paloalto TECHDOCS

Strata Cloud Manager AIOps

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

© 2023-2025 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

Last Revised

February 3, 2025

Table of Contents

AIOps for NGFW 5
- AIOps for NGFW 的区域 7
- 免费版和高级版的功能 9
- 如何激活 AIOps for NGFW 12
- 如何访问 My AIOps for NGFW 功能 17
- **Panorama CloudConnector** 插件 23
- 获取警报通知 27
- NGFW 连接和策略执行异常问题排查 29

AIOps for NGFW 的设备遥测 33
- AIOps for NGFW 所需要的域 35

优化安全态势 37
- 监视安全态势见解 38
- 监视功能采用情况 40
- 监控安全订阅 44
- 评估漏洞 46
- 监视合规性摘要 49
- 主动执行安全检查 51
- 策略分析器 55
  - 策略分析器检测到的异常类型 55
  - 变更前策略分析 56
  - 变更前政策分析报告 60
  - 变更后策略分析 62

NGFW 运行状况和软件管理 65
- 查看设备运行状况 66
- 获取升级建议 67
- 分析指标容量 70

NGFW 的最佳实践 81
- 按需 BPA 报告 84
  - 我是否仍可以从客户支持门户生成 BPA 报告？ 84
- 最佳实践 86

©2025 Palo Alto Networks, Inc.

 ©2025 Palo Alto Networks, Inc.

AIOps for NGFW

利用通过 PAN-OS 设备遥测收集的数据，AIOps for NGFW 为您提供新一代防火墙部署的运行状况和安全性概述，以帮助您确定需要改进的领域并弥补安全差距。AIOps for NGFW 从与设备运行状态相关的设备遥测指标中获取运行状况信息。对于安全信息，AIOps for NGFW 会根据 Palo Alto Networks 最佳实践分析您的设备配置，以指出您的安全态势中的任何潜在差距。

AIOps for NGFW 高级版和 ***Strata Cloud Manager***

Strata Cloud Manager 只能为使用 *AIOps for NGFW* 高级版许可证的 *NGFW* 提供统一管理和操作。

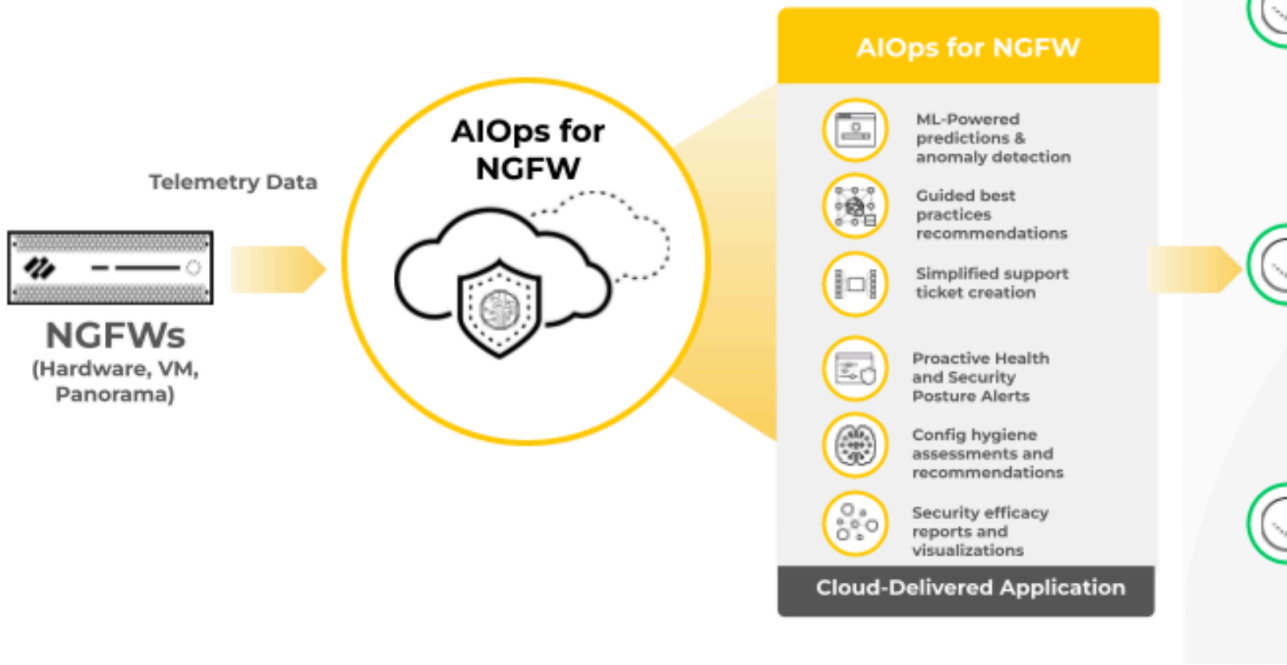
- ***NGFW*** （***PAN-OS*** 和 ***Panorama Managed***）→对于具有 *AIOps for NGFW Premium* 许可证的 *PAN-OS* 和 *Panorama* 托管的 *NGFW*，请使用 *Strata Cloud Manager* 来监督您的部署运行状况和安全态势。
- ***NGFW*** （云管理）→通过 *AIOps for NGFW* 许可证，您还可以使用 *Strata Cloud Manager* 进行 NGFW 的云管理。

从 *2024* 年 *10* 月开始，*Strata Cloud Manager*有两个许可层次：*Strata Cloud Manager Essentials* 和 *Strata Cloud Manager Pro*。这种统一的结构简化了网络安全产品的部署，包括 *AIOps for NGFW*、自主数字体验管理 *(ADEM)*、云管理功能和 *Strata* 日志记录服务。请参阅 Strata Cloud Manager 许可证。

如果您已经在使用 ***AIOps for NGFW*** 免费版 *app* 或是具有 ***AIOps for NGFW*** 高级版许可证的 *Strata Cloud Manager*，则您现有的许可证不受影响，您可以继续修改，扩展或续订许可证。

入门：

- AIOps for NGFW 免费版和高级版
- 激活 AIOps for NGFW
- 开始向 AIOps for NGFW 发送设备遥测
- 新功能
- 按需 BPA 报告
- AIOps for NGFW 事件和警报



 ©2025 Palo Alto Networks, Inc.

AIOps for NGFW 的区域

在何处可以使用？	需要提供什么？
• NGFW，包括由 软件 NGFW 积分提供资助的项目	其中之一： ❑ AIOps for NGFW Free 或 Strata Cloud Manager Essentials ❑ AIOps for NGFW Premium 或 Strata Cloud Manager Pro

您在激活 AIOps for NGFW 时选择的区域将确定 AIOps 处理数据的物理位置。

并非所有支持 Strata Logging Service (SLS) 基础架构的地区都提供 AIOps for NGFW。AIOps for NGFW 部署将很快扩展到其他地区，以匹配遥测数据目的地。目前，如果您将遥测数据发送到不支持 AIOps 应用程序的地区，您的数据将由美国美洲地区的 AIOps for NGFW 实例处理。

在您激活 AIOps for NGFW 后，将自动应用这些限制。例如，如果您选择德国作为激活 AIOps for NGFW 实例的区域，则只有德国的 SLS 租户才能连接到该实例。

支持 *AIOps for NGFW* 的相同区域也支持 *Strata Cloud Manager* 中的 *NGFW*。

请参阅下表以了解各种遥测目标区域的 AIOps 数据处理。

Strata Logging Service 区域	AIOps for NGFW 实例支持处理数据的区域
德国	德国
英国	英国
荷兰 - 欧洲	荷兰 - 欧洲
意大利 - 欧洲	意大利 - 欧洲
西班牙 - 欧洲	西班牙 - 欧洲
瑞士 - 欧洲	瑞士 - 欧洲
法国 - 欧洲	法国 - 欧洲
波兰 - 欧洲	波兰 - 欧洲
韩国	韩国

 ©2025 Palo Alto Networks, Inc.

Strata Logging Service 区域	AIOps for NGFW 实例支持处理数据的区域
印度尼西亚	印度尼西亚
以色列	以色列
中国台湾	中国台湾
卡塔尔	卡塔尔
新加坡	新加坡
澳大利亚	澳大利亚
印度	印度
日本	日本
加拿大	加拿大
其余 SLS 区域	美国-美洲 (US)

 ©2025 Palo Alto Networks, Inc.

免费版和高级版的功能

在何处可以使用？	需要提供什么？
• NGFW，包括由 软件 NGFW 积分提供资助的项目	其中之一： ❑ AIOps for NGFW Free 或 Strata Cloud Manager Essentials ❑ AIOps for NGFW Premium 或 Strata Cloud Manager Pro

AIOps for NGFW 附带两个许可证级别：免费版和高级版。

AIOps for NGFW 免费版功能加强了您对防火墙部署的理解。

免费版功能：

- 评估防火墙的配置并确定需要改进之处
- 轻松访问来自防火墙的运行时和历史遥测数据
- 检测系统问题（与检测方法无关）
- 通过警报/通知工作流缩短解决问题的时间
- 为多个安全订阅提供动态指示板和可视化

使用高级许可证，您可以访问免费功能和高级功能。高级版功能侧重于确保充分利用防火墙给出的结果并最大限度提高安全性。

高级版功能：

- 云管理 NGFW

  联系您的客户团队，使用 *Strata Cloud Manager* 来启用 NGFW 的云管理。

- 使用先进的机器学习技术来提升始终最佳的安全态势，响应不断变化的威胁和网络环境，从而减少攻击面
- 为 WildFire 和 IOC 搜索提供动态指示板和可视化
- 在 Strata Cloud Manager 命令中心中与数据交互并可视化网络中事件之间的关系，以找出异常或找到增强网络安全的方法

Strata Cloud Manager 有两个许可层次：*Strata Cloud Manager Essentials* 和 *Strata Cloud Manager Pro*。这种统一的结构简化了网络安全产品的部署，包括 *AIOps for NGFW*、自主数字体验管理 *(ADEM)*、云管理功能和 *Strata* 日志记录服务。请参阅 Strata Cloud Manager 许可证。

如果您已经在使用 ***AIOps for NGFW*** 免费版 *app* 或是具有 ***AIOps for NGFW*** 高级版许可证的 *Strata Cloud Manager*，则您现有的许可证不受影响，您可以继续修改，扩展或续订许可证。

 ©2025 Palo Alto Networks, Inc.

功能集	免费版	高级版（使用 **Strata Cloud Manager**）
加强安全态势	部分	是
• 安全态势见解	是	是
• 功能采用	是	是
• 安全态势设置	否	是
• 软件升级建议	否	是
• CDSS 采用	是	是
• 策略分析器	否	是
• 按需 BPA 报告	是	是
• Panorama CloudConnector 插件	否	是
• 容量分析器	否	是
• NGFW SDWAN 指示板	否	是
• 合规性摘要指示板	否	是
主动解决防火墙中断	部分	是
• 警报和事件	部分	是
• PAN-OS CVE 指示板	是	是
• 警报的可能原因分析	否	是
使用日志进行故障排除	是	是
• 在日志查看器中查看、查询和导出日志 检查许可证以及有关使用日志查看器的其他要求。	是	是
• 导出元数据以进行故障排除	是	是
• 查看审核日志	是	是
优化您的安全投资	部分	是

 ©2025 Palo Alto Networks, Inc.

功能集	免费版	高级版（使用 **Strata Cloud Manager**）
• 基于运行状况和安全态势的设备排名	是	是
• 除威胁见解指示板外的所有指示板和报告	是	是
• 威胁见解指示板和报告	否	是
• 搜索安全工件	否	是
• 构建自定义指示板	否	是
• Strata Cloud Manager 命令中心	否	是
通知	部分	是
• 电子邮件通知	是	是
• ServiceNow 集成	否	是
参与和支持	否	是
• 针对操作问题的产品内支持票证创建功能需要 防火墙的白金级支持（电源故障警报除外）	否	是

产品中所有功能类别的新功能是分配给免费版层级还是高级版层级将完全由 *Palo Alto Networks* 自行决定。

 ©2025 Palo Alto Networks, Inc.

如何激活 AIOps for NGFW

在何处可以使用？	需要提供什么？
• NGFW，包括由 软件 NGFW 积分提供资助的项目	其中之一： ❑ AIOps for NGFW Free 或 Strata Cloud Manager Essentials ❑ AIOps for NGFW Premium 或 Strata Cloud Manager Pro

以下是激活 AIOps for NGFW 的不同场景：

场景	计划
激活 AIOps for NGFW 免费版	激活 AIOps for NGFW（免费）
激活 AIOps for NGFW 高级版（使用 Strata Cloud Manager app）	通过公共服务激活 AIOps for NGFW
将新设备加载到已激活的 AIOps for NGFW 免费版实例	将设备关联到租户 在设备上启用遥测
将新设备载入到已激活的 AIOps for NGFW 高级版（使用 Strata Cloud Manager 应用程序）	将设备关联到租户 将租户中的设备关联到应用程序 在设备上启用遥测
激活 ELA AIOps for NGFW 高级版	激活企业许可协议 (ELA) AIOps for NGFW 高级版
使用 Strata Cloud Manager（AIOps for NGFW 高级版）管理 VM-Series	激活 Software NGFW Credits 许可证协议
将 Strata Cloud Manager（AIOps for NGFW 高级版）用于 Panorama 托管 VM-Series	为 Panorama 托管 VM-Series 激活 Software NGFW Credits 许可证
将 AIOps for NGFW 高级版试用许可证转换为生产许可证	将试用许可证转换为生产许可证
激活 Strata Cloud Manager Essentials 和 Strata Cloud Manager Pro	• 激活 Strata Cloud Manager Essentials • 激活 Strata Cloud Manager Pro

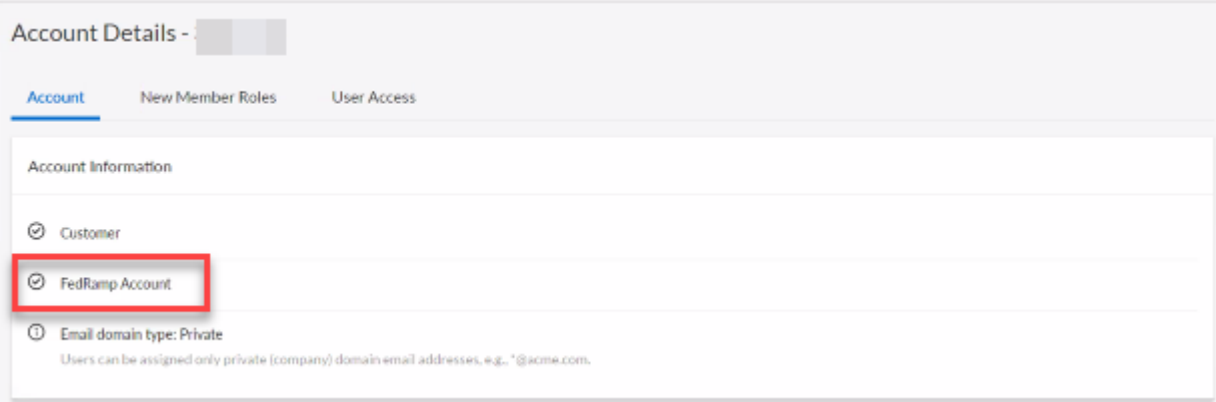
 ©2025 Palo Alto Networks, Inc.

场景	计划
提供了 *Strata Cloud Manager Essentials* 和 *Strata Cloud Manager Pro*，以在不具备以下条件的客户支持门户 *(CSP)* 帐户中激活：具有指定存储的 *Strata* 日志记录服务、*AIOps for NGFW* 免费版/高级版或 *Prisma Access*。	

Strata Cloud Manager 只能为使用 AIOps for NGFW 高级版许可证的 NGFW 提供统一管理和操作。对于已经在 AIOps for NGFW 免费版中载入的 NGFW，继续使用 AIOps for NGFW 免费应用程序。

Strata Cloud Manager 提供两个许可层级：Strata Cloud Manager Essentials 和 Strata Cloud Manager Pro。这种统一的结构简化了网络安全产品的部署，包括 AIOps for NGFW、自主数字体验管理 (ADEM)、云管理功能和 Strata 日志记录服务。如果在引入这些新的许可层级之前就已经在使用 Strata Cloud Manager，则现有的 AIOps for NGFW 高级版和 AIOps for NGFW 免费版许可证仍然受支持。可以继续修改、延长或续订这些许可证。

FedRAMP 帐户无法使用 *AIOps for NGFW*。要检查这是否适用于您，请登录您的客户支持门户帐户，然后选择 ***Account Management***（帐户管理）> ***Account Details***（帐户详细信息）。如果看到列出了 ***FedRamp Account***（***FedRamp*** 帐户），则您无法使用 *AIOps for NGFW*。



激活 **AIOps for NGFW**（免费）

需要用帐户管理员或应用程序管理员角色来进行激活。

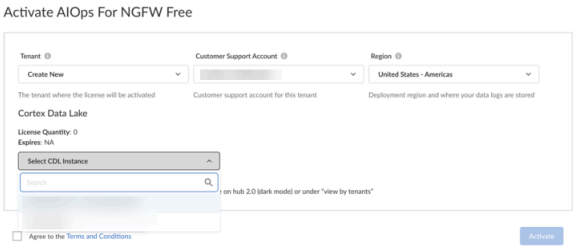
1. 使用以租户为中心的视图登录到中心。

   如果您使用的是“支持帐户”视图，请关闭 **View by Support Account**（按支持帐户查看）。

   如果您没有现有的租户，请使用支持帐户视图登录到中心。

 ©2025 Palo Alto Networks, Inc.

2. 找到 AIOps for NGFW 免费版，然后选择 **Activate**（激活）。
3. 填写表格。

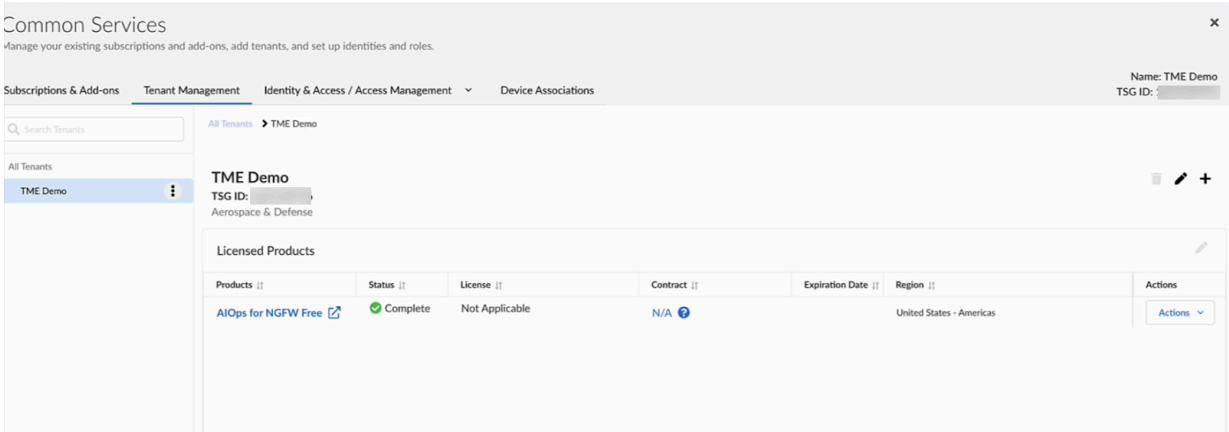


租户	选择要在其中激活 AIOps for NGFW 免费版实例的租户。如果您还没有租户，请选择 **Create New**（新建）。
客户支持帐户	您的客户支持门户帐户 ID。
区域	部署区域以及存储数据日志的区域。请参阅 AIOps for NGFW 的区域。
Strata 日志记录服务	您要将数据发送到 AIOps for NGFW 免费版的 Strata Logging Service。如果您有日志记录 SLS，可以将其与 AIOps for NGFW 免费版进行关联。否则可以跳过。

4. 依次单击 **Agree to the Terms and Conditions**（同意条款和条件）和 **Activate**（激活）。

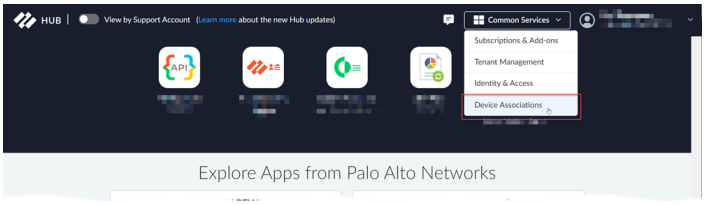
 ©2025 Palo Alto Networks, Inc.

5. **Status**（状态）显示 **Complete**（完成）后，AIOps for NGFW 免费版即已准备就绪。



 ©2025 Palo Alto Networks, Inc.

6. 将设备关联到包含您的 AIOps for NGFW 免费版实例的租户。
   1. 登录到中心。
   2. 选择 **Common Services**（公共服务） > **Device Associations**（设备关联）。



   3. 选择 **Add Device**（添加设备）。
   4. 选择一个或多个防火墙或 Panorama 设备，然后单击 **Save**（保存）。

   如果您正在载入 Panorama 托管的部署，则需要将 Panorama 关联到包含 AIOps for NGFW 免费版的租户。确保将 Panorama 管理的所有防火墙单独关联到租户。

   您与租户关联的设备将自动添加到 AIOps for NGFW 免费版。有关详细信息，请参阅将设备关联到租户。

   - 如果是激活 *AIOps for NGFW* 免费版，则不需要将应用与设备关联。
   - 如果您已经有一个租户，则可以在激活开始时将设备与租户关联。
   - 如果要停用或退回防火墙或 *Panorama* 设备，或者要将其与另一个租户服务组 *(TSG)* 关联，则可以移除设备关联。

7. 在设备上启用遥测。
   1. 确认设备已在客户支持门户中注册，方法如下：登录 support.paloaltonetworks.com， 切换到您的帐户（如有必要）， 并在**Assets**（资产） > **Devices**（设备）中识别您的设备。
   2. 在要载入的设备上安装设备证书。
   3. 在设备上启用遥测共享。

   在您载入设备并启用遥测之后，大约需要几个小时才能在 *AIOps for NGFW* 指示板上看到第一组见解。在设备侧生成和发送遥测的过程是分批完成的，按照某一频率对每个指标进行采样和收集（频率按照指标的用例进行了优化）。此批处理过程可能会导致在载入防火墙与获得见解之间存在延迟。可能要在几个小时之后才能在 *AIOps for NGFW* 指示板上显示与新载入设备相关联的所有见解。

8. 在中心内单击 AIOps for NGFW 免费版的图标以登录。

 ©2025 Palo Alto Networks, Inc.

