paloalto
TECHDOCS

高级威胁防护管理

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

May 18, 2023

Table of Contents

高级威胁防护

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	❑ 高级威胁防护（用于增强功能支持）或威胁防护许可证

Palo Alto Networks® 新一代防火墙威胁入侵防护订阅使用多管齐下的检测机制来保护您的网络并防御商业威胁和高级持续性威胁 (APT)，从而对抗整个威胁形势。Palo Alto Networks 威胁防护解决方案由以下订阅组成：

- 高级威胁防护 — 高级威胁防护云服务使用内联深度学习和机器学习模型，实时防御从未发现过的规避式未知 C2 威胁。作为一种超低延迟的原生云服务，这种可无限扩展的解决方案始终与模型训练改进保持同步。它还支持本地深度学习，这是对高级威胁防护中基于云的内联云分析组件的补充，提供了一种对零日威胁和其他逃避威胁执行快速、基于本地深度学习的分析的机制。高级威胁防护许可证包含威胁防护的所有优势。
- 威胁预防 — 基本威胁预防订阅基于从各 Palo Alto Networks 服务收集的恶意流量数据生成的签名。防火墙使用这些签名根据特定威胁强制执行安全策略，这些威胁包括：命令和控制 (C2)、各种已知恶意软件和漏洞利用；结合防火墙的 App-ID 和 User-ID 识别技术，可以交叉引用上下文数据以生成精细策略。作为威胁缓解策略的一部分，您还可以识别和阻止已知或有风险的文件类型和 IP 地址，其中有几个预建类别可用，包括指定了 Bulletproof 服务提供商和已知恶意 IP 的列表。如果使用专用工具和软件，可以创建自己的漏洞签名，根据网络的独特需求定制入侵防护功能。

为最大限度发挥威胁防护的效果，除高级 | 威胁防护外，Palo Alto Network 还推荐以下订阅服务：

- **DNS** 安全 — DNS 安全云服务，旨在保护您的组织免遭基于 DNS 的高级威胁。DNS 安全将高级机器学习和预测分析应用于各种威胁情报来源，可生成增强的 DNS 签名集并提供 DNS 请求的实时分析，以保护您的网络，防御新生成的恶意域。DNS 安全可以检测各种 C2 威胁，包括 DNS 隧道、DNS 重新绑定攻击、使用自动生成功能创建的域、恶意软件主机等等。DNS 安全需要“高级威胁防护”或“威胁防护”订阅，并与之配合使用，才能全面覆盖 DNS 威胁。

Palo Alto Networks 入侵防护订阅共同提供用于在攻击过程的各个阶段拦截和破坏攻击链的综合解决方案，并且能够让您深入了解如何在网络基础设施上防止安全侵犯。

高级威胁防护检测服务

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	❑ 高级威胁防护（用于增强功能支持）或威胁防护许可证

威胁防护是一种入侵防护系统 (IPS) 解决方案，该方案使用具有在防火墙和云端运行的组件的多层预防系统，可以跨所有端口和协议检测并阻止恶意软件、漏洞利用以及命令和控制 (C2)。威胁防护使用来自 Palo Alto Networks 服务的综合威胁数据来运行多种检测服务以创建签名，每个签名都具有特定的可识别模式，防火墙在检测到匹配威胁和恶意行为时使用该云来强制执行安全策略。根据威胁类型对这些签名进行分类，并为其分配唯一识别码。为了检测与这些签名相对应的威胁，防火墙将运行分析引擎，对表现出异常特征的网络流量进行检查和分类。

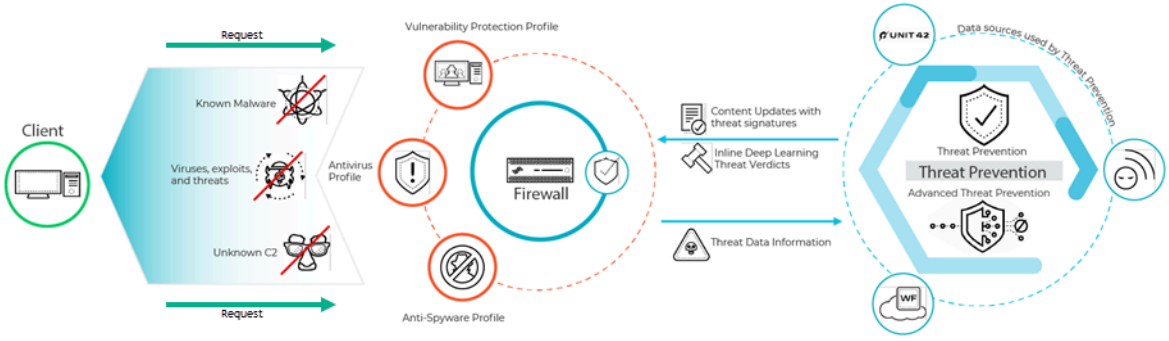
除了基于签名的检测机制外，高级威胁防护还提供内联检测系统，以防止未知和规避性 C2 威胁，包括通过 Empire 框架产生的威胁，以及命令注入和 SQL 注入漏洞。高级威胁防护云会运行可扩展深度学习模型，在防火墙上按请求启用内联分析功能，以防止零日威胁进入网络。这允许您使用带有内联检测器的实时流量检查来防止未知威胁。高级威胁防护云中这些基于 ML 的深度学习检测引擎可分析流量中的未知 C2 和漏洞，这些引擎利用 SQL 注入和命令注入来防范零日威胁。为了提供威胁上下文和全面的检测详细信息，该功能会生成报告，其中包括攻击者使用的工具/技术、检测的范围和影响，以及 MITRE ATT&CK® 框架定义的相应网络攻击分类。

通过运行基于云的检测引擎，您可以访问大量自动更新和部署的检测机制，而无需用户下载更新包，或运行将消耗资源的基于防火墙的流程密集型分析器。基于云的检测引擎逻辑使用 WildFire 的 C2 流量数据集进行持续监控和更新，并将得到 Palo Alto Networks 威胁研究人员的额外支持，由他们提供人工干预来实现高精度检测增强。高级威胁防护的深度学习引擎支持通过 HTTP、HTTP2、SSL、未知 UDP 和未知 TCP 应用程序对基于 C2 的威胁进行分析。其他分析模型通过内容更新提供，但是，对现有模型的增强是将作为云端更新执行，不需要更新防火墙。

高级威胁防护还支持本地深度学习，它提供了一种机制，可以对零日威胁和其他规避威胁执行基于本地深度学习的快速分析，作为高级威胁防护的基于云的内联云分析组件的补充功能。与 Palo Alto Networks 发布的签名集匹配的已知恶意流量将被丢弃（或对其应用另一个用户定义的操作）；但是，与可疑内容条件匹配的某些流量会重新路由，以便使用深度学习分析检测模块进行分析。如果需要进一步分析，流量将发送到高级威胁防护云进行其他分析，以及检查必要的误报和漏报。深度学习检测模块基于在高级威胁防护云中运行的成熟检测模块，因此具有相同的零日威胁检

测和高级威胁检测功能。但是，它们还具有处理更高流量的额外优势，而不会出现与云查询相关的滞后。这使您能够在更短的时间内检查更多流量并接收判定。这在面临具有挑战性的网络条件时尤其有用。

Palo Alto Networks 还提供威胁防护订阅，该订阅不包括基于云的高级威胁防护许可证中的功能。



防火墙使用的威胁签名大致分为三种类型：防病毒、防间谍软件、漏洞，此外，相应的安全配置文件会用这些签名来强制执行用户定义的策略。

Palo Alto Networks 云交付安全服务还会为各自的服务生成 *WildFire* 和 *DNS C2* 签名以及生成文件格式签名，后者可以指定文件类型来代替威胁签名；例如，作为签名例外。

- 防病毒签名可检测各种类型的恶意软件和病毒，包括蠕虫、特洛伊木马和间谍软件下载。
- 防间谍软件签名可在受影响主机上检测试图对外开启背景连线通信，或向外部 C2 服务器发送信标的 C2 间谍软件。
- 漏洞签名可检测利用系统漏洞的行为。

签名具有带关联默认操作的默认严重性级别；例如，如果存在高度恶意的威胁，则设置为“重置两者”。此设置基于 Palo Alto Networks 的安全建议。

如果在部署中存在专门的内部应用程序，或在第三方情报源中使用开源的 Snort 和 Suricata 规则，则可以创建自定义签名以提供专门的保护。

防火墙接收两种形式为更新包的签名更新：每天一次的防病毒内容更新和每周一次的应用程序和威胁内容更新。防病毒内容更新包括防病毒和防间谍软件安全配置文件分别使用的防病毒签名和 DNS (C2) 签名。应用程序和威胁的内容更新包括漏洞和防间谍软件签名，分别由漏洞和防间谍软件安全配置文件使用。更新包还包括其他服务和子功能利用的其他内容。更多信息，请参阅动态内容更新。

威胁签名类别

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	❑ 高级威胁防护（用于增强功能支持）或威胁防护许可证

在防火墙扫描网络流量时用于检测不同威胁类型的 Palo Alto Networks 威胁签名共有三种类型：

- 防病毒签名 — 检测可执行文件和文件类型中发现的病毒和恶意软件。
- 防间谍软件签名 — 检测命令和控制 (C2) 活动，受感染客户端上的间谍软件将通过这些活动，在未经用户同意的情况下收集数据和/或与远程攻击者通信。
- 漏洞签名 — 检测攻击者有可能会试图利用的系统缺陷。

签名的严重性表明检测到事件的风险。签名的默认操作（例如，阻止或警告）正是 Palo Alto Networks 推荐您实施匹配流量的方式。

您必须设置防病毒威胁、防间谍软件和漏洞防护以定义检测到威胁时要采取的行动，并且您可以轻松使用默认安全配置文件，根据 Palo Alto Networks 的建议开始阻止威胁。对于每种签名类型、类别，甚至是特定签名，您都可以继续修改或创建新的配置文件，以便更精细地执行潜在威胁。

下表按类别（防病毒、间谍软件和漏洞）列出了所有可能的签名类别，并包含每个类别中提供签名的内容更新（应用程序和威胁、防病毒或 WildFire）。此外，还可以前往 Palo Alto Networks 威胁库以进一步了解威胁签名。

威胁类别	提供这些签名的内容更新	说明
防病毒签名		
apk	防病毒 WildFire	恶意安卓应用程序 (APK) 文件。
MacOSX	防病毒 WildFire	恶意 MacOSX 文件，包括： • Apple 磁盘映像 (DMG) 文件。 • Mach 对象文件 (Mach-O) 是可执行文件、库和对象代码。

威胁类别	提供这些签名的内容更新	说明
		• Apple 软件安装程序包 (PKG)。
flash	防病毒 Wildfire 或 WildFire Private	嵌入网页的 Adobe Flash 小程序和 Flash 内容。
jar	防病毒 Wildfire	Java applet（JAR/Class 文件类型）。
ms-office	防病毒 Wildfire 或 WildFire Private	Microsoft Office 文件，包括文档（DOC、DOCX、RTF）、工作簿（XLS、XLSX）和 PowerPoint（PPT、PPTX）。还包括 Office Open XML (OOXML) 2007+ 文档。
pdf	防病毒 Wildfire 或 WildFire Private	可移植文档格式 (PDF) 文件。
pe	防病毒 Wildfire 或 WildFire Private	可移植可执行 (PE) 文件可以在 Microsoft Windows 系统上自动执行，并且仅在获得授权时才被允许。这些文件类别包括： • 对象代码。 • 字体 (FON)。 • 系统文件(SYS)。 • 驱动程序文件 (DRV)。 • Windows 控制面板项目 (CPL)。 • 动态链接库 (DLL)。 • 用于 OLE 自定义控件或 ActiveX 控件的库 (OCX)。 • Windows 屏保文件 (SCR)。 • 在 OS 和固件之间运行，以便于设备更新和引导操作的可扩展固件接口 (EFI)。 • 程序信息文件 (PIF)。
linux	防病毒 Wildfire	可执行与可链接格式 (ELF) 文件。
archive	防病毒 Wildfire	Roshal Archive（RAR 和 7-Zip）压缩文件。

威胁类别	提供这些签名的内容更新	说明
间谍软件签名		
通告	应用程序和威胁	监测可能会显示不需要的广告的程序。一些广告软件会修改浏览器以突出显示并超链接 Web 页面上最常搜索的关键字 — 这些链接将用户重定向到广告网站。此外，广告软件还会从命令和控制 (C2) 服务器检索更新，并将这些更新安装到浏览器或客户端系统上。 此类别的新发布保护工具很少见。
autogen	防病毒	这些基于有效负载的签名可以检测命令和控制 (C2) 流量，并自动生成。重要的是，即使是 C2 主机未知或变化迅速，自动生成的签名也能检测到 C2 流量。
后门	应用程序和威胁	检测允许攻击者未经授权远程访问系统的程序。
Botnet	应用程序和威胁	显示 botnet 活动。Botnet 是被攻击者控制的受恶意软件感染的计算机（“机器人”）网络。攻击者可以集中命令 botnet 中的每台计算机，并同时执行协调操作（例如，启动 DoS 攻击等）。
浏览器劫持	应用程序和威胁	检测正在修改浏览器设置的插件或软件。浏览器劫持者可能会接管自动搜过或跟踪用户的 Web 活动，并将此信息发送给 C2 服务器。 此类别的新发布保护工具很少见。
挖矿程序	应用程序和威胁	（有时也称为加密攻击或挖掘程序）检测利用计算资源在用户不知情的情况下挖掘加密货币的恶意程序的下载尝试或产生的网络流量。挖矿程序的二进制文件通常由尝试确定系统基础架构的 Shell 脚本下载器传输，会杀死系统上的其他挖掘程序进程。一些挖掘程序进程在其他进程中执行，例如呈现恶意 Web 页面的 Web 浏览器。
数据窃取	应用程序和威胁	检测向已知 C2 服务器发送信息的系统。 此类别的新发布保护工具很少见。
dns	防病毒	检测连接到恶意域的 DNS 请求。 Dns 和 dns-wildfire 签名检测相同的恶意域；但是，dns 签名包含在日常的防病毒内容更新中，dns-wildfire 签名包含在每 5 分钟发布保护措施的 Wildfire 更新中。
dns-security	防病毒	检测连接到恶意域的 DNS 请求。

威胁类别	提供这些签名的内容更新	说明
		除 DNS 安全服务生成的唯一签名外，dns-security 还包括来自 dns 和 dns-wildfire 的签名。
dns-wildfire	Wildfire 或 WildFire Private	检测连接到恶意域的 DNS 请求。 Dns 和 dns-wildfire 签名检测相同的恶意域；但是，dns 签名包含在日常的防病毒内容更新中，dns-wildfire 签名包含在每 5 分钟发布保护措施的 Wildfire 更新中。
下载程序	应用程序和威胁	（也被称为植入程序、stager 或加载程序）检测利用互联网连接到远程服务器以在受影响系统上下载并执行恶意软件的程序。最常见的用例是在网络攻击第一阶段的最高点部署的下载程序，其中，执行下载程序所获取的有效载荷被视为第二阶段。常见的下载程序类型包括 Shell 脚本（Bash，PowerShell 等）、特洛伊木马、以及 PDF 和 Word 文件等恶意诱惑文档（也称为 maldos）。
欺诈	应用程序和威胁	（包括表单劫持、网络钓鱼和诈骗）检测对已确定会被注入恶意 JavaScript 代码以收集用户敏感信息的受影响网站的访问（例如，从电子商务网站结账页面捕获的付款信息中的名称、地址、电子邮件、信用卡号、CVV、到期日期等）。
黑客工具	应用程序和威胁	检测被恶意操作者用于执行侦听、攻击或访问易受攻击系统、泄漏数据，或创建命令和控制渠道，以在未经授权的情况下暗中控制计算机系统的软件工具生成的流量。这些程序与恶意软件和网络攻击强烈关联。黑客工具可能会以善意方式部署用于红队和蓝组运作、渗透测试和研发。使用或拥有这些工具在某些国家或地区是违法的，这与工具用途无关。
密钥日志记录程序	应用程序和威胁	通过记录按键和捕获屏幕截图检测允许攻击者秘密跟踪用户活动的程序。 按键记录程序使用各种 C2 方法定期将日志和报告发送到预定义的电子邮件地址或 C2 服务器。通过按键记录程序监管，攻击者可以检索能够启用网络访问的凭据。
networm	应用程序和威胁	检测能实施系统间自我复制和传播的程序。网络蠕虫可能会使用共享资源或利用安全故障访问目标系统。
网络钓鱼工具包	应用程序和威胁	在用户尝试连接到网络钓鱼工具包登录页面时进行检测（可能是在接收到包含连接到恶意站点的链接的电子邮件后）。网络钓鱼网站诱使用户提交攻击者可以窃取的凭据，以便登录到网络。

威胁类别	提供这些签名的内容更新	说明
		除了阻止访问网络钓鱼工具包登陆页面外，还要启用多因素身份验证和防止凭证网络钓鱼，以在各个阶段防止网络钓鱼攻击。
利用后	应用程序和威胁	检测指示攻击利用后阶段的活动，此时，攻击者尝试对受攻击系统的价值进行评估。这可能包括评估存储在系统上的数据敏感性，以及系统在进一步危害网络方面的有用性。
webshell	应用程序和威胁	检测 Web 外壳和 Web 外壳流量，包括植入检测以及命令和控制交互。Web 外壳必须首先由恶意操作者植入到受影响的主机中，通常针对的是 Web 服务器或框架。随后与 Web 外壳文件进行的通信经常使恶意操作者在系统中建立立足点，执行服务和网络枚举、泄漏数据，并在 Web 服务器用户上下文中实施远程代码执行。PHP、.NET 和 Perl 标记脚本是最常见的 Web 外壳类型。攻击者还会使用受到 Web 外壳影响的服务器（Web 服务器可以是面向互联网的系统，也可以是内部系统）攻击其他内部系统。
间谍软件	应用程序和威胁	检测出站 C2 通信。这些签名可以自动生成，或是通过 Palo Alto Networks 研究人员手动创建。 间谍软件和自动生成签名都可以检测出站 C2 通信；但是自动生成签名是基于有效负载的，可唯一用于检测与位置或变化迅速的 C2 主机之间的 C2 通信。
漏洞签名		
暴力破解	应用程序和威胁	暴力破解签名检测特定时间范围内多次出现的情况。虽然孤立的活动可能是良性的，但暴力破解签名可以表明发生可疑活动时的频率和速率。例如，单个 FTP 登录失败不会显示恶意活动。但是，短时间内 FTP 多次登录失败可能表示攻击者正尝试通过密码组合来访问 FTP 服务器。 您可以针对暴力破解签名调整活动和触发条件。
代码执行	应用程序和威胁	检测代码执行漏洞（攻击者可利用此漏洞，使用已登录用户的权限在系统上运行代码）。
代码混淆	应用程序和威胁	检测已转换（以隐藏某些数据）但同时又保留了功能的代码。混淆的代码很难或者无法被读取，因此就不知道

威胁类别	提供这些签名的内容更新	说明
		代码正在执行哪些命令，或是代码想要与哪个程序进行交互。最常见的是，恶意操作者会混淆代码以隐藏恶意软件。更为罕见的是，合法的开发人员可能会混淆代码以保护隐私、知识产品或提高用户体验。例如，某些类别的混淆（例如缩小）会减少文件大小，从而减少网站加载时间和带宽使用。
dos	应用程序和威胁	检测拒绝服务 (DoS) 攻击，此时，攻击者尝试使目标系统不可用，暂时中断系统和相关的应用程序和服务。要执行 DoS 攻击，攻击者可能会使目标系统泛滥，或是发送导致其失败的信息。DoS 攻击会使合法用户（员工、成员和账户持有者等）失去其希望访问的服务或资源。
漏洞利用工具包	应用程序和威胁	检测漏洞利用工具包登录页面。漏洞利用工具包登录页面常常包含多个浏览器和插件中针对一个或多个常见漏洞和暴露 (CVE) 的多个漏洞利用。因为目标 CVE 更改速度快，因此，漏洞利用工具包签名可基于漏洞利用数据包登录页面（而非 CVE）触发。 当用户访问带漏洞利用工具包的网站时，漏洞利用工具包就会扫描目标 CVE，并尝试以静默的方式发送恶意有效负载到受害者的计算机。
信息泄露	应用程序和威胁	检测攻击者可以用于窃取敏感信息或专有信息的软件漏洞。通常，因为不存在全面的检查来保护数据，因此信息泄露可能存在，攻击者可以通过发送创建的请求来利用信息泄露。
insecure-credentials	应用程序和威胁	检测是否为软件、网络设备和 IoT 设备使用了弱密码、已泄漏的密码和制造商默认的密码。
溢出	应用程序和威胁	检测溢出漏洞（攻击者可以利用未对请求进行适当检查的情况）。成功的攻击可能会导致使用应用程序、服务器或操作系统权限执行远程代码。
网络仿冒	应用程序和威胁	在用户尝试连接到网络钓鱼工具包登录页面时进行检测（可能是在接收到包含连接到恶意站点的链接的电子邮件后）。网络钓鱼网站诱使用户提交攻击者可以窃取的凭据，以便登录到网络。 除了阻止访问网络钓鱼工具包登陆页面外，还要启用多因素身份验证和防止凭证网络钓鱼，以在各个阶段防止网络钓鱼攻击。

威胁类别	提供这些签名的内容更新	说明
协议异常	应用程序和威胁	检测协议行为偏离标准和合规使用时的协议异常。例如，格式错误的数据包、写入不当的应用程序、或在非标准端口上运行的应用程序等，都将被视为协议异常，并可用作规避工具。最佳实践是阻止任何严重性的协议异常。
Sql 注入	应用程序和威胁	检测一种常见的黑客技术，此时，攻击者将 SQL 查询插入到应用程序的请求中，以便从数据库读取或是修改数据库。这种类型的技术通常用于未全面清理用户输入的网站。

防止网络免遭第 4 层和第 7 层逃避的最佳实践

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	❑ 高级威胁防护（用于增强功能支持）或威胁防护许可证

要监控和防止网络免遭大多数第 4 层和第 7 层攻击，以下是一些建议。

- ❑ 升级到最新的 PAN-OS 软件版本和内容版本，以确保您拥有最新的安全更新。请参阅安装内容和软件更新。
- ❑ 启用 DNS 安全（（需要威胁防护和 DNS 安全订阅许可证））来对恶意 DNS 请求执行 Sinkhole。Palo Alto Networks 建议在防间谍软件配置文件中使用下列 DNS 安全类别配置设置：

SIGNATURE SOURCE	LOG SEVERITY	POLICY ACTION	PACKET CAPTURE
: Palo Alto Networks Content			
default-paloalto-dns		sinkhole	extended-capture
: DNS Security			
Command and Control Domains	default (high)	sinkhole	extended-capture
Dynamic DNS Hosted Domains	default (informational)	sinkhole	disable
Grayware Domains	default (low)	sinkhole	disable
Malware Domains	default (medium)	sinkhole	disable
Parked Domains	default (informational)	sinkhole	disable
Phishing Domains	default (low)	sinkhole	disable
Proxy Avoidance and Anonymizers	default (low)	sinkhole	disable
Newly Registered Domains	default (informational)	sinkhole	disable

  - 对于日志严重性设置，请使用默认设置：
  - 对于策略操作，将所有签名源设为 **sinkhole**。
  - 对于数据包捕获，将命令和控制域设为扩展捕获。将所有其他类别保留为默认设置。

  更多有关防间谍设置的信息，请参阅最佳实践 Internet 网关防间谍配置文件。
- ❑ 如果您订阅了有效的高级威胁防护，请启用内联云分析和本地深度学习（如果有），以实时阻止高级 C2 和间谍软件威胁。每个分析引擎的默认操作都是 **alert**（警报），它会在检测到相应的威胁时生成威胁日志；但是，Palo Alto Networks 建议将所有分析模型操作设置为 **Reset-Both**（重置二者）。这会丢弃匹配的数据包并向客户端和服务器发送 RST，从而中断连接并生成威胁日志条目。

