particular firewall based on its enabled features. That way, you can better understand which vulnerabilities are a concern for the firewall and make a more informed decision about whether to upgrade.



PAN-OS Known Vulnerability - [redacted]

Serial Number: [redacted] | Model: PA-VM | SW Version: 9.1.3 | IP Address: [redacted]

Your current version of PAN-OS has known vulnerabilities.

IMPACT

The current OS has known security vulnerabilities that have been patched in newer versions.

Events

[redacted]

Software Security Advisory Details

Minimum Fixed Version: **9.1.13**

Vulnerabilities on this firewall
Vulnerabilities in this PAN-OS version

ID	Advisory S...	Title	Feature Affected	CVE Fixed Version	Updated Date
CVE-2022-0778	High	Impact of the OpenSSL Infinite Loop Vulnerability CVE-...		>= 10.0.10	25 Jun 2022 at 00:40:12
CVE-2022-0024	High	PAN-OS: Improper Neutralization Vulnerability Leads t...		>= 10.0.10	11 May 2022 at 21:30:25
CVE-2022-0023	Medium	PAN-OS: Denial-of-Service (DoS) Vulnerability in DNS ...	DNS Proxy	>= 10.0.10	13 Apr 2022 at 21:29:59
CVE-2022-0022	Medium	PAN-OS: Use of a Weak Cryptographic Algorithm for St...	non-FIPS-CC operational ...	>= 10.0.7	09 Mar 2022 at 22:21:41
CVE-2021-3061	Medium	PAN-OS: OS Command Injection Vulnerability in the C...		>= 10.0.8	24 Nov 2021 at 00:38:07
CVE-2021-3054	High	PAN-OS: Unsigned Code Execution During Plugin Insta...		>= 10.0.7	13 Sep 2021 at 21:52:33
CVE-2021-3050	High	PAN-OS: OS Command Injection Vulnerability in Web I...		>= 10.0.8	11 Aug 2021 at 21:25:40

RECOMMENDATIONS

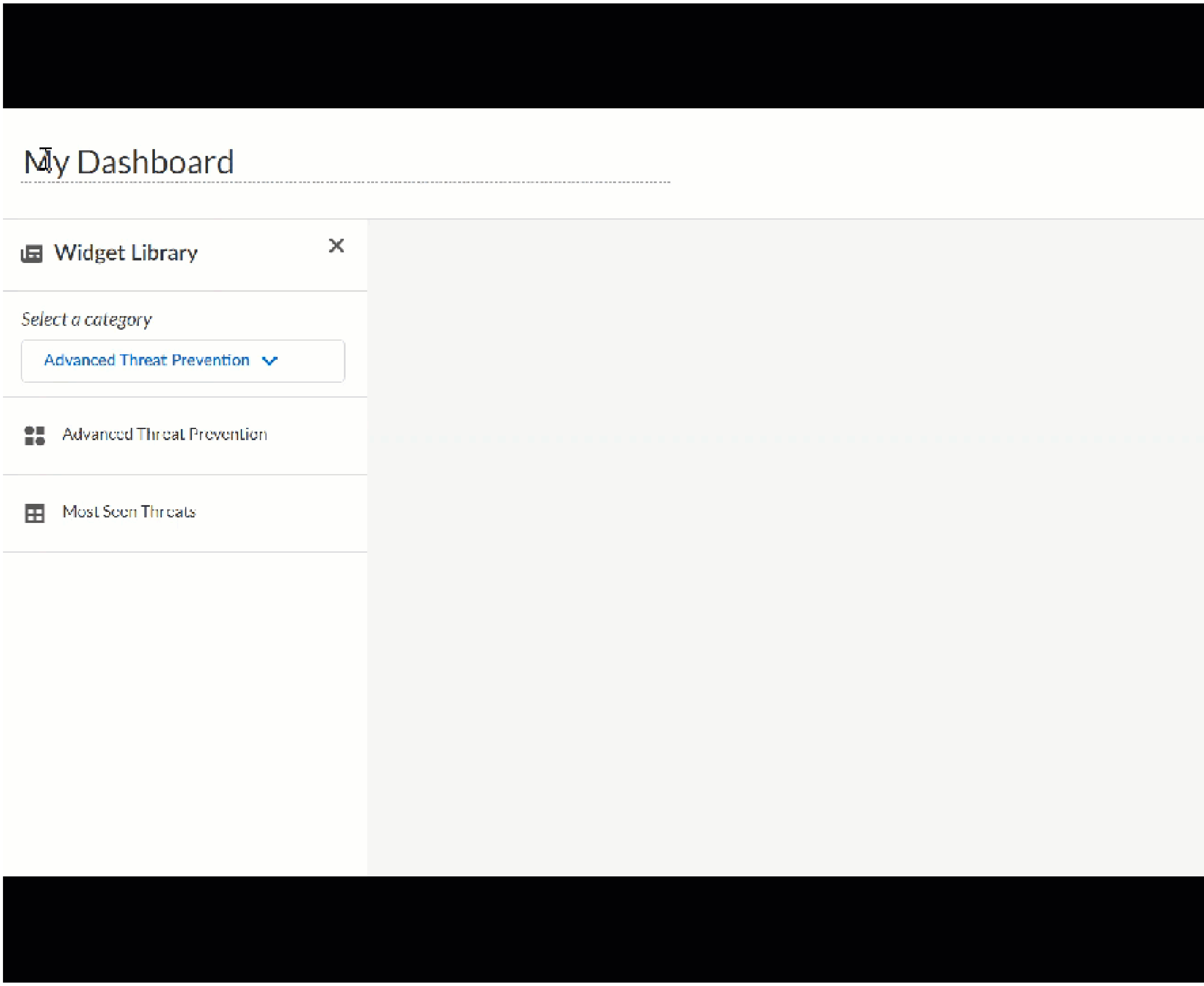
See **Software Security Advisory Details** table for known vulnerabilities found on your current PAN-OS version. Consider updating PAN-OS version based on **CVE Fixed Version** column. Monitor Palo Alto Networks Security Advisories for the latest vulnerabilities

Build a Custom Dashboard

Where Can I Use This?	What Do I Need?
- NGFW (Managed by Strata Cloud Manager) - NGFW (Managed by PAN-OS or Panorama) - VM-Series, funded with Software NGFW Credits	□ Minimum requirement: - AIOps for NGFW Premium license (use the Strata Clou - A role that has permission to create a dashboard □ License to view data from supported product in the dashboard: Prisma Access

Apart from the default dashboards, you can create custom dashboards to get visibility into areas of your interest in your network using widgets. Widgets are components used to create a dashboard. Widgets are categorized and stored in widget library. Click **Dashboards+** and select a category from the drop down list to view the widgets. The widgets available in the widget library depend on your security services subscriptions. For example, if you have AIOps for NGFW Premium and Advanced WildFire licenses, you can view and use all the widgets under WildFire category to create dashboard.

You can add up to 10 widgets in a custom dashboard and create 10 custom dashboards per user. The dashboard and widgets can be customized at any time. You can customize the widget tile, description, show or hide filters, dashboard settings such as layout, dashboard name, and descriptions, and also include filters in the dashboard.



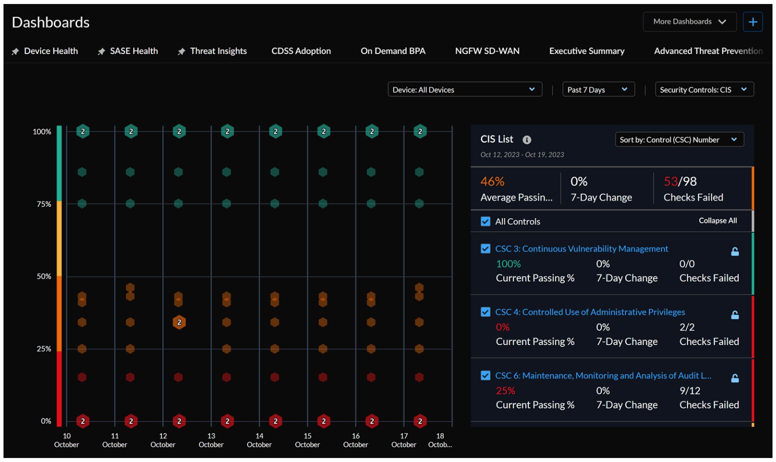
Select a category: Advanced Threat Prevention

For more information, see Dashboard: Build a Custom Dashboard.

Monitor Compliance Summary

Where Can I Use This?	What Do I Need?
• NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series, funded with Software NGFW Credits	□ AIOps for NGFW Premium license (use the Strata Cloud License to view data from supported product in the dashboard: Prisma Access

To get to the Compliance Summary Dashboard, go to **Dashboards**, and then select the **Compliance Summary** tab. You can view a history of changes to the security checks made up to 12 months in the past, grouped together by the Center for Internet Security (CIS) and the National Institute of Standards and Technology (NIST) frameworks. For each framework, you'll see a list of controls as well as the percentage of current and average compliance rate, total number of best practice checks, and the number of failed checks for each control. Interact with the chart and the list to see the relationship between controls and their historical statistics. View details of individual controls and their associated checks, and select a best practice check to view the firewall configuration that is failing the check.**The CIS Critical Security Controls** framework is a prioritized set of recommended actions and best practices that help protect organizations and their data from known cyber attack vectors.



Device: All Devices | Past 7 Days | Security Controls: CIS

CIS List
Oct 12, 2023 - Oct 19, 2023
Sort by: Control (CSC) Number

46% Average Passin... | 0% 7-Day Change | 53/98 Checks Failed

☑ All Controls

☑ CSC 3: Continuous Vulnerability Management
100% Current Passing % | 0% 7-Day Change | 0/0 Checks Failed

☑ CSC 4: Controlled Use of Administrative Privileges
0% Current Passing % | 0% 7-Day Change | 2/2 Checks Failed

☑ CSC 6: Maintenance, Monitoring and Analysis of Audit L...
25% Current Passing % | 0% 7-Day Change | 9/12 Checks Failed

You can view check summaries for 11 of the 16 basic and foundational CIS controls:

- CSC 3: Continuous Vulnerability Management
- CSC 4: Controlled Use of Administrative Privileges
- CSC 6: Maintenance, Monitoring, and Analysis of Audit Logs
- CSC 7: Email and Web Browser Protections
- CSC 8: Malware Defenses
- CSC 9: Limitation and Control of Network Ports, Protocols, and Services
- CSC 11: Secure configuration for Network Devices, such as Firewalls, Routers, and Switches
- CSC 12: Boundary Defense
- CSC 13: Data Protection

- CSC 14: Controlled Access Based on the Need to Know
- CSC 16: Account Monitoring and Control

The NIST Cybersecurity Framework SP 800-53 Controls framework provides guidance for federal agencies and other organizations to implement and maintain security and privacy controls for their information systems. You can view check summaries for eight families of NIST controls:

- SC: Access Control
- AU: Audit and Accountability
- CM: Configuration Management
- CP: Contingency Planning
- IA: Identification and Authentication
- RA: Risk Assessment
- SC: System and Communications Protection
- SI: System and Information Integrity

For more information, see Dashboard: Compliance Summary.

Configure Security Checks And Other Posture Settings

Where Can I Use This?	What Do I Need?
• NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series, funded with Software NGFW Credits	□ AIOps for NGFW Premium license (use the Strata Cloud

In **Posture Settings**, you can customize security posture checks for your deployment to maximize relevant recommendations using the features below.

Go to **Manage** > **Security Posture** > **Settings - Panorama Managed**.

- **Security Checks**

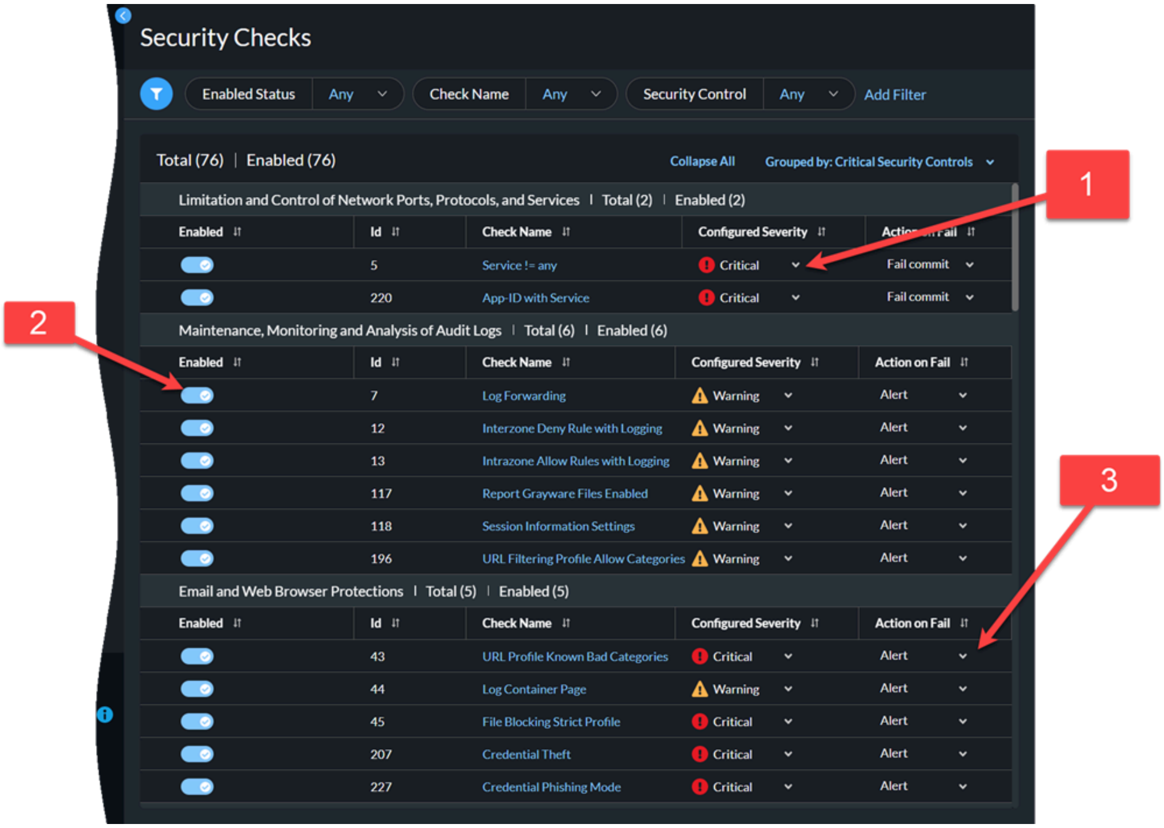
  List of the best practice checks that AIOps for NGFW uses to evaluate your configuration. The configuration of firewalls and Panorama is compared to Palo Alto Networks best practice checks to assess the security posture of your devices and to generate security alerts. You can see a list of the best practice checks that are used to evaluate your configuration.

Here, you can:

1. Set the severity level for checks to identify the checks that are the most critical to your deployment.
2. Temporarily disable checks.

   If you choose to disable a check, you can specify how long it will remain disabled and leave a comment explaining the reason for disabling it.
3. Set the response when a check fails.
   - **Alert** —Raises an alert for the failed check.
   - **Fail Commit** — Panorama blocks commits if the check fails so that you can stop potential misconfigurations before they enter your deployment.

   This requires the Panorama CloudConnector Plugin.



Security Checks

Enabled Status: Any | Check Name: Any | Security Control: Any | Add Filter

Total (76) | Enabled (76) — Collapse All — Grouped by: Critical Security Controls

Limitation and Control of Network Ports, Protocols, and Services | Total (2) | Enabled (2)

Enabled	Id	Check Name	Configured Severity	Action on Fail
☑	5	Service != any	Critical	Fail commit
☑	220	App-ID with Service	Critical	Fail commit

Maintenance, Monitoring and Analysis of Audit Logs | Total (6) | Enabled (6)

Enabled	Id	Check Name	Configured Severity	Action on Fail
☑	7	Log Forwarding	Warning	Alert
☑	12	Interzone Deny Rule with Logging	Warning	Alert
☑	13	Intrazone Allow Rules with Logging	Warning	Alert
☑	117	Report Grayware Files Enabled	Warning	Alert
☑	118	Session Information Settings	Warning	Alert
☑	196	URL Filtering Profile Allow Categories	Warning	Alert

Email and Web Browser Protections | Total (5) | Enabled (5)

Enabled	Id	Check Name	Configured Severity	Action on Fail
☑	43	URL Profile Known Bad Categories	Critical	Alert
☑	44	Log Container Page	Warning	Alert
☑	45	File Blocking Strict Profile	Critical	Alert
☑	207	Credential Theft	Critical	Alert
☑	227	Credential Phishing Mode	Critical	Alert

- **Zone to Role Mapping**

  Map the zones in NGFWs to roles to get customized recommendations.
- **Role to Security Service Mapping**

  Manage the security services needed for traffic between zones and roles in all NGFWs.

Proactively Enforce Security Checks

Where Can I Use This?	What Do I Need?
• NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series, funded with Software NGFW Credits	□ AIOps for NGFW Premium license (use the Strata Cloud

The Panorama CloudConnector Plugin enables you to take proactive measures against suboptimal configurations by blocking commits that do not pass particular best practice checks. When you indicate in AIOps for NGFW that you want a check to **Fail Commit**, Panorama automatically blocks commits of any configuration that does not pass that check. Rather than wait to receive an alert about a failed best practice check, use the plugin to keep configuration issues out of your deployment in the first place.

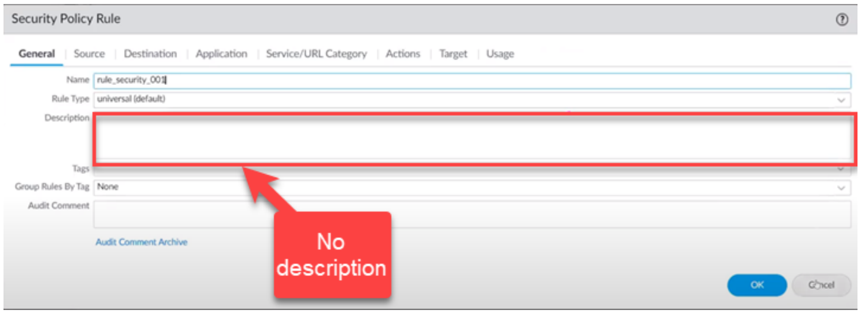
STEP 1 | Ensure that you meet all prerequisites, and install the plugin.

STEP 2 | Specify the best practice checks that will block commits on failure.

1. Select **Manage** > **Security Posture** > **Settings**.
2. Find the check that you want to block commits.
3. Set **Action on Fail** to **Fail Commit**

STEP 3 | Verify by attempting to commit a configuration that does not pass the check.