如何访问 My AIOps for NGFW 功能

本内容适用于具有 *AIOps for NGFW* 和 *Strata Cloud Manager* 的新一代防火墙的云管理。要开始使用 *PAN-OS* 管理新一代防火墙，请单击此处。

在何处可以使用？	需要提供什么？
• NGFW，包括由 软件 NGFW 积分提供资助的项目	其中之一： ☐ AIOps for NGFW Free 或 Strata Cloud Manager Essentials ☐ AIOps for NGFW Premium 或 Strata Cloud Manager Pro

Palo Alto Networks Strata Cloud Manager 是一个全新的 AI 驱动的统一网络安全管理平台。现在，您可以使用 Strata Cloud Manager 来管理 AIOps for NGFW 以及您的其他 Palo Alto Networks 产品和订阅并与之交互。

要启动 **Strata Cloud Manager**，请执行以下操作：

- 前往中心并启动 Strata Cloud Manager 应用程序
- 直接访问 Strata Cloud Manager URL

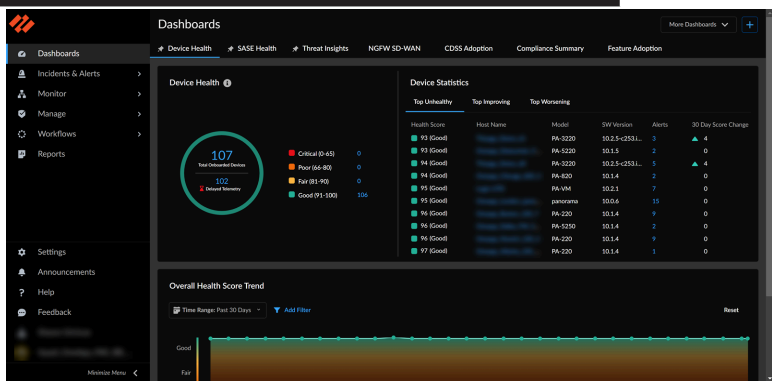
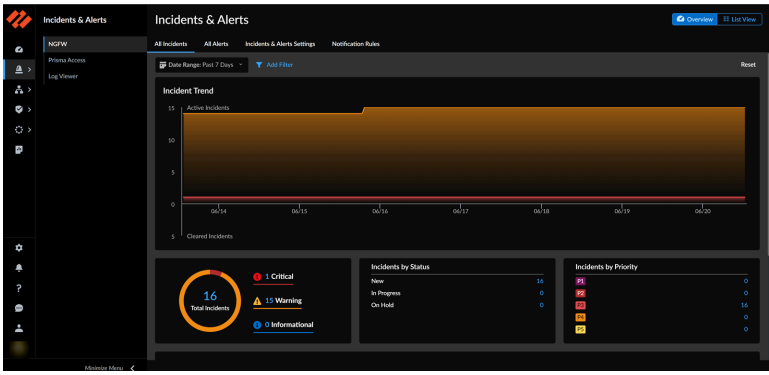
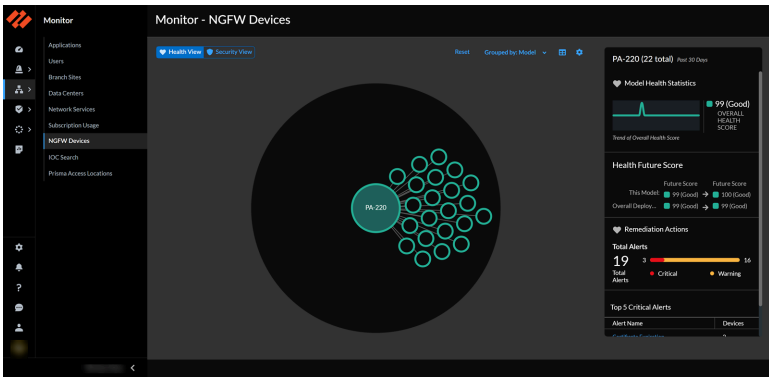
- Strata Cloud Manager 只能为使用 *AIOps for NGFW* 高级版许可证的 *NGFW* 提供统一管理和操作。*AIOps for NGFW*（仅限高级版应用程序）中心上的应用程序磁贴名称现已更改为 *Strata Cloud Manager*。进行此更新后，应用程序 *URL* 也更改为 stratacloudmanager.paloaltonetworks.com，并且您现在还会在左侧导航窗格上看到 *Strata Cloud Manager* 徽标。对于已经在 *AIOps for NGFW* 免费版中载入的 *NGFW*，继续使用 *AIOps for NGFW* 免费应用程序。
- 联系您的客户团队，使用 *Strata Cloud Manager* 来启用 NGFW 的云管理。

如果您之前使用过 AIOps for NGFW 应用程序，您可以在下面所示的路径中找到 Strata Cloud Manager 中的功能：

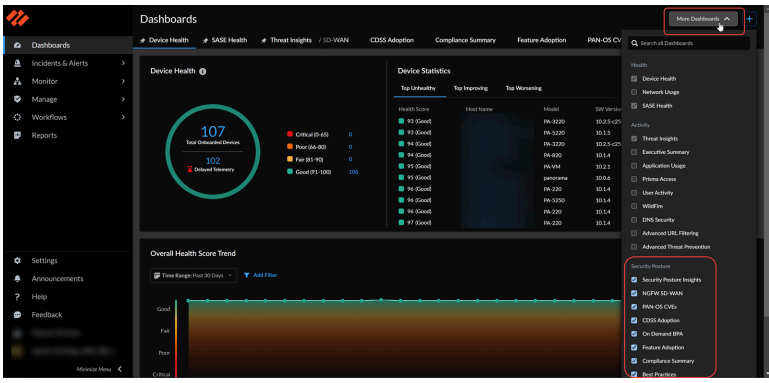
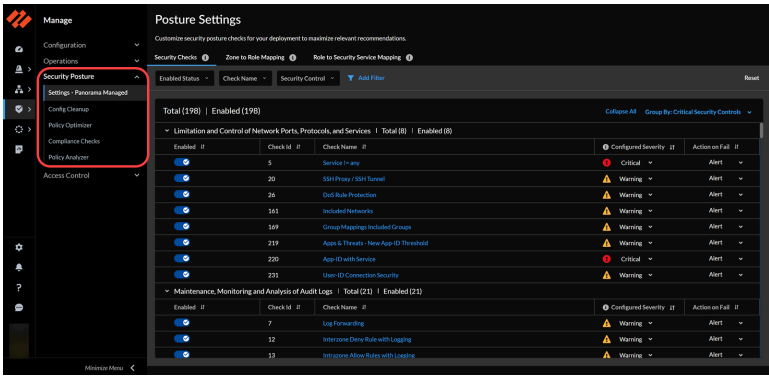
表 **1:**

AIOps for NGFW 应用程序	在哪里可以找到 **Strata Cloud Manager** 中的相同功能：
仪表板	→ Go to（转到）→Dashboards（指示板）→Device Health（设备运行状况）

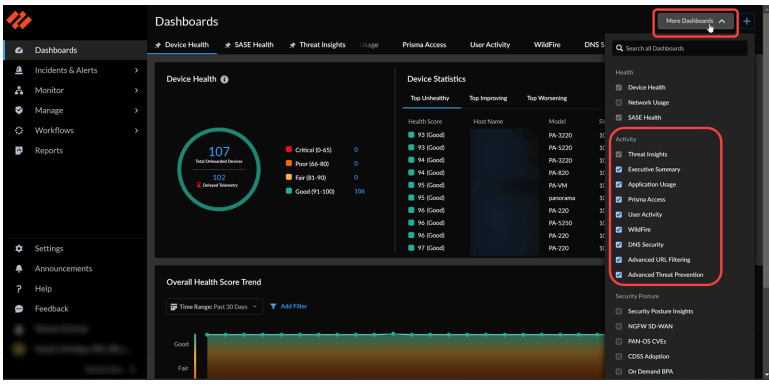
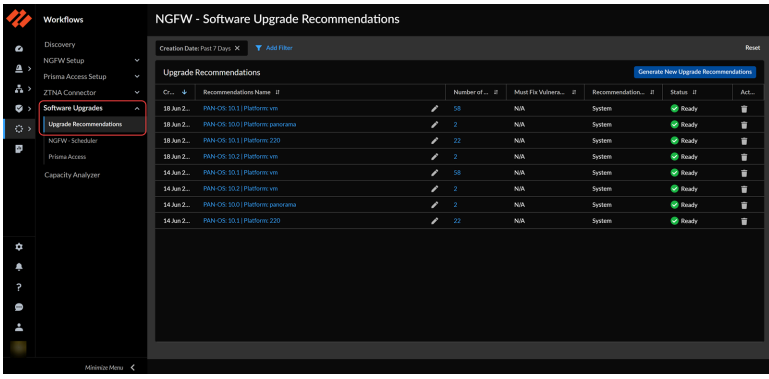
 ©2025 Palo Alto Networks, Inc.

AIOps for NGFW 应用程序	在哪里可以找到 Strata Cloud Manager 中的相同功能：
	
警报	→ Go to（转到）→ Incidents & Alerts（事件和警报）→ NGFW 
监视	→ Go to（转到）→Monitor（监视）→Devices（设备）→NGFW 
态势	→ 进入指示板查看： • 最佳实践指示板 • 安全态势见解指示板 • NGFW SD-WAN 指示板 • 安全公告指示板 (PAN-OS CVE)

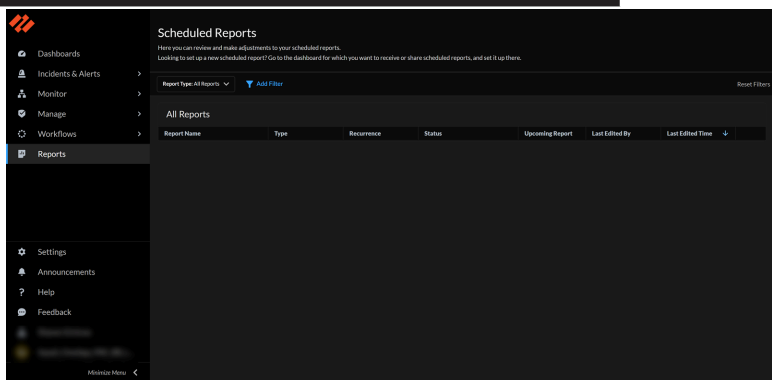
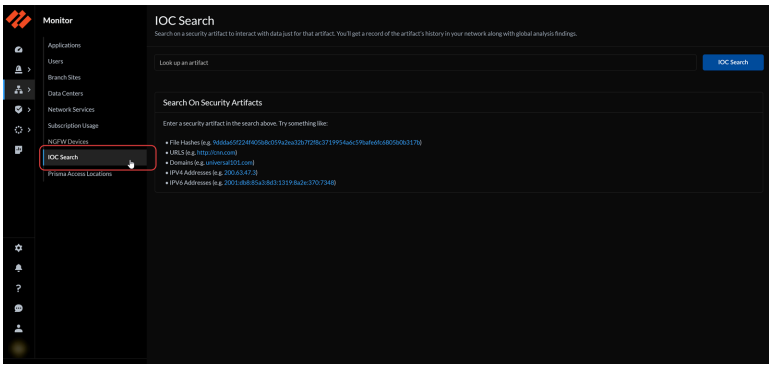
 ©2025 Palo Alto Networks, Inc.

AIOps for NGFW 应用程序	在哪里可以找到 Strata Cloud Manager 中的相同功能：
	• CDSS 采用指示板 • 按需 BPA 指示板 • 功能采用指示板 • 合规性摘要指示板  → Go to（转到）→Manage（管理）→Security Posture to find（要查找的安全态势）： • Settings（设置）- Panorama Managed（Panorama 托管） • 配置清理 • 策略优化器 • 合规性检查 • 策略分析器 
活动	→ 进入指示板查看： • 网络使用情况 • 威胁见解 • 应用程序使用情况

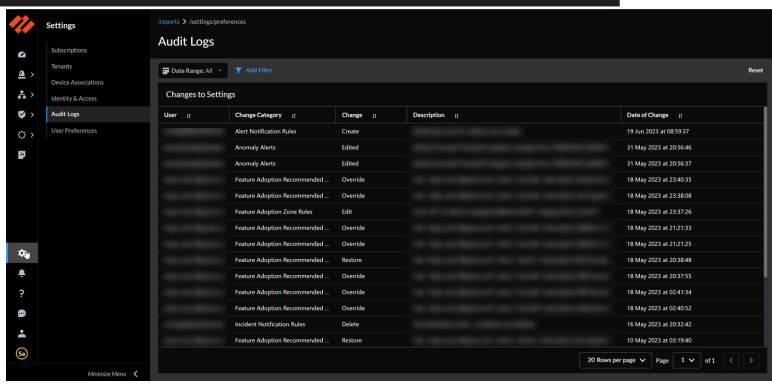
 ©2025 Palo Alto Networks, Inc.

AIOps for NGFW 应用程序	在哪里可以找到 Strata Cloud Manager 中的相同功能：
	• Advanced WildFire • DNS 安全 • 执行摘要 • 用户活动  → 转到 **Reports**（报告）以生成支持的指示板的报告。 → 对于日志查看器，转到 **Incidents & Alerts**（事件和警报）。
工作流程	→ 转到 **Workflows**（工作流程） > **Software Upgrades**（软件升级）以使用 **Upgrade Recommendations**（升级建议）。 
报告	→ 转到 **Reports**（报告）以为支持的指示板安排报告。

 ©2025 Palo Alto Networks, Inc.

AIOps for NGFW 应用程序	在哪里可以找到 Strata Cloud Manager 中的相同功能：
	
搜索	→ 对于 **IoC 搜索**，转到 **Monitor**（监视）。 
设置	→ 转到 **Incidents & Alerts**（事件和警报） > **NGFW** > **Incidents & Alerts Settings**（事件和警报设置）以查看 **Forecast and Anomaly Incidents & Alerts**（预测和异常事件和警报）。 → 转到 **Incidents & Alerts**（事件和警报） > **NGFW** 以设置 **Notification Rules**（通知规则）。 → 转到 **Settings**（设置）以查看： • 审核日志 • 用户首选项

 ©2025 Palo Alto Networks, Inc.

AIOps for NGFW 应用程序	在哪里可以找到 Strata Cloud Manager 中的相同功能：
	 → 转到 **Manage**（管理） > **Security Posture**（安全态势）以自定义 **Settings - Panorama Managed**（设置 - **Panorama** 托管）。 → 转到 **Help**（帮助）→**Export Tenant Metadata**（导出租户元数据）。
–	想要了解如何使用 **Strata Cloud Manager** 来管理 **NGFW?** 仅支持 Strata Cloud Manager 和 AIOps for NGFW Premium，并且不适用于 AIOps for NGFW 应用程序。 → 转到 **Manage**（管理） > **Configuration**（配置） > **NGFWs and Prisma Access**（**NGFW** 和 **Prisma Access**），然后单击 **Workflows**（工作流程） > **NGFW Setup**（**NGFW** 设置）。

 ©2025 Palo Alto Networks, Inc.

Panorama CloudConnector 插件

在何处可以使用？	需要提供什么？
• NGFW，包括由 软件 NGFW 积分提供资助的项目	☐ AIOps for NGFW Premium 或 Strata Cloud Manager Pro

想要主动检查您的策略规则是否符合最佳实践？等待收到警报，然后在推送策略规则后才能解决问题 —— 您完全不必这样做。将 AIOps for NGFW 或 Strata Cloud Manager 连接到您的 Panorama，可先根据某些最佳实践检查来评估您的配置，然后再将其推送到托管防火墙。请参阅主动实施安全检查。

对安全策略规则的更新通常在时间上很敏感，需要您迅速采取行动。但是，您希望确保对安全策略规则库所做的任何更新都符合您的要求，并且不会引入错误或错误配置（例如，导致规则重复或冲突的更改）。

为了实现这一点，Strata Cloud Manager 中的策略分析器使您能够在实施变更请求时优化时间和资源。策略分析器不仅能够分析，就特定规则的可能合并或移除给出建议以满足您的意图，而且还会检查规则库中的异常清空，如遮蔽、冗余、泛化、关联和合并。

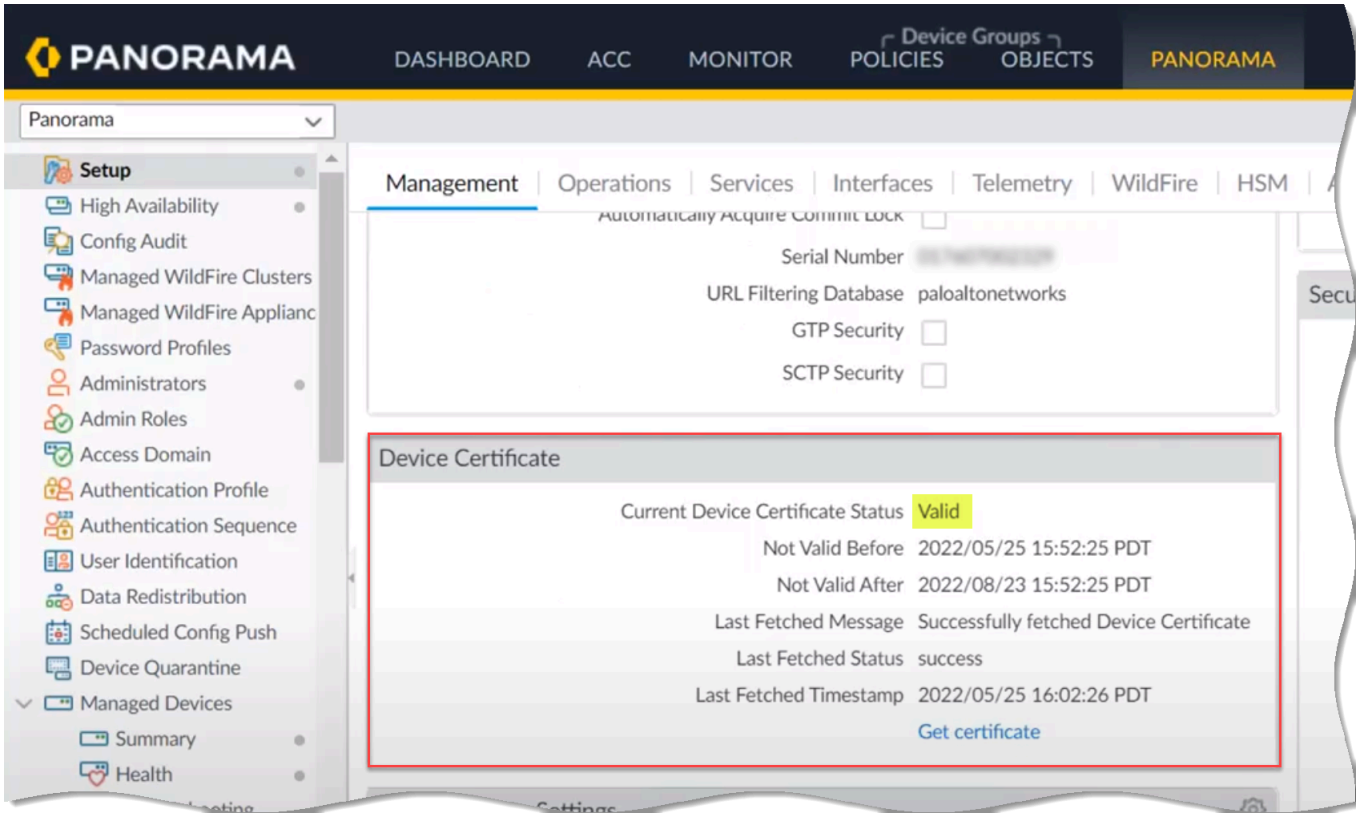
将 AIOps for NGFW 或 Strata Cloud Manager 连接到您的 Panorama，并使用策略分析器添加或优化您的安全策略规则库。请参阅策略分析器。

要将 AIOps for NGFW 连接到您的 Panorama，您需要以下软件：

AIOps for NGFW 或 Strata Cloud Manager 实例：您不需要 AIOps for NGFW 高级版许可证即可安装 Panorama CloudConnector 插件。但要使用策略分析器和主动最佳实践评估 (BPA) 等高级功能，则需要高级版许可证。

 ©2025 Palo Alto Networks, Inc.

安装了设备证书的 Panorama。

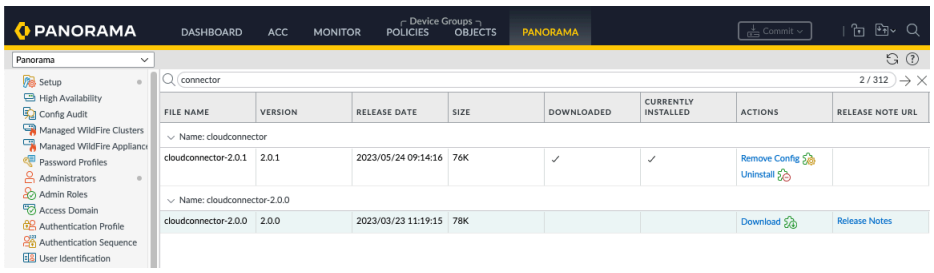


 ©2025 Palo Alto Networks, Inc.

在运行 PAN OS 10.2.3 和更高版本的 Panorama 上安装的 Panorama CloudConnector 插件。

您需要使用以下命令启用此插件：

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



- 为了方便客户，我们在更高的 *Panorama* 版本（*11.0.1* 及更高版本）中预装了此插件。
- 如果您已经安装了 *AIOps* 插件和 *CloudConnector* 插件，请卸载 *AIOps* 插件，因为它们是相同的，只是名称变了。确保您只安装了一个插件，也就是 *CloudConnector* 插件的最新版本。

如果您最初在 PAN-OS 10.2.3 上安装了 AIOps 插件，之后升级到 Pan-OS 11.0.1 或更高版本，则该插件的默认版本将与新的 PAN-OS 版本一起安装。这会导致这两个插件都出现在 Panorama 上。在这种情况下，请执行以下步骤：

1. 在 Panorama Web 界面中，选择 **Panorama > Plugins**（插件），然后选择 **Uninstall**（卸载）以卸载 AIOps 插件。
2. 启用 CloudConnector 插件：

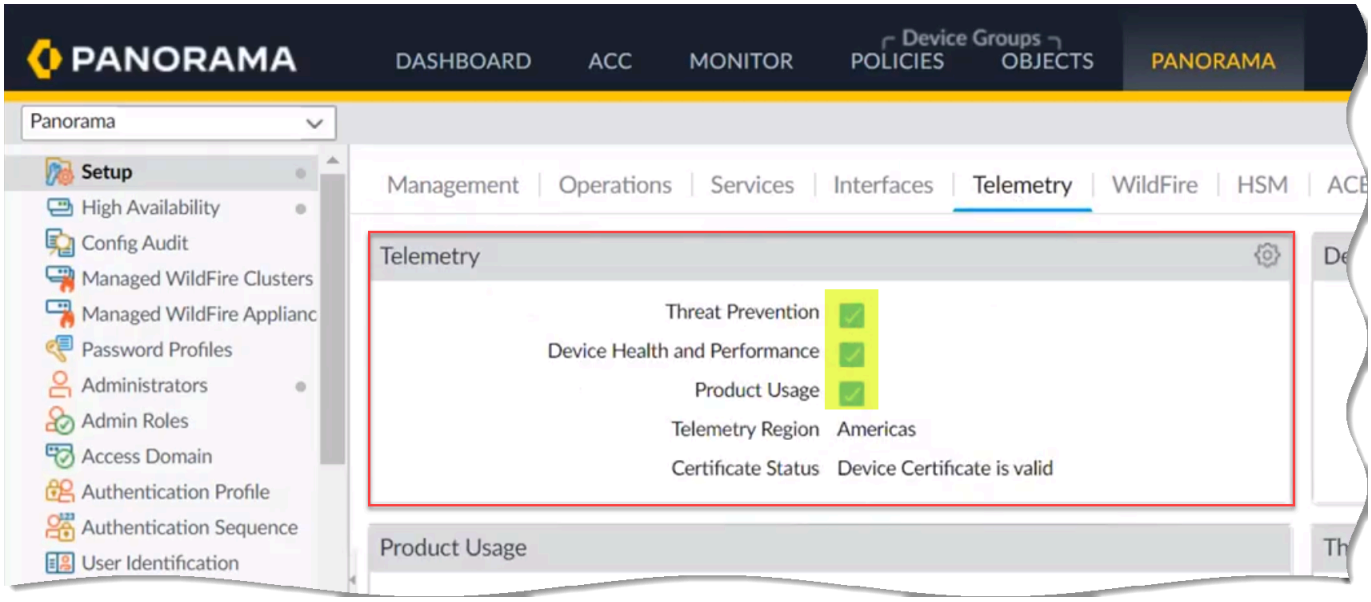
   ```
   > request plugins cloudconnector enable basic
   ```

CloudConnector 插件 2.2.0 支持从 Panorama 进行代理配置设置。这些设置仅在提交后生效。场景如下：

- 配置代理设置：当您配置代理设置并执行提交时，CloudConnector 插件在此提交期间不会识别新的代理设置。提交后，插件将使用代理配置进行将来与云的交互。
- 移除代理设置：当您移除代理设置并执行提交时，CloudConnector 插件不会在提交期间识别已移除的代理设置。提交后，插件将不再使用代理配置进行将来与云的交互。

 ©2025 Palo Alto Networks, Inc.

Panorama 上启用的设备遥测。



一条安全策略规则，该规则允许在 Panorama 和与 Strata Logging Service 主机区域对应的 FQDN 之间进行通信：

美洲 (americas)	https://prod.us.secure-policy.cloudmgmt.paloaltonetworks.com/
澳大利亚 (au)	https://prod.au.secure-policy.cloudmgmt.paloaltonetworks.com/
加拿大 (ca)	https://prod.ca.secure-policy.cloudmgmt.paloaltonetworks.com/
欧洲 (europe)	https://prod.eu.secure-policy.cloudmgmt.paloaltonetworks.com/
FedRAMP (gov)	https://prod.gov.secure-policy.cloudmgmt.paloaltonetworks.com/
德国 (de)	https://prod.de.secure-policy.cloudmgmt.paloaltonetworks.com/
印度 (in)	https://prod.in.secure-policy.cloudmgmt.paloaltonetworks.com/
日本 (jp)	https://prod.jp.secure-policy.cloudmgmt.paloaltonetworks.com/
新加坡 (sg)	https://prod.sg.secure-policy.cloudmgmt.paloaltonetworks.com/
英国 (uk)	https://prod.uk.secure-policy.cloudmgmt.paloaltonetworks.com/

 ©2025 Palo Alto Networks, Inc.

获取警报通知

在何处可以使用？	需要提供什么？
• NGFW，包括由 软件 NGFW 积分提供资助的项目	其中之一： ❑ AIOps for NGFW Free 或 Strata Cloud Manager Essentials ❑ AIOps for NGFW Premium 或 Strata Cloud Manager Pro

将 Strata Cloud Manager 集成到现有运营中时需要设置主动警报，以便您在潜在问题升级为严重问题之前就能检测并管理它们。可以根据您的运营团队的案例管理协议（例如常用的 P1 或 P2）来定制这些警报。

例如，您可以设置一个警报系统，在该系统中代表最严重问题的严重警报会立即上报至您的安全团队，以便立即引起注意。另一方面，可以安排对紧急程度较低但仍然重要的警告警报进行每日审查。这样的安排既能确保有效的事件管理，同时又能保证运营工作的顺利进行。

另一种选择是根据团队来路由警报；某些类别的警报，甚至是特定警报，都可以路由至最有能力处理它们的不同团队。您可以定义通知首选项，例如哪些警报会触发通知、如何接收通知以及接收通知的频率，从而创建通知规则。

以下视频演示了如何创建通知规则。

STEP 1 | 选择 **Incidents & Alerts**（事件和警报） > **Incident & Alert Settings**（事件和警报设置） > **Notification Rules**（通知规则） > **+ Add Notification Rule**（添加通知规则）

STEP 2 | 输入 `Name`（名称）和 `Description`（说明）。

STEP 3 | 选择 **Add New Condition**（添加新条件）以指定将触发通知的规则条件。

例如，要创建硬件警报通知，请选择 **subCategory**（子类别）、**Equals**（等于）和 **Hardware**（硬件）。

 ©2025 Palo Alto Networks, Inc.

STEP 4 | 选择该通知的通知类型和接收者。

1. 如果选择 **Email**（电子邮件），请选择电子邮件组，即将会收到电子邮件通知的一组用户，或 **Create a New Email Group**（创建新的电子邮件组）。

   1. 如果创建新的电子邮件组，请输入电子邮件组名称，然后开始键入要添加到该组的人员的电子邮件地址。填写所有电子邮件地址后，按回车键。
   2. 选择 **Next**（下一步）。
   3. 选择发送这些通知的频率：

   - 立即
   - 分组并每隔 4 小时发送一次
   - 分组并每天发送一次

2. 如果选择 **ServiceNow**，请输入 `ServiceNow URL`、客户端凭据、ServiceNow 凭据和 `ServiceNow API` 版本。

   1. **Test**（测试）您的连接，以确保集成正常工作。
   2. 选择 **Next**（下一步）。

STEP 5 | **Save Rule**（保存规则）。

 ©2025 Palo Alto Networks, Inc.