- 设置防火墙充当代理并启用规避签名：

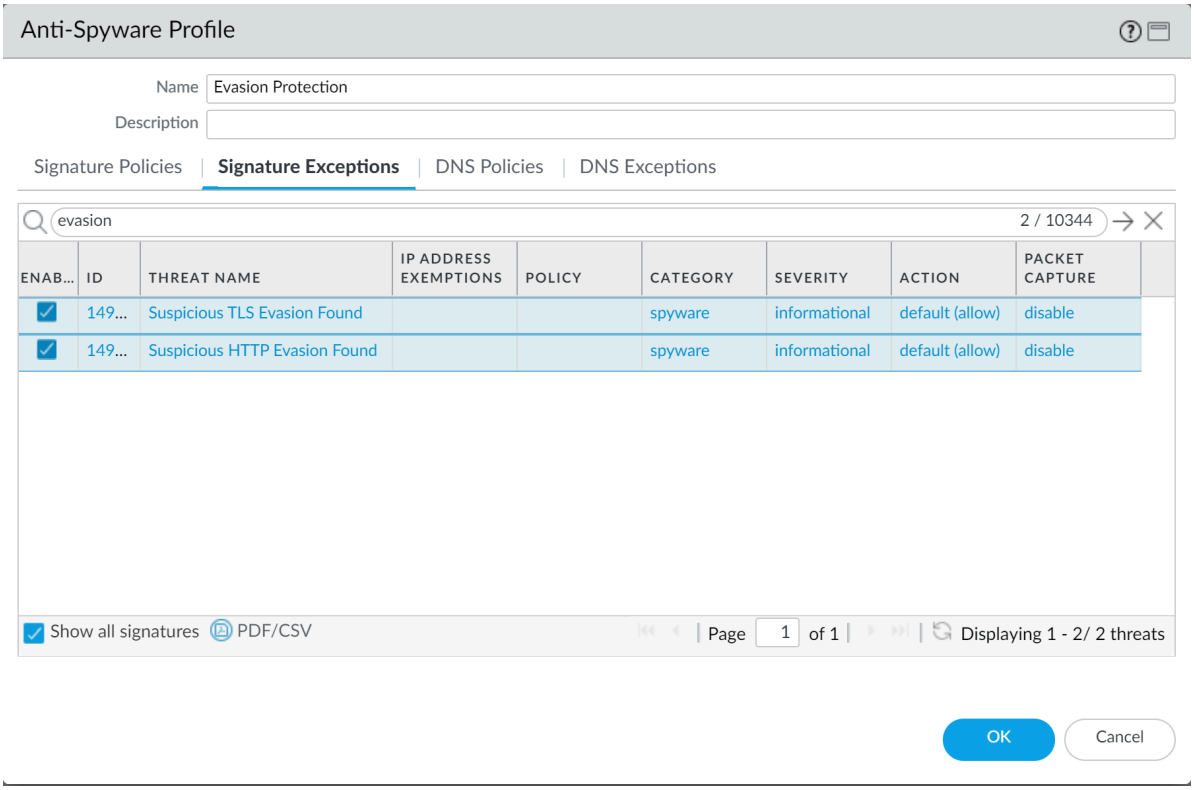
  DSN 代理不属于防火墙安全策略引擎；相反，它会在保持域到 *IP* 映射的同时引导防火墙解析 *DNS* 主机名，这对于防止 *TLS/HTTP* 规避至关重要。

  - 配置 DNS 代理对象。

    作为 DNS 代理，防火墙解析 DNS 请求并缓存主机名到 IP 地址的映射，以便快速高效地解析将来的 DNS 查询。

  - 启用规避签名

    当客户端连接到非源 DNS 请求中指定的域时，用于检测创建的 HTTP 或 TLS 请求的规避签名将发出警报。启用规避签名之前，请务必配置 DNS 代理。若无 DNS 代理，当 DNS 负载均衡配置中的 DNS 服务器向防火墙和客户端返回不同的 IP 地址（用于承载相同资源的服务器）来响应同一 DNS 请求时，可触发规避签名。



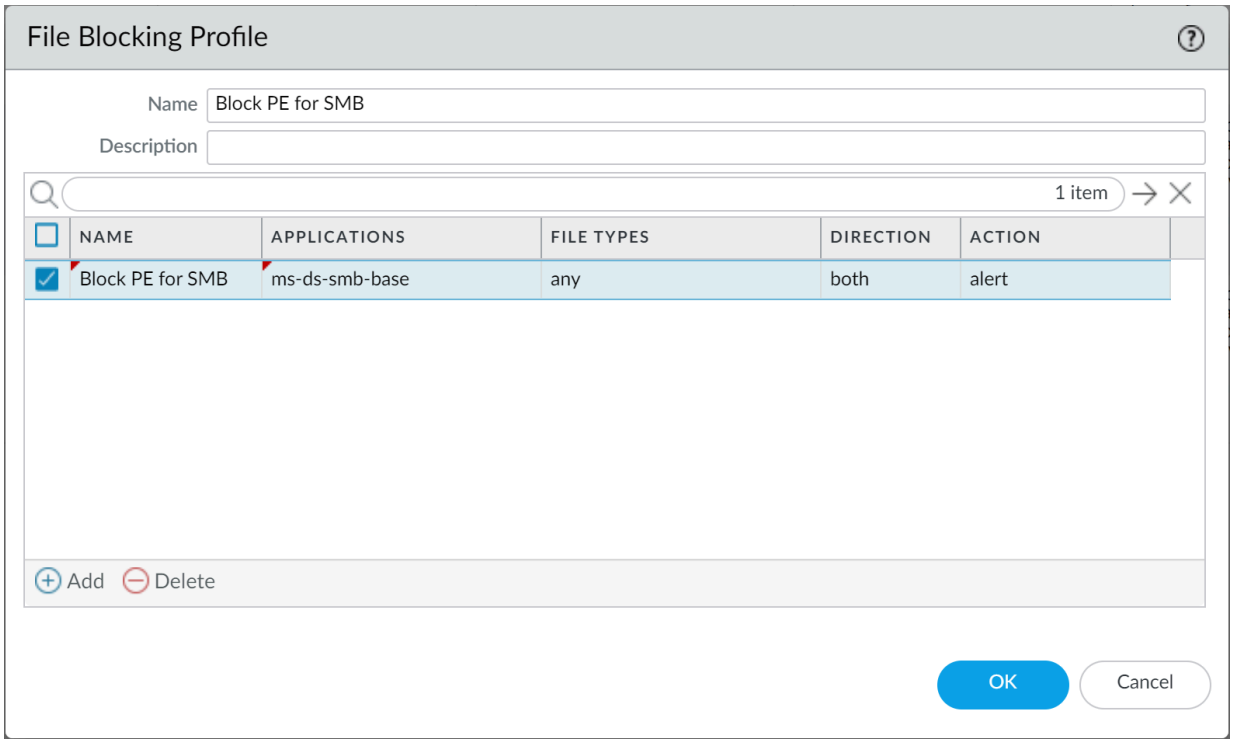
- 对于运行 Prisma Access 的部署或没有内部 DNS 服务器的网络，请将 DNS 策略配置为使用 Palo Alto Networks Sinkhole IP 地址 (72.5.65.111)，而不是默认的 Sinkhole FQDN (sinkhole.paloaltonetworks.com)。

  防间谍软件配置文件使用的 DNS sinkhole 使防火墙能够伪造对域的 DNS 查询的响应，将为 sinkhole 操作配置的类别与指定的 sinkhole 服务器相匹配，从而帮助识别受感染的主机。使用默认的 sinkhole FQDN 时，防火墙会将 CNAME 记录作为响应发送给客户端以期内部 DNS 服务器将解析 CNAME 记录，从而可以记录并标记从客户端到配置的 sinkhole 服务器的恶意通信。但是，如果客户端正在运行 Prisma Access、处于没有内部 DNS 服务器的网络中，或者使用其他无法将 CNAME 正确解析为 A 记录响应的软件或工具，则会丢弃 DNS 请求，从而导致对威胁分析至关重要的流量日志详细信息不完整。

- 对于服务器，创建安全策略规则以仅允许您在每个服务器上批准的应用程序。验证用于应用程序的标准端口与服务器上的侦听端口匹配。例如，为了确保您的电子邮件服务器仅允许 SMTP 通信，将 Application（应用程序）设置为 **smtp** 并将 Service（服务）设置为 **application-default**（应用程序-默认）。如果服务器仅使用一部分标准端口（例如，如果您的 SMTP 服务器仅使用端口 587，同时 SMTP 应用程序有被定义为 25 和 587 的标准端口），应创建仅包括端口 587 的新的自定义服务，并在安全策略规则中使用此新服务，而不是使用 application-default（应用程序-默认）。此外，确保对特定源和目标区域与 IP 地址集的访问受限。

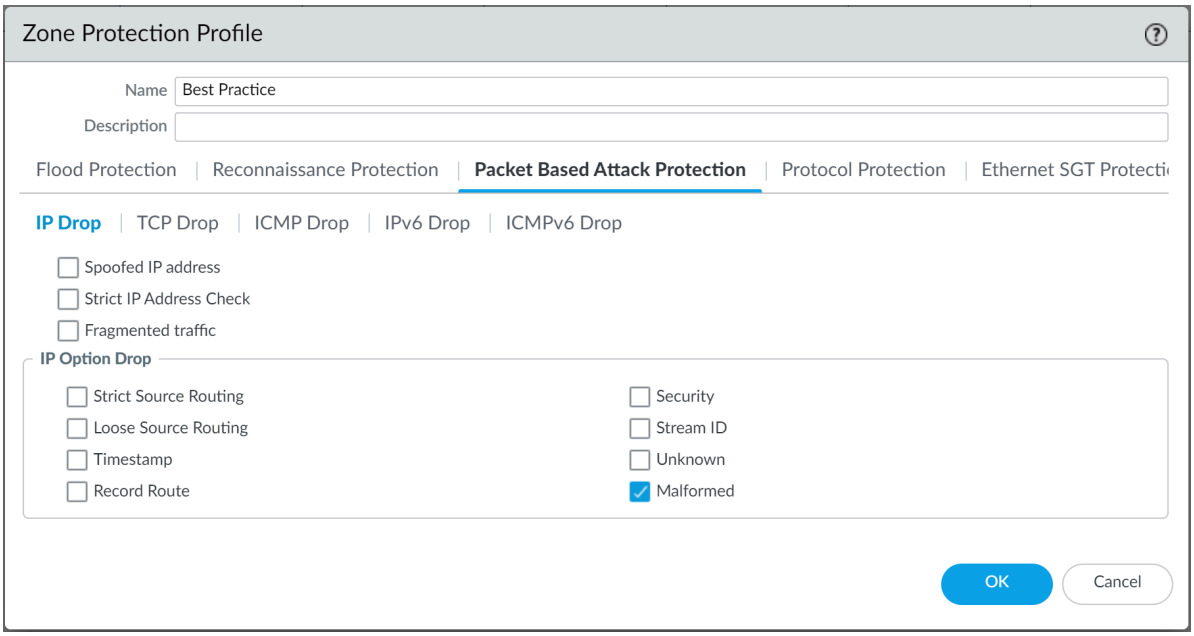
- 使用安全策略阻止所有未知应用程序和流量。通常，分类为未知流量的唯一应用程序是您网络上的内部或自定义应用程序或潜在威胁。未知流量可能是不合规的应用程序或不正常或异常的协议，或者是使用非标准端口的已知应用程序，因此应将这两种应用程序阻止。请参阅管理自定义应用程序或未知应用程序。

- 创建文件传送阻止以阻止基于互联网的服务器消息块 (SMB) 流量的可移植可执行 (PE) 文件类型，该流量从信任区域流向不信任区域（ms-ds-smb 应用程序）。



- 实时阻止 PE（可移植可执行文件）、ELF 和 MS Office 文件，以及 PowerShell 和 Shell 脚本的恶意变体。启用 WildFire 内联机器学习后，您可以在防火墙上使用机器学习动态分析文件。防病毒保护这一附加层是基于 WildFire 的签名的补充，可扩展至尚不存在签名的文件。

- 创建配置的区域保护配置文件，以防范基于数据包的攻击（**Network**（网络） > **Network Profiles**（网络配置文件） > **Zone Protection**（区域保护））：
  - 选择此选项以丢弃 **Malformed**（格式错误）的 IP 数据包（**Packet Based Attack Protection**（基于数据包的攻击保护） > **IP Drop**（**IP** 丢弃））。



  - 启用丢弃 **Mismatched overlapping TCP segment**（不匹配的重叠 **TCP** 分段）选项（**Packet Based Attack Protection**（基于数据包的攻击保护） > **TCP Drop**（**TCP** 丢弃））。

    通过故意建立与重叠的连接，但其中的数据不同，可以尝试导致攻击者误解连接的意图，故意诱发误报或漏报。攻击者还可使用 IP 欺骗和序列号预测来拦截用户的连接并插入自己的数据。选择 **Mismatched overlapping TCP segment**（不匹配的重叠 **TCP** 分段）选项，指定

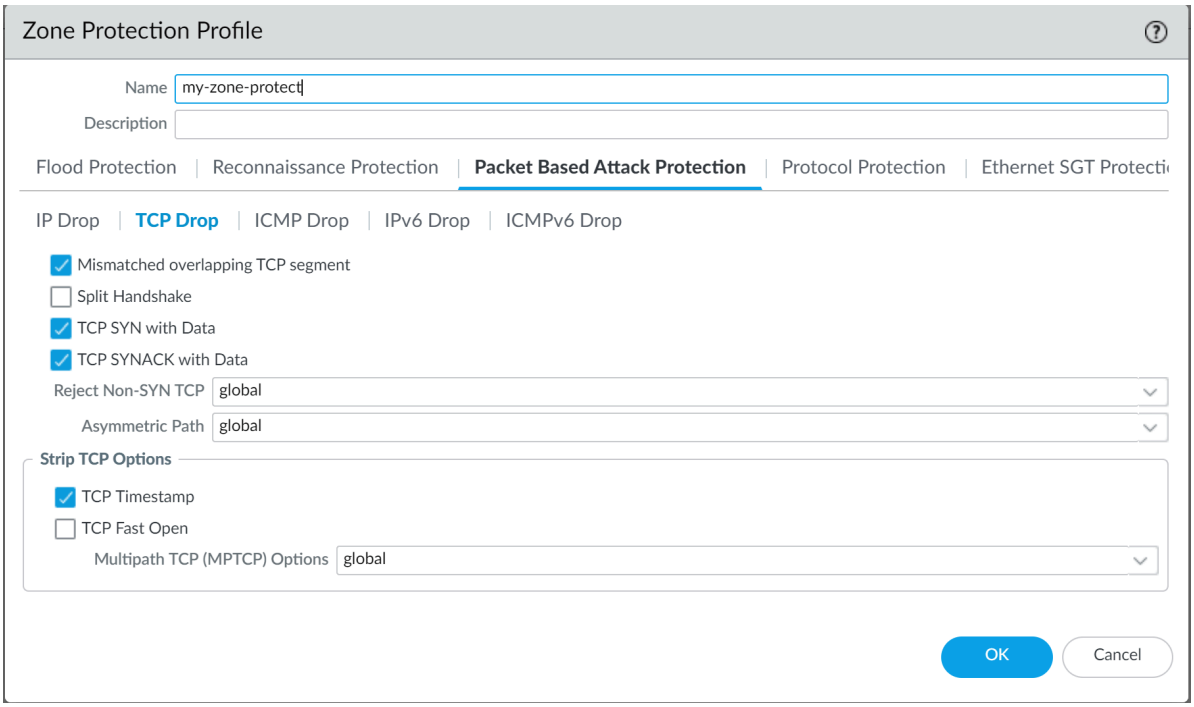
PAN-OS 丢弃具有不匹配的重叠数据的帧。当接收到的分段包含在另一个分段中、与另一个分段部分重叠，或包含另一个完整的分段时，应将其丢弃。

- 启用丢弃 **TCP SYN with Data**（带数据的 **TCP SYN**）和丢弃 **TCP SYNACK with Data**（带数据的 **TCP SYNACK**）选项（**Packet Based Attack Protection**（基于数据包的攻击保护） > **TCP Drop**（**TCP** 丢弃））。

  在三向握手期间，丢弃负载中包含数据的 SYN 和 SYN-ACK 数据包，阻止负载所包含的恶意软件并防止其在 TCP 握手完成之前提取未授权的数据，以增加安全性。

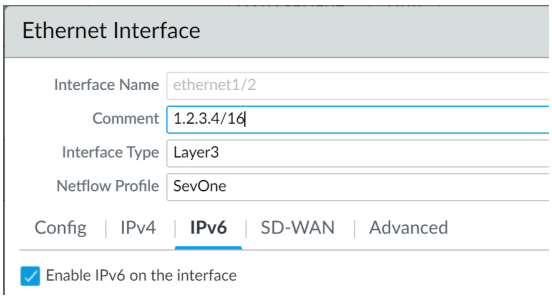
- 在防火墙转发数据包之前，将 TCP 时间戳从 SYN 数据包中删除（**Packet Based Attack Protection**（基于数据包的攻击保护） > **TCP Drop**（**TCP** 丢弃））。

  当您启用 **Strip TCP Options - TCP Timestamp**（删除 **TCP** 选项 — **TCP** 时间戳）选项时，TCP 连接两端的 TCP 堆栈都不会支持 TCP 时间戳。这可以防止攻击同一序列号多个数据包上使用的不同时间戳。

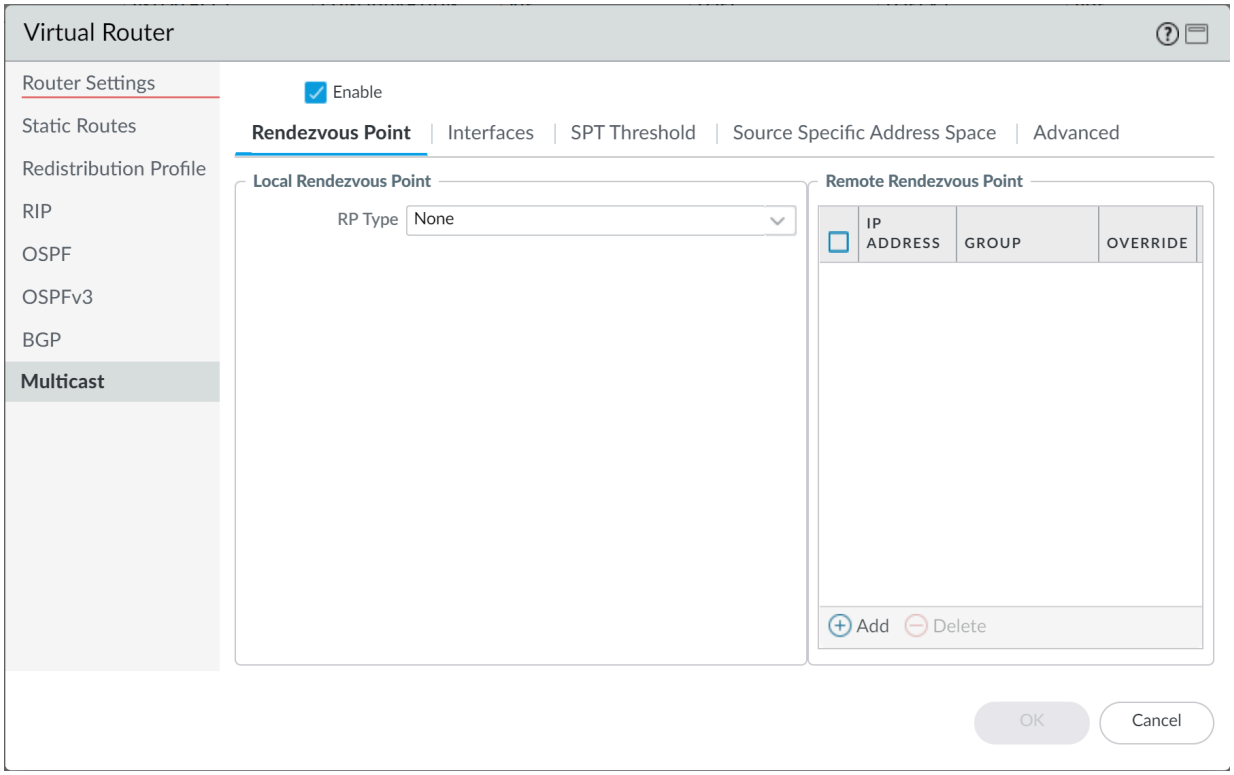


- 如果您在网络主机上配置 IPv6 地址，在务必在尚未启用时启用 IPv6 支持（**Network**（网络）**> Interfaces**（接口） **> Ethernet > IPv6**）。

  启用 IPv6 支持可以访问 IPv6 主机，还允许筛选封装在 IPv4 数据包中的 IPv6 数据包，从而阻止 IPv6 利用 IPv4 多播地址进行网络侦查检测。



- 启用多播流量支持，使防火墙可以对多播流量执行策略（**Network**（网络） **> Virtual Router**（虚拟路由器） **> Multicast**（多播））。



- 禁用 **Forward datagrams exceeding UDP content inspection queue**（转发超过 **UDP** 内容检查队列的数据报）和 **Forward segments exceeding TCP content inspection queue**（转发超过

TCP 内容检查队列的分段）选项（**Device**（设备） > **Setup**（设置） > **Content-ID** > **Content-ID Settings**（**Content-ID** 设置））。

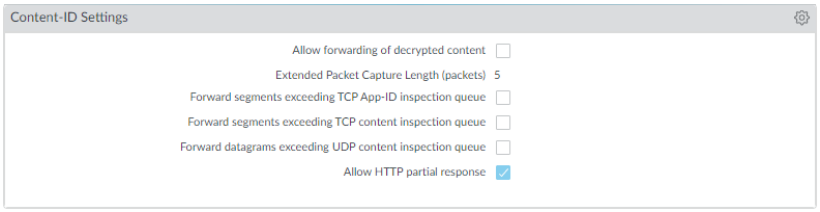
默认情况下，当 TCP 或 UDP 内容检查队列被填满时，防火墙将跳过对超过 64 个队列限制的 TCP 分段或 UDP 数据报的 Content-ID 检查。禁用此选项可确保对防火墙允许的所有 TCP 和 UDP 数据报执行内容检查。仅在特定情况下，例如，如果防火墙平台的规模未进行适当调整，不符合用例要求，则禁用此设置可能会影响性能。

- 禁用 **Allow HTTP partial response**（允许 **HTTP** 部分响应）（**Device**（设备） > **Setup**（设置） > **Content-ID** > **Content-ID Settings**（**Content-ID** 设置））。

  HTTP 部分响应选项可让客户端提取文件的任何部分。传输路径中的下一代防火墙识别并丢弃恶意文件后，它将终止与 RST 数据包的 TCP 会话。如果 Web 浏览器实施了 HTTP 标头范围选项，则将启动新会话，以便仅获取该文件的剩余部分。这可防止防火墙因缺乏上下文而触发相同的签名到初始会话，同时也可防止允许 Web 浏览器重组文件并发送恶意内容。禁用此选项将防止发生此情况。

  防火墙上默认启用“允许 HTTP 部分响应”。这最大限度提高了可用性，但也增加了网络攻击成功的风险。为了最大限度地提高安全性，请禁用此选项，以防止 Web 浏览器在防火墙因恶意活动而终止原始会话后启动新会话来获取文件的其余部分。禁用 HTTP 部分响应会影响使用 RANGE 标头的数据传输（基于 HTTP），这可能会导致某些应用程序的服务异常。禁用 HTTP 部分响应后，请验证业务关键型应用程序的操作。

  如果您在业务关键型应用程序上遇到 HTTP 数据传输中断的情况，则可以为该应用程序创建应用程序覆盖策略。由于应用程序覆盖会绕过 App-ID（包括威胁和内容检查），因此请仅为特定的业务关键型应用程序创建应用程序覆盖策略，并指定源和目标以限制规则（最小特权访问原则）。除非必须，否则不要创建应用程序覆盖策略。有关应用程序覆盖策略的信息，请参阅 https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClVLCA0。

- 创建可用于阻止协议异常以及所有低严重性和高严重性漏洞的漏洞防护配置文件。

  当协议行为偏离标准和合规使用时，就会发生协议异常。例如，格式错误的数据包、写入不当的应用程序、或在非标准端口上运行的应用程序等，都将被视为协议异常，并可用作规避工具。

  如果是任务关键型网络，业务的最高优先级应是应用程序的可用性，您应在协议出现异常的一段时间内发出警报，以确保没有关键内部应用程序正在以非标准方式使用已建立的协议。如果您发现某些关键应用程序触发协议异常签名，则可将这些应用程序从协议异常执行中排除。为