1. Log in to Panorama.
2. Violate the best practice check that you specified to **Fail Commit**.



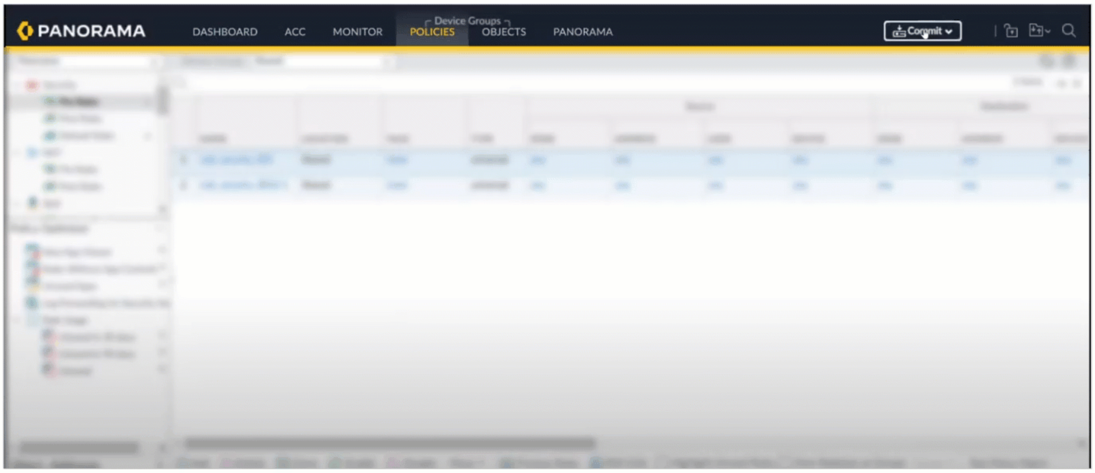
Name rule_security_001

Rule Type universal (default)

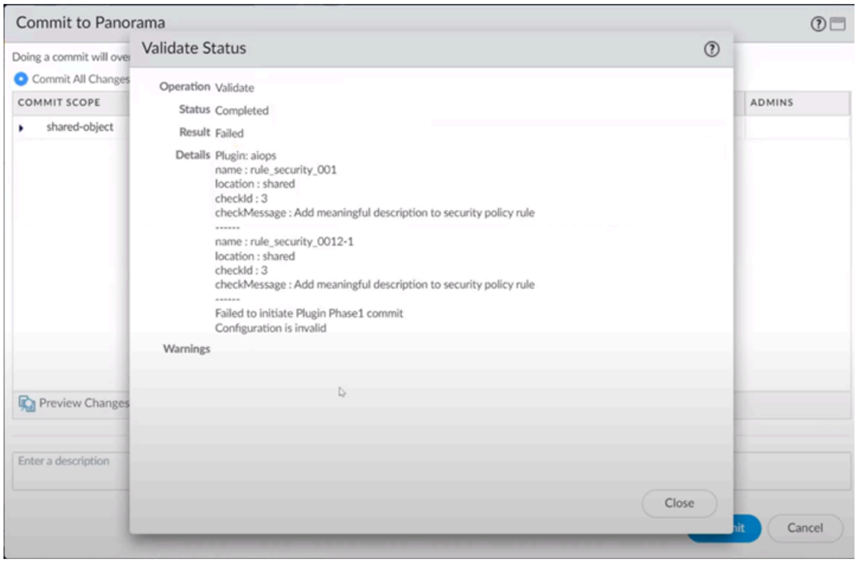
Group Rules By Tag None

No description

3. Select **Commit** > **Commit to Panorama** > **Validate Configuration.**


PANORAMA
DASHBOARD
ACC
MONITOR
Device Groups
POLICIES
OBJECTS
PANORAMA
Commit

You should see a dialog stating that the validation failed because the configuration did not pass the best practice check.



Operation Validate
Status Completed
Result Failed
Details Plugin: aiops

```
name : rule_security_001
location : shared
checkId : 3
checkMessage : Add meaningful description to security policy rule
------
name : rule_security_0012-1
location : shared
checkId : 3
checkMessage : Add meaningful description to security policy rule
------
Failed to initiate Plugin Phase1 commit
Configuration is invalid
```

Warnings

*Setting a check to **Fail Commit** causes the check to fail both validation and the actual commit operation.*

See Manage: Security Posture Settings for more information.

Policy Analyzer

Where Can I Use This?	What Do I Need?
• NGFW (Panorama Managed) • VM-Series, funded with Software NGFW Credits (Panorama Managed) • Prisma Access (Managed by Panorama)	□ AIOps for NGFW Premium license (use the Strata Cloud □ CloudConnector Plugin on Panorama □ Prisma Access license

Updates to your Security policy rules are often time-sensitive and require you to act quickly. However, you want to ensure that any update you make to your Security policy rulebase meets your requirements and does not introduce errors or misconfigurations (such as changes that result in duplicate or conflicting rules).

Policy Analyzer in Strata Cloud Manager enables you to optimize time and resources when implementing a change request. Policy Analyzer not only analyzes and provides suggestions for possible consolidation or removal of specific rules to meet your intent but also checks for anomalies, such as Shadows, Redundancies, Generalizations, Correlations, and Consolidations in your rulebase.

Use Policy Analyzer to add or optimize your Security policy rulebase.

- **Before adding a new rule**—Check to see if new rules need to be added. Policy Analyzer recommends how best to change your existing Security policy rules to meet your requirements without adding another rule, if possible.
- **Streamline and optimize your existing rulebase**—See where you can update your rules to minimize bloat and eliminate conflicts and also to ensure that traffic enforcement aligns with the intent of your Security policy rulebase.

Analyze your Security policy rules both before and after you commit your changes.

- **Pre-Change Policy Analysis**—Enables you to evaluate the impact of a new rule and analyze the intent of the new rules against the rules that already exist to recommend how to best meet the intent.
- **Post-Change Policy Analysis**—Enables you to clean the existing rulebase by identifying Shadows, Redundancies, and other anomalies that have accumulated over time.

- *Policy Analyzer requires the* CloudConnector Plugin *1.1.0 or later on your Panorama appliance. You need to enable this plugin using the command:*

  ```
  > request plugins cloudconnector enable basic
  ```

- *Policy Analyzer requires Panorama to be updated to PAN-OS version 10.2.3 or a later version.*

Types of Anomalies That Policy Analyzer Detects

Policy Analyzer detects the following types of anomalies across your Security policy rulebase:

- Shadows—Rules that are not hit because a rule higher in the rulebase covers the same traffic.

  Security policy rules are evaluated in the rulebase from the top down so shadows are created when a rule higher in the rulebase matches the same traffic that a rule lower in order matches and the rules are configured with a different action. If you remove the rule lower in order, the Security policy does not change.
- Redundancies—Two or more rules that match the same traffic and are configured with the same action.
- Generalizations—When a rule lower in the rulebase matches the traffic of a rule higher in the rulebase, but not the other way around, and the rules take a different action. If the order of the two policy rules is reversed, the Security policy is impacted.
- Correlations—Rules that correlate with another rule when one rule matches some packets of the other rule but results in a different action. If the order of the two rules is reversed, the Security policy is impacted.
- Consolidations—Rules that you can consolidate into a single rule because the action is the same and only one attribute is different. You can merge the rules into a single rule by modifying the attributes of one of the rules and deleting the others.

Pre-Change Policy Analysis

Where Can I Use This?	What Do I Need?
• NGFW (Panorama Managed) • VM-Series, funded with Software NGFW Credits (Panorama Managed) • Prisma Access (Managed by Panorama)	□ AIOps for NGFW Premium license (use the Strata Cloud □ CloudConnector Plugin on Panorama □ Prisma Access license

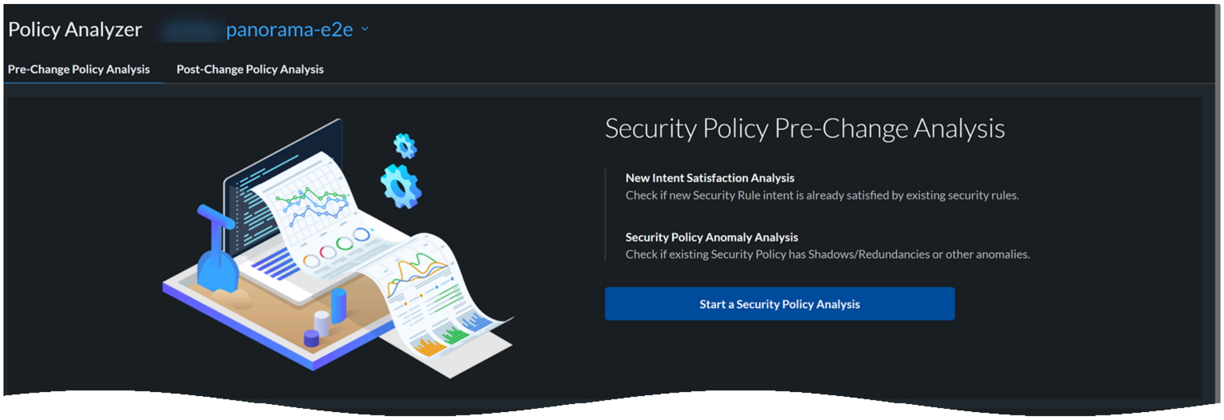
The Security policy rule Pre-Change analysis performs the new intent satisfaction analysis:

- **New Intent Satisfaction Analysis**—Checks whether the intent of a new Security policy rule is already covered by an existing rule.

Before you begin:

1. Go to **Manage** > **Security Posture** > **Policy Analyzer** > **Pre-change Policy Analysis**.

2. At the top of the Policy Analyzer page, select the Panorama instance containing the policy rules that you need to analyze.



Policy Analyzer [redacted]panorama-e2e

Pre-Change Policy Analysis | Post-Change Policy Analysis

Security Policy Pre-Change Analysis

New Intent Satisfaction Analysis
Check if new Security Rule intent is already satisfied by existing security rules.

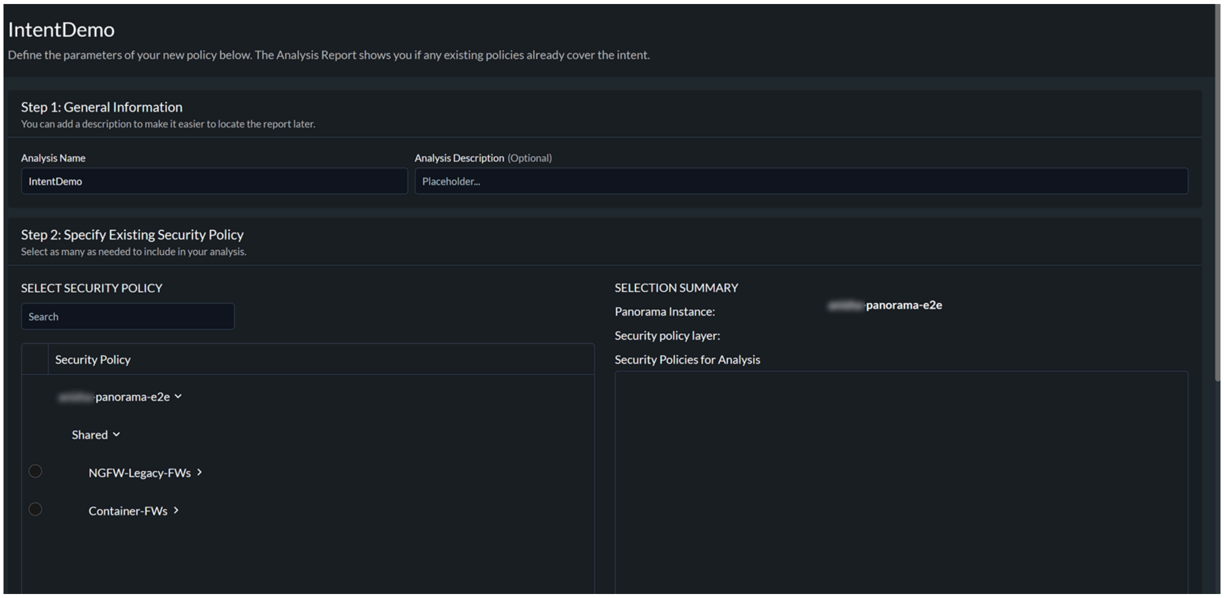
Security Policy Anomaly Analysis
Check if existing Security Policy has Shadows/Redundancies or other anomalies.

Start a Security Policy Analysis

3. **Start a Security Policy Analysis**.

Perform the following steps to start a new analysis:

STEP 1 | Enter **Analysis Name** and **Analysis Description**.



IntentDemo

Define the parameters of your new policy below. The Analysis Report shows you if any existing policies already cover the intent.

Step 1: General Information
You can add a description to make it easier to locate the report later.

Analysis Name: IntentDemo

Analysis Description (Optional): Placeholder...

Step 2: Specify Existing Security Policy
Select as many as needed to include in your analysis.

SELECT SECURITY POLICY

Search

Security Policy
- [redacted]panorama-e2e
  - Shared
    - ○ NGFW-Legacy-FWs
    - ○ Container-FWs

SELECTION SUMMARY

Panorama Instance: [redacted]panorama-e2e

Security policy layer:

Security Policies for Analysis

On a Panorama appliance, device groups are hierarchical. There are four levels of device groups that you can create and you assign NGFWs to the device group at the lowest level of the hierarchy. The policy that you create at a higher level is then inherited by all the device groups under it.

You can run the analysis for up to 10 device groups with NGFWs directly assigned to them, which allows you to analyze all the policy rules that are pushed to that set of directly assigned NGFWs.

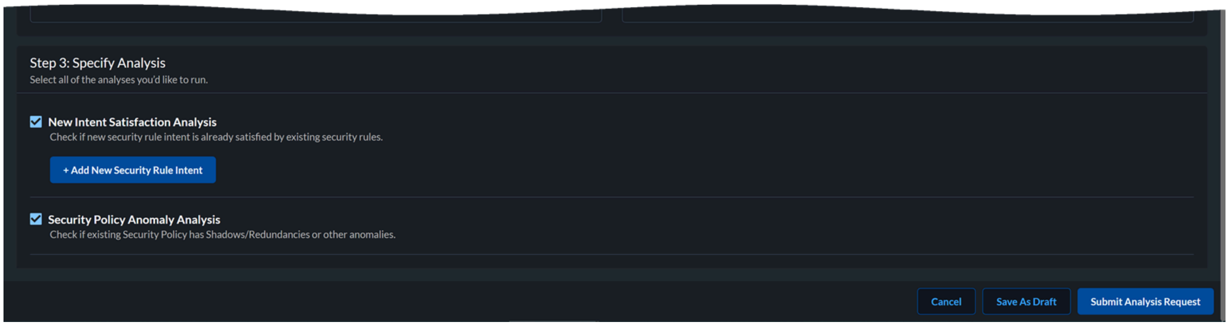
STEP 2 | Select an existing Security policy set to analyze.

You can select a maximum of 10 device groups per analysis.

STEP 3 | Specify the type of analysis by selecting one or more analysis types:

- **New Intent Satisfaction Analysis**

Add New Security Rule Intent for analysis.



Step 3: Specify Analysis

Select all of the analyses you'd like to run.

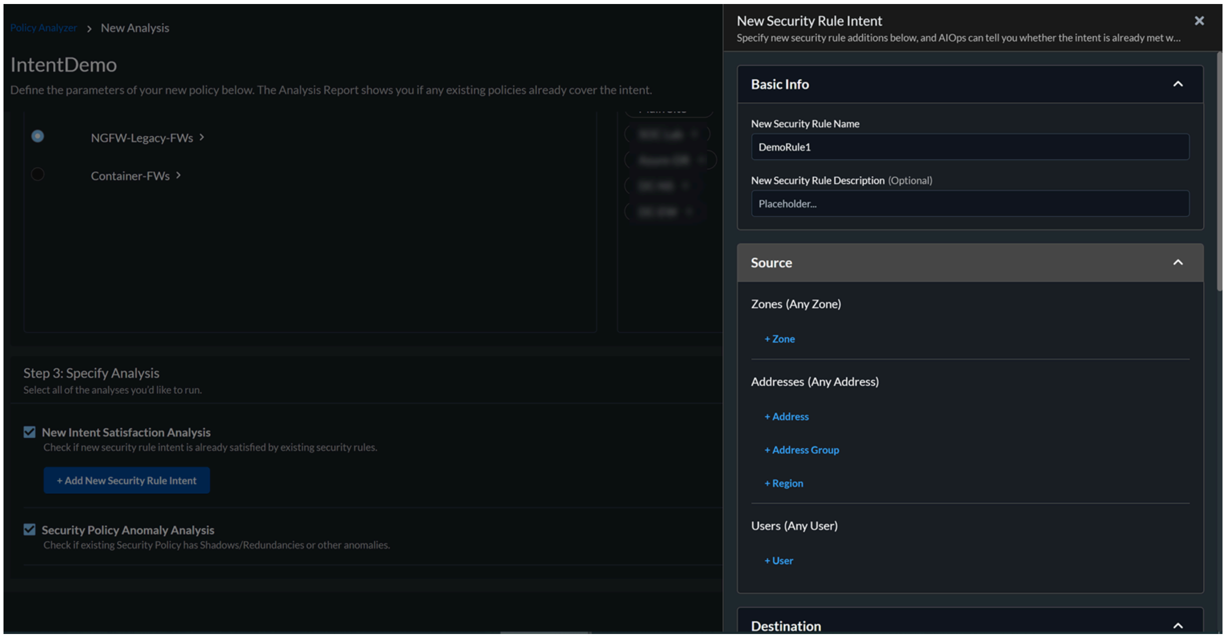
☑ New Intent Satisfaction Analysis

Check if new security rule intent is already satisfied by existing security rules.

☑ Security Policy Anomaly Analysis

Check if existing Security Policy has Shadows/Redundancies or other anomalies.

Specify information about the new security rule, and AIOps for NGFW can check if existing rules cover the intent.



Policy Analyzer > New Analysis

IntentDemo

Define the parameters of your new policy below. The Analysis Report shows you if any existing policies already cover the intent.

● NGFW-Legacy-FWs >

○ Container-FWs >

Step 3: Specify Analysis

Select all of the analyses you'd like to run.

☑ New Intent Satisfaction Analysis

Check if new security rule intent is already satisfied by existing security rules.

+ Add New Security Rule Intent

☑ Security Policy Anomaly Analysis

Check if existing Security Policy has Shadows/Redundancies or other anomalies.

New Security Rule Intent

Specify new security rule additions below, and AIOps can tell you whether the intent is already met w...

Basic Info

New Security Rule Name: DemoRule1

New Security Rule Description (Optional): Placeholder...

Source

Zones (Any Zone)

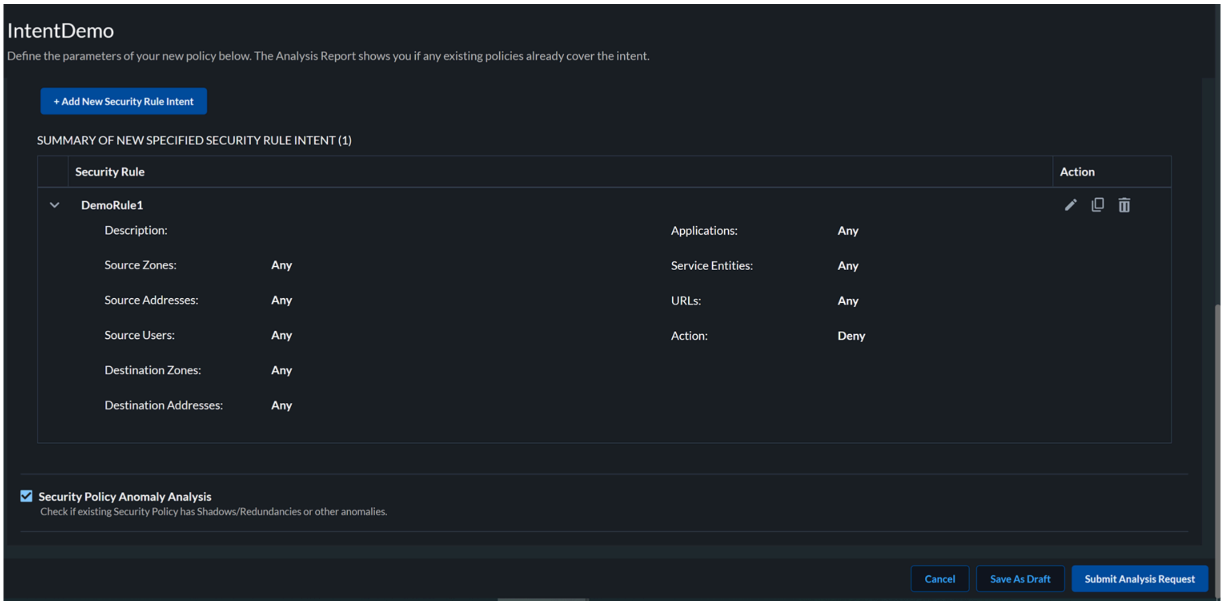
Addresses (Any Address)

Users (Any User)

Enter the values for the components of a security policy rule. The default value for the fields related to a security rule is "Any".

Save the settings.

Review the summary of the new security rule intent.



IntentDemo

Define the parameters of your new policy below. The Analysis Report shows you if any existing policies already cover the intent.