NGFW 连接和策略执行异常问题排查

在何处可以使用？	需要提供什么？
• NGFW，包括由 软件 NGFW 积分提供资助的项目	❑ AIOps for NGFW Premium 或 Strata Cloud Manager Pro ❑ 需要有 Strata 日志记录服务许可证才能进行日志记录 ❑ 如果您拥有 Prisma Access 许可证，则可以使用文件夹管理来查看预定义文件夹，还可以为文件夹启用 Web 安全

通过 Strata Cloud Manager 进行 NGFW 故障排查，而无需在各种防火墙接口之间移动。如果在部署和配置 NGFW 后遇到连接问题，可以获取路由和隧道状态的汇总视图，并深入了解具体情况以找出异常情况和有问题的配置。

对基于身份的策略规则和动态定义的端点进行问题排查。可以检查特定 NGFW 的状态，并揭示您期望的策略工作方式与其实际执行行为之间可能不一致。

通过问题排查，您可以深入了解这些网络和身份功能中可能出现的问题，追踪并解决连接问题或策略实施异常：

网络问题排查

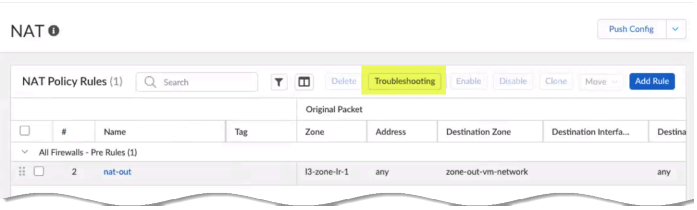
- NAT
- DNS 代理

身份和策略问题排查

- 用户组
- 动态地址组
- 动态用户组
- 用户 ID

防火墙问题排查

- 会话浏览器



转到 **Manage**（管理） > **Configuration**（配置） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Operations**（操作） > > **Troubleshooting**（问题排查） > **Session Browser**（会话浏览器）以开始对浏览器进行问题排查。

 ©2025 Palo Alto Networks, Inc.

或者，您可以转到要排除故障的功能，然后选择 **Troubleshooting**（问题排查）按钮开始。

按状态、操作、搜索目标和时间戳查看和排序您运行的问题排查作业。

功能	功能位置	可用操作	操作范围	作业输出组织方式：
会话浏览器（防火墙）	管理 > 配置 > **NGFW** 和 **Prisma Access** > 操作 > > **Troubleshooting**（问题排查） > 会话浏览器	过滤依据： • Firewalls（防火墙） • Rule Name（规则名称） • Source Zone（源区域） • Source Address（源地址） • Source User（源用户） • Source Port（源端口） • Destination Zone（目标区域） • Destination Address（目标地址） • Destination Port（目标端口） • App-ID	您指定的防火墙	• 会话 ID • 启动时间 • 区域 • 源 • 目标 • 端口 • 协议 • 应用程序 • 入口 • 出口 • 字节
DNS 代理（网络）	管理配置 > **NGFW** 和 **Prisma Access** > 设备设置 > **DNS** 代理	• 显示 DNS 代理缓存 • 搜索 DNS 代理缓存	您指定的防火墙	• 域名 • IP 地址 • 类型 – IPv4 地址记录 (A)、IPv6 地址记录 (AAAA)、规范名称记录

 ©2025 Palo Alto Networks, Inc.

功能	功能位置	可用操作	操作范围	作业输出组织方式：
				(CNAME)、邮件交换记录 (MX) 和规范名称指针 (PTR) • 类：互联网 (IN TCP/IP)、Chaos (CH) 和 Hesiod (HS) • 生存时间 (TTL)，以秒为单位 • 命中数 – 自上次重启以来请求该记录的次数
NAT（网络）	管理配置 > **NGFW** 和 **Prisma Access** > 网络策略 > **NAT**	显示 NAT 规则 IP 池	您指定的防火墙	• rule • 类型 • 已使用 • 可用 • 内存大小比率
用户组（身份）	管理配置 > **NGFW** 和 **Prisma Access** > 身份服务 > 云身份引擎	• 显示用户组 • 搜索用户组	您指定的防火墙	• 用户名 • 群组
动态地址组（身份）	管理配置 > **NGFW** 和 **Prisma Access** > 对象 > 地址 > 地址组	• 显示所有动态地址组 • 搜索动态地址组（从列表中选择）	您指定的防火墙	• 名称 • 筛选器 • 成员
动态用户组（身份）	管理配置 > **NGFW** 和 **Prisma Access** > 对象 > 动态用户组	• 按动态用户组搜索 • 按用户名搜索	您指定的防火墙	• 成员（用户名）和/或动态用户组

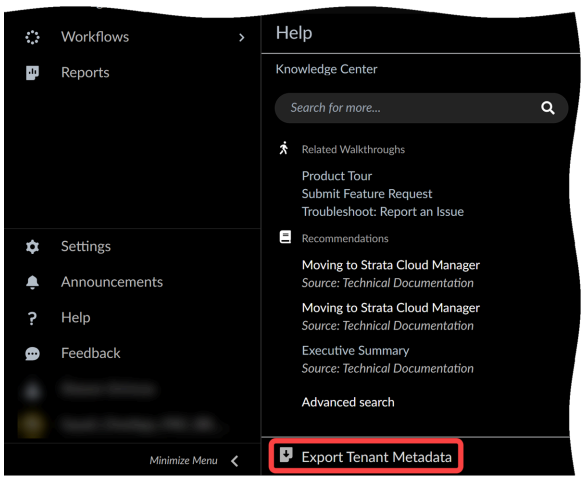
 ©2025 Palo Alto Networks, Inc.

功能	功能位置	可用操作	操作范围	作业输出组织方式：
用户 ID（身份）	管理配置 > **NGFW** 和 **Prisma Access** > 身份服务 > 身份重新分发	• 显示所有用户 IP 映射 • 搜索用户 IP 映射	您指定的防火墙	• IP • 用户 • 从 • 空闲超时 • 最大超时

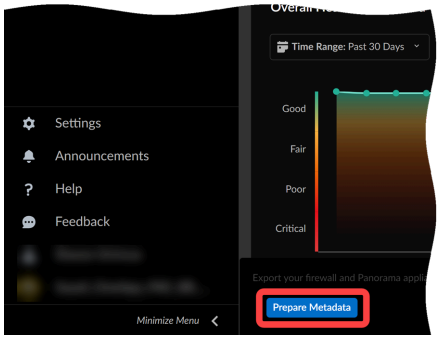
导出元数据以进行故障排除

为了向技术支持部门提供所需的信息，从而更好地为您提供帮助，AIOps for NGFW 能够将部署数据导出到本地计算机。这些数据 JSON 文件形式提供，并以 gzip 格式压缩。

1. 选择 **Help**（帮助）**> Export Tenant Metadata**（导出租户元数据）。



2. 准备元数据。



3. 下载元数据文件。

   元数据文件名包含您的客户支持门户 (CSP) ID、您的 AIOps for NGFW 租户 ID 以及导出的时间戳：*<csp-tenant-timestamp>*.gzip。

 ©2025 Palo Alto Networks, Inc.

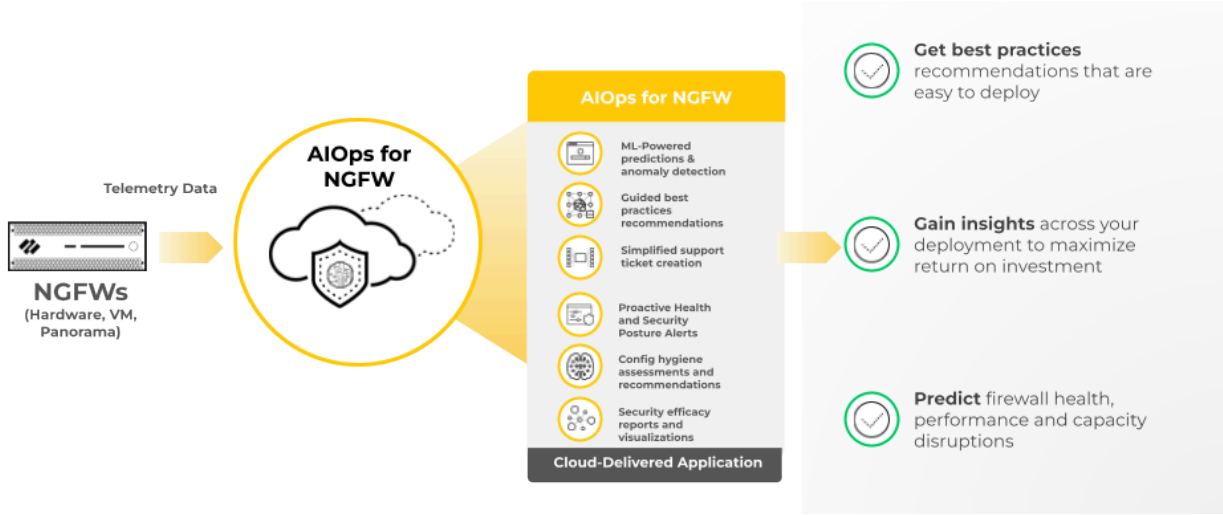
AIOps for NGFW 的设备遥测

在何处可以使用？	需要提供什么？
• ，包括由 软件 NGFW 积分提供资助的项目	其中之一： ❑ 或 ❑ 或

AIOps for NGFW 通过分析PAN-OS设备发送到 Strata Logging Service 的遥测数据来评估部署中防火墙的运行状况。要发送此数据，您必须已经在设备上启用设备遥测。

配置遥测后，新一代防火墙将以固定时间间隔向 Strata Logging Service 发送原始遥测数据。Strata Logging Service 将解析并转换此原始数据，以便 AIOps for NGFW 能够向您提供设备状态、可视化和警报。

载入设备，以开始向 AIOps for NGFW 发送设备遥测。



在设备上启用遥测

要将 AIOps for NGFW 与您的 PAN-OS 设备一起使用，请遵循以下步骤。

如果您的出站流量要经过代理，请确保您已允许 AIOps for NGFW 所需要的域。

如果您正在加载 *Panorama* 托管的部署，则需要在 *AIOps for NGFW* 上载入 *Panorama*。

1. 确认设备已在客户支持门户中注册，方法如下：登录 support.paloaltonetworks.com， 切换到您的帐户（如有必要）， 并在**Assets**（资产） > **Devices**（设备）中识别您的设备。
2. 在要载入的设备上安装设备证书。
3. 在设备上启用遥测共享。

在载入设备并启用遥测之后，大约需要几个小时才能在 *AIOps for NGFW* 指示板上看到第一组见解。在设备侧生成和发送遥测的过程是分批完成的，按照某一频率对每个指标进行采样和收集（频率按照指标的用例进行了优化）。此批处理过程可能会导致在载入防火墙与获得见解之间存在延迟。可能要在几个小时之后才能在 *AIOps for NGFW* 指示板上显示与新载入设备相关联的所有见解。

 ©2025 Palo Alto Networks, Inc.

AIOps for NGFW 所需要的域

在何处可以使用？	需要提供什么？
• ， 包括由 软件 NGFW 积分提供资助的项目	其中之一： ❑ 或 ❑ 或

如果来自设备的出站流量通过代理，请确保您已允许以下 FQDN 才能成功使用 AIOps for NGFW。

要访问 **AIOps for NGFW** 的域

允许以下域以访问 AIOps for NGFW 应用程序，无论您的地理区域如何。

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

要发送遥测数据的 **App-ID** 和域

请参阅Strata Logging Service 所需的 TCP 端口和 FQDN，以了解您必须在 Palo Alto Networks 防火墙上允许的 App-ID 和端口，以便将遥测数据成功发送到 AIOps for NGFW。

在您的代理服务器上，除了允许所需的端口和 FQDN，还要允许与您的地理区域对应的域，以便您的设备可以将遥测数据发送到 AIOps for NGFW。

区域	域
美国	http://br-prd1.us.cdl.paloaltonetworks.com/
Europe	http://br-prd1.nl.cdl.paloaltonetworks.com/
英国	http://br-prd1.uk.cdl.paloaltonetworks.com/
加拿大	http://br-prd1.ca1.ne1.cdl.paloaltonetworks.com/
新加坡	http://br-prd1.sg1.se1.cdl.paloaltonetworks.com/

 ©2025 Palo Alto Networks, Inc.

区域	域
日本	http://br-prd1.jp1.ne1.cdl.paloaltonetworks.com/
澳大利亚	http://br-prd1.au1.se1.cdl.paloaltonetworks.com/
德国	http://br-prd1.de1.ew3.cdl.paloaltonetworks.com/
印度	http://br-prd1.in1.as1.cdl.paloaltonetworks.com/

 ©2025 Palo Alto Networks, Inc.

优化安全态势

在何处可以使用？	需要提供什么？
• ， 包括由 软件 NGFW 积分提供资助的项目	其中之一： ❑ 或 ❑ 或

除了帮助您保持防火墙功能正常之外，AIOps for NGFW 还有助于验证它们是否为您提供了有效的安全威胁防护。

安全态势评估目前不支持多个虚拟系统；在处理配置期间，仅考虑默认虚拟系统 *(vsys1)*。

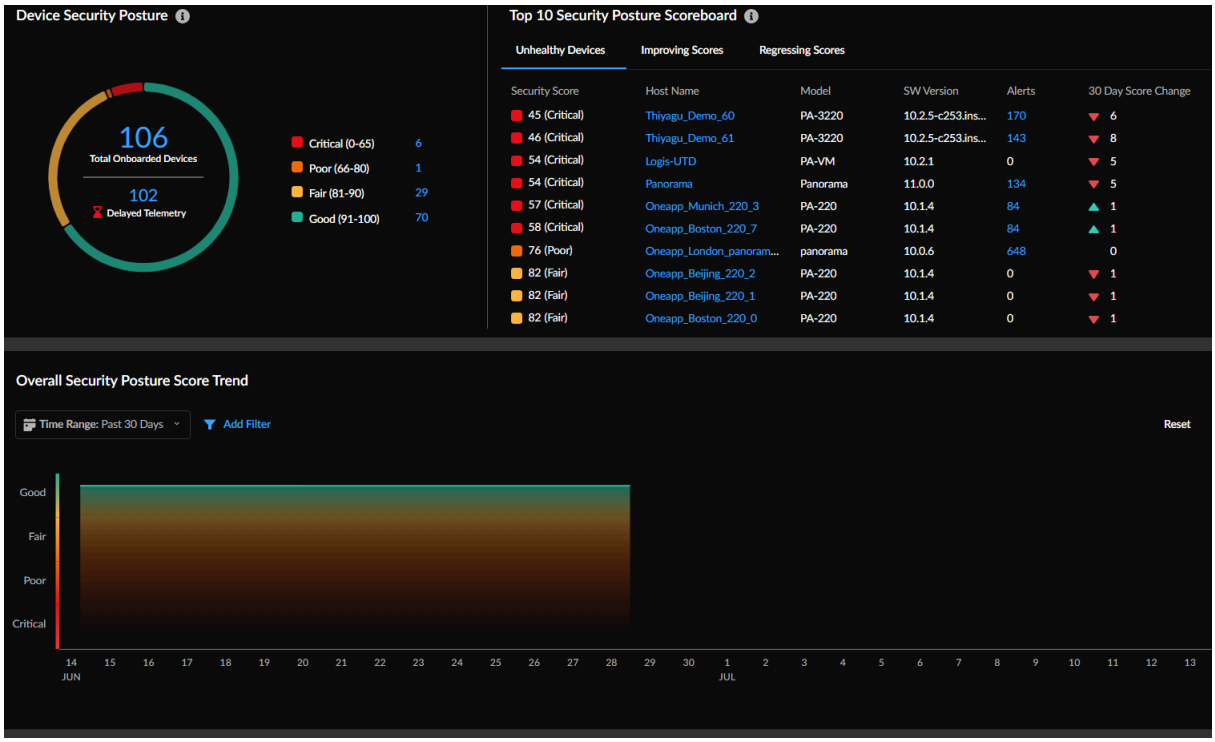
- 监视安全态势见解：根据已载入的 NGFW 设备的安全态势，洞察部署的安全态势和趋势。
- 监视功能采用情况：查看您在部署中使用的安全功能。
- 监控安全订阅：查看推荐的云交付安全服务 (CDSS) 订阅及其在设备中的使用情况。
- 评估漏洞：查看影响特定防火墙和 PAN-OS 版本的漏洞，帮助您就是否需要升级做出决策。
- 监视合规性摘要：查看过去 12 个月内对安全检查所做的更改的历史记录，这些更改由互联网安全中心 (CIS) 和美国国家标准与技术研究院 (NIST) 框架分组在一起。
- 主动执行安全检查：阻止未通过特定最佳实践检查的提交，从而对次优配置采取主动措施。
- 策略分析器：给出特定策略规则的潜在合并或删除的分析和建议，以满足您预期的安全态势，并检查规则库中的异常情况，如遮盖、冗余、泛化、关联和合并。

监视安全态势见解

在何处可以使用？	需要提供什么？
• ， 包括由 软件 NGFW 积分提供资助的项目	• 其中之一： ❑ 或 ❑ 或 • 有权查看指示板的角色

可以使用安全态势见解指示板，根据载入的 NGFW 设备的安全态势来了解部署的安全状态和趋势。安全评分的严重性（0 到 100）及其相应的安全等级（良好、一般、差、极差）决定了设备的安全态势。安全分数的计算依据包括开放警报的优先级、数量、类型和状态。

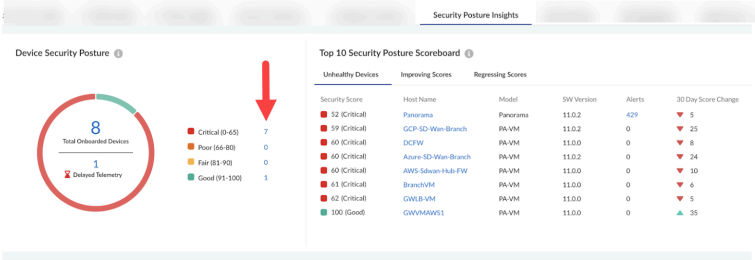
1. 首先导航到 **Dashboards**（指示板） > **Security Posture Insights**（安全态势见解）。



 ©2025 Palo Alto Networks, Inc.

2. 使用 **Device Security Posture**（设备安全态势）来查看设备的运行状况。可以查看以下内容：
   - 已载入的 NGFW 总数。
   - 超过 12 小时未发送遥测数据的设备数量。
   - 部署中载入设备的安全分值的优先级。单击编号链接可了解设备详细信息和安全统计信息。

   例如，您可以查看所有设备的 7 个严重风险。



   在这种情况下，您可以单击严重警报并查看生成警报的设备。您可以进一步向下钻取并注意到防火墙上尚未启用“用户凭据保护”。可以在所有设备上解决此问题，以避免网络钓鱼攻击。

3. 查看过去 30 天内运行状况最差和安全评分下降的设备。可以查看设备的运行状况，包括其运行状态、软件版本和其他重要指标。

   您还可以注意到某些设备是否运行过时的软件版本。在这种情况下，您可以计划升级到最新的建议版本，您可以通过升级建议找到该版本。

4. 检查所选时间段内部署的安全态势趋势。将鼠标悬停在触发点上，可了解影响安全态势趋势的设备和活动警报。您可以查看按主机名、型号或软件版本过滤的一个或多个设备的趋势。

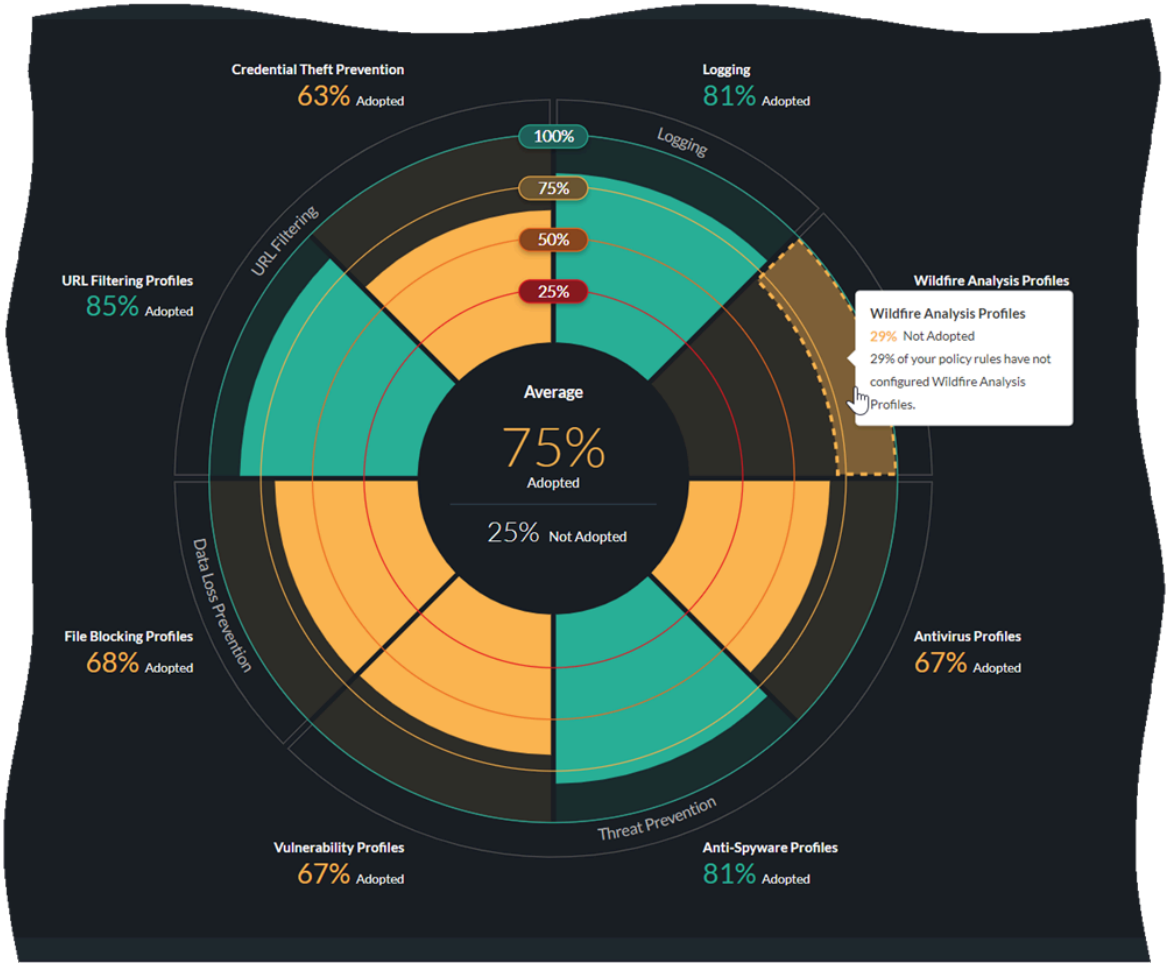
有关详细信息，请参阅指示板：安全态势见解。

 ©2025 Palo Alto Networks, Inc.

监视功能采用情况

在何处可以使用？	需要提供什么？
• ， 包括由 软件 NGFW 积分提供资助的项目	• 其中之一： ❑ 或 ❑ 或 • 有权查看指示板的角色

在 **Dashboards**（仪表板） > **Feature Adoption**（功能采用）， 您可以查看在部署中使用的安全功能。这可以帮助您确保充分利用您的 Palo Alto Networks 安全订阅和防火墙功能。



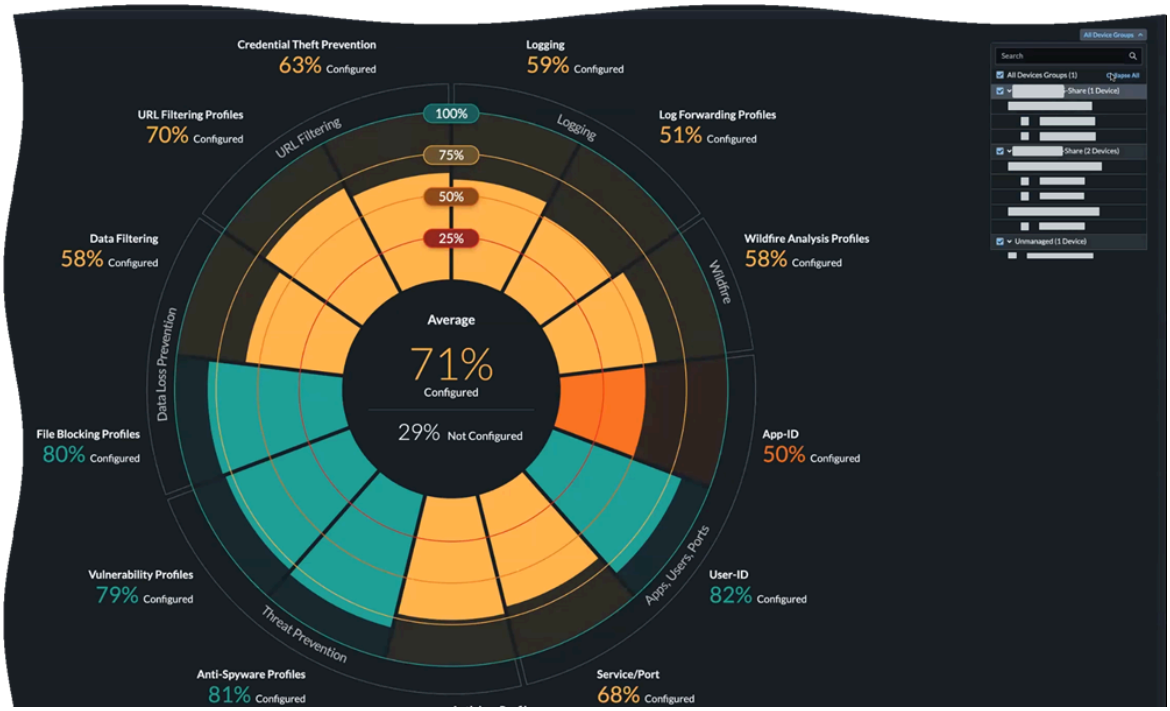
此指示板显示安全策略的强大之处以及功能采用方面的差距，从而让您专注于改进弱点。要获得对流量的最大可见性和最大程度的防御攻击，请设立安全功能采用目标，并将以下建议用作最佳实践基准。根据基准评估您当前的状态，以确定在安全策略功能采用方面的差距。

 ©2025 Palo Alto Networks, Inc.