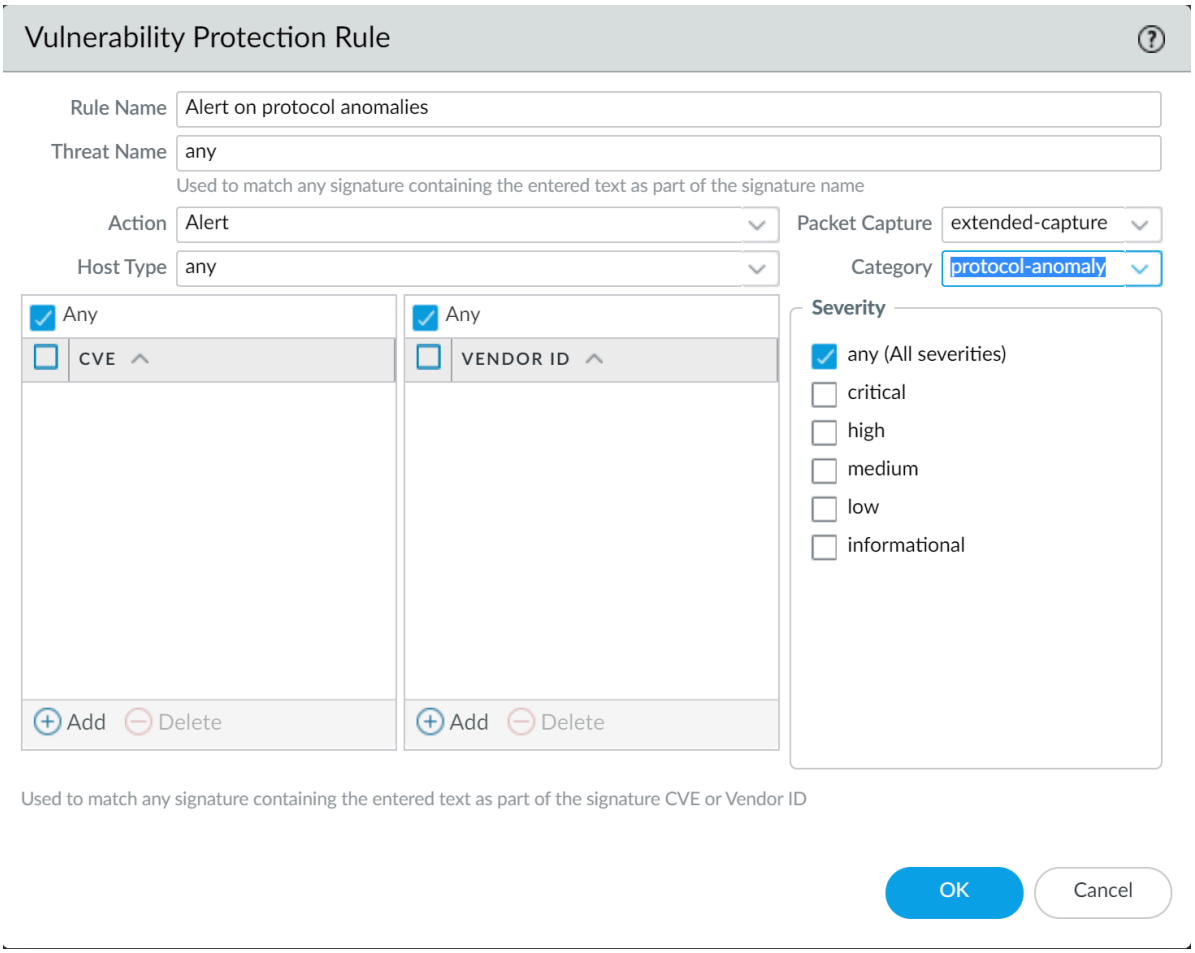
此，请在漏洞防护配置文件中添加另一个规则，允许协议异常，并将配置文件附加到执行关键应用程序往来流量的安全策略规则。

确保允许关键内部应用程序协议异常的漏洞防护配置文件规则和安全策略规则均列在阻止协议异常的规则之上。流量根据安全策略规则和相关的漏洞防护配置文件规则从上到下进行评估，并基于第一个匹配规则执行。

- 从协议异常发出警报开始：

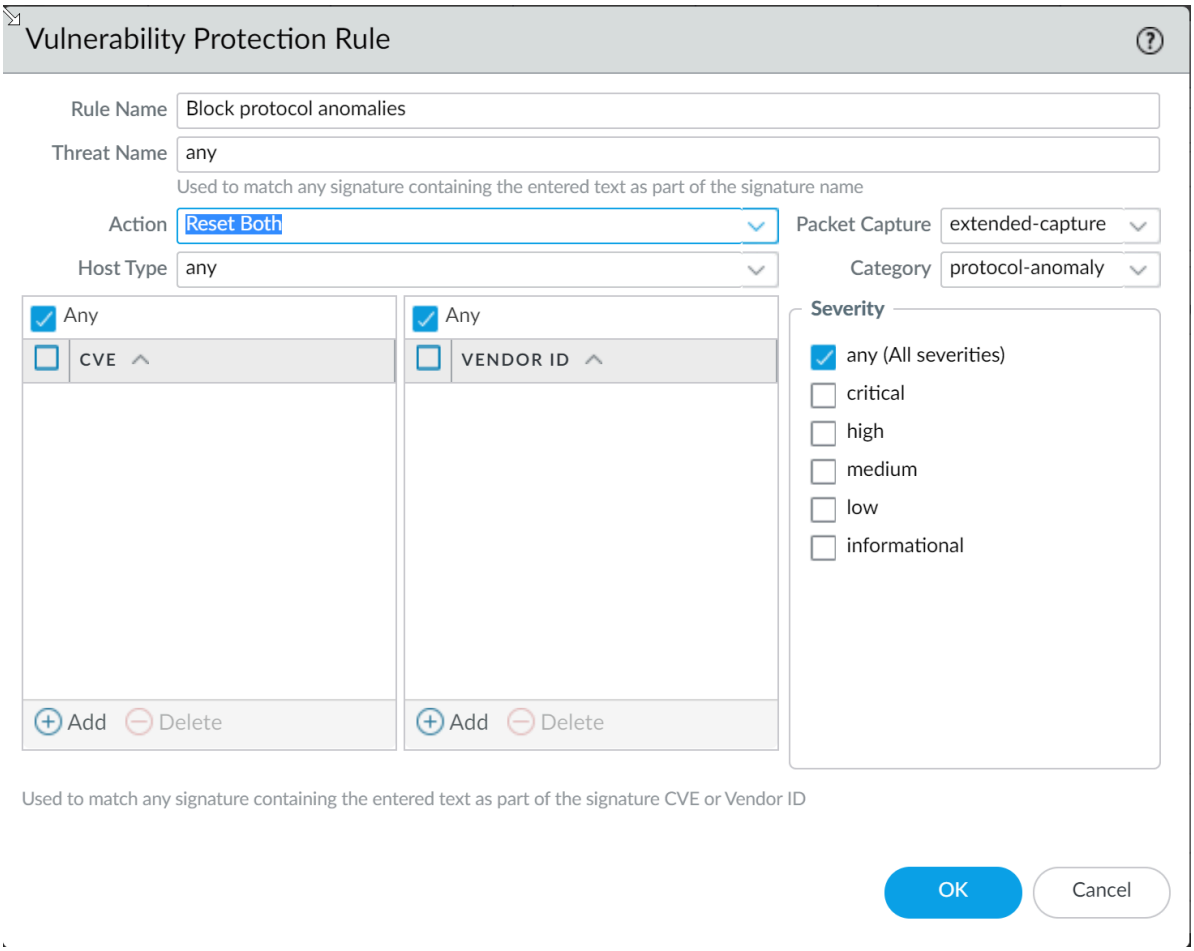
  创建漏洞防护配置文件规则，将 **Action**（操作）设置为警报，将 **Category**（类别）设置为协议异常，将 **Severity**（严重性）设置为任意。监控流量，以确定任何关键内部应用程序是

否正在以非标准方式使用已建立的协议。一旦发现，请继续允许这些应用程序的协议异常，然后阻止所有其他应用程序的协议异常。



- 阻止协议异常：

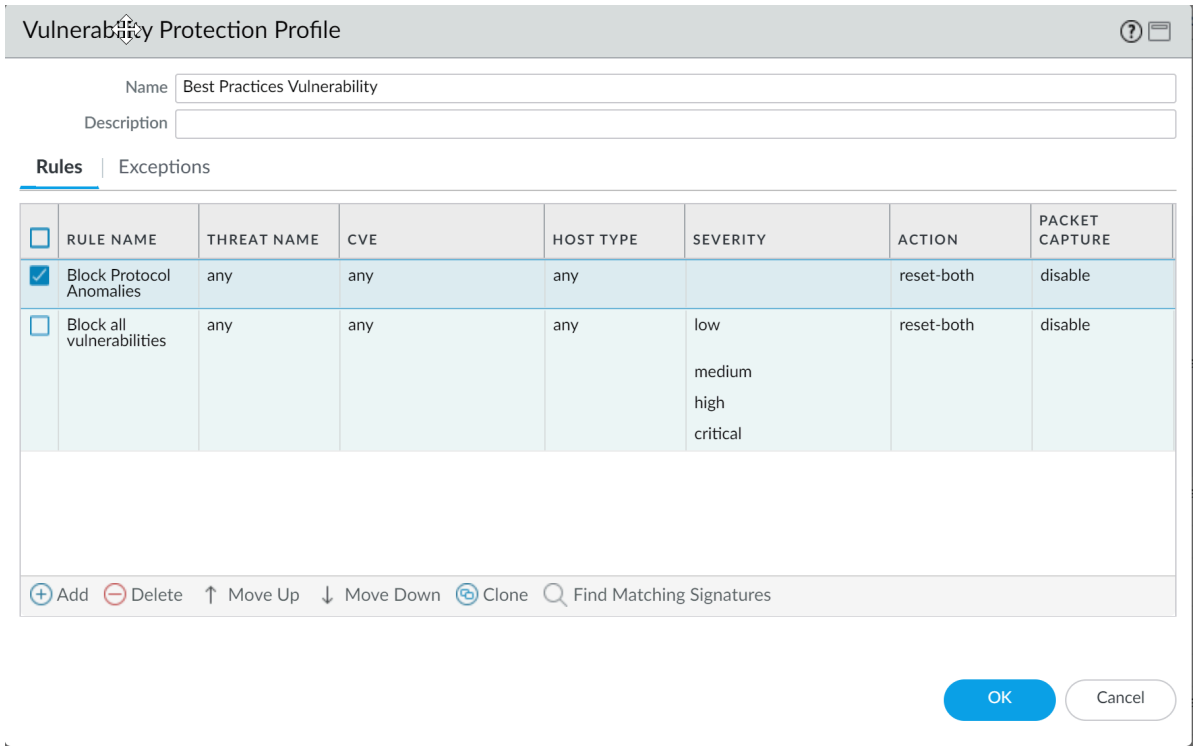
  创建漏洞防护配置文件规则，将 **Category**（类别）设置为协议异常，将规则 **Action**（操作）设置为重置二者，将 **Severity**（严重性）设置为任意。



- 可选择允许以非标准方式使用已建立协议的关键应用程序的协议异常。为此，请创建允许协议异常的漏洞防护配置文件规则：将规则 **Action**（操作）设置为允许，将 **Category**（类

别）设置为协议异常，将 **Severity**（严重性）设置为任意。将漏洞防护配置文件规则附加到执行重要应用程序往来流量的安全策略规则。

- 向用以阻止所有低严重性和高严重性漏洞的漏洞防护配置文件附加另一条规则。此规则必须显示在阻止协议异常的规则后。



- 继续将以下安全配置文件附加到安全策略规则以提供基于签名的保护：
  - 用以阻止严重性偏低和偏高的所有间谍软件的防间谍软件配置文件。
  - 用以阻止与防病毒签名匹配的所有内容的防病毒配置文件。

与 Palo Alto Networks 共享威胁情报

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	❑ 高级威胁防护（用于增强功能支持）或威胁防护许可证

遥测是收集和传输数据进行分析的过程。在防火墙上启用遥测后，防火墙会定期收集并将信息（包括有关应用程序、威胁、设备运行状况等）发送至 Palo Alto Networks。共享威胁情报可提供以下好处：

- 增强向您和全球其他客户提供漏洞和间谍软件签名。例如，当威胁事件触发漏洞或间谍软件签名时，防火墙会与 Palo Alto Networks 威胁研究团队共享与威胁相关联的 URL，以便将该 URL 正确分类为恶意软件。
- 快速测试和评估对您网络没有影响的实验威胁签名，从而更快地将关键威胁阻止签名发布到所有 Palo Alto Networks 客户。
- 提高 PAN-DB URL 筛选、基于 DNS 的命令和控制 (C2) 签名以及 WildFire 的准确性和恶意软件检测能力。

Palo Alto Networks 使用从遥测中提取的威胁情报为您和其他 Palo Alto Networks 用户提供这些优势。所有 Palo Alto Networks 用户都能从每位用户共享的遥测数据中获益，从而使得遥测成为一种社区推动的预防威胁的方法。Palo Alto Networks 不会与其他客户或第三方组织共享您的遥测数据。

要了解有关遥测的更多信息，包括其优势、使用情况和配置，请参阅设备遥测。

高级威胁防护资源

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	❑ 高级威胁防护（用于增强功能支持）或威胁防护许可证

有关威胁阻止最佳实践的详细信息，请参阅以下资源：

- 创建自定义威胁签名
- 防止网络免遭第 4 层和第 7 层逃避的最佳实践
- URL 筛选最佳实践
- 零信任最佳实践
- DoS 和区域保护最佳实践

要查看 Palo Alto Networks 产品可以识别的威胁和应用程序的列表，请使用以下链接：

- Applipedia — 提供有关 Palo Alto Networks 可识别的应用程序的详细信息。
- Threat Vault — 列出 Palo Alto Networks 产品可识别的威胁。您可以按漏洞、间谍软件或病毒进行搜索。单击 ID 号旁边的详细信息图标可获取有关威胁的详细信息。

配置威胁防护

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	❑ 高级威胁防护（用于增强功能支持）或威胁防护许可证

在启用和配置内联云分析之前，您必须获取并安装威胁防护或高级威胁防护（以访问基于云的内联云分析功能）及其运行的任何平台许可证。许可证可通过 Palo Alto Networks 客户支持门户激活，并且必须在启用任何威胁防护功能之前处于活动状态。此外，威胁防护（类似于其他 Palo Alto Networks 安全服务）通过安全配置文件进行管理，而安全配置文件则依赖于通过安全策略规则定义的网络实施策略的配置。在启用威胁防护之前，建议您熟悉启用安全订阅的安全平台的核心组件。有关详细信息，请参阅产品文档。

要启用和配置您的威胁防护订阅，以使其在网络安全部署中发挥最佳功能，请参阅以下任务。虽然可能不需要实施这里显示的所有流程，但 Palo Alto Networks 建议查看所有任务以熟悉成功部署的可用选项。另外，建议您遵循 Palo Alto Networks 提供的 最佳实践，以实现最佳可用性和安全性。

设置防病毒威胁、防间谍软件和漏洞防护

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	❑ 高级威胁防护（用于增强功能支持）或威胁防护许可证

每个 Palo Alto Networks 下一代防火墙均配置有可附加到安全策略规则的预定义防病毒、防间谍软件和漏洞防护配置文件。系统有一个预定义的防病毒配置文件，即 **default**（默认）配置文件，该配置文件对各种协议使用默认操作（阻止 HTTP、FTP 和 SMB 流量，并警告 SMTP、IMAP 和 POP3 流量）。系统有两个预定义的防间谍软件和漏洞防护配置文件：

- **default**（默认）— 对所有客户端和服务器的关键、高和中等严重性间谍软件/安全漏洞防护事件应用默认操作。它不检测低严重性和信息类事件。
- **strict**（严格）— 对所有客户端和服务器的关键、高和中等严重性间谍软件/安全漏洞防护事件应用阻止响应，并对低严重性和信息类事件使用默认操作。

为了确保进入您网络的流量不含任何威胁，请将预定义的配置文件附加到您的基本 Web 访问策略。当监视网络上的通信和扩展策略规则库时，随后可以设计多个更为精细的配置文件来处理特定安全需求。

使用以下工作流程设置默认防病毒、防间谍软件和漏洞防护安全配置文件。

- Strata Cloud Manager
- PAN-OS 和 Panorama

设置防病毒威胁、防间谍软件和漏洞防护 (Cloud Management)

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

威胁阻止订阅将防病毒、防间谍软件和漏洞防护功能绑定在一个许可证中，并且是您的 Prisma Access 订阅的一部分。有关 Prisma Access 随附的应用程序和服务的信息，请参阅所有可用的应用程序和服务。要验证您当前拥有有效许可证的订阅，请检查您的许可证支持哪些功能。

STEP 2 | （可选）创建防病毒、防间谍软件和漏洞防护的自定义安全配置文件。

或者，您也可以使用预定义的最佳实践配置文件。

安全传输到最佳实践安全配置文件以实现最佳安全状态。

- 要创建自定义 WildFire 和防病毒配置文件，请选择 **Manage**（管理） > **Configuration**（配置） > **NGFW** 和 **Prisma Access** > **Security Services**（安全服务） > **WildFire and Antivirus**（**WildFire** 和防病毒），然后 **Add Profile**（添加配置文件）。使用防病毒配置文件传输步骤安全实现您的目标。
- 要创建自定义防间谍软件配置文件，请选择 **Manage**（管理） > **Configuration**（配置） > **NGFW** 和 **Prisma Access** > **Security Services**（安全服务） > **Anti-Spyware**（防间谍软件），然后 **Add Profile**（添加配置文件）。使用防间谍软件配置文件传输步骤安全实现您的目标。
- 要创建自定义漏洞防护配置文件，请选择 **Manage**（管理） > **Configuration**（配置） > **NGFW** 和 **Prisma Access** > **Security Services**（安全服务） > **Vulnerability Protection**（漏洞防护），然后 **Add Profile**（添加配置文件）。使用漏洞防护配置文件传输步骤安全实现您的目标。

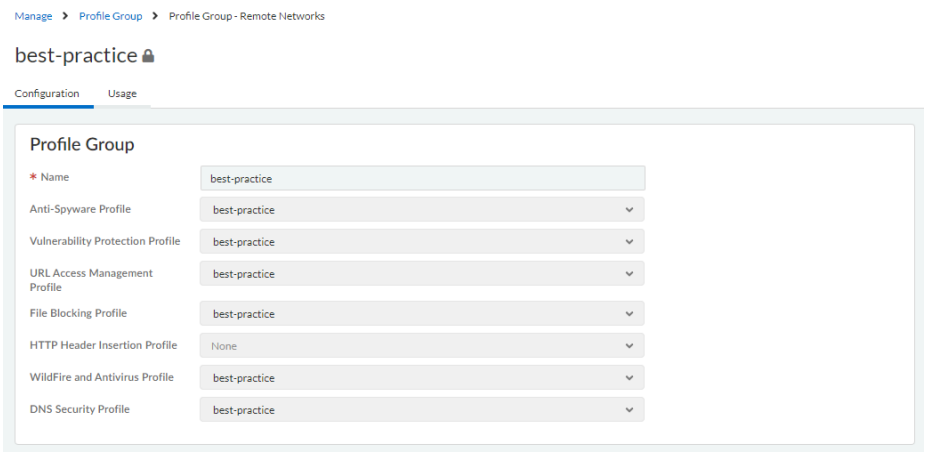
STEP 3 | 将安全配置文件附加到您的 **Security Policy Rules**（安全策略规则）。Prisma Access 默认执行最佳实践安全策略规则。

在配置安全策略规则时，如果检测到漏洞利用或尝试获取未经授权的访问，该规则会使用漏洞防护配置文件进行阻止，*Prisma Access* 会自动阻止该流量并记录这些事件（参阅监控被阻止的 IP 地址）。

1. 选择 **Manage**（管理） > **Configuration**（配置） > **NGFW** 和 **Prisma Access** > **Security Services**（安全服务） > **Security Policy**（安全策略），并选择要修改的规则或 **Add Rule**（添加规则）。
2. 在 **Action and Advanced Inspection**（操作和高级检查）中，选择 **Profile Group**（配置文件组），其中包括以下安全配置文件：**WildFire and Antivirus**（**WildFire** 和防病毒）、**Anti-Spyware**（防间谍软件）和 **Vulnerability Protection**（漏洞防护）。

   在 ***Manage***（管理） > ***Configuration***（配置） > ***NGFW*** 和 ***Prisma Access*** > ***Security Services***（安全服务） > ***Profile Groups***（配置文件组）中，您可以创建新配置文件组。有关更多信息，请参阅启用安全配置文件。

   默认情况下会启用最佳实践配置文件组，其中包含所有可用安全配置文件的最佳实践配置。



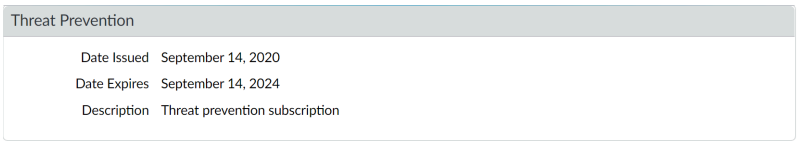
STEP 4 | 提交更改。

设置防病毒威胁、防间谍软件和漏洞防护 (NGFW (Managed by PAN-OS or Panorama))

Palo Alto Networks 定义所有防间谍软件和漏洞防护签名的默认操作。要查看默认操作，请选择 ***Objects***（对象） > ***Security Profiles***（安全配置文件） > ***Anti-Spyware***（防间谍软件）或 ***Objects***（对象） > ***Security Profiles***（安全配置文件） > ***Vulnerability Protection***（漏洞防护），然后选择一个配置文件。单击 *Exceptions*（例外）选项卡，然后单击 *Show all signatures*（显示所有签名），以查看签名列表和相应的默认 ***Action***（操作）。要更改默认操作，请创建一个新的配置文件，并在配置文件中指定一个 ***Action***（操作）和/或将个别签名异常添加到 ***Exceptions***（例外）。

STEP 1 | 验证您是否具有威胁阻止订阅。

威胁阻止订阅将抗病毒、防间谍软件和漏洞防护功能绑定在一个许可证中。要验证是否具有有效的威胁防护订阅，选择 **Device**（设备） > **Licenses**（许可证），并验证 **Threat Prevention**（威胁阻止）过期日期是否设置为将来。



STEP 2 | 下载最新内容。

1. 选择 **Device**（设备） > **Dynamic Updates**（动态更新），然后单击页面底部的 **Check Now**（立即检查）以检索最新签名。
2. 在 **Actions**（操作）列中，单击 **Download**（下载）安装最新的防病毒更新，然后下载，并 **Install**（安装）最新的应用程序和威胁更新。

STEP 3 | 安排内容更新。

有关部署更新的重要信息，请查阅应用程序和威胁内容更新的最佳实践。

1. 选择 **Device**（设备） > **Dynamic Updates**（动态更新），然后单击 **Schedule**（计划），以自动检索 **Antivirus**（防病毒）和 **Applications and Threats**（应用程序和威胁）的签名更新。
2. 指定更新的频率和时间：
   - **download-only**（仅下载）— 防火墙根据您定义的计划自动下载最新更新，但必须手动 **Install**（安装）。
   - **download-and-install**（下载并安装）— 防火墙根据您定义的计划自动下载并安装更新。
3. 单击 **OK**（确定）以保存更新计划；无需提交。
4. （可选）定义 **Threshold**（阈值），以指示在防火墙下载之前更新可用的最短小时数。例如，将 **Threshold**（阈值）设置为 **10**，表示防火墙在至少 10 小时内不会下载更新，而不考虑计划如何。
5. （仅 HA）决定是否 **Sync To Peer**（同步到对端设备），使对端设备在下载和安装后能够同步内容更新（更新计划不会在对端设备之间同步；您必须手动配置两个对端设备的计划）。

   根据您的 HA 部署，决定是否及如何 **Sync To Peer**（同步到对端设备）时还需考虑其他注意事项：

   - 主动/被动 **HA** — 如果防火墙正在使用 MGT 端口进行内容更新，则请安排两个防火墙来单独下载和安装更新。但是，如果防火墙正在使用数据端口进行内容更新，则被动防火墙将不会下载或安装更新，除非变为活动状态。为了在使用数据端口进行更新时保持两个防火墙上的计划同步，请在两个防火墙上安排更新，然后启用 **Sync To Peer**（同步到对端设备），以便确定进行主动下载和安装更新，并将更新推送到被动防火墙。