SUMMARY OF NEW SPECIFIED SECURITY RULE INTENT (1)

Security Rule	Action
DemoRule1	

Description:		Applications:	Any
Source Zones:	Any	Service Entities:	Any
Source Addresses:	Any	URLs:	Any
Source Users:	Any	Action:	Deny
Destination Zones:	Any		
Destination Addresses:	Any		

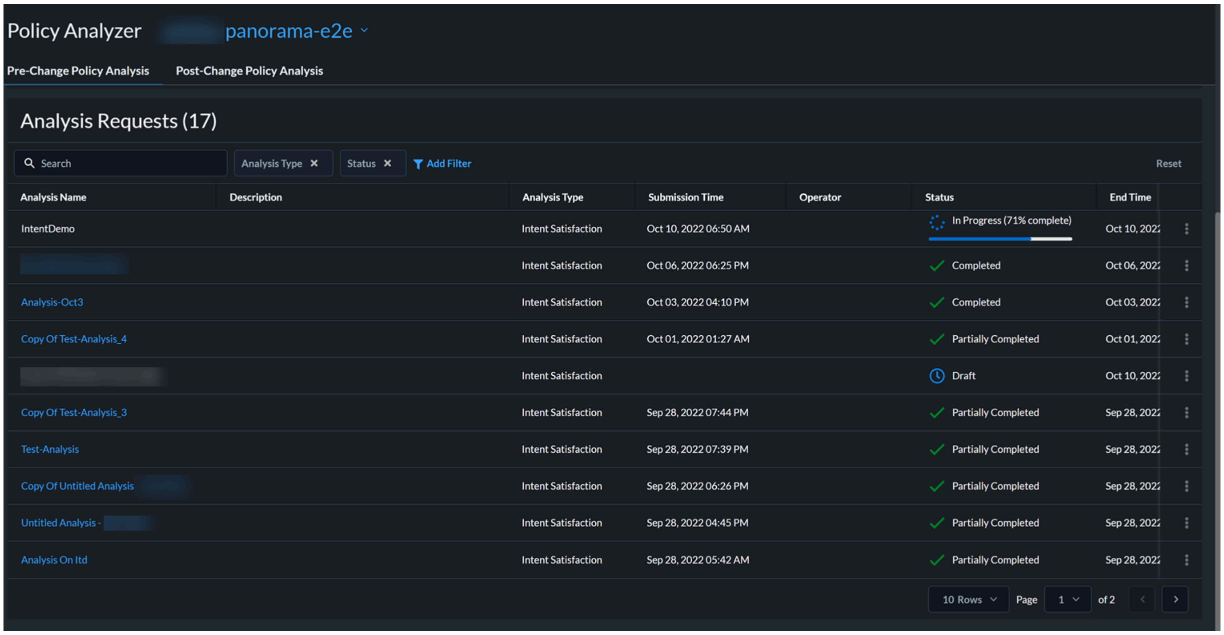
☑ Security Policy Anomaly Analysis

Check if existing Security Policy has Shadows/Redundancies or other anomalies.

You can create up to 10 new security rules, or you can copy a rule and edit it.

STEP 4 | **Submit Analysis Request or Save As Draft** to edit the rule later.

View the status of an analysis on the Policy Analyzer page under Analysis Requests.



Policy Analyzer [redacted] panorama-e2e

Analysis Requests (17)

Analysis Name	Description	Analysis Type	Submission Time	Operator	Status	End Time
IntentDemo		Intent Satisfaction	Oct 10, 2022 06:50 AM		In Progress (71% complete)	Oct 10, 202
[redacted]		Intent Satisfaction	Oct 06, 2022 06:25 PM		✓ Completed	Oct 06, 202
Analysis-Oct3		Intent Satisfaction	Oct 03, 2022 04:10 PM		✓ Completed	Oct 03, 202
Copy Of Test-Analysis_4		Intent Satisfaction	Oct 01, 2022 01:27 AM		✓ Partially Completed	Oct 01, 202
[redacted]		Intent Satisfaction			Draft	Oct 10, 202
Copy Of Test-Analysis_3		Intent Satisfaction	Sep 28, 2022 07:44 PM		✓ Partially Completed	Sep 28, 202
Test-Analysis		Intent Satisfaction	Sep 28, 2022 07:39 PM		✓ Partially Completed	Sep 28, 202
Copy Of Untitled Analysis [redacted]		Intent Satisfaction	Sep 28, 2022 06:26 PM		✓ Partially Completed	Sep 28, 202
Untitled Analysis - [redacted]		Intent Satisfaction	Sep 28, 2022 04:45 PM		✓ Partially Completed	Sep 28, 202
Analysis On Itd		Intent Satisfaction	Sep 28, 2022 05:42 AM		✓ Partially Completed	Sep 28, 202

You can cancel a rule whose status is in-progress and it will be shown as Canceled.

After the analysis is complete, view the analysis report.

Pre-Change Policy Analysis Reports

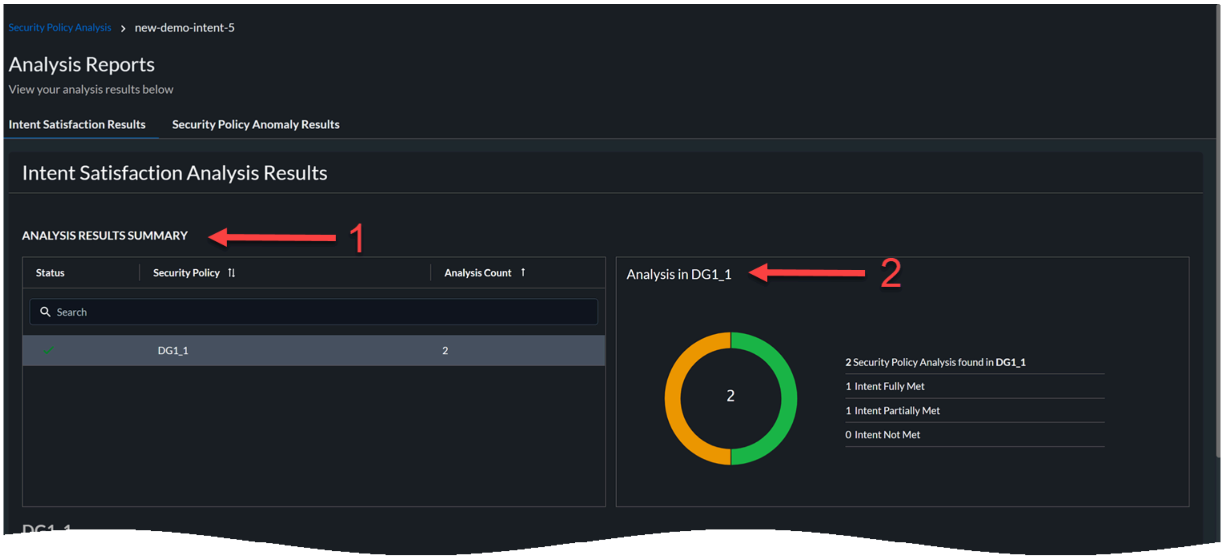
Where Can I Use This?	What Do I Need?
• NGFW (Panorama Managed) • VM-Series, funded with Software NGFW Credits (Panorama Managed) • Prisma Access (Managed by Panorama)	□ AIOps for NGFW Premium license (use the Strata Cloud □ CloudConnector Plugin on Panorama □ Prisma Access license

Select an analysis report whose status is completed to view the results of the policy analysis. You can view the results of the analysis.

Intent Satisfaction Results

From the list of analyses under Analysis Requests, click an analysis to view its analysis results. These results include:

1. Summary of the analysis with details about device groups and the anomaly count.
2. Click the name of a device group to view the result of the intent satisfaction analysis:
   - Intent Fully Met—Your security rule is a duplicate of one of the existing rules in the device group.
   - Intent Partially Met—Your security rule is partially meeting the intent of one of the existing rules in the device group.
   - Intent not met—Your security rule is a unique rule that is not present in the device group. You can add this rule to the device group.



Security Policy Analysis › new-demo-intent-5

Analysis Reports

View your analysis results below

Intent Satisfaction Results | Security Policy Anomaly Results

Intent Satisfaction Analysis Results

ANALYSIS RESULTS SUMMARY

Status	Security Policy	Analysis Count
✓	DG1_1	2

Analysis in DG1_1

2 Security Policy Analysis found in DG1_1

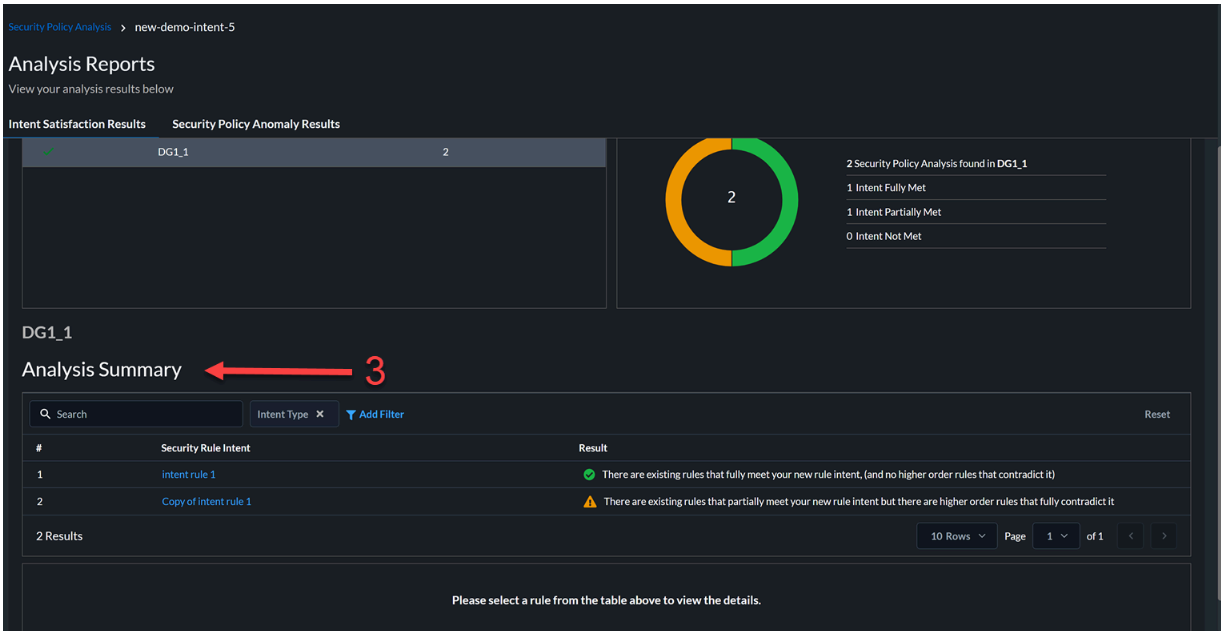
1 Intent Fully Met

1 Intent Partially Met

0 Intent Not Met

DG1_1

3. View the results of the analysis for the new security rule intent.



Security Policy Analysis > new-demo-intent-5

Analysis Reports

View your analysis results below

Intent Satisfaction Results | Security Policy Anomaly Results

✓	DG1_1	2

2 Security Policy Analysis found in DG1_1

1 Intent Fully Met

1 Intent Partially Met

0 Intent Not Met

DG1_1

Analysis Summary

Search | Intent Type ✕ | Add Filter | Reset

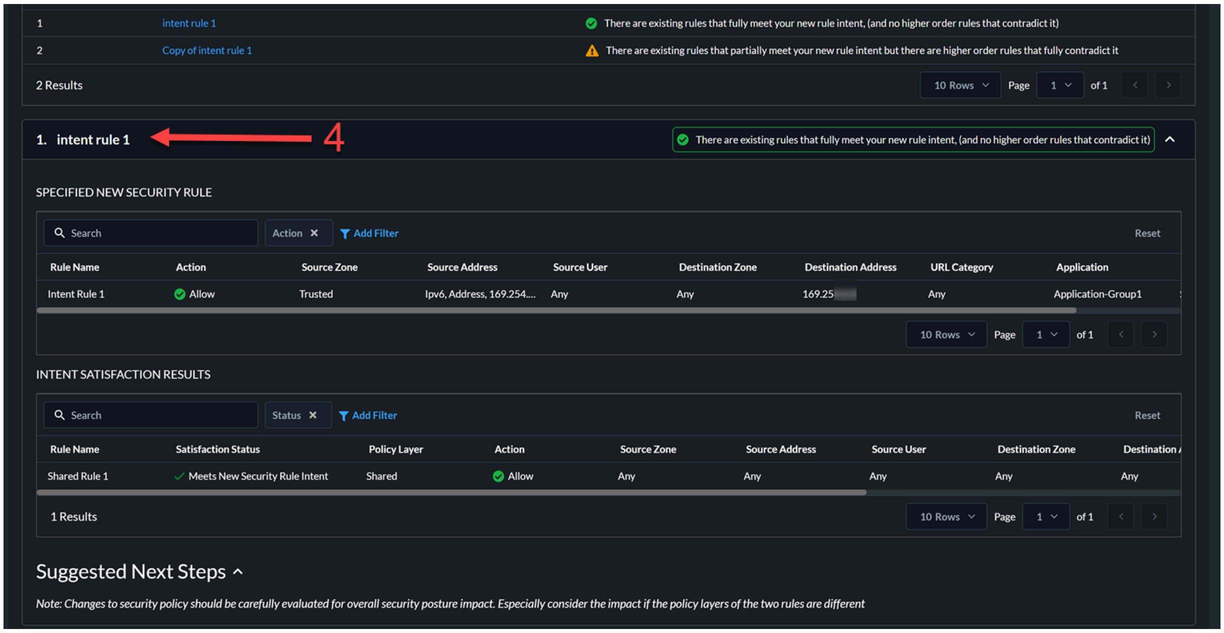
#	Security Rule Intent	Result
1	intent rule 1	✓ There are existing rules that fully meet your new rule intent, (and no higher order rules that contradict it)
2	Copy of intent rule 1	⚠ There are existing rules that partially meet your new rule intent but there are higher order rules that fully contradict it

2 Results — 10 Rows — Page 1 of 1

Please select a rule from the table above to view the details.

In this example, there are two rules. The intent of the first rule matches fully with existing rules and the intent of the second rule matches partially with the existing rules.

4. View the details of the new security rule and check the intent satisfaction results.



1	intent rule 1	✓ There are existing rules that fully meet your new rule intent, (and no higher order rules that contradict it)
2	Copy of intent rule 1	⚠ There are existing rules that partially meet your new rule intent but there are higher order rules that fully contradict it

2 Results — 10 Rows — Page 1 of 1

1. intent rule 1

✓ There are existing rules that fully meet your new rule intent, (and no higher order rules that contradict it)

SPECIFIED NEW SECURITY RULE

Search | Action ✕ | Add Filter | Reset

Rule Name	Action	Source Zone	Source Address	Source User	Destination Zone	Destination Address	URL Category	Application
Intent Rule 1	✓ Allow	Trusted	Ipv6, Address, 169.254....	Any	Any	169.25[redacted]	Any	Application-Group1

10 Rows — Page 1 of 1

INTENT SATISFACTION RESULTS

Search | Status ✕ | Add Filter | Reset

Rule Name	Satisfaction Status	Policy Layer	Action	Source Zone	Source Address	Source User	Destination Zone	Destination
Shared Rule 1	✓ Meets New Security Rule Intent	Shared	✓ Allow	Any	Any	Any	Any	Any

1 Results — 10 Rows — Page 1 of 1

Suggested Next Steps

Note: Changes to security policy should be carefully evaluated for overall security posture impact. Especially consider the impact if the policy layers of the two rules are different

In this example, all the attributes of the new rule intent rule 1 matches the attributes of the existing rule Shared Rule 1. The intent of the new rule fully matches the intent of the existing rule. Therefore, you need not add this new rule to the configuration.

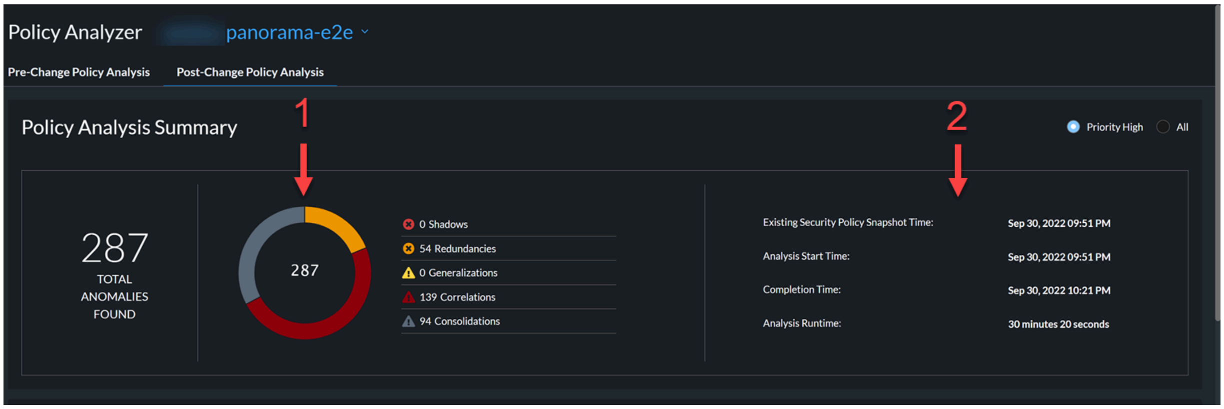
Post-Change Policy Analysis

Where Can I Use This?	What Do I Need?
• NGFW (Panorama Managed) • VM-Series, funded with Software NGFW Credits (Panorama Managed) • Prisma Access (Managed by Panorama)	□ AIOps for NGFW Premium license (use the Strata Cloud □ CloudConnector Plugin on Panorama □ Prisma Access license

When you commit a configuration on Panorama, it's available for analysis through the plugin to Strata Cloud Manager. Policy Analyzer analyzes this configuration for Shadows, Redundancies and other anomalies, and the results are available for review in **Manage** > **Security Posture** > **Policy Analyzer** > **Post-change Policy Analysis**.

You can view the following information:

1. Shows the summary of the analysis across all the policy sets, that is, all the device groups with NGFWs directly assigned to them. You can view the anomalies or the anomalies based on high priority. The values in this report show the unique number of anomalies found in all the device groups. The colors in the chart indicate the different types of anomalies.



Existing Security Policy Snapshot Time: Sep 30, 2022 09:51 PM

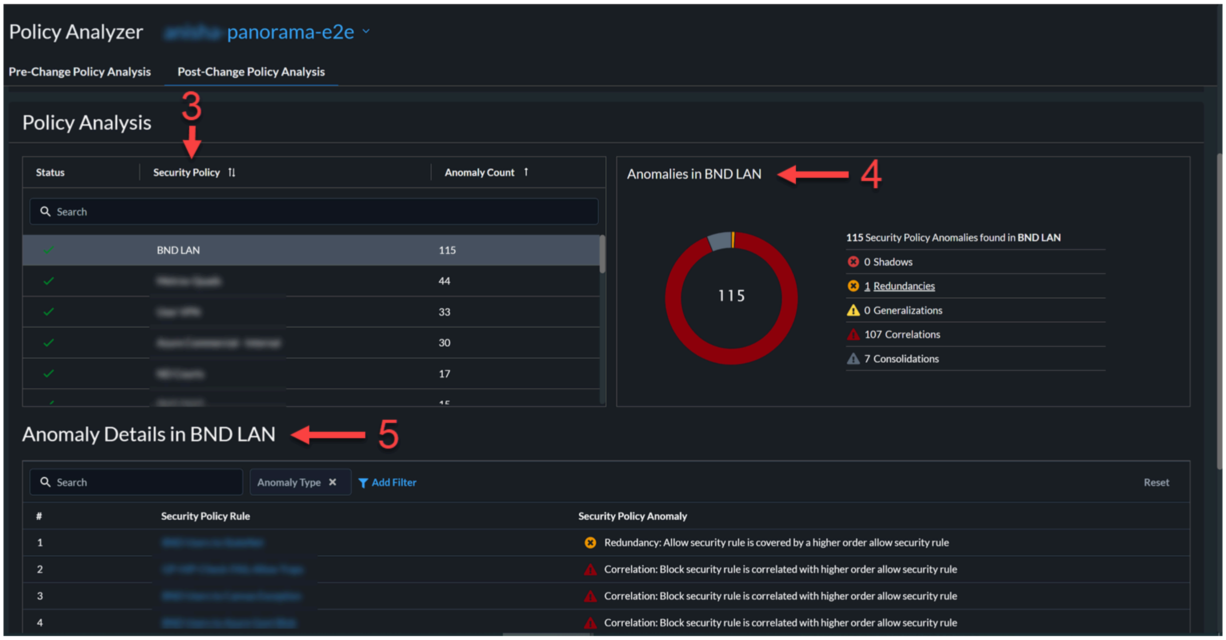
Analysis Start Time: Sep 30, 2022 09:51 PM

Completion Time: Sep 30, 2022 10:21 PM

Analysis Runtime: 30 minutes 20 seconds

2. Timestamps for analysis that includes:
   - Existing Security policy snapshot - Timestamp when the configuration was marked as running in Panorama after a commit.
   - Time analysis started
   - Time analysis finished
   - Time it took to complete the analysis
3. View the status of the Security policy and the number of anomalies for every policy.
4. View a breakdown of anomalies for a selected Security policy.