“采用摘要”可帮助确定您可以改进安全策略功能采用的设备、区域和地域。您可以按设备组、序列号以及 Vsys、区域、基础架构区域、标记、规则详细信息和区域映射查看采用信息。对设备组进行过滤以缩小范围并确定差距。

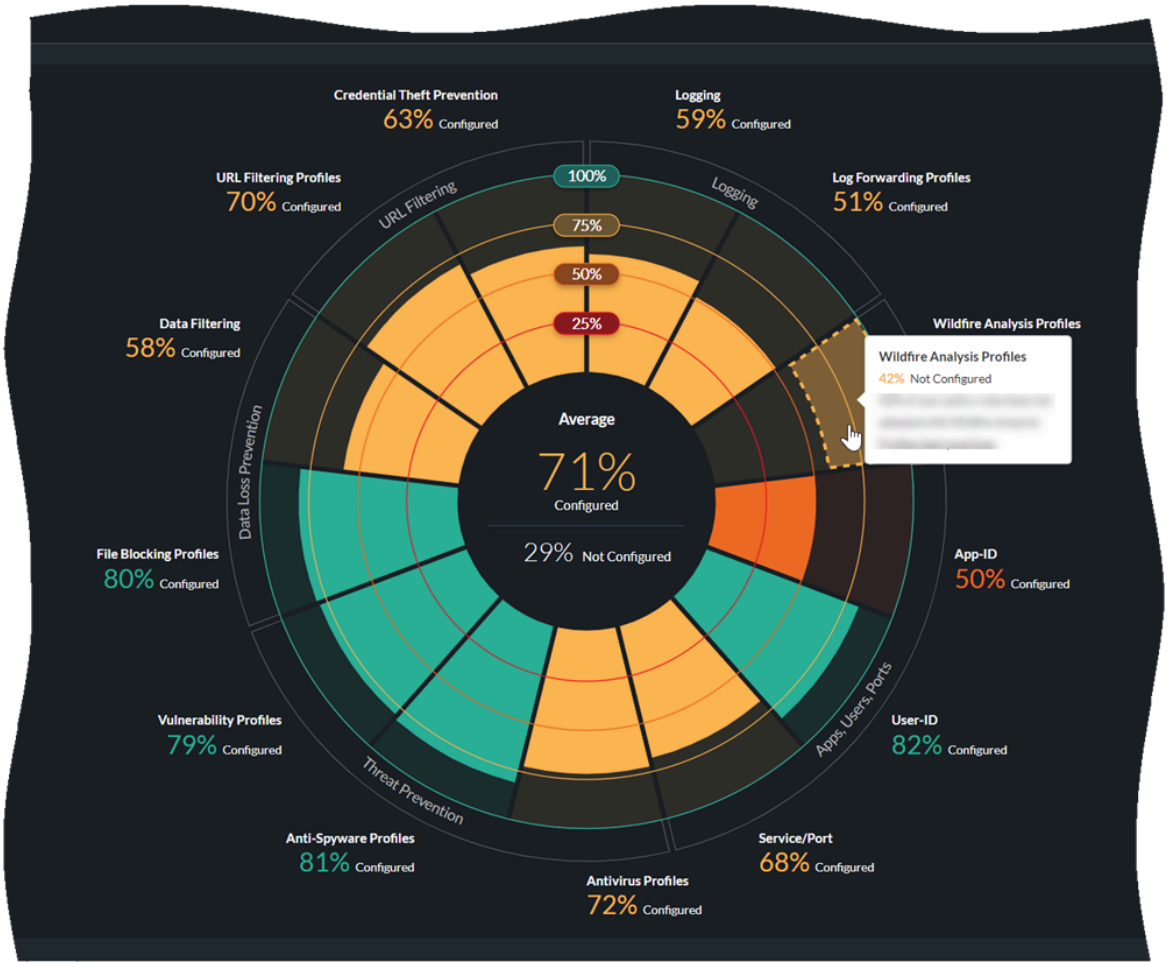
在 **Feature Adoption**（功能采用）中，还可以通过选择 **Best Practices**（最佳实践）来查看您的安全功能是否根据 Palo Alto Networks 最佳实践进行配置。

要关注一组特定防火墙的最佳实践合规性，可以根据设备组过滤图表。



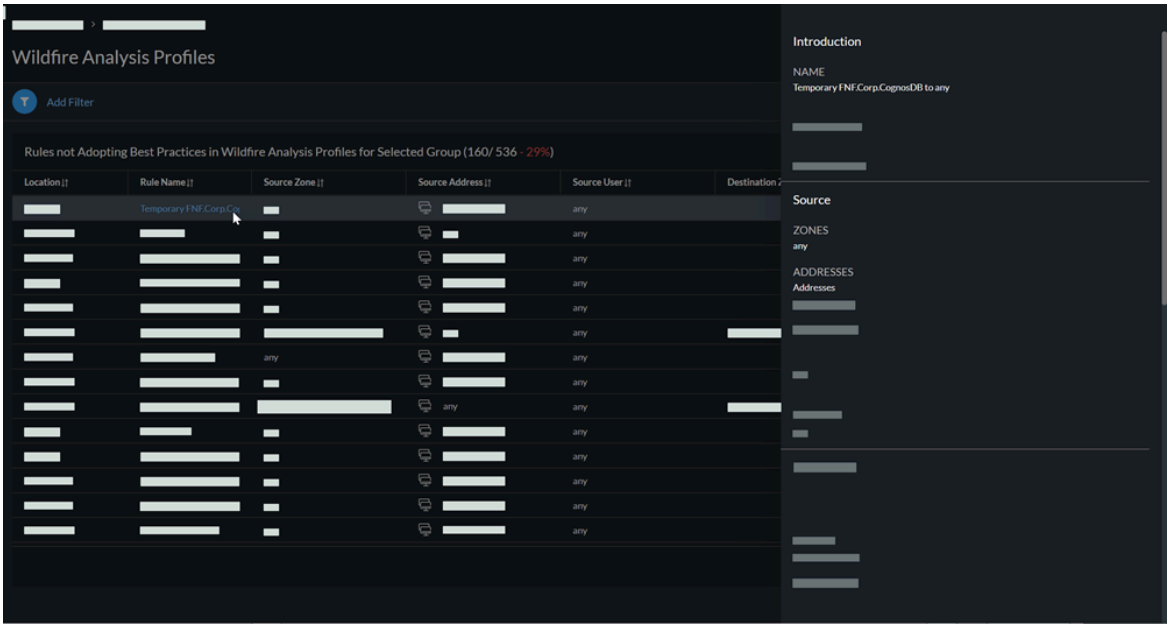
 ©2025 Palo Alto Networks, Inc.

选择图表上某个功能的部分，以查看可以改进的策略规则。



 ©2025 Palo Alto Networks, Inc.

选择一条规则可查看其详细信息，而无需离开应用程序。



有关详细信息，请参阅指示板：功能采用。

 ©2025 Palo Alto Networks, Inc.

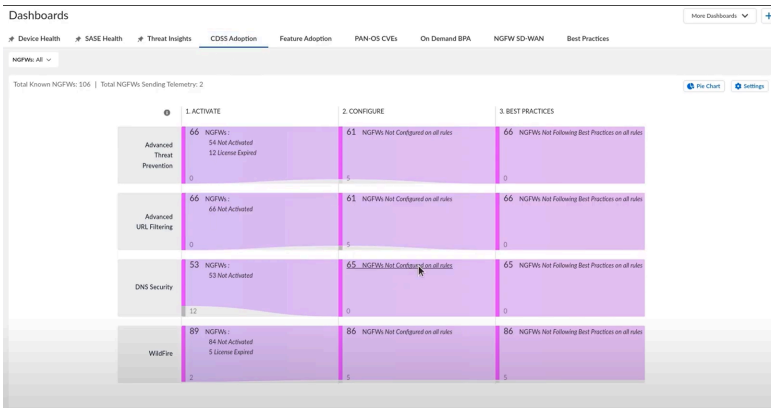
监控安全订阅

在何处可以使用？	需要提供什么？
• ，包括由 软件 NGFW 积分提供资助的项目	• 其中之一： ❑ 或 ❑ 或 • 有权查看指示板的角色

在 **Dashboard**（指示板） > **Posture**（态势） > **CDSS Adoption**（**CDSS** 采用）中，您可以查看推荐的云交付安全服务 (CDSS) 订阅及其在设备中的使用情况。这有助于您识别安全漏洞并强化企业的安全态势。导航到此页面后，您将看到一个弹出窗口，要求您确认或更新 NGFW 中的区域角色，以获取准确的安全服务建议。您可以点击此弹出窗口中的链接以将区域映射到角色。

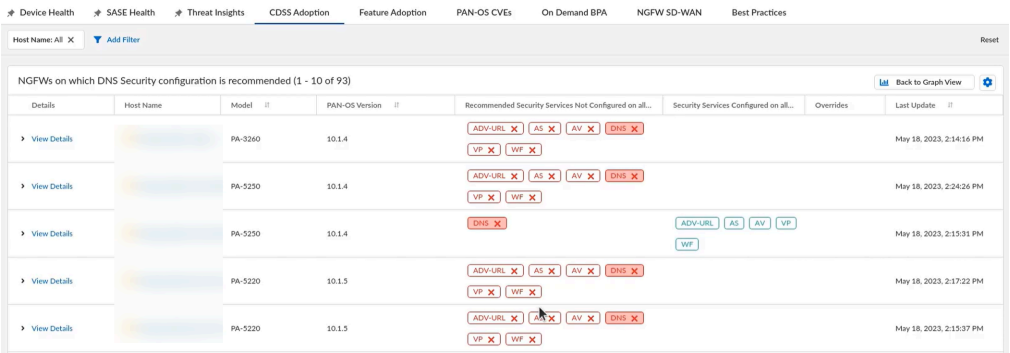
目前，此指示板仅支持四种安全订阅：高级威胁防御、高级 *URL* 过滤、*DNS* 安全和 *Wildfire*。

1. 在 **CDSS Adoption**（**CDSS** 采用）页面顶部，可以查看实例中已知 NGFW 的总数和发送遥测数据的 NGFW 数量。
2. CDSS 采用包括从激活、配置到遵守最佳实践。要跟踪每个订阅的进度，只需单击图表中的数字，即可查看在此过程中需要更新的设备列表。在这种情况下，我们来检查未配置 DNS 安全性的 NGFW。



 ©2025 Palo Alto Networks, Inc.

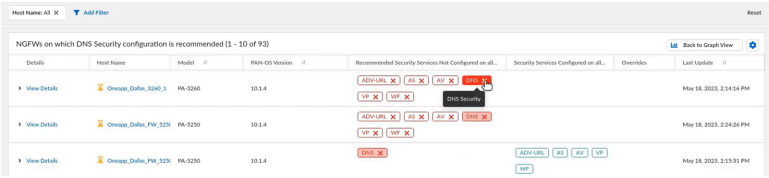
3. 检查那些已建议进行配置但实际未配置 DNS 安全配置的 NGFWS。查看详细信息以检查源角色和目标角色。



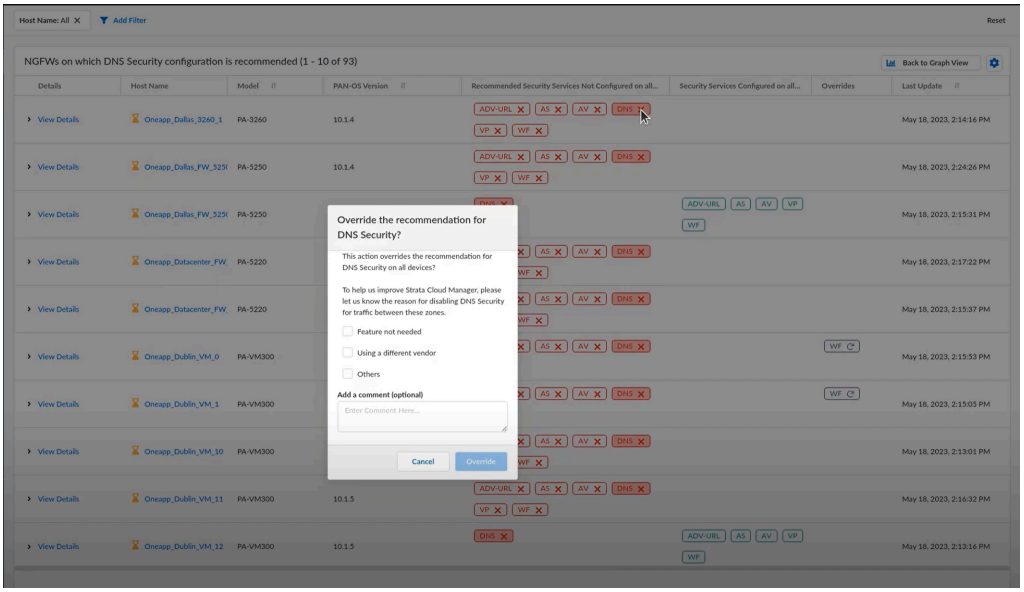
4. 查看策略以查看规则以及相应的源和目标区域的详细信息。

   此外，还可以单击规则名称以查看其详细信息。

5. 导航回漏斗图。也可以以饼图格式查看相同信息。
6. 如果出于任何原因而不需要推荐的安全服务时，可以覆盖。在这种情况下，我们不需要 DNS 安全服务。单击 **DNS** 旁边的取消图标。



7. 选择其中一项覆盖建议的原因。



8. 单击 **Override**（覆盖）。

   本节总结了如何查看推荐的 CDSS 订阅及其在设备中的使用情况。

有关详细信息，请参阅指示板：CDSS 采用。

 ©2025 Palo Alto Networks, Inc.

评估漏洞

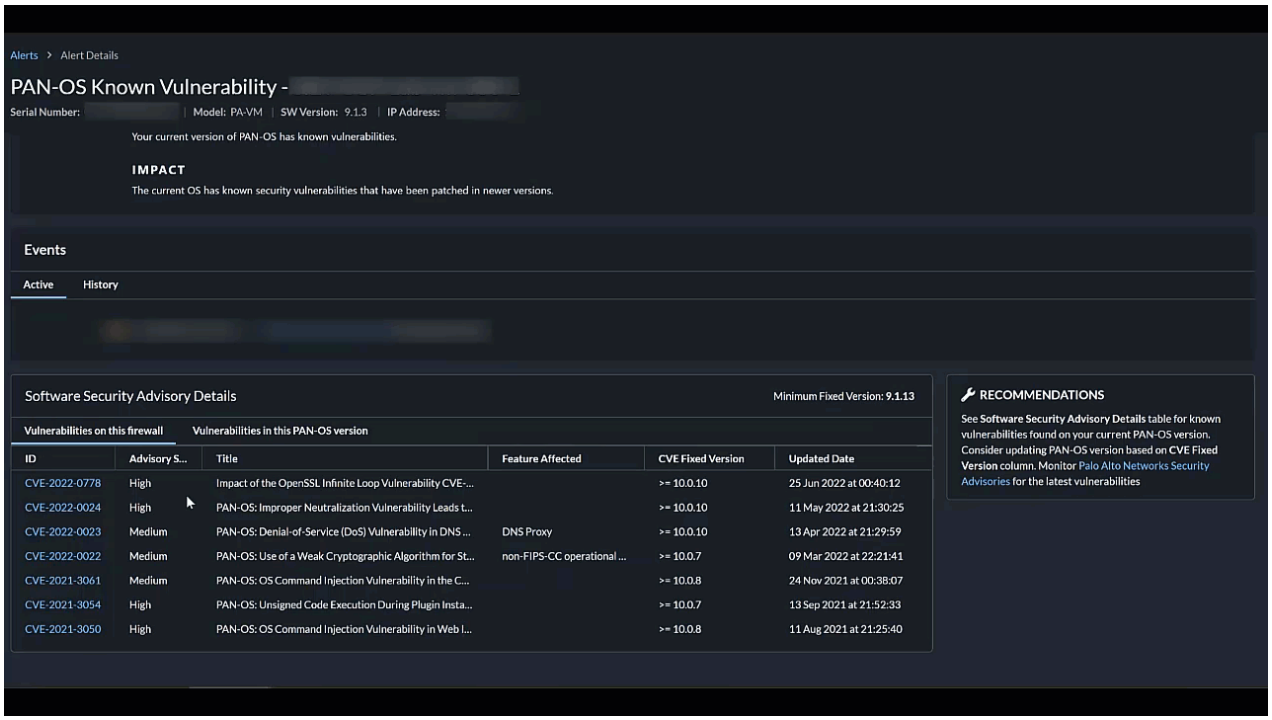
在何处可以使用？	需要提供什么？
• ，包括由 软件 NGFW 积分提供资助的项目	其中之一： ❑ 或 ❑ 或

Strata Cloud Manager 显示哪些漏洞会影响给定防火墙和以及 PAN-OS 版本，以帮助您决定是否应该升级。导航到 **Incidents & Alerts**（事件和警报） > **NGFW** > **All Alerts**（所有警报），然后选择 **PAN-OS Known Vulnerability**（**PAN-OS** 已知漏洞）警报，以查看最新安全建议来修复引发警报的防火墙。

选择 **Vulnerabilities in this PAN-OS version**（此 **PAN-OS** 版本中的漏洞），以在 **Feature Affected**（受影响的功能）列中查看某一漏洞所影响的功能。这有助于您根据漏洞及其对已启用功能的影响程度来决定是否升级防火墙。如果某个 CVE 没有关联功能，则 **Feature Affected**（受影响的功能）为空。这种类型的 CVE 会影响指定型号或版本的防火墙。

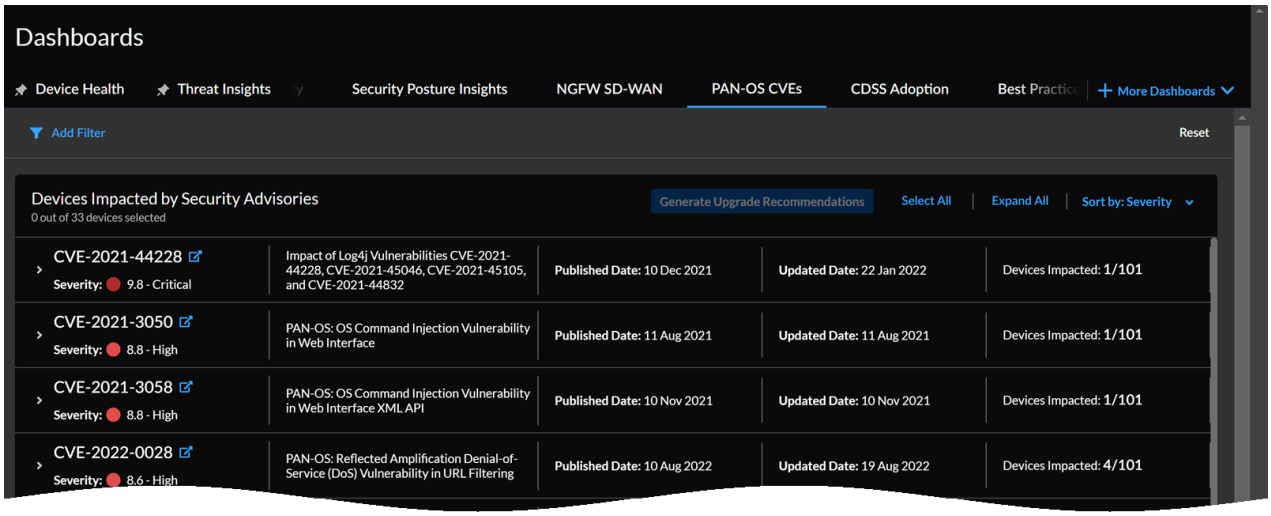
默认情况下，**PAN-OS Known Vulnerability**（**PAN-OS** 已知漏洞）警报显示设备上 PAN-OS 版本中的所有漏洞。但如果已在防火墙上启用了产品使用情况遥测，则可以选择仅查看影响特定防火墙（基于其启用的功能）的漏洞。这样便于更好地了解防火墙关注哪些漏洞，并就是否升级做出更明智的决定。

 ©2025 Palo Alto Networks, Inc.



 ©2025 Palo Alto Networks, Inc.

还可以使用 **PAN-OS CVE** 指示板，其根据设备上已启用的功能来显示特定漏洞所影响的设备数量。Strata Cloud Manager 会分析已启用的功能，以确定 CVE 所影响的设备。以下任务说明如何评估影响设备的漏洞以及如何生成升级修复这些漏洞的建议。



此任务说明如何评估影响设备的漏洞以及如何生成升级修复这些漏洞的建议。

STEP 1 | 从 Strata Cloud Manager 中，导航到 **Dashboards**（指示板）> **PAN-OS CVEs**。

STEP 2 | 展开一个 CVE 以查看其影响的设备。

STEP 3 | 选择要升级以修复漏洞的设备。

STEP 4 | 生成升级建议。

STEP 5 | 单击为设备新生成的报告。

STEP 6 | 选择其中一个升级选项可查看有关新功能、**PAN-OS** 已知漏洞、行为变更和 **PAN-OS** 已知问题的详细信息

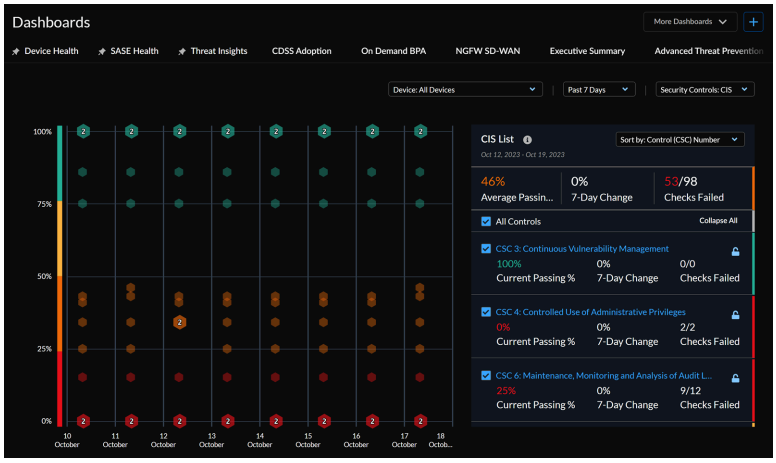
可将详细信息导出为 CSV 文件并下载。

 ©2025 Palo Alto Networks, Inc.

监视合规性摘要

在何处可以使用？	需要提供什么？
• ， 包括由 软件 NGFW 积分提供资助的项目	❑ 或 ❑ 用于在指示板中查看受支持产品数据的许可证：Prisma Access

要访问合规性摘要指示板，请转到 **Dashboards**（指示板），然后选择 **Compliance Summary**（合规性摘要）选项卡。您可以查看过去 12 个月内对安全检查所做的更改的历史记录，这些更改由互联网安全中心 (CIS) 和美国国家标准与技术研究院 (NIST) 框架分组在一起。对于每个框架，您将看到一个控制列表，以及当前和平均符合率的百分比、最佳实践检查的总数以及每个控制的失败检查的数量。与图表和列表交互以查看控件及其历史统计数据之间的关系。查看各项控制及其关联检查的详细信息，并选择最佳实践检查以查看未通过检查的防火墙配置。**CIS** 关键安全控制框架是一组按优先顺序排列的建议措施和最佳实践，可帮助保护组织及其数据不会受到已知网络攻击媒介的攻击。



您可以查看 16 个基本和基础 CIS 控件中的 11 个控件的检查摘要：

- CSC 3：持续漏洞管理
- CSC 4：管理权限的受控使用
- CSC 6：审计日志的维护、监控和分析
- CSC 7：电子邮件和网络浏览器保护
- CSC 8：恶意软件防御
- CSC 9：网络端口、协议和服务的限制和控制
- CSC 11：保护网络设备的配置，如防火墙、路由器和交换机
- CSC 12：边界防御
- CSC 13：数据保护
- CSC 14：基于“按需知悉”的原则进行受控访问

 ©2025 Palo Alto Networks, Inc.

- CSC 16：帐户监视和控制

NIST 网络安全框架 **SP 800-53** 控制框架为联邦机构和其他组织提供指导，帮助其实施和维护其信息系统的安全和隐私控制。您可以查看 NIST 控件的八个系列的检查摘要：

- SC：存取控制
- AU：审计和问责制
- CM：配置管理
- CP：应急计划
- IA：身份识别和身份认证
- RA：风险评估
- SC：系统和通信保护
- SI：系统和信息完整性

有关详细信息，请参阅指示板：合规性摘要。

 ©2025 Palo Alto Networks, Inc.