- 主动/主动 **HA** — 如果防火墙正在使用 MGT 接口进行内容更新，请在两个防火墙上选择 **download-and-install**（下载并安装），但都不启用 **Sync To Peer**（同步到对端设备）。但是，如果防火墙正在使用数据端口，请在两个防火墙上选择 **download-and-install**（下载并安装），然后启用 **Sync To Peer**（同步到对端设备），以便在一个防火墙进入主动-辅助状态时，主动-主要防火墙将下载并安装更新，并将其推送到主动-辅助防火墙。

STEP 4 | （可选）创建防病毒、防间谍软件和漏洞防护的自定义安全配置文件。

或者，您可以使用预定义的默认或严格配置文件。

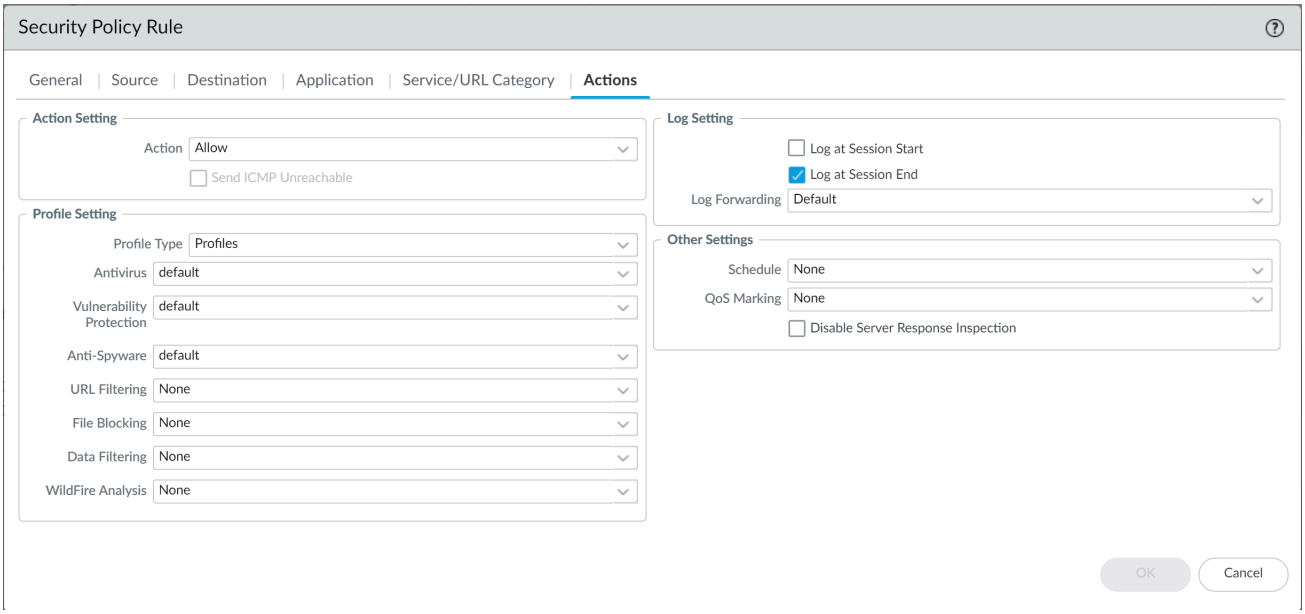
安全传输到最佳实践安全配置文件以实现最佳安全状态。

- 要创建自定义的防病毒配置文件，请选择 **Objects**（对象） > **Security Profiles**（安全配置文件） > **Antivirus**（防病毒）并 **Add**（添加）新配置文件。使用防病毒配置文件传输步骤安全实现您的目标。
- 要创建自定义的防间谍软件配置文件，请选择 **Objects**（对象） > **Security Profiles**（安全配置文件） > **Anti-Spyware**（防间谍软件）并 **Add**（添加）新配置文件。使用防间谍软件配置文件传输步骤安全实现您的目标。
- 要创建自定义的漏洞防护配置文件，请选择 **Objects**（对象） > **Security Profiles**（安全配置文件） > **Vulnerability Protection**（漏洞防护）并 **Add**（添加）新配置文件。使用漏洞防护配置文件传输步骤安全实现您的目标。

STEP 5 | 将安全配置文件附加到安全策略规则。

使用安全策略规则配置防火墙时，防火墙会使用漏洞防护配置文件来阻止连接，因此防火墙将自动阻止硬件中的流量（请参阅监控已阻止的 IP 地址）。

1. 选择 **Policies**（策略） > **Security**（安全），然后选择要修改的规则。
2. 在 **Actions**（操作）选项卡上，选择 **Profiles**（配置文件）作为 **Profile Type**（配置文件类型）。
3. 选择您为 **Antivirus**（防病毒）、**Anti-Spyware**（防间谍软件）和 **Vulnerability Protection**（漏洞防护）创建的安全配置文件。



STEP 6 | 提交更改。

单击 **Commit**（提交）。

配置内联云分析

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	❑ 高级威胁防护（用于增强功能支持）

内联云分析是一项高级威胁防护功能，可通过查询高级威胁防护云服务，实时检测高级、高规避的零日命令控制 (C2) 威胁以及命令注入和 SQL 注入漏洞。内联云分析保护通过您的防间谍软件和漏洞防护安全配置文件提供，前者处理高级 C2（命令和控制）和间谍软件威胁，后者处理命令注入和 SQL 注入漏洞。

对于支持运行 PAN-OS 11.2 及更高版本部署的防火墙，还可以访问本地深度学习以进行高级威胁防护。本地深度学习是对高级威胁防护中基于云的内联云分析组件的补充，它提供了一种对零日威胁和其他逃避威胁执行快速、基于本地深度学习的分析的机制。本地深度学习模型的更新通过内容更新提供。由于运行本地深度学习检测模块需要额外的系统资源，因此，本地深度学习仅在以下平台上可用：

- PA-5400 系列，不包括 PA-5450 设备。
- VM-Series（必须分配至少 16GB 的总内存）
- VM-Series 公共云
- VM-Series 私有云

要启用和配置内联云分析和本地深度学习，您必须激活高级威胁防护许可证，并创建（或修改）防间谍软件和漏洞防护安全配置文件。然后为每个类别分析引擎配置策略设置，然后将配置文件附加到安全策略规则。

有关创建安全策略规则的详细信息，请参阅《PAN-OS® 管理员指南》的策略一章。

- Strata Cloud Manager
- PAN-OS 和 Panorama

配置内联云分析（PAN-OS 和 Panorama）

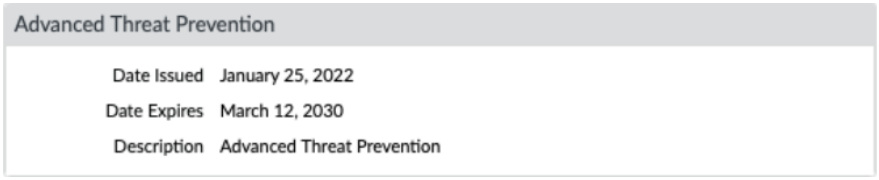
高级威胁防护内联云分析支持多个检测引擎，这些引擎需要不同的最低 *PAN-OS* 版本来启用：

- 检测高级 *C2*（命令和控制）和间谍软件威胁需要 *PAN-OS 10.2* 或更高版本。
- 检测零日漏洞利用威胁需要 *PAN-OS 11.0* 及更高版本。
- *LDL*（本地深度学习）支持需要 *PAN-OS 11.2* 及更高版本。

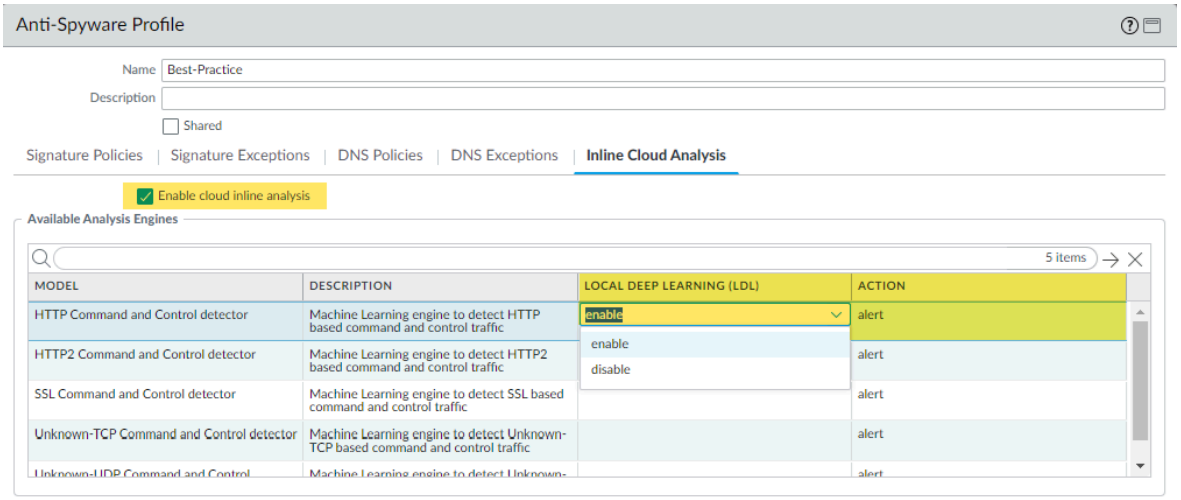
STEP 1 | 登录 PAN-OS Web 界面。

STEP 2 | 要利用内联云分析，必须订阅有效的高级威胁防护。

若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已过期。



STEP 3 | 更新或创建新的防间谍软件安全配置文件，启用内联云分析（实时分析高级 C2 [命令和控制]和间谍软件威胁的流量）。



1. 选择现有 **Anti-Spyware Profile**（防间谍软件配置文件），或者 **Add**（添加）新的配置文件（**Objects**（对象） > **Security Profiles**（安全配置文件） > **Anti-Spyware**（防间谍软件））。
2. 选择防间谍软件配置文件，然后转到 **Inline Cloud Analysis**（内联云分析）并 **Enable inline cloud analysis**（启用内联云分析）。
3. （本地深度学习 [PAN-OS 11.2 及更高版本中支持]）为每个带有 **Local Deep Learning (LDL)**（本地深度学习 **(LDL)**）选项的可用分析引擎选择 **Enable**（启用）。目前有两个带有可

选 LDL 模式的分析引擎：**HTTP Command and Control Detector**（**HTTP** 命令与控制检测器）和 **HTTP2 Command and Control Detector**（**HTTP2** 命令与控制检测器）。

4. 指定在使用相应的分析引擎检测到威胁时要执行的 **Action**（操作）。

   每个分析引擎的默认操作都是 ***Alert***（警报），但是，*Palo Alto Networks* 建议将所有操作设置为 ***Reset-Both***（重置二者），以实现最佳安全状态。

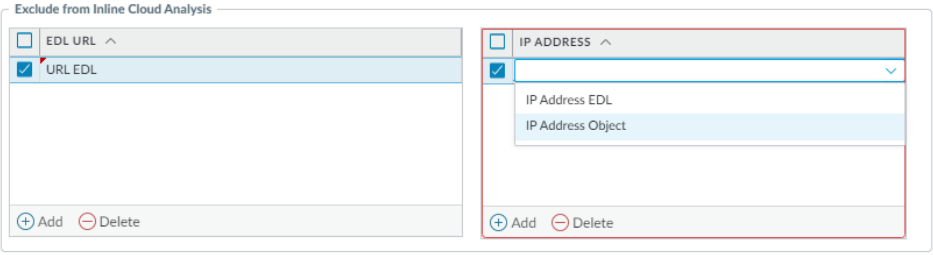
   - **Allow**（允许）— 允许请求且不生成任何日志条目。
   - **Alert**（警报）— 允许请求且生成威胁日志条目。
   - **Drop**（丢弃）— 丢弃请求；不向主机/应用程序发送重置操作。
   - **Reset-Client**（重置客户端）— 重置客户端一侧的连接。
   - **Reset-Server**（重置服务器）— 重置服务器一侧的连接。
   - **Reset-Both**（重置两者）— 重置客户端和服务器端的连接。

5. 单击 **OK**（确定）以退出防间谍软件配置文件的配置对话框，然后 **Commit**（提交）更改。

STEP 4 | （可选）如果内联云分析生成误报，请将 URL 和/或 IP 地址例外添加到您的防间谍软件配置文件中。您可以通过指定（URL 或 IP 地址列表类）外部动态列表或 **Address**（地址）对象来添加例外。

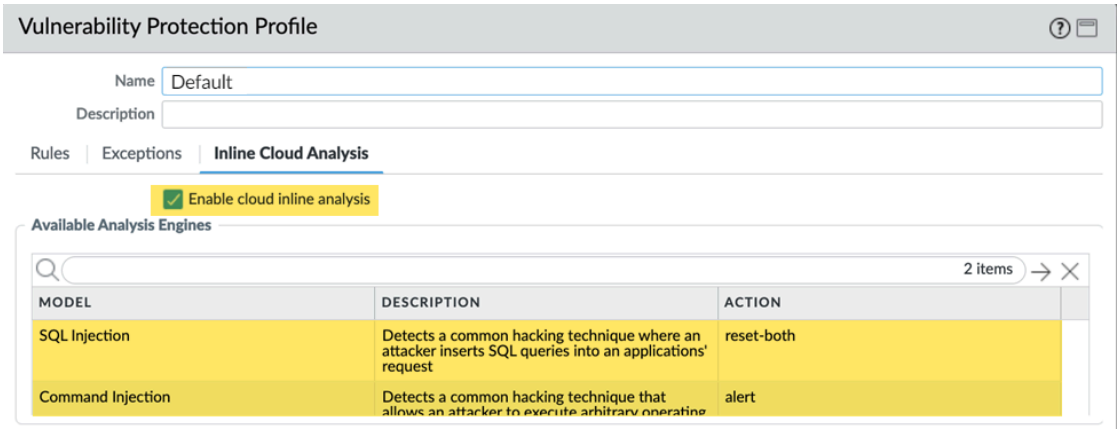
1. 添加 **External Dynamic Lists**（外部动态列表）或 **[IP] Addresses**（地址）对象例外。
2. 选择 **Objects**（对象）> **Security Profiles**（安全配置文件）> **Anti-Spyware**（防间谍软件）。
3. 选择要排除其特定 URL 和/或 IP 地址的防间谍软件配置文件，然后选择 **Inline Cloud Analysis**（内联云分析）。
4. 根据要添加的例外类型 **Add**（添加） **EDL URL** 或 **IP Address**（**IP** 地址），然后选择预先存在的 URL 或 IP 地址外部动态列表。如果没有可用列表，请创建一个新的外部动态列表。对于 IP 地址例外，您可以选择一个 **Address**（地址）对象列表。

   在 *Panorama* 托管的防火墙上配置为 ***Shared***（共享）的防间谍软件配置文件不能将 *IP* 地址对象添加到内联云分析例外列表中。



5. 单击 **OK**（确定）以保存防间谍软件配置文件，然后 **Commit**（提交）更改。

STEP 5 | （在 PAN-OS 11.0 及更高版本中支持）更新或创建新的漏洞防护安全配置文件，以启用内联云分析（实时分析命令注入和 SQL 注入漏洞的流量）。

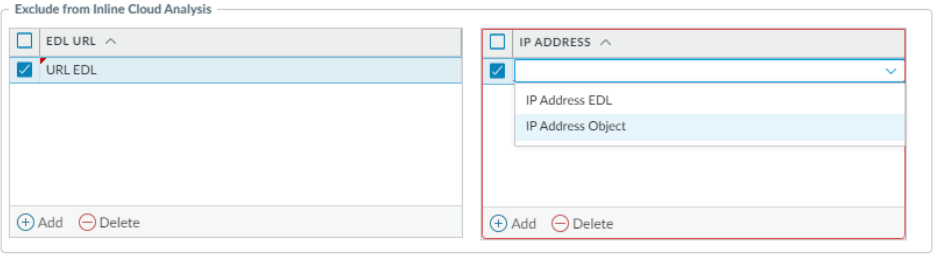


1. 选择现有的漏洞防护安全配置文件，或 **Add**（添加）新的配置文件（**Objects**（对象） > **Security Profiles**（安全配置文件） > **Vulnerability Protection**（漏洞防护））。
2. 选择您的漏洞防护配置文件，然后转到 **Inline Cloud Analysis**（内联云分析） 和**Enable Cloud Inline Analysis**（启用云内联分析）。
3. 指定在使用相应的分析引擎检测到漏洞利用时要执行的 **Action**（操作）。目前有两个可用的分析引擎：**SQL Injection**（SQL 注入）和 **Command Injection**（命令注入）。
   - **Allow**（允许）— 允许请求且不生成任何日志条目。
   - **Alert**（警报）— 允许请求且生成威胁日志条目。
   - **Reset-Client**（重置客户端）— 重置客户端一侧的连接。
   - **Reset-Server**（重置服务器）— 重置服务器一侧的连接。
   - **Reset-Both**（重置两者）— 重置客户端和服务器端的连接。
4. 单击 **OK**（确定）以退出漏洞防护配置文件的配置对话框，然后 **Commit**（提交）更改。

STEP 6 | （可选）如果内联云分析生成误报，请将 URL 和/或 IP 地址例外添加到您的漏洞防护配置文件中。您可以通过指定（URL 或 IP 地址列表类）外部动态列表或 **Address**（地址）对象来添加例外。

1. 添加 **External Dynamic Lists**（外部动态列表）或 **[IP] Addresses**（地址）对象例外。
2. 选择 **Objects**（对象）> **Security Profiles**（安全配置文件）> **Vulnerability**（漏洞）以返回漏洞防护配置文件。
3. 选择要排除其特定 URL 和/或 IP 地址的漏洞配置文件，然后选择 **Inline Cloud Analysis**（内联云分析）。
4. 根据要添加的例外类型 **Add**（添加） **EDL URL** 或 **IP Address**（**IP** 地址），然后选择预先存在的 URL 或 IP 地址外部动态列表。如果没有可用列表，请创建一个新的外部动态列表。对于 IP 地址例外，您可以选择一个 **Address**（地址）对象列表。

   对于在 *Panorama* 管理的防火墙上配置为 ***Shared***（共享）的漏洞配置文件，不能将 *IP* 地址对象添加到内联云分析例外列表中。



5. 单击 **OK**（确定）以保存漏洞防护配置文件，并 **Commit**（提交）更改。

STEP 7 | 配置超时延迟和当请求超过最大延迟时要执行的操作。

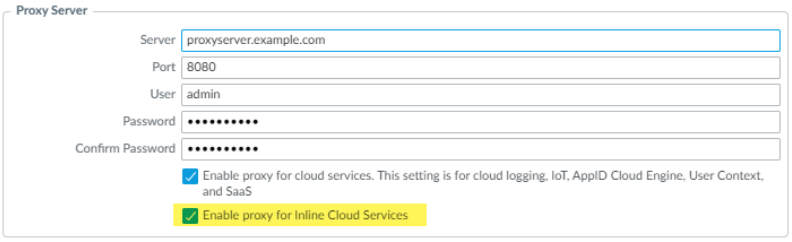
1. 选择 **Device**（设备）> **Setup**（设置）> **Content-ID** > **Threat Prevention Inline Cloud Analysis**（威胁防护内联云分析）。
2. 指定超时值和达到内联云分析请求的延迟限制时要执行的相关操作：
   - 最大延迟（毫秒）— 指定内联云分析返回结果的最长可接受处理时间（以毫秒为单位）。
   - 达到最大延迟时允许 — 使防火墙在达到最大延迟时执行“允许”操作。取消选择此选项会将防火墙操作设置为“阻止”。
   - 记录未扫描的流量 — 使防火墙记录表现出异常特征的流量请求，这些异常特征指示存在高级以及规避性命令和控制 (C2) 威胁，但这些威胁尚未由威胁防护内联云分析器处理。
3. 单击 **OK**（确定） 以确认您的更改。

STEP 8 | 为所有启用内联云分析的防火墙安装设备证书。

STEP 9 | （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。可以指定单个代理服务器，并应用于所有 Palo Alto Networks 更新服务，包括所有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. （仅适用于以下版本：PAN-OS 10.2.11 及更高版本和 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 10 | （可选）设置防火墙用于处理内联云分析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。

> 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。

验证防火墙是否使用您所在区域的正确内容云 FQDN（**Device**（设备） > **Setup**（设置） > **Content-ID**（内容 **ID**） > **Content Cloud Setting**（内容云设置）），并在必要时更改 FQDN：

> 如果您的 *NGFW* 采用内联方式配置，以便部署 *SaaS Security*，请注意，位于法国和日本的 *FQDN* 目前不支持 *SaaS Security* 功能。

- 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（瑞士苏黎世）— **ch.hawkeye.services-edge.paloaltonetworks.com**

STEP 11 | （可选）检查防火墙与高级威胁防护云服务的连接状态。

在防火墙上使用以下 CLI 命令查看连接状态。

```
show ctd-agent status security-client
```

例如：

```
show ctd-agent status security-client ...Security Client AceMlc2(1)
 Current cloud server: hawkeye.services-edge.paloaltonetworks.com
 Cloud connection: connected ...
```

> 为简洁起见，上述 *CLI* 输出进行了截短。

如果无法连接到高级威胁防护云服务，请确认以下域是否被阻止：hawkeye.services-edge.paloaltonetworks.com。

STEP 12 | （可选） 监控高级威胁防护

配置内联云分析 (Strata Cloud Manager)

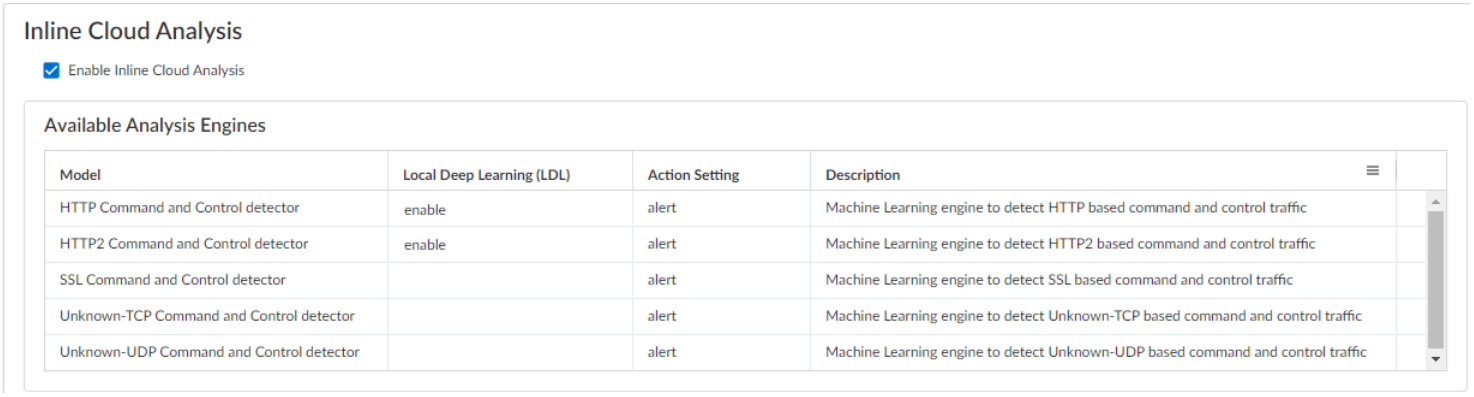
STEP 1 | 要利用在线云分析，您必须拥有有效的 Prisma Access 订阅，这样才能访问高级威胁防护功能。有关 Prisma Access 随附的应用程序和服务的信息，请参阅所有可用的应用程序和服务。

要验证您当前拥有有效许可证的订阅，请检查您的许可证支持哪些功能。

STEP 2 | 使用与 Palo Alto Networks 支持帐户关联的凭据，登录到中心的 Strata Cloud Manager。

STEP 3 | 更新或创建新的防间谍软件安全配置文件以启用在线云分析（实时分析高级 C2 [命令和控制]和间谍软件威胁的流量）。

1. 选择 **Manage**（管理） > **Configuration**（配置） > **NGFW** 和 **Prisma Access** > **Security Services**（安全服务） > **Anti-Spyware**（防间谍软件）。
2. 选择防间谍软件安全配置文件，然后导航到 **Inline Cloud Analysis**（内联云分析）面板并 **Enable Inline Cloud Analysis**（启用内联云分析）。