5. View anomaly details for every rule in a Security policy.



Policy Analysis

Status	Security Policy	Anomaly Count
✓	BND LAN	115
✓	[redacted]	44
✓	[redacted]	33
✓	[redacted]	30
✓	[redacted]	17
✓	[redacted]	15

Anomalies in BND LAN

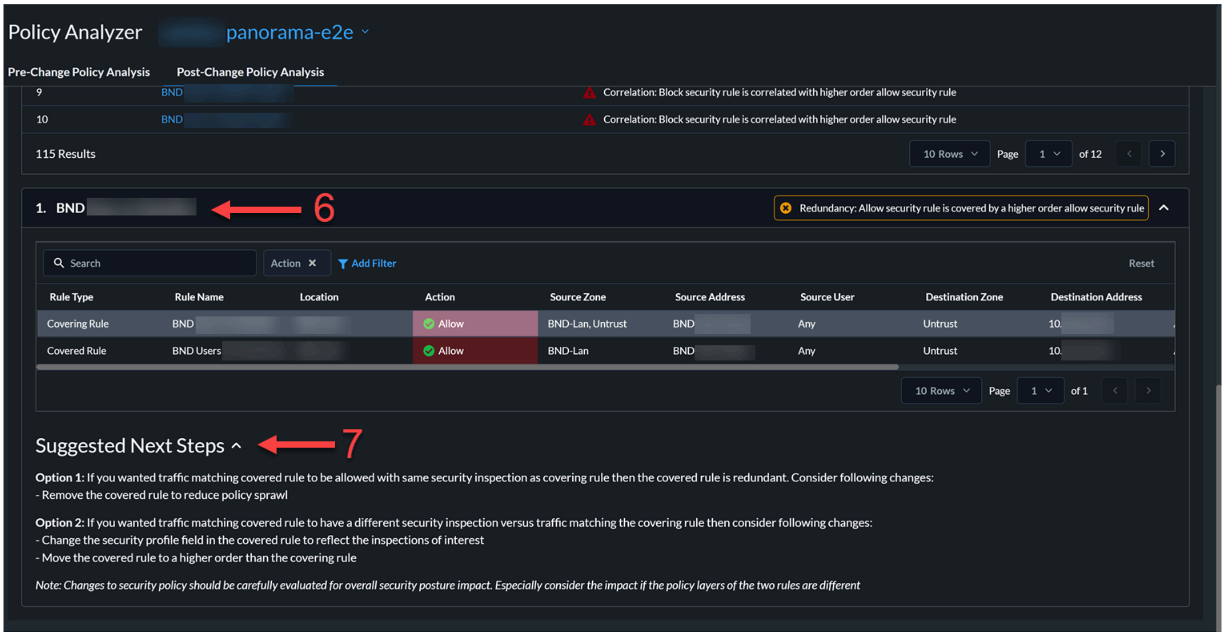
115 Security Policy Anomalies found in **BND LAN**
- 0 Shadows
- 1 Redundancies
- 0 Generalizations
- 107 Correlations
- 7 Consolidations

Anomaly Details in BND LAN

Search | Anomaly Type ✕ | Add Filter | Reset

#	Security Policy Rule	Security Policy Anomaly
1	[redacted]	Redundancy: Allow security rule is covered by a higher order allow security rule
2	[redacted]	Correlation: Block security rule is correlated with higher order allow security rule
3	[redacted]	Correlation: Block security rule is correlated with higher order allow security rule
4	[redacted]	Correlation: Block security rule is correlated with higher order allow security rule

6. View the attributes of a selected rule and the details of the anomaly.



9	BND [redacted]	Correlation: Block security rule is correlated with higher order allow security rule
10	BND [redacted]	Correlation: Block security rule is correlated with higher order allow security rule

115 Results — 10 Rows | Page 1 | of 12

1. BND [redacted] — Redundancy: Allow security rule is covered by a higher order allow security rule

Search | Action ✕ | Add Filter | Reset

Rule Type	Rule Name	Location	Action	Source Zone	Source Address	Source User	Destination Zone	Destination Address
Covering Rule	BND [redacted]	[redacted]	Allow	BND-Lan, Untrust	BND [redacted]	Any	Untrust	10. [redacted]
Covered Rule	BND Users [redacted]	[redacted]	Allow	BND-Lan	BND [redacted]	Any	Untrust	10. [redacted]

10 Rows | Page 1 | of 1

Suggested Next Steps

Option 1: If you wanted traffic matching covered rule to be allowed with same security inspection as covering rule then the covered rule is redundant. Consider following changes:
- Remove the covered rule to reduce policy sprawl

Option 2: If you wanted traffic matching covered rule to have a different security inspection versus traffic matching the covering rule then consider following changes:
- Change the security profile field in the covered rule to reflect the inspections of interest
- Move the covered rule to a higher order than the covering rule

Note: Changes to security policy should be carefully evaluated for overall security posture impact. Especially consider the impact if the policy layers of the two rules are different

This image shows an example of the redundancy anomaly. In this example, the BND rule is already covered by another BND Users rule. Therefore, you can remove the BND rule.

7. View the suggested next steps to remediate an anomaly.

NGFW Health and Software Management

This chapter describes how to manage NGFW health and software upgrades.

- View Network Usage - View what’s driving your network traffic. Dive in to see who or what is using your network (users, apps, IP addresses, and countries), and the apps and sites they’re accessing and their threat exposure.
- View Device Health - View the cumulative health status and performance of your deployment based on the health scores of the onboarded NGFWs.
- Upgrade Recommendations - Create recommendations to determine the best software version for your devices that can be upgraded.
- Analyze Metric Capacity - Analyze and monitor your devices' resource capacity by keeping track of their metrics usage based on their model types.

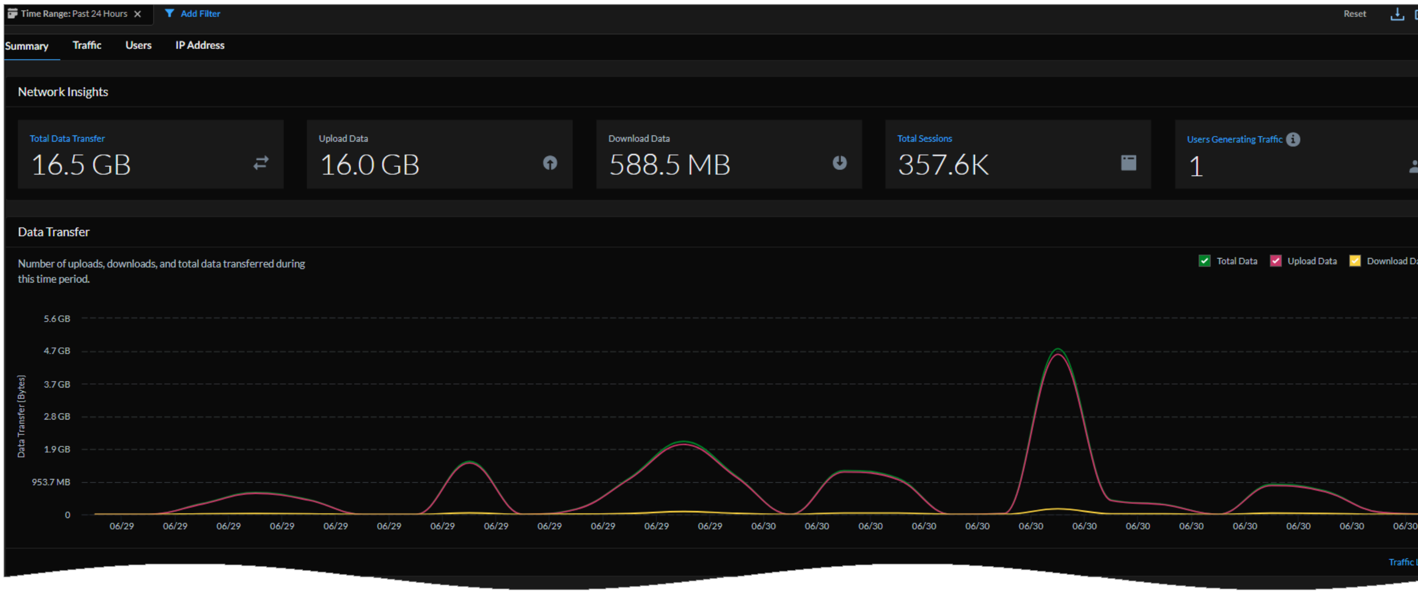
View Network Usage

Where Can I Use This?	What Do I Need?
• NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series, funded with Software NGFW Credits This dashboard is supported for both AIOps for NGFW and Prisma Access.	□ AIOps for NGFW Free (use the AIOps for NGFW Free ap or AIOps for NGFW Premium license (use the Strata Cloud □ Strata Logging Service license □ A role that has permission to view the dashboard □ License to view data from supported product in the dashboard: Prisma Access

The **Network Usage** dashboard shows what's driving your network traffic. Dive in to see who or what is using your network (users, apps, IP addresses, and countries), and the apps and sites they're accessing and their threat exposure.

This dashboard:

- helps you understand the traffic traversing your network, including source to destination flows, and all the users and IP addresses generating traffic. This data helps to decide if you need to refine traffic attributes (source and destination security zone, the source and destination IP address, the application, and the user) in your security rules.
- provides interactive drill downs for you to filter on specific attributes, such as IP address, username, and source location.
- gives you contextual links into Log Viewer, so you can review the log records associated with dashboard data and activities.



Time Range: Past 24 Hours

Network Insights

Total Data Transfer 16.5 GB

Upload Data 16.0 GB

Download Data 588.5 MB

Total Sessions 357.6K

Users Generating Traffic 1

Data Transfer

Number of uploads, downloads, and total data transferred during this time period.

For more information, see Dashboard: Network Usage.

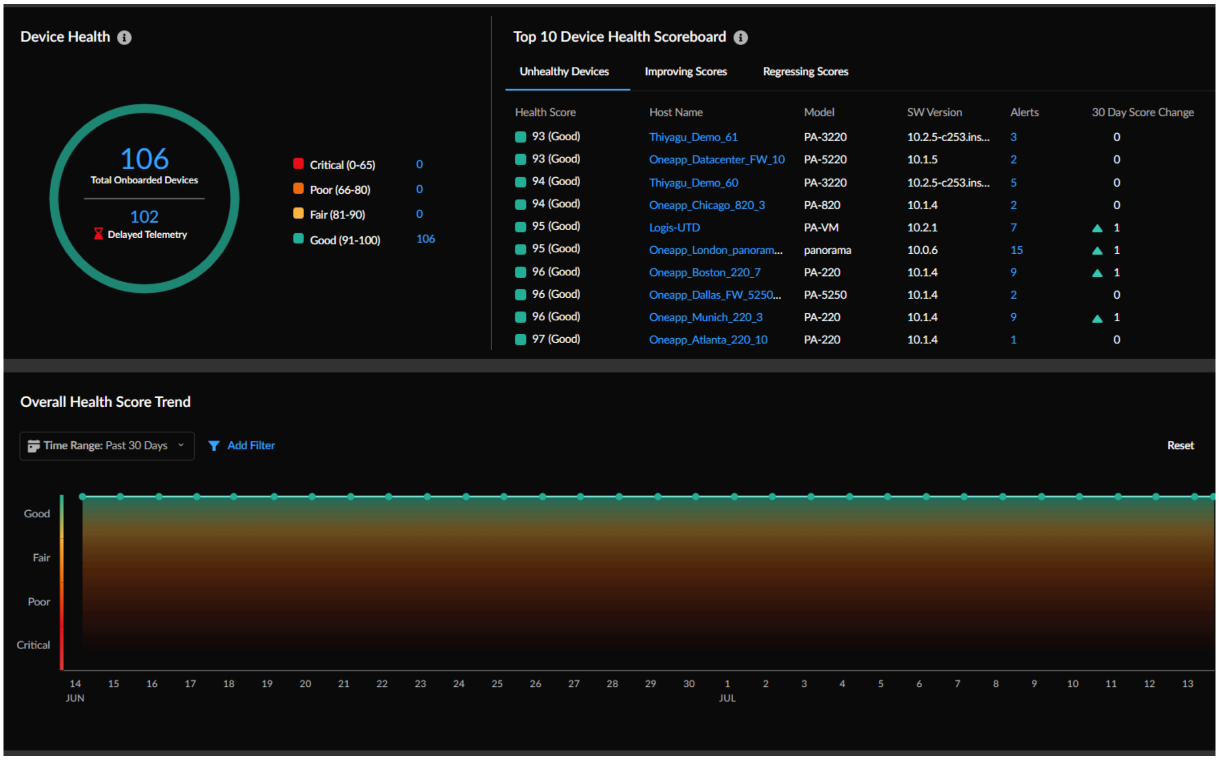
View Device Health

Where Can I Use This?	What Do I Need?
• NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series, funded with Software NGFW Credits	• AIOps for NGFW Free (use the AIOps for NGFW Free ap or • AIOps for NGFW Premium license (use the Strata Cloud

The **Device Health** dashboard shows you the cumulative health status and performance of your deployment based on the health scores of the onboarded NGFWs. The device health is determined by the severity of the health score (0-100) and its corresponding health grade (good, fair, poor, critical). The health score is calculated based on the priority, quantity, type, and status of the open alerts.

This dashboard helps you:

- Understand the deployment improvements that you have made over a period by looking at the historical health score data.
- Narrow down devices that require attention in your deployment and prioritize the issues to resolve them.



Device Health

106 Total Onboarded Devices

102 Delayed Telemetry

🟥 Critical (0-65)	0
🟧 Poor (66-80)	0
🟨 Fair (81-90)	0
🟩 Good (91-100)	106

Top 10 Device Health Scoreboard

Unhealthy Devices | Improving Scores | Regressing Scores

Health Score	Host Name	Model	SW Version	Alerts	30 Day Score Change
🟩 93 (Good)	Thiyagu_Demo_61	PA-3220	10.2.5-c253.ins...	3	0
🟩 93 (Good)	Oneapp_Datacenter_FW_10	PA-5220	10.1.5	2	0
🟩 94 (Good)	Thiyagu_Demo_60	PA-3220	10.2.5-c253.ins...	5	0
🟩 94 (Good)	Oneapp_Chicago_820_3	PA-820	10.1.4	2	0
🟩 95 (Good)	Logis-UTD	PA-VM	10.2.1	7	▲ 1
🟩 95 (Good)	Oneapp_London_panoram...	panorama	10.0.6	15	▲ 1
🟩 96 (Good)	Oneapp_Boston_220_7	PA-220	10.1.4	9	▲ 1
🟩 96 (Good)	Oneapp_Dallas_FW_5250...	PA-5250	10.1.4	2	0
🟩 96 (Good)	Oneapp_Munich_220_3	PA-220	10.1.4	9	▲ 1
🟩 97 (Good)	Oneapp_Atlanta_220_10	PA-220	10.1.4	1	0

Overall Health Score Trend

Time Range: Past 30 Days

For more information, see Dashboard: Device Health.

Get Upgrade Recommendations

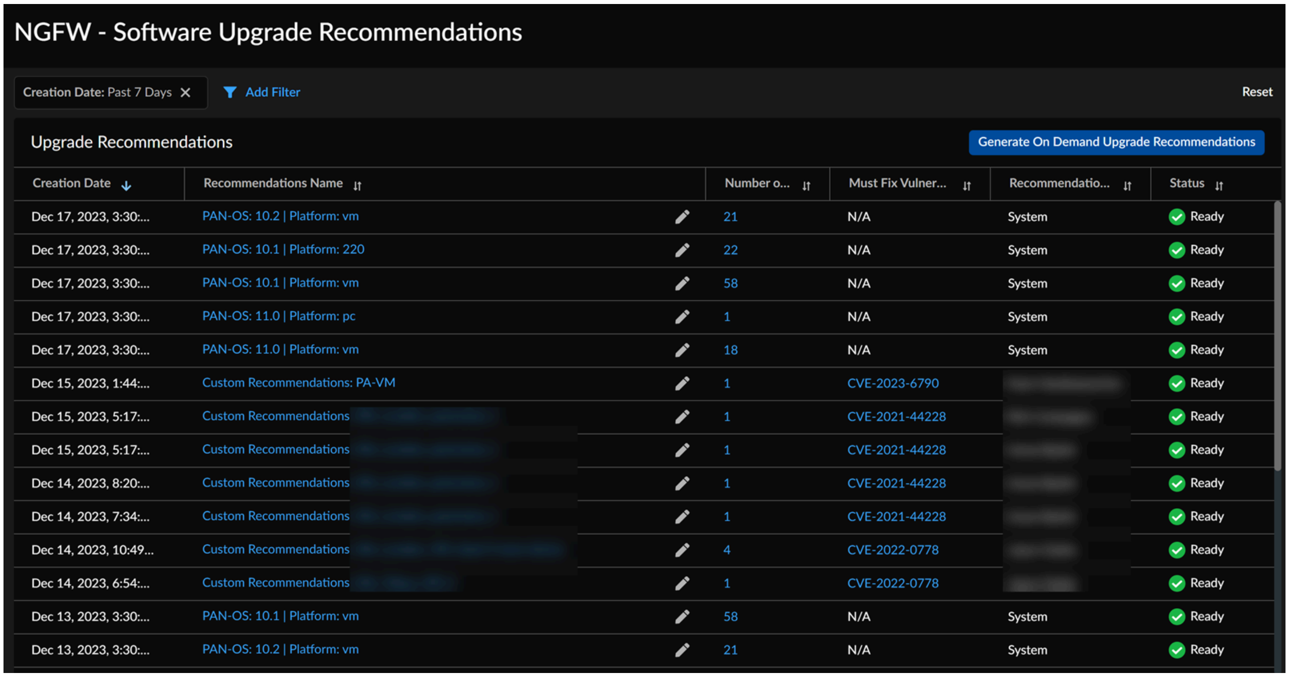
Where Can I Use This?	What Do I Need?
• NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series, funded with Software NGFW Credits	☐ AIOps for NGFW Premium license (use the Strata Cloud

In **Workflows** > **Software Upgrades** > **Upgrade Recommendations**, you can use Strata Cloud Manager to analyze the enabled features on firewalls and create a customized recommendation that includes:

- Best software version for your devices that you can upgrade.
- Information about new features, changes to behavior, vulnerabilities, and software issues in each recommended software version.

The types of upgrade recommendations are:

- System-generated recommendations that are generated from device telemetry data twice a week.
- User-generated custom recommendations that are generated by selecting devices for specific CVEs in PAN-OS CVEs.
- User-generated recommendations that are generated by uploading a Tech Support File (TSF) of a firewall.