主动执行安全检查

在何处可以使用？	需要提供什么？
• ，包括由 软件 NGFW 积分提供资助的项目	☐ 或

可以使用下面的功能为您的部署自定义安全态势检查，以充分利用相关建议。

- 安全检查

  AIOps for NGFW 用于评估配置的最佳实践检查列表。比较防火墙和 Panorama 的配置与 Palo Alto Networks 的最佳实践检查清单，以评估设备的安全态势并生成安全警报。可以看到用于评估您的配置的最佳实践检查清单。

  在这里，您可以：

  1. 设置检查的严重性级别，以标识对部署最关键的检查。
  2. 临时禁用检查。

     如果选择禁用检查，可以指定该检查将保持禁用状态的时间，并留言以解释禁用该检查的原因。
  3. 设置检查失败时的响应。
- 区域到角色的映射

  将 NGFW 中的区域映射到角色以获得定制建议。
- 角色到安全服务的映射

  管理所有 NGFW 中区域和角色之间的流量所需的安全服务。

通过 Panorama CloudConnector 插件，可以阻止未通过特定最佳实践检查的提交，从而对次优配置采取主动措施。当您在 AIOps for NGFW 中指示希望检查提交失败时，Panorama 会自动阻止提交任何未通过该检查的配置。应首先使用插件来避免部署中出现配置问题，而非等待接收有关最佳实践检查失败的警报。

STEP 1 | 确保您满足所有先决条件，然后安装插件。

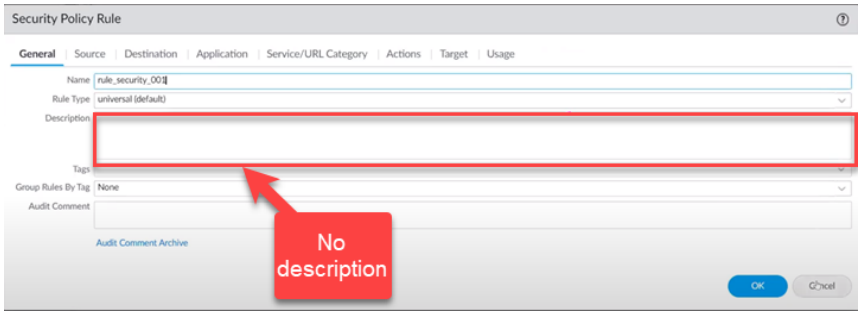
STEP 2 | 指定在失败时阻止提交的最佳实践检查清单。

1. 选择 **Manage**（管理） > **Security Posture**（安全态势） > **Settings**（设置）。
2. 找到您想要阻止提交的检查。
3. 将 **Action on Fail**（失败时的操作）设置为 **Fail Commit**（提交失败）。

 ©2025 Palo Alto Networks, Inc.

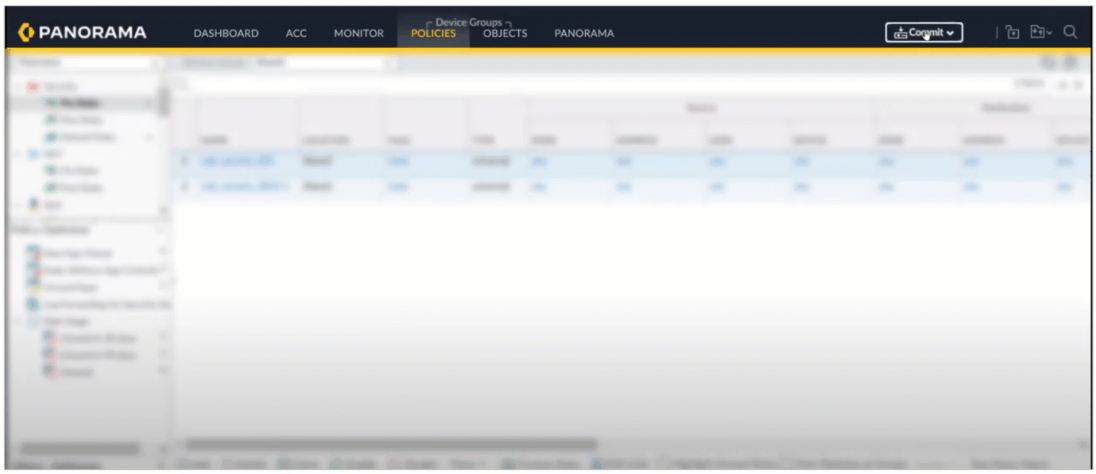
STEP 3 | 通过尝试提交未通过检查的配置进行验证。

1. 登录到 Panorama。
2. 将违反您指定的最佳实践检查时的操作设置为 **Fail Commit**（提交失败）。



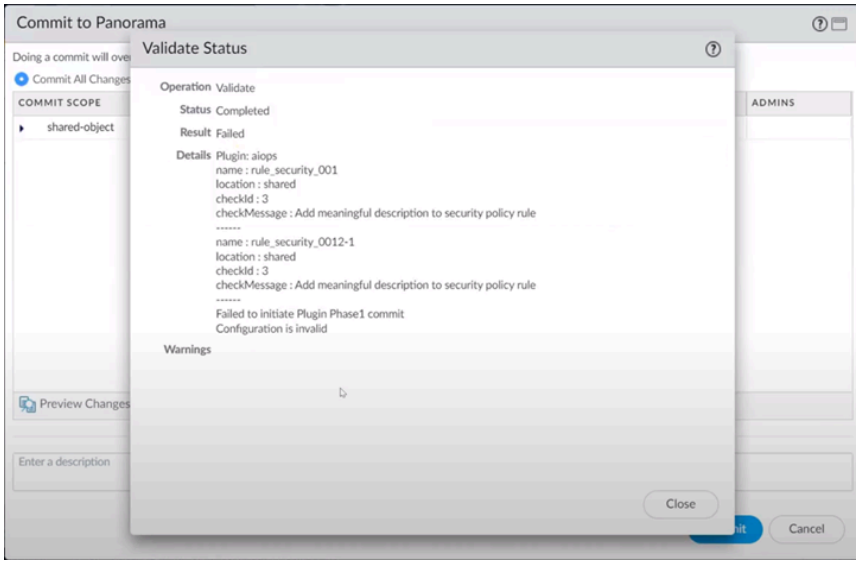
3. 选择 **Commit**（提交） > **Commit to Panorama**（提交到 **Panorama**） > **Validate Configuration**（验证配置）。

 ©2025 Palo Alto Networks, Inc.



 ©2025 Palo Alto Networks, Inc.

您应该会看到一个对话框，指出验证失败，因为配置未通过最佳实践检查。



如果将检查设置为 ***Fail Commit***（提交失败），则检查的验证和实际提交操作都将失败。

请参阅管理：安全态势设置以了解更多信息。

 ©2025 Palo Alto Networks, Inc.

策略分析器

在何处可以使用？	需要提供什么？
• NGFW（Panorama 托管） • （Panorama 托管） •	❑ 或 ❑ Panorama CloudConnector 插件，用于 Panorama 托管部署

对安全策略规则的更新通常在时间上很敏感，需要您迅速采取行动。但是，您希望确保对安全策略规则库所做的任何更新都符合您的要求，并且不会引入错误或错误配置（例如，导致规则重复或冲突的更改）。

利用 Strata Cloud Manager 中的策略分析器，您可以在实施变更请求时优化时间和资源。策略分析器不仅能够分析，就特定规则的可能合并或移除给出建议以满足您的意图，而且还会检查规则库中的异常清空，如遮蔽、冗余、泛化、关联和合并。

使用策略分析器来添加或优化您的安全策略规则库。

- 添加新规则之前 — 检查是否确实需要添加新规则。策略分析器会尽可能建议如何在不添加其他规则的情况下，以最佳方式更改现有安全策略规则来满足您的要求。
- 简化并优化您现有的规则库 — 找出可以更新规则的机会，最大限度地减少规则库膨胀并消除冲突，并确保流量强制执行与安全策略规则库的意图保持一致。

在提交更改之前和之后都要分析您的安全策略规则。

- 变更前策略分析 — 能够评估新规则的影响，并根据现有规则分析新规则的意图，以就如何最好地满足意图给出建议。
- 变更后策略分析 — 通过识别逐渐积累的遮蔽、冗余和其他异常，从而清理现有的规则库。

- 策略分析器要求 *Panorama* 设备上具有 CloudConnector 插件 *1.1.0* 或更高版本。您需要使用以下命令启用此插件：

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

- 策略分析器要求将 *Panorama* 更新至 *PAN-OS* 版本 *10.2.3* 或更高版本。

策略分析器检测到的异常类型

策略分析器可检测安全策略规则库中以下类型的异常：

- 遮盖 — 由于规则库中更高级别的规则覆盖了相同流量而导致未被命中的规则。

  将按照从上到下的顺序对规则库中的安全策略规则进行评估，因此，如果规则库中级别较高的规则与级别较低的规则所匹配的流量相同，而且这些规则配置了不同操作时，就会产生遮盖的情况。如果移除较低顺序的规则，安全策略不会改变。
- 冗余 — 两个或更多个规则匹配相同流量且配置了相同操作。
- 泛化 — 是指规则库中较低的规则与规则库中较高的规则的流量匹配（反之则不匹配），并且规则采取不同的操作。如果两条策略规则的顺序颠倒，安全策略就会受到影响。

 ©2025 Palo Alto Networks, Inc.

- 关联 — 规则与另一条规则相关，此时一条规则与另一条规则的某些数据包匹配，但会导致的操作不同。如果两条规则的顺序颠倒，安全策略就会受到影响。
- 合并 — 您可以将这些规则合并为单个规则，因为操作相同且只有一个属性不同。通过修改其中一个规则的属性并删除其他规则，可以将这些规则合并为单个规则。

变更前策略分析

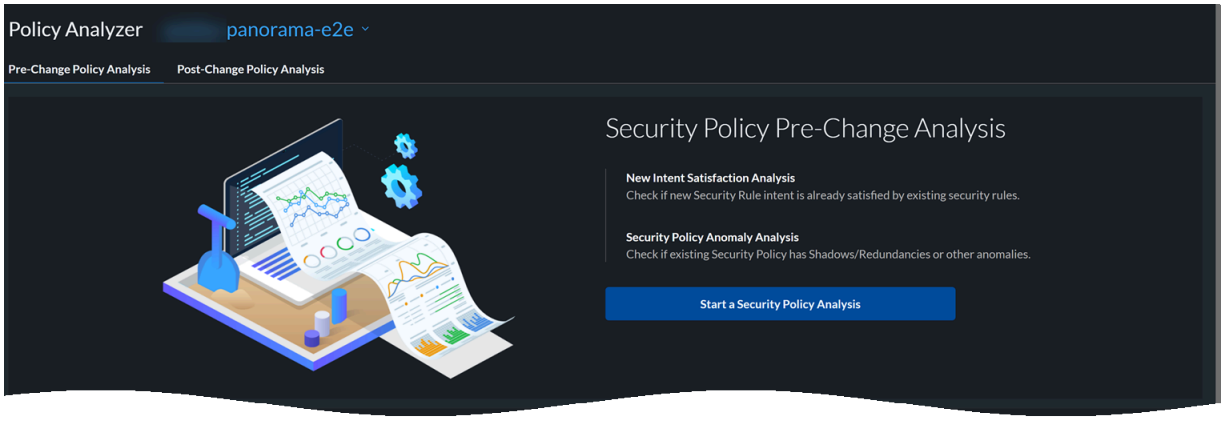
在何处可以使用？	需要提供什么？
• NGFW（Panorama 托管） • （Panorama 托管） •	❑ 或 ❑ Panorama CloudConnector 插件，用于 Panorama 托管部署

安全策略规则变更前分析会执行新的意图满意度分析：

- 新意图满意度分析 — 检查新安全策略规则的意图是否已被现有规则覆盖。

准备工作：

1. 转至 **Manage**（管理） > **Security Posture**（安全态势） > **Policy Analyzer**（策略分析器） > **Pre-change Policy Analysis**（变更前策略分析）。
2. 在策略分析器页面顶部，选择包含您需要分析的策略规则的 Panorama 实例。

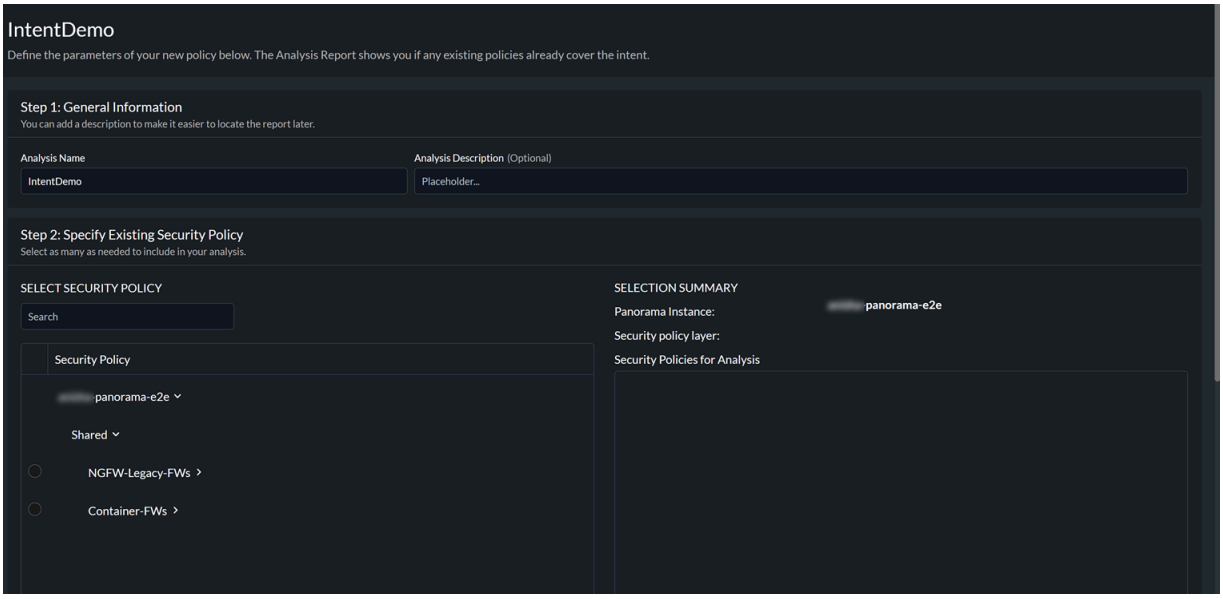


3. 开始安全策略分析。

执行以下步骤开始新的分析：

 ©2025 Palo Alto Networks, Inc.

STEP 1 | 输入分析名称和分析说明。



在 Panorama 设备上，设备组是分层的。可以创建四个级别的设备组，可将 NGFW 分配给最低级别层次结构的设备组。您在较高级别创建的策略将由其涵盖的所有设备组继承。

可以对最多 10 个直接分配了 NGFW 的设备组运行分析，能够分析推送到该组直接分配的 NGFW 的所有策略规则。

STEP 2 | 选择一个现有的安全策略集进行分析。

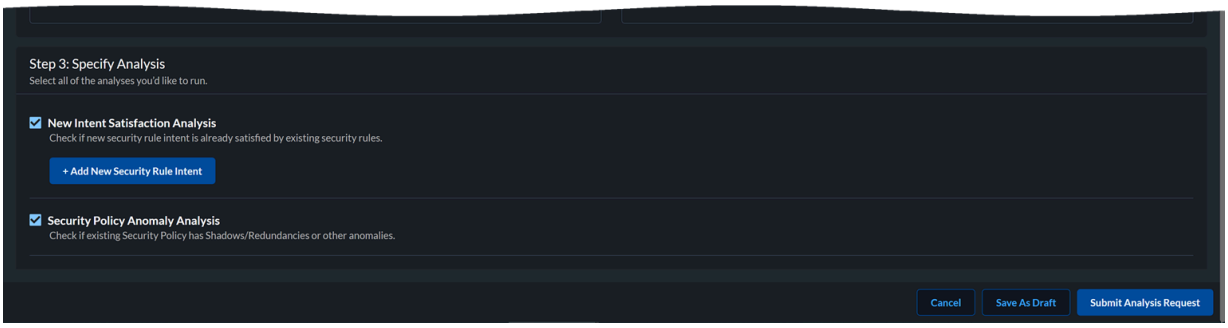
每次分析最多可以选择 10 个设备组。

 ©2025 Palo Alto Networks, Inc.

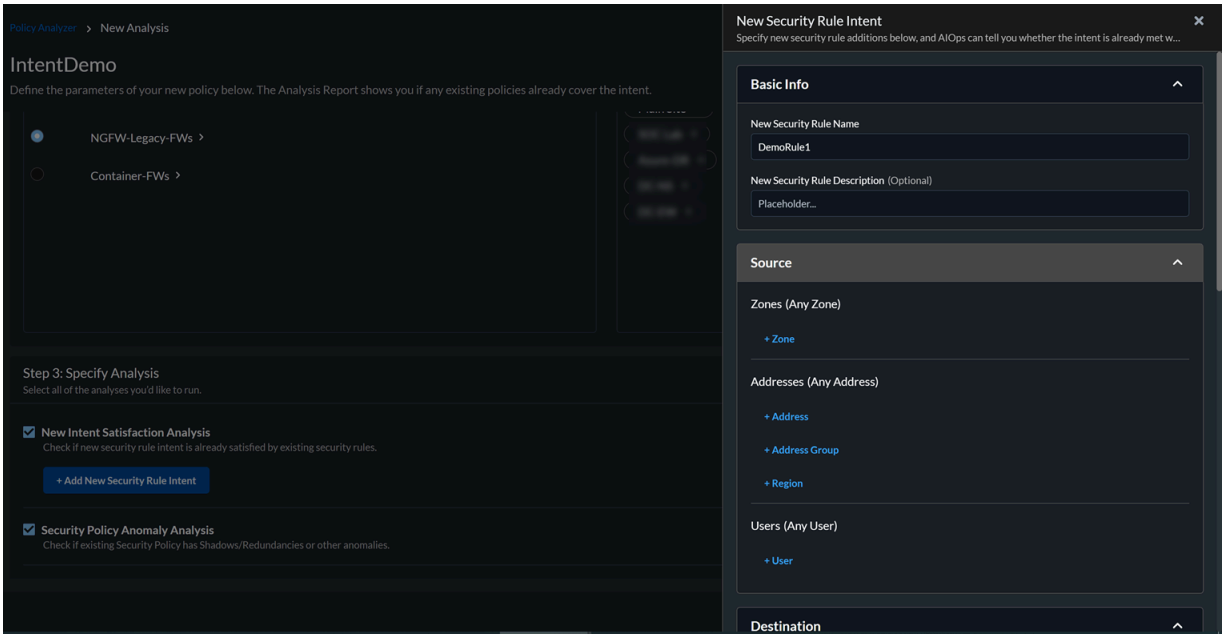
STEP 3 | 选择一种或多种分析类型来指定分析类型：

- 新增意向满意度分析

添加新的安全规则意图以供分析。



指定有关新安全规则的信息，并且 AIOps for NGFW 可以检查现有规则是否涵盖该意图。

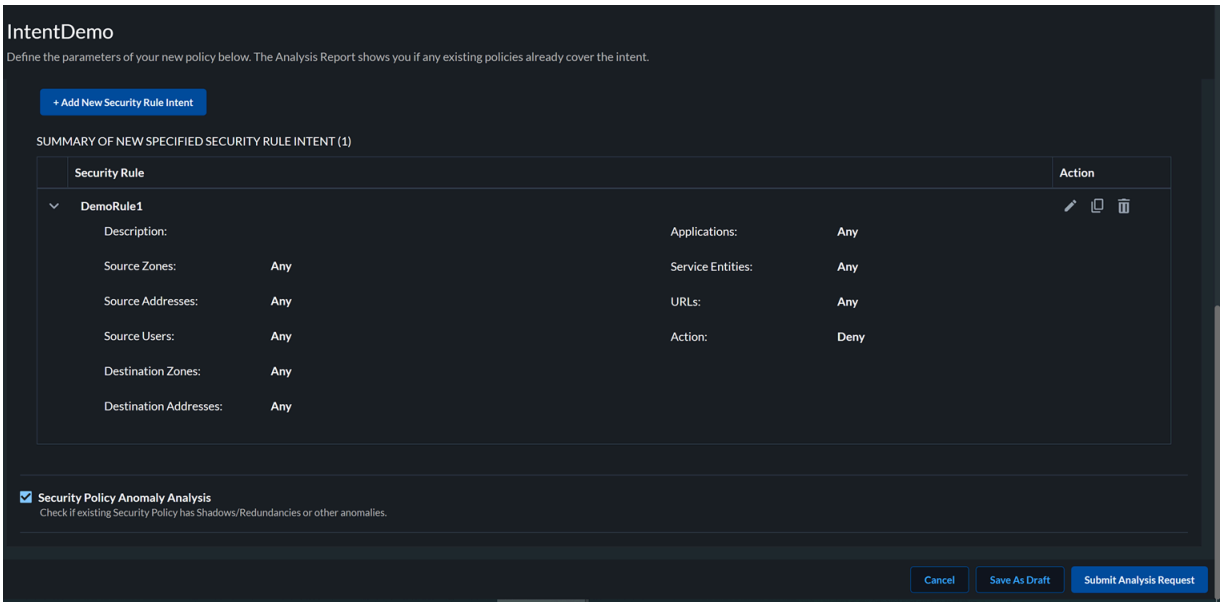


输入安全策略规则组件的值。与安全规则相关的字段的默认值是“Any”。

保存设置。

查看新安全规则意图的摘要。

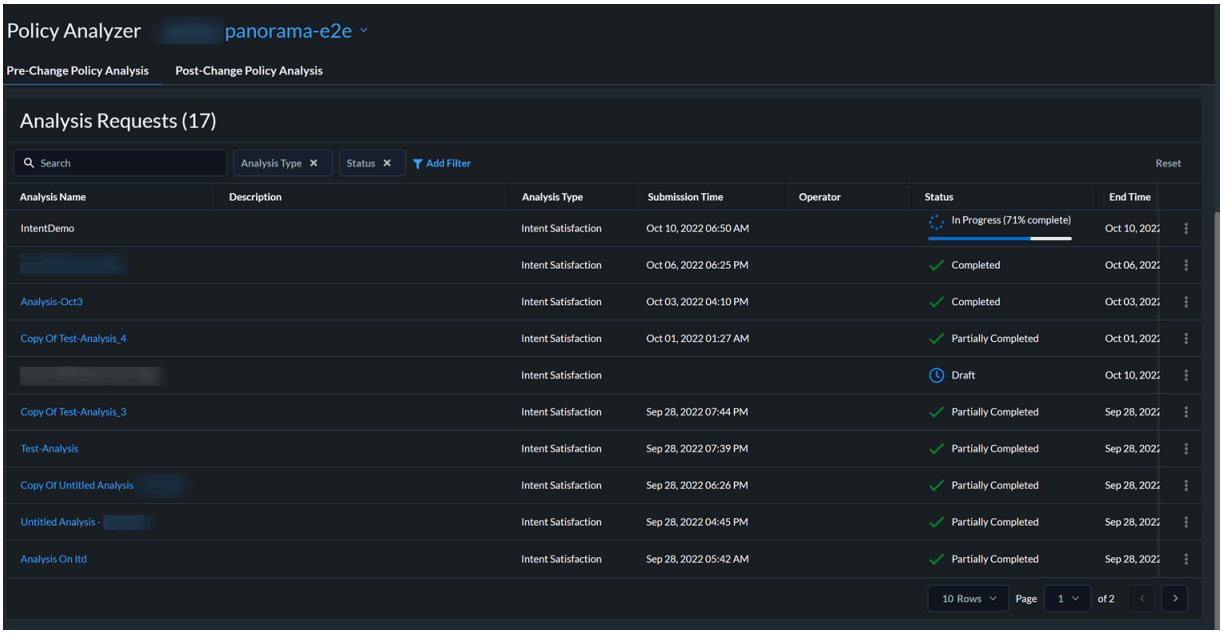
 ©2025 Palo Alto Networks, Inc.



最多可以创建 10 条新的安全规则，也可以复制规则并进行编辑。

STEP 4 | 提交分析请求或另存为草稿以便稍后编辑规则。

在策略分析器页面上“Analysis Requests（分析请求）”下的页面中查看分析状态。



可以取消状态为“进行中”的规则，随后该规则将显示为“已取消”。

分析完成后，查看分析报告。

 ©2025 Palo Alto Networks, Inc.

变更前政策分析报告

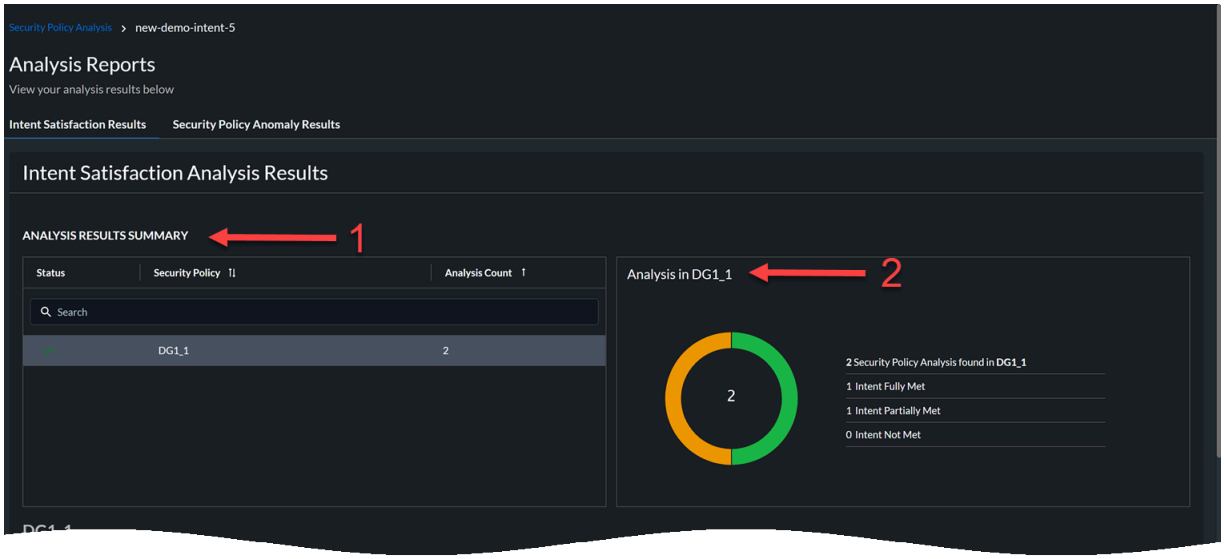
在何处可以使用？	需要提供什么？
• NGFW（Panorama 托管） • （Panorama 托管） •	❑ 或 ❑ Panorama CloudConnector 插件，用于 Panorama 托管部署

选择状态为“已完成”的分析报告，查看策略分析的结果。可以查看分析结果。

意向满意度结果

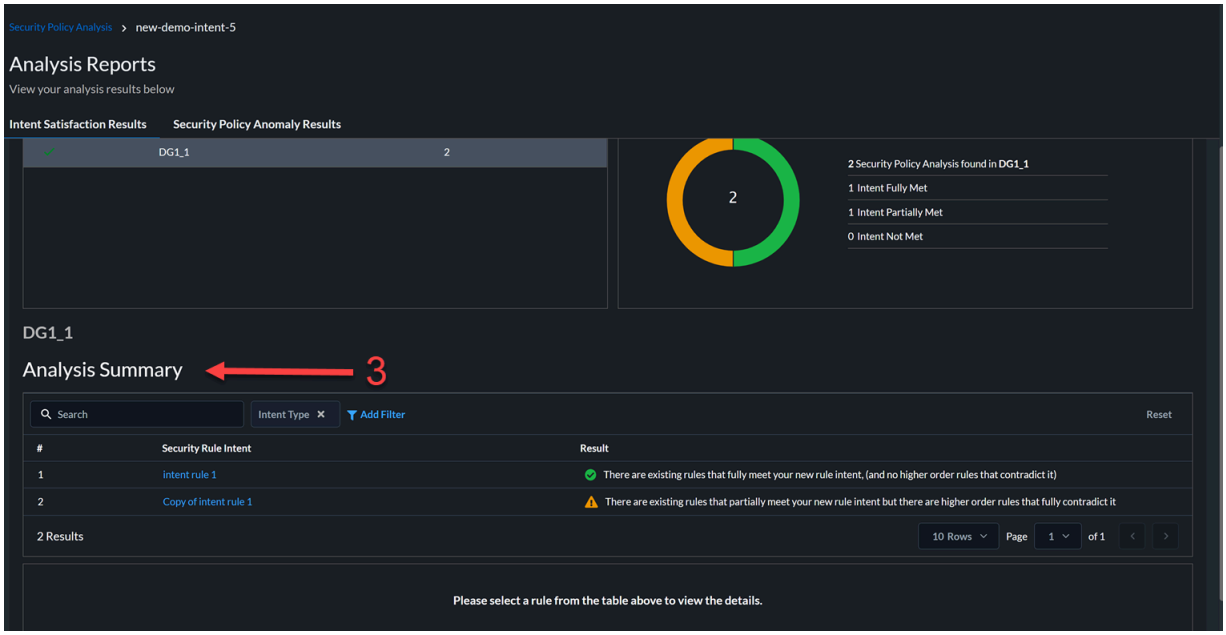
在“Analysis Requests（分析请求）”下的分析列表中，单击一个分析以查看其分析结果。这些结果包括：

1. 分析摘要，其中包含有关设备组和异常计数的详细信息。
2. 单击设备组名称可查看意向满足度分析的结果：
   - 意向完全满足 — 您的安全规则与设备组中的某条现有规则完全一致。
   - 意图部分满足 — 您的安全规则部分满足设备组中某条现有规则的意图。
   - 意图未满足 — 您的安全规则是唯一的，在设备组中不存在。可以将此规则添加到设备组。



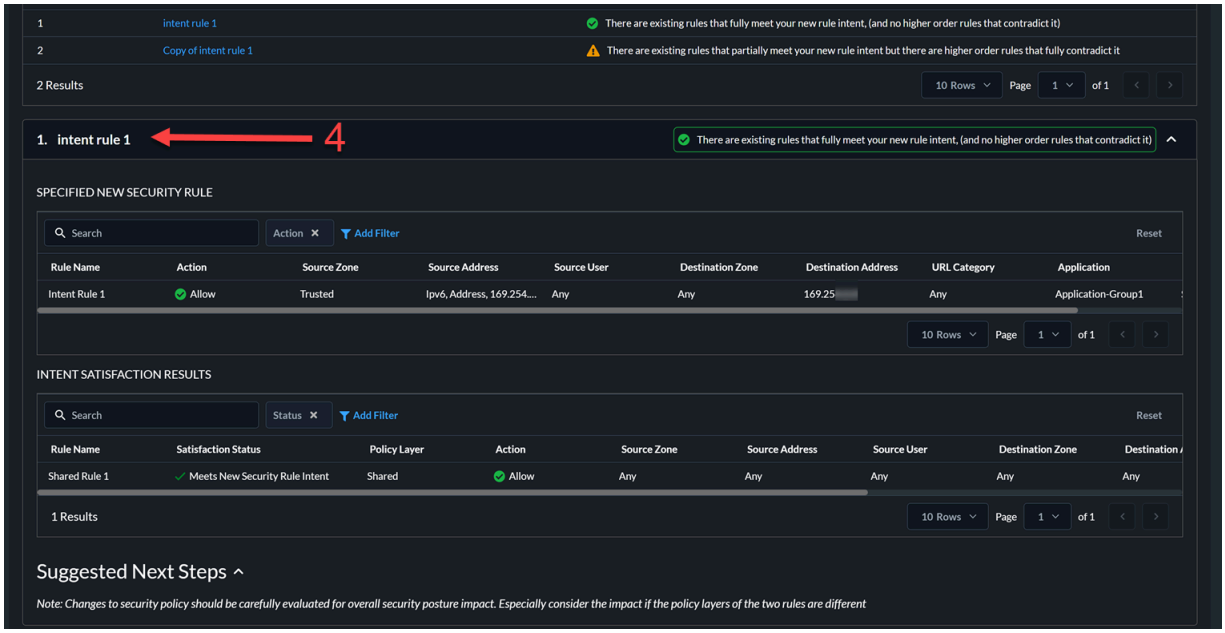
 ©2025 Palo Alto Networks, Inc.

3. 查看新安全规则意图的分析结果。



这个示例中有两条规则。第一条规则的意图与现有规则完全一致，第二条规则的意图与现有规则部分一致。

4. 查看新安全规则的详细信息并检查意图满足结果。



在此示例中，新规则意图规则 1 的所有属性与现有规则共享规则 1 的属性均一致。新规则的意图与现有规则的意图完全一致。因此不需要将此新规则添加到配置中。

 ©2025 Palo Alto Networks, Inc.

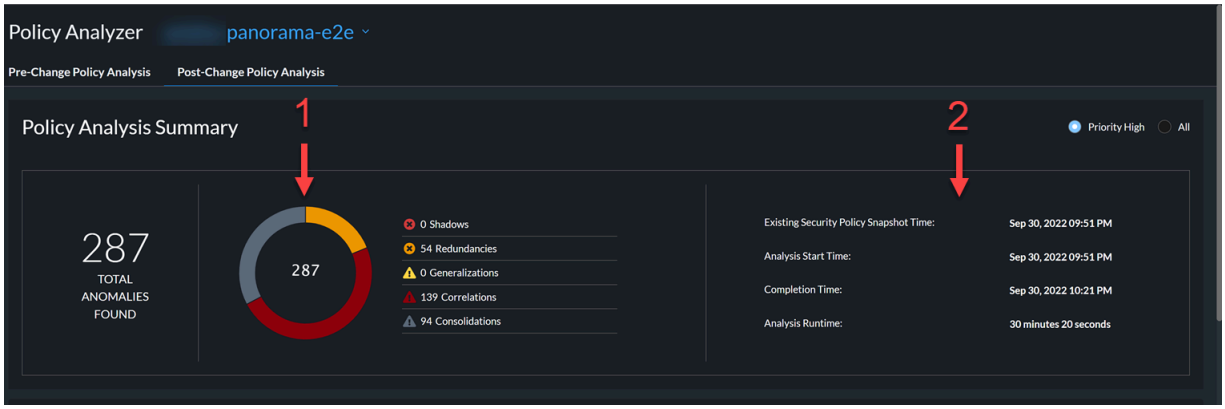
变更后策略分析

在何处可以使用？	需要提供什么？
• NGFW（Panorama 托管） • （Panorama 托管） •	❑ 或 ❑ Panorama CloudConnector 插件，用于 Panorama 托管部署

在 Panorama 上提交配置时，可以通过 Strata Cloud Manager 的插件来分析配置。策略分析器分析此配置的遮盖、冗余和其他异常，您可在 **Manage**（管理） > **Security Posture**（安全态势） > **Policy Analyzer**（策略分析器） > **Post-change Policy Analysis**（变更后策略分析）中查看分析结果。

可以查看以下信息：

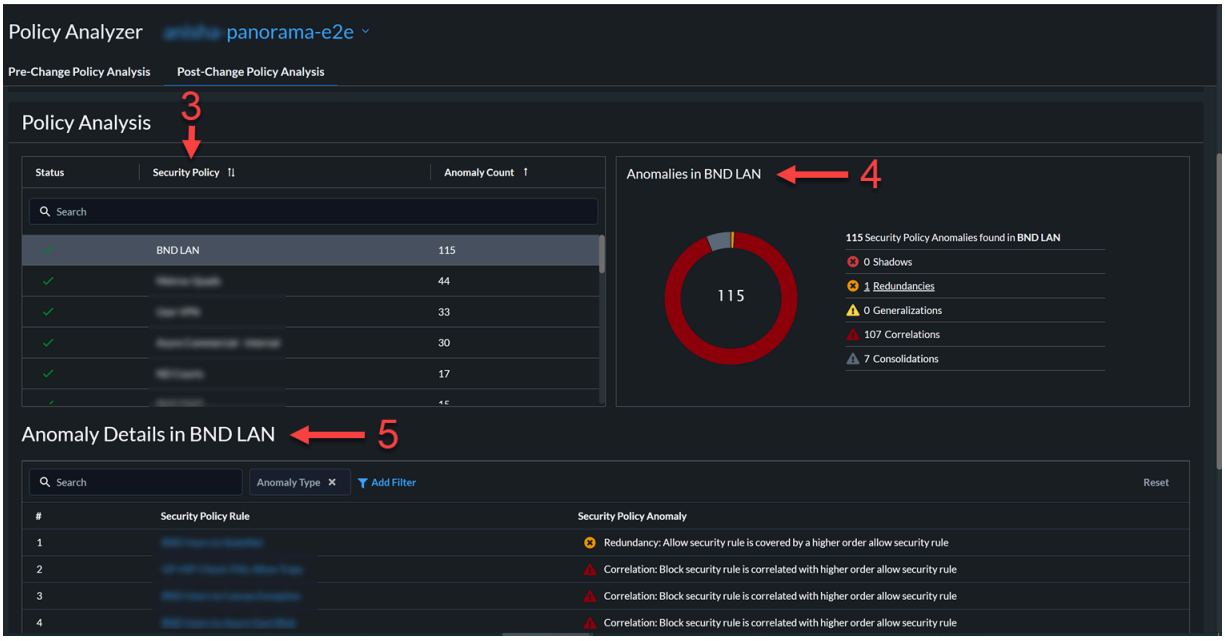
1. 显示所有策略集（即直接分配了 NGFW 的所有设备组）的分析摘要。可以查看异常或基于高优先级的异常。此报告中的值显示所有设备组中发现的异常的唯一数量。图表中的颜色表示不同类型的异常。



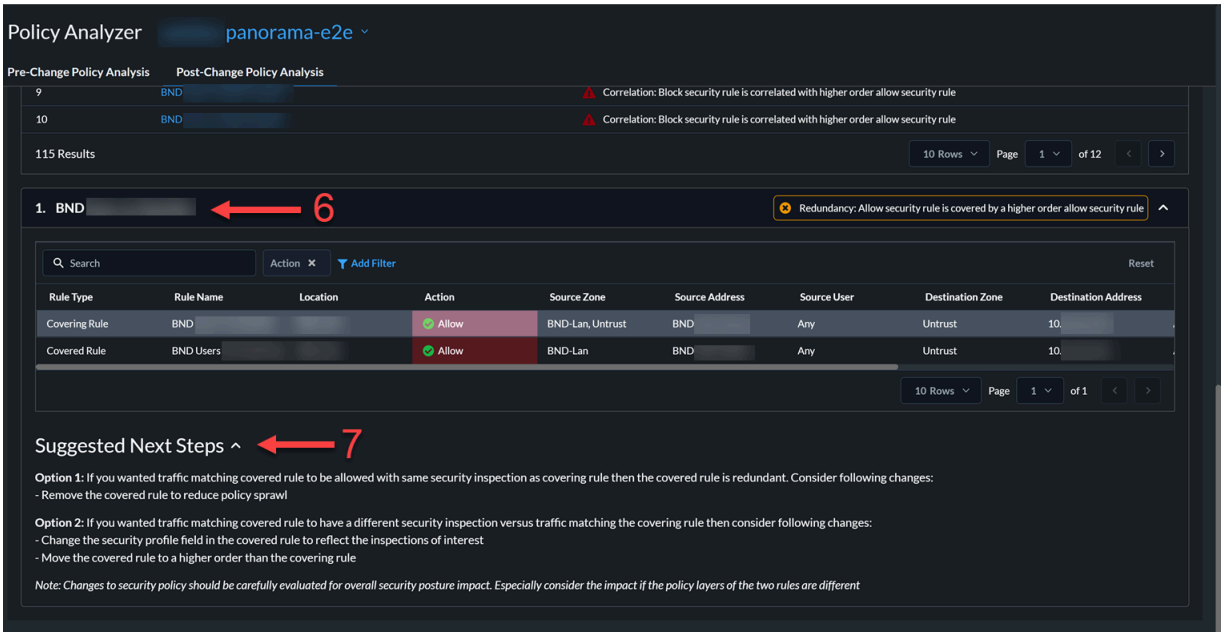
2. 分析的时间戳包括：
   - 现有安全策略快照 - 配置提交后标记为在 Panorama 中运行的时间戳。
   - 分析开始时间
   - 时间完成分析
   - 完成分析所需的时间
3. 查看安全策略的状态以及每项策略的异常数量。
4. 查看所选安全策略的异常细分。

 ©2025 Palo Alto Networks, Inc.

5. 查看安全策略中每个规则的异常详细信息。



6. 查看选定规则的属性和异常的详细信息。



该图显示了一个冗余异常示例。在此示例中，BND 规则已被另一个 BND 用户规则涵盖。因此，您可以移除 BND 规则。

7. 查看建议的后续步骤来补救异常。

 ©2025 Palo Alto Networks, Inc.

 ©2025 Palo Alto Networks, Inc.

NGFW 运行状况和软件管理

本章介绍如何管理 NGFW 运行状况和软件升级。

- 查看设备运行状况 - 查看根据已载入的 NGFW 的运行状况得分的部署的累积运行状况和性能。
- 升级建议 - 创建建议以确定可升级的设备的最佳软件版本。
- 分析指标容量 - 根据设备型号跟踪其指标使用情况，以此来分析和监视设备的资源容量。

查看设备运行状况

在何处可以使用？	需要提供什么？
• ，包括由 软件 NGFW 积分提供资助的项目	其中之一： ❑ 或 ❑ 或

设备运行状况仪表板根据已载入的 NGFW 的运行状况得分来显示部署的累积运行状况和性能。设备运行状况由运行状况分数的严重性（0 到 100）及其相应的运行状况等级（良好、一般、差、严重）确定。运行状况分数的计算依据包括开放警报的优先级、数量、类型和状态。

此指示板可帮助您：

- 查看历史运行状况评分数据，从而了解您在一段时间内所做的部署改进。
- 缩小在部署中需要注意的设备范围，并对问题进行优先排序以解决这些问题。

有关详细信息，请参阅指示板：设备运行状况。

 ©2025 Palo Alto Networks, Inc.

获取升级建议

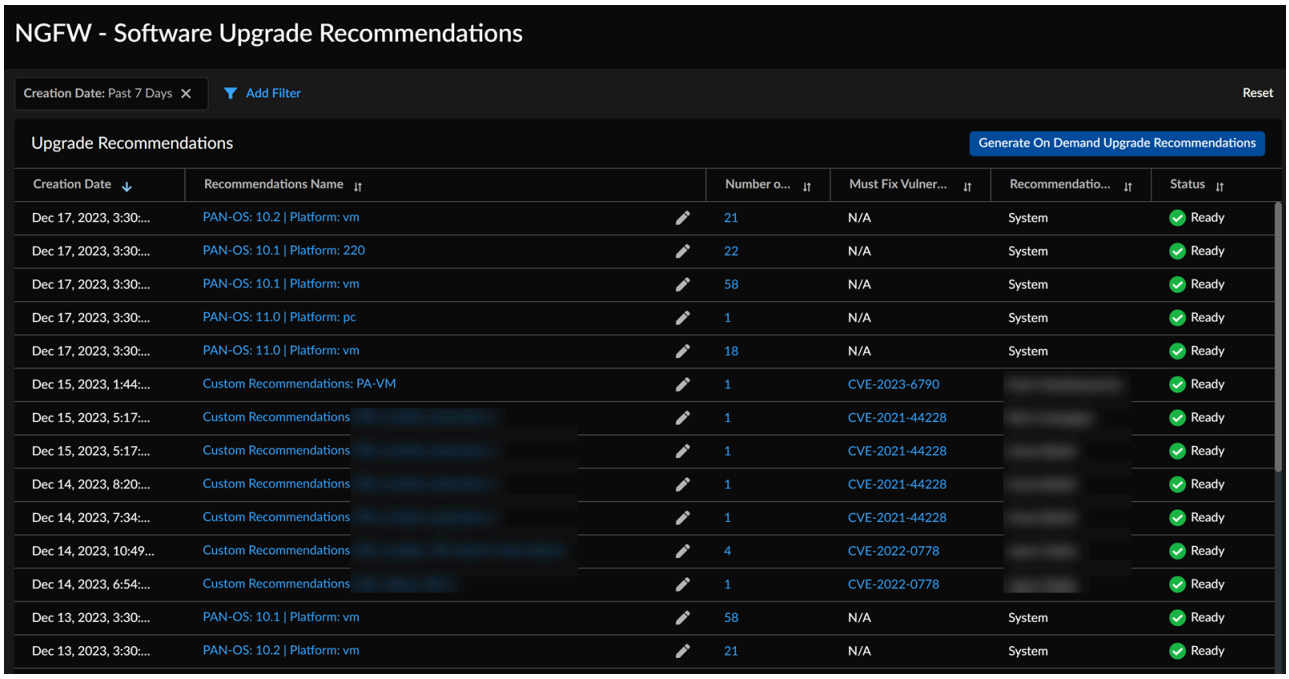
在何处可以使用？	需要提供什么？
• ，包括由 软件 NGFW 积分提供资助的项目	☐ 或

选择 **Workflows**（工作流） > **Software Upgrades**（软件升级） > **Upgrade Recommendations**（升级建议）以使用 Strata Cloud Manager 分析防火墙上启用的功能，并创建自定义建议来提供您的网络的具体信息。

- 要在您的设备上运行的最佳软件版本。
- 有关每个推荐软件版本中的新功能、行为更改、漏洞和软件问题的信息。

升级建议的类型：

- 由系统根据设备遥测数据生成的建议，每周生成两次。
- 用户生成的自定义建议，当您为特定 PAN-OS CVE 选择了设备时生成。
- 用户生成的建议，是由您通过上传防火墙的技术支持文件 (TSF)来生成的。



对于每个建议，可以执行以下任务。

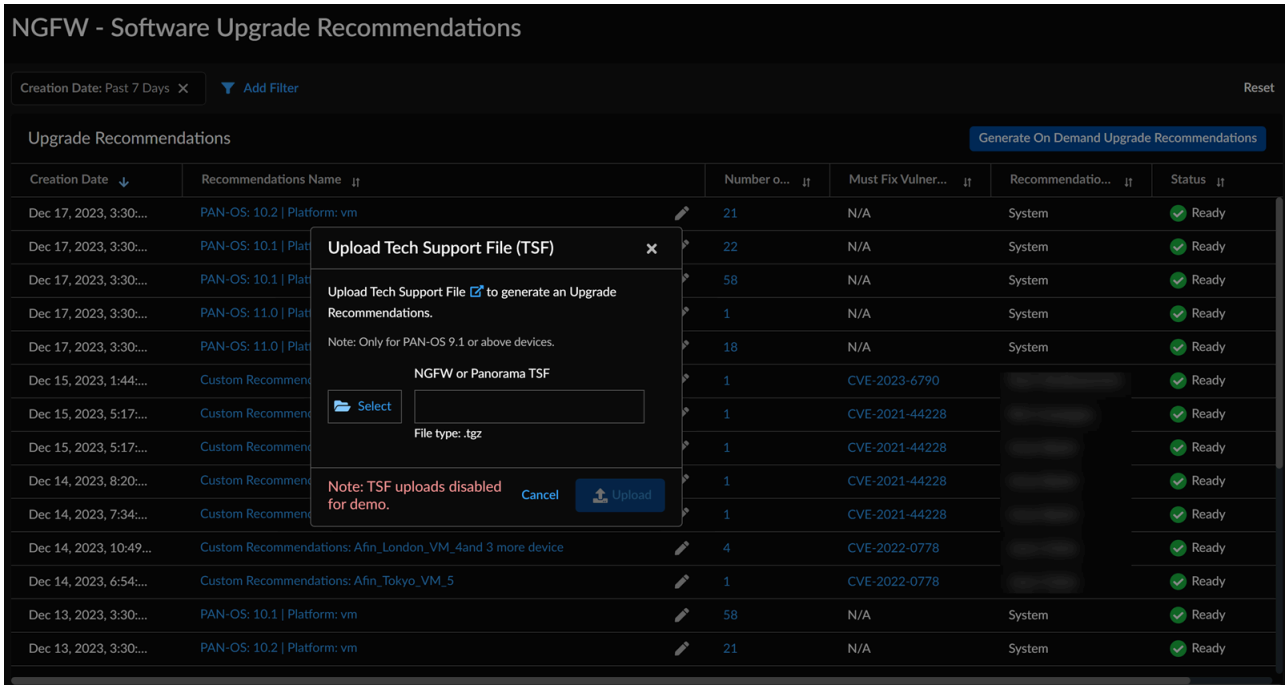
- 查看需要升级的设备数量以及需要解决的任何漏洞。
- 编辑建议的名称以区分自定义建议。
- 按创建日期、建议名称和建议生成者来过滤建议。
- 删除失败或不再适用的建议。

 ©2025 Palo Alto Networks, Inc.

生成按需升级建议

1. 生成按需升级建议。
2. 选择一个技术支持文件 (TSF) 并上传。

- 一次只能上传一台设备的 *TSF*，并且 *TSF* 必须为 *.tgz* 格式。
- 只能通过为防火墙生成的 *TSF* 来生成软件升级建议，而且只能从运行 *PAN-OS 9.1* 或更高 *PAN-OS* 版本的防火墙中升级。



3. 在状态为 Ready（就绪）后查看软件升级建议。

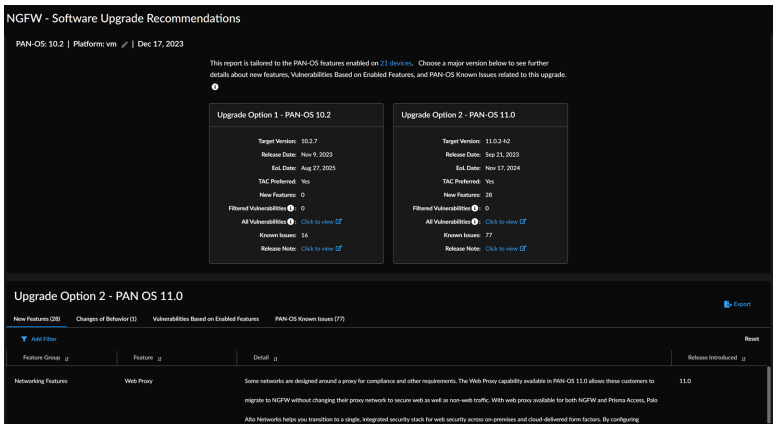
   还可以检查 Status（状态），以查看是否存在与 TSF 的上传、文件格式或处理相关的任何错误。

查看软件升级建议报告

单击建议可查看包含设备升级选项的详细报告。选择升级选项可查看有关新功能、行为变更、基于已启用功能的漏洞以及 **PAN-OS** 已知问题的详细信息。还可以用 CSV 格式导出该报告。

- 建议报告包括特定于设备上已启用功能的信息。
- 对于 ***PAN-OS*** 已知问题，*“Associated Case Count*（关联的案例数）*”* 表示报告问题的客户数量。

 ©2025 Palo Alto Networks, Inc.



 ©2025 Palo Alto Networks, Inc.

分析指标容量

在何处可以使用？	需要提供什么？
•	❑ 或

从 Strata Cloud Manager 导航到 **Monitor**（监视） > **Capacity Analyzer**（容量分析器），根据设备型号跟踪其指标使用情况，以此来分析和监视设备的资源容量。可以使用以下方法来分析指标：

- 根据指标、型号和设备分析指标容量
- 根据设备型号分析指标容量
- 根据指标分析指标容量

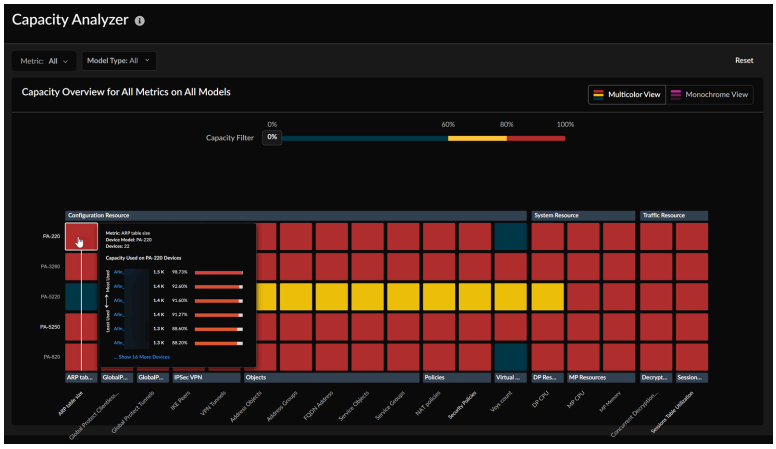
容量分析器已进行了增强，支持警报，可帮助您预测接近最大容量的资源消耗并发出警报。请参阅管理容量分析器警报。

VM-Series 防火墙不支持 ***Capacity Analyzer***（容量分析器）功能。

根据指标、型号和设备分析指标容量

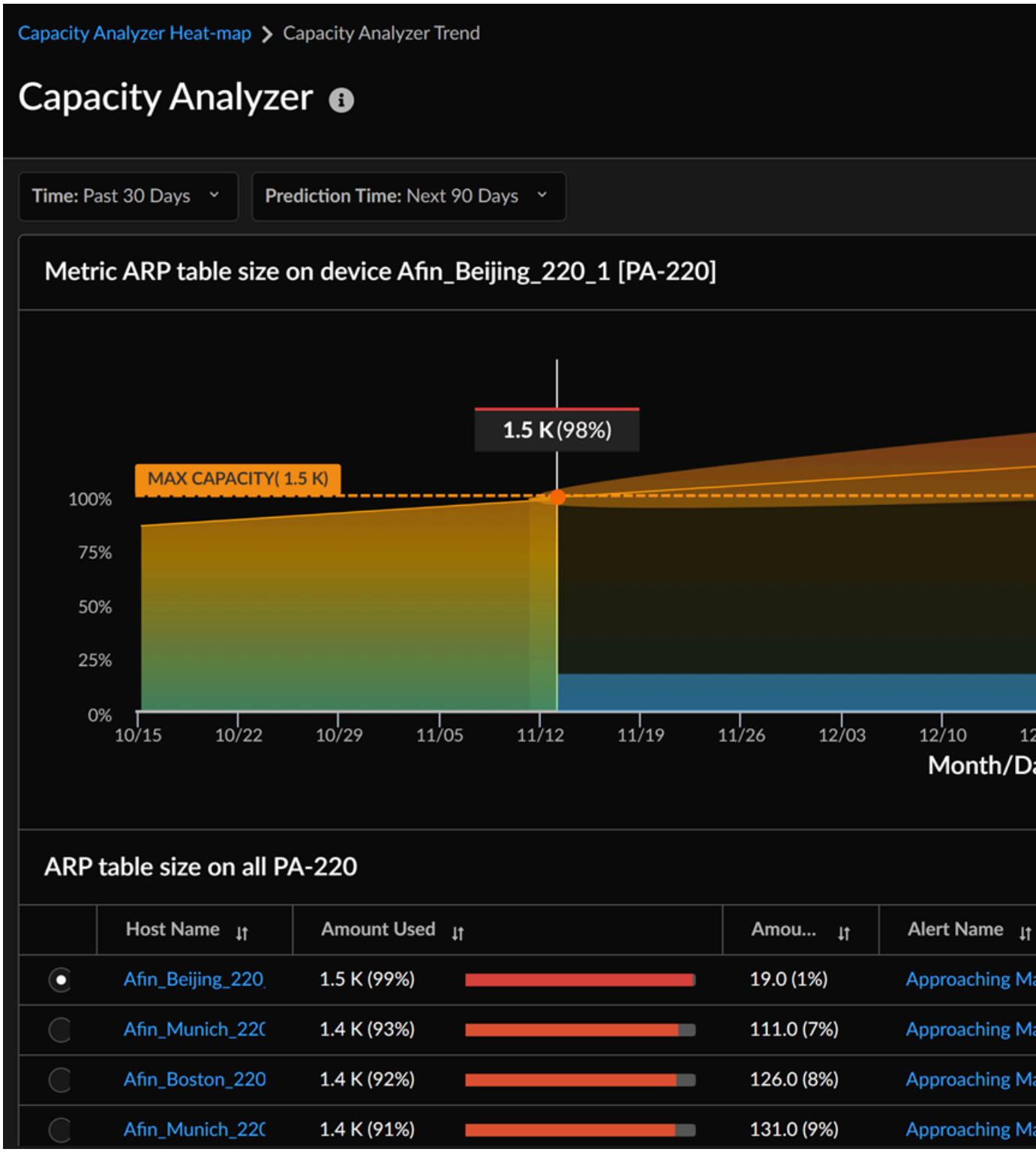
1. 在容量分析器热图上，将光标悬停在某个单元格上即可查看属于相应设备型号的所有设备的指标容量使用情况。

   在此示例中，弹出窗口显示属于 **PA-220** 型号的所有设备的 **ARP** 表大小指标容量。



 ©2025 Palo Alto Networks, Inc.

2. 单击与设备型号和指标对应的单元格即可查看容量使用情况。在此示例中，我们单击 **PA-220** 设备型号的 ARP 表大小。



可以查看以下内容：

- 所有属于 **PA-220** 型号的设备的 ARP 表大小指标容量。

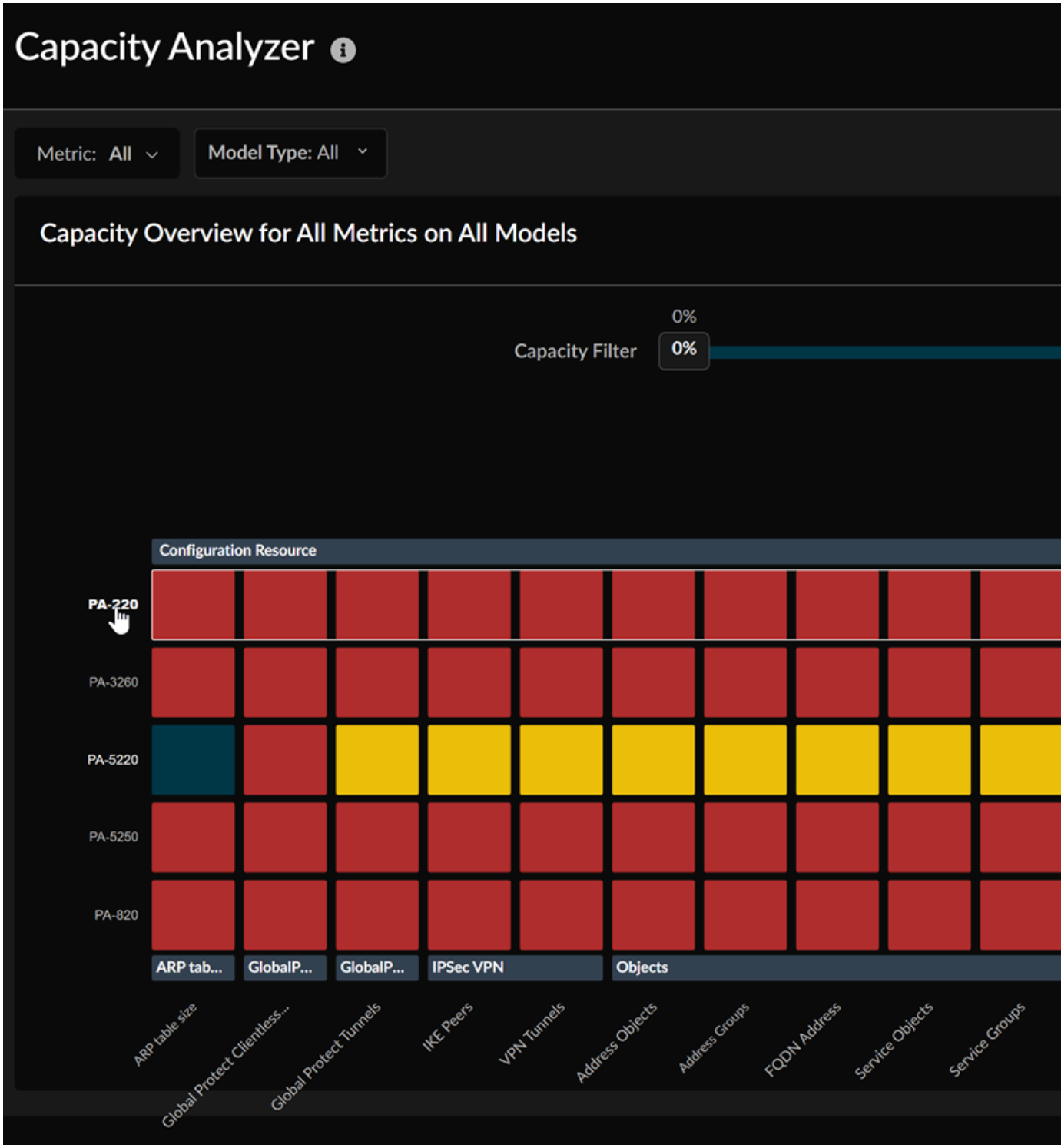
 ©2025 Palo Alto Networks, Inc.

- 选择其中一个主机名可查看指标容量趋势。
- 针对该指标发出的警报以及预计该指标达到其最大容量的日期。
- 该指标的预测趋势。Strata Cloud Manager 预测指标达到最大容量的日期。您可以将光标悬停在图表上，以查看任何特定时间点的指标容量。

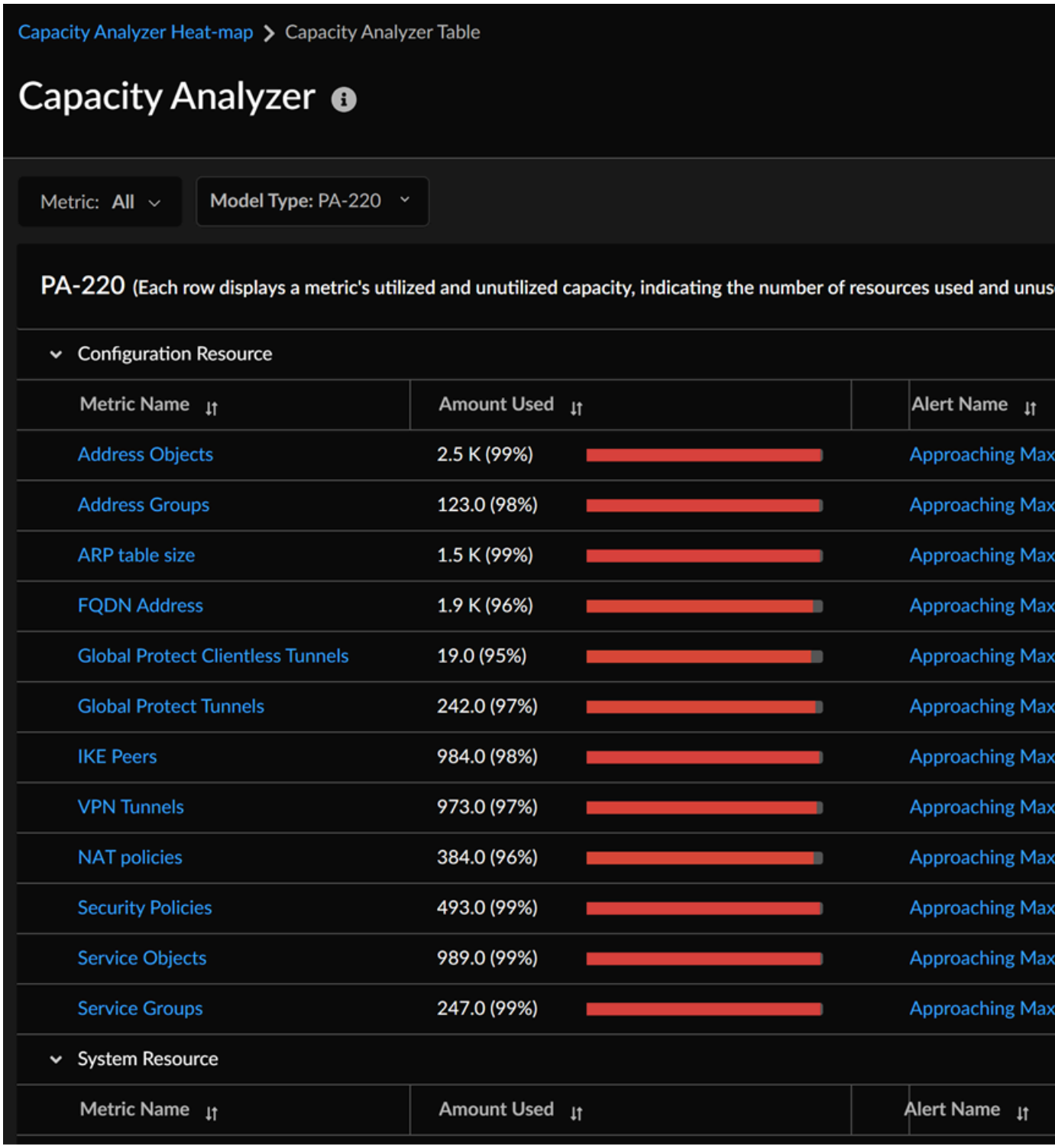
 ©2025 Palo Alto Networks, Inc.

根据设备型号分析指标容量

1. 从容量分析器热图中，选择一个设备信号以查看其所有关联指标。



 ©2025 Palo Alto Networks, Inc.



每行显示一个指标的利用容量，指示设备中该指标占用的资源数量。此外，您还可以查看针对该指标发出的警报以及该指标达到最大容量的预计日期。

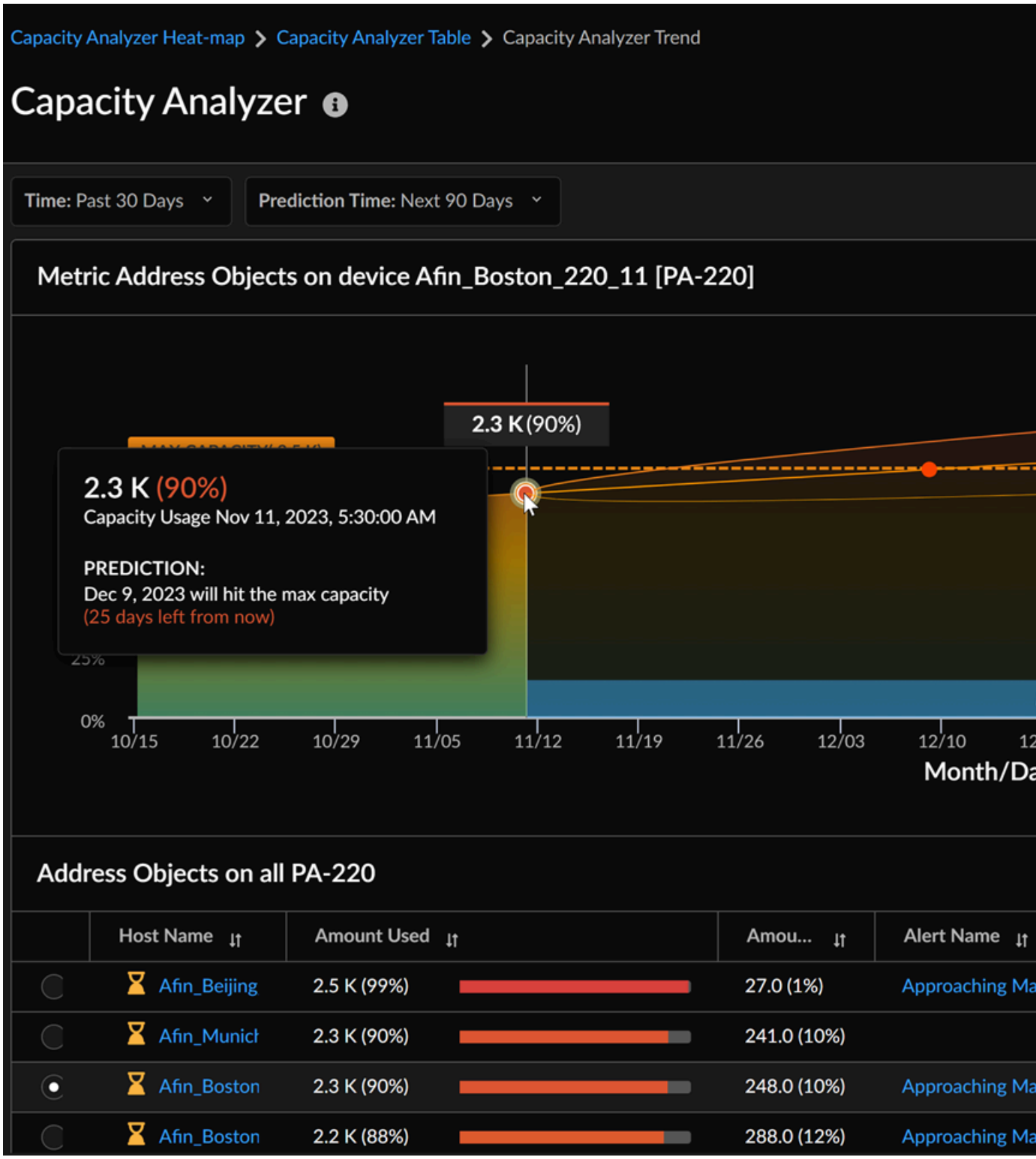
2. 在容量分析器表中，选择一个指标以查看其在设备上的趋势。

 ©2025 Palo Alto Networks, Inc.

3. 选择一个设备以查看其指标趋势。

   可以选择 **Prediction Time**（预测时间）以查看指标的预测趋势。Strata Cloud Manager 预测指标达到最大容量的日期。

   您可以将光标悬停在图表上，以查看任何特定时间点的指标容量。



 ©2025 Palo Alto Networks, Inc.

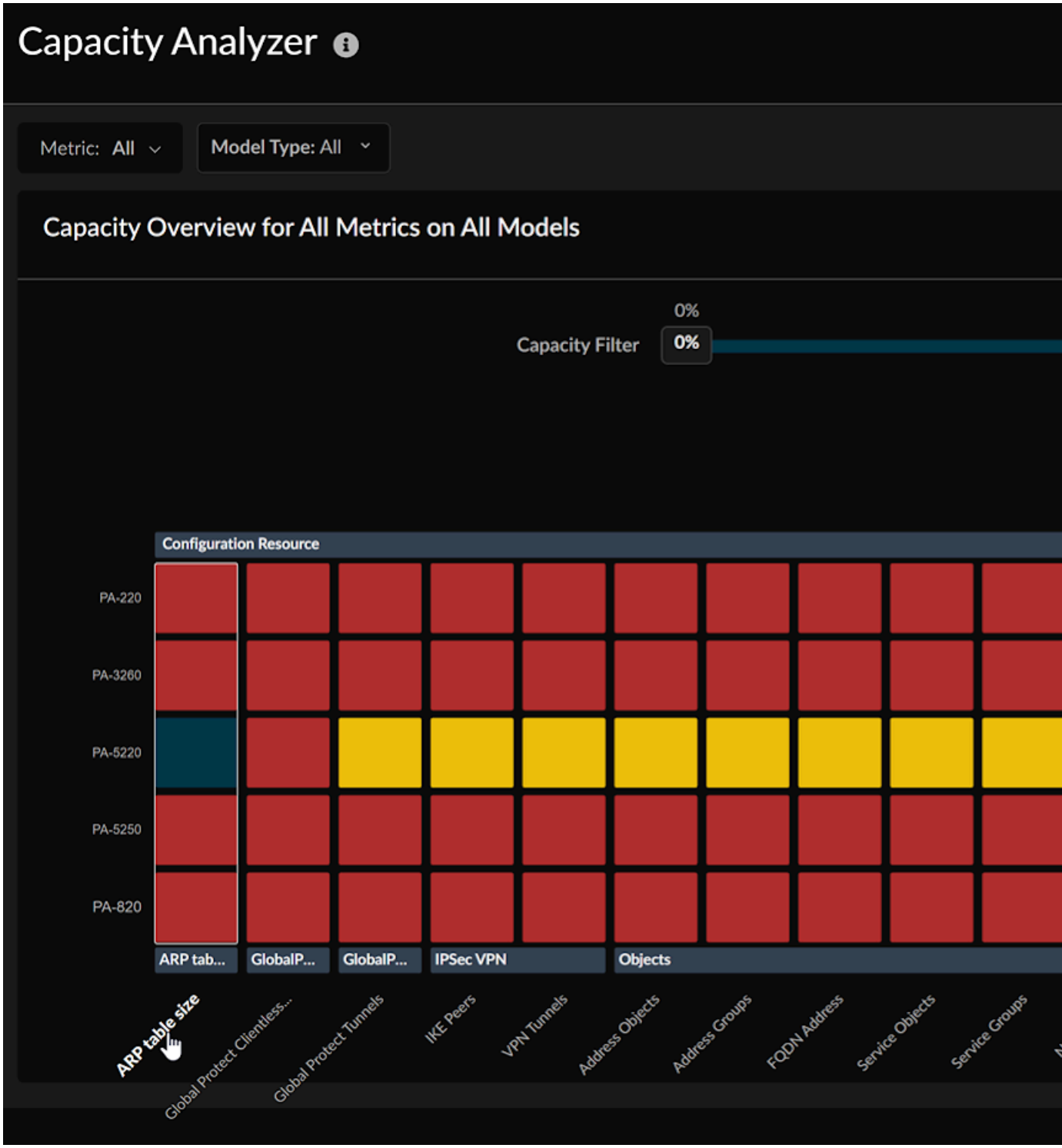
在 **Alert Name**（警报名称）下，可以查看针对与主机名对应的地址对象指标发出的警报。

 ©2025 Palo Alto Networks, Inc.

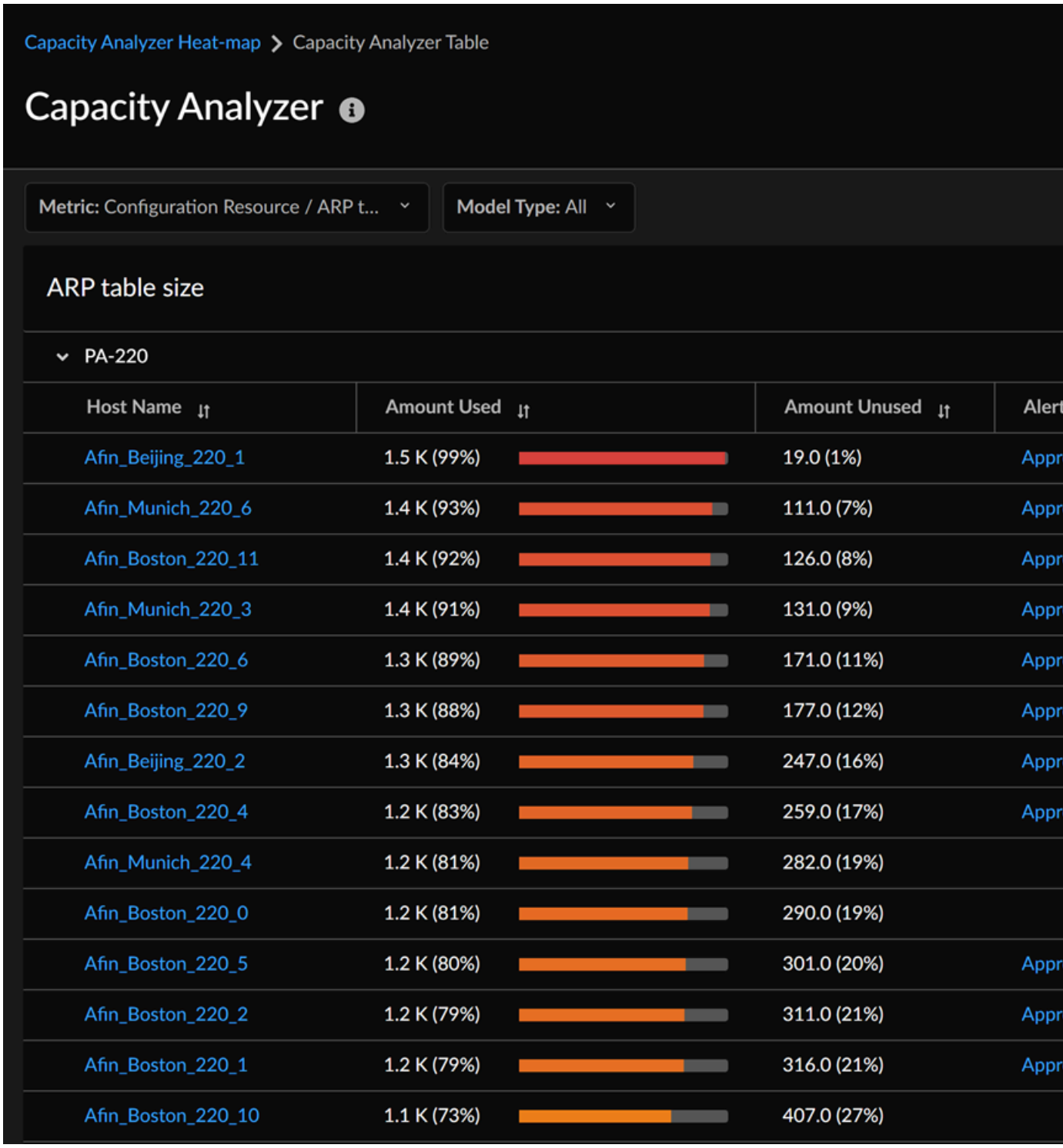
根据指标分析指标容量

1. 从容量分析器热图中，选择一个指标，以表格形式查看其在所有设备中的容量。在此示例中，选择了 **ARP** 表大小指标。

您还可以选择一种指标类型并向下钻取到某个指标，以表格形式查看其在所有设备中的容量。例如，配置资源类型指标 > 对象 > 地址对象。



 ©2025 Palo Alto Networks, Inc.

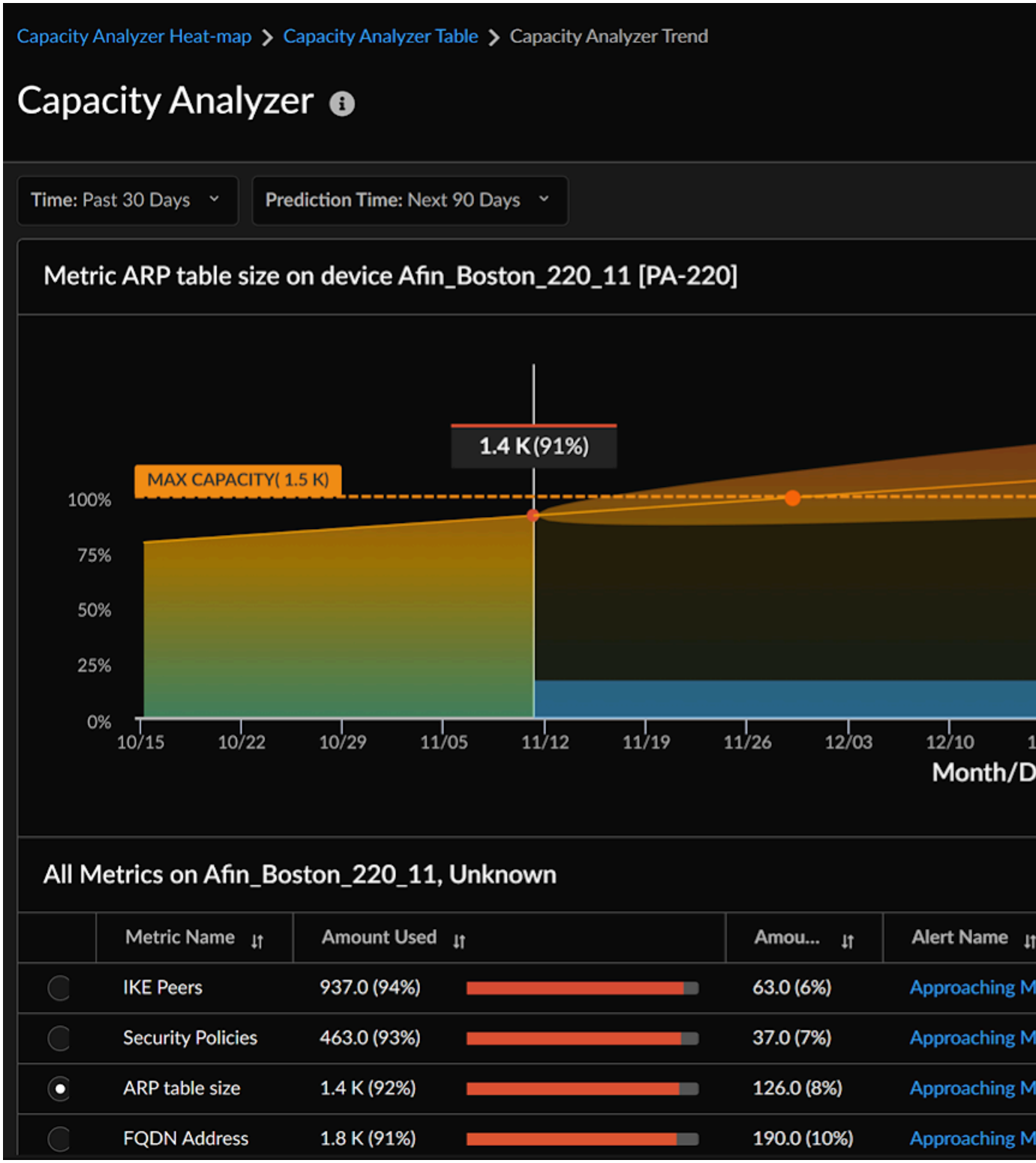


每行显示设备型号下每个主机的 **ARP** 表大小指标的已用和未用容量。此外，还可以查看针对每个主机针对该指标发出的警报以及该指标达到其最大容量的预计日期。

 ©2025 Palo Alto Networks, Inc.

2. 选择一个主机名以查看所选指标的图形趋势。

   可以选择 **Prediction Time**（预测时间）以查看指标的预测趋势。Strata Cloud Manager 预测指标达到最大容量的日期。



   您可以将光标悬停在图表上，以查看任何特定时间点的指标容量。

 ©2025 Palo Alto Networks, Inc.

 ©2025 Palo Alto Networks, Inc.

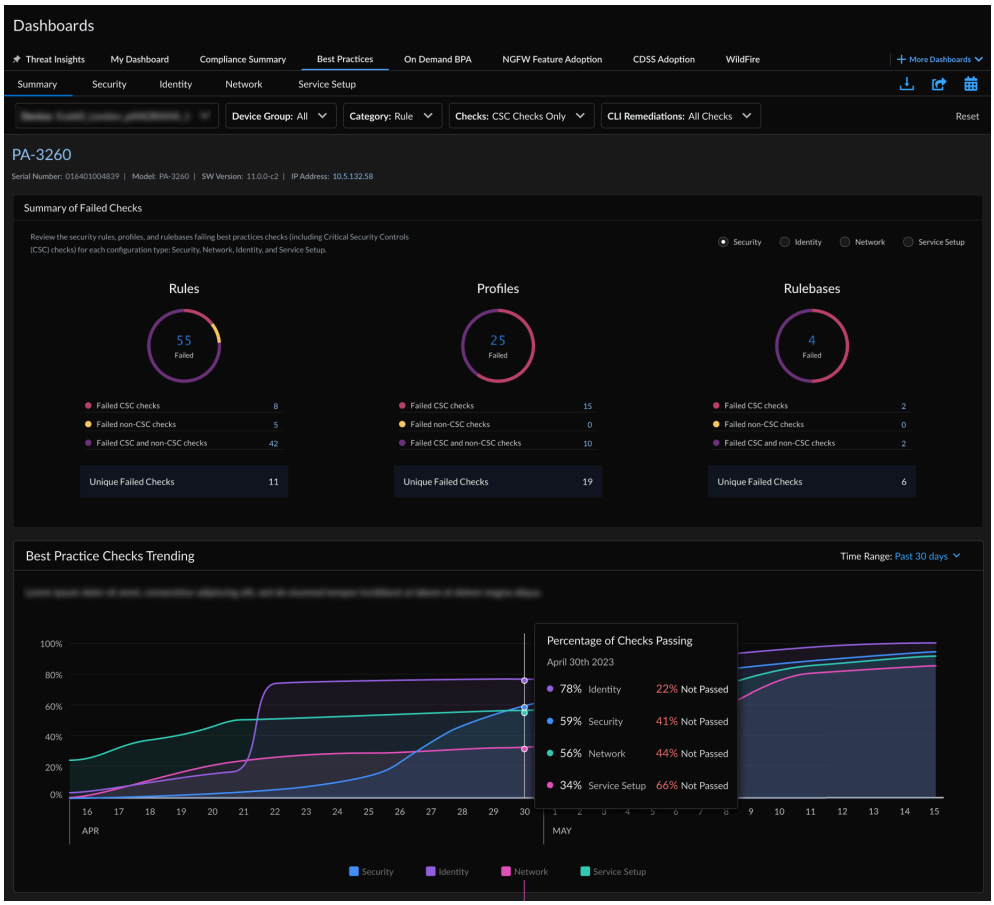
NGFW 的最佳实践

在何处可以使用？	需要提供什么？
• ，包括由 软件 NGFW 积分提供资助的项目	其中之一： ❑ 或 ❑ 或

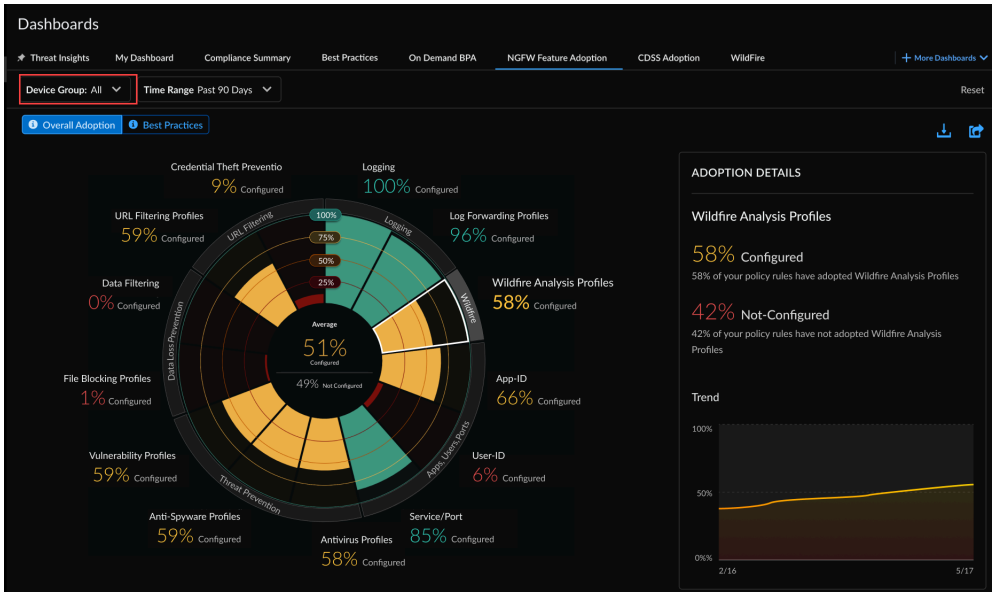
AIOps for NGFW 通过与最佳实践保持一致，帮助您加强安全态势。可以利用 AIOps for NGFW，根据最佳实践评估您的 Panorama、NGFW 和 Panorama 托管 Prisma Access 安全配置，并补救失败的最佳实践检查。AIOps for NGFW 简化了检查网络基础设施上信息安全合规性的流程。

AIOps for NGFW 是免费的，以下 AIOps 最佳实践评估 (BPA) 功能无需 AIOps 高级版许可证即可使用。有关可用最佳实践功能的完整列表，请参阅内置最佳实践：

- 检查每日最佳实践报告的最佳实践仪表板，以及它们与互联网安全中心的关键安全控制 (CSC) 检查的映射，以帮助您确定可以进行更改的区域，从而提高您的最佳实践合规性。以 PDF 格式共享最佳实践报告，并安排定期将其发送到您的收件箱。

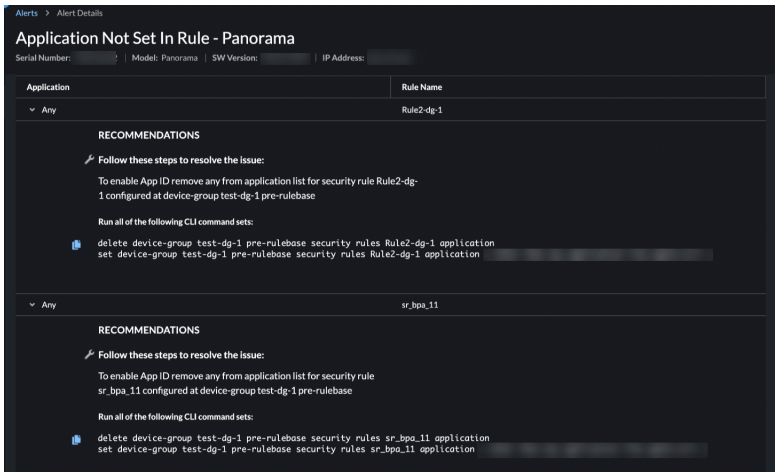


- 监视功能采用情况，并及时了解您在部署中使用的安全功能以及潜在的覆盖漏洞。



- 从 AIOps for NGFW 获取安全态势警报，以了解在什么情况下需要仔细查看您的安全设置。

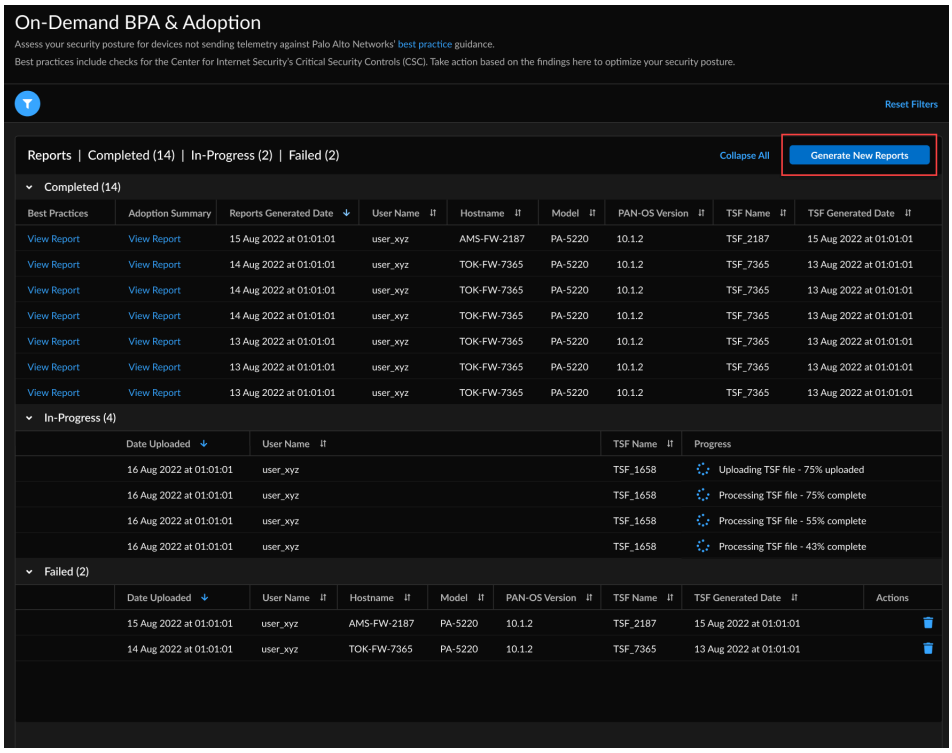
  在 **Alerts**（警报） > **Security**（安全） > **Alert Details**（警报详细信息）下的 AIOps for NGFW，还提供了命令行接口 (CLI) 修正。查看旨在帮助您修正触发警报的问题的建议。



安全警报和 *CLI* 修正仅适用于共享遥测的设备。对于运行 *9.1* 及更高版本的 *PAN-OS* 设备，此功能不支持手动上传技术支持文件 *(TSF)*。

 ©2025 Palo Alto Networks, Inc.

- 为运行 9.1 及更高版本的（非遥测）PAN-OS 设备生成 BPA 报告，现在包括功能采用指标。如果您一直在使用 BPA 独立工具来生成 BPA 报告，您可能会问自己："我是否仍可以从客户支持门户生成 BPA 报告？"我们也为您提供了这方面的信息。



通过高级版许可证，AIOps for NGFW 还提供了高级安全态势功能。高级版功能侧重于确保充分利用防火墙给出的结果并最大限度提高安全性。了解免费版和高级版许可证提供的功能。

 ©2025 Palo Alto Networks, Inc.

按需 BPA 报告

在何处可以使用？	需要提供什么？
• ，包括由 软件 NGFW 积分提供资助的项目	其中之一： ❑ 或 ❑ 或

现在，您可以直接从 Strata Cloud Manager 运行最佳实践评估 (BPA) 和功能采用摘要。只需上传技术支持文件 (TSF)。可以为未发送遥测数据或未载入到 AIOps for NGFW 的设备生成按需 BPA 报告。

BPA 根据 Palo Alto Networks 的最佳实践来评估您的安全态势，并确定设备的各种改进的优先级。安全最佳实践可防止已知和未知威胁，缩小攻击范围并提供流量可见性，从而可以了解和控制网络上的应用程序、用户以及内容。此外，最佳实践还包括检查互联网安全中心的关键安全控制 (CSC)。请参阅最佳实践指南以强化安全态势并实施改进。

我是否仍可以从客户支持门户生成 BPA 报告？

在 AIOps 出现之前，您是通过访问客户支持门户来访问和运行 BPA。现在，生成和下载 NGFW/Panorama 托管 Prisma Access 的最佳实践评估报告的首选方式是通过 AIOps。

2023 年 7 月 17 日之后，您将无法再从客户支持门户访问和运行 BPA。

STEP 1 | 转到中心，然后激活 AIOps for NGFW。免费。如果您不想在此时启用遥测的情况下载入设备，则可以在没有 Strata Logging Service 的情况下激活。

> 如果设备是在未启用 *Strata Logging Service* 或遥测的情况下载入的，则最佳实践指示板、安全警报和采用摘要功能不适用。

STEP 2 | 登录到已激活的 AIOps for NGFW 实例。即使没有 Strata Logging Service，也可以看到以下选项卡：

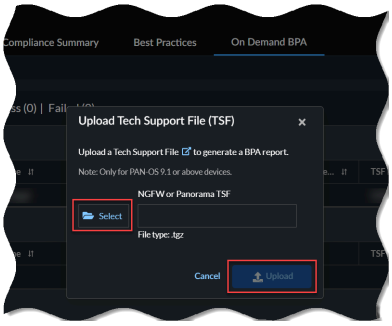
- 态势
- 活动
- 设置

STEP 3 | 转到 **Dashboards**（指示板） > **On Demand BPA**（按需 **BPA**）。

STEP 4 | 生成新的 **BPA** 报告。

 ©2025 Palo Alto Networks, Inc.

STEP 5 | 选择 **TSF** 和上传 **TSF** 文件。



上传时间取决于 .tgz 文件大小和互联网速度。如果文件较大，上传文件可能需要几分钟时间。展开 **In-Progress**（进行中）可查看 TSF 文件的状态。

- 按需 *BPA* 仅支持 *.tgz* 文件格式的技术支持文件 *(TSF)*。
- 按需 *BPA* 支持使用 *PAN-OS* 版本为 *9.1* 或更高版本的设备提供的 *TSF* 来生成报告。

STEP 6 | 在处理完 TSF 后，在 **Completed**（已完成）下面选择 **View Report**（查看报告），以从您的设备查看生成的 BPA 报告。

 ©2025 Palo Alto Networks, Inc.

最佳实践

在何处可以使用？	需要提供什么？
• •	❑ 或 ❑ 许可证 ❑ 在设备上启用遥测共享

这个指示板显示哪些内容？

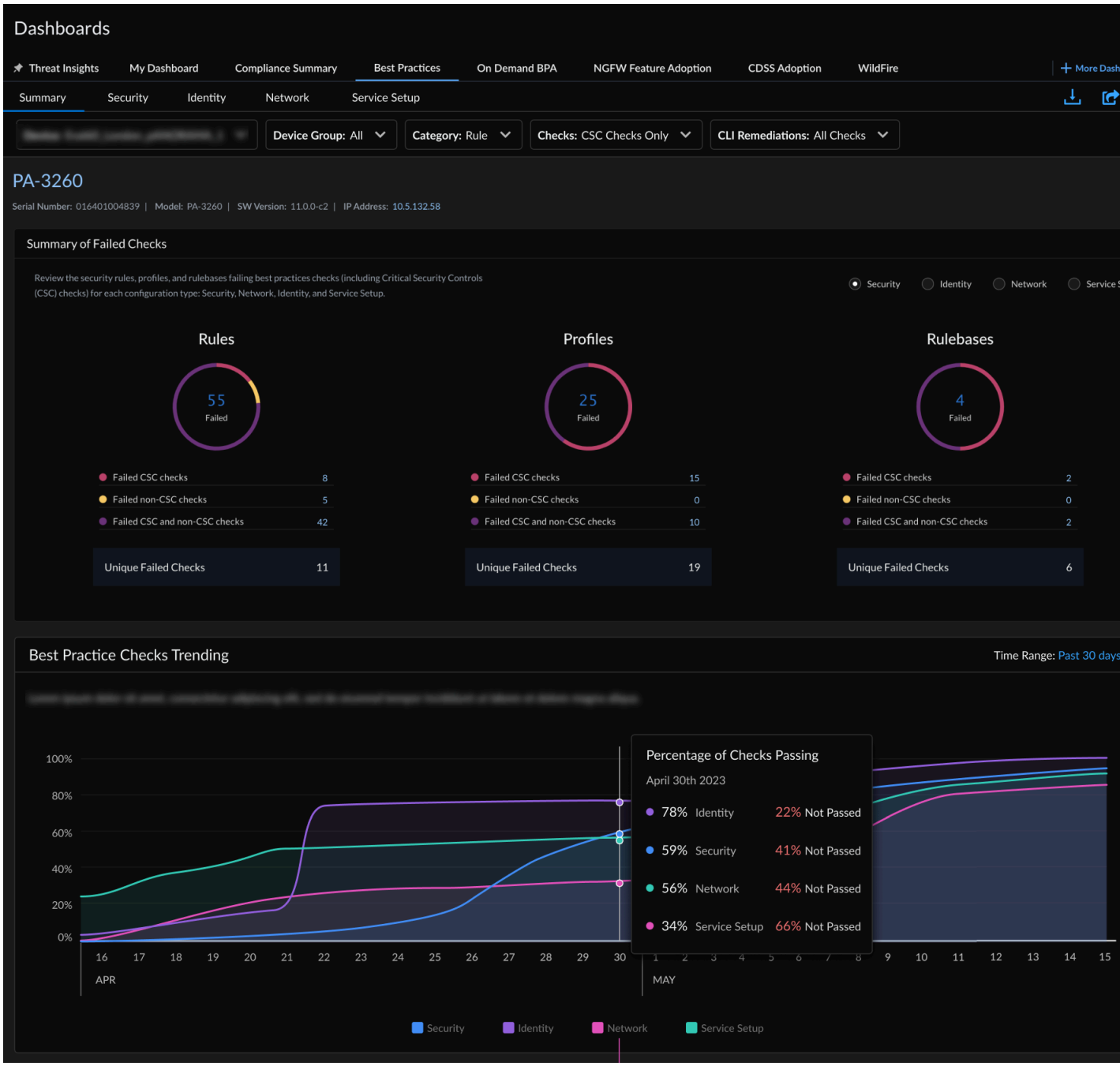
指示板显示与您的租户关联的每个 *Prisma Access* 和 *NGFW/Panorama* 的聚合数据。

导航到**Strata Cloud Manager** > **Dashboards**（指示板） > **More Dashboards**（更多指示板） > **Best Practices**（最佳实践）指示板，根据 Palo Alto Networks 的最佳实践指南衡量您的安全态势。重要的是，最佳实践评估包括对互联网安全中心关键安全控制 (CSC) 的检查。CSC 检查与其他最佳实践检查是分开进行，因此您可以轻松挑选并优先安排能让您实现 CSC 合规性的更新。

如何使用指示板中的数据？

虽然最佳实践指导旨在帮助您加强安全态势，但本报告中的调查结果还可以帮助您确定有哪些领域需要改进，以更有效地管理环境。

 ©2025 Palo Alto Networks, Inc.



最佳实践指示板分为五个部分：

- 摘要

  提供跨配置类型（安全、网络、身份和服务设置）的设备所有失败检查的综合视图，查看 BPA 检查的历史趋势图，并评估关键功能领域的最佳实践采用率。

 ©2025 Palo Alto Networks, Inc.

- 安全

  显示选定设备和位置中未能通过最佳实践和 CSC 检查的规则、规则库或配置文件。如果可用，CLI 修正允许您解决策略规则的问题。CLI 修正是使用您在生成 按需 BPA 报告 时上传的 TSF 数据生成的。

  - 规则库

    查看策略的组织方式，以及跨多个规则应用的配置设置是否符合最佳实践（包括 CSC 检查）。

  - 规则

    显示未通过最佳实践和 CSC 检查的规则。查看您可以在哪里采取快速操作来修复失败的检查。规则是根据会话计数排序的，因此您可以线查看和更新影响最大流量的规则。

  - 配置文件

    向您展示您的配置文件与最佳实践（包括 CSC 检查）之间的差距。配置文件可对与安全或解密规则匹配的通信执行高级检查。

- 标识

  显示设备的身份验证强制设置（身份验证规则、身份验证配置文件和身份验证门户）是否满足最佳做法并符合 CSC 检查。

- 网络

  检查应用程序覆盖规则和网络设置是否符合最佳实践和 CSC 检查。

- 服务设置

  查看设备上启用的订阅与最佳实践和 CSC 检查结果之间的匹配程度。可以在此处查看 WildFire 设置、GlobalProtect 门户和 GlobalProtect 网关配置，还可修复失败的检查。

 ©2025 Palo Alto Networks, Inc.

共享、下载和计划指示板的报告

您可以下载、共享和计划这些报告，其内容涵盖了指示板以 *PDF* 和 *.CSV* 格式显示的数据以及以 *.txt* 格式显示的 *CLI* 修正。这些图标位于指示板右上角：

 ©2025 Palo Alto Networks, Inc.

 ©2025 Palo Alto Networks, Inc.