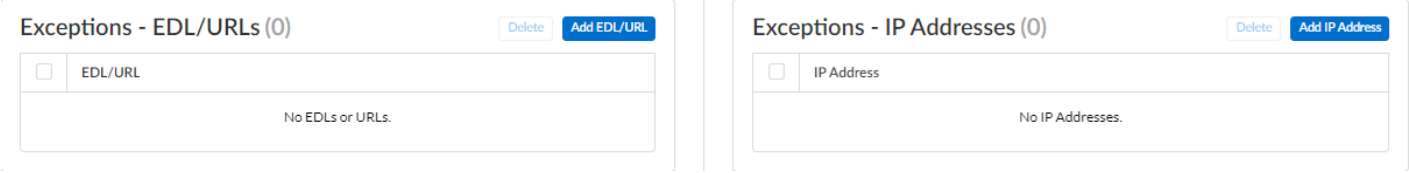
3. 使用 **Local Deep Learning (LDL)**（本地深度学习 **(LDL)**）选项为每个可用分析引擎选择 **Enable**（启用）。目前有两个带有可选 LDL 模式的分析引擎：**HTTP Command and Control Detector**（**HTTP** 命令与控制检测器）和 **HTTP2 Command and Control Detector**（**HTTP2** 命令与控制检测器）。
4. 指定在使用相应的分析引擎检测到威胁时要执行的 **Action**（操作）。

   每个分析引擎的默认操作都是 ***Alert***（警报），但是，*Palo Alto Networks* 建议将所有操作设置为 ***Reset-Both***（重置二者），以实现最佳安全状态。

   - **Allow**（允许）— 允许请求且不生成任何日志条目。
   - **Alert**（警报）— 允许请求且生成威胁日志条目。
   - **Drop**（丢弃）— 丢弃请求；不向主机/应用程序发送重置操作。
   - **Reset-Client**（重置客户端）— 重置客户端一侧的连接。
   - **Reset-Server**（重置服务器）— 重置服务器一侧的连接。
   - **Reset-Both**（重置两者）— 重置客户端和服务器端的连接。
5. 单击 **OK**（确定）以退出防间谍软件配置文件的配置对话框，然后 **Commit**（提交）更改。

STEP 4 | （可选）如果内联云分析生成误报，请将 URL 和/或 IP 地址例外添加到您的防间谍软件配置文件中。您可以通过指定外部动态列表（URL 或 IP 地址列表类）或 **Addresses**（地址）策略对象来添加例外。

1. 添加 **External Dynamic Lists**（外部动态列表）或 **[IP] Addresses**（地址）对象例外。
2. 选择 **Manage**（管理） > **Configuration**（配置） > **Anti-Spyware**（防间谍软件）。
3. 选择要排除其特定 URL 和/或 IP 地址的防间谍软件配置文件，然后转到 **Inline Cloud Analysis**（内联云分析）窗格。
4. 根据要添加的例外类型 **Add EDL/URL**（添加 **EDL/URL**）或 **Add IP Address**（添加 **IP** 地址），然后选择预先存在的 URL 或 IP 地址外部动态列表。如果没有可用的外部动态列表策略对象，则创建一个新的外部动态列表策略对象。对于 IP 地址例外，您可以选择一个 **Address**（地址）对象列表。



5. 单击 **OK**（确定）以保存防间谍软件配置文件，然后 **Commit**（提交）更改。

STEP 5 | （可选） 监控高级威胁防护

防止暴力攻击

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	❑ 高级威胁防护（用于增强功能支持）或威胁防护许可证

暴力攻击使用来自同一源或目标 IP 地址的大量请求/响应攻击系统。攻击者采用反复试验法猜出对挑战或请求的响应。

防火墙上的漏洞防护配置文件包括可用来防止暴力攻击的签名。每个签名都拥有 ID、威胁名称、严重性且在记录模式时触发。模式指定将流量识别为暴力攻击的条件和时间间隔；一些签名与另一个严重性较低的子签名关联，并用于指定要匹配的模式。当模式与签名或子签名匹配时，它会触发签名的默认操作。

要加强保护：

- 将漏洞防护配置文件附加至安全策略规则。请参阅设置防病毒威胁、防间谍软件和漏洞防护。
- 安装包含新签名的内容更新以防止新出现的威胁。请参阅安装内容和软件更新。

自定义暴力签名的操作和触发条件

在何处可以使用？	需要提供什么？
• NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ 高级威胁防护（用于增强功能支持）或威胁防护许可证

防火墙包括两种类型的预定义暴力签名：父签名和子签名。子签名是与签名匹配的流量模式的一个单一事件。父签名与子签名关联，并在指定时间间隔内发生多个事件且与在子签名中定义的流量模式匹配时触发。

通常，子签名的默认操作为*允许*，因为单个事件并不代表攻击。这样可确保不会阻止合法流量，并且也不会为不值得关注的事件生成威胁日志。Palo Alto Networks 建议您在更改默认操作前应仔细考虑。

在大多数情况下，暴力签名是一个值得关注的事件，因为它会频繁发生。如果需要，可以执行以下操作之一来自定义暴力签名的操作：

- 创建规则以修改暴力类别中所有签名的默认操作。可以选择允许、警报、阻止、重置或丢弃流量。
- 定义特定签名的例外。例如，可以搜索 CVE 并为其定义例外。

对于父签名，可以同时修改触发条件和操作；对于子签名，只能修改操作。

要有效地减轻攻击，请指定 *block-ip* 地址操作，而不是丢弃或重置大多数暴力签名的操作。

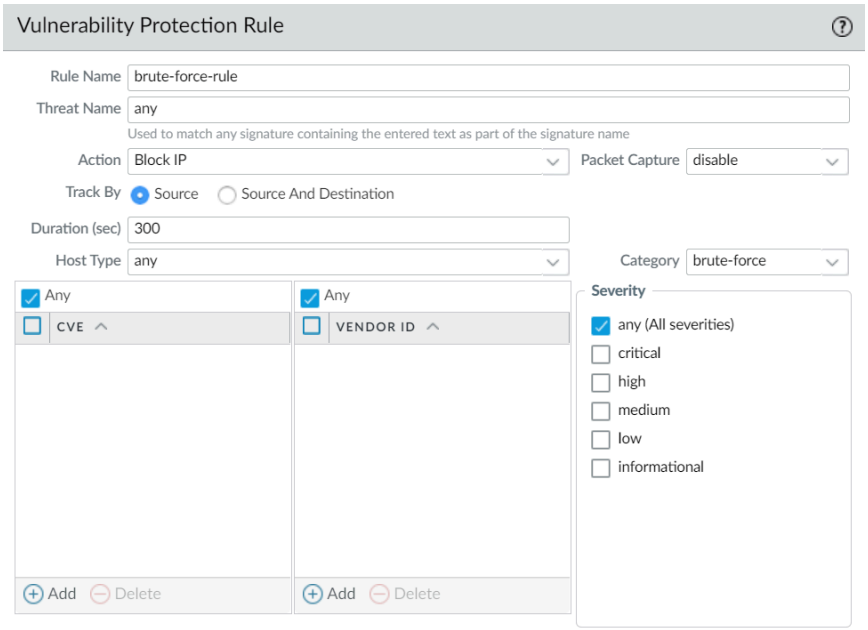
STEP 1 | 创建新的漏洞防护配置文件。

1. 选择 **Objects**（对象） > **Security Profiles**（安全配置文件） > **Vulnerability Protection**（漏洞防护）并 **Add**（添加）配置文件。
2. 输入漏洞防护配置文件的 **Name**（名称）。
3. （可选）输入 **Description**（说明）。
4. （可选）指定配置文件与以下内容 **Shared**（共享）：
   - **Every virtual system (vsys) on a multi-vsys firewall**（多虚拟系统防火墙上的每个虚拟系统 **(vsys)**）— 如果取消选中（禁用），该配置文件仅对 **Objects**（对象）选项卡中选择的虚拟系统可用。
   - **Every device group on Panorama**（**Panorama** 上的每个设备组）— 如果取消选中（禁用），该配置文件仅对 **Objects**（对象）选项卡中选择的设备组可用。
5. （可选 — 仅限 Panorama）选择 **Disable override**（禁用覆盖）可阻止管理员替代设备组中继承配置文件的漏洞防护配置文件的设置。默认情况下，未选中此选项，这意味着管理员可以替代继承配置文件的所有设备组的设置。

STEP 2 | 创建规则用于定义类别中所有签名的操作。

1. 在 **Rules**（规则）选项卡上，**Add**（添加）并输入新规则的 **Rule Name**（规则名称）。
2. （可选）指定特定的威胁名称（默认为 **any**（任何））。
3. 设置 **Action**（操作）。在本例中，将其设置为 **Block IP**（阻止 **IP**）。

   如果将漏洞防护配置文件设置为阻止 *IP*，则防火墙首先使用硬件来阻止 *IP* 地址。如果攻击流量超过硬件的阻止能力，则防火墙会使用软件阻止机制来阻止剩余的 *IP* 地址。
4. 将 **Category**（类别）设置为 **brute-force**（暴力）。
5. （可选）如果阻止，请指定要阻止的 **Host Type**（主机类型）：**server**（服务器） 或 **client**（客户端） （默认为**any**（任何））。
6. 请参阅步骤 3 以自定义特定签名的操作。
7. 请参阅步骤 4 以自定义父签名的触发阈值。



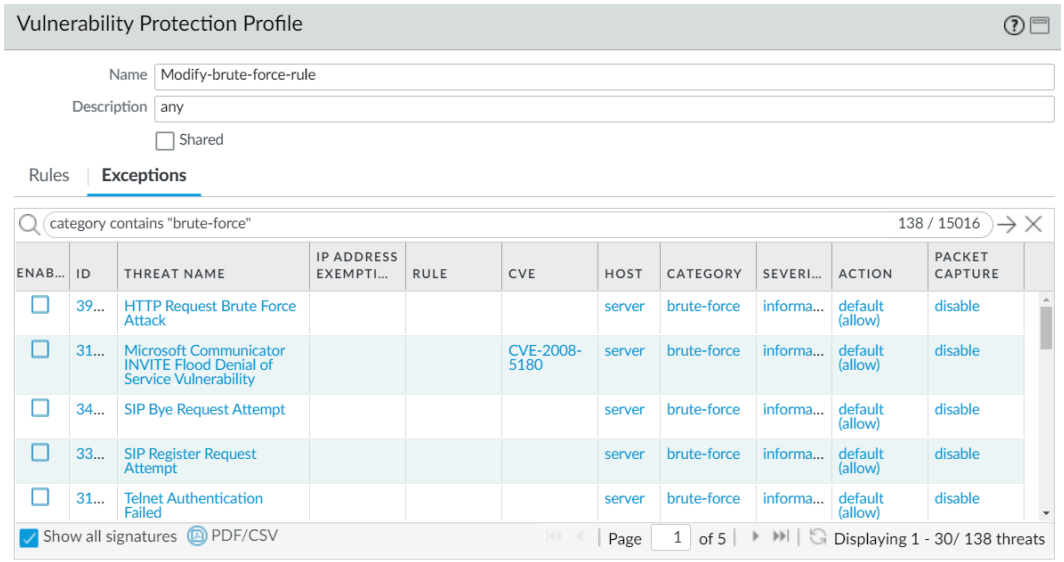
8. 单击 **OK**（确定）以保存规则和配置文件。

STEP 3 | （可选）自定义特定签名的操作。

1. 在 **Exceptions**（例外）选项卡上，**Show all signatures**（显示所有签名）以查找要修改的签名。

   要查看暴力类别中的所有签名，搜索 `category contains 'brute-force'`（包含"`brute-force`"的类别）。

2. 要编辑特定签名，单击 Action（操作）列中的预定义默认操作。



3. 设置操作：**Allow**（允许）、**Alert**（警报）、**Block Ip**（阻止 **Ip**）或 **Drop**（丢弃）。如果选择 **Block Ip**（阻止 **Ip**），请完成以下额外任务：
   1. 指定在之后触发操作的 **Time**（时间）段（以秒为单位）。
   2. 指定是否使用 **IP source**（IP 源）或 **IP source and destination**（IP 源和目标）**Track By**（跟踪标准）并阻止 IP 地址。
4. 单击 **OK**（确定）。
5. 对于每一个修改的签名，选中 **Enable**（启用）列中的复选框。
6. 单击 **OK**（确定）。

STEP 4 | 自定义父签名的触发条件。

可以编辑的父签名使用此图标标记：。

在本例中，搜索条件为暴力类别和 CVE-2008-1447。

1. 编辑 ( ) 签名的时间属性和聚合条件。
2. 要修改触发阈值，请指定每 **seconds**（秒）的 **Number of Hits**（击中数）。
3. 指定是否按 **source**（源）、**destination**（目标）或 **source-and-destination**（源到目标）汇总击中数（**Aggregation Criteria**（聚合标准））。
4. 单击 **OK**（确定）。

STEP 5 | 将新配置文件附加到安全策略规则。

1. 选择 **Policies**（策略） > **Security**（安全），并 **Add**（添加）或修改安全策略规则。
2. 在 **Actions**（操作）选项卡上，选择 **Profiles**（配置文件）作为配置文件设置的 **Profile Type**（配置文件类型）。
3. 选择您的 **Vulnerability Protection**（漏洞防护）配置文件。
4. 单击 **OK**（确定）。

STEP 6 | 提交更改。

1. 单击 **Commit**（提交）。

启用规避签名

在何处可以使用？	需要提供什么？
• NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ 高级威胁防护（用于增强功能支持）或威胁防护许可证

Palo Alto Networks 规避签名检测创建的 HTTP 或 TLS 请求，并且可以向客户端连接到除 DNS 查询中指定域之外的域的实例提供警报。只有在防火墙还能够充当 DNS 代理并解析域名查询时，规避签名才有效。最佳实践是采取以下步骤启用规避签名。

STEP 1 | 启用客户端和服务器的防火墙中介，以充当 DNS 代理。

配置 DNS 代理对象，包括：

- 指定想要防火墙侦听 DNS 查询的接口。
- 定义防火墙将与其通信以解析 DNS 请求的 DNS 服务器。
- 设置防火墙无需联系 DNS 服务器即可在本地解析的静态 FQDN 到 IP 地址条目。
- 为已解析的主机名到 IP 地址映射启用缓存。

STEP 2 | 获取最新的应用程序和威胁内容版本（至少为内容版本 579 或更高版本）。

1. 选择**Device**（设备） > **Dynamic Updates**（动态更新）。
2. **Check Now**（立即检查）以获取最新的应用程序和威胁内容更新。
3. 下载并安装应用程序和威胁内容版本 579（或更高版本）。

STEP 3 | 定义防火墙如何执行与规避签名相匹配的流量。

1. 选择 **Objects**（对象） > **Security Profiles**（安全配置文件） > **Anti-Spyware**（防间谍软件），然后 **Add**（添加）或修改防间谍软件配置文件。
2. 选择 **Exceptions**（例外），然后选择 **Show all signatures**（显示所有签名）。
3. 基于关键字 `evasion`（规避）筛选签名。
4. 对于所有规避签名，将 **Action**（操作）设置为除允许或默认操作之外的任何设置（对于规避签名，默认操作为允许）。例如，将签名 ID 14978 和 14984 的 **Action**（操作）设置为 **alert**（警报）或 **drop**（丢弃）。
5. 单击 **OK**（确定）以保存更新后的防间谍软件配置文件。
6. 将防间谍软件配置文件附加至安全策略规则：选择 **Policies**（策略） > **Security**（安全），再选择要修改的目标策略，最后单击 **Actions**（操作）选项卡。在“配置文件设置”中，单击 **Anti-Spyware**（防间谍软件）旁边的下拉列表，然后选择刚修改的防间谍软件配置文件以执行规避签名。

STEP 4 | 提交更改。

单击 **Commit**（提交）。

创建威胁异常

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	❑ 高级威胁防护（用于增强功能支持）或威胁防护许可证

Palo Alto Networks 对威胁签名的建议默认操作（如阻止或警报）进行定义。您可以使用威胁 ID 将威胁特征从强制执行中排除，或者修改针对该威胁特征强制执行的操作。例如，您可以修改在网络上触发误报的威胁签名的操作。

配置防病毒、漏洞、间谍软件和 DNS 签名的威胁例外，以更改威胁处理方式。但是，在开始之前，请确保根据默认或最佳实践签名设置正确检测和处理威胁，以获得最佳安全状态：

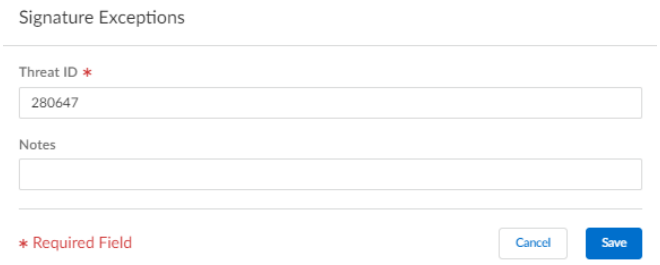
- 获取最新防病毒、威胁和应用程序以及 WildFire 签名更新（用于防火墙）。
- 设置防病毒威胁、防间谍软件和漏洞防护并将这些安全配置文件应用到安全策略。
- Strata Cloud Manager
- PAN-OS 和 Panorama

创建威胁异常 (Strata Cloud Manager)

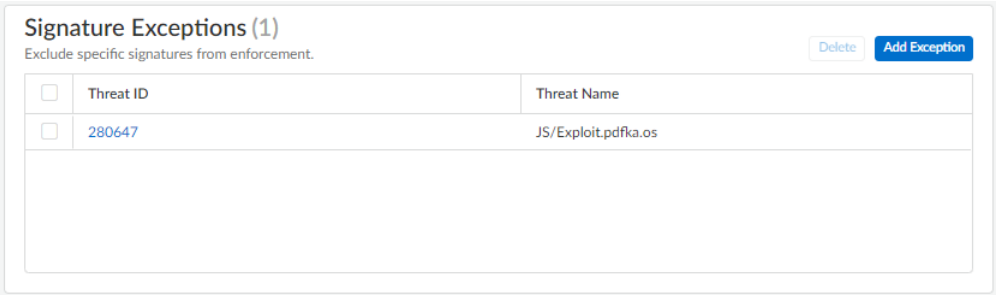
STEP 1 | 从执行中排除防病毒签名。

虽然您可以使用 *WildFire* 和防病毒 配置文件将防病毒签名排除在处理范围之外，但您无法更改针对特定防病毒签名强制执行的操作。但是，您可以编辑安全配置文件强制执行的操作，从而定义在不同类型的流量中发现病毒时可执行的操作。

1. 选择 **Manage**（管理） > **Configuration**（配置） > **NGFW** 和 **Prisma Access** > **Security Services**（安全服务） > **WildFire and Antivirus**（**WildFire** 和防病毒）。
2. **Add Profile**（添加配置文件）或选择要从中排除威胁签名的现有 WildFire 和防病毒配置文件，然后转到 **Advanced Settings**（高级设置）选项卡。
3. 在 **Signature Exceptions**（签名例外）菜单中**Add Exception**（添加例外），并提供要从强制执行中排除的威胁签名的 **Threat ID**（威胁 **ID**）。您可以选择要在签名异常中添加注释。



4. 完成后 **Save**（保存）签名例外。
5. 威胁名称字段中会自动填充有效的威胁签名 ID。您可以查看活动签名例外情况的完整列表，也可以 **Delete**（删除）不再需要的条目。

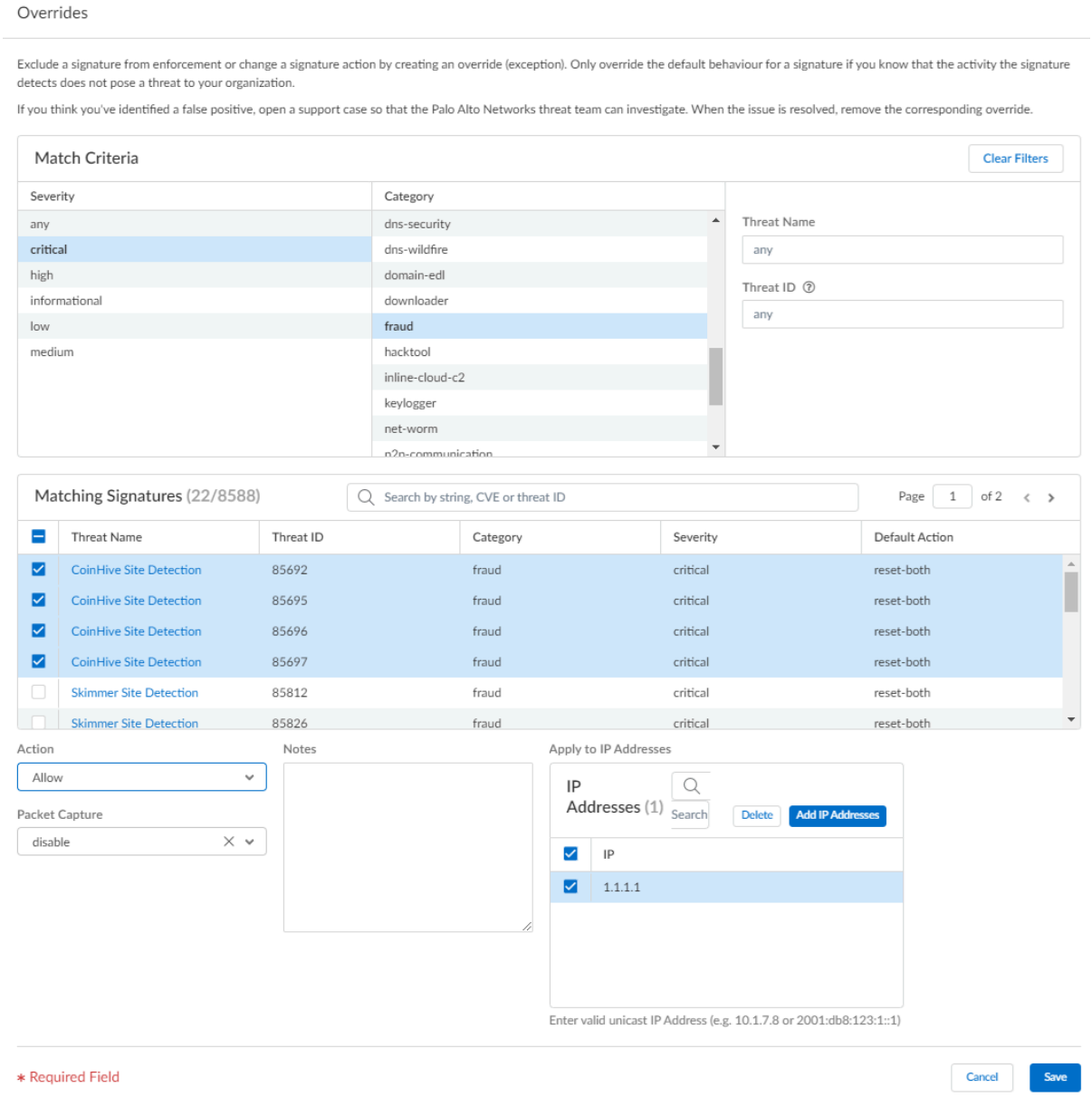


6. 重复添加其他例外，或在添加所有威胁例外后单击 **Save**（保存）。

STEP 2 | 修改漏洞和间谍软件签名（DNS 签名除外；虽然它们是间谍软件签名，但 DNS 签名通过 Prisma Access 中的 DNS 安全订阅进行处理）。

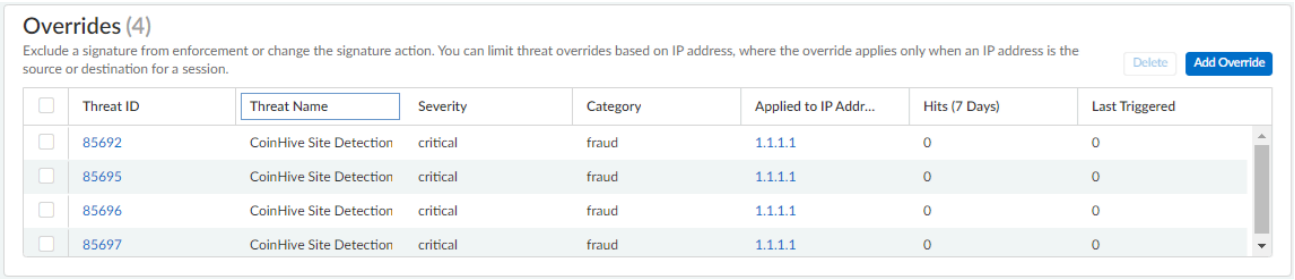
1. 根据签名类型，选择 **Manage**（管理） > **Configuration**（配置） > **NGFW** 和 **Prisma Access** > **Security Services**（安全服务） > **Anti-Spyware**（防间谍软件），或选择 **Manage**（管理） > **Configuration**（配置） > **NGFW** 和 **Prisma Access** > **Security Services**（安全服务） > **Vulnerability Protection**（漏洞防护）。
2. **Add Profile**（添加配置文件）或选择要修改签名强制的现有防间谍软件或漏洞防护配置文件，然后选择 **Add Override**（添加覆盖）。

3. 通过提供相关的 **Match Criteria**（匹配标准）来搜索间谍软件或漏洞签名。这将自动筛选可用签名并在 **Matching Signatures**（匹配签名）部分显示结果。
4. 选中与要修改强制执行的签名对应的复选框。
5. 提供所选签名的更新的 **Action**（操作）、**Packet Capture**（数据包捕获）和 **IP Addresses**（**IP** 地址），即您希望修改后的强制规则对其适用的操作。



6. **Save**（保存）更新后的签名强制配置。

7. 您可以查看 **Overrides**（覆盖）的完整列表，包括各种统计信息，也可以 **Delete**（删除）不再需要的条目。

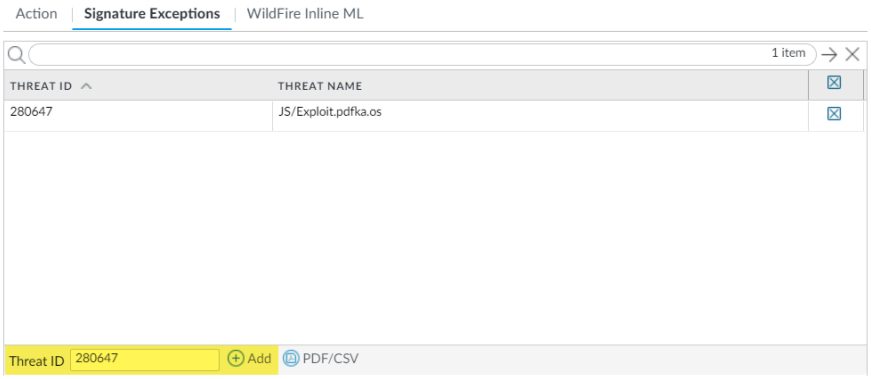


创建威胁异常 (NGFW (Managed by PAN-OS or Panorama))

STEP 1 | 从执行中排除防病毒签名。

虽然您可以使用防病毒配置文件将防病毒签名从执行中排除，但无法更改防火墙对特定防病毒签名执行的操作。但是，您可以通过编辑解码器（***Objects***（对象）**>** ***Security Profiles***（安全配置文件）**>** ***Antivirus***（防病毒）**>** ***<antivirus-profile>*** **>** ***Antivirus***）来定义防火墙的操作，以处理不同类型流量中的病毒。

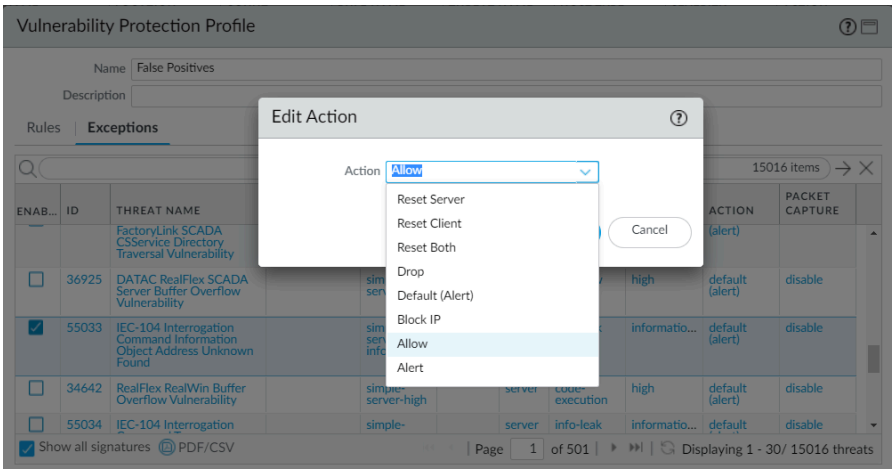
1. 选择 **Objects**（对象）**>** **Security Profiles**（安全配置文件）**>** **Antivirus**（防病毒）。
2. **Add**（添加）或修改要从中排除威胁签名的现有防病毒配置文件，然后选择 **Signature Exception**（签名例外）。
3. **Add**（添加）要从执行中排除的威胁签名的 **Threat Id**（威胁 **ID**）。



4. 单击 **OK**（确定）以保存防病毒配置文件。

STEP 2 | 修改对漏洞和间谍软件签名的执行（DNS 签名除外；跳到下一个选项以修改 DNS 签名的执行，这是一种间谍软件签名）。

1. 选择 **Objects**（对象） > **Security Profiles**（安全配置文件） > **Anti-Spyware**（防间谍软件）或 **Objects**（对象） > **Security Profiles**（安全配置文件） > **Vulnerability Protection**（漏洞防护）。
2. **Add**（添加）或修改要排除威胁签名的现有防间谍软件或漏洞防护配置文件，然后选择 **Signature Exceptions**（签名例外）（对于防间谍保护配置文件）或 **Exceptions**（例外）（对于漏洞防护配置文件）。
3. **Show all signatures**（显示所有签名），然后筛选以选择要修改其执行规则的签名。
4. 对于您想要修改其实施的签名，勾选 **Enable**（启用）列下的复选框。
5. 选择让防火墙处理该威胁签名的 **Action**（操作）。



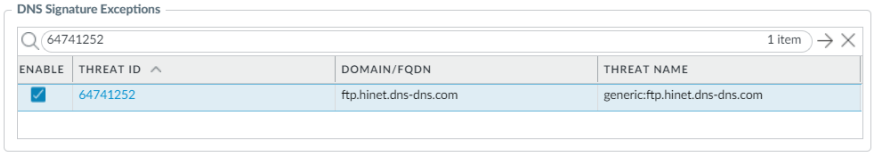
对于要从执行中排除的签名，因为这些签名会触发误报，请将 **Action**（操作）设置为 **Allow**（允许）。

6. 单击 **OK**（确定）以保存新的或修改过的防间谍软件或漏洞防护配置文件。

STEP 3 | 修改 DNS 签名的执行。

默认情况下，对侦测到 DNS 签名的恶意主机名的 DNS 查找将被 sinkhole。

1. 选择 **Objects**（对象） > **Security Profiles**（安全配置文件） > **Anti-Spyware**（防间谍软件）。
2. **Add**（添加）或修改要从中排除威胁签名的防间谍软件配置文件，然后选择 **DNS Exceptions**（**DNS** 例外）。
3. 搜索要从执行中排除的 DNS 签名的 DNS 威胁 ID，然后选择相应签名的方框：



4. 单击 **OK**（确定）以保存新的或修改过的防间谍软件配置文件。

使用 DNS 查询来确定网络上受感染的主机

在何处可以使用？	需要提供什么？
• NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ 高级威胁防护（用于增强功能支持）或威胁防护许可证

防间谍软件配置文件中的 DNS Sinkhole 操作可让防火墙对已知恶意域或自定义域的 DNS 查询伪造响应，以便您能够在网络上识别已被恶意软件感染的主机。受影响的主机可能通过命令和控制 (C2) 服务器启动通讯—一旦实现连接，攻击者可远程控制受感染的主机，从而进一步渗透网络或外泄数据。

对 Palo Alto Networks DNS 签名列表中包括的任何域的 DNS 查询将被 sinkhole 到 Palo Alto Networks 服务器 IP 地址。

防火墙有两个 DNS 签名源，可用于识别恶意和 C2 域：

- （需要高级 | 威胁防护订阅）本地 DNS 签名 — 这是一组有限的内置 DNS 签名，防火墙可以使用它来识别恶意域。防火墙获得新 DNS 签名作为日常防病毒更新的一部分。
- （需要 DNS 安全订阅）DNS 安全签名 — 防火墙访问 Palo Alto Networks DNS 安全云服务，以检查是否有针对 DNS 签名完整数据库的恶意域。特定签名—仅由 DNS 安全提供—可专门检测使用机器学习技术的 C2 攻击，比如域生成算法 (DGA) 和 DNS 隧道。有关 DNS 安全订阅的更多信息，请参阅《DNS 安全指南》。

  如果您想要为 DNS 安全签名指定 Sinkhole 操作，则可以在 DNS 安全配置文件中配置这些设置。

本地 DNS 签名集或 DNS 安全签名集内域的 DNS 查询被导向至 Palo Alto Networks 服务器，而主机无法访问恶意域。下列主题提供了有关如何启用 DNS Sinkholing 以便您识别受感染的主机的详细信息。

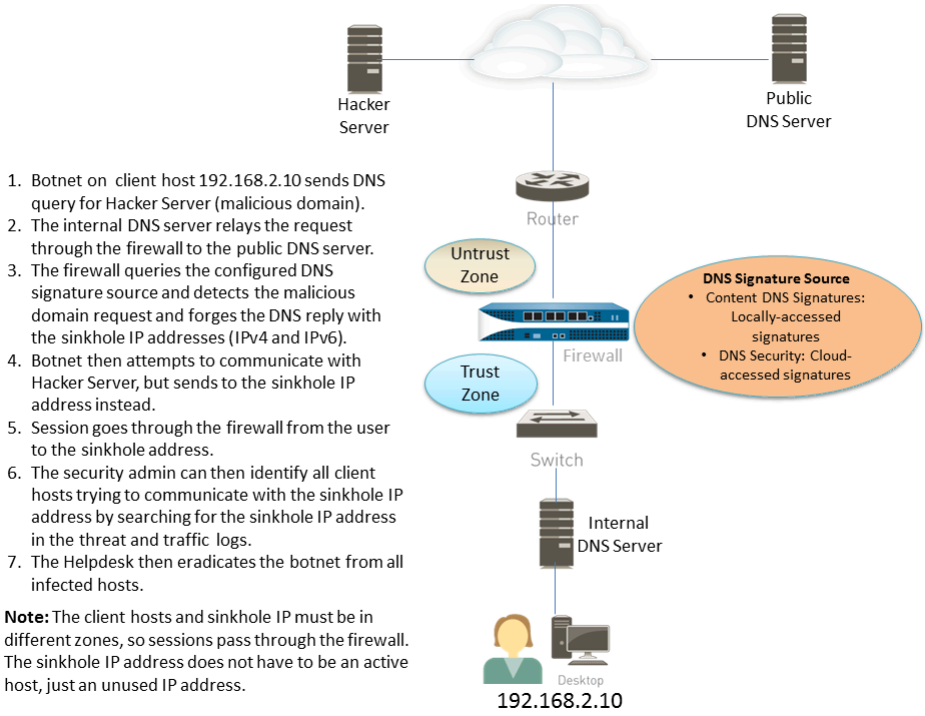
- DNS Sinkholing 的工作原理
- 配置 DNS Sinkholing
- 为自定义域列表配置 DNS Sinkholing
- 将 Sinkholing IP 地址配置为网络上的本地服务器
- 查看试图连接到恶意域的受感染主机

DNS Sinkholing 的工作原理

在何处可以使用？	需要提供什么？
• NGFW (Managed by PAN-OS or Panorama) • VM-SERIES	❑ 高级威胁防护（用于增强功能支持）或威胁防护许可证

在何处可以使用？	需要提供什么？
• CN-Series	

DNS Sinkholing 可帮助您在防火墙无法看到受感染的 DNS 查询的情况下识别受使用 DNS 流量的网络保护的感染主机（即防火墙无法看到 DNS 查询的始发者）。在防火墙在本地 DNS 服务器中检测不到任何内容的典型部署中，威胁日志将确定本地 DNS 解析器作为流量的来源，而不是实际受感染的主机。Sinkholing 恶意 DNS 查询通过伪造对恶意域中定向客户端主机查询的响应解决这种可见性问题，以便客户端试图连接到恶意域（如对于命令和控制），而不是试图连接到默认的 Palo Alto Networks Sinkhole IP 地址（或当您选择为自定义域列表配置 DNS Sinkholing 时定义的 IP 地址）。可在流量日志中轻松识别受感染的主机。



配置 DNS Sinkholing

在何处可以使用？	需要提供什么？
• NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ 高级威胁防护（用于增强功能支持）或威胁防护许可证

要启用 DNS Sinkholing，请将默认的防间谍软件配置文件附加到防火墙安全策略规则（请参阅设置防病毒威胁、防间谍软件和漏洞防护）。对 Palo Alto Networks DNS 签名源中包括的任何域的 DNS 查询将被解析到默认的 Palo Alto Networks Sinkhole IP 地址。IP 地址当前为 IPv4 — sinkhole.paloaltonetworks.com，回环地址当前为 Ipv6 地址 — ::1。这些地址可能出现变更，可随内容更新而更新。

STEP 1 | 为外部动态列表中的自定义域列表启用 DNS Sinkholing。

1. 选择 **Objects**（对象） > **Security Profiles**（安全配置文件） > **Anti-Spyware**（防间谍软件）。
2. 修改现有配置文件，或者从现有的默认配置文件中选择一个并进行克隆。
3. 为配置文件 **Name**（命名），然后选择 **DNS Policies**（**DNS** 策略）选项卡。
4. 确认 **Signature Source**（签名源）中是否存在 **default-paloalto-dns**。
5. （可选）在 **Packet Capture**（数据包捕获）下拉列表中，选择 **single-packet**（单个数据包）以捕获会话的第一个数据包，或选择 **extended-capture**（扩展捕获）以设置为 1-50 个数据包之间的值。然后您可使用数据包捕获进行进一步分析。

STEP 2 | 验证防间谍软件配置文件中的启用 Sinkholing 设置。

1. 在 **DNS Policies**（**DNS** 策略）选项卡中，确认 DNS 查询的 **Policy Action**（策略操作）是否为 **Sinkhole**。
2. 在“DNS Sinkhole 设置”部分中，确认是否已启用 **Sinkhole** 。为方便起见，已设置访问 Palo Alto Networks 服务器的默认 Sinkhole IP 地址。Palo Alto Networks 可通过内容更新自动刷新此 IP 地址。

   如果想要修改到网络上的本地服务器或回环地址的 **Sinkhole Ipv4** 或 **Sinkhole Ipv6** 地址，请参阅将 Sinkholing IP 地址配置为网络上的本地服务器。
3. 单击 **OK**（确定）以保存防间谍软件配置文件。

STEP 3 | 将防间谍软件配置文件附加至安全策略规则。

1. 选择 **Policies**（策略） > **Security**（安全），然后选择安全策略规则。
2. 在 **Actions**（操作）选项卡上，选中 **Log at Session Start**（在会话开始时记录）复选框以启用日志记录。
3. 在配置设置部分中，单击 **Profile Type**（配置类型）下拉列表以查看所有 **Profiles**（配置文件）。在 **Anti-Spyware**（防间谍软件）下拉列表中选择新的配置文件。
4. 单击 **OK**（确定）以保存策略规则。

STEP 4 | 通过监控防火墙上的活动，测试策略操作是否已实施。

1. 选择 **ACC** 并添加 URL 域作为查看访问域的威胁活动和阻止的活动的全局筛选器。
2. 选择 **Monitor**（监控） > **Logs**（日志） > **Threat**（威胁），并通过 `(action eq sinkhole)` 筛选以查看被 Sinkhole 的域上的日志。

为自定义域列表配置 DNS Sinkholing

在何处可以使用？	需要提供什么？
• NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ 高级威胁防护（用于增强功能支持）或威胁防护许可证

要为自定义域列表启用 DNS Sinkholing，必须创建包括域的外部动态列表，在防间谍软件配置文件中启用 Sinkhole 操作，并将配置文件附加到安全策略规则。当客户端尝试访问列表中的某个恶意域时，防火墙会将数据包中的目标 IP 地址伪造为默认的 Palo Alto Networks 服务器或用户针对 Sinkholing 定义的 IP 地址。

对于外部动态列表中包括的每个自定义域，防火墙将生成基于 DNS 的防间谍软件签名。签名将被命名为 Custom Malicious DNS Query <domain name>，属于中等严重性类型的间谍软件；每个签名为域名的 24 字节哈希值。

有关域列表条目限制的信息，请参阅外部动态列表。

STEP 1 | 为外部动态列表中的自定义域列表启用 DNS Sinkholing。

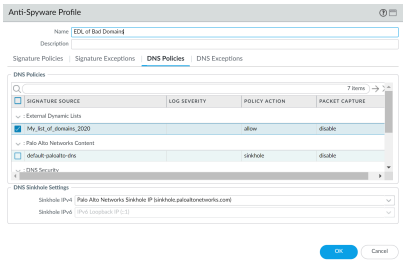
1. 选择 **Objects**（对象） > **Security Profiles**（安全配置文件） > **Anti-Spyware**（防间谍软件）。
2. 修改现有配置文件，或者从现有的默认配置文件中选择一个并进行克隆。
3. 为配置文件 **Name**（命名），然后选择 **DNS Policies**（**DNS** 策略）选项卡。
4. 从 **External Dynamic Lists**（外部动态列表）签名源中选择 EDL。

   如果您已创建***Domain List***（域列表）类型的外部动态列表，您可以从此处选择。此列表不显示您可能创建的 *URL* 或 *IP* 地址类型的外部动态列表。
5. 从防间谍软件配置文件配置外部动态列表（请参阅将防火墙配置为访问外部动态列表）。**Type**（类型）预设为 **Domain List**（域列表）。
6. （可选）在 **Packet Capture**（数据包捕获）下拉列表中，选择 **single-packet**（单个数据包）以捕获会话的第一个数据包，或选择 **extended-capture**（扩展捕获）以设置为 1-50 个数据包之间的值。然后您可使用数据包捕获进行进一步分析。

STEP 2 | 验证防间谍软件配置文件中的启用 Sinkholing 设置。

1. 在 **DNS Policies**（**DNS** 策略）选项卡中，确认 DNS 查询的 **Policy Action**（策略操作）是否为 **Sinkhole**。
2. 在“DNS Sinkhole 设置”部分中，确认是否已启用 **Sinkhole** 。为方便起见，已设置访问 Palo Alto Networks 服务器的默认 Sinkhole IP 地址。Palo Alto Networks 可通过内容更新自动刷新此 IP 地址。

   如果想要修改到网络上的本地服务器或回环地址的 **Sinkhole Ipv4** 或 **Sinkhole Ipv6** 地址，请参阅将 Sinkhole IP 地址配置为网络上的本地服务器。



3. 单击 **OK**（确定）以保存防间谍软件配置文件。

STEP 3 | 将防间谍软件配置文件附加至安全策略规则。

1. 选择 **Policies**（策略） > **Security**（安全），然后选择安全策略规则。
2. 在 **Actions**（操作）选项卡上，选中 **Log at Session Start**（在会话开始时记录）复选框以启用日志记录。
3. 在配置设置部分中，单击 **Profile Type**（配置类型）下拉列表以查看所有 **Profiles**（配置文件）。在 **Anti-Spyware**（防间谍软件）下拉列表中选择新的配置文件。
4. 单击 **OK**（确定）以保存策略规则。

STEP 4 | 测试是否实施了策略操作。

1. 查看外部动态列表条目（该条目属于域列表），并从列表中访问域。
2. 监控防火墙上的活动：
    1. 选择 **ACC** 并添加 URL 域作为查看访问域的威胁活动和阻止的活动的全局筛选器。
    2. 选择 **Monitor**（监控） > **Logs**（日志） > **Threat**（威胁），并通过 `(action eq sinkhole)` 筛选以查看被 Sinkhole 的域上的日志。

STEP 5 | 验证外部动态列表中的条目已忽略或跳过。

在防火墙上使用以下 CLI 命令查看列表的详细信息。

```
request system external-list show type domain name <list_name>
```

例如：

```
request system external-list show type domain name
 My_List_of_Domains_2015 vsys1/EBLDomain:Next update
 at :Thu May 21 10:15:39 2015 Source : https://1.2.3.4/
My_List_of_Domains_2015 Referenced :Yes Valid :Yes Number of
 entries :3 domains:www.example.com baddomain.com qqq.abcedfg.com
```

STEP 6 | （可选）按需检索外部动态列表。

要强制防火墙按需检索更新后的列表，而不是在下一次刷新时间间隔后进行检索（您为外部动态列表定义的 **Repeat**（重复）频率），使用以下 CLI 命令：

```
request system external-list refresh type domain name  <list_name>
```

或者，您可以使用防火墙接口从 Web 服务器检索外部动态列表。

将 Sinkholing IP 地址配置为网络上的本地服务器

在何处可以使用？	需要提供什么？
• NGFW (Managed by PAN-OS or Panorama) • VM-SERIES	☐ 高级威胁防护（用于增强功能支持）或威胁防护许可证

在何处可以使用？	需要提供什么？
• CN-Series	

默认情况下，将为所有 Palo Alto Networks DNS 签名启用 Sinkholing，且将设置访问 Palo Alto Networks 服务器的默认 Sinkhole IP 地址。如果想要将 Sinkhole IP 地址设置为网络上的本地服务器，请使用本部分中的说明。

必须获取要用作为 Sinkhole IP 地址的 IPv4 和 IPv6 地址，因为恶意软件可能使用这两种协议中的一种，也可能同时使用两种来执行 DNS 查询。DNS Sinkhole 地址必须位于与客户端主机所在区域不同的区域中，从而确保当受感染的主机尝试启动与 Sinkhole IP 地址的会话时，可通过防火墙进行路由。

该 *Sinkhole* 地址必须保留用于此目的，并且不需要分配给物理主机。您可以选择性地使用诱惑服务器作为物理主机，以进一步分析恶意流量。

要遵循的配置步骤使用以下示例 *DNS Sinkhole* 地址：

IPv4 DNS Sinkhole 地址—*10.15.0.20*

IPv6 DNS Sinkhole 地址—*fd97:3dec:4d27:e37c:5:5:5:5*

STEP 1 | 配置 Sinkhole 接口和区域

必须将客户端主机所在区域的流量转发到定义 Sinkhole IP 地址的区域，因此必须记录流量。

请为 *Sinkhole* 流量使用专用区域，因为受感染的主机会将流量发送到此区域。

1. 选择 **Network**（网络） > **Interfaces**（接口）并选择一个要配置为 Sinkhole 接口的接口。
2. 在 **Interface Type**（接口类型）下拉列表中，选择 **Layer3**（第 **3** 层）。
3. 要添加 IPv4 地址，请选择 **Ipv4** 选项卡，再选择 **Static**（静态），然后单击 **Add**（添加）。在本例中，请将 10.15.0.20 添加为 IPv4 DNS Sinkhole 地址。
4. 选择 **Ipv6** 选项卡并单击 **Static**（静态），然后单击 **Add**（添加）并输入 IPv6 地址和子网掩码。在本例中，请输入 fd97:3dec:4d27:e37c::/64 作为 IPv6 Sinkhole 地址。
5. 单击 **OK**（确定）以保存。
6. 要为 Sinkhole 添加一个区域，请选择 **Network**（网络） > **Zones**（区域）并单击 **Add**（添加）。
7. 输入区域 **Name**（名称）。
8. 在 **Type**（类型）下拉列表中，选择 **Layer3**（第 **3** 层）。
9. 在 **Interfaces**（接口）部分，单击 **Add**（添加）并添加您刚才配置的接口。
10. 单击 **OK**（确定）。

STEP 2 | 启用 DNS Sinkholing。

默认情况下，将为所有 Palo Alto Networks DNS 签名启用 Sinkholing。要将 Sinkhole 地址更改为本地服务器，请参阅为自定义域列表配置 DNS Sinkhole 中的第 2 步。

STEP 3 | 请编辑安全策略，以允许信任区域中客户端主机的流量流向非信任区域，从而包括 Sinkhole 区域作为目标，并附加防间谍软件配置文件。

编辑安全策略规则，以允许信任区域中的客户端主机的流量流向非信任区域，从而确保标识来自受感染主机的流量。通过将 Sinkhole 区域添加为规则中的目标，您可以让受感染的客户端向 DNS Sinkhole 发送伪造的 DNS 查询。

1. 选择 **Policies**（策略） > **Security**（安全）。
2. 选择允许客户端主机区域的流量流向非信任区域的现有策略。
3. 在 **Destination**（目标）选项卡上，**Add**（添加）Sinkhole 区域。这允许客户端主机流量流向 Sinkhole 区域。
4. 在 **Actions**（操作）选项卡上，选中 **Log at Session Start**（在会话开始时记录）复选框以启用日志记录。这样可以确保在访问非信任或 Sinkhole 区域时，来自信任区域的客户端主机的流量可以得到记录。
5. 在 **Profile Setting**（配置文件设置）部分，选择您启用 DNS Sinkholing 的 **Anti-Spyware**（防间谍软件）配置文件。
6. 单击 **OK**（确定）以保存安全策略，然后单击 **Commit**（提交）。

STEP 4 | 为了确认您可以识别受感染的主机，请验证从信任区域的客户端主机流向新的 Sinkhole 区域的流量得到了记录。

在本示例中，受感染的客户端主机是 192.168.2.10，而 Sinkhole IPv4 地址为 10.15.0.20。

1. 在信任区域的客户端主机中，打开命令提示窗口并运行以下命令：

```
C:\>ping <sinkhole address>
```

以下示例显示了对 DNS Sinkhole 地址 10.15.0.2 执行 Ping 请求所产生的输出，结果显示 `Request timed out`，这是因为在示例中，Sinkhole IP 地址未分配给物理主机：

```
C:\>ping 10.15.0.20 Pinging 10.15.0.20 with 32 bytes of
 data:Request timed out.Request timed out.Ping statistics for
 10.15.0.20:Packets:Sent = 4, Received = 0, Lost = 4 (100%
 loss)
```

2. 在防火墙上，选择 **Monitor**（监控） > **Logs**（日志） > **Traffic**（流量）并找到源为 192.168.2.10 且目标为 10.15.0.20 的日志条目。这将确认 Sinkhole IP 地址的流量正在流向防火墙区域。

您可以搜索和/或筛选日志，使其仅显示目标为 *10.15.0.20* 的日志。为此，请在 ***Destination***（目标）列中单击 *IP* 地址 *(10.15.0.20)*，这会将筛选条件 *(addr.dst in 10.15.0.20)* 添加到搜索字段。单击位于搜索字段右侧的“应用筛选器”图标以应用筛选条件。

STEP 5 | 测试 DNS Sinkholing 是否正确配置。

您正在模拟当恶意应用程序尝试调用主页时受感染的应用程序将执行的操作。

1. 找到防火墙的当前防病毒签名数据库中包括的一个恶意域以测试 Sinkholing。
   1. 选择 **Device**（设备） > **Dynamic**（动态）**Updates**（更新）并在 **Antivirus**（防病毒）部分单击当前安装的防病毒数据库的 **Release Notes**（发布说明）链接。您还可以在 Palo Alto Networks 支持站点上的动态更新下找到列出增量签名更新的防病毒发布说明。
   2. 在发布说明的第二列，找到带有域扩展名的一行项目（例如，com、edu 或 net）。左列将显示域名。例如，在防病毒版本 1117-1560 中，左列包括一个名为“tbsbana”的项目，且右列为“net”。

      下面显示了这一行在发布说明中的内容：

      ```
      conficker:tbsbana 1 variants: net
      ```
2. 在客户端主机上打开命令提示窗口。
3. 对您识别为恶意域的 URL 执行 NSLOOKUP。

   例如，使用 URL `track.bidtrk.com`:

   ```
   C:\>nslookup track.bidtrk.com Server: my-local-
   dns.local Address:10.0.0.222 Non-authoritative
    answer:Name: track.bidtrk.com.org Addresses:
    fd97:3dec:4d27:e37c:5:5:5:510.15.0.20
   ```

   在输出中，请注意恶意域的 NSLOOKUP 已使用配置的 Sinkhole IP 地址 (10.15.0.20) 进行伪造。由于该域与一个恶意 DNS 签名匹配，因此会执行 Sinkhole 操作。
4. 选择 **Monitor**（监控） > **Logs**（日志） > **Threat**（威胁）并找到相应的日志条目，从而验证对 NSLOOKUP 请求执行了正确的操作。
5. 对 **`track.bidtrk.com`** 执行 Ping，这将产生到 Sinkhole 地址的网络流量。

查看试图连接到恶意域的受感染主机

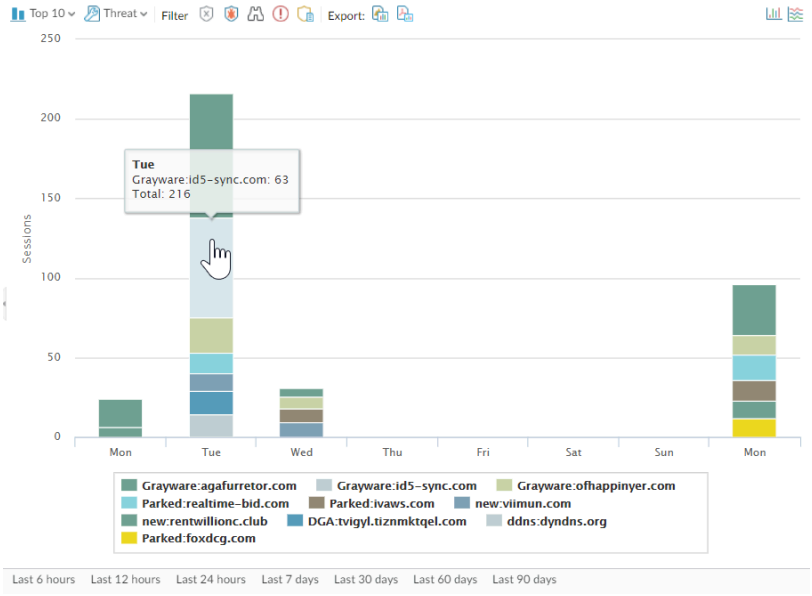
在何处可以使用？	需要提供什么？
• NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ 高级威胁防护（用于增强功能支持）或威胁防护许可证

在您配置 DNS Sinkholing 并验证恶意域的流量流向 Sinkhole 地址后，您应定期监控流向该 Sinkhole 地址的流量，从而跟踪受感染的主机并消灭威胁。

使用 App Scope 识别受感染的客户端主机。

1. 选择 **Monitor**（监控） > **App Scope**并选择 **Threat Monitor**（威胁监控）。
2. 单击显示页面顶部的 **Show spyware**（显示间谍软件）按钮。
3. 选择一个时间范围。

   以下屏幕截图显示了可以 DNS 查询的三个实例，均为测试客户端主机在已知恶意域上执行 NSLOOKUP 时产生。单击图表可查看关于事件的更多详细信息。



对自定义报告进行配置，从而识别将流量发送到 Sinkhole IP 地址的所有客户端主机，本例中为 10.15.0.20。

转发到 *SNMP* 管理器、*Syslog* 服务器和/或 *Panorama* 以对这些事件发出警报。

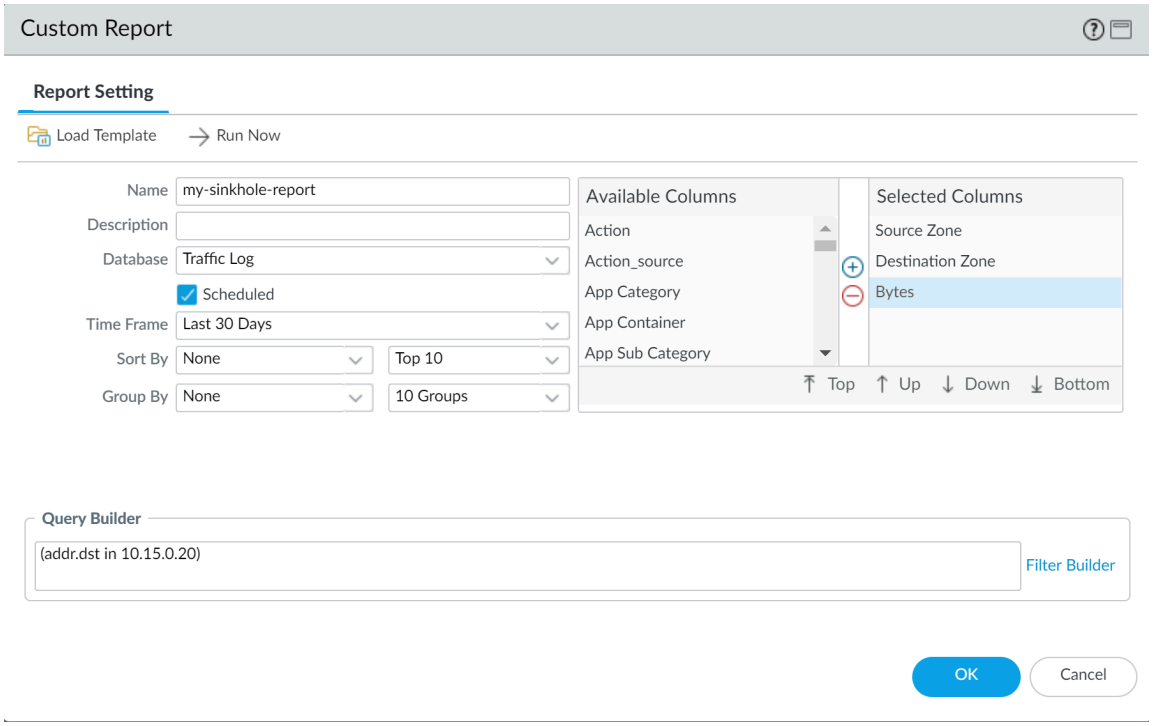
在本例中，受感染的客户端主机对列于 Palo Alto Networks DNS 签名数据库中的已知恶意域执行了 NSLOOKUP。发生此事件时，系统会将查询发送到本地 DNS 服务器，该服务器随后通过防火墙将请求转发到外部 DNS 服务器。具有所配置的防间谍软件配置文件的防火墙安全策略将查询与 DNS 签名数据库进行匹配，然后使用 Sinkhole 地址 10.15.0.20 和 fd97:3dec:4d27:e37c:5:5:5:5 伪造回复。客户端尝试启动会话，而流量日志则会记录活动的源主机和目标地址，这将重定向到伪造的 Sinkhole 地址。

查看防火墙上的流量日志可让您识别将流量发送到 Sinkhole 地址的任何客户端主机。在本例中，日志显示发送恶意 DNS 查询的源地址为 192.168.2.10。该主机随后将被找到并进行清理。如果没有 DNS Sinkhole 选项，管理员可能只会将本地 DNS 服务器看做执行查询的系统，并且不会发现受感染的客户端主机。如果您尝试使用操作“Sinkhole”对威胁日志运行报告，该日志可能会显示本地 DNS 服务器而不是受感染的主机。

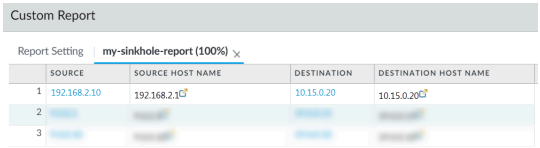
1. 选择 **Monitor**（监控） > **Manage Custom Reports**（管理自定义报告）。
2. 单击 **Add**（添加）并 **Name**（命名）报告。

3. 定义一个自定义报告，用于捕获 Sinkhole 地址的流量，如下：
   - **Database**（数据库）— 选择 **Traffic Log**（流量日志）。
   - **Scheduled**（已计划）— 启用 **Scheduled**（已计划），报告将每晚运行。
   - **Time Frame**（时间范围）— 30 天
   - **Selected Columns**（所选列）— 选择 **Source address**（源地址）或 **Source User**（源用户）（如果您已配置 User-ID），这将识别出报告中受感染的客户端主机；并且选择 **Destination address**（目标地址），这就是 Sinkhole 地址。
   - 在该屏幕底部的部分，为 Sinkhole 地址（本例中为 10.15.0.20）的流量创建一条自定义查询。您可以在 **Query Builder**（查询生成器）窗口中输入目标地址 **(addr.dst in 10.15.0.20)**，也可以在每列中选择以下地址并单击 **Add**（添加）：Connector = and,

Attribute = Destination Address, Operator = in, and Value = 10.15.0.20.单击 **Add**（添加）以添加查询。



4. 单击 **Run Now**（立即运行）以运行报告。该报告将显示所有将流量发送到 Sinkhole 地址的客户端主机，即表示这些主机很可能已经被感染。现在您可以跟踪这些主机并检查其中是否有恶意软件了。



5. 要查看已运行的已计划报告，请选择 **Monitor**（监控） > **Reports**（报告）。

自定义签名

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) • VM-SERIES • CN-Series	❑ 高级威胁防护（用于增强功能支持）或威胁防护许可证

您可以创建自定义威胁签名来检测和阻止特定流量。当防火墙由 Panorama 管理服务器管理时，ThreatID 将映射到防火墙上相应的自定义威胁，使防火墙生成已填充有自定义 ThreatID 的威胁日志。更多信息，请访问我们的自定义设备和威胁签名指南。

监控高级威胁防护

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	❑ 高级威胁防护（用于增强功能支持）或威胁防护许可证

Palo Alto Networks 提供了多个选项来监控高级威胁防护处理的活动，以适应依赖高级威胁防护和相关数据的一系列产品的情报检索。根据产品平台，您可以访问高级指示板，该指示板还提供 DNS 请求统计数据和使用趋势，包括网络活动上下文以及来自特定用户的 DNS 请求详细信息。

您还可以通过 Strata Cloud Manager 命令中心查看高级威胁防护如何与其他 Palo Alto Networks 应用程序和安全服务集成，以便保护您的组织安全，防止遭受威胁，以及如何从总体上了解您的部署的整体运行状况。该命令中心是 NetSec 主页，并通过具有多个数据方面的交互式可视化指示板来提供有关网络健康状况、安全性和效率的全面摘要，以便于一目了然地进行评估。

要从高层视角了解网络活动，您可以查看指示板，它可以显示网络的整体威胁管理数据以及各种 DNS 趋势。每个指示板卡都以图形报告格式提供威胁对您的网络影响的独特视图。这可以根据应用程序、用户以及哪些安全规则正在执行组织的政策，提供对受威胁影响最大的实体的概览式洞察。

Palo Alto Networks 提供了几种监控威胁活动的方法：

- Strata Cloud Manager 命令中心
- 查看威胁日志
- 查看高级威胁防护报告
- 监控阻止 IP 列表
- 进一步了解威胁签名
- 根据威胁类别创建自定义报告

查看威胁日志

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	❑ 高级威胁防护（用于增强功能支持）或威胁防护许可证

威胁类别将不同类型的威胁签名进行分类，以帮助您了解和划出事件威胁签名检测之间的连接。威胁类别是更广泛的威胁特征类型的子集：间谍软件、漏洞和防病毒。威胁日志条目显示每个已记录事件的 **Threat Category**（威胁类别）。

您可以浏览、搜索和查看检测到威胁时自动生成的高级威胁防护日志。通常，这包括威胁防护功能（包括内联机器学习）分析的任何合格威胁签名匹配，除非它专门配置了无日志严重性级别。日志条目提供了有关事件的大量详细信息，包括威胁级别以及（如果适用）威胁的性质。

- Strata Cloud Manager
- PAN-OS 和 Panorama

查看威胁日志 (Cloud Management)

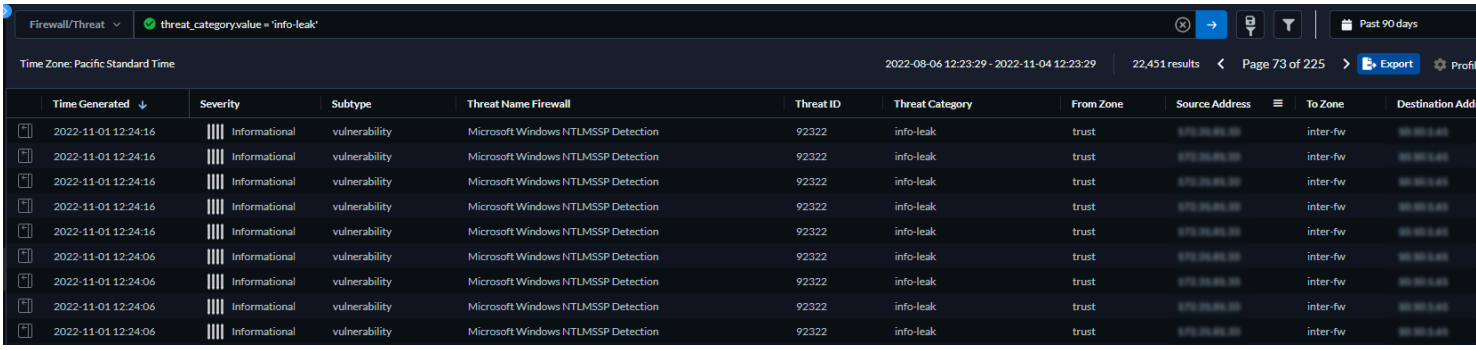
STEP 1 | 使用与 Palo Alto Networks 支持帐户关联的凭据，登录到中心的 Strata Cloud Manager。

有关使用活动指示板的更多信息，请参阅日志查看器。

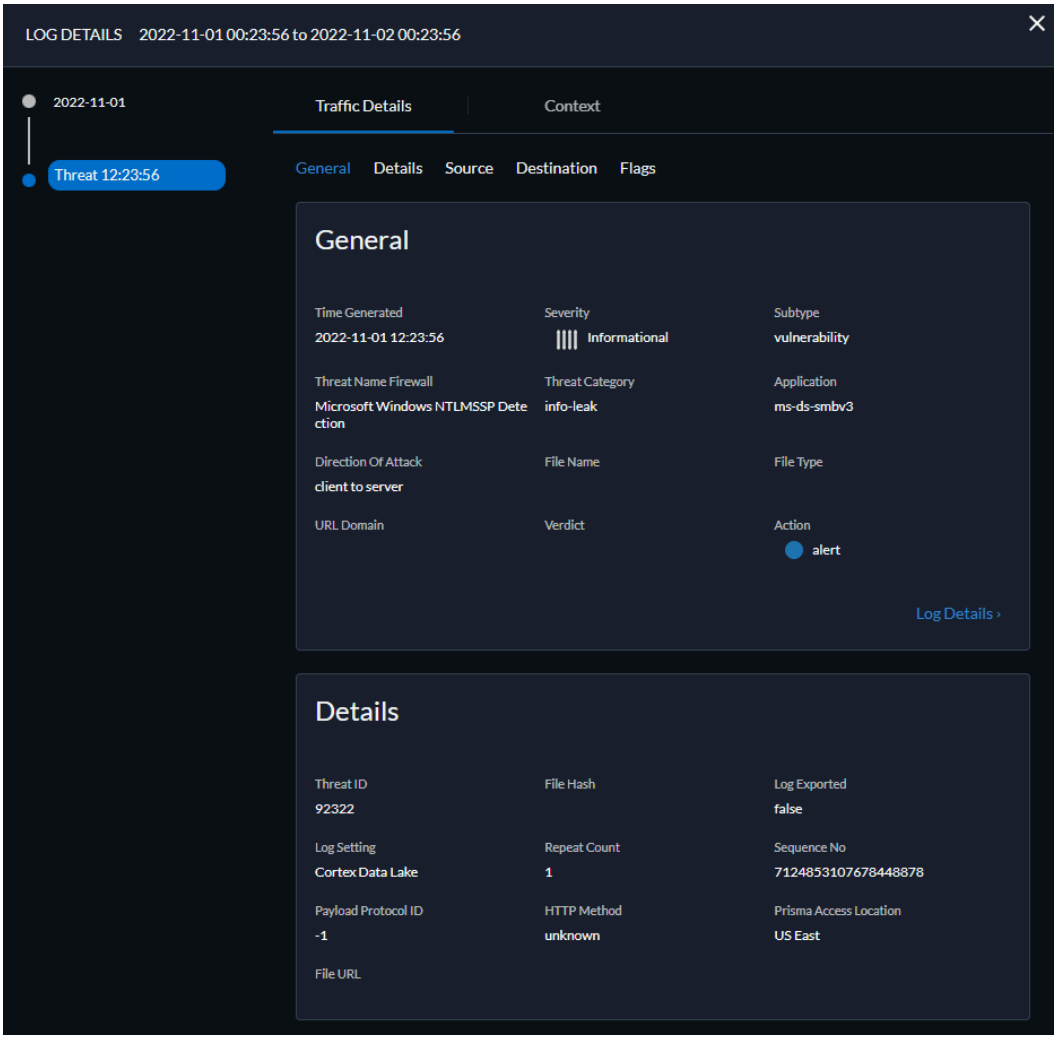
STEP 2 | 根据 Prisma Access 中的**Threat Category**（威胁类别）或 **Subtype**（子类型）过滤威胁日志。

1. 选择 **Incidents & 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. 利用防病毒、防间谍软件或漏洞防护配置文件（分别为 **Antivirus**（防病毒）、**Spyware**（间谍软件）和 **Vulnerability**（漏洞））使用的威胁特征码子类型之一或使用查询生成器基于威胁类别来创建搜索过滤器。例如，您可以使用 `sub_type.value = 'spyware'` 查看已确定为间谍软件的威胁的日志。要搜索其他子类型，请将上例中的间谍软件替换为其他支持的子类型（**Vulnerability**（漏洞）或 **Spyware**（间谍软件））。您还可以使用以下查询 `threat_category.value = 'info-leak'` 基于特定 **Threat Category**（威胁类别）进行搜索，例如信息泄露漏洞。有关可使用的有效类别的列表，

请参阅威胁签名类别。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。



4. 完成过滤器设置后运行查询。
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 **Category**（类别）显示在详细日志视图的 **Details**（详细信息）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。

STEP 3 | 按使用内联云分析（间谍软件）检测到的威胁 [类别] 筛选威胁日志。

基于 *HTTP* 的 *C2* 流量刚开始使用威胁名称 *Inline Cloud Analyzed HTTP* 命令和控制流量检测进行分类，它与多个威胁 *ID* 相关联，并且现在分为三个唯一的威胁名称以对应唯一的威胁 *ID*，从而更准确地描述高级威胁防护所做的检测：***Evasive HTTP C2 Traffic Detection***（规避性 ***HTTP C2*** 流量检测）（威胁 *ID*：*89950*）、***Evasive Cobalt Strike C2 Traffic Detection***（***Evasive Cobalt Strike C2*** 流量检测）（威胁 *ID*：*89955*、*89956* 和 *89957*）和 ***Evasive Empire C2 Traffic Detection***（***Evasive Empire C2*** 流量检测）（威胁 *ID*：*89958*）。

2023 年 *12* 月 *11* 日之前生成的基于 *HTTP* 的 *C2* 流量日志将继续以威胁名称内联云分析 *HTTP* 命令和控制流量检测进行分类。

1. 选择 **Incidents & 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. 使用内联云分析（间谍软件）专用的威胁类别创建搜索过滤器：`threat_category.value = 'inline-cloud-c2'`。您可以通过交叉引用与特定 C2 类型对应的威胁 ID 值来进一步限制搜索。例如，`threat_category.value = 'inline-cloud-c2' AND Threat ID = 89958`，其中 89958 表示规避 Empire C2 流量的威胁 ID。
4. 选择日志条目以查看检测到的 C2 威胁的详细信息。
5. 威胁 **Category**（类别）显示在日志详细信息的 **General**（常规）窗格中。使用内联云分析检测到的 C2 威胁的类别为 inline-cloud-c2。您可以交叉引用 **Details**（详细信息）窗格中的威胁 **ID** 值，以确定检测到的特定 C2 类型。

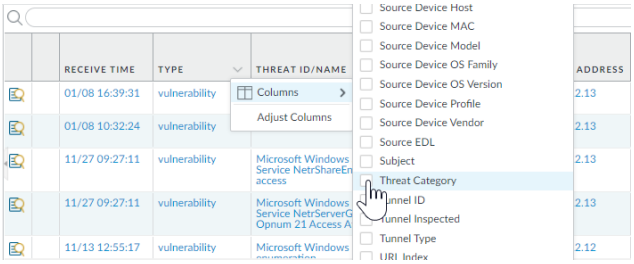
STEP 4 | 按使用内联云分析（漏洞）检测到的威胁 [类别] 过滤威胁日志。

1. 选择 **Incidents & 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. 使用内联云分析（漏洞）专用的威胁类别创建搜索过滤器：`threat_category.value = 'inline-cloud-exploit'`。
4. 选择一个日志条目以查看检测到的命令注入和 SQL 注入漏洞的详细信息。内联漏洞（SQL 注入）威胁的 ID 为 99950，而内联漏洞（命令注入）威胁的 ID 为 99951。

查看威胁日志 (NGFW (Managed by PAN-OS or Panorama))