NGFW - Software Upgrade Recommendations

Creation Date: Past 7 Days ✕
Add Filter
Reset
Generate On Demand Upgrade Recommendations

Upgrade Recommendations

Creation Date	Recommendations Name	Number o...	Must Fix Vulner...	Recommendatio...	Status
Dec 17, 2023, 3:30:...	PAN-OS: 10.2 | Platform: vm	21	N/A	System	✓ Ready
Dec 17, 2023, 3:30:...	PAN-OS: 10.1 | Platform: 220	22	N/A	System	✓ Ready
Dec 17, 2023, 3:30:...	PAN-OS: 10.1 | Platform: vm	58	N/A	System	✓ Ready
Dec 17, 2023, 3:30:...	PAN-OS: 11.0 | Platform: pc	1	N/A	System	✓ Ready
Dec 17, 2023, 3:30:...	PAN-OS: 11.0 | Platform: vm	18	N/A	System	✓ Ready
Dec 15, 2023, 1:44:...	Custom Recommendations: PA-VM	1	CVE-2023-6790	[redacted]	✓ Ready
Dec 15, 2023, 5:17:...	Custom Recommendations [redacted]	1	CVE-2021-44228	[redacted]	✓ Ready
Dec 15, 2023, 5:17:...	Custom Recommendations [redacted]	1	CVE-2021-44228	[redacted]	✓ Ready
Dec 14, 2023, 8:20:...	Custom Recommendations [redacted]	1	CVE-2021-44228	[redacted]	✓ Ready
Dec 14, 2023, 7:34:...	Custom Recommendations [redacted]	1	CVE-2021-44228	[redacted]	✓ Ready
Dec 14, 2023, 10:49...	Custom Recommendations [redacted]	4	CVE-2022-0778	[redacted]	✓ Ready
Dec 14, 2023, 6:54:...	Custom Recommendations [redacted]	1	CVE-2022-0778	[redacted]	✓ Ready
Dec 13, 2023, 3:30:...	PAN-OS: 10.1 | Platform: vm	58	N/A	System	✓ Ready
Dec 13, 2023, 3:30:...	PAN-OS: 10.2 | Platform: vm	21	N/A	System	✓ Ready

For every recommendation, you can:

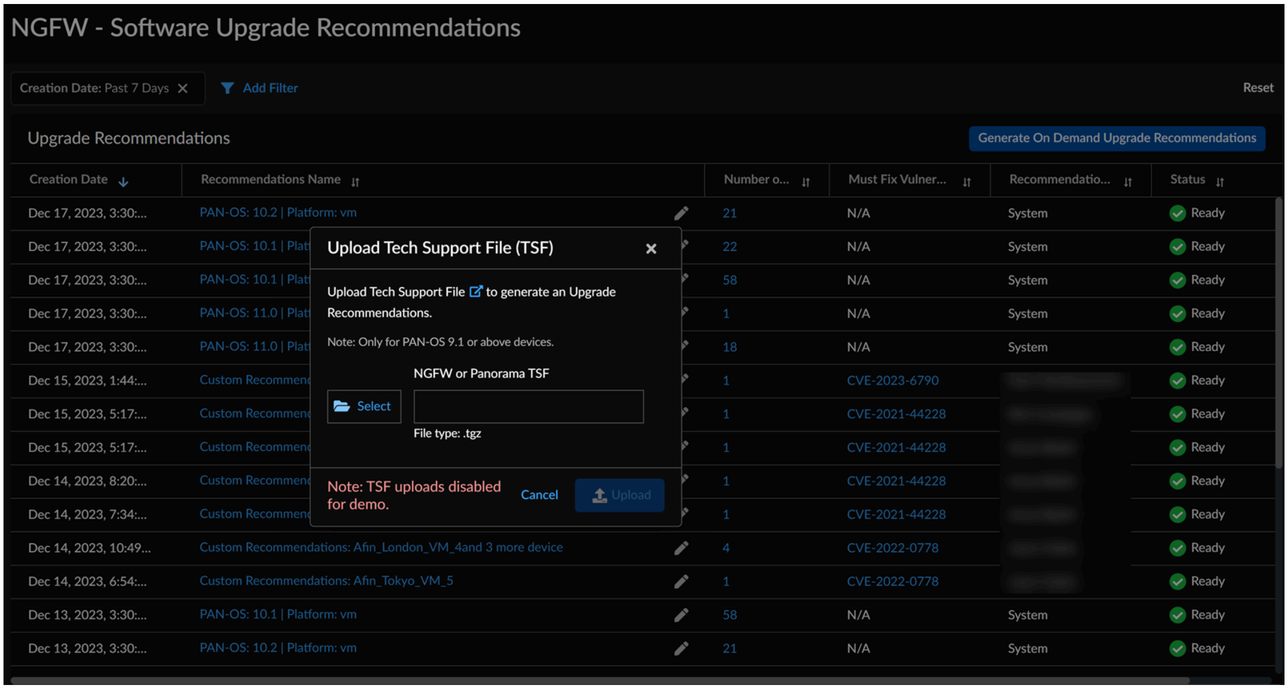
- view the number of devices that require an upgrade and the must fix vulnerabilities.

- edit the name of a recommendation to differentiate custom recommendations.
- filter the recommendations by **Creation Date**, **Recommendations Name**, and **Recommendations Generated By**.
- delete recommendations that failed or are no longer necessary.

Generate On-Demand Upgrade Recommendations

1. From **Upgrade Recommendations**, **Generate On Demand Upgrade Recommendations**.
2. **Select** a Tech Support File (TSF) and **Upload**.

   - *You can upload TSF of only one device at a time and it must be TSF in the .tgz file format.*
   - *Software Upgrade Recommendations supports TSF from devices with the PAN-OS version 9.1 or above for report generation.*



NGFW - Software Upgrade Recommendations

Creation Date: Past 7 Days ✕
Add Filter
Reset
Generate On Demand Upgrade Recommendations

Upgrade Recommendations

Creation Date	Recommendations Name	Number o...	Must Fix Vulner...	Recommendatio...	Status
Dec 17, 2023, 3:30:...	PAN-OS: 10.2 | Platform: vm	21	N/A	System	✓ Ready
Dec 17, 2023, 3:30:...	PAN-OS: 10.1 | Plat	22	N/A	System	✓ Ready
Dec 17, 2023, 3:30:...	PAN-OS: 10.1 | Plat	58	N/A	System	✓ Ready
Dec 17, 2023, 3:30:...	PAN-OS: 11.0 | Plat	1	N/A	System	✓ Ready
Dec 17, 2023, 3:30:...	PAN-OS: 11.0 | Plat	18	N/A	System	✓ Ready
Dec 15, 2023, 1:44:...	Custom Recommen	1	CVE-2023-6790	[redacted]	✓ Ready
Dec 15, 2023, 5:17:...	Custom Recommen	1	CVE-2021-44228	[redacted]	✓ Ready
Dec 15, 2023, 5:17:...	Custom Recommen	1	CVE-2021-44228	[redacted]	✓ Ready
Dec 14, 2023, 8:20:...	Custom Recommen	1	CVE-2021-44228	[redacted]	✓ Ready
Dec 14, 2023, 7:34:...	Custom Recommen	1	CVE-2021-44228	[redacted]	✓ Ready
Dec 14, 2023, 10:49...	Custom Recommendations: Afin_London_VM_4and 3 more device	4	CVE-2022-0778	[redacted]	✓ Ready
Dec 14, 2023, 6:54:...	Custom Recommendations: Afin_Tokyo_VM_5	1	CVE-2022-0778	[redacted]	✓ Ready
Dec 13, 2023, 3:30:...	PAN-OS: 10.1 | Platform: vm	58	N/A	System	✓ Ready
Dec 13, 2023, 3:30:...	PAN-OS: 10.2 | Platform: vm	21	N/A	System	✓ Ready

Upload Tech Support File (TSF) ✕

Upload Tech Support File to generate an Upgrade Recommendations.

Note: Only for PAN-OS 9.1 or above devices.

NGFW or Panorama TSF

File type: .tgz

Note: TSF uploads disabled for demo.

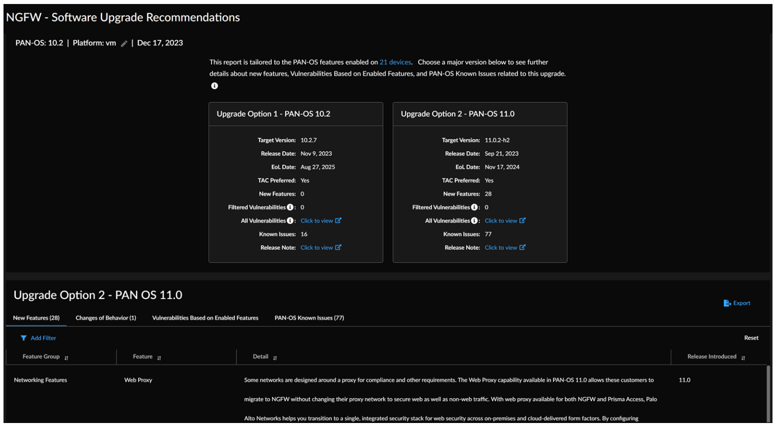
3. View the software upgrade recommendations after the status is **Ready**.

   You can also check the **Status** column to see if there are any errors related to the upload, file format, or processing of the TSF file.

View Software Upgrade Recommendation Report

Click a recommendation to view the detailed report with the upgrade options for the devices. Choose an upgrade option to view further details about **New Features**, **Changes of Behavior**, **Vulnerabilities Based on Enabled Features**, and **PAN-OS Known Issues**. You can click **Export** to download this report in a CSV format.

- *The recommendation report is generated based on the enabled features within your devices.*
- *For a known issue under* ***PAN-OS Known Issues****, the value under* ***Associated Case Count*** *is obtained by the number of customers who have reported this issue.*



NGFW - Software Upgrade Recommendations

PAN-OS: 10.2 | Platform: vm | Dec 17, 2023

This report is tailored to the PAN-OS features enabled on 21 devices. Choose a major version below to see further details about new features, Vulnerabilities Based on Enabled Features, and PAN-OS Known Issues related to this upgrade.

Upgrade Option 1 - PAN-OS 10.2

Target Version: 10.2.7
Release Date: Nov 9, 2023
EoL Date: Aug 27, 2025
TAC Preferred: Yes
New Features: 0
Filtered Vulnerabilities: 0
All Vulnerabilities: Click to view
Known Issues: 16
Release Note: Click to view

Upgrade Option 2 - PAN-OS 11.0

Target Version: 11.0.2-h2
Release Date: Sep 21, 2023
EoL Date: Nov 17, 2024
TAC Preferred: Yes
New Features: 28
Filtered Vulnerabilities: 0
All Vulnerabilities: Click to view
Known Issues: 77
Release Note: Click to view

Upgrade Option 2 - PAN OS 11.0

Feature Group	Feature	Detail	Release Introduced
Networking Features	Web Proxy	Some networks are designed around a proxy for compliance and other requirements. The Web Proxy capability available in PAN-OS 11.0 allows these customers to migrate to NGFW without changing their proxy network to secure web as well as non-web traffic. With web proxy available for both NGFW and Prisma Access, Palo Alto Networks helps you transition to a single, integrated security stack for web security across on-premises and cloud-delivered form factors. By configuring	11.0

Analyze Metric Capacity

Where Can I Use This?	What Do I Need?
- NGFW (Managed by Strata Cloud Manager) - NGFW (Managed by PAN-OS or Panorama)	□ AIOps for NGFW Premium license (use the Strata Cloud

From Strata Cloud Manager, navigate to **Monitor** > **Capacity Analyzer** to analyze and monitor your devices' resource capacity by keeping track of their metrics usage based on their model types. You can analyze metrics using the following methods:

- Analyze Metric Capacity based on Metric, Model, and Device
- Analyze Metric Capacity Based on Based on Device Models
- Analyze Metric Capacity Based on Metrics

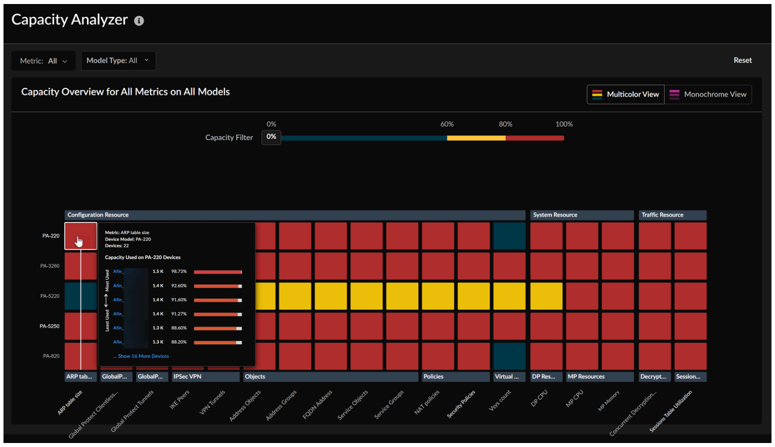
Capacity Analyzer is enhanced to support alerts that help you to anticipate resource consumption nearing its maximum capacity and raise alerts. See Manage Capacity Analyzer Alerts.

*The **Capacity Analyzer** feature is not supported for the VM Series firewalls.*

Analyze Metric Capacity based on Metric, Model, and Device

1. On the Capacity Analyzer Heatmap, hover your cursor over a cell to view the metric capacity usage for all devices belonging to the corresponding device model.

   In this example, the pop-up window displays the **ARP table size** metric capacity for all the devices that belong to the **PA-220** model.



Metric: All
Model Type: All

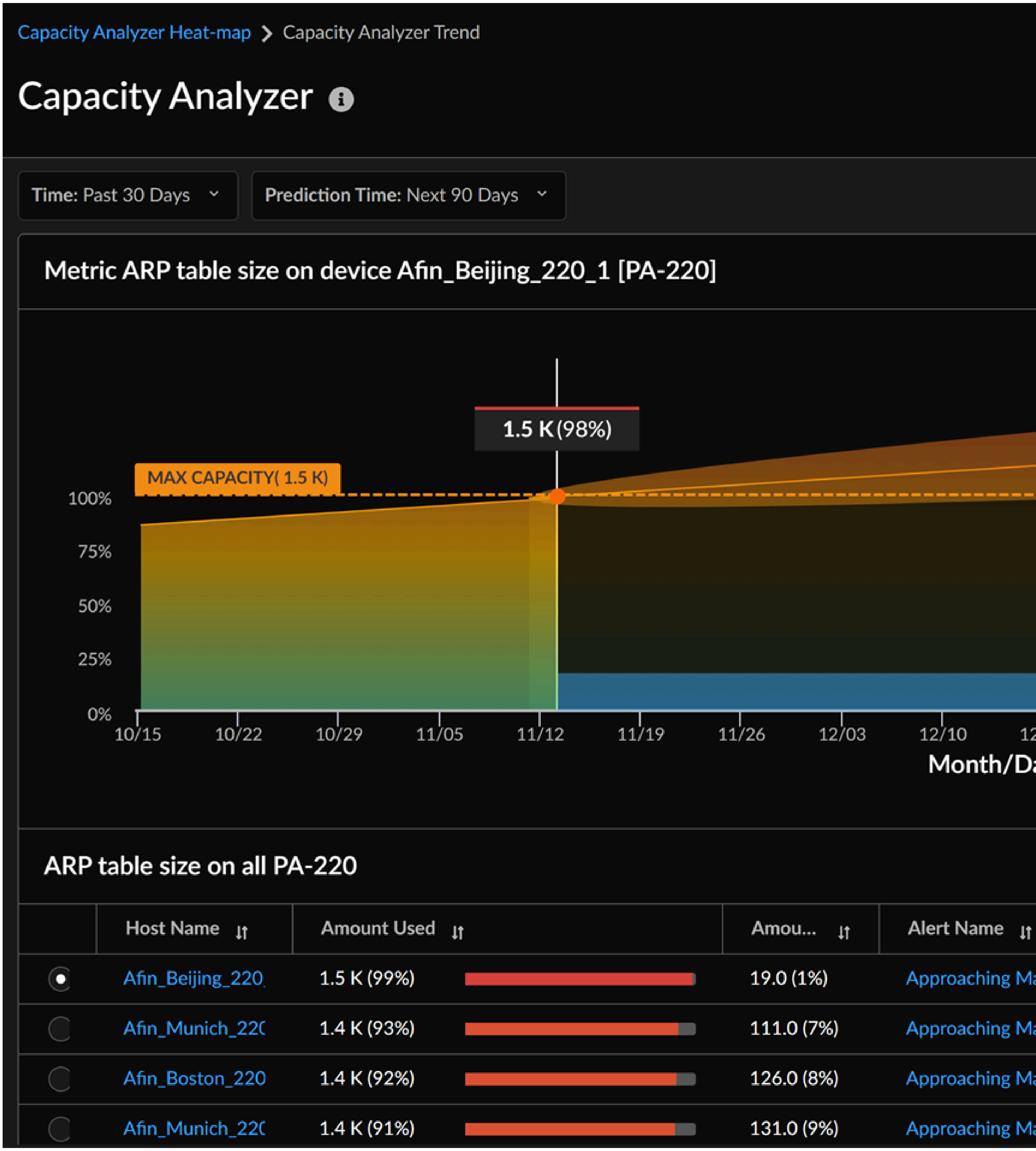
Metric: ARP table size
Device Model: PA-220
Devices: 22

Capacity Used on PA-220 Devices

Afin_	1.5 K	98.73%
Afin_	1.4 K	92.60%
Afin_	1.4 K	91.60%
Afin_	1.4 K	91.27%
Afin_	1.3 K	88.60%
Afin_	1.3 K	88.20%

... Show 16 More Devices

2. Click a cell corresponding to the device model and the metric to check the capacity usage. In this example, we are clicking the ARP table size for the **PA-220** device model.



Capacity Analyzer Heat-map > Capacity Analyzer Trend

Capacity Analyzer

Time: Past 30 Days

Prediction Time: Next 90 Days

Metric ARP table size on device Afin_Beijing_220_1 [PA-220]

ARP table size on all PA-220

	Host Name	Amount Used	Amou...	Alert Name
●	Afin_Beijing_220	1.5 K (99%)	19.0 (1%)	Approaching Ma
○	Afin_Munich_220	1.4 K (93%)	111.0 (7%)	Approaching Ma
○	Afin_Boston_220	1.4 K (92%)	126.0 (8%)	Approaching Ma
○	Afin_Munich_220	1.4 K (91%)	131.0 (9%)	Approaching Ma

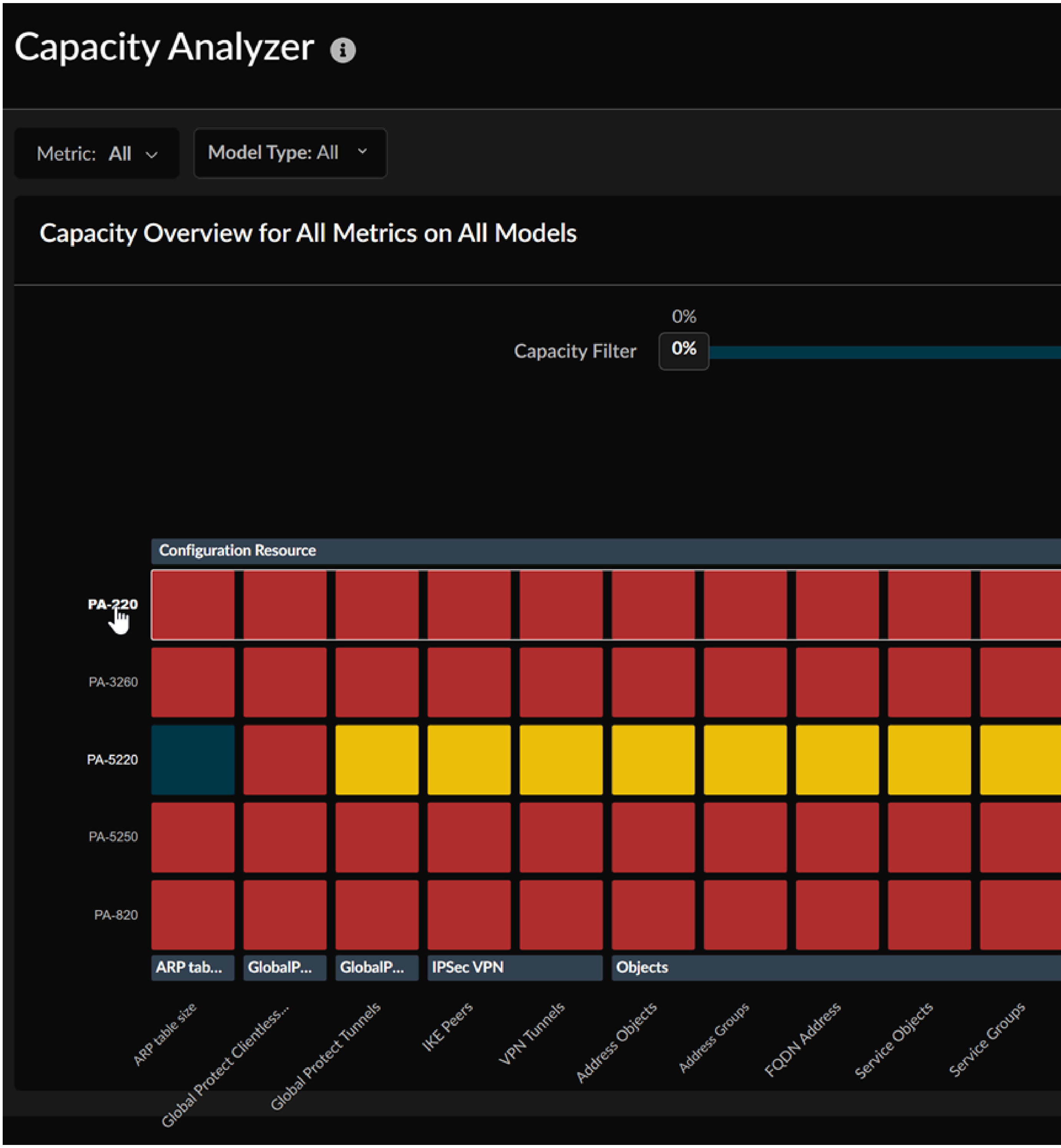
You can view the following:

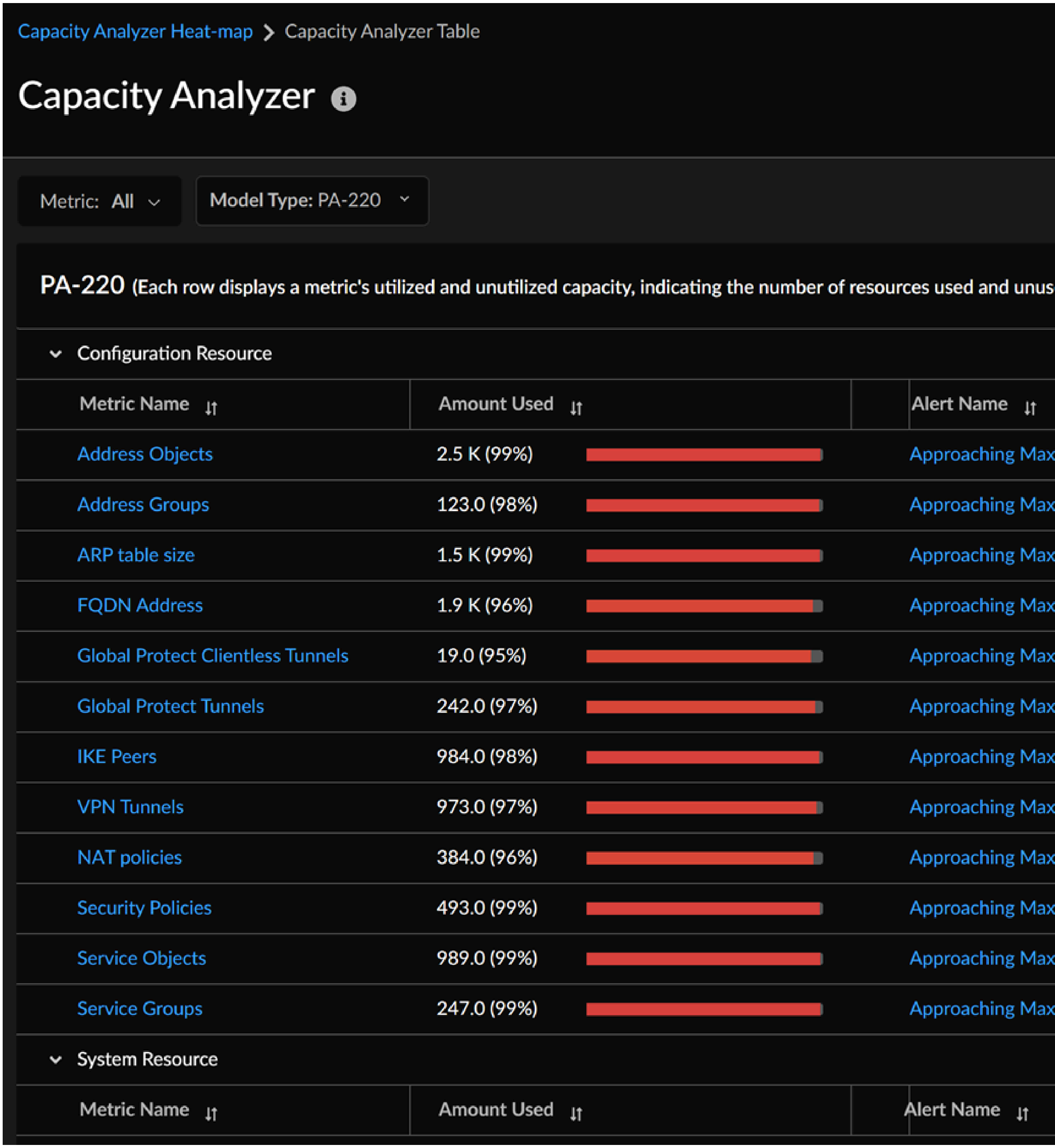
- ARP table size metric capacity for all devices belonging to the **PA-220** model.

- Select one of the host names to view the metric capacity trend.
- Alerts raised for the metric and predicted date when the metric will reach its maximum capacity.
- Predicted trend for the metric. Strata Cloud Manager forecasts the date when the metric will hit the maximum capacity. You can hover your cursor over the graph to check the metric capacity at any specific point of time.

Analyze Metric Capacity Based on Device Models

1. From the Capacity Analyzer heat map, select a device model to view all its associated metrics.





Capacity Analyzer Heat-map > Capacity Analyzer Table

Capacity Analyzer

Metric: All

Model Type: PA-220

PA-220 (Each row displays a metric's utilized and unutilized capacity, indicating the number of resources used and unus

Configuration Resource

Metric Name	Amount Used	Alert Name
Address Objects	2.5 K (99%)	Approaching Max
Address Groups	123.0 (98%)	Approaching Max
ARP table size	1.5 K (99%)	Approaching Max
FQDN Address	1.9 K (96%)	Approaching Max
Global Protect Clientless Tunnels	19.0 (95%)	Approaching Max
Global Protect Tunnels	242.0 (97%)	Approaching Max
IKE Peers	984.0 (98%)	Approaching Max
VPN Tunnels	973.0 (97%)	Approaching Max
NAT policies	384.0 (96%)	Approaching Max
Security Policies	493.0 (99%)	Approaching Max
Service Objects	989.0 (99%)	Approaching Max
Service Groups	247.0 (99%)	Approaching Max

System Resource

Metric Name	Amount Used	Alert Name

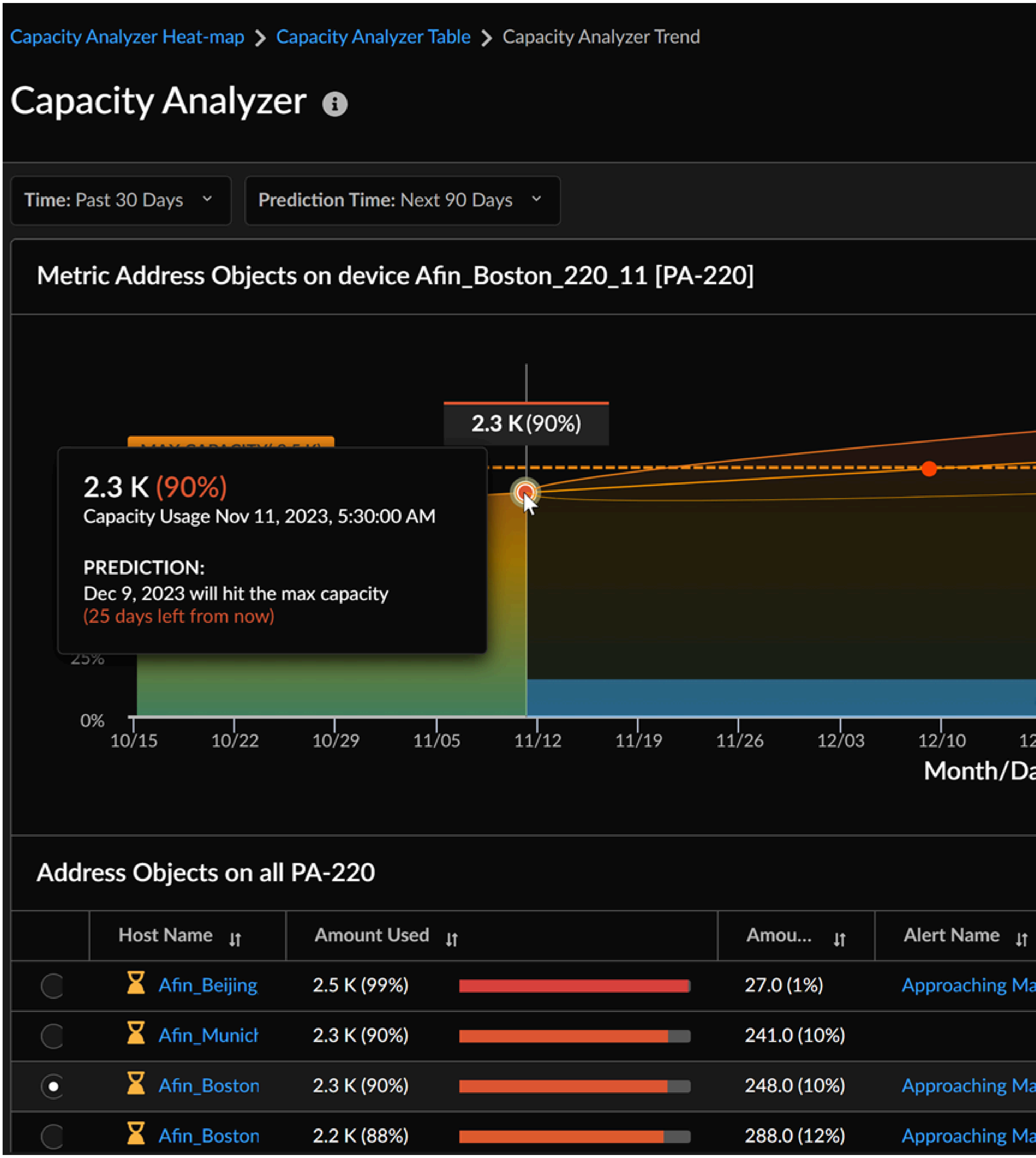
Each row displays a metric's utilized capacity, indicating the number of resources used for that metric in a device. Additionally, you can view the alerts raised for the metric and predicted date when the metric will reach its maximum capacity.

2. In the Capacity Analyzer table, select a metric to view its trend on a device.

3. Select a device to view the metric trend for it.

   You can select the **Prediction Time** to check the predicted trend for the metric. Strata Cloud Manager forecasts the date when the metric will hit the maximum capacity.

   You can hover your cursor over the graph to check the metric capacity at any specific point of time.



Capacity Analyzer Heat-map > Capacity Analyzer Table > Capacity Analyzer Trend

Capacity Analyzer

Time: Past 30 Days

Prediction Time: Next 90 Days

Metric Address Objects on device Afin_Boston_220_11 [PA-220]

2.3 K (90%)

Capacity Usage Nov 11, 2023, 5:30:00 AM

PREDICTION:

Dec 9, 2023 will hit the max capacity

(25 days left from now)

Address Objects on all PA-220

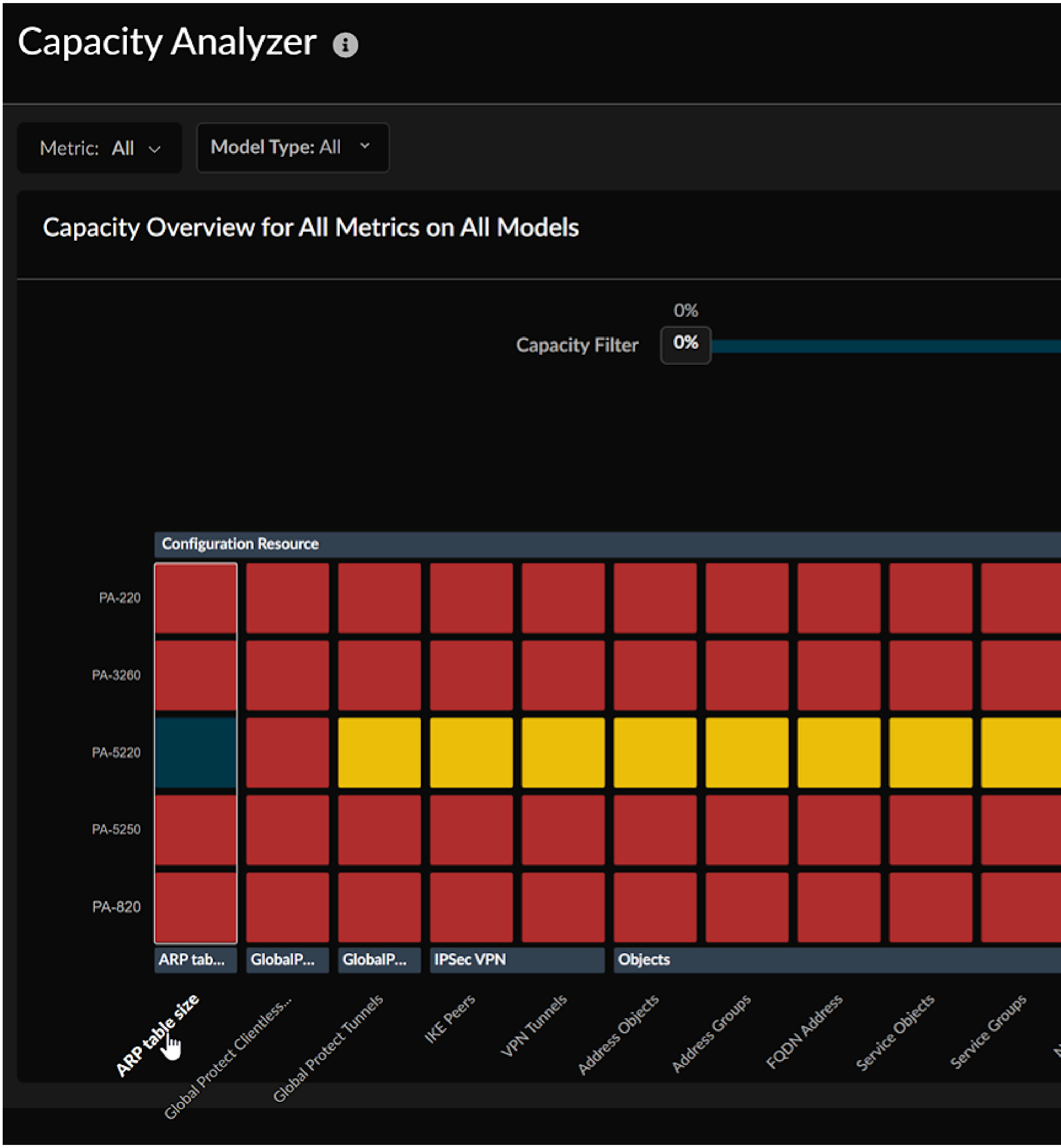
	Host Name	Amount Used		Amou...	Alert Name
○	⌛ Afin_Beijing	2.5 K (99%)		27.0 (1%)	Approaching Ma
○	⌛ Afin_Munich	2.3 K (90%)		241.0 (10%)	
●	⌛ Afin_Boston	2.3 K (90%)		248.0 (10%)	Approaching Ma
○	⌛ Afin_Boston	2.2 K (88%)		288.0 (12%)	Approaching Ma

Under **Alert Name**, you can view the alerts raised for the address objects metric corresponding to a host name.

Analyze Metric Capacity Based on Metrics

1. From the Capacity Analyzer heat map, select a metric to view its capacity in all the devices in a tabular format. In this example, the **ARP table size** metric is selected.

   *You can also select a metric type and drill down to a metric to view its capacity in all the devices in a tabular format. For example, **Configuration Resource** type metric > **Objects** > **Address Objects**.*



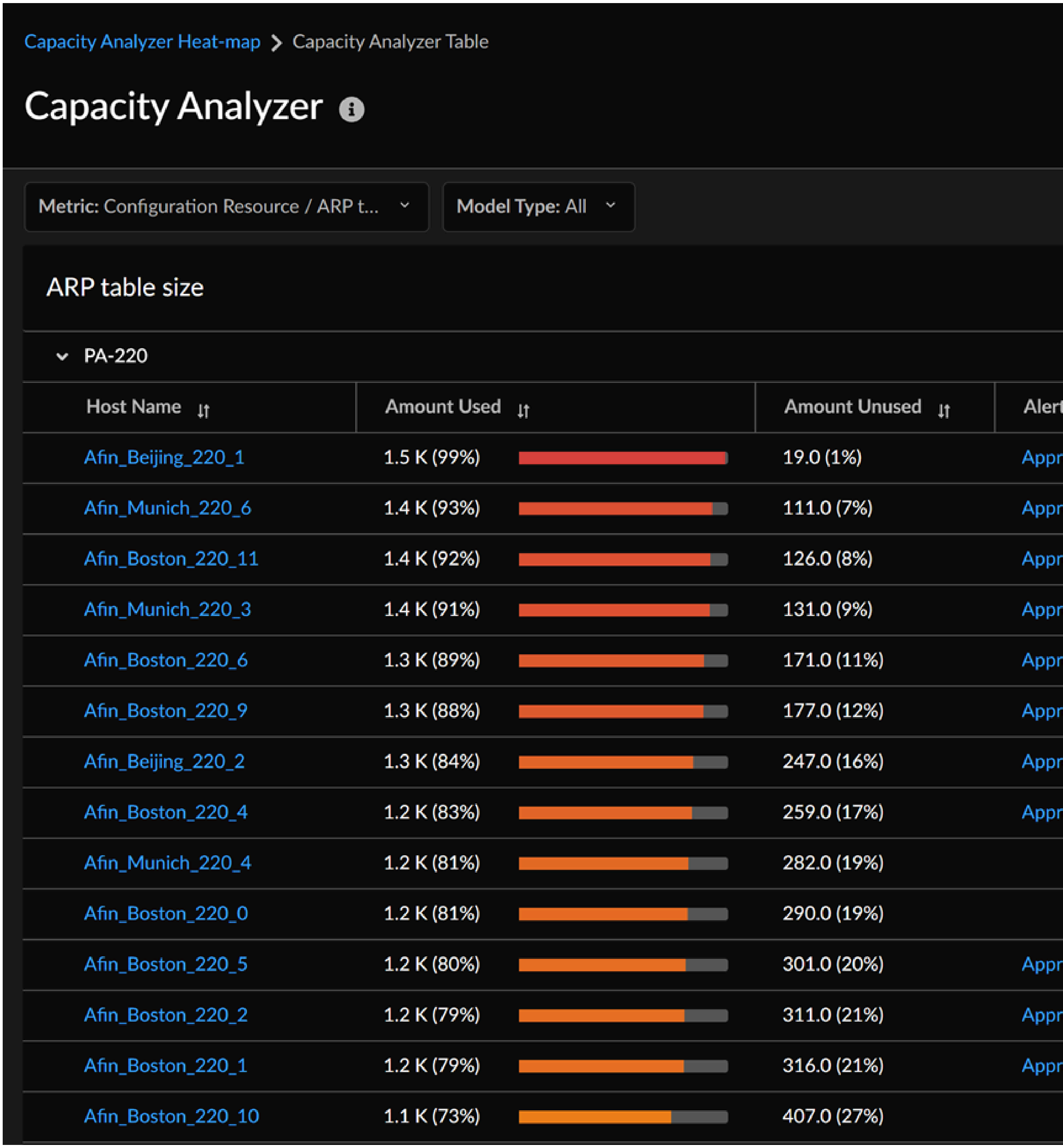
Capacity Analyzer

Metric: All

Model Type: All

Capacity Overview for All Metrics on All Models

Capacity Filter 0%



Capacity Analyzer Heat-map > Capacity Analyzer Table

Capacity Analyzer

Metric: Configuration Resource / ARP t...

