paloalto TECHDOCS

Advanced WildFire 管理

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

Last Revised

April 8, 2025

Table of Contents

Advanced WildFire 概述

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Advanced WildFire 许可证 对于 *Prisma Access*，凭借 *Prisma Access* 许可证，这通常会包含在内。

Advanced WildFire™ 结合使用动态/静态分析和智能运行时内存分析来检测和预防零日恶意软件，以检测高度规避性威胁，并创建保护措施来阻止恶意软件。

Advanced WildFire 分析环境识别之前未知的恶意软件，并生成签名以便 Palo Alto Networks 防火墙用于检测和阻止恶意软件。当 Palo Alto Networks 防火墙检测到未知样本时，防火墙会自动将所有支持的文件类型从任何应用程序转发到 WildFire 公共云服务，以进行 Advanced WildFire 分析。根据样本在沙箱中分析和执行时显示的属性、行为和活动，Advanced WildFire 将样本确定为良性、灰色软件、网络钓鱼或恶意样本，然后生成签名以识别新发现的恶意软件，并在全球范围内提供最新的签名以供实时检索。然后，所有 Palo Alto Networks 防火墙都可以将传入的样本与这些签名进行比较，从而自动阻止首先由单个防火墙检测到的恶意软件。

要了解有关 Advanced WildFire 的更多信息或开始使用，请参阅以下主题：

- 参阅 Advanced WildFire 概念，了解更多关于您可以提交以进行 Advanced WildFire 分析、WildFire 判定和 WildFire 签名的样本类型。
- 进一步了解您可以通过防火墙设置的 Advanced WildFire 部署。您可以提交您希望分析的样本至 Palo Alto Networks 主机 WildFire 云、本地主机 WildFire 专有云，或您可以使用混合云，让防火墙提交特定样本至公共云或专有云。
- 开始使用 Advanced WildFire 用于定义您想要提交进行分析的样本，并开始提交样本至 WildFire 云。
- 如果您正在部署 WildFire 设备，请参阅 WildFire 设备管理。

订阅选项

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Advanced WildFire 许可证 对于 *Prisma Access*，凭借 *Prisma Access* 许可证，这通常会包含在内。

WildFire 基本服务作为 Palo Alto Networks 下一代防火墙的一部分包含在呢，且不需要 Advanced WildFire 订阅。凭借 WildFire 基本服务，防火墙可转发可移植的可执行文件 (PE) 进行 Advanced WildFire 分析，且可以检索只包含防病毒软件和/或威胁防护更新（每 24-48 小时提供）的 Advanced WildFire 签名。

Palo Alto Networks 提供多种订阅选项：

- **WildFire** — WildFire 订阅通过将样本转发到 Advanced WildFire 云来提供对恶意软件的保护，在该云中，一系列分析环境用于通过生成阻止更多威胁实例的保护来检测和防止未知的恶意软件威胁。作为订阅的一部分，您可以定期访问 Advanced WildFire 签名更新、高级文件类型转发以及使用 WildFire API 上传文件。如果您运行的环境需要本地解决方案，则可以使用 WildFire 订阅将文件转发到本地 WildFire 设备。
- **Advanced WildFire** — （PAN-OS 10.0 及更高版本）Advanced WildFire 订阅包含标准 WildFire 订阅中的所有功能，并通过基于云的高级探测器提供样本分析对其进行了改进。高级检测系统使用智能实时运行时内存分析、运行时 DLL 仿真、自动解包、系列分类、隐身观察和其他技术来分析样本，以锁定高度规避性恶意软件。
- 独立版 **WildFire API** — 使用 SOAR 工具、自定义安全应用程序和其他威胁评估软件的 Palo Alto Networks 客户可以通过仅提供 API 访问权限的独立订阅来访问 WildFire 云的高级文件分析功能。这使您可以利用基于 WildFire 的分析，而不必依赖 Palo Alto Networks 防火墙作为转发机制。WildFire 独立 API 订阅允许您直接查询 WildFire 云威胁数据库以获取有关潜在恶意内容的信息，并根据组织的特定要求，使用 WildFire 的高级威胁分析功能提交文件进行分析。订阅的增强访问限制允许各种规模的组织根据其使用情况自定义访问限制 — 这包括允许特定数量的文件/报告查询、样本提交（用于 Advanced WildFire 分析）或两者结合的可扩展许可证。有关更多信息，请参阅 WildFire API 参考。

标准的 WildFire 订阅可解锁以下功能：

- 实时更新 — （PAN-OS 10.0 及更高版本）只要Advanced WildFire 公有云生成新发现的恶意软件的Advanced WildFire 签名，防火墙就可以检索这些签名。样本检查期间下载的签名将被保存在防火墙缓存中，可用于快速（本地）查找。此外，为扩大覆盖范围，防火墙还可在启用实时签

名后，定期自动下载签名数据包。这些补充签名将被添加到防火墙缓存中，且一直可用，直至签名失效，被刷新或被新签名覆盖。推荐使用实时 Advanced WildFire 更新这一最佳实践设置。

选择**Device**（设备） > **Dynamic Update**（动态更新）并启用防火墙以实时获取最新的 Advanced WildFire 签名。

- 五分钟更新 — （所有 PAN-OS 版本）Advanced WildFire 公有云可以针对新发现的恶意软件每五分钟生成并分发 Advanced WildFire 签名，您可以设置防火墙每分钟检索并安装这些签名（使防火墙可在一分钟可用性范围内获取最新签名）。

  如果您使用的是 *PAN-OS 10.0* 或更高版本，则最好是使用实时 *Advanced WildFire* 更新，而不是计划重复更新。

  选择 **Device**（设备） > **Dynamic Update**（动态更新）以启用防火墙获取最新的 Advanced WildFire 签名。根据您的 Advanced WildFire 部署，您可以设置以下签名数据包更新的一个或两个都设置：

  - **WildFire** — 从 WildFire 公共云获取最新签名。
  - **WF-Private** — 从设置为本地生成签名和 URL 类别的 WildFire 设备获取最新签名。

- **Advanced WildFire** 内联机器学习 —（PAN-OS 10.0 及更高版本）在防火墙数据平面使用机器学习 (ML)，实时防止可迁移可执行文件、可执行链接格式 (ELF) 文件和 PowerShell 脚本的恶意软件变体进入您的网络。借助在防火墙上使用的 Advanced WildFire 云分析技术，Advanced WildFire 内联机器学习 可通过评估不同文件的详细信息（包括解码器字段和模式），动态检测特定类型的恶意文件，从而实现文件的高分类率。这种保护可扩展至当前已知以及未来可能会发生变化、与 Palo Alto Networks 识别为恶意的特征相匹配的威胁。Advanced WildFire inline 机器学习将执行您现有的防病毒配置文件保护配置。此外，您还可以指定文件哈希例外以排除遇到的误报情况，这能使您创建更加精确的规则，从而支持您特定的安全需求。
- 文件类型支持 — 除了 PE，还可转发高级文件类型进行 Advanced WildFire 分析，包括 APK、Flash 文件、PDF、Microsoft Office 文件、Java Applet、Java 文件（jar 和 .class）以及 HTTP/HTTPS 电子邮件链接的高级文件类型转发包含在 SMTP 和 POP3 电子邮件消息内。（WildFire 专有云分析不支持 APK、Mac OS X、Linux (ELF)、压缩 (RAR/7-Zip) 和脚本（JS、BAT、VBS、Shell 脚本、PS1 和 HTA）文件）。
- **Advanced WildFire API** — 访问 WildFire API，促成对 Advanced WildFire 公共云或 WildFire 私有云的直接编程访问。使用 API 提交文件进行分析，并检索后续的 Advanced WildFire 分析报告。根据 Advanced WildFire 订阅，您每天最多可以执行 150 次样本提交和最多 1,050 次样本查询。每日样本提交次数限制可以根据贵组织的特定需求扩展。详细信息，请联系您的 Palo Alto Networks 销售代表。
- **WildFire** 私有云和混合云支持 — 转发文件以进行 Advanced WildFire 分析。WildFire 专有云和 WildFire 混合云部署都要求防火墙能够提交样本至 WildFire 设备。启用 WildFire 设备仅需一份支持许可证。

如果您已购买 Advanced WildFire 订阅，则必须先激活许可证才能使用需订阅才能使用的 WildFire 功能。

Advanced WildFire 订阅可解锁以下功能：

- 智能运行时内存分析 — 智能运行时内存分析是一种基于云的高级分析引擎，可补充静态和动态分析引擎，用于检测和防止规避性恶意软件威胁。高级威胁使用的这些规避技术包括但不限于使用隐身策略的恶意软件，显示使用复杂工具创建的定制设计/短暂行为的迹象，并表现出快速传播的品质。通过利用基于云的检测基础架构，内省分析探测器可以运行各种检测机制，这些机制可以自动更新和部署，而无需用户下载内容更新包或运行资源密集型、基于设备的分析器。基于机器学习的数据集持续监控和更新基于机器学习的数据集，这些数据集用于分析 Advanced WildFire 样本，并得到 Palo Alto Networks 威胁研究人员的额外支持，他们为高度准确的检测增强提供人为干预。

  智能运行时内存分析依赖于现有的 Advanced WildFire 分析配置文件设置，不需要任何其他配置；但是，您必须拥有有效的 Advanced WildFire 许可证。显示或以其他方式表明规避和/或高级恶意软件特性的样本会自动转发到相应的分析环境。

Advanced WildFire 概念

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Advanced WildFire 许可证 对于 *Prisma Access*，凭借 *Prisma Access* 许可证，这通常会包含在内。

- 样本
- 防火墙转发
- 会话信息共享
- 分析环境
- Advanced WildFire Inline Cloud Analysis
- Advanced WildFire 内联机器学习
- 判定结果
- 文件分析
- 电子邮件链接分析
- URL 分析
- 压缩和编码文件分析
- Advanced WildFire 签名
- Advanced Wildfire 示例

样本

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Advanced WildFire 许可证 对于 *Prisma Access*，凭借 *Prisma Access* 许可证，这通常会包含在内。

在何处可以使用？	需要提供什么？
• VM-SERIES • CN-Series	

样本是指从防火墙和公共 API 提交供 Advanced WildFire 分析的所有文件类型和电子邮件链接。有关防火墙可提交进行 Advanced WildFire 分析的文件类型和链接的详细信息，请参阅 文件分析和 电子邮件链接分析。

防火墙转发

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Advanced WildFire 许可证 对于 *Prisma Access*，凭借 *Prisma Access* 许可证，这通常会包含在内。

防火墙根据已配置的 Advanced WildFire 分析配置文件设置（**Objects**（对象） > **Security Profiles**（安全配置文件） > **WildFire Analysis**（**WildFire** 分析））转发未知样本和符合防病毒签名而被阻止的文件。除了检测电子邮件中包含的链接、电子邮件中的附件文件以及基于浏览器的下载文件，防火墙还可利用 App-ID 检测应用程序内的文件传输。对于防火墙检测的样本，防火墙分析样本结构和内容，并将其与现有签名对比。如果样本符合签名，防火墙应用针对该签名定义的操作（允许、警报或阻挡）。如果该样本符合防病毒签名，或如果该样本在与 Advanced WildFire 签名比较后仍然未知，则防火墙转发该样本进行 Advanced WildFire 分析。

默认情况下，防火墙检测会话中未知样本时，还会转发该会话的相关信息。要管理防火墙转发会话的信息，选择 **Device**（设备） > **Setup**（设置） > **WildFire** 并编辑会话信息设置。

会话信息共享

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Advanced WildFire 许可证 对于 *Prisma Access*，凭借 *Prisma Access* 许可证，这通常会包含在内。

在何处可以使用？	需要提供什么？
• VM-SERIES • CN-Series	

除了转发未知和阻挡的样本进行分析外，防火墙还转发关于样本的网络会话信息。Palo Alto Networks 使用会话信息以了解可以网络事件的内容，与恶意软件相关破坏的指示、受影响的主机和客户端，以及用于传播恶意软件的应用程序。

默认情况下启用会话信息转发；但是，您可以调整默认设置，并选择将会话信息转发到其中一个 WildFire 云选项的类型。

- Strata Cloud Manager
- PAN-OS 和 Panorama

会话信息共享 (Cloud Management)

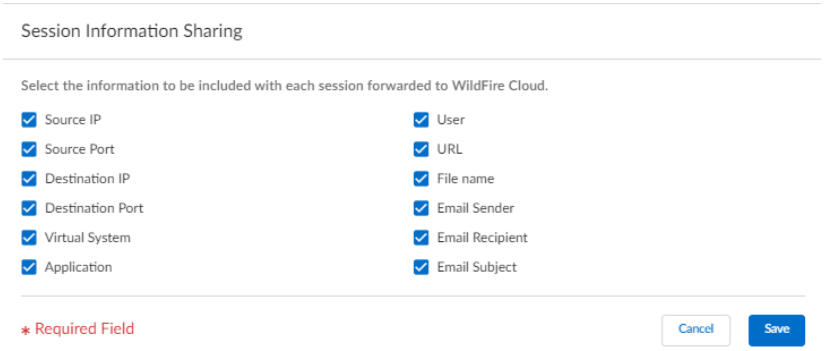
如果您使用 ***Panorama*** 来管理 ***Prisma Access***：

切换到 ***PAN-OS*** 选项卡并遵循相应的指导。

如果你使用 ***Prisma Access*** 云管理，请在这里继续。

STEP 1 | 使用与 Palo Alto Networks 支持帐户关联的凭据，登录到中心上的 Strata Cloud Manager 应用程序。

STEP 2 | 选择 **Manage**（管理） > **Configuration**（配置） > **NGFW** 和 **Prisma Access** > **Security Services**（安全服务） > **WildFire and Antivirus**（**WildFire** 和 **Antivirus**），然后配置 **Session Information Settings**（会话信息设置）选项。



- **Source IP**（源 **IP**）— 转发发送未知文件的源 IP 地址。
- **Source Port**（源端口）— 转发发送未知文件的源端口。
- **Destination IP**（目标 **IP**）— 转发未知文件的目标 IP 地址。
- **Destination Port**（目标端口）— 转发未知文件的目标端口。
- **Virtual System**（虚拟系统）— 转发检测未知文件的虚拟系统。
- **Application**（应用程序）— 转发传输未知文件的用户应用程序。

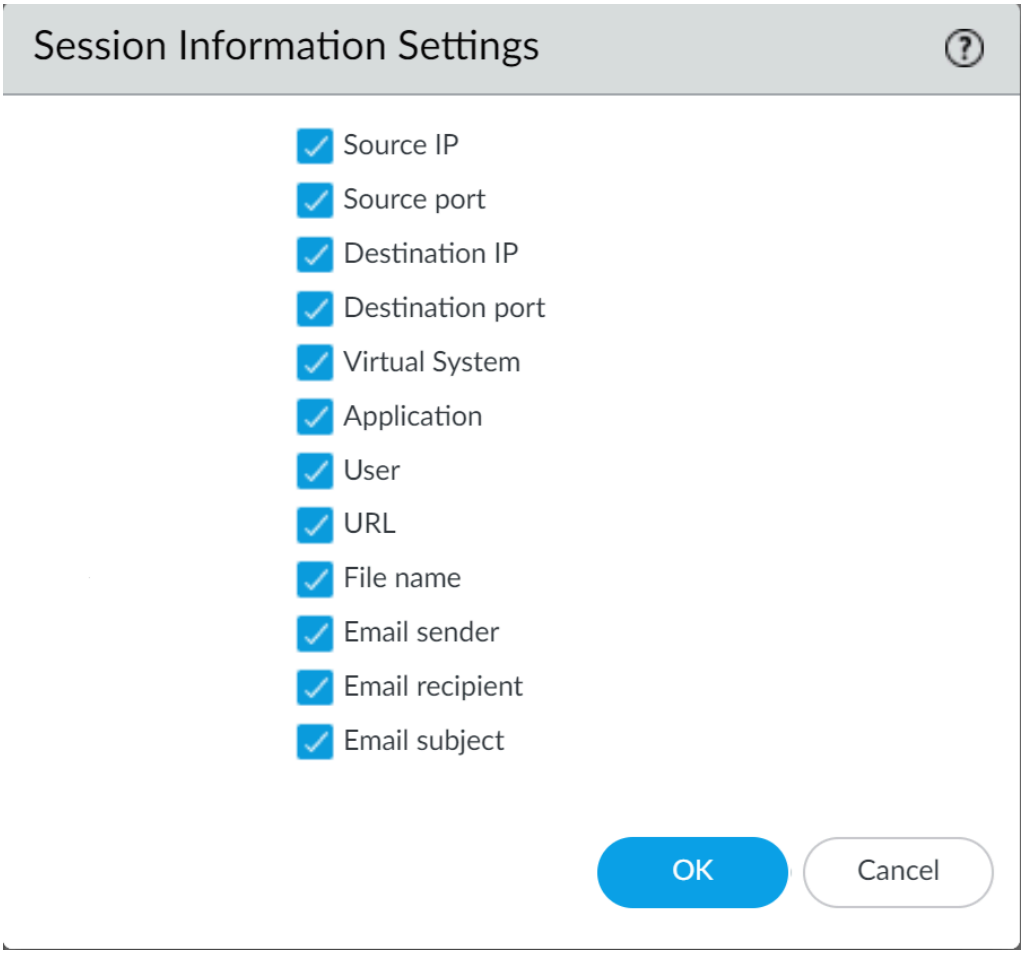
- **User**（用户）— 转发目标用户。
- **URL** — 转发与未知文件关联的 URL。
- **Filename**（文件名）— 转发未知文件的文件名。
- **Email sender**（电子邮件发件人）— 转发未知电子邮件链接的发件人（该电子邮件发件人的名称也显示在 WildFire 日志和报告中）。
- **Email sender**（电子邮件收件人）— 转发未知电子邮件链接的收件人（该电子邮件收件人的名称也显示在 WildFire 日志和报告中）。
- **Email subject**（电子邮件主题）— 转发未知电子邮件链接的主题（该电子邮件主题也显示在 WildFire 日志和报告中）。

STEP 3 | **Save**（保存）更改。

会话信息共享（**PAN-OS** 和 **Panorama**）

STEP 1 | 登录 PAN-OS Web 界面。

STEP 2 | 选择 **Device**（设备） > **Setup**（设置） > **WildFire** 并选中或清除以下 **Session Information Settings**（会话信息设置）选项。



- **Source IP**（源 **IP**）— 转发发送未知文件的源 IP 地址。
- **Source Port**（源端口）— 转发发送未知文件的源端口。
- **Destination IP**（目标 **IP**）— 转发未知文件的目标 IP 地址。
- **Destination Port**（目标端口）— 转发未知文件的目标端口。
- **Virtual System**（虚拟系统）— 转发检测未知文件的虚拟系统。
- **Application**（应用程序）— 转发传输未知文件的用户应用程序。
- **User**（用户）— 转发目标用户。
- **URL** — 转发与未知文件关联的 URL。
- **Filename**（文件名）— 转发未知文件的文件名。
- **Email sender**（电子邮件发件人）— 转发未知电子邮件链接的发件人（该电子邮件发件人的名称也显示在 WildFire 日志和报告中）。
- **Email sender**（电子邮件收件人）— 转发未知电子邮件链接的收件人（该电子邮件收件人的名称也显示在 WildFire 日志和报告中）。

- **Email subject**（电子邮件主题）— 转发未知电子邮件链接的主题（该电子邮件主题也显示在 WildFire 日志和报告中）。

STEP 3 | 单击 **OK**（确定）保存更改。

分析环境

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Advanced WildFire 许可证 对于 *Prisma Access*，凭借 *Prisma Access* 许可证，这通常会包含在内。

Advanced WildFire 再现各种分析环境，包括操作系统，以识别样本内的恶意行为。根据样本的特征和功能，可能使用多种分析环境以决定文件性质。Advanced WildFire 通过机器学习能力使用静态分析，确定已知和已知样本变体是否为恶意。基于对提交内容的初始判定，Advanced WildFire 发送未知样本至分析环境，通过从动态分析提取额外的信息和指数，更详细地检查文件。如果使用自定义或开源方法对文件进行模糊处理，则 Advanced Wildfire 云会在动态分析环境中内存中的文件进行压缩和解密，然后使用静态分析进行分析。在动态分析过程中，Advanced WildFire 观察文件在客户端系统中执行时的行为，查找恶意活动的各种迹象，比如更改浏览器安全设置、将代码注入其他进程、修改操作系统文件夹中的文件或样本尝试访问恶意域等等。此外，在 Advanced WildFire 云中进行动态分析时生成的 PCAP 将经过深入检查，并用于创建网络活动配置文件。网络流量配置文件可使用一对多配置文件匹配来检测已知恶意软件和之前未知的恶意软件。

Advanced WildFire 可以根据样本特征使用以下方法分析文件：

- **Static Analysis**（静态分析） — 在执行之前，通过分析样本特征检测已知威胁。
- **Machine Learning**（机器学习） — 通过将恶意软件特征集与动态更新的分级系统对比，识别已知威胁变体。
- **Dynamic Unpacking (WildFire Cloud analysis only)**（动态解包（仅 **Advanced Wildfire** 全球云）— 使用自定义/开源方法标识并解包加密文件，并为静态分析做好准备。
- **Dynamic Analysis**（动态分析） — 自定义构建的防规避虚拟环境，之前未知的提交情况在此进行测试，以确定实际影响和行为。
- 智能运行时内存分析（**Advanced WildFire** 许可证 **|** 仅**Advanced WildFire** 全球云 — 需要在 **NGFW** 上使用 **PAN-OS 10.0** 及更高版本）— 基于云的分析环境，运行高级检测器，用于利用多种规避技术分析现代威胁。

Advanced WildFire 运行可以复制下列操作系统的分析环境：

- **Microsoft Windows XP 32** 位（仅作为 **WildFire** 私有云的选项支持）
- **Microsoft Windows 7 64** 位
- **Microsoft Windows 7 32** 位（仅作为 **WildFire** 私有云的可选项提供支持）
- **Microsoft Windows 10 64** 位（作为运行 **PAN-OS 10.0** 或更高版本的 **Advanced WildFire** 公共云和 **WildFire** 私有云的选项提供支持）
- **Mac OS X**（仅限 **Advanced WildFire** 公共云）
- **Android**（仅限 **Advanced WildFire** 公共云）
- **Linux**（仅限 **Advanced WildFire** 公共云）

Advanced WildFire 公共云还通过多个版本的软件分析文件，以准确识别以特定客户端应用程序版本为目标的恶意软件。WildFire 专有云不支持多版本付息，且不会跨多版本分析指定应用程序的文件。

Advanced WildFire Inline Cloud Analysis

在何处可以使用？	需要提供什么？
• NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Advanced WildFire 许可证

Advanced WildFire 云运行一系列基于 ML 的内联云检测引擎，分析遍历网络的 PE（便携式可执行文件）样本，以实时检测和预防未知的恶意软件。这使 Advanced WildFire 云服务能够检测前所未见的恶意软件（没有现有 WildFire 签名或可通过本地 Advanced WildFire 内联云机器学习检测器）检测并阻止其感染客户端。其中包括某些之前不受阻碍地运行的恶意软件类型，这些是在外部环境中未曾见过，也没有被 Advanced WildFire Inline ML 拦截过的恶意软件，这是因为文件签名过期或签名数据库容量限制，这些最近出现的文件不足以使其签名出现在防火墙上。新定义的恶意文件将在后续遇到时被防火墙阻止，因为其签名已添加到当前签名集中，但是，这种情况发生在 WildFire 云分析恶意文件之后。

Advanced WildFire Inline Cloud 可以保存阻止下载文件（并可能在您的网络内传播），并以实时交换的方式分析云中的这些可疑文件是否存在恶意软件。与 WildFire 分析的其他恶意内容一样，Advanced WildFire Inline Cloud 检测到的任何威胁都会生成威胁签名，该签名由 Palo Alto Networks 通过签名更新包传播给客户，从而在未来为所有 Palo Alto Networks 客户提供防御。

Advanced WildFire Inline Cloud 在防火墙上使用轻量级转发机制运行，以最大限度地减少对本地性能的影响；为了跟上威胁格局的最新变化，云端内联机器学习检测模型在云端无缝添加和更新，无需内容更新或功能发布支持。

Advanced WildFire Inline Cloud Analysis 通过 WildFire Analysis 配置文件启用和配置，需要具有有效的 Advanced WildFire 许可证的 PAN-OS 11.1 或更高版本。

Advanced WildFire 内联机器学习

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Advanced WildFire 许可证 对于 *Prisma Access*，凭借 *Prisma Access* 许可证，这通常会包含在内。

通过 Antivirus 配置文件中的 Advanced WildFire inline ML 选项，防火墙数据面板可在 PE（可迁移可执行文件）、ELF（可执行与链接格式）和 MS Office 文件以及 PowerShell 和 Shell 脚本上实时应用机器学习。这一层防病毒保护是对基于 Advanced WildFire 的签名的补充，可扩展至尚不存在签名的文件。各个 inline ML 模型通过评估文件详细信息（包括解码器字段和模式），动态检测特定类型的恶意文件，从而形成文件的高概率分类。这种保护可扩展至当前已知以及未来可能会发生变化的、与 Palo Alto Networks 标识为恶意的特征相匹配的威胁。为了跟上威胁形势的最新变化，可以通过内容发布添加或更新 inline ML 模式。在启用 Advanced WildFire 内联机器学习之前，您必须拥有有效的 Advanced WildFire 或标准 WildFire 订阅。

作为 URL 过滤配置的一部分，还可启用基于 Inline ML 的保护以实时检测恶意 URL。

VM-50 或 *VM50L* 虚拟设备不支持 *Advanced WildFire* 内联机器学习。

判定结果

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Advanced WildFire 许可证 对于 *Prisma Access*，凭借 *Prisma Access* 许可证，这通常会包含在内。

当 Advanced WildFire 分析一个 Palo Alto Networks 托管的 Advanced WildFire 公共云或本地托管的 WildFire 专有云中之前未知的样本时，将产生判定以鉴别样本为恶意、不需要（灰色软件被视为强加但非恶意）、网络钓鱼或良性：

- 良性 — 样本为安全状态，不会表现出恶意行为。
- 灰色软件 — 样本不会带来直接的安全威胁，但可能在其他方面表现出妨碍性行为。典型的灰色软件包括 Adware、Spyware、Browser Helper Objects (BHOs) 等等。
- 网络钓鱼 — 链接将用户导向网络钓鱼网站，并构成安全威胁。网络钓鱼站点是攻击者伪装成合法网站的站点，目的是窃取用户信息，尤其是可访问您网络的公司密码。WildFire 设备不支持网络钓鱼判断，并将此类链接归为恶意。
- 恶意软件 — 样本为恶意软件并构成安全威胁。我们可能遇及的恶意软件包括病毒、蠕虫、特洛伊木马、远程访问工具 (RAT)、Rootkit、Botnets 等等。对于被识别为恶意软件的文件，将生成并分发签名，以防止将来遭受威胁。

每个 Advanced WildFire 云（全球（美国）和区域）以及 WildFire 私有云都可以独立于其他 WildFire 云选项来分析样本并生成 WildFire 判决。除了 WildFire 专有云判定以外，其他判定是全球共享的，因而 Advanced WildFire 用户可以访问全世界威胁数据的数据库。

您怀疑是错误的正面判定或负面判定，都可以提交至 *Palo Alto Networks* 威胁小组，进行进一步分析。您也可以手动更改提交至 *WildFire* 设备的样本判定。

文件分析

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Advanced WildFire 许可证 对于 *Prisma Access*，凭借 *Prisma Access* 许可证，这通常会包含在内。

Palo Alto Networks 防火墙可配置 Advanced WildFire 分析配置文件，以便根据文件类型转发样本进行 Advanced WildFire 分析（包括电子邮件链接）。此外，防火墙可解码已经编码或压缩多达四次（比如 ZIP 格式的文件）的文件；如果解码后的文件与 Advanced WildFire 分析配置文件标准相匹配，防火墙会转发解码后的文件进行 Advanced WildFire 分析。

Advanced WildFire 分析功能也可以在防火墙上启用，以提供内联防病毒保护。通过防病毒配置文件中的 Advanced WildFire 内联机器学习选项，防火墙数据面板可在 PE 和 ELF 文件以及 PowerShell 脚本上实时使用机器学习分析。各个 inline ML 模型通过评估文件详细信息（包括解码器字段和模式），动态检测特定类型的恶意文件，从而形成文件的高概率分类。这种保护可扩展至

当前已知以及未来可能会发生变化的、与 Palo Alto Networks 标识为恶意的特征相匹配的威胁。为了跟上威胁形势的最新变化，可以通过内容发布添加或更新 inline ML 模式。如需更多信息，请参阅 Advanced WildFire 内联机器学习。

Advanced WildFire 云还能分析某些作为多级 PE、APK 和 ELF 恶意软件包一部分，从而被用作辅助负载的文件类型。分析辅助负载可提供其他覆盖范围，以通过高级威胁破坏复杂攻击。这些高级威胁由激活其他恶意负载的执行代码操作，包括那些旨在协助规避安全措施和促进主负载扩散的代码。Advanced WildFire 通过在静态和动态分析环境中处理多级威胁来对其进行分析。在分析过程中，独立处理由多级恶意软件引用的文件；因此，在完成每个文件后即可立即提交判定结果和保护措施。多级文件的总体判定结果根据在所有攻击分析阶段发现的恶意内容威胁评估进行确定。在多级文件分析过程中发现的任何恶意内容，均会立即将该文件标记为恶意文件。

拥有恶意软件安全处理程序的组织可以通过 API 或 WildFire 门户用 RAR 格式手动提交受密码保护的样本。当 Advanced WildFire 云收到已用密码 *infected* 或 *virus* 加密的样本时，Advanced WildFire 云将进行解密并分析压缩文件。您可以按接收文件时的格式（在本例中为压缩文件）查看判定和分析结果。

尽管防火墙可以转发下面列出的所有文件类型，Advanced WildFire 分析支持可随着您提交样本的 Advanced WildFire 云不同而异。参阅 Advanced WildFire 文件类型支持以了解更多信息。

支持 **WildFire** 转发的文件类型	说明
`apk`	Android 应用程序包 (APK) 文件。 *APK* 文件中包含的 *DEX* 文件将作为 *APK* 文件分析的一部分进行分析。
`flash`	嵌入网页的 Adobe Flash 小程序和 Flash 内容。
`jar`	Java applet（JAR/Class 文件类型）。
`ms-office`	Microsoft Office 使用的文件，包括文档（DOC、DOCX 和 RTF）、工作簿（XLS 和 XLSX）、PowerPoint（PPT 和 PPTX）演示文档和 Office Open XML (OOXML) 2007+ 文档。内容版本 8462 支持互联网查询 (IQY) 和符号链接 (SLK) 文件。
`pe`	可移植可执行 (PE) 文件。PE 文件包括可执行文件、对象代码、DLL、FON（字体）和 LNK 文件等等。内容版本 8462 支持 MSI 文件。对 PE 文件进行 WildFire 分析无需配备订阅，但分析其他所有支持文件类型都需要配备订阅。
`pdf`	可移植文档格式 (PDF) 文件。

支持 **WildFire** 转发的文件类型	说明
`MacOSX`	macOS 平台使用的各种文件类型。DMG、PKG 和 ZBundle 文件的静态分析仅在 Advanced WildFire Global（美国）和欧洲云区域可用，但是，所有区域云均支持对其他 Mac OS X 文件（FAT 和 Mach-O 文件）进行静态分析。只有 Advanced WildFire Global（美国）和欧洲云区域支持所有 Mac OS X 文件的动态分析。有关详细信息，请参阅文件类型支持。
`email-link`	SMTP 和 POP3 电子邮件消息中包含的 HTTP/HTTPS 链接。参见电子邮件链接分析。
`archive`	Roshal Archive（RAR 和 7-Zip）压缩文件。被分为若干小文件，而无法提交用于分析的多卷压缩文件。 Advanced WildFire 云仅解密和分析用密码 *infected* 或 *virus* 加密的 RAR 文件。 虽然防火墙能够在 *ZIP* 压缩文件解码后转发其中包含的受支持文件，但它无法转发处于编码状态的完整 *ZIP* 文件。如果您想提交完整的 *ZIP* 文件，您可以使用 *WildFire* 门户或通过 *WildFire API* 手动上传 *ZIP* 文件。
`linux`	可执行与可链接格式 (ELF) 文件。
`script`	各种脚本文件。 • 内容版本 8101 支持 Jscript (JS)、VBScript (VBS) 和 PowerShell Script (PS1)。 • 内容版本 8168 支持批处理 (BAT) 文件。 • 内容版本 8229 支持 HTML 应用程序 (HTA) 文件。

电子邮件链接分析

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Advanced WildFire 许可证 对于 *Prisma Access*，凭借 *Prisma Access* 许可证，这通常会包含在内。

在何处可以使用？	需要提供什么？
• VM-SERIES • CN-Series	

Palo Alto Networks 防火墙可提取 SMTP 和 POP3 电子邮件消息中包含的 HTTP/HTTPS 链接，并转发这些链接进行分析。防火墙仅从电子邮件消息中提取链接和相关的会话信息（发件人、收件人和主题），防火墙不接收、存储、转发或查看电子邮件消息。

WildFire 访问链接以确定相应的网页是否存在漏洞或显示网络钓鱼活动。WildFire 发现的恶意或网络钓鱼链接：

- 作为 WildFire 提交情况日志条目记录在防火墙上。每个 WildFire 提交情况日志条目都有 WildFire 分析报告，该报告详细描述了观察到的链接行为和活动。该日志条目还包括电子邮件标题信息（电子邮件发件人、收件人和主题），您可据此来辨识消息，并决定是否将其从邮件服务器中删除，而如果已投递和/或打开此电子邮件，则可选择采取其他措施来减轻威胁。
- 添加到 PAN-DB 且 URL 被分类为恶意链接。

防火墙可分批转发电子邮件链接（每批 100 个电子邮件链接），或每两分钟转发一次，具体取决于先达到何种方式的上限。每个上传到 WildFire 的批处理都算作一次上传，计入给定防火墙防火墙文件转发容量（按型号）的每分钟上传容量。如果电子邮件中包含的链接与文件下载而非 URL 相对应，则仅当对应的文件类型可用于进行 WildFire 分析时，防火墙才会转发此文件。

要使防火墙能够转发电子邮件中包含的链接以进行 WildFire 分析，请参阅转发文件以进行 Advanced WildFire 分析。凭借 Advanced URL Filtering 许可证，您也可以阻止用户访问恶意和网络钓鱼网站。

URL 分析

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Advanced WildFire 许可证 对于 *Prisma Access*，凭借 *Prisma Access* 许可证，这通常会包含在内。

Advanced WildFire 全球云（美国）和地区云可以分析 URL，并扩展至分析电子邮件链接，通过 WildFire API 提供标准化的判定结果和报告。通过收集所有 Palo Alto Networks 服务（包括 PAN-DB）的威胁分析详细信息，Advanced WildFire 能够生成更加准确的结论并提供一致的 URL 分析数据。

在 Advanced WildFire 全球云（美国）中运行的 URL 分析程序处理 URL 源、相关的 URL 源（例如电子邮件链接）、NRD（新注册的域）列表、PAN-DB 内容和手动上传的 URL，为所有 Advanced WildFire 云提供改进后的功能，而不会影响 GDPR 合规性。处理 URL 之后，您可以检索 URL 分析报告（包括结论）、检测原因和证据、屏幕截图以及生成的网络请求分析数据。您也可以检索 URL 分析过程中发现的网页构件（下载文件和屏幕截图）以进一步分析异常活动。

使用此功能无需额外配置，但是，如果您想要自动提交电子邮件链接以进行分析（这些链接现在通过此服务分析），您必须转发文件以进行 Advanced WildFire 分析。

您怀疑是错误的正面判定或负面判定，都可以提交至 Palo Alto Networks 威胁小组，进行进一步分析。

压缩和编码文件分析

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Advanced WildFire 许可证 对于 *Prisma Access*，凭借 *Prisma Access* 许可证，这通常会包含在内。

默认情况下，防火墙可解码已经编码或压缩多达四次的文件，包括使用 ZIP 格式压缩的文件。然后，防火墙检查并强制执行已解码的文件上的策略；如果文件未知，防火墙会转发已解码的文件进行 WildFire 分析。虽然防火墙无法转发完整的 ZIP 压缩文件用于 Advanced WildFire 分析，但您可以使用 WildFire 门户或 WildFire API 直接将文件提交到 Advanced WildFire 公共云中。

防火墙不解码 *RAR* 和 *7-Zip* 压缩文件。这些文件的所有处理都发生在 *Advanced WildFire* 公共云中。

Advanced WildFire 签名

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Advanced WildFire 许可证 对于 *Prisma Access*，凭借 *Prisma Access* 许可证，这通常会包含在内。

在何处可以使用？	需要提供什么？
• VM-SERIES • CN-Series	

Advanced WildFire 可以在 Web 流量 (HTTP/HTTPS)、电子邮件协议（SMTP、IMAP 和 POP）和 FTP 流量中发现零日恶意软件，并且可以快速生成签名以识别和防止以后感染所发现的恶意软件。Advanced WildFire 会基于样本的恶意软件有效内容自动生成一个签名，并测试该签名的精确性和安全性。

每个 Advanced WildFire 云都会独立于其他 Advanced WildFire 云来分析样本并生成恶意软件签名。WildFire 专有云签名的例外情况除外，Advanced WildFire 签名都是全球共享的，从而让全世界的用户都可以从对恶意软件的覆盖获益，且无论该恶意软件是在何处被首次侦测到。由于恶意软件的变异速度非常快，所以 Advanced WildFire 生成的签名可以解决恶意软件的多个变体。

一旦最新的 Advanced WildFire 签名可用，拥有有效 Advanced WildFire 许可证的防火墙就可以实时进行检索。如果没有 Advanced WildFire 订阅，则可在 24-48 小时内作为防病毒更新的一部分对具有有效威胁阻止许可证的防火墙提供签名。

防火墙下载和安装新的签名后，将立即自动阻止包含该恶意软件（或其变体）的任何文件。恶意软件签名不会侦测恶意和网络钓鱼链接；要强制侦测这些链接，您必须拥有 PAN-DB URL 筛选许可证。.之后，您可以阻止用户对恶意和网络钓鱼网站的访问。

Advanced WildFire 部署

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Advanced WildFire 许可证 对于 *Prisma Access*，凭借 *Prisma Access* 许可证，这通常会包含在内。

您可以设置 Palo Alto Networks 防火墙提交未知样本至一个 Palo Alto Networks 托管的 Advanced WildFire 公共云、U.S.Government 云或本地托管的 WildFire 专有云，或者启用防火墙将特定样本转发至一个 Advanced WildFire 公共云选项，另将特定样本转发至 WildFire 专有云：

- Advanced WildFire 公共云
- WildFire 私有云
- WildFire 混合云
- WildFire：U.S.Government 云

Advanced WildFire 公共云

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Advanced WildFire 许可证 对于 *Prisma Access*，凭借 *Prisma Access* 许可证，这通常会包含在内。

Palo Alto Networks 防火墙可以转发未知文件和电子邮件链接至 Advanced WildFire 全球云（美国）或 Palo Alto Networks 拥有并维护的 Advanced WildFire 地区云。根据您的位置和组织需求，选择您提交样本进行分析的 Advanced WildFire 公共云：

- **Advanced WildFire** 全球云（美国）

  Advanced WildFire 全球云（美国）是托管于美国的公共云环境。

  使用下列 URL 提交文件至 Advanced WildFire 全球云（美国）进行分析，并访问 Advanced WildFire 全球云（美国）门户：wildfire.paloaltonetworks.com。

- **Advanced WildFire Europe** 云

  WildFire 欧洲云是托管于荷兰的地区公共云环境。其旨在符合欧盟 (EU) 数据隐私条例，提交至 WildFire 欧洲云的样本留存在欧洲边境范围以内。

  使用下列 URL 以提交文件至 WildFire 欧洲云进行分析，并访问 Advanced WildFire 欧洲云门户：eu.wildfire.paloaltonetworks.com。

- **Advanced WildFire** 日本云

  Advanced WildFire 日本云是托管于日本的地区公共云环境。

  使用下列 URL 提交文件至 Advanced WildFire 日本云进行分析，并访问 Advanced WildFire 日本云门户：jp.wildfire.paloaltonetworks.com。

- **Advanced WildFire** 新加坡云

  Advanced WildFire 新加坡云是托管于新加坡的地区公共云环境。

  使用下列 URL 以提交文件至 Advanced WildFire 新加坡云进行分析，并访问 Advanced WildFire 新加坡云门户：sg.wildfire.paloaltonetworks.com。

- **Advanced WildFire** 英国云

  Advanced WildFire 英国云是托管于英国的地区公共云环境。

  使用下列 URL 将文件提交至 Advanced WildFire 英国云进行分析，并访问 Advanced WildFire 英国云门户：uk.wildfire.paloaltonetworks.com。

- **Advanced WildFire** 加拿大云

  WildFire 加拿大云是托管于加拿大的地区公共云环境。

  使用下列 URL 以提交文件至 Advanced WildFire 加拿大云进行分析，并访问 Advanced WildFire 加拿大云门户：ca.wildfire.paloaltonetworks.com。

- **Advanced WildFire** 澳大利亚云

  WildFire 澳大利亚云是托管于澳大利亚的地区公共云环境。

  使用下列 URL 提交文件至 Advanced WildFire 澳大利亚云进行分析，并访问 Advanced WildFire 澳大利亚云门户：au.wildfire.paloaltonetworks.com。

- **Advanced WildFire** 德国云

  Advanced WildFire 德国云是托管于德国的地区公共云环境。

  使用下列 URL 以提交文件至 Advanced WildFire 德国云进行分析，并访问 Advanced WildFire 德国云门户：de.wildfire.paloaltonetworks.com。

- **Advanced WildFire** 印度云

  Advanced WildFire 印度云是托管在印度的地区性公共云环境。

  使用下列 URL 以提交文件至 Advanced WildFire 印度云进行分析，并访问 Advanced WildFire 印度云门户：in.wildfire.paloaltonetworks.com。

- **Advanced WildFire** 瑞士云

  Advanced WildFire 瑞士云是在瑞士托管的区域公共云环境。

  使用以下 URL 将文件提交到 Advanced WildFire 瑞士云进行分析并访问 Advanced WildFire 瑞士云门户：ch.wildfire.paloaltonetworks.com。

- **Advanced WildFire** 波兰云

  Advanced WildFire 波兰云是在波兰托管的区域公共云环境。

  使用以下 URL 将文件提交到 Advanced WildFire 波兰云进行分析并访问 Advanced WildFire 波兰云门户：pl.wildfire.paloaltonetworks.com。

- **Advanced WildFire** 印度尼西亚云

  Advanced WildFire 印度尼西亚云是在印度尼西亚托管的区域公共云环境。

  使用以下 URL 将文件提交到 Advanced WildFire 印度尼西亚云进行分析并访问 Advanced WildFire 印度尼西亚云门户：id.wildfire.paloaltonetworks.com。

- **Advanced WildFire** 台湾云

  Advanced WildFire 台湾云是在台湾托管的区域公共云环境。

  使用以下 URL 将文件提交到 Advanced WildFire 台湾云进行分析并访问 Advanced WildFire 台湾云门户：tw.wildfire.paloaltonetworks.com。

- **Advanced WildFire** 法国云

  Advanced WildFire 法国云是在法国托管的区域公共云环境。

  使用以下 URL 将文件提交到 Advanced WildFire 法国云进行分析并访问 Advanced WildFire 法国云门户：fr.wildfire.paloaltonetworks.com。

- **Advanced WildFire** 卡塔尔云

  Advanced WildFire 卡塔尔云是在卡塔尔托管的地区性公共云环境。

  使用以下 URL 将文件提交到 Advanced WildFire 卡塔尔云进行分析并访问 Advanced WildFire 卡塔尔云门户：qatar.wildfire.paloaltonetworks.com。

- **Advanced WildFire South Korea** 云

  Advanced WildFire South Korea 云是在韩国托管的区域公共云环境。

  使用以下 URL 将文件提交到 Advanced WildFire South Korea 云进行分析，并访问 Advanced WildFire South Korea 云门户：kr.wildfire.paloaltonetworks.com。

- **Advanced WildFire Israel** 云

  Advanced WildFire Israel 云是托管在以色列的区域公共云环境。

  使用以下 URL 将文件提交到 Advanced WildFire Israel 云进行分析，并访问 Advanced WildFire Israel 云门户：il.wildfire.paloaltonetworks.com。

- **Advanced WildFire Saudi Arabia** 云

  Advanced WildFire Saudi Arabia 云是一个托管在沙特阿拉伯的区域公共云环境。

  使用以下 URL 将文件提交到 Advanced WildFire Saudi Arabia 云进行分析，并访问 Advanced WildFire Saudi Arabia 云门户：sa.wildfire.paloaltonetworks.com。

- **Advanced WildFire Spain** 云

  Advanced WildFire Spain 云是托管在西班牙的区域公共云环境。

  使用以下 URL 将提交文件至 Advanced WildFire Spain 云进行分析，并访问 Advanced WildFire Spain 云门户：es.wildfire.paloaltonetworks.com。

每个 Advanced WildFire 云（全球（美国）和地区云）都会独立于其他 WildFire 云分析样本、生成恶意软件签名以及进行判断。随后，Advanced WildFire 签名和判断都会在全球进行共享，从而让全世界的 WildFire 用户都可以从对恶意软件的覆盖中获益，无论在何处首次被检测到该恶意软件。查看 Advanced WildFire 文件类型支持以进一步了解各种云分析的文件类型。

如果您有 WildFire 设备，您可以启用 WildFire 混合云 部署，其中的防火墙可以转发特定文件至 WildFire 公共云，其他文件则转发至 WildFire 专有云进行本地分析。也可以配置 WildFire 设备，通过在分析前查询公共云，快速收集对已知样本的判断。这允许 WildFire 设备将分析资源专门用于分析对您的专有网络和全球 WildFire 社区而言，都处于未知状态的样本。

WildFire 私有云

在何处可以使用？	需要提供什么？
• NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Advanced WildFire 或 WildFire 许可证

在 Palo Alto Networks 专有云部署中，Palo Alto Networks 防火墙会转发文件至用于托管专有云分析位置的企业网络上的 WildFire 设备。

有关混合云转发的更多信息，请参阅《WildFire 设备管理员指南》。

WildFire 混合云

在何处可以使用？	需要提供什么？
• NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Advanced WildFire 或 WildFire 许可证

WildFire 混合云部署中的防火墙可以转发特定样本至 Palo Alto Networks 托管的 WildFire 公共云之一，并将其他样本转发至 WildFire 设备托管的 WildFire 专有云。

有关混合云转发的更多信息，请参阅《WildFire 设备管理员指南》。

WildFire FedRAMP 授权云平台

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Advanced WildFire 许可证 对于 *Prisma Access*，凭借 *Prisma Access* 许可证，这通常会包含在内。 ❑ Advanced WildFire FedRAMP 附加组件

除了 WildFire Global 云、私有云和混合云部署选项外，Palo Alto Networks 还为需要遵守安全云运营标准的组织提供多个高安全性、FedRAMP 授权的云环境。FedRAMP 授权的云有两种影响级别：高级和中级，其中中级有两种云配置可供选择。Advanced WildFire Government 云符合 FedRAMP 高级认证标准，而 Advanced WildFire Government 云和 WildFire U.S.Government 云符合 FedRAMP 中级认证标准。

WildFire U.S.Government 云（符合 *FedRAMP* 中级认证标准）计划将停用。对于所有新客户，*Palo Alto Networks* 建议使用 *Advanced WildFire Public Sector* 云，它具有增强的功能集并支持 *Advanced WildFire Cloud*。

FedRAMP 中级云（Advanced WildFire Government 云和 WildFire U.S.Government 云）通常可供 Palo Alto Networks 客户使用，但符合 FedRAMP 高级认证标准的 Advanced WildFire Government 云仅可供联邦政府、国防部或经批准的国防工业基地 (DIB) 客户使用。

由于这些服务的敏感性，FedRAMP 云具有与其他服务不同的特定初始配置流程。有关更多信息，请请参阅具体的 FedRAMP 云类型：

- Advanced WildFire Government 云
- Advanced WildFire Public Sector Cloud
- WildFire：U.S.Government 云

上面列出的 FedRAMP 云不能在同一设备上混合搭配，也不能与 Advanced WildFire 全球或区域云同时使用。但是，任何 FedRAMP 云都可以与其他基于云的安全服务（例如 Advanced Threat Prevention、DLP 等）结合使用。如果您需要在单个设备上采用多个 FedRAMP 安全级别，则必须使用单独的帐户 ID。初始配置完成后，您可以在 Antivirus 安全配置文件和 API 中引用 FedRAMP 云 URL，就像任何其他 Advanced WildFire 云一样。

Advanced WildFire Government 云

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Advanced WildFire 许可证 对于 *Prisma Access*，凭借 *Prisma Access* 许可证，这通常会包含在内。 ❑ Advanced WildFire GovCloud 附加组件

Palo Alto Networks 为联邦、国防部或经批准的国防工业基地 (DIB) 客户提供 Advanced WildFire Government 云，这是一个符合 FedRAMP（联邦风险与授权管理计划）高认证标准的高安全性恶意软件分析平台。

Advanced WildFire Public Sector 云作为独立于商业或Government 云区域的实体运营 — 发送来进行分析的样本中可能存在的任何隐私信息（例如电子邮件地址、IP 地址和被动 DNS）都不会与任何其他 WildFire 云实例共享。但是，它仍然能够利用 WildFire 公共云生成的威胁数据，以便最大限度扩大覆盖功能，也能够利用通过文件分析生成的保护和防病毒签名。

有关 *Palo Alto Networks Advanced WildFire FedRAMP* 授权的更多详细信息，请访问：FedRAMP.gov

有关 Palo Alto Network 的 WildFire FedRAMP 授权的更多详细信息，请访问：Palo Alto Networks Government 云服务 - WildFire

Advanced WildFire Government Cloud 与标准商业 Advanced WildFire 公共云有几个功能存在差异。连接到 Advanced WildFire Government 云的客户无法使用以下功能：

- Advanced WildFire U.S.Government 云区域不支持裸机分析
- 无法通过 WildFire 门户访问 Advanced WildFire Government 云。
- 如果没有服务请求，则无法使用删除功能的权利。

开始使用 **Advanced WildFire Government** 云

遵循所有内部程序措施，以确定是否在您的网络中是否适合使用 Advanced WildFire U.S.Government 云，例如但不限于进行风险分析、CSP 提交数据包评估和授权审批。请联系 Palo Alto Networks 销售代表/Advanced WildFire：U.S.Government 云联络点用于讨论任何其他操作详细信息。

当您满足运营 FedRAMP 授权服务的适当组织要求时，就可以开始访问 Advanced WildFire U.S.Government 云。

联系 Palo Alto Networks 客户团队，启动培训流程。完成 Advanced WildFire 激活后，重新配置防火墙，以便使用以下 URL 转发未知文件和电子邮件链接来进行分析：gov-cloud.wildfire.paloaltonetworks.com。有关更多信息，请参阅转发文件进行 WildFire 分析。如果您需要任何其他帮助，请联系 Palo Alto Networks 客户支持。

Advanced WildFire Public Sector Cloud

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Advanced WildFire 许可证 对于 *Prisma Access*，凭借 *Prisma Access* 许可证，这通常会包含在内。 ❑ Advanced WildFire PubSec 附加组件

Palo Alto Networks 为客户提供了 Advanced WildFire Public Sector Cloud，这是一款符合 FedRAMP（联邦风险和授权管理计划）中等认证标准的高安全性恶意软件分析平台。Advanced WildFire Public Sector Cloud 用于取代 WildFire U.S.Government 云引入新客户。

Advanced WildFire Public Sector 云作为独立于商业或Government 云区域的实体运营 — 发送来进行分析的样本中可能存在的任何隐私信息（例如电子邮件地址、IP 地址和被动 DNS）都不会与任何其他 WildFire 云实例共享。但是，它仍然能够利用 WildFire 公共云生成的威胁数据，以便最大限度扩大覆盖功能，也能够利用通过文件分析生成的保护和防病毒签名。

有关 *Palo Alto Networks Advanced WildFire FedRAMP* 授权的更多详细信息，请访问：FedRAMP.gov

Advanced WildFire Public Sector 云与标准商用 Advanced WildFire 公有云有一些功能上的差异。对于连接至 Advanced WildFire Public Sector 云的客户，以下功能不可用：

- Advanced WildFire U.S.Government 云区域不支持裸机分析。
- Advanced WildFire U.S.Public Sector 云区域无法通过 WildFire 门户访问。
- 如果没有服务请求，则无法使用删除功能的权利。

Advanced WildFire Public Sector 云使用入门

遵循所有内部程序措施，以确定在您的网络中使用 Advanced WildFire Public Sector 云的适用性，例如但不限于进行风险分析、评估 CSP 提交包和授权审批。请联系 Palo Alto Networks 销售代表/Advanced WildFire：U.S.Public Sector 云联络点，以讨论任何其他运营详细信息。

当您满足运营 FedRAMP 授权服务的适当组织要求时，即可开始访问 Advanced WildFire Public Sector 云区域。

联系 Palo Alto Networks 客户团队，启动培训流程。完成 Advanced WildFire 激活后，重新配置防火墙，以便使用以下 URL 转发未知文件和电子邮件链接来进行分析：pubsec-cloud.wildfire.paloaltonetworks.com。

有关更多信息，请参阅转发文件进行 WildFire 分析。如果您需要任何其他帮助，请联系 Palo Alto Networks 客户支持。

WildFire：U.S.Government 云

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Advanced WildFire 许可证 对于 *Prisma Access*，凭借 *Prisma Access* 许可证，这通常会包含在内。 ❑ WildFire U.S.Government 初始配置

截至 *2024* 年 *7* 月 *15* 日，*Palo Alto Networks WildFire U.S.Government* 云已被 Advanced WildFire Government 云 和 Advanced WildFire Public Sector Cloud 取代，后两者可以访问运行具有增强功能集的较新代码库的高安全性 *Advanced WildFire* 云环境。因此，*Palo Alto Networks* 不再为 *WildFire U.S.Government* 云引入新客户。现有客户可以继续访问 *WildFire U.S.Government* 云可供继续使用至 *2024* 年 *11* 月 *30* 日，然后就会停用，届时现有 *URI* 将重定向至 *Advanced WildFire Public Sector* 云。

有关新云产品的详细信息，请联系 *Palo Alto Networks* 销售代表，以便讨论任何其他运营详细信息。

Palo Alto Networks WildFire U.S.Government 云是一个高安全性恶意软件分析平台，经 FedRAMP（联邦风险和授权管理计划）授权。此 WildFire 云环境仅供要求采用标准化方法对云产品和服务进行安全评估、授权和持续监控的美国联邦机构使用。WildFire：U.S.Government 云作为独立的实体运行——任何发送以供分析的样本中的隐私信息（例如电子邮件、IP 地址和被动 DNS），均不会与任何 WildFire 云实例共享。但是，它仍然能够利用 WildFire 公共云生成的威胁数据最大化覆盖功能，以及通过文件分析生成的保护和防病毒签名。

有关 Palo Alto Network 的 WildFire FedRAMP 授权的更多详细信息，请访问：Palo Alto Networks Government 云服务 - WildFire

WildFire 公共云（全球和地区云）和 WildFire U.S.Government 云有几个与公共云不同的功能。对于连接至 WildFire 的客户，以下功能不可用：U.S.Government 云

- U.S. Government 云不支持裸机分析。
- 当前不支持脚本文件（Bat、JS、BVS、PS1、Shell script 和 HTA）分析。
- WildFire：U.S.Government 云无法通过 WildFire 门户访问。
- WildFire：U.S. Government 云不可集成其他基于云的服务。
- 删除功能权限不可用。
- WildFire：U.S. Government 云当前不支持 Advanced WildFire 分析。

WildFire 入门：U.S.Government 云

以便连接到 WildFire：U.S.Government 云，必须申请才能访问。遵循所有内部程序措施，以确定是否适合使用 WildFire：您网络中的 U.S. Government 云，例如但不限于进行风险分析、CSP 提交数据包评估和批准授权。请联系 Palo Alto Networks 销售代表/WildFire：U.S.Government 云联络点用于讨论任何其他操作详细信息。

当您满足操作 FedRAMP 授权服务的适当组织要求时，就可以请求访问 WildFire U.S. Government 云。可访问 WildFire U.S.Government 云的实体有两类：美国政府承包商和美国联邦机构（以及其他经批准的政府部门）。这两类实体在访问 WildFire U.S.Government 云时均有特定要求

1. 美国联邦机构

   美国联邦机构、部门和事务所必须获得指定许可机构 (DAA) 颁发的运营授权 (ATO)，从而在授予访问权限之前，授权可在机构内部运营 WildFire U.S. Government 云。

   1. 告知 Palo Alto Networks 联络点 (fedramp@paloaltonetworks.com) 使用 WildFire U.S.Government 云的意图。
   2. 发送请求至 info@fedramp.gov。
   3. 填写 FedRAMP 套餐访问请求表，并将其提交至 info@fedramp.gov。

      FedRAMP 项目管理办公室 (PMO) 将会审核该表，并且通常会签发有关 WildFire FedRAMP 套餐的 30 天临时访问权限。
   4. 为 WildFire U.S.Government 云审核 FedRAMP 安全套餐。完成将 WildFire U.S.Government 云部署到贵组织所需的所有内部流程。
   5. 签发 ATO。
   6. 向 FedRAMP PMO 发送请求，申请永久访问 WildFire U.S.Government 云。

2. 美国政府承包商

   美国使用或访问 WildFire（美国）的政府承包商Government 云必须满足以下要求。

   1. 必须为美国公民。
   2. 与美国签订有效合同（或分包合同）联邦政府机构，其工作需要使用互联网进行信息交换，例如电子邮件通信、文档共享和其他形式的互联网通信。
   3. 承包商的雇佣关系终止后，用户必须停止使用或访问 WildFireGovernment 云的意图。
   4. 遵守 Palo Alto Networks EULA 中的保密条款。

在您的组织颁发经营许可 (ATO)，或适用的美国政府承包商符合所有使用要求后，才能联系 Palo Alto Networks 客户团队，以便提出访问 WildFire U.S.Government 的请求。

1. 请联系您的 FedRAMP 项目管理办公室 (PMO)，确定 U.S. Government 云是否可以满足您的安全需求。
2. 联系 FedRAMP Marketplace（FedRAMP 市场）中指定的 Palo Alto Networks 联络点。联络点会提供有关服务的其他信息，以及任何与您特定 WildFire 部署相关的其他操作详细信息。
3. 联系 Palo Alto Networks 客户团队，启动培训流程。客户团队需要以下有关客户详细信息和部署详情的信息。
   - 联系信息。
   - 有关迁移至 WildFire U.S.Government 云。
   - 有关组织遵守 Palo Alto Networks EULA 中概述的保密规定的声明。
   - 所有防火墙网关（包括管理层）的传出 IP 地址，以及所有 Panorama 实例。
4. 在 WildFire 项目管理办公室批准使用 WildFire U.S.Government 云后（通常在 1-3 个工作日内），Palo Alto Networks 开发运营部门将会应用适当的控件。
5. 授予访问 WildFire U.S.Government 云的权限后，请使用以下 URL 重新配置防火墙来转发未知文件和电子邮件链接，以便进行分析：wildfire.gov.paloaltonetworks.com。有关更多信息，请参阅转发文件进行 WildFire 分析。如果您需要任何其他帮助，请联系 Palo Alto Networks 客户支持。

文件类型支持

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Advanced WildFire 许可证 对于 *Prisma Access*，凭借 *Prisma Access* 许可证，这通常会包含在内。

下表列出了支持在 WildFire 云环境中进行分析的文件类型。

有关 *WildFire* 支持的特定文件类型的完整列表，请参阅支持的文件类型（完整列表）。

支持分析的文件类型	**Advanced WildFire** 公共云（所有地区）	**WildFire U.S.Government** 云	**Advanced WildFire** 门户 **| API**（直接上传；所有地区）
电子邮件中的链接	✓	✓	✓
Android 应用程序包 (APK) 文件	✓	✓	✓
Adobe Flash 文件	✓	✓	✓
Java 压缩 (JAR) 文件	✓	✓	✓
Microsoft Office文件（包括 SLK 和 IQY 文件）	✓	✓	✓
可迁移可执行文件（包括 MSI 文件）	✓	✓	✓

支持分析的文件类型	**Advanced WildFire** 公共云（所有地区）	**WildFire U.S.Government** 云	**Advanced WildFire** 门户 **| API**（直接上传；所有地区）
可移植文档格式 (PDF) 文件	✓	✓	✓
Mac OS X* 文件	✓	✓	✓
Linux（ELF 文件和 Shell 脚本）文件	✓	✓	✓
存档（RAR、7-Zip、ZIP**）文件	✓	✓	✓
脚本（BAT、JS、VBS、PS1 和 HTA）文件	✓	✗	✓
Python 脚本	✓	✓	✓
Perl 脚本	✗	✗	✓
存档（ZIP [直接上传] 和 ISO）文件	✗	✗	✓
图像（JPG 和 PNG）文件	✗	✗	✓

* DMG、PKG 和 ZBundle 文件的静态分析仅在 Advanced WildFire Global（美国）和欧洲云区域可用，但是，所有区域云均支持对其他 Mac OS X 文件（FAT 和 Mach-O 文件）进行静态分析。只有 Advanced WildFire Global（美国）和欧洲云区域支持所有 Mac OS X 文件的动态分析。

* 不会将 ZIP 文件直接转发到 Advanced WildFire 云进行分析。防火墙会先对其进行解码，然后单独转发与 WildFire 分析配置文件条件匹配的文件以进行分析。

了解更多？

- 有关每个 *Advanced WildFire* 云部署的详细信息，请参阅 Advanced WildFire 部署。
- 关于支持 *WildFire* 分析的各种文件类型详细信息，请参阅文件分析。

支持的文件类型（完整列表）

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Advanced WildFire 许可证 对于 *Prisma Access*，凭借 *Prisma Access* 许可证，这通常会包含在内。

下表列出了 WildFire 分析支持的文件类型。对于转发支持列中标记为“是”的文件，这包括在网络流量 (HTTP/HTTPS) 和电子邮件协议（SMTP、IMAP、POP）中采用 MIME 编码的文件。

支持的内容类型	扩展示例	转发支持
7zip 存档	7z	是
Adobe Flash 文件	swf	是
安卓 APK	apk	是
安卓 DEX	dex	是
批处理文件	bat	是
bzip2 存档	bz	是
逗号分隔值	csv	否
DLL、DLL64	dll	是
ELF	elf	是
Gzip 存档	gz	否
HTML 应用程序	hta	是
ISO	iso	否
JAVA 类	class	是

支持的内容类型	扩展示例	转发支持
JAVA JAR	jar	是
JavaScript/JScript	js、jse、wsf	是（仅限 JS）
Joint Photographic Experts Group	jpg	否
链接	elink	是
Mach-O	macho	是
macOS 应用安装程序	pkg	是
ZIP 存档中的 macOS 应用捆绑包	zbundle	否
macOS 通用二进制文件	fat	否
macOS 磁盘映像	dmg	是
Microsoft Excel 97 - 2003 文档	xls	是
Microsoft Excel 文档	xlsx	是
Microsoft One Note 文档	one	是
Microsoft PowerPoint 97 - 2003 文档	ppt	是
Microsoft PowerPoint 文档	pptx	是
Microsoft 符号链接文件	slk	是
Microsoft Web 查询文件	iqy	是
Microsoft Word 97 - 2003 文档	doc	是
Microsoft Word 文档	docx	是
OpenDocument 电子表格文档	ods	否

支持的内容类型	扩展示例	转发支持
OpenDocument 文本文档	odt	否
PDF	pdf	是
PE、PE64	exe	是
Perl 脚本	pl	否
便携式网络图形文件	png	否
PowerShell	ps1	是
Python 脚本	py	是
RAR 存档	rar	是
RTF	rtf	是
Shell 脚本	sh	是
Tar 存档	tar	否
VBScript	vbs、vbe	是（仅限 VBS）
Windows 安装程序包	msi	是
Windows 链接文件	lnk	是
Windows 脚本	wsf	否
Zip 存档	zip	否
活动服务器页面	asp	否
Active Server Pages Extended	aspx	否
可扩展标记语言	xml	否
超文本标记语言	html	否

Advanced Wildfire 示例

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Advanced WildFire 许可证 对于 *Prisma Access*，凭借 *Prisma Access* 许可证，这通常会包含在内。

以下示例案例总结了 Advanced WildFire™ 的完整生命周期。在此示例中，Palo Alto Networks 的销售代表下载销售合作伙伴上传至 Dropbox 的新软件销售工具。销售合作伙伴在未知情况下上传了一个受感染的销售工具安装文件版本，随后下载了受感染的文件。

此示例将显示 Palo Alto Networks 防火墙如何与 Advanced WildFire 一起发现最终用户下载的零天恶意软件，即使对通信进行 SSL 加密的情况下也不例外。在 Advanced WildFire 识别出恶意软件后，系统会将日志发送到防火墙，防火墙会向管理员发出警报，而管理员随后会联系用户根除恶意软件。然后，Advanced WildFire 会为恶意软件生成新的签名，之后防火墙会自动下载签名以防止未来的暴露。虽然某些文件共享 Web 站点在上传文件时具有检查文件的防病毒功能，但是这些功能只能防范已知的恶意软件。

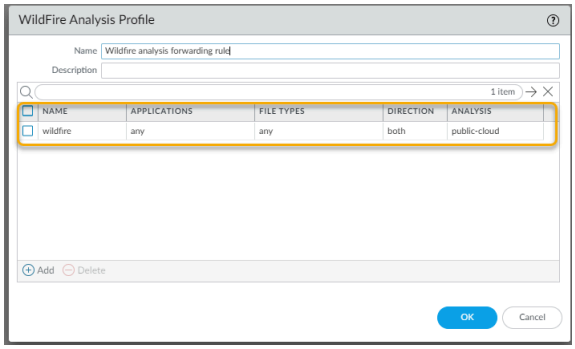
此示例将描述使用了 *SSL* 加密的 *Web* 站点。在此情况下，防火墙已启用解密设置，包括可转发解密内容进行分析的选项。

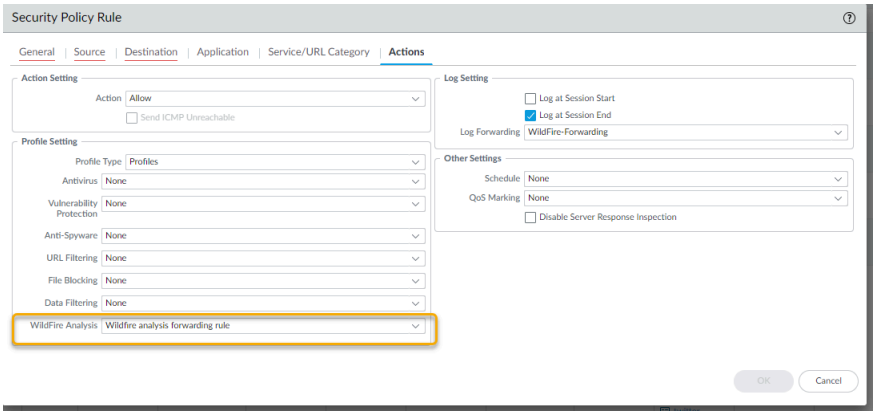
STEP 1 | 合作伙伴公司的销售人员将名为 sales-tool.exe 的销售工具文件上传到其 Dropbox 帐户，然后向 Palo Alto Networks 销售人员发送包含文件链接的电子邮件。

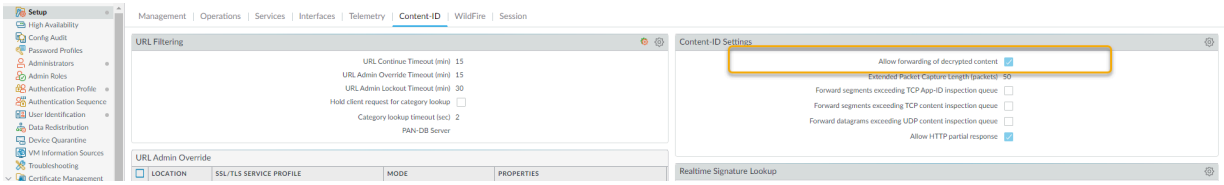
STEP 2 | Palo Alto 销售人员收到来自销售合作伙伴的电子邮件，然后单击下载链接，该链接可引导她访问 Dropbox 站点。她随后单击 **Download**（下载），将文件保存到自己的桌面。

STEP 3 | 保护 Palo Alto 销售代表的防火墙设有附加到安全策略规则的 WildFire 分析配置文件规则，该规则将寻找用于下载或上传任何受支持文件类型的任何应用程序中的文件。此外，还可以将防火墙配置为转发电子邮件链接文件类型，此配置可让防火墙提取 SMTP 和 POP3 电子邮件消息中包含的 HTTP/HTTPS 链接。只要销售代表单击“下载”，防火墙就会将 sales-toole.exe 文件转发到 Advanced WildFire，Advanced WildFire 会分析文件是否有零天恶意软件。即使销售代表是使用 Dropbox（使用 SSL 加密），也可将防火墙配置为解密流量，以便检测所有流

量。下面的屏幕截图显示了 WildFire 分析的配置文件规则、配置有附加 WildFire 分析配置文件规则的安全策略规则，以及允许启用转发加密内容的选项。

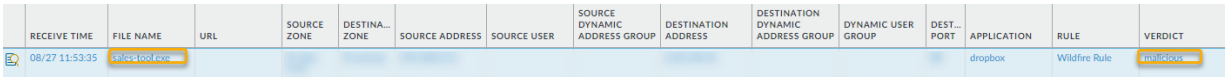






STEP 4 | 此时，Advanced WildFire 已经收到文件，并分析其超过 200 个不同的恶意行为。

STEP 5 | Advanced WildFire 完成文件分析后，它会将包含分析结果的 Advanced WildFire 日志发回防火墙。在此示例中，日志显示该文件是恶意的。



STEP 6 | 使用以下日志转发配置文件配置防火墙：在发现恶意软件时向安全管理员发送警报。

NAME	LOCATION	DESCRIPTION	LOG TYPE	FILTER	PANORAMA	SNMP	EMAIL	SYSLOG	HTTP	QUARANTINE	BUILT-IN ACTIONS
WildFire-Forwarding			threat	(severity eq critical)			WildFire-Forwarding				
			wildfire	(category eq benign)	☐						
			wildfire	(category neq benign) and (category neq malicious)			WildFire-Forwarding				
			wildfire	(category eq malicious)	☐		WildFire-Forwarding				

STEP 7 | 安全管理员按名称识别用户（如果已配置 User-ID）；或者如果未启用 User-ID，则按 IP 地址识别。此时，管理员可断开销售代表使用的网络或 VPN 连接，然后联系桌面支持小组，以便与用户一起检查并清理系统。

通过使用 Advanced WildFire 的详细分析报告，桌面支持人员可查看 Advanced WildFire 分析报告中详述的文件、流程以及详细注册表信息，从而确定用户是否受到恶意软件的感染。如果用户运行恶意软件，则支持人员可尝试手动清理系统或重建系统映像。

FILE INFORMATION

File Type	PE
File Signer	
SHA-256	721b79505757ec7831844795afc4e88c23ce57cd4590118895cbfb86bcd34a77
SHA-1	2e8a6dd285f8fa829918aae60cb1b6172d918437
MD5	c67fdb7887368e41469a1a2556ac30df
File Size	55296 bytes
First Seen Timestamp	2016-12-13 18:39:45 UTC
Sample File	Download File
Verdict	Malware

SESSION INFORMATION

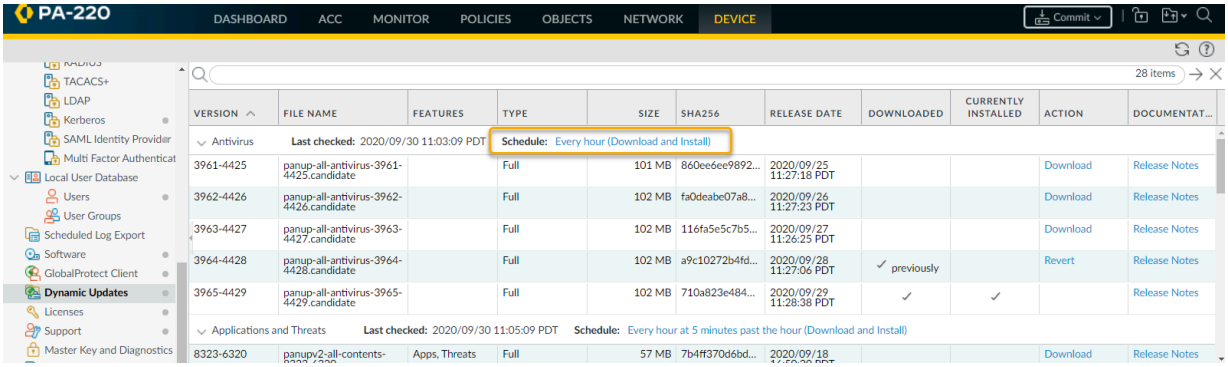
File Source	
File Destination	
User-ID	
Timestamp	2016-12-13 18:39:45 UTC
Serial Number	Manual
Firewall Hostname/IP	
Virtual System	
Application	
URL	
File Name	wildfire-test-pe-file (3).exe
Status	

COVERAGE STATUS

For endpoint antivirus coverage information for this sample, visit VirusTotal

STEP 8 | 既然管理员已识别出恶意软件且正在检查用户系统，那么如何防范以后遭到入侵？答案：在此示例中，管理员在防火墙上设置了一个每 15 分钟下载和安装 Advanced WildFire 签名的计划，同时每天下载和安装一次防病毒更新。当销售代表下载受感染的文件后，在不到一

个半小时的时间内，Advanced WildFire 就会识别出零天恶意软件和生成签名，并将其添加到由 Palo Alto Networks 提供的 Advanced WildFire 更新签名数据库中，防火墙随后即可下载和安装新的签名。此防火墙和配置为下载 Advanced WildFire 和防病毒签名的其他任何 Palo Alto Networks 防火墙现在均可防范此类新发现的恶意软件。以下屏幕截图显示了 Advanced WildFire 更新计划：



大多数防病毒供应商甚至还没有发现零天恶意软件，这一切就已经发生了。在本示例中，在很短的时间内，恶意软件不再被视为零天恶意软件，因为 Palo Alto Networks 已经识别此恶意软件，并且已经向客户提供防范此恶意软件以后入侵的保护。

开始使用 Advanced WildFire

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Advanced WildFire 许可证 对于 *Prisma Access*，凭借 *Prisma Access* 许可证，这通常会包含在内。

以下步骤提供了在防火墙上开始使用 Advanced WildFire™ 的快速工作流程。如果您希望在开始之前了解有关 Advanced WildFire 的更多信息，请查看 Advanced WildFire 概述并查阅 Advanced WildFire 最佳实践。

有关使用 WildFire 私有云或混合云的信息，请参阅 WildFire 设备管理。

如果您在 Prisma Access 上使用 Advanced WildFire，请先熟悉该产品，然后再配置您的 WildFire Analysis 安全配置文件以转发文件以进行 Advanced WildFire 分析。

STEP 1 | 获取 Advanced WildFire 或 WildFire 订阅。如果未购买订阅服务，您仍然可以转发 PE 进行 WildFire 分析。

STEP 2 | 确定以下哪种 Advanced WildFire 部署 适合您：

- Advanced WildFire 公共云 — 转发样本至 Palo Alto Networks 托管的 Advanced WildFire 公共云。
- WildFire 美国Government 云 — 转发样本至 Palo Alto Networks 托管的 WildFire U.S.Government 云。

如果您要部署 *WildFire* 私有云或混合云，请参阅 *WildFire* 设备管理。

STEP 3 | 确认您的许可证在防火墙上处于激活状态。

1. 登录到防火墙。
2. 选择 **Device**（设备） > **Licenses**（许可证），并检查此 WildFire 许可证是否有效。

   如果未显示 WildFire 许可证，请选择 License Management（许可证管理）中的选项来激活许可证。

STEP 4 | 连接防火墙至 WildFire 并配置 WildFire 设置。

1. 选择 **Device**（设备） > **Setup**（设置） > **WildFire**，然后编辑常规设置。
2. 使用 **WildFire Public Cloud**（**WildFire** 公共云）字段将示例转发到 Advanced WildFire 公共云。
3. 定义防火墙转发和配置 WildFire 日志记录和报告设置的文件大小限制。

   Advanced WildFire 最佳实践 是将 *PE* 的 ***File Size***（文件大小）设置为最大 *10 MB*，将其他所有文件类型的 ***File Size***（文件大小）保留默认值。
4. 单击 **OK**（确定）以保存 WildFire General Settings（常规设置）。

STEP 5 | 使防火墙可转发解密后的 SSL 通信来进行 Advanced WildFire 分析。

这是建议的 Advanced WildFire 最佳实践。

STEP 6 | 开始提交样本进行分析。

1. 定义待转发进行 WildFire 分析的流量。（选择 **Objects**（对象） > **Security Profiles**（安全配置文件） > **WildFire Analysis**（**WildFire** 分析），然后修改或 **Add**（添加） WildFire 分析配置文件）。

   作为最佳实践，使用 *WildFire* 分析默认配置文件，确保全面覆盖防火墙允许的流量。如果您仍决定创建自定义的 *WildFire* 分析配置文件，设置配置文件以转发 ***Any***（任何）文件类型——这样可使防火墙自动开始转发新支持的文件类型进行分析。
2. 对于每个配置文件规则，将 **public-cloud** 设置为 **Destination**（目标），以将样本转发到 Advanced WildFire 云进行分析。
3. 将 WildFire 分析配置文件附加到安全策略规则。与策略规则相符的通信被转发以进行 WildFire 分析 （**Policies**（策略） > **Security**（安全性） 并 **Add**（添加） 或修改安全性策略规则）。

STEP 7 | 启用防火墙获得最新的 Advanced WildFire 签名。

实时检索新 Advanced WildFire 签名以检测和识别恶意软件。如果您运行的是 PAN-OS 9.1 或更早版本，您可以每 5 分钟接收一次新签名。

- PAN-OS 9.1 及更早版本
  1. 选择**Device**（设备） > **Dynamic Updates**（动态更新）：
     - 检查 **WildFire** 更新是否显示。
     - 选择 **Check Now**（现在检查）以检索最新的签名更新包。
  2. 设置下载和安装最新 Advanced WildFire 签名的 **Schedule**（计划）。
  3. 使用 **Recurrence**（重复）字段将防火墙检查新更新的频率设置为 **Every Minute**（每分钟）。

     由于会每隔五分钟提供一个新的 *WildFire* 签名，此设置可确保防火墙在一分钟可用性范围内检索这些签名。
  4. 启用防火墙在检索这些更新时 **Download and Install**（下载和安装）它们。
  5. 单击 **OK**（确定）。
- PAN-OS 10.0 及更高版本
  1. 选择**Device**（设备） > **Dynamic Updates**（动态更新）：
  2. 检查 **WildFire** 更新是否显示。
  3. 选择 Schedule（计划）以配置更新频率，然后使用 **Recurrence**（重复）字段配置防火墙以 **Real-time**（实时）检索 WildFire 签名。
  4. 单击 **OK**（确定）。

STEP 8 | 开始扫描通信的威胁，包括 Advanced WildFire 识别的恶意软件。

将 **default**（默认） 防病毒配置文件附加至安全性策略规则，以基于 WildFire 防病毒签名扫描策略允许的通信（选择 **Policies**（策略） > **Security**（安全性） 并添加或修改为规则定义的 **Actions**（操作））。

STEP 9 | 控制站点对被 Advanced WildFire 识别为与恶意或网络钓鱼有关链接网站的访问。

此选项需要 *PAN-DB URL* 筛选许可证。了解 *URL* 筛选的更多详情，以及它如何基于 *URL* 分类让您控制网站访问和企业凭据提交情况（以防止网络钓鱼尝试）。

要配置 URL 筛选：

1. 选择 **Objects**（对象） > **Security Profiles**（安全配置文件） > **URL Filtering**（**URL** 筛选），并 **Add**（添加）或修改 URL 筛选配置文件。
2. 选择 **Categories**（类别）并为网络钓鱼和恶意 URL 类别定义 **Site Access**（网站访问）。
3. **Block**（阻挡）用户访问这些类别中的统一网站，或允许访问，但在用户访问这些类别中的网站时生成 **Alert**（警报），确保您知晓此类事件。
4. 启用凭据网络钓鱼防护，阻止用户提交凭据至不受信任的网站，但不阻挡其对此类网站的访问。
5. 应用新的的或更新的 URL 筛选配置文件，并将其附加至安全策略规则，以将配置文件设置应用至允许的通信中：
    1. 选择 **Policies**（策略） > **Security**（安全），并 **Add**（添加） 或修改安全策略规则。
    2. 选择 **Actions**（操作），然后在配置文件设置部分，将 **Profile Type**（配置文件类型）设置为配置文件。
    3. 将新的或已更新的 **URL Filtering**（**URL** 筛选）配置文件附加到安全策略规则。
    4. 单击 **OK**（确定）以保存安全策略规则。

STEP 10 | 确认防火墙已成功转发样本。

- 如果已启用良性文件的日志记录，请选择 **Monitor**（监控） > **WildFire Submissions**（**WildFire** 提交情况），并检查记录的已提交进行分析的良性文件条目。（如果您希望在确认防火墙已连接至 WildFire 云后禁用良性文件的日志记录，请选择 **Device**（设备） > **Setup**（设置） > **WildFire**，然后清除 **Report Benign Files**（报告良性文件）。
- 的其他选项允许您确认防火墙已转发特定样本，查看防火墙根据文件类型转发的样本，以及查看防火墙转发的样本总数。
- 测试样本恶意软件文件以测试完整的 WildFire 配置。

STEP 11 | 调查分析结果。

- 查找分析结果：
    - 使用防火墙监视恶意软件并查看样本的 WildFire 分析报告。
    - 对于提交至 Advanced WildFire 公共云的所有样本，查看 Advanced WildFire 门户上的报告，包括您手动提交至 WildFire 公共云的样本。
    - 使用 Advanced WildFire API 从 WildFire 设备检索样本判定结果和报告。

STEP 12 | 下一步：

查看并执行 Advanced WildFire 最佳实践。

Advanced WildFire 部署最佳实践

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Advanced WildFire 许可证 对于 *Prisma Access*，凭借 *Prisma Access* 许可证，这通常会包含在内。

以下主题介绍了部署和配置，将其作为您的网络威胁检测和防护解决方案的一部分。

- Advanced WildFire 最佳实践

Advanced WildFire 最佳实践

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Advanced WildFire 许可证 对于 *Prisma Access*，凭借 *Prisma Access* 许可证，这通常会包含在内。

Prisma Access 用户 — 有关用户界面的产品特定信息，请参阅 Prisma Access 文档。

- ❑ 遵循最佳措施以保护您的网络避免第 4 层和第 7 层规避，确保可靠的内容识别和分析。特别是，请确保为 TCP 设置（**Device**（设备） > **Setup**（设置） > **Session**（会话） > **TCP Settings**（设置））和 Content-ID™ 设置（**Device**（设备） > **Setup**（设置） > **Content-ID** > **Content-ID Settings**（**Content-ID** 设置））实施最佳实践。
- ❑ 还要确保您有可用的威胁防护订阅。Advanced WildFire® 和威胁防护共同确保全面的威胁检测和防护。
- ❑ 每日下载、安装内容更新，以接收 Palo Alto Networks 生成的最新产品更新和威胁保护。查看安装内容和软件更新的说明，了解有关更新包中包含的内容的详细信息。
- ❑ 如果您使用的是 PAN-OS 10.0 或更高版本，则需配置您的防火墙以实时检索 Advanced WildFire 签名。这样，只要 Advanced WildFire 公共云能够生成恶意软件签名，就可以立即访问这些新发现的签名，从而通过最大程度缩短您暴露在恶意活动中的时间来防止攻击成功。
- ❑ 如果您将防火墙配置为解密 SSL 流量，则为 WildFire 分析启用防火墙转发解密后的 SSL 通信。只有超级用户才能启用此选项。
- ❑ 使用默认 WildFire 分析配置文件以定义防火墙为进行分析而转发的流量（**Objects**（对象） > **Security Profiles**（安全配置文件） > **WildFire Analysis**（**WildFire** 分析））。默认 WildFire 分

析配置文件确保了对您的安全策略允许的所有流量的完整 WildFire 覆盖——其指定转发以进行 Advanced WildFire 分析的所有应用程序的所有支持文件类型，且无论该文件是上传或下载的。

如果您选择创建自定义 WildFire 分析配置文件，将配置文件设置为转发**any**（任意）文件类型仍是最佳措施。当文件类型支持分析时，这使防火墙能够自动开始转发该文件类型。

有关将 WildFire 分析配置文件应用于防火墙流量的详细信息，请查看如何转发文件以进行 Advanced WildFire 分析。

如果流量生成的 *Advanced WildFire* 签名会导致重置或丢弃操作，那么防病毒软件配置文件内的 *WildFire* 操作设置可能会影响该流量。您可以排除诸如软件分发应用程序等内部流量，并由此部署定制程序以安全 转换 至最佳实践，因为 *Advanced WildFire* 可能将定制程序识别为恶意软件并为其生成签名。检查 ***Monitor***（监控）> ***Logs***（日志）> ***WildFire Submissions***（***WildFire*** 提交情况）以查看是否有任何内部定制程序触发 *Advanced WildFire* 签名。

- 将防火墙配置为转发文件以进行 Advanced WildFire 分析时，请查看所有受支持的文件类型的文件大小限制。将所有文件类型的 **Size Limit**（大小限制） 设置为默认限制。（选择 **Device**（设备）> **Setup**（设置）> **WildFire** 并编辑常规设置以根据文件类型调整文件尺寸限制。您可以查看帮助信息，以查找每种文件类型的默认大小限制）。

  关于 **WildFire** 转发的默认文件尺寸限制

  防火墙的默认文件尺寸限制旨在包含自由环境下的大部分恶意软件（此类软件通常小于默认尺寸限制），并排除极不可能是恶意软件的大文件，大文件可对 WildFire 转发容量造成影响。由于防火墙有特定的、用于转发 Advanced WildFire 分析用文件的预留容量，转发大量大文件可能导致防火墙跳过部分文件的转发。当某个文件类型以配置的最大文件尺寸限制在防火墙上高速率转发时，会出现此情况。这种情况下，潜在的恶意文件可能未被转发以供 Advanced WildFire

分析。当您想要增加 PE 文件以外的其他文件至超出其默认尺寸限制时，需要考虑到这种可能性。

下图是恶意软件文件尺寸分布的代表图，Palo Alto Networks 威胁研究团队以此图划分文件尺寸。您可以将防火墙默认文件尺寸设置增加至最大文件尺寸设置，以在各文件类型的恶意软件捕获率方面获得相对较小的提升。

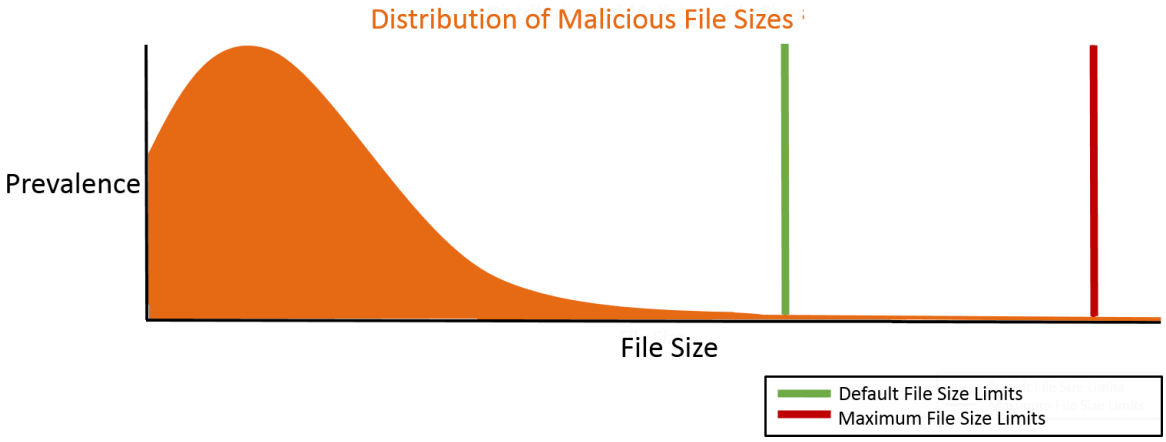


图 **1:** 捕获非常见大恶意文件的建议文件尺寸限制

如果您对非常见大恶意文件存在顾虑，那么您可能会想要增大文件尺寸限制至超过默认设置。在这种情况下，建议采用下列设置以捕获罕见、较大的恶意文件。

选择 **Device**（设备） > **Setup**（设置） > **WildFire** 并编辑常规设置以根据各文件类型调整 **Size Limit**（尺寸限制）：

文件类型	**PAN-OS 9.0** 及更高版本文件转发最大尺寸建议	**PAN-OS 8.1** 文件转发最大尺寸建议
pe	16MB	10MB
apk	10MB	10MB
pdf	3,072KB	1,000KB
ms-office	16,384KB	2,000KB
jar	5MB	5MB
flash	5MB	5MB
MacOSX	10MB	1MB
archive	50MB	10MB
linux	50MB	10MB
script	20KB	20KB

配置 Advanced WildFire 分析

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Advanced WildFire 许可证 对于 *Prisma Access*，凭借 *Prisma Access* 许可证，这通常会包含在内。

以下主题介绍如何在网络部署中启用 Advanced WildFire™ 分析。您可设置 Palo Alto Networks 防火墙将未知文件自动转发至 Advanced WildFire 公共云或 WildFire 专有云，同时您也可使用 Advanced WildFire 门户来手动提交文件进行分析。为分析提交的样本将收到一份判定结果，判定其为良性、灰色软件、恶意软件或网络钓鱼，同时也会对每个样本生成一份详细的分析报告。

- 转发文件以进行 Advanced WildFire 分析
- 转发解密后的 SSL 流量以进行 Advanced WildFire 分析
- 启用 Advanced WildFire 内联机器学习
- 启用 Advanced WildFire Inline Cloud Analysis
- 启用保持模式以进行实时签名查找
- 验证 WildFire 提交情况
- 手动上传文件至 WildFire 门户
- 基于型号的防火墙文件转发容量

转发文件以进行 Advanced WildFire 分析

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Advanced WildFire 许可证 对于 *Prisma Access*，凭借 *Prisma Access* 许可证，这通常会包含在内。

配置 Palo Alto Networks 防火墙以转发未知文件或电子邮件链接，并阻挡匹配现有防病毒签名的文件以进行分析。使用 **WildFire Analysis**（**WildFire** 分析）配置文件，定义将文件转发至 Advanced WildFire 公共云选项之一，然后再将配置文件附加至安全规则，以便触发针对零日恶意软件进行的检查。

根据使用中的应用程序、检测到的文件类型、电子邮件消息中包含的链接，或样本传输方向（上传、下载或二者皆有），指定待转发进行分析的流量。例如，您可设置防火墙以转发可移植可执行文件 (PE)，或用户在 Web 浏览会话期间尝试下载的任何文件。除了未知样本外，防火墙还转发匹配现有防病毒前面的已阻挡文件。根据签名已成功阻止，但之前未见过的恶意软件变体，这为 Palo Alto Networks 提供了有价值的威胁情报来源。

如果您正在使用 WildFire 设备来托管 WildFire 专有云，则您可将 WildFire 分析资源扩展至 WildFire 混合云，具体操作为：配置防火墙以继续将敏感文件转发至您的 WildFire 专有云进行本地分析，而将敏感性相对较低的文件或不受支持的文件转发至 WildFire 公共云。有关使用和配置 WildFire 设备的更多信息，请参阅 WildFire 设备管理。

准备工作：

- Advanced WildFire 云区域之间的文件分析支持可能略有不同。有关详细信息，请参阅文件类型支持。
- 如果在您正配置将文件转发到的防火墙与 Advanced WildFire 云之间存在防火墙，请确保处于中间位置的防火墙可允许以下端口：

端口	使用情况
443	注册、PCAP 下载、样本下载、报告检索、文件提交、PDF 报告下载
10443	动态更新

- Strata Cloud Manager
- PAN-OS 和 Panorama

转发文件以进行 Advanced WildFire 分析 (Cloud Management)

如果您使用 ***Panorama*** 来管理 ***Prisma Access***：

切换到 ***PAN-OS*** 选项卡并遵循相应的指导。

如果你使用 ***Prisma Access*** 云管理，请在这里继续。

STEP 1 | 指定要将样本转发到的 Advanced WildFire 云。

选择 **Manage**（管理） > **Configuration**（配置） > **NGFW** 和 **Prisma Access** > **Security Services**（安全服务） > **WildFire and Antivirus**（**WildFire** 和 **Antivirus**） > **General Settings**（常规设置），并根据您的 WildFire 云部署（公共、政府、私有或混合）编辑常规设置。

WildFire U.S.Government 云作为可选分析环境，仅供美国联邦政府机构使用。

添加云环境的 **WildFire Cloud**URL 以转发样本来进行分析。

Advanced WildFire 公共云选项：

1. 输入 **WildFire Public Cloud**（**WildFire** 公共云） URL：
   - 美国：**wildfire.paloaltonetworks.com**
   - 欧洲：**eu.wildfire.paloaltonetworks.com**
   - 日本：**jp.wildfire.paloaltonetworks.com**
   - 新加坡：**sg.wildfire.paloaltonetworks.com**
   - 英国：**uk.wildfire.paloaltonetworks.com**
   - 加拿大：**ca.wildfire.paloaltonetworks.com**
   - 澳大利亚：**au.wildfire.paloaltonetworks.com**
   - 德国：**de.wildfire.paloaltonetworks.com**
   - 印度：**in.wildfire.paloaltonetworks.com**
   - 瑞士：**ch.wildfire.paloaltonetworks.com**
   - 波兰：**pl.wildfire.paloaltonetworks.com**
   - 印度尼西亚：**id.wildfire.paloaltonetworks.com**
   - 中国台湾：**tw.wildfire.paloaltonetworks.com**
   - 法国：**fr.wildfire.paloaltonetworks.com**
   - 卡塔尔：**qatar.wildfire.paloaltonetworks.com**

- 韩国：**kr.wildfire.paloaltonetworks.com**
- 以色列：**il.wildfire.paloaltonetworks.com**
- 沙特阿拉伯：**sa.wildfire.paloaltonetworks.com**
- 西班牙：**es.wildfire.paloaltonetworks.com**

2. 确保 **WildFire Private Cloud**（**WildFire** 专有云）字段已清空。

WildFire FedRAMP 云选项：

1. 输入 **WildFire FedRAMP Cloud**（**WildFire FedRAMP** 云）URL：
   - U.S.Government 云：**wildfire.gov.paloaltonetworks.com**
   - Advanced WildFire Government 云：gov-cloud.wildfire.paloaltonetworks.com
   - Advanced WildFire Public Sector 云：pubsec-cloud.wildfire.paloaltonetworks.com
2. 确保 **WildFire Private Cloud**（**WildFire** 专有云）字段已清空。

STEP 2 | 通过选择 **Allow Forwarding of Decrypted Content**（允许转发解密内容），启用 Prisma Access 来转发解密的 SSL 流量，以便进行 Advanced WildFire 分析。根据安全策略规则评估解密的流量；如果它与附加到安全规则的 WildFire 分析配置文件匹配，则解密的流量将在重新加密之前转发以进行分析。

转发解密的 *SSL* 通信进行分析是 *Advanced WildFire* 最佳实践。

STEP 3 | 定义 Prisma Access 转发以进行分析的样本的大小限制。

将文件转发值设置为默认设置是 Advanced WildFire 最佳实践。

STEP 4 | 配置提交日志设置。

1. 选择 **Report Benign Files**（报告良性文件），以对收到良性判定结果的文件进行记录。
2. 选择 **Report Grayware Files**（报告灰色软件文件），以对收到灰色软件判定结果的文件进行记录。

STEP 5 | 完成后，**Save**（保存）您的更改。

STEP 6 | 定义要转发以进行分析的流量。

1. 选择 **Manage**（管理） > **Configuration**（配置） > **NGFW** 和 **Prisma Access** > **Security Services**（安全服务） > **WildFire and Antivirus**（**WildFire** 和 **Antivirus**），然后 **Add Profile**（添加配置文件）。提供配置文件的 **Name**（名称）和 **Description**（说明）。
2. **Add Rule**（添加规则）以定义待转发进行分析的流量，然后再为此规则输入描述性 **Name**（名称），如 local-PDF-analysis。
3. 定义配置文件规则，以匹配未知流量并根据以下几个方面进行样本转发：
   - **Direction of Traffic**（流量方向）— 根据文件的传输方向（**Upload**（上传）、**Download**（下载）或 **Upload and Download**（上传和下载））转发文件以进行分析。例如，选择 **Upload and Download**（上传和下载），即可转发所有未知 PDF 进行分析，不论其传输方向如何。
   - **Applications**（应用程序） — 根据正在使用的应用程序，转发文件进行分析。
   - **File Types**（文件类型） — 根据文件类型来转发文件进行分析，包括在电子邮件消息中包含的链接。例如，选择 **PDF**，即可转发防火墙检测到的未知 PDF 进行分析。
   - 选择要转发的流量以进行分析的目的地。
     - 选择 **Public Cloud**（公共云），以使与规则匹配的所有流量转发到 Advanced WildFire 公共云进行分析。
     - 选择 **Private Cloud**（私有云），以使与规则匹配的所有流量转发到 WildFire 设备进行分析。
     - 完成后 **Save**（保存）WildFire 分析转发规则。
4. **Save**（保存） WildFire 和防病毒安全配置文件。

STEP 7 | 启用 WildFire 和防病毒安全配置文件。

安全策略规则允许的流量根据附加的 WildFire 分析配置文件进行评估；Prisma Access 转发与 WildFire 分析的配置文件匹配的流量。

STEP 8 | 推送配置更改。

STEP 9 | （可选） 启用 Advanced WildFire 内联机器学习

STEP 10 | 选择下一步...

- 验证 WildFire 提交情况，确认防火墙是否已成功转发文件进行分析。
- 监控 WildFire 活动以评估警报，并报告恶意软件的详细信息。

转发文件以进行 Advanced WildFire 分析（PAN-OS 和 Panorama）

STEP 1 | （仅适用于 PA-7000 系列防火墙）如需启用 PA-7000 系列防火墙，以便转发样本来进行分析，必须先将 NPC 上的数据端口配置为日志卡接口。如果您的 PA-7000 系列设备配备了

LFC（日志转发卡），则必须配置 LFC 使用的端口。配置后，在转发样本时，日志卡端口或 LFC 接口优先于管理端口。

STEP 2 | 指定要将样本转发到的 Advanced WildFire 部署。

选择 **Device**（设备） > **Setup**（设置） > **WildFire** 并根据您的 WildFire 云部署编辑常规设置（公共、政府、专有或混合）。

WildFire 美国*Government* 云作为可选分析环境，仅供美国联邦政府机构使用。

Advanced WildFire 公共云

1. 输入 **WildFire Public Cloud**（**WildFire** 公共云） URL：
   - 美国：**wildfire.paloaltonetworks.com**
   - 欧洲：**eu.wildfire.paloaltonetworks.com**
   - 日本：**jp.wildfire.paloaltonetworks.com**
   - 新加坡：**sg.wildfire.paloaltonetworks.com**
   - 英国：**uk.wildfire.paloaltonetworks.com**
   - 加拿大：**ca.wildfire.paloaltonetworks.com**
   - 澳大利亚：**au.wildfire.paloaltonetworks.com**
   - 德国：**de.wildfire.paloaltonetworks.com**
   - 印度：**in.wildfire.paloaltonetworks.com**
   - 瑞士：**ch.wildfire.paloaltonetworks.com**
   - 波兰：**pl.wildfire.paloaltonetworks.com**
   - 印度尼西亚：**id.wildfire.paloaltonetworks.com**
   - 中国台湾：**tw.wildfire.paloaltonetworks.com**
   - 法国：**fr.wildfire.paloaltonetworks.com**
   - 卡塔尔：**qatar.wildfire.paloaltonetworks.com**
   - 韩国：**kr.wildfire.paloaltonetworks.com**
   - 以色列：**il.wildfire.paloaltonetworks.com**
   - 沙特阿拉伯：**sa.wildfire.paloaltonetworks.com**
   - 西班牙：**es.wildfire.paloaltonetworks.com**
2. 确保 **WildFire Private Cloud**（**WildFire** 专有云）字段已清空。

WildFire FedRAMP 云选项：

1. 输入 **WildFire FedRAMP Cloud**（**WildFire FedRAMP** 云）URL：
   - 美国Government 云：**wildfire.gov.paloaltonetworks.com**
   - Advanced WildFire Government 云：gov-cloud.wildfire.paloaltonetworks.com
   - Advanced WildFire Public Sector 云：pubsec-cloud.wildfire.paloaltonetworks.com

2. 确保 **WildFire Private Cloud**（**WildFire** 专有云）字段已清空。

STEP 3 | 定义防火墙转发的文件的大小限制，并配置日志记录和报告设置。

继续编辑常规设置（**Device**（设备） > **Setup**（设置） > **WildFire**）。

- 查看从防火墙转发文件的 **File Size Limits**（文件大小限制）。

  Advanced WildFire 最佳实践 是将 *PE* 的 ***File Size***（文件大小）设置为最大 *10 MB*，将其他所有文件类型的 ***File Size***（文件大小）保留默认值。

- 选择 **Report Benign Files**（报告良性文件），以对收到良性判定结果的文件进行记录。
- 选择 **Report Grayware Files**（报告灰色软件文件），以对收到灰色软件判定结果的文件进行记录。
- 通过编辑会话信息设置，定义 WildFire 分析报告中记录的会话信息。在默认情况下，所有会话信息均将显示在 WildFire 分析报告中。取消选中复选框，以从 WildFire 分析报告中删除相应的字段，然后单击 **OK**（确认）保存设置。

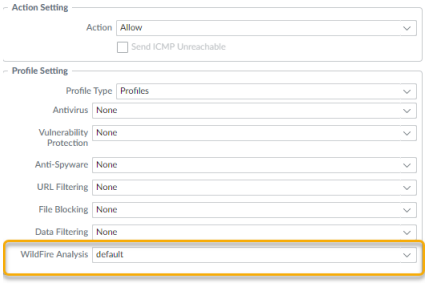
STEP 4 | 定义要转发以进行分析的流量。

1. 选择 **Objects**（对象） > **Security Profiles**（安全性配置文件） > **WildFire Analysis**（**WildFire** 分析），**Add**（添加） 新的 WildFire 分析配置文件，再为其输入描述性 **Name**（名称）。
2. **Add**（添加）配置文件规则，以定义待转发进行分析的流量，然后再为此规则输入描述性**Name**（名称），如 local-PDF-analysis。
3. 定义配置文件规则，以匹配未知流量并根据以下几个方面进行样本转发：
   - **Applications**（应用程序） — 根据正在使用的应用程序，转发文件进行分析。
   - **File Types**（文件类型） — 根据文件类型来转发文件进行分析，包括在电子邮件消息中包含的链接。例如，选择 **PDF**，即可转发防火墙检测到的未知 PDF 进行分析。
   - **Direction**（方向） — 根据文件传输方向（上传、下载或二者皆有），转发文件进行分析。例如，选择 **both**（皆有），即可转发所有未知 PDF 进行分析，不论其传输方向如何。
4. 单击 **OK**（确定）以保存 WildFire 分析配置文件。

STEP 5 | 将 WildFire 分析配置文件附加至安全策略规则。

安全策略规则允许的流量将根据附加的 WildFire 分析配置文件予以评估，防火墙将转发与该配置文件相匹配的流量来进行 WildFire 分析。

1. 选择 **Policies**（策略） > **Security**（安全性），然后**Add** （添加） 或修改策略规则。
2. 单击策略规则中的 **Actions**（操作）选项卡。
3. 在 Profile Settings（配置文件设置）部分中，选择作为 **Profile Type**（配置文件类型）的 **Profiles**（配置文件），然后选择 **WildFire Analysis**（**WildFire** 分析）配置文件以附加至策略规则



STEP 6 | 确保启用防火墙以同时转发解密后的 SSL 通信来进行 Advanced WildFire 分析。

这是建议的最佳做法。

STEP 7 | （可选） 启用 Advanced WildFire 内联机器学习

STEP 8 | （可选） 启用保持模式以进行实时签名查找

STEP 9 | 查看并执行 Advanced WildFire 最佳实践。

STEP 10 | 单击 **Commit**（提交）以应用更新的设置。

STEP 11 | （可选） 安装设备证书以更新到防火墙用于与 Palo Alto Networks 云服务通信的最新版本的证书。

STEP 12 | （可选） 配置 Content Cloud FQDN 设置。

STEP 13 | 选择下一步...

- 验证 WildFire 提交情况，确认防火墙是否已成功转发文件进行分析。
- 监控 WildFire 活动以评估警报，并报告恶意软件的详细信息。

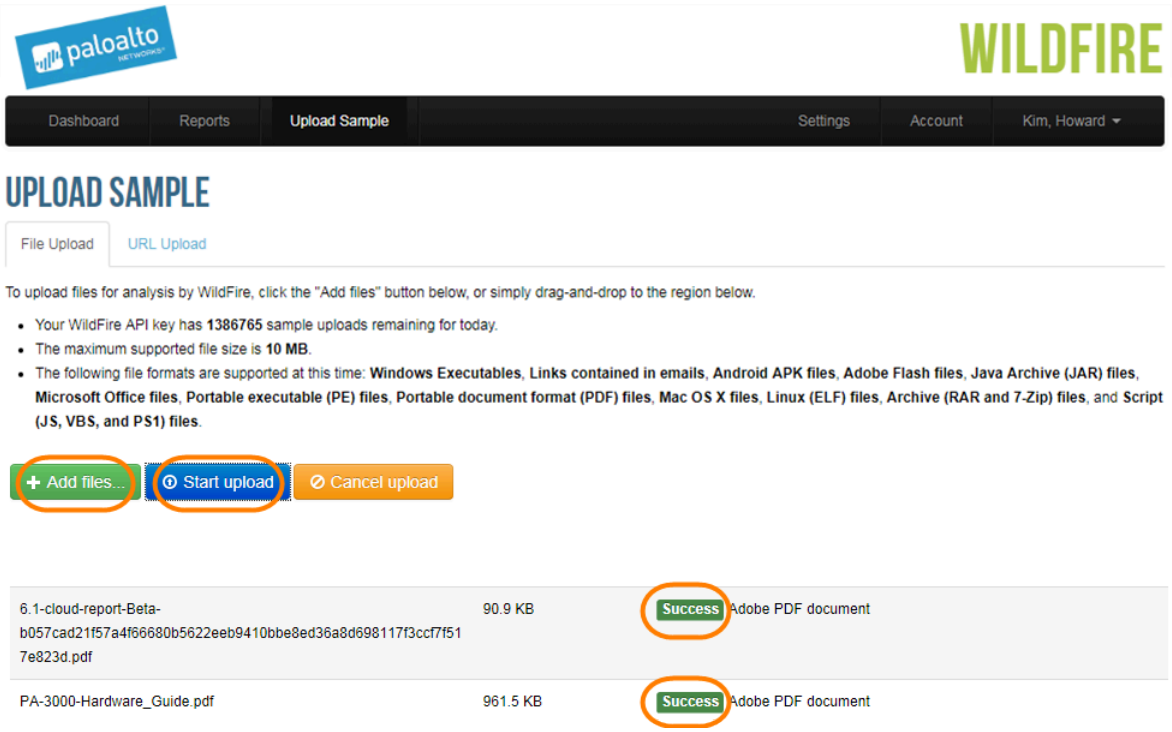
手动上传文件至 WildFire 门户

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Advanced WildFire 许可证 对于 *Prisma Access*，凭借 *Prisma Access* 许可证，这通常会包含在内。

所有拥有支持帐户的 Palo Alto Networks 用户均可使用 Palo Alto Networks WildFire 门户来手动提交样本进行分析，且每天最多可提交五份样本。如果您订阅了 Advanced WildFire，可以手动将样本提交至门户，每天最多可上传 1000 份样本；但是，请记住每天 1000 份样本的限制也包括 WildFire API 提交情况。

STEP 1 | 手动上传文件或 URL 至 WildFire 门户进行分析。

1. 登录到 WildFire 门户。
2. 单击菜单栏上的 **Upload Sample**（上传样本）。
   - 要提交文件进行分析，请选择 **File Upload**（文件上传）并 **Open**（打开）您想要上传以进行分析的文件。单击 **Start**（开始）以开始单个文件的分析，或单击 **Start Upload**（开始上传）以提交您添加的所有进行分析的文件。
   - 要提交 URL 进行分析，单击 **URL Upload**（**URL** 上传），输入 URL，然后 **Submit**（提交）以进行分析。



3. 关闭 **Uploaded File Information**（已上传文件信息）弹出窗口。

STEP 2 | 查看文件的判断和分析结果。

请等待至少 5 分钟，以便 Advanced WildFire 分析样本。

由于手动上传与特定的防火墙无关，所以手动上传不会在报告中显示会话信息。

1. 返回 WildFire 门户仪表盘。
2. 在 Previous 1 Hour（之前 1 小时）区域，在来源栏下方选择 **Manual**（手动）以查看最近手动提交的样本的分析信息。
3. 找到您上传的文件或 URL，并单击 Received Time（接收时间）左侧的详细信息图标。

转发解密后的 SSL 流量以进行 Advanced WildFire 分析

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Advanced WildFire 许可证 对于 *Prisma Access*，凭借 *Prisma Access* 许可证，这通常会包含在内。

使防火墙可转发解密后的 SSL 通信来进行 Advanced WildFire 分析。防火墙解密的通信根据安全性策略规则进行评估；如果其符合安全性规则附加的 WildFire 分析配置文件，则在防火墙重新加密之前，该解密的通信被转发以进行分析。只有超级用户才能启用此选项。

转发解密的 *SSL* 流量进行分析是Advanced WildFire 最佳实践。

在没有启用多个虚拟系统的防火墙上：

1. 如果尚未启用，请启用防火墙以执行解密和转发文件以进行 Advanced WildFire 分析。
2. 选择 **Device**（设备） > **Setup**（设置） > **Content - ID**（内容 **ID**）。
3. 编辑内容 ID 设置，然后 **Allow Forwarding of Decrypted Content**（允许转发解密内容）。
4. 单击 **OK**（确定）保存更改。

在启用虚拟系统的防火墙上：

1. 如果尚未启用解密，请启用解密和转发文件以进行 Advanced WildFire 分析。
2. 选择 **Device**（设备） > **Virtual Systems**（虚拟系统），单击要修改的虚拟系统，然后 **Allow Forwarding of Decrypted Content**（允许转发解密内容）。

对于 Prisma Access，这是作为 **WildFire and Antivirus**（**WildFire** 和 **Antivirus**）安全配置文件设置的一部分进行配置的。有关详细信息，请参阅有关 Prisma Access 的转发文件以进行 Advanced WildFire 分析。

启用 Advanced WildFire Inline Cloud Analysis

在何处可以使用？	需要提供什么？
• NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Advanced WildFire 许可证

Palo Alto Networks Advanced WildFire 运行一系列基于云的 ML 检测引擎，这些引擎提供对遍历网络的 PE（可移植可执行文件）文件的内联分析，以实时检测和防止高级恶意软件。与 WildFire 检测到其他恶意内容一样，Advanced WildFire Inline Cloud Analysis 检测到威胁时会生成一个签名，然后通过更新包分发给客户，从而在未来为所有 Palo Alto Networks 客户提供防御。

基于云的引擎能够检测未曾见过的恶意软件（例如，Palo Alto Networks 零日恶意软件 - 以前在外部环境中从未见过，或 Palo Alto Networks 从未检测到过的恶意软件）并阻止其进入您的环境。Advanced WildFire Inline Cloud Analysis 在防火墙上使用轻量级转发机制，以最大限度减少对性能的影响。基于云的 ML 模型可以无缝更新，以应对不断变化的威胁形势，而无需内容更新或功能发布支持。

Advanced WildFire Inline Cloud Analysis 通过 WildFire Analysis 配置文件启用和配置，需要具有有效的 Advanced WildFire 许可证的 PAN-OS 11.1 或更高版本。

STEP 1 | 安装更新的防火墙设备证书，以用于向 Advanced WildFire 云分析服务进行身份验证。对为内联云分析启用的所有防火墙重复此操作。

如果您已在防火墙上安装当前版本的设备证书，则无需执行此步骤。

STEP 2 | 登录 PAN-OS Web 界面。

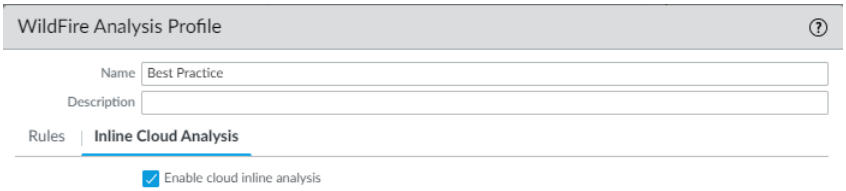
STEP 3 | 要启用 Advanced WildFire Inline Cloud Analysis，您必须拥有有效的 Advanced WildFire 订阅。有关详细信息，请参阅：许可、注册和激活。

要检查您是否拥有当前有效的许可证订阅，请选择 **Device**（设备） > **Licenses**（许可证），确认是否有相应的许可证以及许可证是否过期。

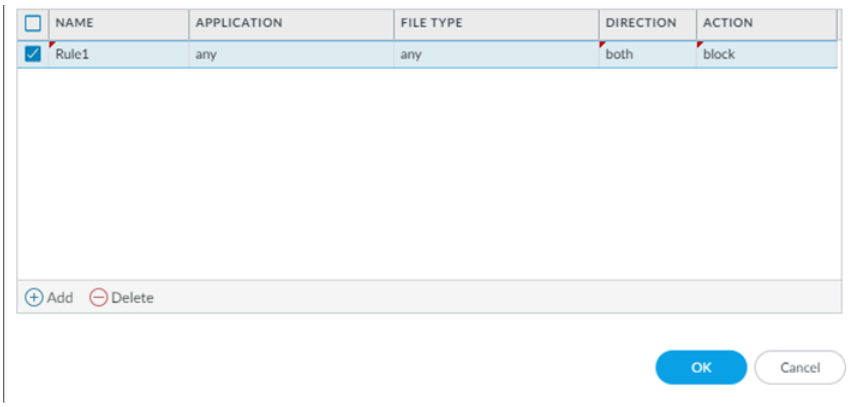
如果您当前的 *WildFire* 许可证已过期，并且您正在安装 *Advanced WildFire* 许可证，则必须先从 *NGFW* 中删除 *WildFire* 许可证，然后再安装 *Advanced WildFire* 许可证。

STEP 4 | 更新或创建新的 WildFire Analysis 安全配置文件以启用 Advanced WildFire Inline Cloud Analysis。

1. 选择现有 **WildFire Analysis Profile**（**WildFire Analysis** 配置文件）或 **Add**（添加）新配置文件（**Objects**（对象） > **Security Profiles**（安全配置文件） > **WildFire Analysis**）。
2. 选择您的 WildFire Analysis 配置文件，然后转到 **Inline Cloud Analysis**（内联云分析）并 **Enable cloud inline analysis**（启用云内联分析）。



3. 指定一条规则，定义 Advanced WildFire Inline Cloud Analysis 检测到高级恶意软件时要采取的操作。



- 输入添加到配置文件的所有规则的描述性名称（最多 31 个字符）。
- 应用程序 — 添加要匹配的应用程序流量，规则针对该流量定义要管控的 Inline Cloud ML 操作。
- 文件类型 — 选择要在为规则定义的分析目标处分析的文件类型。

  目前仅支持 *PE*（可移植可执行文件）。

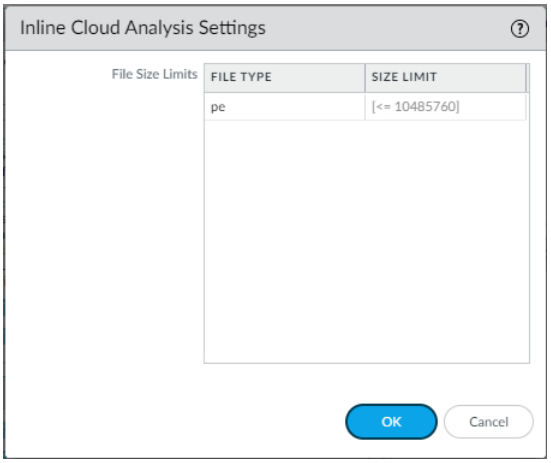
- 方向 — 根据传输方向将规则应用于流量。您可以应用该规则来下载流量。
- 操作 — 配置使用 Advanced WildFire Inline Cloud Analysis 检测到威胁时要采取的操作。您可以允许要继续发送到目标的应用程序流量，或者阻止来自“源”或“源-目标”的流量。

  Palo Alto Networks 建议将操作设置为“阻止”以获得最佳安全性。

4. 点击确定以退出 WildFire Analysis Profile 配置对话框。

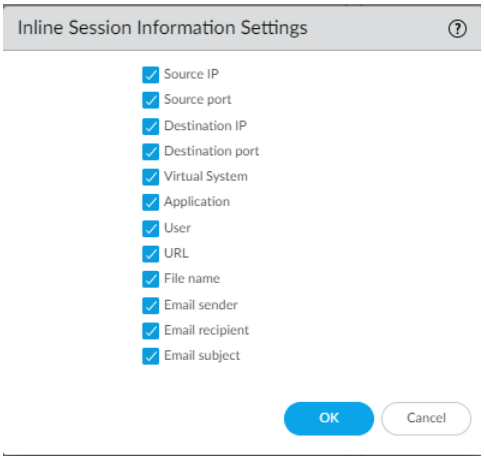
STEP 5 | 使用 Advanced WildFire Inline Cloud Analysis 查看可转发以进行分析的最大文件大小。

Advanced WildFire Inline Cloud Analysis 提供快速的 *WildFire* 判定，但是，只有在样本经过完整的动态分析后才能获得恶意样本的完整报告，这可能需要长达 *30* 分钟。



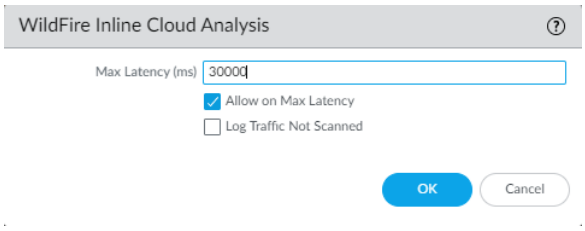
1. 选择 **Device**（设备） > **Setup**（设置） > **WildFire** > **Inline Cloud Analysis Settings**（**Inline Cloud Analysis** 设置）并审核文件大小限制。
2. 单击 **OK**（确定） 以确认您的更改。

STEP 6 | 指定防火墙转发的有关指定样本的网络会话信息。Palo Alto Networks 使用会话信息以了解可以网络事件的内容，与恶意软件相关破坏的指示、受影响的主机和客户端，以及用于传播恶意软件的应用程序。默认情况下，这些选项处于启用状态。



1. 选择 **Device**（设备） > **Setup**（设置） > **WildFire** > **Inline Session Information Settings**（内联会话信息社会自），然后根据需要选择或清除选项。
   - **Source IP**（源 **IP**）— 转发发送未知文件的源 IP 地址。
   - **Source Port**（源端口）— 转发发送未知文件的源端口。
   - **Destination IP**（目标 **IP**）— 转发未知文件的目标 IP 地址。
   - **Destination Port**（目标端口）— 转发未知文件的目标端口。
   - **Virtual System**（虚拟系统）— 转发检测未知文件的虚拟系统。
   - **Application**（应用程序）— 转发传输未知文件的用户应用程序。
   - **User**（用户）— 转发目标用户。
   - **URL** — 转发与未知文件关联的 URL。
   - **Filename**（文件名）— 转发未知文件的文件名。
   - **Email sender**（电子邮件发件人）— 转发未知电子邮件链接的发件人（该电子邮件发件人的名称也显示在 WildFire 日志和报告中）。
   - **Email sender**（电子邮件收件人）— 转发未知电子邮件链接的收件人（该电子邮件收件人的名称也显示在 WildFire 日志和报告中）。
   - **Email subject**（电子邮件主题）— 转发未知电子邮件链接的主题（该电子邮件主题也显示在 WildFire 日志和报告中）。
2. 单击 **OK**（确定） 以确认您的更改。

STEP 7 | 配置超时延迟和请求超过最大延迟时要采取的操作。

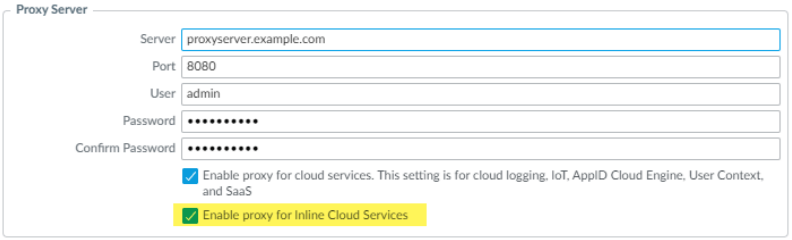


1. 指定当达到 Advanced WildFire Inline Cloud Analysis 请求的延迟限制时要采取的操作：
   - 最大延迟（毫秒）— 指定 Advanced WildFire Inline Cloud Analysis 返回结果的最大可接受处理时间（以毫秒为单位）。
   - 达到最大延迟时允许 — 允许防火墙在达到最大延迟时执行允许操作。取消选择此选项会将防火墙操作设置为“阻止”。
   - 记录未扫描的流量 — 使防火墙能够记录显示存在高级恶意软件但尚未由 Advanced WildFire 云处理的 Advanced WildFire Inline Cloud Analysis 请求。
2. 单击 **OK**（确定） 以确认您的更改。

STEP 8 | （使用显式代理服务器部署防火墙时需要）配置用于访问服务器的代理服务器，以便所有配置的内联云分析功能生成请求。可指定单个代理服务器，并将其应用于所有 Palo Alto Networks 更新服务，包括所有已配置的内联云和日志记录服务。

1. （PAN-OS 11.2.3 及更高版本）通过 PAN-OS 配置代理服务器。
   1. 选择 **Device**（设备） > **Setup**（设置） > **Services**（服务），然后编辑 **Services**（服务）详细信息。
   2. 指定 **Proxy Server**（代理服务器）设置并 **Enable proxy for Inline Cloud Services**（为 **Inline Cloud Services** 启用代理）。您可以在 **Server**（服务器）字段中提供 IP 地址或 FQDN。

      代理服务器密码必须至少包含 *6* 个字符。

   3. 单击 **OK**（确定）。
2. （PAN-OS 11.1.5 及更高版本）通过防火墙 CLI 配置代理服务器。
   1. 访问防火墙 CLI。
   2. 使用以下 CLI 命令配置基本代理服务器设置：

      ```
      set deviceconfig system secure-proxy-server <FQDN_or_IP>
       set deviceconfig system secure-proxy-port <1-65535>
      ```

```
set deviceconfig system secure-proxy-user <value> set
deviceconfig system secure-proxy-password <value>
```

代理服务器密码必须至少包含 *6* 个字符。

3. 启用代理服务器以使用以下 CLI 命令将请求发送到内联云服务服务器：

```
debug dataplane mica set inline-cloud-proxy enable
```

4. 使用以下 CLI 命令查看内联云服务的当前代理支持运行状态：

```
debug dataplane mica show inline-cloud-proxy
```

例如：

```
debug dataplane mica show inline-cloud-proxy Proxy for
 Advanced Services is Disabled
```

STEP 9 | （推荐）将防火墙配置为在防火墙因检测到恶意活动而终止原始会话后，禁止客户端获取文件的一部分并随后启动新会话来获取文件的其余部分。当 Web 浏览器实现 HTTP Range 选项时，会发生这种情况。启用 **Allow HTTP partial response**（允许 **HTTP** 部分响应）以提供最大可用性，但这也可能会增加网络攻击成功的风险。Palo Alto Networks 建议禁用 **Allow HTTP partial response**（允许 **HTTP** 部分响应），以获得最大的安全性。

Allow HTTP partial response（允许 ***HTTP*** 部分响应）是一项全局设置，会影响使用 *RANGE* 标头的基于 *HTTP* 的数据传输，这可能会导致某些应用程序出现服务异常。禁用 ***Allow HTTP Partial Response***（允许 ***HTTP*** 部分响应）后，请验证业务关键型应用程序的操作。

1. 选择 **Device**（设备） > **Setup**（设置） > **Content-ID** > **Content-ID Settings**（**Content-ID** 设置）。
2. 取消选择 **Allow HTTP Partial Response**（允许 **HTTP** 部分响应），然后单击 **OK**（确定）。

STEP 10 | **Commit**（提交）更改。

STEP 11 | （可选） 配置 Content Cloud FQDN 设置。

启用 Advanced WildFire 内联机器学习

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Advanced WildFire 许可证 对于 *Prisma Access*，凭借 *Prisma Access* 许可证，这通常会包含在内。

您可以在防火墙数据平面使用机器学习 (ML)，从而实时防止可移植可执行文件和 PowerShell 脚本的恶意软件变体进入您的网络。借助在安全平台上使用的 WildFire® 云分析技术，Advanced WildFire 内联机器学习可通过评估不同文件的详细信息（包括解码器字段和模式），动态检测特定类型的恶意文件，从而实现文件的高识别率。这种保护可扩展至当前已知以及未来可能会发生变化、与 Palo Alto Networks 识别为恶意的特征相匹配的威胁。Advanced WildFire inline 机器学习将执行您现有的防病毒配置文件保护配置。此外，您还可以指定文件哈希例外以排除遇到的误报情况，这能使您创建更加精确的规则，从而支持您特定的安全需求。

要启用 Advanced WildFire Inline ML，您必须拥有有效的 Advanced WildFire 或 WildFire 订阅，创建（或修改）Antivirus（或用于 Prisma Access 的 WildFire 和 Antivirus）安全配置文件以配置和启用该服务，然后将 Antivirus 配置文件附加到安全策略规则。

VM-50 或 *VM50L* 虚拟设备当前不支持 *Advanced WildFire* 内联机器学习。

- Strata Cloud Manager
- PAN-OS 和 Panorama

启用 Advanced WildFire Inline ML（PAN-OS 和 Panorama）

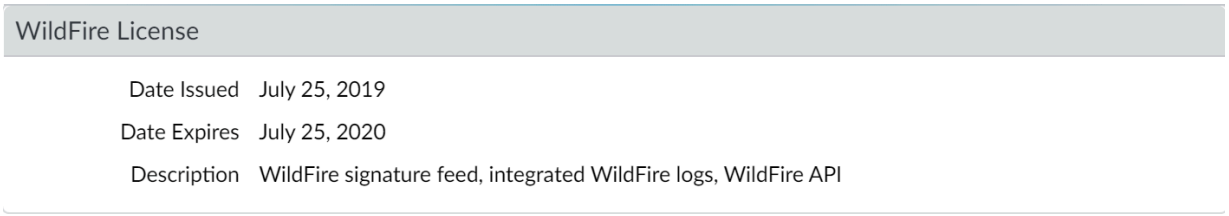
要启用 WildFire 内联机器学习配置，请将使用内联机器学习设置配置的防病毒配置文件附加到安全策略规则。

要绕过 Advanced WildFire Inline ML，您必须根据每个模型将 **Action Setting**（操作设置）设为 **Disable (for all protocols)**（禁用（针对所有协议）），或者使用部分哈希创建 WildFire Inline ML 文件例外情况。请勿根据 WildFire Inline ML 威胁 ID 配置带有签名例外情况的防病毒配置文件。这会导致防火墙阻止从您的网络传输到该 IP 地址的所有流量。

VM-50 或 *VM50L* 虚拟设备当前不支持 *WildFire inline ML*。

STEP 1 | 若要利用 WildFire inline ML，必须具有一个可用于分析 Windows 可执行文件的有效 WildFire 订阅。

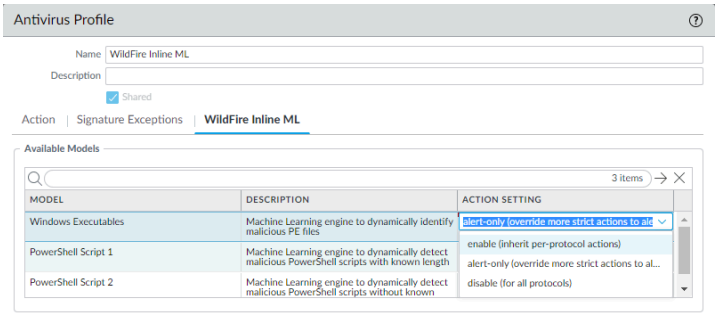
确认您是否具有 WildFire 订阅。若要确认您当前拥有许可证是何种订阅，请选择 **Device**（设备）> **Licenses**（许可证），确认是否显示相应的许可证，许可证是否已过期。



STEP 2 | 创建新的防病毒安全配置文件，或是更新现有防病毒安全配置文件以使用实时 WildFire inline ML 模式。

1. 选择现有 **Antivirus Profile**（防病毒配置文件）或新建一个（选择 **Objects**（对象） > **Security Profiles**（安全配置文件） > **Antivirus**（防病毒）并 **Add**（添加）新配置文件）。
2. 配置防病毒配置文件。
3. 选择 **WildFire Inline ML**选项卡，并为每个 WildFire Inline ML 模式使用 **Action Setting**（操作设置）。这会强制针对每种模式为所有协议配置 WildFire Inline ML 操作设置。以下分类引擎可用：

   - Windows 可执行文件
   - PowerShell Scripts 1
   - PowerShell Scripts 2
   - 可执行链接格式 —（安装有 PAN-OS 内容版本 8367 及更高版本时可用）
   - MSOffice（安装有 PAN-OS 内容版本 8434 及更高版本时可用）
   - Shell 脚本（安装有 PAN-OS 内容版本 8543 及更高版本时可用）
   - OOXML（安装 PAN-OS 11.1.3 及更高版本以及 PAN-OS 内容版本 8825 及更高版本后可用）
   - Mach-O（安装 PAN-OS 11.1.3 及更高版本和 PAN-OS 内容版本 8885-8930 及更高版本后可用）



可使用以下操作设置：

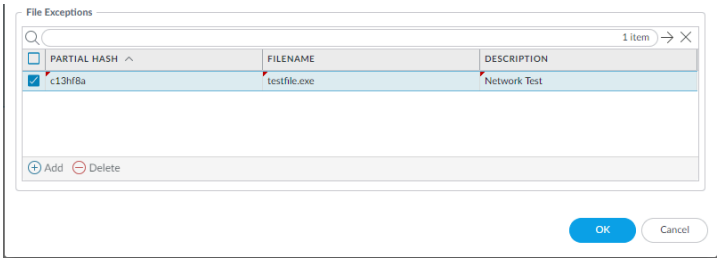
- **enable (inherit per-protocol actions)**（启用（继承每个协议操作））— WildFire 根据您在 **Action**（操作）选项卡“解码器”部分“WildFire Inline ML 操作”列中的选择检查流量。
- **alert-only (override more strict actions to alert)**（仅警报（替代更严格的警报操作））— WildFire 根据您在 **Action**（操作）选项卡“解码器”部分“WildFire Inline ML 操作”列中的选择检查流量，并以高于警报（丢弃、重置客户端、重置服务器、重置两者）的严重性级别替代任何操作，警报允许流量通过，同时仍能生成警报并保存到威胁日志中。
- **disable (for all protocols)**（禁用（对于所有协议））— WildFire 允许流量通过，无需任何策略操作。

4. 单击 **OK**（确定）从防病毒配置文件的配置窗口退出，并 **Commit**（提交）新设置。

STEP 3 | （可选）如果遇到误报，添加例外文件到您的防病毒安全配置文件。这通常针对那些不将文件转发给 WildFire 进行分析的用户。您可以直接将例外文件详细信息添加到例外列表，或是通过指定威胁日志中的文件添加例外文件详细信息。

如果您的 *WildFire* 分析安全配置文件配置为转发使用 *WildFire inline ML* 分析的文件类型，则会在收到误报时自动予以更正。如果您仍然看到被 *WildFire* 分析归类为良性的文件的 *ml-virus* 警报，请联系 *Palo Alto Networks* 支持。

- 直接将例外文件添加到例外列表。
  1. 选择 **Objects**（对象）> **Security Profiles**（安全配置文件）> **Antivirus**（防病毒）。
  2. 选择想要排除特定文件的防病毒配置文件，然后选择 **WildFire Inline ML**。
  3. 添加要从实施中排除的文件的哈希、文件名和说明。



  4. 单击 **OK**（确定）以保存防病毒配置文件，然后 **Commit**（提交）更新。
- 从威胁日志条目中添加例外文件。
  1. 选择 **Monitor**（监控）> **Logs**（日志）> **Threat**（威胁），然后在日志中筛选 **ml-virus** 威胁类型。为要创建例外的文件选择威胁日志。
  2. 前往 **Detailed Log View**（详细日志视图），然后向下滚动至 **Details**（详细信息）窗格，选择 **Create Exception**（创建例外）。

  3. 添加 **Description**（说明），然后单击 **OK**（确定）以添加例外文件。
  4. 可在 **Objects**（对象）> **Security Profiles**（安全配置文件）> **Antivirus**（防病毒）> **WildFire Inline ML** 下的 **File Exceptions**（例外文件）列表中找到新的例外文件。

STEP 4 | （可选）检查防火墙与 Inline ML 云服务的连接状态。

在防火墙上使用以下 CLI 命令查看连接状态。

```
show mlav cloud-status
```

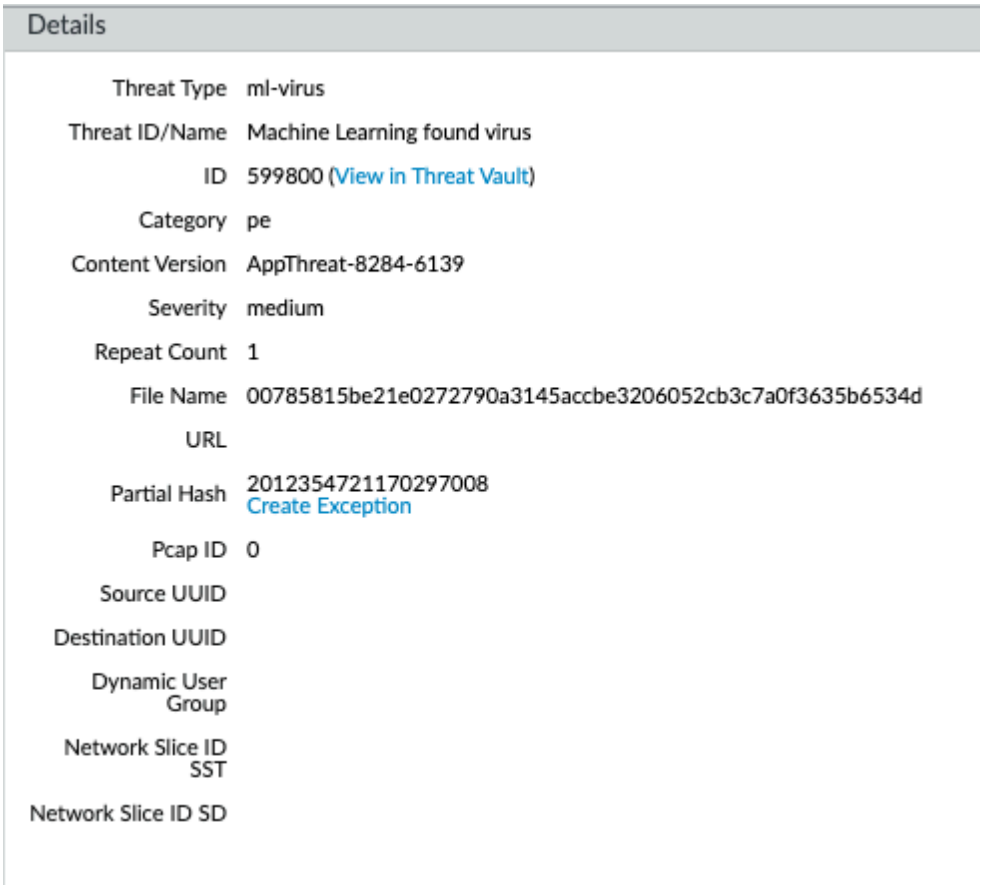
例如：

```
show mlav cloud-status MLAV cloud Current cloud server:
 ml.service.paloaltonetworks.com Cloud connection: connected
```

如果无法连接到 Inline ML 云服务，请检验以下域是否被阻止：ml.service.paloaltonetworks.com。

STEP 5 | （可选）配置 Content Cloud FQDN 设置。

若要查看 WildFire Inline ML 检测到的文件信息，请检查威胁日志（**Monitor**（监控） > **Logs**（日志） > **Threat**（威胁），然后从列表中选择日志类型）。使用 WildFire inline ML 分析过的文件将被标记为威胁类型 **ml-virus**：



启用 Advanced WildFire Inline ML (Cloud Management)

如果您使用 ***Panorama*** 来管理 ***Prisma Access***：

切换到 ***PAN-OS*** 选项卡并遵循相应的指导。

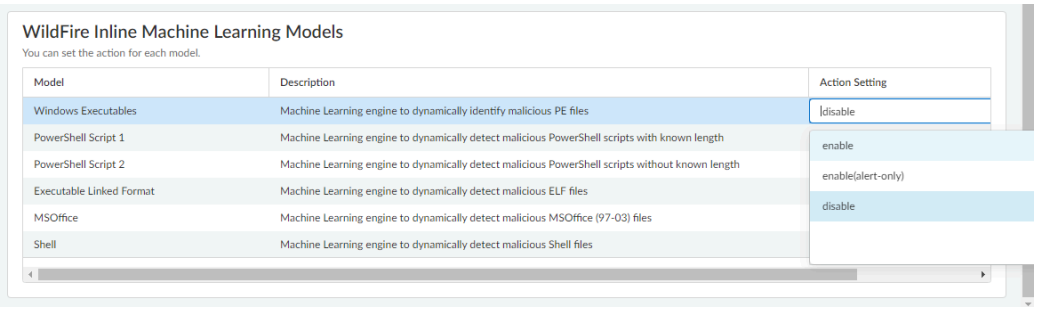
如果你使用 ***Prisma Access*** 云管理，请在这里继续。

STEP 1 | 要利用 WildFire Inline ML 学习，您必须拥有一个活跃的 WildFire 订阅作为 Prisma Access 订阅的一部分。

验证您是否拥有有效且未过期的 WildFire 订阅。

STEP 2 | 新建或更新现有 **WildFire** 和防病毒安全配置文件以使用实时 WildFire 内联机器学习模式。

1. 选择现有 **WildFire and Antivirus**（**WildFire** 和 **Antivirus**）安全配置文件，或创建新的配置文件（选择 **Manage**（管理）> **Configuration**（配置）> **NGFW** 和 **Prisma Access** > **Security Services**（安全服务）> **WildFire and Antivirus**（**WildFire** 和 **Antivirus**）），然后 **Add Profile**（添加配置文件）。
2. 配置 WildFire and Antivirus profile（WildFire 和防病毒）配置文件以转发样本进行分析。
3. 选择 **WildFire Inline Machine Learning Models**（**WildFire** 内联机器学习模式），并为每个 WildFire 内联机器学习模式应用 **Action Setting**（操作设置）。这会强制针对每种模式为所有协议配置 WildFire Inline ML 操作设置。



以下分类引擎可用：

- Windows 可执行文件
- PowerShell Scripts 1
- PowerShell Scripts 2
- 可执行链接格式
- MSOffice
- Shell 脚本
- 启用 — WildFire 根据在 **Action**（操作）选项卡“解码器”部分“WildFire 内联机器学习操作”列中的选择检查流量。
- 启用（仅警报） — WildFire 根据您在 **Action**（操作）选项卡“解码器”部分“WildFire 内联机器学习操作”列中的选择检查流量，并以高于警报（丢弃、重置客户端、重置服务

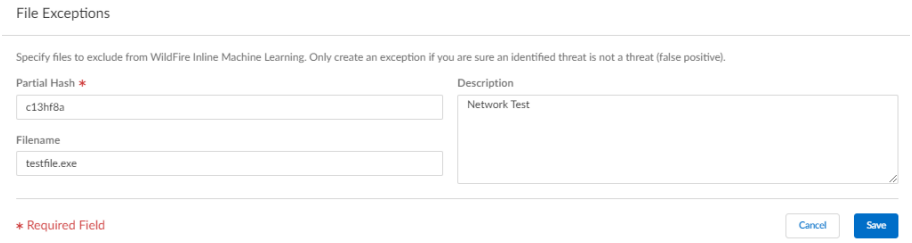
器、重置两者）的严重性级别替代任何操作，警报允许流量通过，同时仍能生成警报并保存到威胁日志中。

- **disable** — WildFire 允许流量通过而不执行任何策略操作。

STEP 3 | （可选）如果遇到误报，则添加例外文件到 WildFire 和防病毒安全配置文件中。这通常针对那些不将文件转发给 WildFire 进行分析的用户。您可以直接将例外文件详细信息添加到例外列表，或是通过指定威胁日志中的文件添加例外文件详细信息。

如果您的 *WildFire* 分析安全配置文件配置为转发使用 *WildFire inline ML* 分析的文件类型，则会在收到误报时自动予以更正。如果您仍然看到被 *WildFire* 分析归类为良性的文件的 *ml-virus* 警报，请联系 *Palo Alto Networks* 支持。

- 直接将例外文件添加到例外列表。
  1. 在 **File Exceptions**（文件例外）窗格中选择 **Advanced Settings**（高级设置）并 **Add Exception**（添加例外）。
  2. 添加要从实施中排除的文件的哈希、文件名和说明。



  3. 完成后，**Save**（保存）文件例外。

STEP 4 | **Save**（保存）WildFire 和防病毒配置文件的配置并推送配置更改。

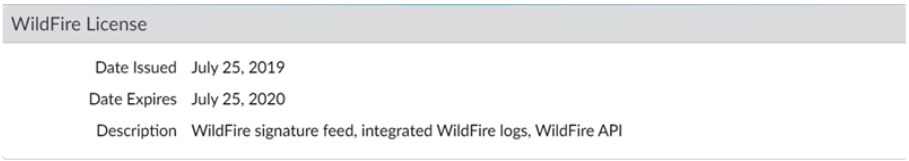
启用保持模式以进行实时签名查找

在何处可以使用？	需要提供什么？
• NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Advanced WildFire 许可证

您可以将防火墙配置为在实时签名云执行签名查找时保持样本传输。查找完成后，将根据组织针对特定 WildFire 判定的安全策略将文件释放到请求客户端（或阻止），从而防止已知恶意软件的初始传输。您可以基于每个防病毒配置文件配置保持模式，并为签名查找超时和相关操作应用全局设置。

此功能适用于运行 PAN-OS 11.0.2 及更高版本，并且具有有效 WildFire 或 Advanced WildFire 许可证的所有用户。

STEP 1 | 要为 WildFire 实时特征码查找启用保留模式，您必须拥有 WildFire 或 Advanced WildFire 订阅服务许可证。如果尚未激活防火墙上的许可证，请确保激活。要检查您是否有当前有效的许可证订阅，请选择 **Device**（设备）> **Licenses**（许可证），确认是否显示相应的许可证，以及许可证是否已过期。以下示例显示了标准 WildFire 许可证的说明。



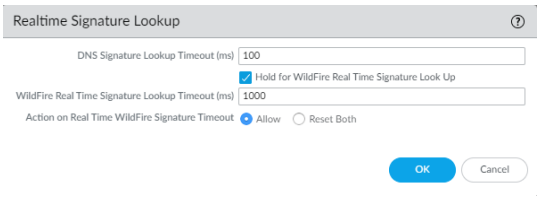
STEP 2 | 设置防火墙实时检索 WildFire 签名的时间表。

即使将防火墙配置为使用实时签名，仍会定期安装补充签名包。当您遇到连接问题时，这将提供最新的签名来源，而当签名在本地可用时，还能带来速度优势。

1. 选择 **Device**（设备）> **Dynamic Updates**（动态更新）。
2. 选择 WildFire 更新的 **Schedule**（计划）。
3. 设置 **Real-time**（实时）更新的 **Recurrence**（重复频率）（防火墙检查 Palo Alto Networks 更新服务器是否有新签名的频率）。
4. 单击 **OK**（确定）以保存 WildFire 更新计划，然后 **Commit**（提交）更改。

STEP 3 | 配置超时设置和请求超时后的操作。

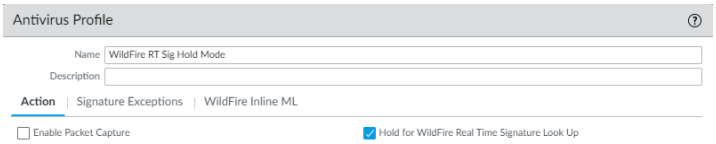
必须先全局启用保持模式，然后才能基于每个防病毒配置文件为 *WildFire* 实时签名查找启用保持模式。



1. 选择 **Device Setup**（设备设置） > **ContentID** > **Realtime Signature Lookup**（实时签名查找）
2. 启用**Hold for WildFire Real Time Signature Look Up**（等待 **WildFire** 实时签名查找）。
3. 以毫秒为单位指定 **WildFire** 实时特征码查找超时 **(ms)**（默认值为 1000）。

   Palo Alto Networks 建议使用默认值 *1000ms*，除非您在测试期间遇到重复超时。
4. 指定 **Action On Real Time WildFire Signature Timeout**（针对实时 **WildFire** 签名超时的操作）。默认值为 **Allow**（允许），但是，Palo Alto Networks 建议在启用保持模式时将其设置为 **Reset-Both**（重置 - 两者）。选项包括：
   - 允许 — 当达到保持超时阈值时，NGFW 允许数据包通过。
   - 重置两者 - 当达到保持超时阈值时，NGFW 将重置客户端和服务器端的连接。
5. 完成后选择 **OK**（确定）。

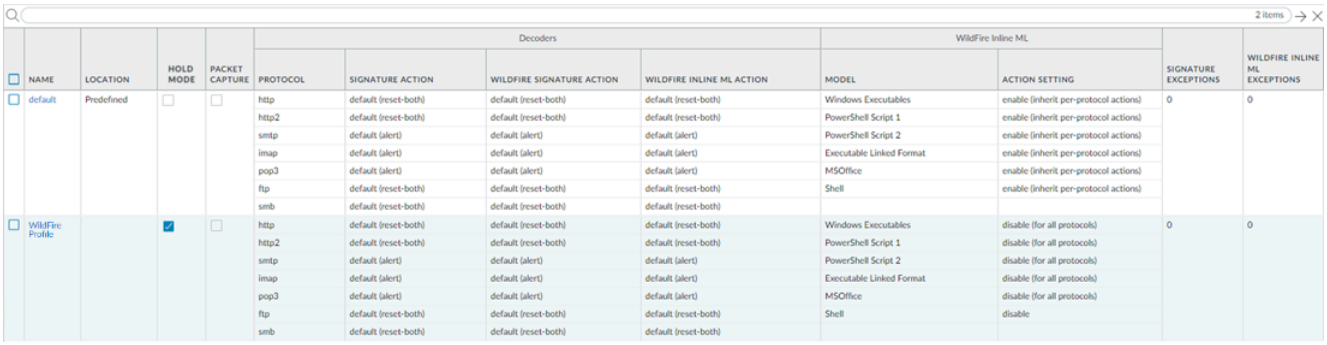
STEP 4 | 更新或创建新的防病毒安全配置文件，以启用 WildFire 实时签名查找的保持模式。



1. 选择现有的防病毒安全配置文件或 **Add**（添加）新的防病毒安全配置文件（**Objects**（对象） > **Security Profiles**（安全配置文件） > **Antivirus**（防病毒））。
2. 选择防病毒安全配置文件，然后转到 **Action**（操作）。
3. 选择 **Hold for WildFire Real Time Signature Look Up**（等待 **WildFire** 实时签名查找）。
4. 对于要为其启用 WildFire 实时签名查找保持模式的所有活动防病毒配置文件，请重复步骤 4.1-4.3。

STEP 5 | **Commit**（提交）更改。

STEP 6 | （可选）您可以在防病毒摘要视图页面上查看防病毒安全配置文件设置的摘要，包括保持模式启用。



2 items

					Decoders				WildFire Inline ML			
NAME	LOCATION	HOLD MODE	PACKET CAPTURE	PROTOCOL	SIGNATURE ACTION	WILDFIRE SIGNATURE ACTION	WILDFIRE INLINE ML ACTION	MODEL	ACTION SETTING	SIGNATURE EXCEPTIONS	WILDFIRE INLINE ML EXCEPTIONS
default	Predefined			http	default (reset-both)	default (reset-both)	default (reset-both)	Windows Executables	enable (inherit per-protocol actions)	0	0
				http2	default (reset-both)	default (reset-both)	default (reset-both)	PowerShell Script 1	enable (inherit per-protocol actions)		
				smtp	default (alert)	default (alert)	default (alert)	PowerShell Script 2	enable (inherit per-protocol actions)		
				imap	default (alert)	default (alert)	default (alert)	Executable Linked Format	enable (inherit per-protocol actions)		
				pop3	default (alert)	default (alert)	default (alert)	MSOffice	enable (inherit per-protocol actions)		
				ftp	default (reset-both)	default (reset-both)	default (reset-both)	Shell	enable (inherit per-protocol actions)		
				smb	default (reset-both)	default (reset-both)	default (reset-both)				
WildFire Profile		☑		http	default (reset-both)	default (reset-both)	default (reset-both)	Windows Executables	disable (for all protocols)	0	0
				http2	default (reset-both)	default (reset-both)	default (reset-both)	PowerShell Script 1	disable (for all protocols)		
				smtp	default (alert)	default (alert)	default (alert)	PowerShell Script 2	disable (for all protocols)		
				imap	default (alert)	default (alert)	default (alert)	Executable Linked Format	disable (for all protocols)		
				pop3	default (alert)	default (alert)	default (alert)	MSOffice	disable (for all protocols)		
				ftp	default (reset-both)	default (reset-both)	default (reset-both)	Shell	disable		
				smb	default (reset-both)	default (reset-both)	default (reset-both)				

配置 Content Cloud FQDN 设置

在何处可以使用？	需要提供什么？
• NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Advanced WildFire 许可证

您可以指定 NGFW 用于处理 Advanced WildFire 服务请求的云内容完全限定域名 (FQDN)。默认 FQDN 将连接到 hawkeye.services-edge.paloaltonetworks.com，然后解析到最近的云服务服务器。您可以通过指定最能满足数据驻留要求和性能要求的区域云内容服务器来覆盖自动选择的服务器。请注意，云内容 FQDN 是一种全局使用的资源，它会影响依赖此连接的其他服务发送流量负载的方式。

在某些情况下，云内容 *FQDN* 可能不完全支持某些地区的特定 *Palo Alto Networks* 产品的功能。在更改云内容 *FQDN* 之前，请验证产品是否完全受支持。

根据您使用的服务，云内容 FQDN 为包括流量有效负载在内的分析服务请求提供便利，从而将数据发送到所选区域的服务器。如果您指定的内容云 FQDN 位于您所在区域之外（例如，如果您在欧盟区域，但指定亚太地区 FQDN），则可能会违反您所在国家/地区或组织的隐私和法律法规。有关您的 Palo Alto Networks 产品如何使用云内容 FQDN 的信息，请参阅特定的产品文档。

如果您遇到服务连接问题，请确认配置的云内容 *FQDN* 未被屏蔽。

STEP 1 | 登录 PAN-OS Web 界面。

STEP 2 | 选择（**Device**（设备） > **Setup**（设置） > **Content-ID** > **Content Cloud Settings**（内容云设置））并根据需要更改 FQDN：

- 默认 — **hawkeye.services-edge.paloaltonetworks.com**
- 美国中部（美国爱荷华州）— **us.hawkeye.services-edge.paloaltonetworks.com**
- 欧洲（德国法兰克福）— **eu.hawkeye.services-edge.paloaltonetworks.com**
- 亚太地区（新加坡）— **apac.hawkeye.services-edge.paloaltonetworks.com**
- 印度（孟买）— **in.hawkeye.services-edge.paloaltonetworks.com**
- 英国（英国伦敦）— **uk.hawkeye.services-edge.paloaltonetworks.com**
- 法国（法国巴黎）— **fr.hawkeye.services-edge.paloaltonetworks.com**
- 日本（日本东京）— **jp.hawkeye.services-edge.paloaltonetworks.com**
- 澳大利亚（澳大利亚悉尼）— **au.hawkeye.services-edge.paloaltonetworks.com**
- 加拿大（加拿大蒙特利尔）— **ca.hawkeye.services-edge.paloaltonetworks.com**
- 瑞士 — **ch.hawkeye.services-edge.paloaltonetworks.com**
- 荷兰 — **nl.hawkeye.services-edge.paloaltonetworks.com**
- 印度尼西亚 — **id.hawkeye.services-edge.paloaltonetworks.com**
- 卡塔尔 — **qa.hawkeye.services-edge.paloaltonetworks.com**
- 台湾 — **tw.hawkeye.services-edge.paloaltonetworks.com**
- 波兰 — **pl.hawkeye.services-edge.paloaltonetworks.com**
- 韩国（韩国首尔）— **kr.hawkeye.services-edge.paloaltonetworks.com**
- 沙特阿拉伯 — **sa.hawkeye.services-edge.paloaltonetworks.com**
- 意大利 — **it.hawkeye.services-edge.paloaltonetworks.com**

STEP 3 | 单击 **OK**（确定）。

验证样本提交

在何处可以使用？	需要提供什么？
• NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Advanced WildFire 许可证

使用恶意软件测试样本来测试部署，同时也验证防火墙是否已正确地转发文件进行 WildFire 分析。

- 测试样本恶意软件文件
- 验证文件转发

测试样本恶意软件文件

在何处可以使用？	需要提供什么？
• NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Advanced WildFire 或 WildFire 许可证

Palo Alto Networks 提供了一个样本恶意软件文件，可用于测试 Advanced WildFire 配置。按以下步骤下载此恶意软件样本文件，验证是否已转发此文件进行 Advanced WildFire 分析，并查看分析结果。

STEP 1 | 下载其中一个恶意软件测试文件。您可以从 PE、APK、MacOSX 和 ELF 中进行选择。

> 下载加密 *WildFire* 样本恶意软件文件之前，您必须从***Device***（设备）**>*Certificate Management***（证书管理）**>*SSL Decryption Exclusion***（*SSL* 解密排除）页面的解密排除列表中暂时禁用 **.wildfire.paloaltonetworks.com* 条目，否则无法正确下载该样本。执行验证测试后，请确保在 *SSL* 解密排除页面重新启用 **.wildfire.paloaltonetworks.com* 条目。

- 如果您在防火墙上启用了 SSL 解密，请使用下列 URL 之一：
  - PE — https://wildfire.paloaltonetworks.com/publicapi/test/pe
  - APK — https://wildfire.paloaltonetworks.com/publicapi/test/apk
  - MacOSX — https://wildfire.paloaltonetworks.com/publicapi/test/macos
  - ELF — wildfire.paloaltonetworks.com/publicapi/test/elf
- 如果您尚未在防火墙上启用 SSL 解密，请使用下列 URL 之一代替：
  - PE — http://wildfire.paloaltonetworks.com/publicapi/test/pe
  - APK — http://wildfire.paloaltonetworks.com/publicapi/test/apk
  - MacOSX — http://wildfire.paloaltonetworks.com/publicapi/test/macos
  - ELF — wildfire.paloaltonetworks.com/publicapi/test/elf

此测试文件名为 wildfire-test-*file_type*-file.exe，且每个测试文件均具备唯一的 SHA-256 哈希值。

> 您也可以使用 *WildFire API* 检索恶意软件测试文件。有关详细信息，请参阅《WildFire API 参考》。

STEP 2 | 在防火墙 Web 界面上选择 **Monitor**（监控）> **WildFire Submissions**（**WildFire** 提交情况），确认是否已转发此文件进行分析。

请等待至少 5 分钟，之后，此文件的分析结果将显示在 **WildFire Submissions**（**WildFire** 提交）页面上。测试文件的判定结果将始终显示为恶意软件。

验证文件转发

在何处可以使用？	需要提供什么？
• NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Advanced WildFire 或 WildFire 许可证

在将防火墙设置为转发文件以进行 Advanced WildFire 分析之后，使用以下选项来验证防火墙与 Advanced WildFire 公共或 WildFire 专有云之间的连接，并监控文件的转发情况。

数个可用于验证防火墙是否正转发样本进行分析的选项均为 *CLI* 命令，如需了解并使用 *CLI*，请参阅《PAN-OS CLI 快速入门指南》。

验证防火墙连接至 Advanced WildFire 公共云和/或 WildFire 私有云的状态，包括防火墙转发进行分析的文件总数。

使用 **`show wildfire status`** 命令以：

- 检查连接防火墙的 Advanced WildFire 公共云和/或 WildFire 专有云的状态。如状态为 `Idle`，则表明 Advanced WildFire 云（公共云或专有云）已准备好接收文件进行分析。
- 确认防火墙转发文件的配置大小限制（**Device**（设备） > **Setup**（设置） > **WildFire**）。
- 监控文件的转发情况，包括防火墙转发进行分析的文件总数。如果防火墙在 WildFire 混合云部署中，则还会显示转发至 WildFire 公共云和 WildFire 专有云的文件数。

以下示例显示了在 WildFire 专有云部署中，防火墙的 `show wildfire status` 命令输出结果：

```
admin@VM-FW> show wildfire status

Connection info:
  Signature verification:            enable
  Server selection:                  enable
  File cache:                        enable
WildFire Public Cloud:
  Server address:                    wildfire.paloaltonetworks.com
  Status:                            Disabled due to configuration
  Best server:
  Device registered:                 no
  Through a proxy:                   no
  Valid wildfire license:            yes
  Service route IP address:          X.X.X.X
WildFire Private Cloud:
  Server address:                    X.X.X.X
  Status:                            Idle
  Best server:                       X.X.X.X:XXXXX
  Device registered:                 yes
  Through a proxy:                   no
  Valid wildfire license:            yes
  Service route IP address:          X.X.X.X
File size limit info:
  pe                                  9 MB
  apk                                 49 MB
  pdf                                 1000 KB
  ms-office                           9500 KB
  jar                                 9 MB
  flash                               10 MB
  MacOSX                              1 MB
Forwarding info:
  file idle time out (second):       90
  total concurrent files:            0
  Public Cloud:
    total file forwarded:            0
    file forwarded in last minute:   0
    concurrent files:                0
  Private Cloud:
    total file forwarded:            0
    file forwarded in last minute:   0
    concurrent files:                0
```

如需查看仅限于 Advanced WildFire 公共云或 WildFire 专有云的转发信息，请使用以下命令：

- **`show wildfire status channel public`**
- **`show wildfire status channel private`**

根据文件类型（包括电子邮件链接）查看防火墙转发的样本。

使用此选项以确认电子邮件链接正转发至进行分析，因为仅收到恶意软件或网络钓鱼判定结果的电子邮件链接会在防火墙上被记录为 ***WildFire Submissions (WildFire 提交情况)***条目，即使已启用记录良性和灰色软件样本，也不例外。这是由于 *WildFire* 提交情况条目的绝对数量会针对良性电子邮件链接予以记录。

使用 **`show wildfire statistics`** 命令，确认正被转发至 Advanced WildFire 公共云或 WildFire 专有云的文件类型：

- 此命令将显示工作防火墙的输出结果，同时显示防火墙转发进行分析的每种文件类型的计数情况。如果计数字段显示为 0，则表示防火墙未转发此文件类型。
- 通过检查以下计数器是否未显示为 0，确认系统正转发电子邮件链接进行分析：
- `FWD_CNT_APPENDED_BATCH` — 指示添加到等待上传到 Advanced WildFire 公有云或 WildFire 私有云的批处理的电子邮件链接数。
- `FWD_CNT_LOCAL_FILE` — 指示上传到 Advanced WildFire 公有云或 WildFire 专有云的电子邮件链接总数。

验证特定样本是否已被防火墙转发，同时检查此样本的状态。

此选项可能有助于解决以下问题：

- 确认防火墙是否已正确转发尚未收到判定结果的样本。鉴于**WildFire Submissions**（**WildFire** 提交情况）仅在分析完成时记录于防火墙上，且相关样本已收到判定结果，故请使用此选项来验证防火墙当前是否已正确转发样本进行分析。
- 根据您的安全策略，追踪其允许的、与 WildFire 分析配置文件相匹配的单个文件或电子邮件的状态，然后将其转发用以进行分析。
- 检查在混合云部署中的防火墙是否正转发正确的文件类型和电子邮件链接至 Advanced WildFire 公共云或 WildFire 专有云。

在防火墙上执行以下 CLI 命令以查看防火墙转发以供分析的样本：

- 使用“**debug wildfire upload-log**” CLI 命令，查看防火墙转发的所有样本。
- 使用 **debug wildfire upload-log channel public** CLI 命令，仅查看转发至 Advanced WildFire 公共云的样本。
- 使用“**debug wildfire upload-log channel private**” CLI 命令，仅查看转发至 WildFire 专有云的样本。

以下示例显示了在 Advanced WildFire 公共云部署中发出上述 3 个命令的输出结果：

```
user@firewall> debug wildfire upload-log
+ channel   WildFire channel (Public/Private)
  |         Pipe through a command
  <Enter>   Finish input

user@firewall> debug wildfire upload-log channel private

Private Cloud upload logs:


user@firewall> debug wildfire upload-log channel public

Public Cloud upload logs:

    log: 0, filename: support-login.swf
    processed 353590 seconds ago, action: skipped - remote benign dup
    vsys_id:  1, session_id: 169651, transaction_id: 261
    file_len:  91536, flag: 0x81c, file type: flash
    threat id: 52145, user_id: 1238, app_id: 872
    from XX.XX.XX.XX/XXXX to XX.XXX.XXX.XXX/XXX
    SHA256: 6b2f1a23407ab2db9a17ccdf686bacc6dad7d2489c65ba90dbdf02508b3d4efd

    log: 1, filename: G2M_D_because_12.03.2014_300x250.swf
    processed 611505 seconds ago, action: skipped - remote benign dup
    vsys_id:  1, session_id: 259049, transaction_id: 260
    file_len:  39206, flag: 0x81c, file type: flash
    threat id: 52145, user_id: 20583, app_id: 872
    from XX.XX.XX.XX/XXXXX to XXX.XX.XXX.XXX/XX
    SHA256: cd52d1b7a7521a14237c1531edb109627fee084806a300d907b57322b1efd6e7
```

监控是否已成功提交样本进行分析。

使用防火墙 Web 界面，选择**Monitor**（监控） > **Logs**（日志） > **WildFire Submissions**（**WildFire** 提交情况）。所有经防火墙转发至 Advanced WildFire 公共云或 WildFire 专有云进行分析的文件均会记录在 WildFire 提交情况页面上。

- 检查对样本的判定结果：

  在默认情况下，仅被判定为恶意软件或网络钓鱼的样本会显示为 **WildFire Submissions**（**WildFire** 提交情况）条目。要为良性和/或灰色软件样本启用日志记录，请选择 **Device**（设备） > **Setup**（设置） > **WildFire** > **Report Benign Files**（报告良性文件）/ **Report Grayware Files**（报告灰色软件文件）。

  启用良性文件记录作为快速故障排除的步骤之一，以验证防火墙是否在转发文件。检查 ***WildFire Submissions***（***WildFire*** 提交情况）日志，以验证系统正提交文件进行分析且正在接收判定结果（在此情况下，即指良性判定结果）。

- 确认样本的分析位置：

  WildFire Cloud（**WildFire** 云）列将显示接收转发的文件并对其进行分析的位置。这在部署混合云时非常有用。

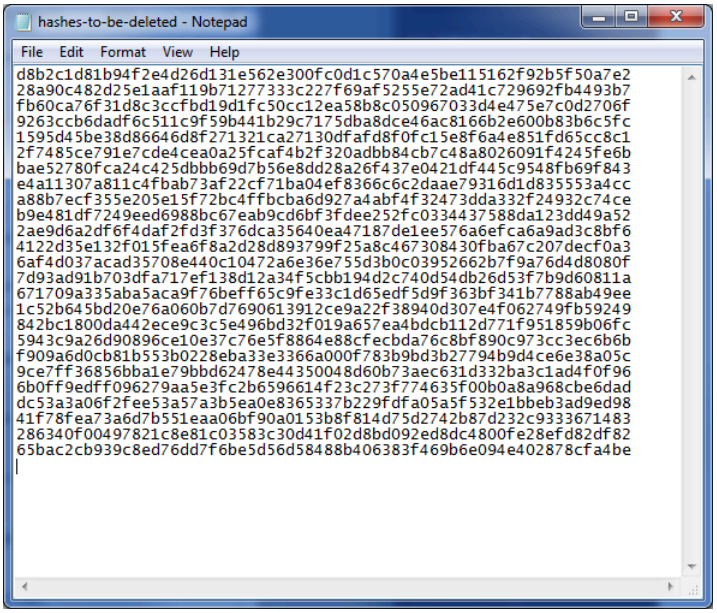
样本移除请求

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Advanced WildFire 许可证 对于 *Prisma Access*，凭借 *Prisma Access* 许可证，这通常会包含在内。

发送至 Advanced WildFire 云进行分析的唯一样本可由用户决定是否删除。为此，接受数据保护策略的用户（包括必须遵守 GDPR 的用户）可以根据其组织的保留策略拥有永久处理这些样本数据的权利。样本数据包括会话/上传数据和样本文件。

STEP 1 | 创建一个包含待删除样本的 SHA256 或 MD5 哈希列表的文本文件。每个哈希必须位于文件的单行中，可最多包含 100 个样本。

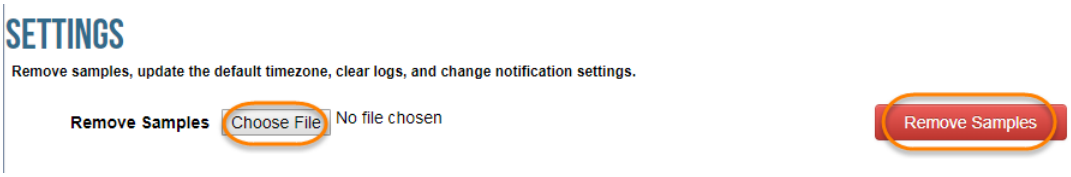
只能删除环境特有的文件。如果在其他公共或专有订阅源中发现可用文件，则仅删除用于指定帐户的会话和上传数据。



STEP 2 | 使用 Palo Alto Networks 支持凭据或 WildFire 帐户登录到 WildFire 门户。

STEP 3 | 在菜单栏选择 **Settings**（设置）。

STEP 4 | 单击 **Choose File**（选择文件）并选择在步骤 1 中创建的哈希列表文本文件，然后 **Remove Samples**（删除样本）。成功上传文件后，将收到一条确认消息。



STEP 5 | 从 WildFire 云中删除样本后，您将收到一份到包含请求详细信息的确认电子邮件。这包括请求删除的样本列表以及每个样本的删除状态。该过程可能最多需要 7 天才能完成。

```
Dear WildFire customer,
your request for removal of samples from WildFire cloud has been completed. In total 1 samples were removed from WildFire,
the following table shows removal status for each individual sample hash

+------------------------------------------------------------------+----------+---------------------+
| Hash                                                             | Status   |      Information    |
+------------------------------------------------------------------+----------+---------------------+
|6d2ef9f79b5b81429cb1ffeebd6b2919a9a84ec0cc0e5023cbf45a68967c6e1c | Deleted  ||                    |
+------------------------------------------------------------------+----------+---------------------+
```

不存在或不是您环境特有的样本将分别返回 ***Not found***（未发现）和 ***Rejected***（已拒绝）状态。

防火墙文件转发容量（按型号）

在何处可以使用？	需要提供什么？
• NGFW (Managed by PAN-OS or Panorama) • VM-SERIES	❑ Advanced WildFire 许可证

文件转发容量是每个 Palo Alto Network 防火墙型号每分钟可向 Advanced WildFire® 云提交文件来进行分析的最大速率。如果达到此每分钟的速率限制，则防火墙会将所有剩余的样本加入等待队列。

下表中保留的驱动器空间列出了防火墙上为排队文件保留的驱动器空间量。如果达到驱动器空间限制，防火墙会取消向 WildFire 转发新文件，直至队列中有更多可用空间为止。

防火墙向 *Advanced WildFire* 云转发文件的速度还取决于防火墙上传链路的带宽。

平台	每分钟的最大文件数	保留的驱动器空间
VM-50	5	100MB
VM-100	10	100MB
VM-200	15	200MB
VM-300	25	200MB
VM-500	30	250MB
VM-700	40	250MB
PA-220	20	100MB
PA-400	20	100MB
PA-820	75	300MB
PA-850	75	300MB
PA-1400 系列	20	100MB
PA-3220	100	200MB
PA-3250/3260	100	500MB

平台	每分钟的最大文件数	保留的驱动器空间
PA-800 系列	100	500MB
PA-5200 系列	250	1500MB
PA-5400 系列	250	1500MB
PA-7000 系列	300	1GB

监控活动

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Advanced WildFire 许可证 对于 *Prisma Access*，凭借 *Prisma Access* 许可证，这通常会包含在内。

您可使用WildFire 门户来查看提交至 Wildfire 的样本以及每个样本的分析结果，具体取决于您的 WildFire™ 部署是属于公共云、专有云还是混合云。如需使用此门户，您可通过访问提交样本的防火墙（或在集中管理多个防火墙的情况下，使用 Panorama）或通过使用 WildFire API。

在 WildFire 完成样本分析并对恶意、网络钓鱼、灰色软件或良性软件进行判定后，会对每个样本生成一份详细的分析报告。在提交样本的防火墙上查看的 WildFire 分析报告中也包括检测样本期间所进行会话的详细信息。对于被识别为恶意软件的样本，WildFire 分析报告中会包括现有 WildFire 签名的详细信息，此类签名可能关系到新识别的恶意软件，以及指示样本属于恶意样本的文件属性、行为及活动方面的信息。

通过 Strata Cloud Manager 命令中心，您还可以查看 Advanced WildFire 如何与其他 Palo Alto Networks 应用程序和安全服务集成，从而保护您的组织安全，防止遭受威胁入侵，并获得有关部署的整体运行状况的高级视图。命令中心是您的 NetSec 主页，通过具有多个数据方面的交互式可视化指示板来提供网络健康状况、安全性和效率的全面摘要，以便于一目了然地进行评估。

根据产品平台，您可以访问提供 Advanced WildFire 恶意软件检测统计数据和使用趋势的高级指示板，包括以分析见解形式呈现的网络活动背景等。

Palo Alto Networks 提供了多种方法来监控 Advanced WildFire 活动：

- Strata Cloud Manager 命令中心
- Advanced WildFire 指示板
- 关于 WildFire 日志和报告
- 配置 WildFire 提交情况日志的设置
- 使用 WildFire 门户监控恶意软件
- 集中查看 WildFire 分析报告
- 设置恶意软件的警报

关于 WildFire 日志和报告

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Advanced WildFire 许可证 对于 *Prisma Access*，凭借 *Prisma Access* 许可证，这通常会包含在内。

通过 WildFire 门户、Strata Cloud Manager，或利用 WildFire API，您可以在防火墙上监控活动。

对于 WildFire 分析的每一个样本，WildFire 会将样本划分为恶意软件、网络钓鱼、灰色软件或良性文件，同时也会在 WildFire 分析报告中提供详细的样本信息和行为。如需获取 WildFire 分析报告，可访问提交该样本的防火墙，以及对其进行分析的 WildFire 云（公共云或专有云），或者可使用 WildFire API 检索：

- 在防火墙上 — 所有由防火墙提交的用于进行 WildFire 分析的样本均会被记录为 WildFire 提交条目。WildFire 提交情况日志中的操作列显示文件被防火墙允许或阻挡。对于每一条 WildFire 提交情况条目，您均可打开详细的日志视图，以查看相关样本的 WildFire 分析报告或将其下载为 PDF 文件。
- 在 WildFire 门户上 — 监控 WildFire 活动，包括各样本的 WildFire 分析报告等（也可将其下载为 PDF 文件）。在 WildFire 专有云部署中，WildFire 门户可提供各样本的详细信息，包括手动上传至 WildFire 门户的样本，以及经启用了云智能的 WildFire 设备所提交的样本。

  在门户上查看 *WildFire* 分析报告仅支持已启用云情报功能的 *WildFire* 设备。

- 在 Strata Cloud Manager 上 — 所有由 Prisma Access 提交的用于进行 WildFire 分析的样本均会被记录为 WildFire 日志，并且可通过 Strata Cloud Manager 日志查看器进行研读。您可以查看流量详细信息、上下文和其他相关详细信息，包括有关样本如何逐步通过您的网络的信息。
- 使用 WildFire API — 从 WildFire 设备或从 WildFire 公共云检索 WildFire 分析报告。

Advanced WildFire 分析报告 — 深度报告

在何处可以使用？	需要提供什么？
• NGFW (Managed by PAN-OS or Panorama) • VM-SERIES	❑ Advanced WildFire 许可证

在何处可以使用？	需要提供什么？
• CN-Series	

在防火墙、WildFire 门户和 WildFire API 上访问 Advanced WildFire 分析报告。

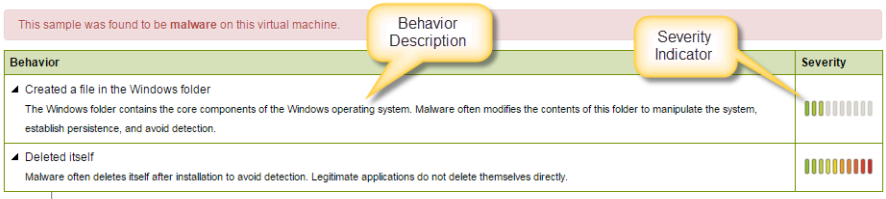
Advanced WildFire 分析报告将显示详细的样本信息、目标用户的相关信息、电子邮件标题信息（如已启用）、交付文件的应用程序，以及所有与文件命令和控制活动相关的 URL。根据在转发文件的防火墙上配置的会话信息以及针对该文件观察到的行为，Advanced WildFire 报告将包含下表中介绍的某些或全部信息。

查看手动或使用 *Advanced WildFire API* 上传到 *WildFire* 门户的文件的 *WildFire* 报告时，报告不会显示会话信息，因为流量不会穿越防火墙。例如，报告不会显示攻击者/源和受害者/目标。

报告标题	说明

文件信息	• **File Type**（文件类型）— Flash、PE、PDF、APK、JAR/Class、压缩文件、linux、脚本或 MS Office。对于 HTTP/HTTPS 电子邮件链接报告，此字段名为 URL，并会显示分析的 URL。
	• **File Signer**（文件签名人） — 签署文件以供确认真实性的实体。
	• **Hash Value**（哈希值） — 文件哈希值很像唯一识别文件的指纹，用于确保不以任何方式对文件进行修改。下面列出了 WildFire 为分析的每个文件生成的哈希版本：
	  • **SHA-1** — 显示文件的 SHA-1 值。
	  • **SHA-256** — 显示文件的 SHA-256 值。
	  • **MD5** — 显示文件的 MD5 信息。
	• **File Size**（文件大小） — WildFire 分析的文件的大小（以字节为单位）。
	• **First Seen Timestamp**（首次检测时间戳记） — 如果 WildFire 系统之前已分析了该文件，则这是首次检测该文件的日期/时间。
	• **Verdict**（结果） — 显示分析结果。
	• **Sample File**（样本文件） — 单击**Download File**（下载文件）链接可将样本文件下载到您的本地系统。注意，只能下载判定结果为恶意软件的文件，不能下载良性文件。

报告标题	说明
覆盖状态	单击**Virus Total**（病毒总计）链接以查看其他供应商已识别的样本的端点防病毒覆盖信息。如果列出的所有供应商都从未见过此文件，则会显示文件未找到。 此外，当报告显示在防火墙上时，Palo Alto Networks 当前提供的防范威胁的签名和 URL 筛选覆盖情况的相关最新信息也会显示在此部分。由于此信息是动态检索的信息，因此不会显示在 PDF 报告中。 以下覆盖信息是为活动签名提供的： • **Coverage Type**（覆盖类型） — Palo Alto Networks 所提供保护的类型（病毒、DNS、WildFire 或恶意软件 URL）。 • **Signature ID**（签名 **ID**） — 分配给 Palo Alto Networks 提供的每个签名的唯一 ID 号。 • **Detail**（详细信息） — 众所周知的病毒名称。 • **Date Released**（发布日期） — Palo Alto Networks 发布防范恶意软件的覆盖范围的日期。 • **Latest Content Version**（最新内容版本） — 防范恶意软件的内容版本的版本号。
会话信息	基于流量包含会话信息，因为此信息穿越了转发样本的防火墙。要定义 WildFire 将在报告中包含的会话信息，请选择**Device**（设备） > **Setup**（设置） > **WildFire** > **Session Information Settings**（会话信息设置）。 提供了以下选项： • 源 IP • 源端口 • 目标 Ip • 目标端口 • 虚拟系统（如果已在防火墙上配置 multi-vsys） • 应用程序 • 用户（如果已在防火墙上配置用户 ID） • 网址 • 文件名 • 电子邮件发件人

报告标题	说明
	• 电子邮件收件人 • 电子邮件主题 会话信息默认包含字段状态，表示防火墙允许或阻挡样本。
动态分析	如果某个文件为低风险并且 WildFire 可以轻松确定该文件是安全的，则仅对此文件执行静态分析，而非动态分析。 执行动态分析时，此部分包含显示样本正在其中运行的每个环节类型的分析结果。例如，“虚拟机 4”选项卡可能会显示运行 Windows 7、Adobe Reader 11、Flash 11 和 Office 2010 的分析环境。 在 *WildFire* 设备上，仅使用一个虚拟机进行分析，并且是基于与本地环境最一致的分析环境属性来选择虚拟机。例如，如果大部分用户有 *Windows 7 32* 位，则会选择该虚拟机。
行为总结	每个虚拟机选项卡都总结了特定环境中样本文件的行为。示例包括样本是否创建或修改文件、启动进程、生成新进程、修改注册表或安装浏览器帮助程序对象。 “严重性”列指示每种行为的严重性。严重性仪表将对低严重性显示一个条形，对较高的严重性级别显示更多条形。此信息也会增加到动态和静态分析部分。 **BEHAVIORAL SUMMARY**  下面介绍分析的各种行为： • **Network Activity**（网络活动） — 显示实例执行的网络活动，如访问网络上的其他主机、DNS 查询和回拨活动。将提供一个用于下载包捕获的链接。 • **Host Activity (by process)**（主机活动（按进程））— 列出在主机上执行的活动，如设置、修改或删除的注册表项。

报告标题	说明
	• **Process Activity**（进程活动） — 列出启动父级进程、进程名称以及进程执行的操作的文件。 • **File**（文件） — 列出启动子进程、进程名称以及进程执行的操作的文件。 • **Mutex**（互斥体） — 如果样本文件生成了其他程序线程，则该字段中会记录互斥体名称和父进程。 • **Activity Timeline**（活动时间线） — 提供了样本中所有已记录活动的详细列表。这将有助于了解在分析期间发生的事件的顺序。 活动时间线信息仅在 *WildFire* 报告的 *PDF* 导出格式中提供。
提交恶意软件	使用此选项可将样本手动提交到 Palo Alto Networks。WildFire 云随后会重新分析此样本，然后在确定此样本是恶意的时生成一个签名。此选项可用于没有生成签名或启用云智能的 WildFire 设备，它可用于将恶意软件从此设备转发到 WildFire 云。
报告不正确的判定结果	如果您认为判断为误报或漏报，请单击此链接以将样本提交到 Palo Alto Networks 威胁团队。威胁团队将对样本执行进一步分析以确定是否应将其重新分类。如果某个恶意软件样本被确定是安全的，则该文件的签名会在下次上传防病毒签名更新时被禁用，或者如果某个良性文件被确定为是恶意的，则会生成一个新签名。调查完成后，您将收到一封说明已采取的操作的电子邮件。

配置 WildFire 提交情况日志的设置

在何处可以使用？	需要提供什么？
• NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Advanced WildFire 许可证

当 Palo Alto Networks 网络安全平台将示例（文件和电子邮件链接）转发到 WildFire 云来进行基于 WildFire 分析配置文件设置（对象 > 安全配置文件 > WildFire 分析）的分析时，WildFire 提交日志是一个自动生成的带时间戳的文件。为转发到已完成样本静态和/或动态分析的 WildFire 云的每个样本生成 WildFire 提交日志条目。WildFire 提交日志条目包括对样本采取的操作（允许或阻止）、通过 WildFire 分析确定的已提交样本的 WildFire 判决、样本的严重性级别以及其他详细信息。

默认情况下，会为良性和恶意样本创建 WildFire 提交日志；而灰色软件和良性样本不生成日志。您可以更改 WildFire 提交日志设置以包括灰色软件和良性样本以及电子邮件链接中包含的其他会话信息。

为 **WildFire Submissions**（**WildFire** 提交情况）日志启用以下选项：

- 启用良性软件和灰色软件样本的日志记录
- 在 WildFire 日志和报告中纳入邮件标题信息

启用良性软件和灰色软件样本的日志记录

在何处可以使用？	需要提供什么？
• NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Advanced WildFire 许可证

良性软件和灰色软件样本的日志记录已默认设置为禁用。接收良性或灰色软件判断结果的邮件链接未被记录于日志中。

STEP 1 | 选择 **Device**（设备） > **Setup**（设置） > **WildFire**，然后编辑 **General Settings**（常规设置）。

STEP 2 | 选择 **Report Benign Files**（报告良性文件）和/或 **Report Grayware Files**（报告灰色软件文件），然后单击 **OK**（确定）保存设置。

在 WildFire 日志和报告中纳入邮件标题信息

在何处可以使用？	需要提供什么？
• NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Advanced WildFire 许可证

按以下步骤操作，即可在 WildFire 日志和报告中纳入邮件标题信息，包括邮件的发件人、收件人和主题等。

会话信息将随样本一起被转发至 WildFire 云，然后用于生成 WildFire 分析报告。防火墙和 WildFire 云均不可用于接收、存储或查看确切的邮件内容。

会话信息可帮助您快速跟踪并修复邮件附件或链接中检测到的威胁，包括如何识别已下载或访问恶意内容的收件人等等。

STEP 1 | 选择 **Device**（设备） > **Setup**（设置） > **WildFire**。

STEP 2 | 编辑“会话信息设置”部分，启用一个或多个选项（**Email sender (**电子邮件发件人**)**、**Email recipient (**电子邮件收件人**)**和**Email subject (**电子邮件主题**)**）。

STEP 3 | 单击 **OK**（确定）以保存。

设置恶意软件的警报

在何处可以使用？	需要提供什么？
• NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Advanced WildFire 许可证

您可对 Palo Alto Networks 防火墙进行配置，以在 WildFire 识别出恶意或网路钓鱼样本时发送警报。您也可针对良性和灰色软件文件进行警报配置，但不可针对良性和灰色软件的电子邮件链接配置警报。本示例将介绍如何配置电子邮件警报，但您也可通过配置日志转发来设置以 Syslog 消息、SNMP 陷阱或 Panorama 警报等形式发送警报。

STEP 1 | 配置电子邮件服务器配置文件。

1. 选择 **Device**（设备） > **Server Profiles**（服务器配置文件） > **Email**（电子邮件） 。
2. 单击 **Add**（添加），然后输入配置文件的 **Name**（名称）。例如 WildFire-Email-Profile。
3. （可选）从**Location**（位置）下拉列表中选择要应用此配置文件的虚拟系统。
4. 单击 **Add**（添加）以添加新电子邮件服务器条目，并输入连接到简单邮件传输协议 (SMTP) 服务器和发送电子邮件所需的信息（最多可以将四台电子邮件服务器添加到配置文件中）：
   - **Server**（服务器） — 标识邮件服务器的名称（1-31 个字符）。此字段仅是一个标签，不必用作现有 SMTP 服务器的主机名。
   - **Display Name**（显示名称） — 显示在电子邮件的“发件人”字段中的名称。
   - 发件人 — 发送通知电子邮件的源电子邮件地址。
   - 收件人 — 将通知电子邮件发送到的电子邮件地址。
   - **Additional Recipient(s)**（其他收件人） — 输入将通知发送给另一位收件人的电子邮件地址。
   - **Gateway**（网关） — 用于发送电子邮件的 SMTP 网关的 IP 地址或主机名。
5. 单击 **OK**（确定）保存服务器配置文件。
6. 单击 **Commit**（提交）以将更改保存到正在运行的配置中。

STEP 2 | 测试电子邮件服务器的配置文件。

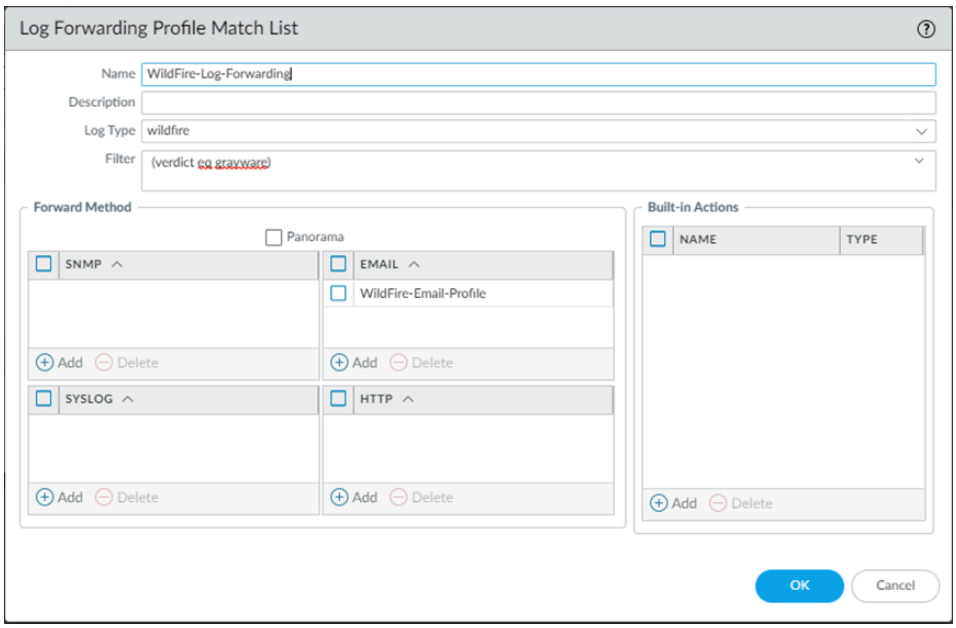
1. 选择 **Monitor (**监控**)** > **PDF Reports (PDF** 报告**)** > **Email Scheduler (**电子邮件调度程序**)**。
2. 单击 **Add**（添加）并从 **Email Profile**（电子邮件配置文件）下拉列表中选择新的电子邮件配置文件。
3. 单击 **Send test email**（发送测试电子邮件）按钮，随后会发送一封测试电子邮件至电子邮件配置文件中定义的收件人。

STEP 3 | 配置日志转发配置文件，以启用转发 WildFire 日志至 Panorama、电子邮件帐户、SNMP 、Syslog 服务器，并作为 HTTP 请求转发。

在此示例中，您将针对样本被确定为恶意的情况来设置电子邮件日志。您还可以启用转发良性和灰色软件日志，从而在测试时产生更多活动。

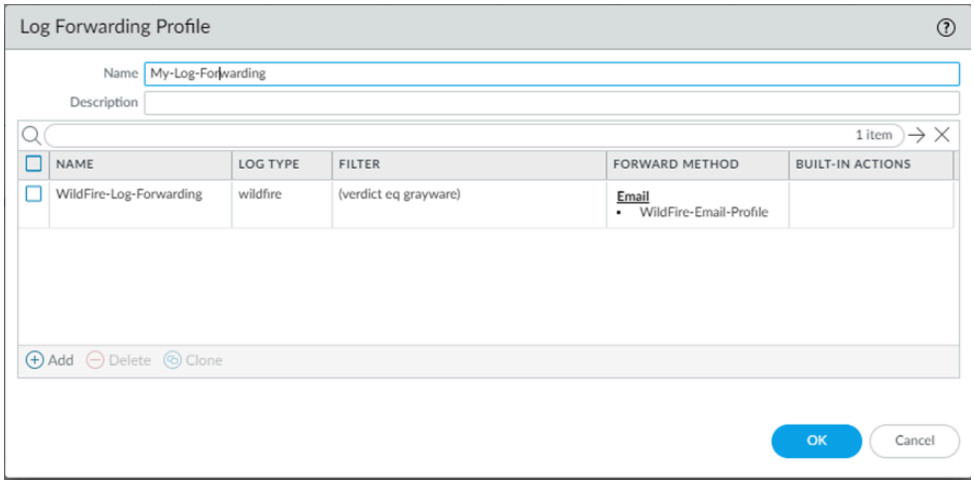
防火墙不转发被阻止文件的 *WildFire* 日志到电子邮件帐户。

1. 选择 **Objects**（对象） > **Log Forwarding**（日志转发）。
2. **Add**（添加）配置文件并命名，如 WildFire-Log-Forwarding。您可以选择为日志转发配置文件添加 **Description**（描述）。
3. **Add**（添加） 以配置转发方式。



1. 为 **Log Fowarding Profile Match List**（日志转发配置文件匹配列表）命名。
2. 选择 **WildFire** 日志类型。
3. 单击 **Filter**（筛选）按钮，通过 **(verdict eq malicious)** 查询过滤日志。
4. 在 **Forward Method**（转发方式） 选项下，选择步骤 1（在本例中为 WildFire-电子邮件-配置文件）中创建的电子邮件配置文件，然后单击 **OK**（确定）以保存匹配列表更新。

4. 再次单击 **OK**（确定）以保存日志转发配置文件更新。



STEP 4 | 添加日志转发配置文件至用于 WildFire 转发的安全策略（含附加的 WildFire 分析配置文件）。

WildFire 分析配置文件将定义防火墙转发用于进行 Advanced WildFire 分析的流量。要设置 WildFire 分析配置文件并将其附加到安全策略规则，请参阅转发文件以进行 Advanced WildFire 分析。

1. 选择 **Policies**（策略）> **Security**（安全性），然后单击用于 WildFire 转发的策略。
2. 在 **Actions**（操作）选项卡的 **Log Setting**（日志设置）部分中，选择已配置的 **Log Forwarding**（日志转发）配置文件。
3. 单击 **OK**（确定）保存更改，然后 **Commit**（提交）配置。

查看 WildFire 日志和分析报告

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Advanced WildFire 许可证 对于 *Prisma Access*，凭借 *Prisma Access* 许可证，这通常会包含在内。

WildFire 日志包含有关上传到 WildFire 云进行分析的样本（文件和电子邮件链接）的信息。其中包括工件，这些工件是与记录的事件相关联的属性、活动或行为，例如攻击者的应用程序类型或 IP 地址，以及 WildFire 特定的质量，例如高级分析结果，包括将样本分类为恶意软件、网络钓鱼、灰色软件或良性，并详细说明样本信息。查看 WildFire 提交日志还可以指示您网络中的用户是否下载了可疑文件。WildFire 分析报告将显示详细的样本信息、目标用户的相关信息、电子邮件标题信息（如已启用）、交付文件的应用程序，以及所有与文件命令和控制活动相关的 URL。它通知您文件是否存在恶意、是否修改注册表项、读/写文件、创建新文件、打开网络通信通道、导致应用程序崩溃、产生进程、下载文件或表现出其他恶意行为。

WildFire 日志在 NGFW 防火墙上显示为 WildFire 提交日志，而在云管理平台上，您必须先配置日志转发以将相关日志上传到 Strata Logging Service，随后它会将 WildFire 日志显示为威胁日志（WildFire 类型）。

- Strata Cloud Manager
- PAN-OS 和 Panorama

查看 WildFire 日志和分析报告（PAN-OS 和 Panorama）

防火墙提交用于 WildFire 分析的样本会在防火墙 Web 接口上显示为 **WildFire Submissions (WildFire** 提交情况**)**日志中的条目。对于每条 WildFire 条目，您均可打开扩展日志视图，以查看日志的详细信息和 WildFire 提供的样本分析报告。

Mozilla Firefox 用户：*WildFire* 分析报告仅能在 *Firefox v54* 和更低版本中正确显示。如果您在查看报告时遇到问题，请考虑使用其他 *Web* 浏览器，例如 *Google Chrome*。或者，您可以下载并打开 *PDF* 版本或通过 *WildFire* 门户查看报告。

STEP 1 | 转发文件以进行 Advanced WildFire 分析.

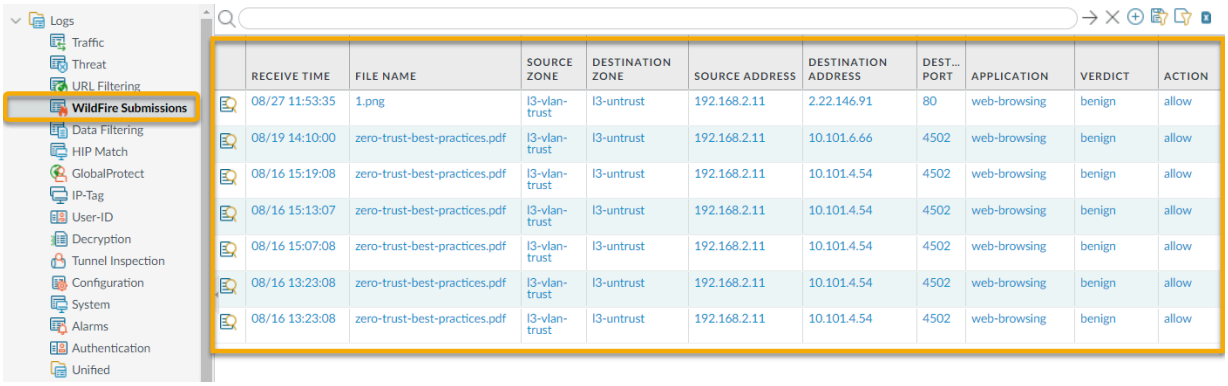
STEP 2 | 配置 WildFire 提交情况日志的设置。

STEP 3 | 如需查看防火墙向 WildFire 公共、专有或混合云提交的样本，请选择 **Monitor**（监控）> **Logs**（日志）> **WildFire Submissions**（**WildFire** 提交情况）。WildFire 样本分析完成后，其结果会发送回提交样本的防火墙，且可在 WildFire 提交情况日志中进行查看。提交日志包含给定样本的详细信息，包括以下信息：

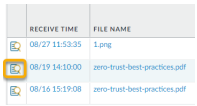
- Verdict（判定）列将显示样本是属于良性、恶性、网络钓鱼还是灰色软件。
- Action（操作）列显示防火墙已允许或阻挡了样本。
- 严重性列显示样本对组织的威胁，通过下列值显示：关键、高、中、低和参考。

以下严重性级别的值根据判定和操作值组合确定。

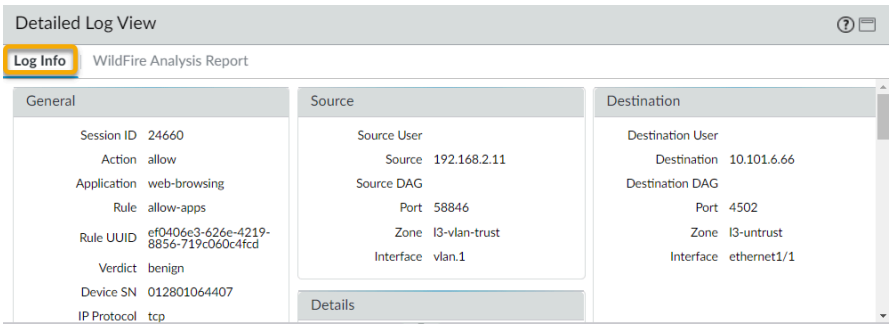
- 低 — 操作设置为允许的灰色软件样本。
- 高 — 操作设置为允许的恶意软件样本。
- 参考：
  - 操作设置为允许的良性软件样本。
  - 带其操作设置为阻止的任何判定的样本。



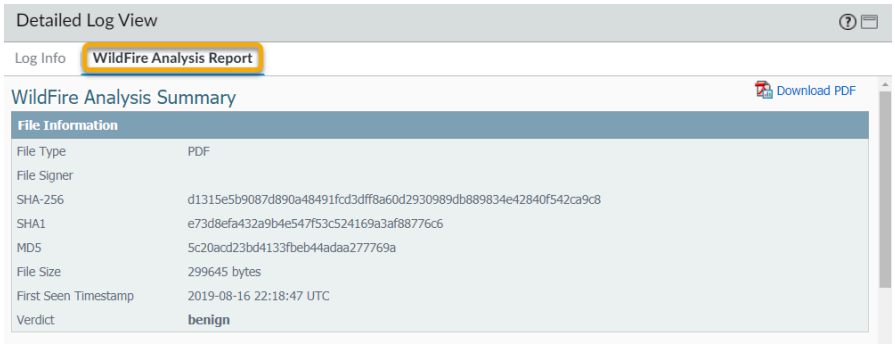
STEP 4 | 对于所有条目，选择 Log Details（日志详细信息）图标，即可打开对应条目的详细日志视图：



详细日志视图将显示 Log Info（日志信息）和对应条目的 WildFire 分析报告。如果防火墙已启用数据包捕获 (PCAP)，则样本的数据包捕获 (PCAP) 结果也会予以显示。



对于所有样本，WildFire 分析报告都会显示文件和会话的详细信息。对于恶意软件样本，WildFire 分析报告将进一步纳入可指示文件为恶意文件的文件属性和行为信息。



STEP 5 | （可选）**Download PDF**（下载 **PDF**） 形式的 WildFire 分析报告。

查看 WildFire 日志和分析报告 (Cloud Management)

如果您使用 ***Panorama*** 管理 ***Prisma Access***，则可以按照以下流程访问 *Prisma Access* 中的内容，或者切换到 ***PAN-OS*** 选项卡并按照相应的指导进行操作。

STEP 1 | 使用与 Palo Alto Networks 支持帐户关联的凭据，登录到中心上的 Strata Cloud Manager 应用程序。

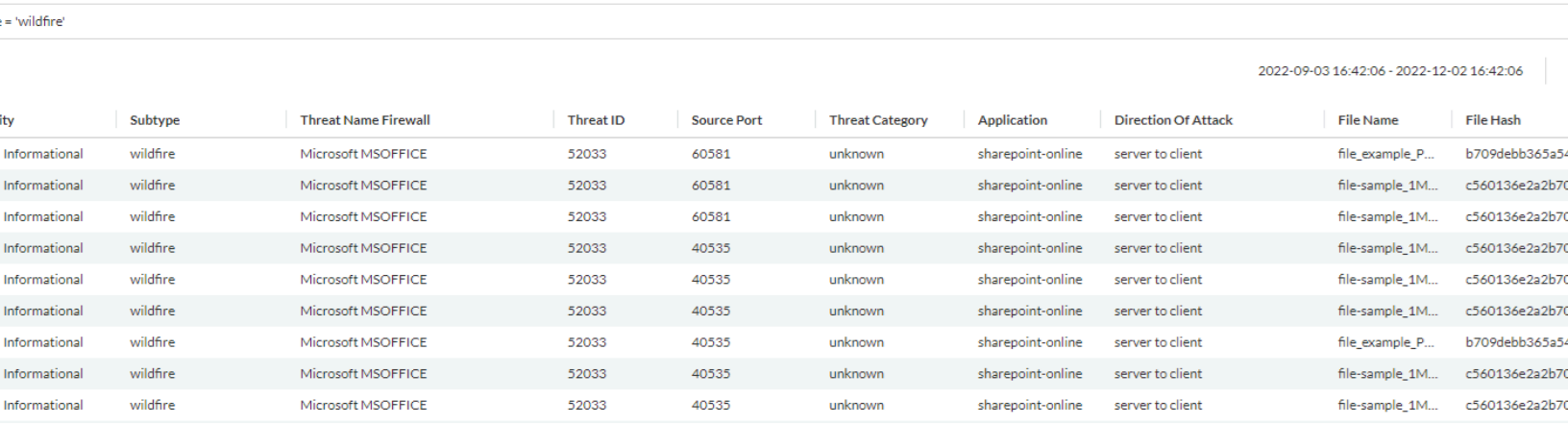
有关使用活动的更多信息，请参阅日志查看器。

STEP 2 | 过滤威胁日志以在 Prisma Access 中显示您提交的 WildFire 样本。

1. 选择 **Incidents and Alerts**（事件和警报）> **Log Viewer**（日志查看器）。
2. 将要搜索的日志类型更改为 **Threat**（威胁）。
3. 使用 WildFire 子类型创建搜索过滤器，该子类型用于指示使用查询生成器的 WildFire 样本提交。例如，您可以使用 `sub_type.value = 'wildfire'` 来查看 WildFire 日志。

根据搜索需要调整搜索条件，包括其他查询参数（例如严重性级别和操作）以及日期范围。

要查看 *WildFire* 分析报告，您必须登录到 *WildFire* 门户并使用哈希值或文件名检索报告文件。有关详细信息，请参阅在 WildFire 门户上查看报告。

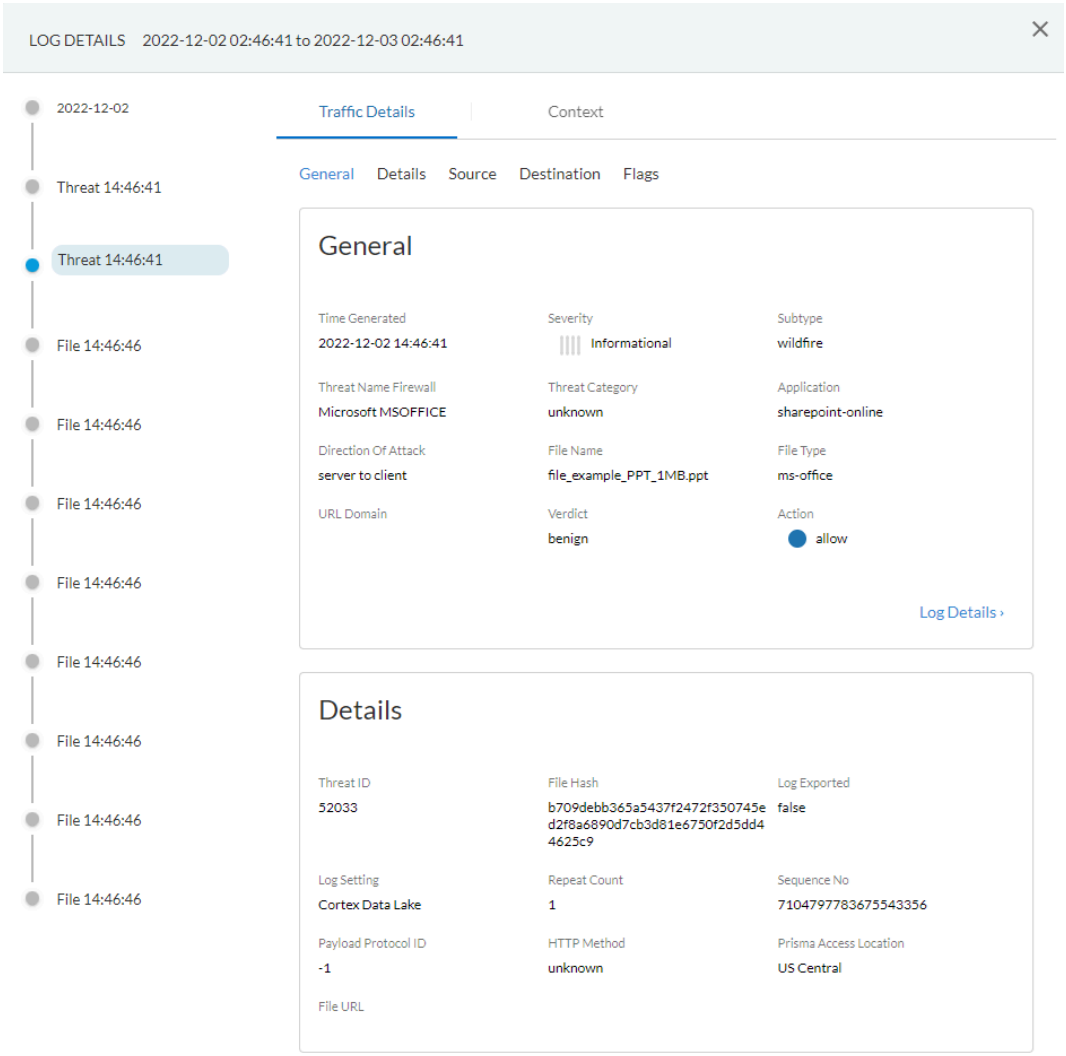


= 'wildfire'

2022-09-03 16:42:06 - 2022-12-02 16:42:06

ity	Subtype	Threat Name Firewall	Threat ID	Source Port	Threat Category	Application	Direction Of Attack	File Name	File Hash
Informational	wildfire	Microsoft MSOFFICE	52033	60581	unknown	sharepoint-online	server to client	file_example_P...	b709debb365a54
Informational	wildfire	Microsoft MSOFFICE	52033	60581	unknown	sharepoint-online	server to client	file-sample_1M...	c560136e2a2b70
Informational	wildfire	Microsoft MSOFFICE	52033	60581	unknown	sharepoint-online	server to client	file-sample_1M...	c560136e2a2b70
Informational	wildfire	Microsoft MSOFFICE	52033	40535	unknown	sharepoint-online	server to client	file-sample_1M...	c560136e2a2b70
Informational	wildfire	Microsoft MSOFFICE	52033	40535	unknown	sharepoint-online	server to client	file-sample_1M...	c560136e2a2b70
Informational	wildfire	Microsoft MSOFFICE	52033	40535	unknown	sharepoint-online	server to client	file-sample_1M...	c560136e2a2b70
Informational	wildfire	Microsoft MSOFFICE	52033	40535	unknown	sharepoint-online	server to client	file_example_P...	b709debb365a54
Informational	wildfire	Microsoft MSOFFICE	52033	40535	unknown	sharepoint-online	server to client	file-sample_1M...	c560136e2a2b70
Informational	wildfire	Microsoft MSOFFICE	52033	40535	unknown	sharepoint-online	server to client	file-sample_1M...	c560136e2a2b70

4. 设置完过滤器后运行查询。
5. 从结果中选择一个日志条目以查看日志详细信息。
6. 威胁日志 **Subtype**（子类型）与有关样本的其他信息一起显示在 **General**（常规）窗格中。有关威胁的其他相关详细信息显示在相应的窗口中。



使用 WildFire 门户监控恶意软件

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Advanced WildFire 许可证 对于 *Prisma Access*，凭借 *Prisma Access* 许可证，这通常会包含在内。

使用 Palo Alto Networks 支持凭据或 WildFire 帐户登录至 Palo Alto Networks 的 WildFire 门户。门户打开后将显示仪表盘，其中列出与特定 WildFire 订阅或支持帐户关联的所有防火墙的摘要报告信息。对于列出的每台设备，此门户均会显示已检测到的恶意软件样本数量、已分析的良性样本以及待分析的待定文件数量的统计信息。您的 WildFire 门户帐户将显示在连接至 WildFire 公共云的网络上通过防火墙提交的所有样本的数据，以及手动提交至门户的样本的数据。此外，如果您已启用 WildFire 设备，将恶意软件转发至 WildFire 公共云以完成签名的生成和分发，那么您也可通过此门户来查看上述恶意软件样本的报告。

请参阅以下章节，了解有关使用 WildFire 门户监控 WildFire 活动的详细信息：

- 配置 WildFire 门户设置
- 添加 WildFire 门户用户
- 在 WildFire 门户上查看报告

配置 WildFire 门户设置

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Advanced WildFire 许可证 对于 *Prisma Access*，凭借 *Prisma Access* 许可证，这通常会包含在内。

本节将介绍可针对 WildFire 云帐户进行的自定义设置，比如对连接至帐户的各防火墙进行的时区设置和电子邮件通知等。此外，您还可选择删除存储在云中的防火墙日志。

STEP 1 | 访问门户设置。

1. 登录到 WildFire 门户。
2. 在菜单栏选择 **Settings**（设置）。

STEP 2 | 配置 WildFire 云帐户的时区。

从 **Set Time Zone**（设置时区）下拉列表中选择时区，然后选择 **Update Time Zone**（更新时区）以保存更改。

显示在 *WildFire* 分析报告上的时间戳基于针对 *WildFire* 云帐户配置的时区。

STEP 3 | （可选）删除特定防火墙托管于云上的 WildFire 日志。

1. 在 **Delete WildFire Reports**（删除 **WildFire** 报告）下拉列表中，按序列号选择防火墙，再选择 **Delete Reports**（删除报告）即可从 WildFire 门户删除该防火墙的日志。此操作不会删除存储于防火墙上的日志。
2. 单击 **OK**（确定）以继续执行删除。

STEP 4 | （可选）配置基于 WildFire 分析判定的电子邮件通知。

WildFire 门户不为被阻挡的文件发送警报，此类文件已被防火墙转发进行 *WildFire* 分析。

1. 在 Configure Alerts（配置警报）部分中，选择 **Malware**（恶意软件）、**Phishing**（网络钓鱼）、**Grayware**（灰色软件）和/或 **Benign**（良性）复选框，以接收基于此类判定的电子邮件通知：
   - 在 **All**（所有）行中选择判定复选框，以接收针对上传至 WildFire 云的所有样本的判定通知。
   - 在 **Manual**（手动）行中选择判定复选框，以使用 WildFire 门户接收手动上传至 WildFire 公共云的所有样本的判定通知。
   - 选择一个或多个防火墙序列号的复选框，以接收这些防火墙所提交样本的判定通知。
2. 选择 **Update Notification**（更新通知）以使判定通知可通过电子邮件发送至与您支持帐户相关联的电子邮件地址。

添加 WildFire 门户用户

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Advanced WildFire 许可证 对于 *Prisma Access*，凭借 *Prisma Access* 许可证，这通常会包含在内。

WildFire 门户帐户由超级用户（或 Palo Alto Networks 设备的注册所有者）创建，以使其他用户能够登录至 WildFire 云，并查看与超级用户特别授权设备相关的数据。WildFire 用户可以是与现有 Palo Alto Networks 帐户相关联的用户，或是不与 Palo Alto Networks 支持帐户相关联的用户，您可使用此类用户身份来访问 WildFire 公共云，以及特定的防火墙数据集。

STEP 1 | 选择您希望添加的可用于访问 WildFire 门户的用户帐户。

WildFire 门户用户可查看与支持帐户相关联的所有防火墙的数据。

1. 登录到 Palo Alto Networks 支持门户。
2. 在 **Manage Account**（管理帐户）下单击 **Users and Accounts**（用户和帐户）。
3. 选择现有的帐户或子帐户。

STEP 2 | 添加 WildFire 用户。

1. 单击 **Add WildFire User**（添加 **WildFire** 用户）。
2. 输入您希望添加的用户的电子邮件地址。

   唯一的限制是所添加用户的电子邮件地址不能是来自基于 *Web* 的免费电子邮件帐户（如 *Gmail*、*Hotmail*、*Yahoo* 等）。如果为不支持的域输入电子邮件地址，则会弹出一个警告。

STEP 3 | 向新用户帐户分配防火墙，并访问 WildFire 云。

按序列号选择您希望希望授权访问的防火墙，并填写可选帐户的详细信息。

拥有现有支持帐户的用户将会收到一封包含现在可查看 WildFire 报告的防火墙列表的电子邮件。如果用户没有支持帐户，则门户会发送一封说明如何访问门户以及如何设置新密码的电子邮件。

新用户现在可登录至 WildFire 云，并查看用户已授权访问的防火墙的 WildFire 报告。用户还可以为这些设备配置自动的电子邮件警报，以接收已分析文件相关的警报。这些用户可选择接收恶意和/或良性文件相关的报告。

在 WildFire 门户上查看报告

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Advanced WildFire 许可证 对于 *Prisma Access*，凭借 *Prisma Access* 许可证，这通常会包含在内。

Wildfire 门户将显示通过防火墙提交、手动上传，或使用 WildFire API 上传的样本的报告。选择 **Reports**（报告）以显示经 WildFire 云分析的样本的最新报告。对于各列出的样本，报告条目将显示经云接收的样本的日期和时间、提交文件的防火墙的序列号、文件名或 URL，以及 WildFire 发送的判定结果（良性、灰色软件、恶意软件或网络钓鱼）。

使用搜索选项以根据文件名或样本哈希值搜索报告。您也可缩小搜索后的显示结果，选择仅查看经特定 **Source**（来源）提交的样本的报告（仅查看经手动方式或特定防火墙提交的结果），或仅查看收到 WildFire **Verdict**（判定结果）（任意、良性、恶性软件、灰色软件、网络钓鱼或待定）的样本的报告。

要查看门户中的个别报告，请单击报告名称左侧的 **Reports**（报告）图标。要保存详细报告，请单击报告页面右上角的 **Download as PDF**（下载为 **PDF**） 按钮。有关 WildFire 分析报告的详细信息，请参阅集中查看 WildFire 分析报告。

以下显示了经特定防火墙提交的样本文件的列表：