按威胁类别筛选威胁日志。

1. 选择 **Monitor**（监视器） > **Logs**（日志） > **Threat**（威胁）。
2. 添加威胁类别列，以查看每个日志条目的威胁类别：



3. 要根据威胁类别筛选：
   - 使用日志查询构建器添加具有 **Attribute**（属性）威胁类别的筛选器，并在 **Value**（值）字段中输入威胁类别。
   - 选择任何日志条目的威胁类别，并将该类别添加到筛选器：

按威胁签名类型筛选威胁日志。

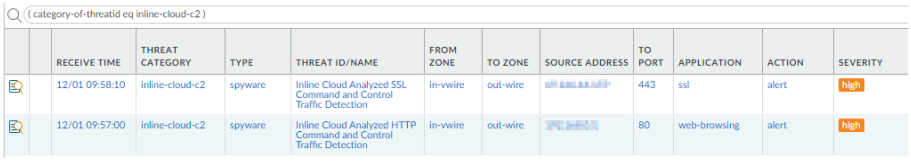
1. 选择 **Monitor**（监视器） > **Logs**（日志） > **Threat**（威胁）。
2. 添加 **Type**（类型）列（如果不存在），这样您就可以查看每个日志条目的威胁签名类别：
3. 要根据签名类型进行过滤，请执行以下操作：
   - 使用日志查询构建器添加具有威胁类别的 **Attribute**（属性）的筛选器，并在 **Value**（值）字段中输入威胁签名类别。您可以选择 **Vulnerability**（漏洞）、**Virus**（病毒）和 **Spyware**（间谍软件），这些漏洞、病毒和间谍软件分别与漏洞防护、防病毒和防间谍软件安全配置文件处理的签名对应。
   - 选择任何日志条目的 **Type**（类型），将该威胁签名类型添加到过滤器中。您也可以使用过滤器和威胁签名类型手动构建查询。

按使用内联云分析（间谍软件）检测到的威胁 [类别] 筛选威胁日志。

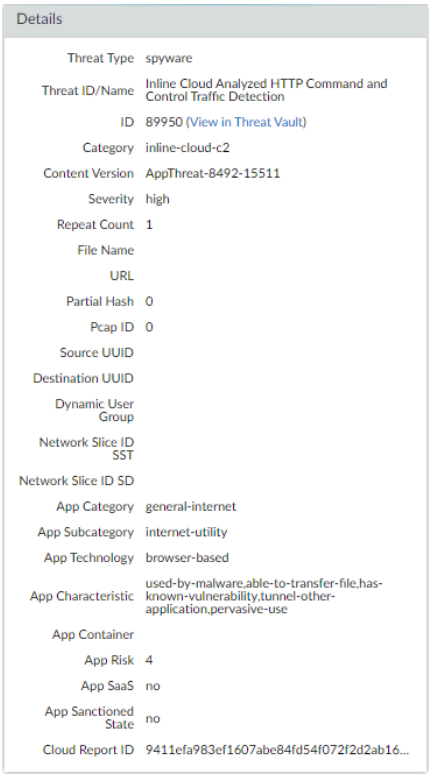
基于 *HTTP* 的 *C2* 流量刚开始使用威胁名称 *Inline Cloud Analyzed HTTP* 命令和控制流量检测进行分类，它与多个威胁 *ID* 相关联，并且现在分为三个唯一的威胁名称以对应唯一的威胁 *ID*，从而更准确地描述高级威胁防护所做的检测：***Evasive HTTP C2 Traffic Detection***（规避性 ***HTTP C2*** 流量检测）（威胁 *ID*：*89950*）、***Evasive Cobalt Strike C2 Traffic Detection***（***Evasive Cobalt Strike C2*** 流量检测）（威胁 *ID*：*89955*、*89956* 和 *89957*）和 ***Evasive Empire C2 Traffic Detection***（***Evasive Empire C2*** 流量检测）（威胁 *ID*：*89958*）。

如果您未安装更新内容或正在查看 *2023* 年 *12* 月 *11* 日（内容更新的发布日期）之前生成的基于 *HTTP* 的 *C2* 流量日志，则所有基于 *HTTP* 的 *C2* 流量将继续使用威胁名称 *Inline Cloud Analyzed HTTP* 命令和控制流量检测进行分类。

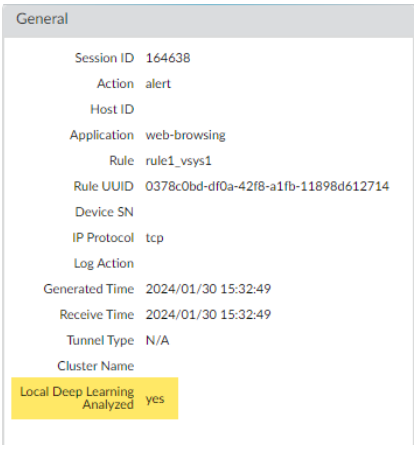
1. 选择 **Monitor**（监控） > **Logs**（日志） > **Threat**（威胁）。您可以根据威胁的某些特征筛选日志。考虑以下示例：
   - 使用 `( category-of-threatid eq inline-cloud-c2 )` 筛选以查看已使用高级威胁防护的内联云分析机制分析的 C2 威胁的日志。
   - 您可以通过交叉引用与特定 C2 类型对应的威胁 ID 值来进一步限制搜索。例如，`( category-of-threatid eq inline-cloud-c2 ) and (name-of-threatid eq 89958)`，其中 89958 表示规避 Empire C2 流量的威胁 ID。
   - 使用 `(local_deep_learning eq yes)` 进行过滤，查看已使用高级威胁防护的本地深度分析机制分析的威胁日志。



2. 选择日志条目以查看检测到的 C2 威胁的详细信息。
3. 威胁 **Category**（类别）显示在详细日志视图的 **Details**（详细信息）窗格中。使用内联云分析检测到的 C2 威胁的类别为 inline-cloud-c2。您可以交叉引用威胁 **ID** 值来确定已检测到的 C2 的特定类型。



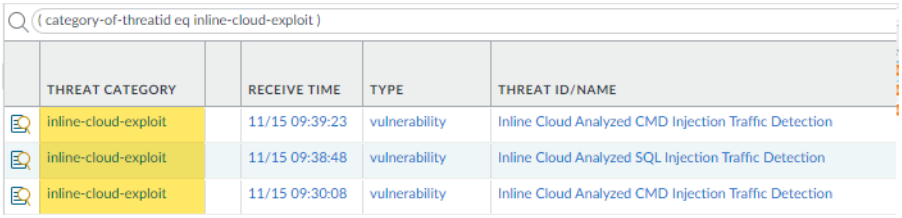
4. 如果使用本地深度学习分析威胁，则本地深度学习分析字段显示“是”。



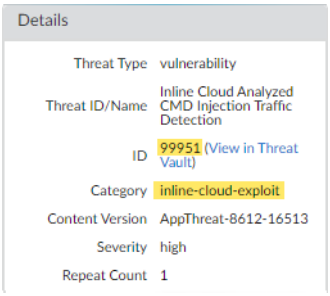
监控防火墙上的活动，以发现使用在线云分析（漏洞）检测到的漏洞利用。

1. 选择 **Monitor**（监控） > **Logs**（日志） > **Threat**（威胁）并按 `(category-of-threatid eq inline-cloud-exploit)` 进行筛选，以查看已使用高级威胁防护的

内联云分析机制分析的日志。内联漏洞（SQL 注入）威胁的 ID 为 99950，而内联漏洞（命令注入）威胁的 ID 为 99951。

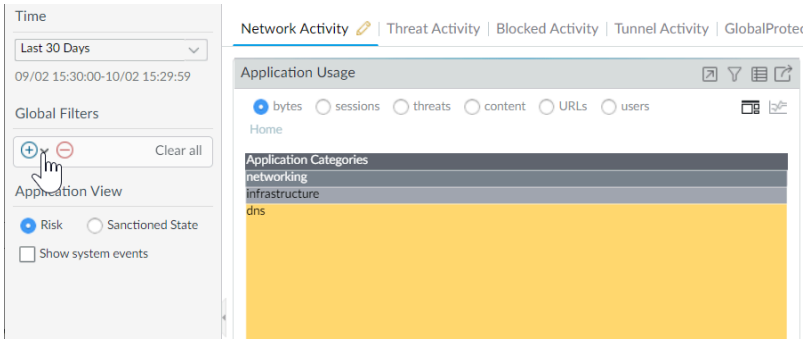


2. 选择日志条目以查看漏洞利用的详细信息。
3. 威胁 **Category**（类别）显示在详细日志视图的 **Details**（详细信息）窗格中。使用内联云分析检测到的漏洞利用的威胁类别为 inline-cloud-exploit。

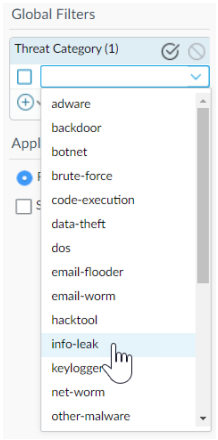


按威胁类别筛选 ACC 活动。

1. 选择 **ACC** 并添加威胁类别作为全局筛选器：



2. 选择威胁类别以筛选所有 ACC 选项卡。



查看高级威胁防护报告

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	❑ 高级威胁防护（用于增强功能支持）或威胁防护许可证

通过 Threat Vault API 可获取高级威胁防护报告，其中提供了详细的分析和检测信息，以及有关事务、会话和其他相关过程的信息。该报告包含下表中描述的部分或全部信息，这些信息基于在防火墙上配置的用于处理该文件的会话信息，以及 JSON 格式的文件的分析详细信息。

NGFW 无法通过 *PAN-OS* 直接访问报告；相反，您必须引用与威胁日志关联的 *cloud_reportid*，并使用 *Threat Vault API* 来搜索和检索报告。

对于*Prisma Access*（通过 Strata Cloud Manager），可以从日志查看器 (查看威胁日志) 查看报告。在 ***Cloud ReportID***（云报告 ***ID***）列下的报告 *ID* 值旁，生成的高级威胁防护报告的日志条目有一个下载链接。

报告标题	说明
常规信息	包含有关处理威胁的防火墙/安全平台的信息。 • 包含高级威胁报告数据的云报告 ID 号。 • 在创建报告期间可能生成的错误消息。
PAN-OS 信息	包含有关处理威胁的防火墙/安全平台的信息。 • 防火墙接口 (IPv4/IPv6) • 内容包版本 • 防火墙主机名 • 防火墙型号 • 序列号 • PAN-OS 版本
会话信息	包含基于通过转发威胁的防火墙/安全平台传输的流量的会话信息。

报告标题	说明
	提供了以下选项： • 源 IP • 源端口 • 目标 Ip • 目标端口 • 会话 ID • 会话时间戳 • 有效负载类型
事务数据	事务数据概述有效负载的详细信息，并包含检测服务报告。 提供了以下选项： • 事务 ID • 有效负载的 SHA256 哈希值
检测服务结果	当威胁分析由高级威胁防护云执行时，本部分包含显示分析结果的条目。这包括检测服务报告，该报告还提供所采用的 MITRE ATT&CK® 机密技术以及有效负载的详细信息。 Empire C2 框架的命令和控制检测显示了额外的上下文信息。这包括在不同会话中发生的攻击的分阶段和命令（攻击后）阶段生成的报告。 以下信息条目可用： • 攻击描述 — 描述 C2 攻击的性质。 • 攻击详情 — 指示 Empire C2 攻击的阶段，并描述服务器和客户端之间的交流。 • 攻击证据 — 列出与已知 Empire C2 一致的行为和操作。 基于 *Empire* 的 *C2* 使用一个子模块检测器进行检测，该检测器包含在 ***Inline Cloud Analyzed HTTP*** 命令和控制流量检测分析引擎中，其唯一威胁 *ID* 为 *89958*。

监控阻止 IP 列表

在何处可以使用？	需要提供什么？
• NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ 高级威胁防护（用于增强功能支持）或威胁防护许可证

防火墙维护其阻止的源 IP 地址阻止列表。当防火墙阻止源 IP 地址时，例如当您配置以下任一策略规则时，防火墙在这些数据包使用 CPU 或数据包缓冲区资源之前阻止硬件流量：

- 分类的 DoS 保护策略规则，具有 **Protect**（保护）操作（分类的 DoS 保护策略指定传入连接匹配源 IP 地址、目标 IP 地址或源和目标 IP 地址对，并与分类的 DoS 保护配置文件相关联，如针对新会话的泛滥攻击配置 DoS 保护中所述）。
- 使用漏洞防护配置文件的安全策略规则

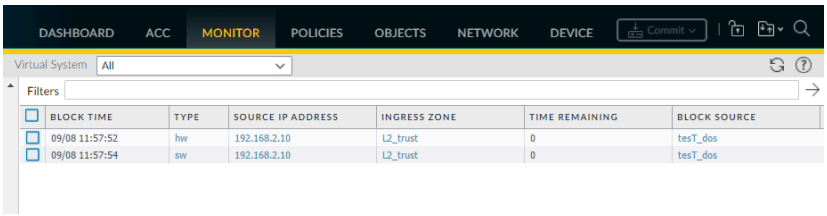
PA-3200 系列、PA-5200 系列、PA-5400 系列（PA-5450 除外）和 PA-7000 系列防火墙支持阻止硬件 IP 地址。

您可以查看阻止列表，获取有关阻止列表中 IP 地址的详细信息，或查看硬件和软件正在阻止的地址数。如果认为不应该阻止，可以从列表中删除 IP 地址。您可以更改列表中地址详细信息的来源。您还可以更改硬件阻止 IP 地址的时长。

查看阻止列表条目。

1. 选择 **Monitor**（监控） > **Block IP List**（阻止 **IP** 列表）。

   在类型列表中指示硬件 (hw) 或软件 (sw) 是否阻止阻止列表中的条目。
2. 在屏幕底部查看：
   - 防火墙支持的阻止 IP 地址数量中的 **Total Blocked IPs**（总阻止 **IP**）计数。
   - 防火墙使用的阻止列表百分比。
3. 要筛选显示的条目，请在列中选择一个值（在 **Filters**（筛选器）字段中创建一个筛选器），并应用筛选器 (→)。否则，防火墙将显示前 1,000 个条目。
4. 输入 **Page**（页面）编号，或单击屏幕底部的箭头，以向前滚动条目页。
5. 要查看阻止列表上地址的详细信息，请将鼠标悬停在源 IP 地址上，然后单击向下箭头链接。点击 **Whois** 链接，显示有关地址的网络解决方案 Whois 信息。



删除阻止列表条目。

如果确定不应该阻止 *IP* 地址，则删除该条目。然后，应修改导致防火墙阻止地址的策略规则。

1. 选择 **Monitor**（监控） > **Block IP List**（阻止 **IP** 列表）。
2. 选择一个或多个条目，然后单击 **Delete**（删除）。
3. （可选）选择 **Clear All**（清除所有）以从列表中删除所有条目。

禁用或重新启用硬件 IP 地址阻止以进行排除故障。

禁用硬件 *IP* 地址阻止，防火墙仍执行您配置的任何软件 *IP* 地址阻止。

```
> set system setting hardware-acl-blocking [enable | disable]
```

为节省 *CPU* 和数据包缓冲区资源，并将硬件 *IP* 地址阻止保持启用的状态，除非 *Palo Alto Networks* 的技术支持要求您禁用，例如，正在调试流量时。

调整硬件阻止的 IP 地址保留在阻止列表中的秒数（范围为1-3,600；默认为 1）。

```
> set system setting hardware-acl-blocking duration <seconds>
```

硬件阻止列表条目的保留时间短于软件阻止列表条目，以减少超出硬件阻止能力的事件发生。

更改默认网站，从网络解决方案 Who Is 到不同的网站查找更多有关 IP 地址的消息。

```
# set deviceconfig system ip-address-lookup-url <url>
```

查看硬件和软件阻止的源 IP 地址数量，例如查看攻击速率。

查看硬件阻止表和阻止列表上的 IP 地址条目总和（被硬件和软件阻止）：

```
> show counter global name flow_dos_blk_num_entries
```

查看硬件阻止表上被硬件阻止的 IP 地址条目数：

```
> show counter global name flow_dos_blk_hw_entries
```

查看阻止列表上被软件阻止的 IP 地址条目数：

```
> show counter global name flow_dos_blk_sw_entries
```

查看 PA-7000 系列防火墙上每个插槽的阻止列表信息。

```
> show dos-block-table software filter slot <slot-number>
```

进一步了解威胁签名

在何处可以使用？	需要提供什么？
• NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ 高级威胁防护（用于增强功能支持）或威胁防护许可证

防火墙威胁日志记录根据威胁签名 (设置防病毒威胁、防间谍软件和漏洞防护) 检测到的所有威胁来记录所有威胁，ACC 会显示网络上主要威胁的概览。防火墙记录的每个事件都包括标识相关威胁签名的 ID。

您可以使用威胁日志或 ACC 条目找到威胁 ID，以便：

- 轻松检查威胁签名是否已配置为安全策略的例外 (创建威胁异常)。
- 查找有关特定威胁的最新威胁库信息。因为威胁库与防火墙集成，可让您在防火墙的上下文中直接查看有关威胁签名的详细信息，或者在新的浏览器窗口中为防火墙记录的威胁启动威胁库搜索。

如果签名已禁用，则签名 *UTID* 可能会重新用于新签名。

查看内容更新发行说明，了解新签名和禁用签名相关的通知。签名在以下情况下可能被禁用：签名检测到的活动由于攻击者的攻击而停用，签名产生了重大的误报，或是签名与其他类似签名合并为单个签名（签名优化）。

STEP 1 | 确认防火墙已连接到威胁库。

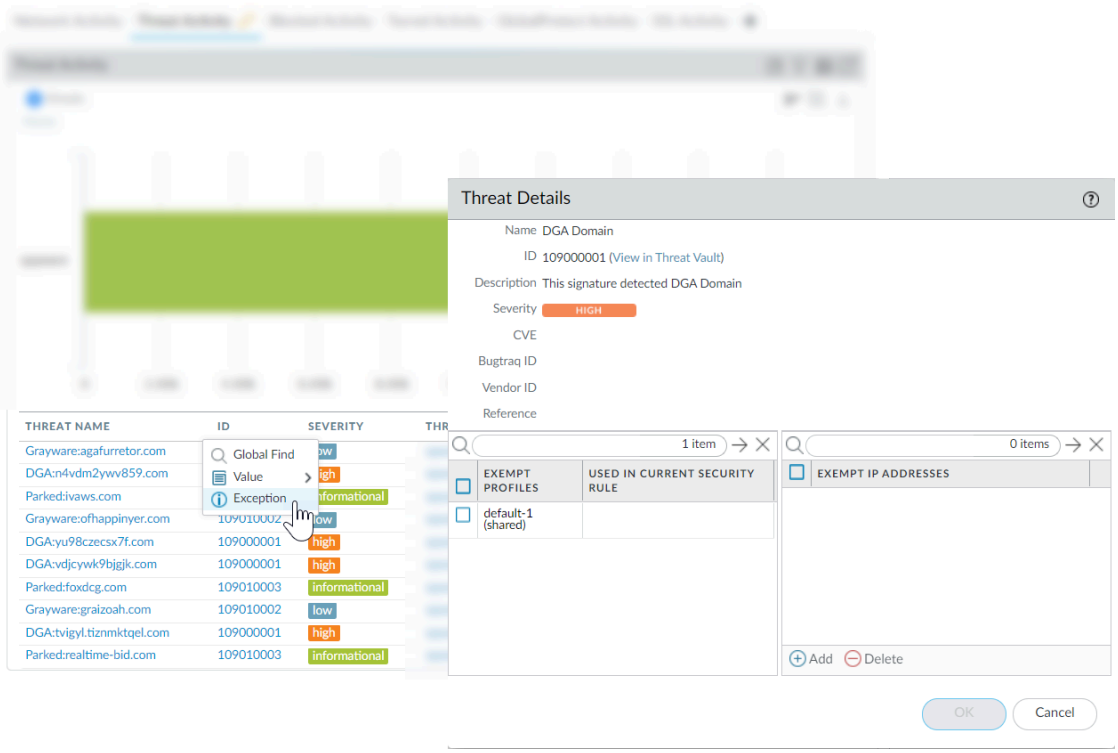
选择 **Device**（设备） > **Setup**（设置） > **Management**（管理）并编辑 **Logging and Reporting**（日志记录和报告）设置为 **Enable Threat Vault Access**（启用威胁库访问）。默认情况下启用威胁库访问。

STEP 2 | 查找防火墙检测到的威胁的威胁 ID。

- 要查看防火墙根据威胁签名检测到的每个威胁事件，请选择 **Monitor**（监控） > **Logs**（日志） > **Threat**（威胁）。可以在 ID 列中找到威胁条目的 ID，或选择日志条目以查看日志详细信息，包括威胁 ID。
- 要查看网络上最高威胁的概述，请选择 **ACC** > **Threat Activity**（威胁活动），并查看“威胁活动”小部件。ID 列显示每个已显示威胁的威胁 ID。
- 要查看可将其配置为威胁例外的威胁的详细信息（即，防火墙执行的威胁与为威胁签名定义的默认操作不同），请选择 **Objects**（对象） > **Security Profiles**（安全配置文件） > **Anti-Spyware/Vulnerability Protection**（防间谍软件/漏洞防护）。**Add**（添加）或修改配置文件，然后单击 **Exceptions**（异常）选项卡来查看已配置的异常。如果没有配置异常，可筛选威胁签名，或选择 **Show all signatures**（显示所有签名）。

STEP 3 | 悬停在 **Threat Name**（威胁名称）或威胁 **ID** 上打开下拉列表，然后单击 **Exception**（异常）查看威胁详细信息以及如何配置防火墙以执行威胁。

例如，进一步了解有关 ACC 的最高威胁：



STEP 4 | 查看威胁的最新 **Threat Details**（威胁详细信息），并根据威胁 ID 启动威胁库搜索。

- 显示的威胁详细信息包括威胁的最新威胁库信息、可用于进一步了解威胁的资源以及与威胁相关联的 CVE。
- 选择 **View in Threat Vault**（在威胁库中查看）以在新窗口中打开威胁库搜索，并查找 Palo Alto Networks 威胁数据库具有的针对该威胁签名的最新信息。

STEP 5 | 检查是否已将威胁签名配置为安全策略的异常。

- 如果 **Used in current security rule**（在当前安全规则中使用）列已清除，防火墙将根据建议的默认签名操作（例如，阻止或警报）实施该威胁。
- 在 **Used in current security rule**（在当前安全规则中使用）列中任何位置使用的复选标记均表示安全策略规则已配置为基于相关联的 **Exempt Profiles**（免除配置文件）设置对威胁执行非默认操作（例如，允许）。

仅当安全策略规则已配置威胁异常时 ***Used in security rule column***（在当前安全规则中使用）才不会指示安全策略规则是否已启用。选择 ***Policies***（策略） > ***Security***（安全），以检查是否启用指定的安全策略规则。

STEP 6 | **Add**（添加）IP 地址，在其上筛选威胁异常或查看现有 **Exempt IP Addresses**（免除 **IP** 地址）。

仅有当关联的会话具有匹配的源 IP 地址或目标 IP 地址时，才配置免除 IP 地址来执行威胁异常；对于所有其他会话，将基于默认签名操作来执行威胁。

根据威胁类别创建自定义报告

在何处可以使用？	需要提供什么？
• NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ 高级威胁防护（用于增强功能支持）或威胁防护许可证

您可以在防火墙上创 自定义报告，以根据您想要检索和分析的属性或关键信息生成（按需）或安排（每晚）报告。

根据威胁类别创建自定义报告，以接收防火墙检测到的特定威胁类型相关的信息。

1. 选择 **Monitor**（监控） > **Manage Custom**（管理自定义）报告以添加新的自定义报告或修改现有报告。
2. 选择 **Database**（数据库）作为自定义报告的来源；在这种情况下，从两种类型的数据库源（摘要数据库和详细日志）中选择 **Threat**（威胁）。精简摘要数据库数据，以便在生成报告时获取更快的响应时间。详细日志需要更长的生成时间，但为每个日志条目提供一个逐项和完整的数据集。
3. 在查询构建器中，添加带有属性 **Threat Category**（威胁类别）的报告筛选器，然后在“值”字段中，根据您的报告选择一个威胁类别。
4. 要测试新报告设置，请选择 **Run Now**（立即运行）。
5. 单击 **OK**（确定）以保存报告。