Model Type: All

ARP table size

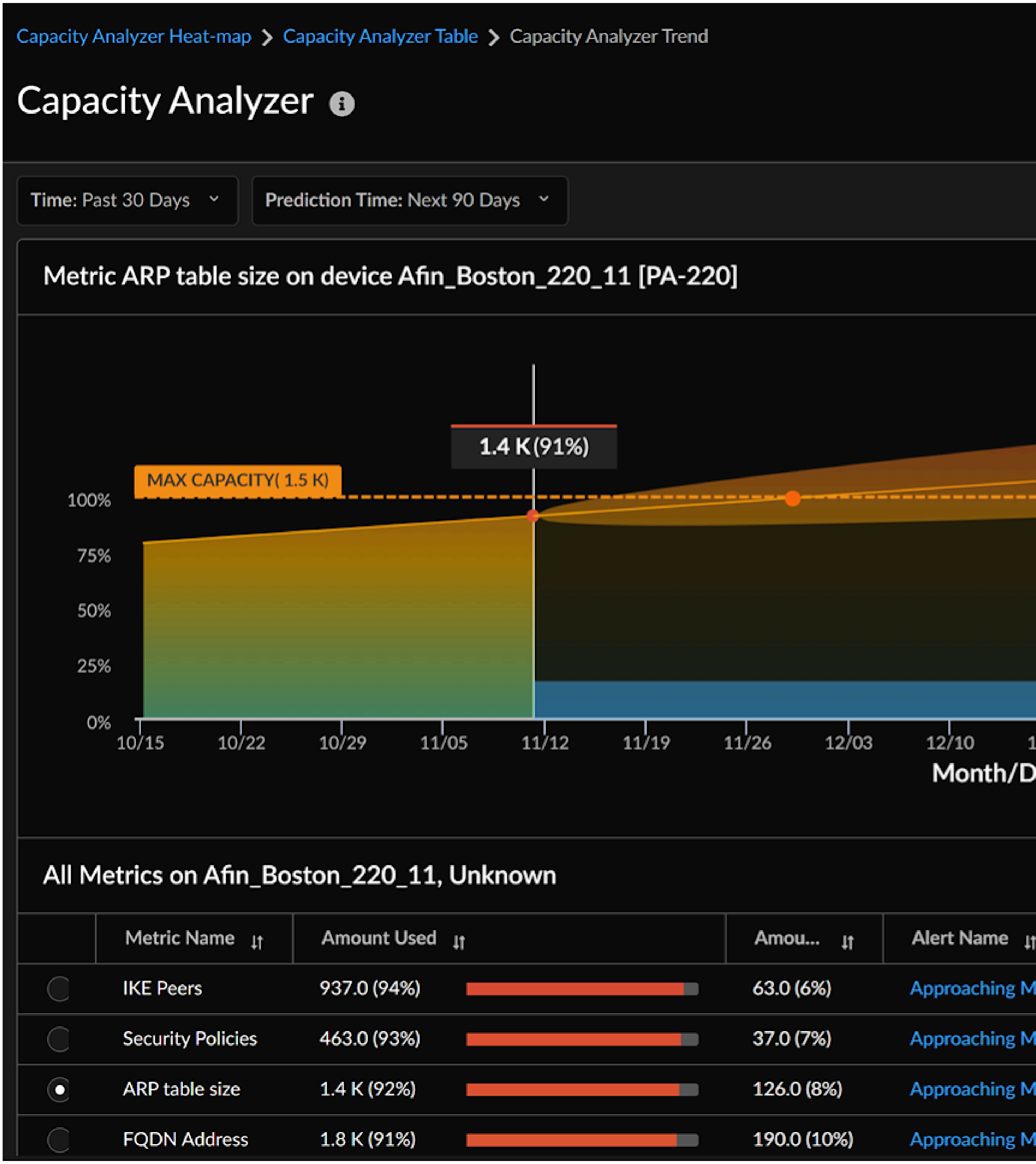
PA-220

Host Name	Amount Used	Amount Unused	Aler
Afin_Beijing_220_1	1.5 K (99%)	19.0 (1%)	Appr
Afin_Munich_220_6	1.4 K (93%)	111.0 (7%)	Appr
Afin_Boston_220_11	1.4 K (92%)	126.0 (8%)	Appr
Afin_Munich_220_3	1.4 K (91%)	131.0 (9%)	Appr
Afin_Boston_220_6	1.3 K (89%)	171.0 (11%)	Appr
Afin_Boston_220_9	1.3 K (88%)	177.0 (12%)	Appr
Afin_Beijing_220_2	1.3 K (84%)	247.0 (16%)	Appr
Afin_Boston_220_4	1.2 K (83%)	259.0 (17%)	Appr
Afin_Munich_220_4	1.2 K (81%)	282.0 (19%)	
Afin_Boston_220_0	1.2 K (81%)	290.0 (19%)	
Afin_Boston_220_5	1.2 K (80%)	301.0 (20%)	Appr
Afin_Boston_220_2	1.2 K (79%)	311.0 (21%)	Appr
Afin_Boston_220_1	1.2 K (79%)	316.0 (21%)	Appr
Afin_Boston_220_10	1.1 K (73%)	407.0 (27%)	

Each row displays the **ARP table size** metric's used and unused capacity for every host under device models. Additionally, you can view the alerts raised for this metric for every host and the predicted date when the metric will reach its maximum capacity.

2. Select a host name to view the graphical trend of the selected metric.

   You can select the **Prediction Time** to check the predicted trend for the metric. Strata Cloud Manager forecasts the date when the metric will hit the maximum capacity.



Capacity Analyzer Heat-map > Capacity Analyzer Table > Capacity Analyzer Trend

Capacity Analyzer

Time: Past 30 Days

Prediction Time: Next 90 Days

Metric ARP table size on device Afin_Boston_220_11 [PA-220]

All Metrics on Afin_Boston_220_11, Unknown

	Metric Name	Amount Used		Amou...	Alert Name
○	IKE Peers	937.0 (94%)		63.0 (6%)	Approaching M
○	Security Policies	463.0 (93%)		37.0 (7%)	Approaching M
●	ARP table size	1.4 K (92%)		126.0 (8%)	Approaching M
○	FQDN Address	1.8 K (91%)		190.0 (10%)	Approaching M

You can hover your cursor over the graph to check the metric capacity at any specific point of time.

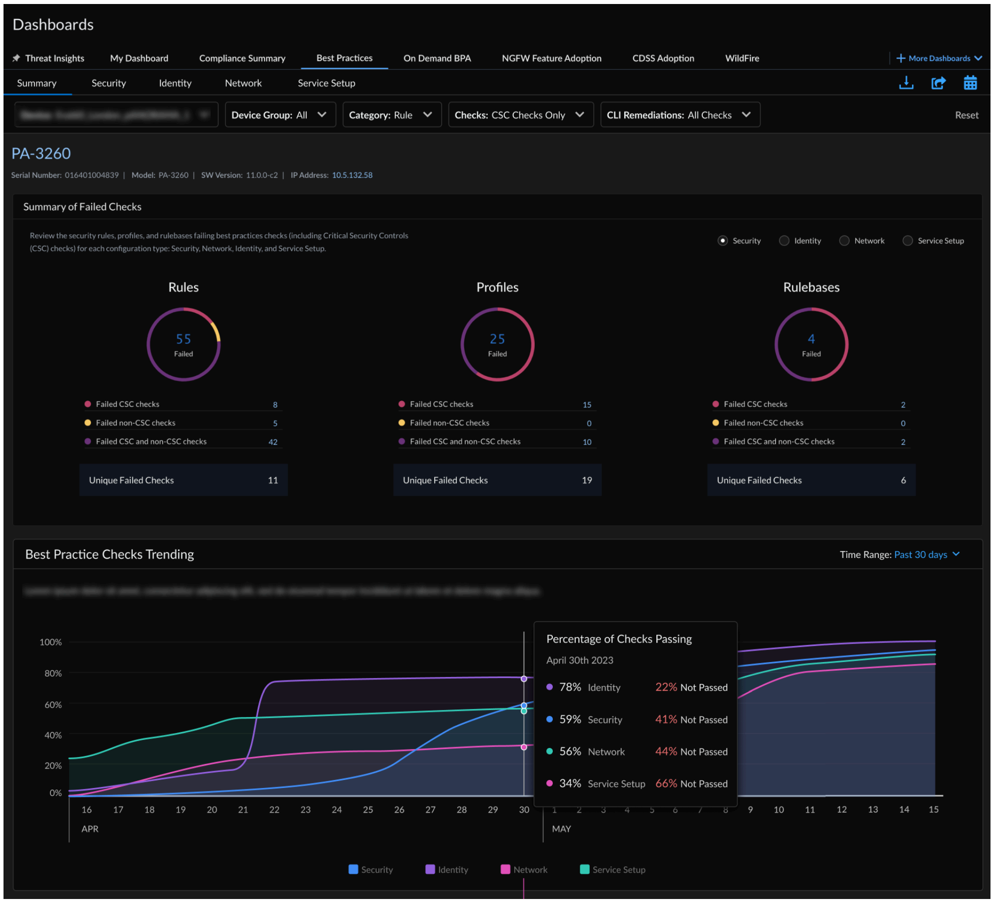
Best Practices in NGFWs

Where Can I Use This?	What Do I Need?
• NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series, funded with Software NGFW Credits	• AIOps for NGFW Free (use the AIOps for NGFW Free ap or • AIOps for NGFW Premium license (use the Strata Cloud

AIOps for NGFW helps you tighten security posture by aligning with best practices. You can leverage AIOps for NGFW to assess your Panorama, NGFW, and Panorama-managed Prisma Access security configurations against best practices and remediate failed best practice checks. AIOps for NGFW streamlines the process of checking InfoSec compliance on your network infrastructure.

AIOps for NGFW is free, and the following AIOps Best Practice Assessment (BPA) capabilities are available without an AIOps premium license. For the full list of available Best Practice features, see Built-In Best Practices:

- Check the Best Practices Dashboard for daily best practices reports, and their mapping to Center for Internet Security's Critical Security Controls (CSC) checks, to help you identify areas where you can make changes to improve your best practices compliance. Share the best practice report as a PDF and schedule it to be regularly delivered to your inbox.



[redacted] | Device Group: All | Category: Rule | Checks: CSC Checks Only | CLI Remediations: All Checks

PA-3260

Serial Number: 016401004839 | Model: PA-3260 | SW Version: 11.0.0-c2 | IP Address: 10.5.132.58

Summary of Failed Checks

Review the security rules, profiles, and rulebases failing best practices checks (including Critical Security Controls (CSC) checks) for each configuration type: Security, Network, Identity, and Service Setup.

● Security ○ Identity ○ Network ○ Service Setup

	Rules	Profiles	Rulebases
Failed	55	25	4
Failed CSC checks	8	15	2
Failed non-CSC checks	5	0	0
Failed CSC and non-CSC checks	42	10	2
Unique Failed Checks	11	19	6

Best Practice Checks Trending

Time Range: Past 30 days

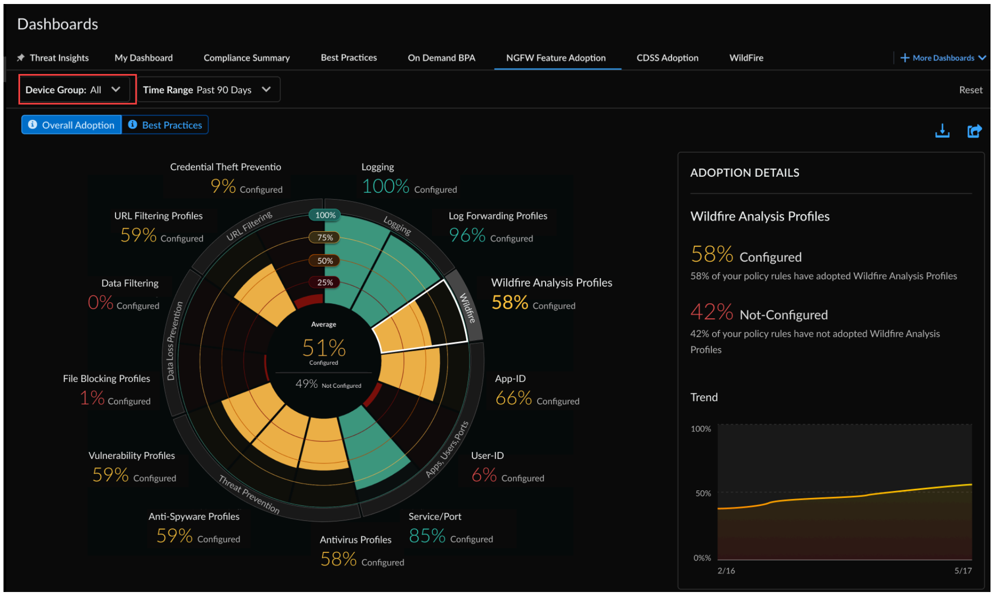
[redacted]

Percentage of Checks Passing

April 30th 2023

78%	Identity	22% Not Passed
59%	Security	41% Not Passed
56%	Network	44% Not Passed
34%	Service Setup	66% Not Passed

- Monitor Feature Adoption and stay abreast of which security features you're using in your deployment and potential gaps in coverage.



Device Group: All | Time Range Past 90 Days

Feature	Configured
Credential Theft Preventio	9% Configured
Logging	100% Configured
URL Filtering Profiles	59% Configured
Log Forwarding Profiles	96% Configured
Data Filtering	0% Configured
Wildfire Analysis Profiles	58% Configured
File Blocking Profiles	1% Configured
App-ID	66% Configured
Vulnerability Profiles	59% Configured
User-ID	6% Configured
Anti-Spyware Profiles	59% Configured
Service/Port	85% Configured
Antivirus Profiles	58% Configured

Average 51% Configured

49% Not Configured

ADOPTION DETAILS

Wildfire Analysis Profiles

58% Configured

58% of your policy rules have adopted Wildfire Analysis Profiles

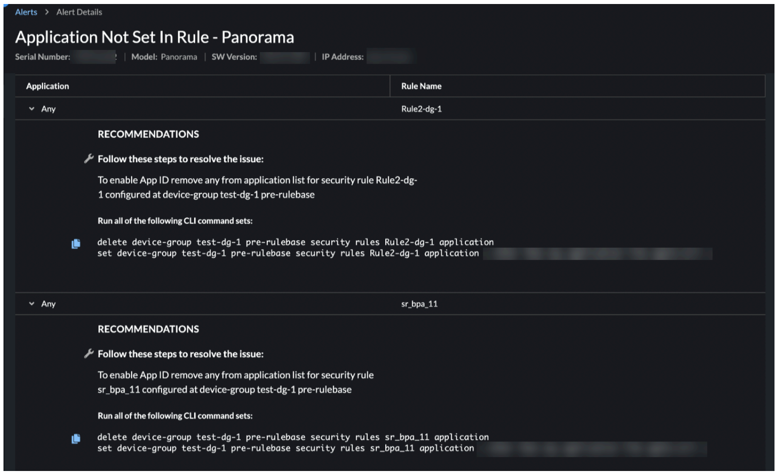
42% Not-Configured

42% of your policy rules have not adopted Wildfire Analysis Profiles

Trend

- Get Security Posture Alerts from AIOps for NGFW to know when your security settings may need a closer look.

  Command Line Interface (CLI) remediations are also available in AIOps for NGFW under **Alerts** > **Security** > **Alert Details**. View recommendations intended to help you to remediate the issues triggering an alert.

  Alerts > Alert Details

  Application Not Set In Rule - Panorama

  Serial Number: [redacted] | Model: Panorama | SW Version: [redacted] | IP Address: [redacted]

Application	Rule Name
Any	Rule2-dg-1

  RECOMMENDATIONS

  Follow these steps to resolve the issue:

  To enable App ID remove any from application list for security rule Rule2-dg-1 configured at device-group test-dg-1 pre-rulebase

  Run all of the following CLI command sets:

  ```
  delete device-group test-dg-1 pre-rulebase security rules Rule2-dg-1 application
  set device-group test-dg-1 pre-rulebase security rules Rule2-dg-1 application [redacted]
  ```

Application	Rule Name
Any	sr_bpa_11

  RECOMMENDATIONS

  Follow these steps to resolve the issue:

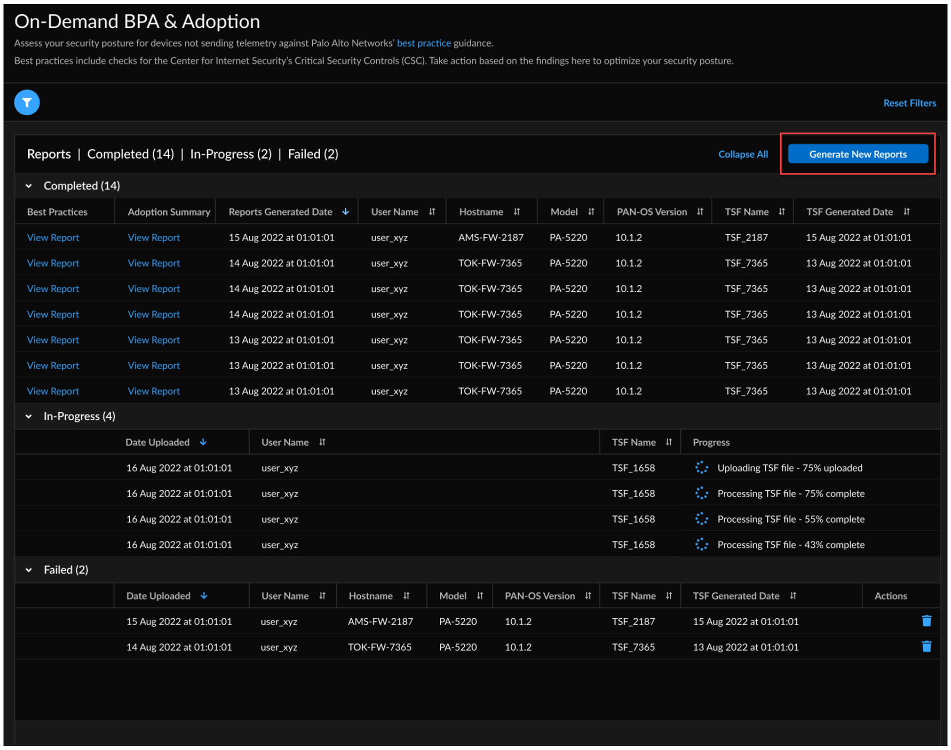
  To enable App ID remove any from application list for security rule sr_bpa_11 configured at device-group test-dg-1 pre-rulebase

  Run all of the following CLI command sets:

  ```
  delete device-group test-dg-1 pre-rulebase security rules sr_bpa_11 application
  set device-group test-dg-1 pre-rulebase security rules sr_bpa_11 application [redacted]
  ```

  Security alerts and CLI remediations are available only for devices sharing telemetry. This feature doesn't support Tech Support File (TSF) manual upload for PAN-OS devices running versions 9.1 and above.

- Generate BPA reports for (non-telemetry) PAN-OS devices running versions 9.1 and above, now including feature adoption metrics. If you've been using the BPA standalone tool to generate BPA reports, you might be wondering "Can I Still Generate BPA Reports from the Customer Support Portal?" We've got you covered as well.

  On-Demand BPA & Adoption

  Assess your security posture for devices not sending telemetry against Palo Alto Networks' best practice guidance.

  Best practices include checks for the Center for Internet Security's Critical Security Controls (CSC). Take action based on the findings here to optimize your security posture.

  Reports | Completed (14) | In-Progress (2) | Failed (2)

  Completed (14)

Best Practices	Adoption Summary	Reports Generated Date	User Name	Hostname	Model	PAN-OS Version	TSF Name	TSF Generated Date
View Report	View Report	15 Aug 2022 at 01:01:01	user_xyz	AMS-FW-2187	PA-5220	10.1.2	TSF_2187	15 Aug 2022 at 01:01:01
View Report	View Report	14 Aug 2022 at 01:01:01	user_xyz	TOK-FW-7365	PA-5220	10.1.2	TSF_7365	13 Aug 2022 at 01:01:01
View Report	View Report	14 Aug 2022 at 01:01:01	user_xyz	TOK-FW-7365	PA-5220	10.1.2	TSF_7365	13 Aug 2022 at 01:01:01
View Report	View Report	14 Aug 2022 at 01:01:01	user_xyz	TOK-FW-7365	PA-5220	10.1.2	TSF_7365	13 Aug 2022 at 01:01:01
View Report	View Report	13 Aug 2022 at 01:01:01	user_xyz	TOK-FW-7365	PA-5220	10.1.2	TSF_7365	13 Aug 2022 at 01:01:01
View Report	View Report	13 Aug 2022 at 01:01:01	user_xyz	TOK-FW-7365	PA-5220	10.1.2	TSF_7365	13 Aug 2022 at 01:01:01
View Report	View Report	13 Aug 2022 at 01:01:01	user_xyz	TOK-FW-7365	PA-5220	10.1.2	TSF_7365	13 Aug 2022 at 01:01:01

  In-Progress (4)

Date Uploaded	User Name	TSF Name	Progress
16 Aug 2022 at 01:01:01	user_xyz	TSF_1658	Uploading TSF file - 75% uploaded
16 Aug 2022 at 01:01:01	user_xyz	TSF_1658	Processing TSF file - 75% complete
16 Aug 2022 at 01:01:01	user_xyz	TSF_1658	Processing TSF file - 55% complete
16 Aug 2022 at 01:01:01	user_xyz	TSF_1658	Processing TSF file - 43% complete

  Failed (2)

Date Uploaded	User Name	Hostname	Model	PAN-OS Version	TSF Name	TSF Generated Date	Actions
15 Aug 2022 at 01:01:01	user_xyz	AMS-FW-2187	PA-5220	10.1.2	TSF_2187	15 Aug 2022 at 01:01:01	🗑
14 Aug 2022 at 01:01:01	user_xyz	TOK-FW-7365	PA-5220	10.1.2	TSF_7365	13 Aug 2022 at 01:01:01	🗑

With a premium license, AIOps for NGFW also offers advanced security posture capabilities. Premium features focus on ensuring full utilization and maximal security from your firewalls. Check out what both free and premium licenses have to offer.

On-Demand BPA Report

Where Can I Use This?	What Do I Need?
• NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series, funded with Software NGFW Credits	• AIOps for NGFW Free (use the AIOps for NGFW Free ap or • AIOps for NGFW Premium license (use the Strata Cloud

You can now run the Best Practice Assessment (BPA) and Feature Adoption summary directly from Strata Cloud Manager. Just upload a Tech Support File (TSF). You can generate the on-demand BPA report for devices that are not sending telemetry data or onboarded to AIOps for NGFW.

The BPA evaluates your security posture against Palo Alto Networks best practices and prioritizes improvements for devices. Security best practices prevent known and unknown threats, reduce the attack surface, and provide visibility into traffic, so you can know and control which applications, users, and content are on your network. Additionally, best practices include checks for the Center for Internet Security's Critical Security Controls (CSC). See the best practices guidance to bolster security posture and implement improvements.

Can I Still Generate BPA Reports from the Customer Support Portal?

Before AIOps existed, you went to the Customer Support Portal to access and run the BPA. Today, the preferred way to generate and download the Best Practice Assessment report for NGFW/Panorama Managed Prisma Access is from AIOps.

After July 17, 2023 you'll no longer be able to access and run the BPA from the Customer Support Portal.

STEP 1 | Go to the Hub and activate AIOps for NGFW. It's free. You can activate without Strata Logging Service if you don't want to onboard devices with telemetry enabled at this time.

The best practices dashboard, security alerts, and adoption summary features are not available for devices onboarded without Strata Logging Service or telemetry enabled.

STEP 2 | Log in to your activated instance AIOps for NGFW. You'll see the following tabs, even without Strata Logging Service:

- Posture
- Activity
- Settings

STEP 3 | Go to **Dashboards** > **On Demand BPA**.

STEP 4 | Select **Generate New BPA Report** to upload a valid TSF from a device running PAN-OS version 9.1 or higher.

STEP 5 | Select **View Report** below **Completed** after the TSF is processed to view the generated BPA report from your device.

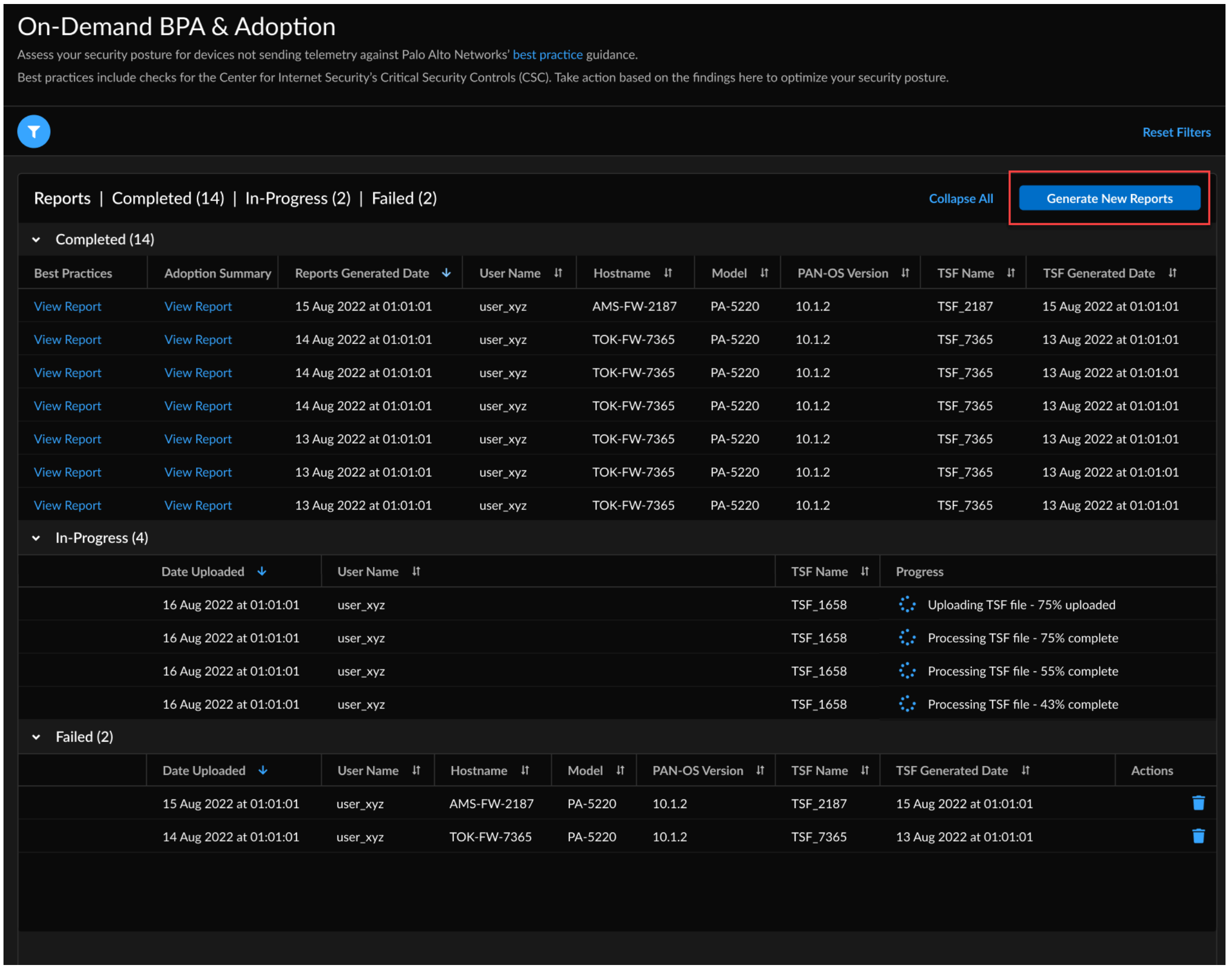
Generate Your BPA & Adoption Summary Report, On Demand

Where Can I Use This?	What Do I Need?
• NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series, funded with Software NGFW Credits	• AIOps for NGFW Free (use the AIOps for NGFW Free ap or • AIOps for NGFW Premium license (use the Strata Cloud

Follow these steps to generate the BPA Report on demand.

STEP 1 | Navigate to **Dashboards** > **On-Demand BPA**.

STEP 2 | **Generate New BPA Report**.



On-Demand BPA & Adoption

Assess your security posture for devices not sending telemetry against Palo Alto Networks' best practice guidance.

Best practices include checks for the Center for Internet Security's Critical Security Controls (CSC). Take action based on the findings here to optimize your security posture.

Completed (14)

Best Practices	Adoption Summary	Reports Generated Date	User Name	Hostname	Model	PAN-OS Version	TSF Name	TSF Generated Date
View Report	View Report	15 Aug 2022 at 01:01:01	user_xyz	AMS-FW-2187	PA-5220	10.1.2	TSF_2187	15 Aug 2022 at 01:01:01
View Report	View Report	14 Aug 2022 at 01:01:01	user_xyz	TOK-FW-7365	PA-5220	10.1.2	TSF_7365	13 Aug 2022 at 01:01:01
View Report	View Report	14 Aug 2022 at 01:01:01	user_xyz	TOK-FW-7365	PA-5220	10.1.2	TSF_7365	13 Aug 2022 at 01:01:01
View Report	View Report	14 Aug 2022 at 01:01:01	user_xyz	TOK-FW-7365	PA-5220	10.1.2	TSF_7365	13 Aug 2022 at 01:01:01
View Report	View Report	13 Aug 2022 at 01:01:01	user_xyz	TOK-FW-7365	PA-5220	10.1.2	TSF_7365	13 Aug 2022 at 01:01:01
View Report	View Report	13 Aug 2022 at 01:01:01	user_xyz	TOK-FW-7365	PA-5220	10.1.2	TSF_7365	13 Aug 2022 at 01:01:01
View Report	View Report	13 Aug 2022 at 01:01:01	user_xyz	TOK-FW-7365	PA-5220	10.1.2	TSF_7365	13 Aug 2022 at 01:01:01

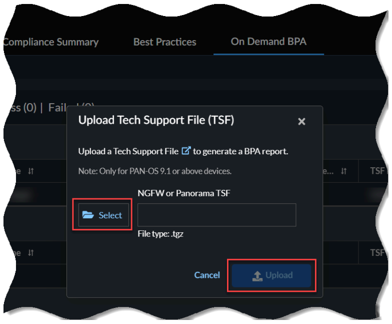
In-Progress (4)

Date Uploaded	User Name	TSF Name	Progress
16 Aug 2022 at 01:01:01	user_xyz	TSF_1658	Uploading TSF file - 75% uploaded
16 Aug 2022 at 01:01:01	user_xyz	TSF_1658	Processing TSF file - 75% complete
16 Aug 2022 at 01:01:01	user_xyz	TSF_1658	Processing TSF file - 55% complete
16 Aug 2022 at 01:01:01	user_xyz	TSF_1658	Processing TSF file - 43% complete

Failed (2)

Date Uploaded	User Name	Hostname	Model	PAN-OS Version	TSF Name	TSF Generated Date	Actions
15 Aug 2022 at 01:01:01	user_xyz	AMS-FW-2187	PA-5220	10.1.2	TSF_2187	15 Aug 2022 at 01:01:01	🗑
14 Aug 2022 at 01:01:01	user_xyz	TOK-FW-7365	PA-5220	10.1.2	TSF_7365	13 Aug 2022 at 01:01:01	🗑

STEP 3 | **Select TSF** and **Upload TSF** file.



Upload Tech Support File (TSF)

Upload a Tech Support File to generate a BPA report.

Note: Only for PAN-OS 9.1 or above devices.

NGFW or Panorama TSF

Select

File type: .tgz

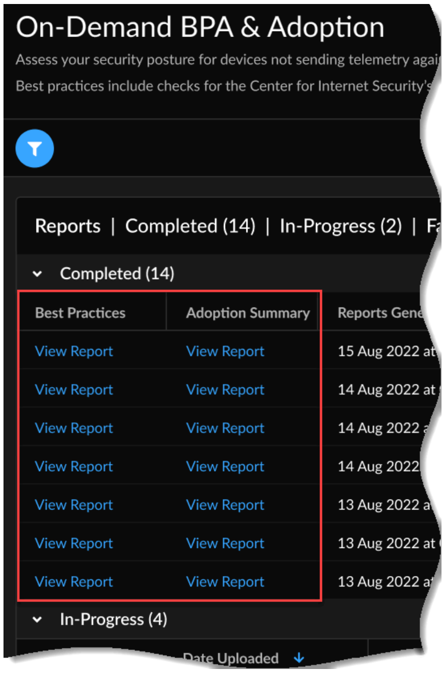
Cancel

Upload

The upload time is dependent on the size of your .tgz file and your Internet speed. Uploading the file could take a few minutes for larger files. Expand **In-Progress** to view the status of the TSF files.

- *On-demand BPA supports only the Tech Support Files (TSF) in the .tgz file format.*
- *On-demand BPA supports TSFs from devices with the PAN-OS version 9.1 or above for report generation.*

STEP 4 | **View Report** below **Completed** to view the results.



On-Demand BPA & Adoption

Assess your security posture for devices not sending telemetry agai

Best practices include checks for the Center for Internet Security's

Reports | Completed (14) | In-Progress (2) | F

Completed (14)

Best Practices	Adoption Summary	Reports Gene
View Report	View Report	15 Aug 2022 at
View Report	View Report	14 Aug 2022 at
View Report	View Report	14 Aug 2022 a
View Report	View Report	14 Aug 2022
View Report	View Report	13 Aug 2022 a
View Report	View Report	13 Aug 2022 at
View Report	View Report	13 Aug 2022 at

In-Progress (4)

Date Uploaded

Best Practices

Where Can I Use This?	What Do I Need?
• NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series, funded with Software NGFW Credits	□ Prisma Access □ AIOps for NGFW Premium license (use the Strata Cloud □ Enable telemetry sharing on devices

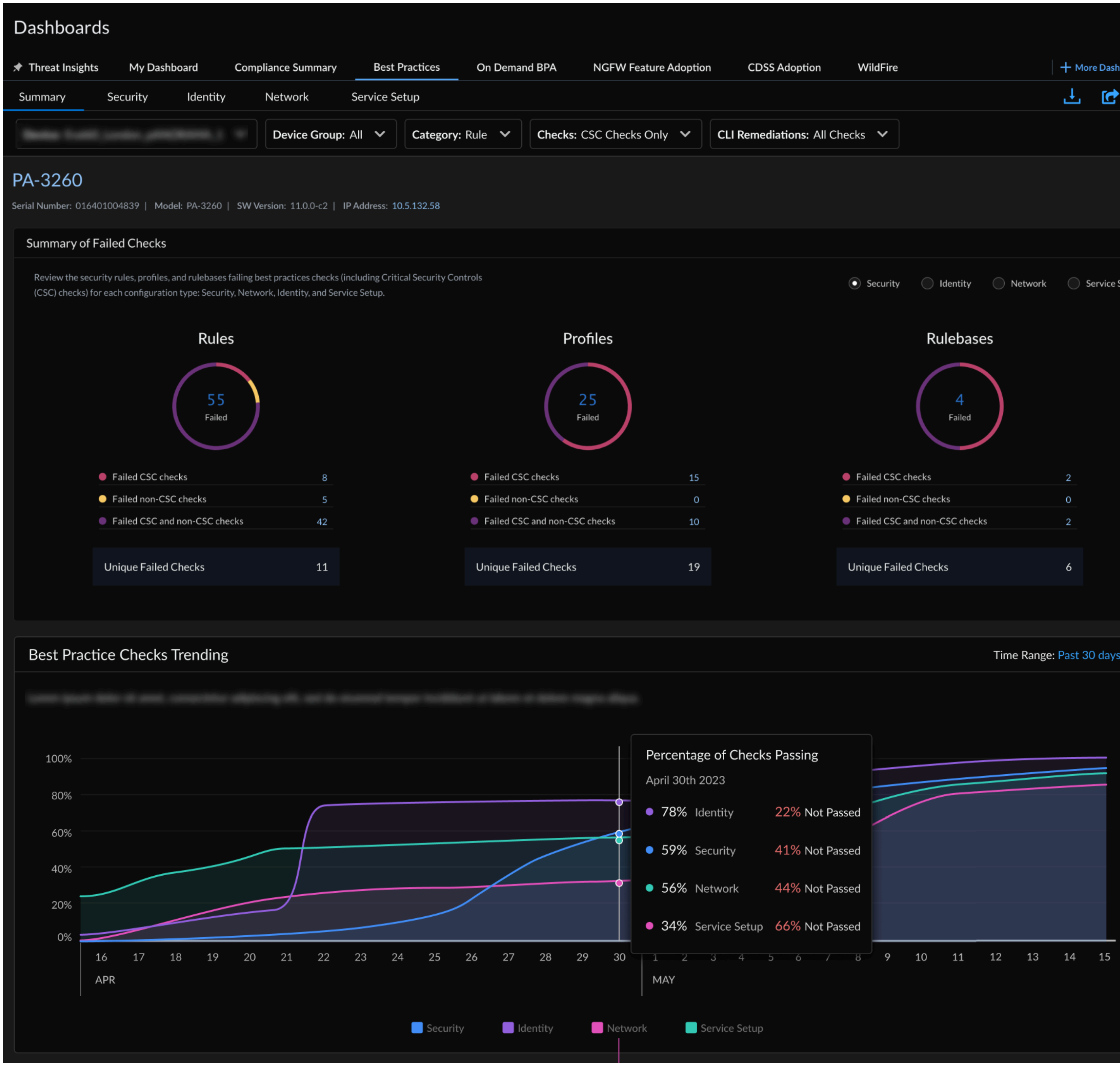
What does this dashboard show you?

The dashboard shows aggregated data per Prisma Access and NGFW/Panorama associated with your tenant.

Navigate to **Strata Cloud Manager** > **Dashboards** > **More Dashboards** > **Best Practices** dashboard to measure your security posture against Palo Alto Networks' best practice guidance. Importantly, the best practices assessment includes checks for the Center for Internet Security's Critical Security Controls (CSC). CSC checks are called out separately from other best practice checks, so you can easily pick out and prioritize updates that will bring you up to CSC compliance.

How can you use the data from the dashboard?

While best practice guidance aims to help you bolster your security posture, findings in this report can also help you to identify areas where you can make changes to more effectively manage your environment.



Dashboards

[redacted]

Device Group: All | Category: Rule | Checks: CSC Checks Only | CLI Remediations: All Checks

PA-3260

Serial Number: 016401004839 | Model: PA-3260 | SW Version: 11.0.0-c2 | IP Address: 10.5.132.58

Summary of Failed Checks

Review the security rules, profiles, and rulebases failing best practices checks (including Critical Security Controls (CSC) checks) for each configuration type: Security, Network, Identity, and Service Setup.

● Security ○ Identity ○ Network ○ Service S

	Rules	Profiles	Rulebases
Failed	55	25	4
Failed CSC checks	8	15	2
Failed non-CSC checks	5	0	0
Failed CSC and non-CSC checks	42	10	2
Unique Failed Checks	11	19	6

Best Practice Checks Trending

Time Range: Past 30 days

[redacted]

Percentage of Checks Passing

April 30th 2023

78% Identity	22% Not Passed
59% Security	41% Not Passed
56% Network	44% Not Passed
34% Service Setup	66% Not Passed

The best practice dashboard is divided into five sections:

- **Summary**

  Gives you a comprehensive view of all the failed checks for a device across the configuration types (Security, Network, Identity, and Service Setup), View historical trend charts for BPA checks and assess your best practice adoption rate for key feature areas.

- **Security**

  Shows the rules, rulebases, or profiles that are failing best practice and CSC checks for the selected device and location. When available, CLI remediations allow you to resolve issue with your policy rules. CLI remediations are generated using TSF data you upload when generating an On-Demand BPA Report.

  - **Rulebases**

    Looks at how your policy is organized, and whether configuration settings that apply across many rules align with best practices (including CSC checks).

  - **Rules**

    Shows you the rules failing best practice and CSC checks. See where you can take quick action to fix failed checks. Rules are sorted based on session count, so you can start by reviewing and updating the rules that are impacting the most traffic.

  - **Profiles**

    Shows you how your profiles stack up against best practices, including CSC checks. Profiles perform advanced inspection for traffic matched to a security or decryption rule.

- **Identity**

  Shows whether the authentication enforcement settings (authentication rule, authentication profile, and authentication portal) for a device meet the best practices and comply with CSC checks.

- **Network**

  Checks whether the application override rules and network settings align with best practice and CSC checks.

- **Service Setup**

  See how the subscriptions you have enabled on your devices are aligning with the best practice and CSC checks. You can review the WildFire setup, GlobalProtect portal and GlobalProtect gateway configurations here and fix the failed checks.

Share, Download, and Schedule Reports for a Dashboard

You can download, share, and schedule reports covering the data the dashboard displays in PDF and .csv formats displays, and CLI remediations in .txt format. Find these icons in the top right of the dashboard: