paloalto TECHDOCS

Advanced DNS Security 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

November 23, 2022

Table of Contents

关于 DNS Security 订阅服务

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	❑ Advanced DNS Security 许可证（用于增强功能支持）或 DNS Security 许可证 ❑ 高级威胁防护或威胁防护许可证

Palo Alto Networks® 通过两个安全订阅选项提供针对基于 DNS 的威胁的专门集成保护：DNS Security 和 Advanced DNS Security。这些 云交付的安全订阅 使用与 Palo Alto Networks 的共享基础进行操作 威胁防护解决方案 提供全面的 DNS Security 解决方案，因此需要 Advanced Threat Prevention 或 Threat Prevention 订阅。

DNS Security 云服务旨在保护您的组织安全，防止遭到多种基于 DNS 的高级威胁入侵。DNS Security 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 Security 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。

通过在受支持的网络安全平台上运行的主动威胁防护解决方案，客户可以使用 Palo Alto Networks 生成的域列表对 DNS 请求执行 Sinkhole。这些本地访问的自定义 DNS 签名列表与 防病毒程序以及 WildFire 更新一同打包，并涵盖了在发布时与策略实施和保护关联性最高的威胁。为通过 DNS 获得对威胁的更全面涵盖，DNS Security 订阅让用户可以通过高级预测分析，访问实时保护。通过诸如 DGA/DNS 隧道检车和机器学习之类的技术，DNS 流量中隐藏的威胁可被主动识别，并通过无限扩展的云服务进行共享。由于 DNS 签名和保护储存在基于云的架构中，您可以访问不断扩展的完整签名数据库，这些签名是通过众多数据源而生产的。这允许您通过 DNS 实时防御各种威胁，以及新生成的恶意域。要对抗以后的威胁，可通过新内容的发布，实现对 DNS Security 服务分析、检测和预防能力的更新。

要访问基本 *DNS Security* 服务，除了运行网络安全平台所需的任何基本许可证外，您还必须拥有有效的 *Advanced Threat Prevention* 或 *Threat Prevention* 许可证以及 *Advanced DNS Security* 或 *DNS Security* 许可证。

以下 Palo Alto Networks 网络安全平台上提供 DNS Security 订阅：

- 新一代防火墙，包括 VM-Series 和 CN-Series
- Prisma Access

Advanced DNS Security 服务是一项补充订阅产品，与 DNS Security 订阅一起运行，允许访问 Advanced DNS Security 云中的新域检测器，这些检测器检查 DNS 响应的变化，以实时检测各种类型的 DNS 劫持。通过访问在 PAN-OS 11.2 及更高版本上运行的 Advanced DNS Security，您可以检测和阻止来自被劫持域和错误配置域的 DNS 响应。通过直接操纵 DNS 响应或利用组织的 DNS 基础设施的配置设置，可以将被劫持和配置错误的域引入您的网络，以便将用户重定向到恶意域，从而发起其他攻击。这两种技术之间的主要区别在于漏洞利用发生的位置。在 DNS 劫持的情况下，攻击者通过破坏组织 DNS 基础设施的某些方面（无论是 DNS 提供商的管理访问权限、DNS 解析过程中的 MiTM 攻击还是 DNS 服务器本身），从而获得将 DNS 查询解析到攻击者操作的域的能力。配置错误的域也存在类似的问题 - 攻击者试图通过利用域配置问题、过时的 DNS 记录，从而获得客户子域的所有权，并将自己的恶意域合并到组织的 DNS 中。

Advanced DNS Security 可以通过运行基于云的检测引擎实时检测和分类被劫持和配置错误的域，这些引擎通过使用基于 ML 的分析来分析 DNS 响应，从而检测恶意活动并提供 DNS 运行状况支持。由于这些检测器位于云中，因此，您可以访问各种自动更新和部署的检测机制，而无需用户在更改检测器时下载更新包。在初始发布时，Advanced DNS Security 支持两个分析引擎：DNS 错误配置域和劫持域。此外，所有 DNS 查询的 DNS 响应都会发送到 Advanced DNS Security 云，以增强响应分析，从而更准确地分类并在实时交换中返回结果。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。通过 Anti-Spyware（或 DNS Security）配置文件启用并配置 Advanced DNS Security，并且需要有效的 Advanced DNS Security 和 Advanced Threat Prevention（或 Threat Prevention）许可证。

要访问 *Advanced DNS Security* 服务，除了运行网络安全平台所需的任何基本许可证外，您还必须拥有有效的 *Advanced Threat Prevention* 或 *Threat Prevention* 许可证以及 *Advanced DNS Security* 许可证。

以下 Palo Alto Networks 网络安全平台上提供 Advanced DNS Security 订阅：

- 新一代防火墙，包括 VM-Series 和 CN-Series

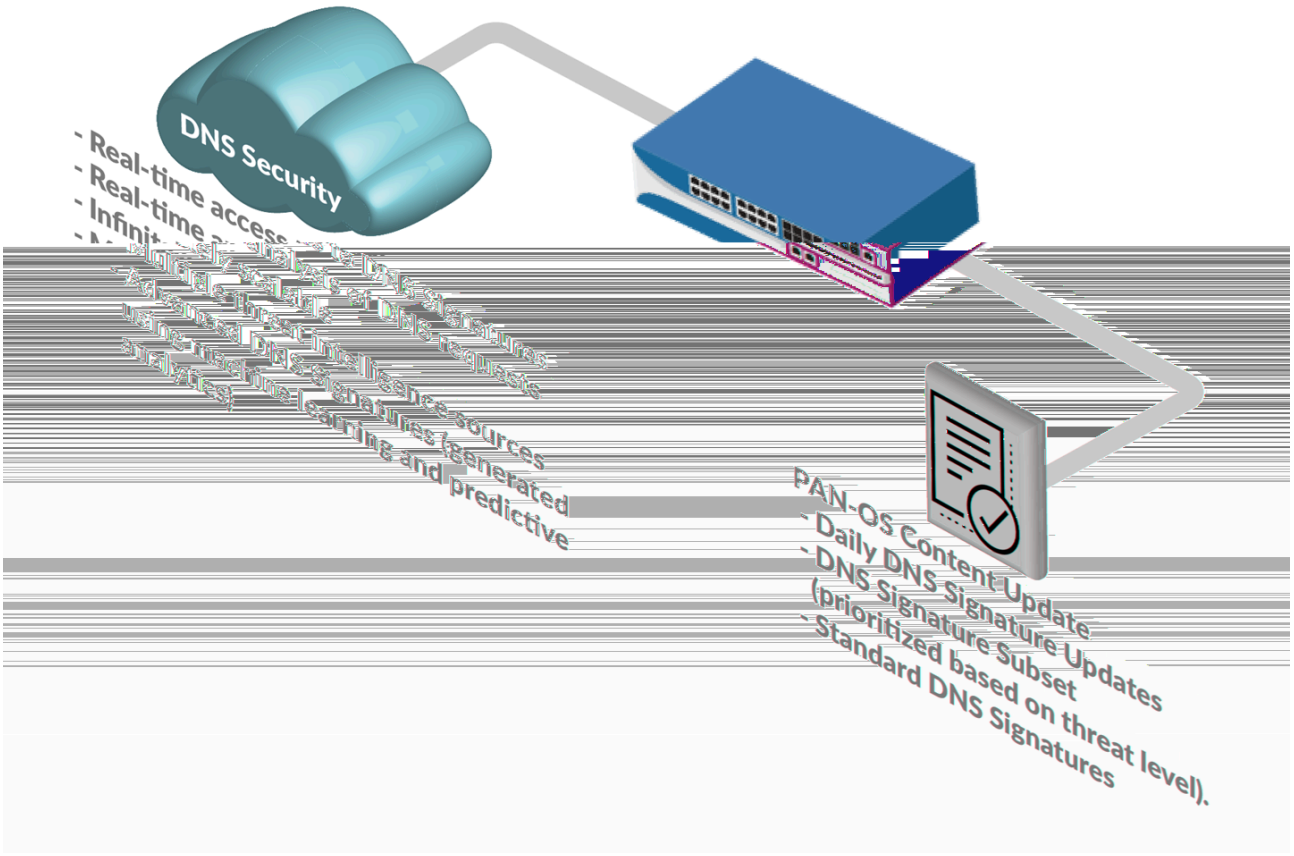
了解如何在网络中部署和监控 DNS Security 以及 Advanced DNS Security：

- 配置 DNS Security 订阅服务
- 监控 DNS Security 订阅服务

云 DNS 签名和保护

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	❑ Advanced DNS Security 许可证（用于增强功能支持）或 DNS Security 许可证 ❑ 高级威胁防护或威胁防护许可证

作为基于云的服务，DNS Security 允许您访问可无限扩展的 DNS 签名和保护源，以免让您的公司受到恶意域的攻击。Palo Alto Networks 生成的域签名和保护从多个源衍生而来，包括 WildFire 流量分析、被动 DNS、主动 Web 抓取和恶意 Web 内容分析、URL 沙箱分析、蜜网、DGA 反向工程、遥测数据、whois、Unit 42 研究组织和第三方数据源，如 网络威胁联盟。此按需云数据库为用户提供了对完整 Palo Alto Network 的 DNS 签名集的访问，包括使用高级分析技术生成的签名，以及实时的 DNS 请求分析。本地可用的可下载 DNS 签名集（与防病毒程序以及 WildFire 更新打包）配有 100k 签名的硬编码容量限制，且不包含通过高级分析生成的签名。为了更好的接收日常生成的新 DNS 签名流入，基于云的签名数据库为用户提供了对新添加 DNS 签名的即时访问，而无需下载更新。如果网络连接出现故障或不可用，防火墙使用指定的 DNS 签名集。



DNS Security 服务通过对多个 DNS 数据源使用预测分析和机器学习来执行实时 DNS 请求分析。该服务用于针对基于 DNS 的威胁提供防护，可通过配置附加到安全策略规则的防间谍软件安全配置文件来实时访问。每个 DNS 威胁类别（DNS 签名源）都允许您定义单独的策略操作，记录特定签名类型的严重性级别。这样，您就可以按照网络安全协议，根据威胁性质创建特定的安全策略。Palo Alto Networks 还会根据 PAN-DB 和 Alexa 指标生成并保留明确允许的域列表。可以经常访问这些允许域列表，且该列表已知没有恶意内容。DNS Security 类别和允许列表可通过 PAN-OS 内容版本进行更新和扩展。

PAN-OS 9.1 及更低版本的 *DNS Security* 源类别范围有限。

DNS Security 和 Advanced DNS Security 当前支持检测以下 DNS 威胁类别：

通用威胁 *ID* 编号（在威胁日志中表示为 *ID*）映射到 *DNS Security* 用于对域进行分类的特定 *DNS* 检测机制。这显示了域的精确分类，以及域所属的广义威胁类别。

- **Command and Control Domains**（命令和控制域）— C2 包括恶意软件和/或受影响系统用于暗中与攻击者远程服务器进行通信的 URL 和域，以接收恶意命令或泄漏数据（这包括 DNS 隧道检测和 DGA 检测）、或耗尽目标权威 DNS 服务器（如 NXNSattack）资源。
  - **DNS** 隧道检测（UTID：109001001/109001002）— DNS 隧道可被攻击者用于在 DNS 查询和响应中，对非 DNS 程序和协议的数据进行编码。其为攻击者提供了开放的反向隧道，攻击者可通过该隧道传输文件或远程访问系统。DNS 隧道检测使用机器学习以分析 DNS 查询的行为质量，包括域、熵、查询率和模式的 n-gram 频率分析，以确定查询是否与基于隧道的 DNS 攻击一致。这包括某些下一代 DNS 隧道恶意软件，它们会跨多个域缓慢地渗漏数据以避免检测，如 TriFive 和 Snugy。通过与防火墙的自动化策略操作结合，其允许您快速检测隐藏在 DNS 隧道内的 C2 或数据窃取，并根据您定义的策略规则自动阻挡。

    确定拥有 DNS 隧道功能的域名将得到进一步分析，以提供有关 DNS Security 用于将数据嵌入 DNS 查询和响应的工具以及相关恶意软件活动名称的详细信息。在 Prisma Access 上，威胁日志中为防火墙和 DNS Security 日志提供了威胁 ID/名称属性的详细信息，并且防火墙使用以下格式将其作为威胁名称：Tunneling:<*optional_list_of_tools/campaigns*; 点分隔字符串)>:<*domain_name*> 或 Tunneling_infil:<*optional_list_of_tools/campaigns*; 点分隔字符串)>:<*domain_name*>，具体取决于特定 DNS 隧道域类型。
  - **DGA** 域检测（UTID：109000001）— 域生成算法 (DGA) 用于自动生成域，特别是在建立恶意命令和控制 (C2) 通讯隧道时会生成大量域。基于 DGA 的恶意软件（如 Pushdo、BankPatch 和 CryptoLocker）会通过在大量的可疑内容中隐藏其主动 C2 服务器位置来限制被阻止的域数量，而且可基于多种因素（如时间、加密密钥、目录衍生的命名方案或其他唯一值）通过算法生成。DGA 生成的大部分域并不会解析为有效域，其必须全部被识别，以提供对给定威胁的全面抵御。DGA 分析可确定域是否由机器生成而非人工生成，其方法是通过反向工程和分析在 DGA 中发现的其他频繁使用的技术。而后，Palo Alto Networks 使用这些特征实时识别和阻挡之前未知的、基于 DGA 的威胁。
  - **NXNSAttack**（UTID：109010007）— DNS 协议中存在的 NXNSAttack 漏洞影响所有递归 DNS 解析器，恶意行为者可以利用它来发起类似 DDOS 的放大攻击，以破坏易受攻击的权威 DNS 服务器的正常运行。NXNSAttack 可以通过强制递归 DNS 解析器发出大量无效请求来关闭服务器，从而在权威 DNS 服务器上引入大量流量峰值。
  - **DNS** 重新绑定（UTID：109010009）— DNS 重新绑定攻击将用户引诱到攻击者控制的域，该域配置了一个短 TTL 参数，可操纵域名解析方式，从而利用和绕过浏览器中的同源策略。这样，恶意行为者能够使用客户端机器作为中介，攻击或访问私有网络中包含的资源。
  - **DNS** 渗透（UTID：109001003）— DNS 渗透包括 DNS 查询，后者使恶意行为者能够通过响应欺诈性 A (IPv4) 和 AAAA (IPv6) 记录请求来隐藏和解析微小负载。当客户端解析多个子域时，每个子域都包含一个带有编码组件的 A/AAAA 记录，其中包含的数据可能会被合并，形成恶意负载，之后该负载可以在客户端机器执行。执行负载后，它可以引入辅助负载来建立 DNS 隧道或其他漏洞。
  - **DNS** 流量分析（UTID：109010010）—（需要 Advanced DNS Security）DNS 流量分析是一个基于云的分析器，它根据对 DNS 流量模式的评估来检测试图建立 C2 连接的恶意软件。当 Advanced DNS Security 监控组织的 DNS 流量时，出站 DNS 请求序列会被矢量化，以便创建 DNS 流量配置文件，然后使用 ML 技术进行分析，该技术可以将唯一的 DNS 请求模式与可识别的恶意 C2 域配置文件相关联。

- 动态 **DNS** 托管域（UTID：109020002）— 动态 DNS (DDNS) 服务提供主机名和 IP 地址之间近乎实时的映射，从而在静态 IP 不可用时，使不断变化的 IP 地址保持与特定域的链接。这让攻击者有机会通过使用 DDNS 服务更改用于托管命令和控制服务器的 IP 地址，从而入侵网络。恶意软件活动和漏洞利用工具包将 DDNS 服务作为其有效载荷分发策略的组成部分加以利用。攻击者将 DDNS 域作为其主机名基础结构的组成部分加以利用，就能更改与特定 DNS 记录关联的 IP 地址，这样就能更容易避开检测。DNS Security 通过筛选和交叉引用来自各种源的 DNS 数据，生成随后可被进一步验证以提高准确性的待选列表，从而检测有漏洞的 DDNS 服务。
- 恶意软件域 — 恶意软件域用于托管和分发恶意软件，可能包括尝试安装各种威胁（如可执行文件、脚本、病毒、隐蔽强迫式下载）的网站。恶意软件域与 C2 的区别在于，恶意软件域通过外部源将恶意有效载荷传输到您的网络，而对于 C2，受影响的端点通常会尝试连接到远程服务器，以检索其他指令或其他恶意内容。
  - 受恶意软件影响的 **DNS**（UTID：109003001）— 受恶意软件影响的 DNS 包括一系列技术，其中一些合法，这些技术会导致生成看似真实而实际是恶意的主机名和子域。包括新发现的主机名，这些主机名模仿现有的信誉良好的主机名，试图冒充或以其他方式误导并规避以数据库为中心的安全解决方案。此类主机名可以快速地批量生成，以抢先将其添加到数据库列表中。域名阴影通常在攻击者通过更常规的攻击获得对域帐户的控制之后发生。这提供了创建用于协调攻击的非法子域所需的访问权限，即使根域仍然合法有效，也会增加规避网络安全措施的可能性。
  - 勒索软件域名（UTID：109003002)— 勒索软件是恶意软件的一个子类别，它会锁定或以加密方式阻止用户访问数据，从而换取赎金，之后攻击者可能会将系统权限释放给用户。勒索软件可以通过恶意勒索软件域进行传播，这些域托管看似合法的文件并诱使用户下载。
- 新注册域（UTID：109020001）— 新注册域是指 TLD 运营商最近添加的域或在过去 32 天内所有权发生变更的域。虽然可以根据法律要求创建新的域，但是，绝大多数域通常都是用于协助执行恶意活动，例如作为 C2 服务器运行或是用于分发恶意软件、垃圾邮件、PUP/广告软件。Palo Alto Networks 通过监控特定馈送（域注册表和注册器），并使用区域文件、被动 DNS、WHOIS 数据来检测注册活动，从而检测新注册域。
- 网络钓鱼域（UTID：109010001）— 网络钓鱼域尝试通过网络钓鱼或网络欺骗伪装成合法网站，诱使用户提交个人信息或用户凭据等敏感数据。这些恶意活动可通过社会工程活动（凭借看似可信的源，操纵用户通过电子邮件或其他形式的电子通信提交个人信息）或 Web 流量重定向（将用户定向到看似合法的欺诈站点）进行。

- 灰色软件域（UTID：109010002）—（安装有 PAN-OS 内容版本 8290 以及更高版本时可用）。灰色软件域通常不会直接构成安全威胁，但是，他们会协助攻击向量，产生各种不良行为，或是可能只包含可疑/攻击性内容。可能包括以下网站和域名：
  - 试图欺骗用户授予远程访问权限。
  - 利用流行的网络托管和动态域名系统 (DDNS) 服务的子域来托管和分发恶意内容（子域信誉 - UTIDL 109002004）。
  - 包含广告软件和其他未经请求的应用程序（例如，挖矿软件、劫持程序和 PUP [潜在有害程序]）。
  - 使用快速通量技术部署域标识隐藏操作（快速通量检测 — UTID：109010005）。
  - 通过 DNS Security 预测分析演示恶意行为和使用（恶意 **NRD** — UTID：109010006）。
  - 由于权威 DNS 服务器上配置不当或过时的 DNS 记录尚未移除或以其他方式予以更正，因此将流量从合法来源重定向到恶意网站（悬空 **DNS** — UTID：109010008）。
  - 宣传非法活动或诈骗。
  - 包括通配符 DNS 条目，这些条目可用于通过将流量路由到恶意网站来避开阻止列表或启用通配符 DNS 攻击（通配符滥用 — UTID：109002001）。
  - 指出与根据收集的 DNS 数据建立的基线配置文件相比时，存在具有异常特征的 DNS 流量（异常检测）。
  - 已提前数月或数年注册，并处于休眠状态，以便在变为活动状态时避开声誉检查。此外，还包括从未见过或以其他方式评估过的新观察到的域名（策略性老化域名 — UTID：109002002）。
  - 根据证书透明度日志，未使用的域名是否已被可能有恶意的攻击者注册：（**Stockpile Domain** 检测 - UTID：109002005）。
  - 通过模仿流行品牌域名以及错误输入的网页地址来欺骗用户，目的是将用户引导至假冒和欺诈网站。（域名抢注/误植域名 - UTID：109002003）。
- 寄放域（UTID：109010003）—（安装有 PAN-OS 内容版本 8318 以及更高版本时可用）寄放域通常是指用于托管有限内容的非活动网站，通常以点阅广告的形式出现，可为主题实体带来收益，但其中包含的内容通常对最终用户没用。尽管他们通常充当合法占位符或是仅起到良性妨碍的作用，但是，他们还可用作分发恶意软件的潜在媒介。
- 代理规避和匿名程序（UTID：109010004）—（安装有 PAN-OS 内容版本 8340 以及更高版本时可用）代理规避和匿名者是指用于绕过内容过滤策略的服务流量。尝试通过匿名程序代理服务绕过组织内容过滤策略的用户在 DNS 级别会被阻止。
- 广告跟踪域（UTID：109004000）—（安装 PAN-OS 内容版本 8586 及更高版本后可用）广告跟踪域为网页提供某些类型的营销自动化内容，以跟踪用户参与度（例如链接点击、网页浏览等）。通常，这些第三方域名通过使用没有实名地址的网址来隐藏真实身份，使其看起来像是原始域名的一部分。
  - **CNAME** 隐藏（UTID：109004001）— CNAME 隐藏提供了一种隐藏 URL 的替代方法，即通过修改子域名的 Web 请求，使其看起来好像来自同一个网站，但实际上，子域名使用

CNAME 将其解析为第三方域名。该技术会绕过一些基于浏览器的隐私保护机制，可能会连接到可疑的 CNAME 目标。

- 域名被劫持（UTID：109004000）—（需要 Advanced DNS Security）域名劫持包括，攻击者能够将合法域名解析为由攻击者操纵的 IP 地址的域名，这通常是通过破坏组织的 DNS 基础设施的某些方面来实现的。其中可能包括对 DNS 提供商的未经授权的管理访问、DNS 解析过程中的 MiTM 攻击或对 DNS 服务器本身的访问。
- 配置错误的域（UTID：109004000）—（需要 Advanced DNS Security）配置错误的域使攻击者能够利用域配置问题来将自己的恶意域合并到组织的 DNS 中。利用这些过时的 DNS 记录，攻击者可以掌控客户的子域，并将用户重定向到攻击者控制的 IP 或网站，以便实现恶意目的。这些无法解析的错误配置域基于在 Advanced DNS Security 配置期间指定的面向公众的父域。
  - 错误配置的区域：（UTID：109004200）— 与任何其他错误配置类别均不对应的错误配置域的通用类别。
  - 错误配置区域无关联（UTID：109004201）— 由于组织面向公众的域中的权威 DNS 服务器上的 DNS 记录配置不当或过时，配置错误的域会将流量从合法来源重定向到恶意网站。
  - 配置错误可声明 **NX**（UTID：109004202）— 作为组织 DNS 配置的一部分定义的错误配置域名（但已不存在）(NXDOMAINS)，可能会被攻击者秘密注册并用于将用户重定向到恶意网站，并可能允许攻击者访问客户的网络。

数据收集和记录

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 DNS Security 许可证（用于增强功能支持）或 DNS Security 许可证 ❑ 高级威胁防护或威胁防护许可证

在执行域查找，以便为基于 Strata Logging Service 的活动应用程序（AIOps for NGFW Free、Prisma Access、Strata Logging Service 等）生成 DNS Security 日志时，DNS Security 服务会根据防火墙的安全策略规则、相关操作和 DNS 查询详细信息收集服务器响应和请求信息。此外，网络安全平台会将补充 DNS 数据转发到 DNS Security 云服务器，Palo Alto Networks 服务将使用其来提供更准确的域信息（例如提供商 ASN、托管信息和地理位置标识）。虽然这些补充数据对于运行 DNS Security 服务并不必需，但其提供了生成改进的分析、DNS 检测和预防功能的资源。此操作将在数据收集后不到 30 秒内发生。为了最大限度地减少对防火墙性能的影响，DNS Security 遥测以最小的开销运行，这可能会限制发送到 Strata Logging Service 的 DNS 遥测数据的总量；因此，只有一部分 DNS 查询会作为 DNS Security 日志条目转发到 Strata Logging Service。因此，Palo Alto Networks 建议将恶意 DNS 请求的日志视为威胁日志，而不是 DNS Security 日志。

恶意 *DNS* 查询也会记录为威胁日志，如果配置正确的话，将使用 *PAN-OS* 日志转发提交给 *Strata Logging Service*。

DNS Security 可以提交以下数据字段：

字段	说明
操作	显示对 DNS 查询采取的策略操作。
类型	显示 DNS 记录类型。
响应	DNS 查询中的域解析到的 IP 地址。
响应码	作为 DNS 查询答案而收到的 DNS 响应码。
源 IP	发出 DNS 请求的系统的 IP 地址。
源用户	启用防火墙 User-ID 功能后，将显示 DNS 请求者的身份。

字段	说明
Source Zone（源区域）	安全策略规则中引用的已配置源区域。

添加到 *DNS* 异常中允许列表的域将绕过 *DNS* 扩展的数据收集。

可以使用以下 CLI 命令禁止自动提交可用于潜在识别用户身份（源 IP、源用户和源区域）的数据字段：**`set deviceconfig setting ctd cloud-dns-privacy-mask yes`**。您必须 **`Commit`**（提交）更改才能使更新生效。

区域服务域

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 DNS Security 许可证（用于增强功能支持）或 DNS Security 许可证 ❑ 高级威胁防护或威胁防护许可证

Palo Alto Networks 维护着一个全球和区域服务域网络，为 DNS Security 和 Advanced DNS Security 运营提供服务。这些服务域运行实时 DNS 请求分析器，访问 DNS 签名数据库，并提供依赖高级云的功能。默认情况下，DNS Security 和 Advanced DNS Security 会连接到全局服务域（分别为 dns.service.paloaltonetworks.com 和 adv-dns.service.paloaltonetworks.com），然后会自动重定向到最接近网络安全平台位置的区域服务域。

DNS Security 区域服务域

Palo Alto Networks 建议使用默认全局服务域配置，以改进故障转移处理；但是，如果您由于位置的特殊性（例如，跨多个重叠的区域服务域时）而遇到延迟问题，则可以手动指定服务域。要指定 DNS Security 使用的区域服务域，您必须为 dns.service.paloaltonetworks.com 添加一个 DNS 条目，其中包含一个 CNAME 记录，该记录指示作为 DNS 服务器配置一部分的有效区域服务域。连接到区域服务域后，可以在防火墙上发出以下 CLI 命令来查看平均延迟：

```
show dns-proxy dns-signature counters
```

。相关部分位于签名查询 API 标题下。

下表列出了 DNS Security 服务域：

位置	网址
南非开普敦	dns-za.service.paloaltonetworks.com
中国香港	dns-hk.service.paloaltonetworks.com
日本东京	dns-jp.service.paloaltonetworks.com
新加坡	dns-sg.service.paloaltonetworks.com

位置	网址
印度孟买	dns-in.service.paloaltonetworks.com
澳大利亚悉尼	dns-au.service.paloaltonetworks.com
英国伦敦	dns-uk.service.paloaltonetworks.com
德国法兰克福	dns-de.service.paloaltonetworks.com
荷兰埃姆斯哈文	dns-nl.service.paloaltonetworks.com
法国巴黎	dns-fr.service.paloaltonetworks.com
巴林	dns-bh.service.paloaltonetworks.com
加拿大魁北克蒙特利尔	dns-ca.service.paloaltonetworks.com
巴西圣保罗奥萨斯科	dns-br.service.paloaltonetworks.com
美国爱荷华州康瑟尔布拉夫斯	dns-us-ia.service.paloaltonetworks.com
美国弗吉尼亚州北部阿什本	dns-us-va.service.paloaltonetworks.com
美国俄勒冈州戴尔斯	dns-us-or.service.paloaltonetworks.com
美国加利福尼亚州洛杉矶	dns-us-ca.service.paloaltonetworks.com

Advanced DNS Security 区域服务域

您可以手动指定便于进行 Advanced DNS Security 查询的服务器。虽然 Palo Alto Networks 建议使用默认的全局服务域，但如果遇到高于预期的延迟或其他与服务相关的问题，则可以覆盖所选服务器。

您可以在 PAN-OS 中指定 Advanced DNS Security 服务域，导航路径为 **Device**（设备） > **Setup**（设置） > **Management**（管理） > **Advanced DNS Security** > **DNS Security Server**（**DNS Security** 服务器）。

此设置不影响标准 *DNS Security* 查询的处理方式。

下表列出了 Advanced DNS Security 服务域：

位置	网址
南非开普敦	za.adv-dns.service.paloaltonetworks.com
巴林	bh.adv-dns.service.paloaltonetworks.com
中国香港	hk.adv-dns.service.paloaltonetworks.com
日本东京	jp.adv-dns.service.paloaltonetworks.com
新加坡	sg.adv-dns.service.paloaltonetworks.com
印度孟买	in.adv.dns.service.paloaltonetworks.com
澳大利亚悉尼	au.adv-dns.service.paloaltonetworks.com
英国伦敦	uk.adv-dns.service.paloaltonetworks.com
德国法兰克福	de.adv.dns.service.paloaltonetworks.com
荷兰埃姆斯哈文	nl.adv.dns.service.paloaltonetworks.com
法国巴黎	fr.adv-dns.service.paloaltonetworks.com
巴林	bh.adv-dns.service.paloaltonetworks.com
加拿大魁北克蒙特利尔	ca.adv.dns.service.paloaltonetworks.com
巴西圣保罗奥萨斯科	br.adv.dns.service.paloaltonetworks.com
美国爱荷华州康瑟尔布拉夫斯	us-ia.adv.dns.service.paloaltonetworks.com
美国弗吉尼亚州北部阿什本	us-va.adv.dns.service.paloaltonetworks.com
美国俄勒冈州戴尔斯	us-or.adv.dns.service.paloaltonetworks.com
美国加利福尼亚州洛杉矶	us-ca.adv.dns.service.paloaltonetworks.com

配置 DNS Security 订阅服务

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	❑ Advanced DNS Security 许可证（用于增强功能支持）或 DNS Security 许可证 ❑ 高级威胁防护或威胁防护许可证

在启用和配置 Advanced DNS Security 或 DNS Security 之前，除了需要它们运行的任何平台的许可证外，还必须获得并安装 Threat Prevention（或 Advanced Threat Prevention）许可证以及 Advanced DNS Security 或 DNS Security 许可证。许可证从 Palo Alto Networks 客户支持门户激活，并且在进行 DNS 分析之前必须处于活动状态。此外，DNS Security 订阅服务（类似于其他 Palo Alto Networks 安全服务）通过安全配置文件进行管理，这又取决于通过安全策略规则定义的网络实施策略的配置。在启用 DNS Security 订阅服务之前，建议您熟悉启用安全订阅的安全平台的核心组件。有关更多信息，请参阅您的产品文档。

要启用并配置 DNS Security 订阅服务，使其在网络安全部署中以最佳方式运行，请参阅下面的任务。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。

- 在我的网络安全平台上启用 DNS Security 或 Advanced DNS Security，以防止 DNS 威胁进入我的网络（必需）
- 创建域签名例外，允许列表限制误报，防止内部 DNS 服务器触发 DNS 分类
- 测试为可用域类别配置的策略操作
- 验证防火墙与 DNS Security 服务的连接性
- 通过在防火墙上自定义我的 DNS 查找超时设置来限制由于我的延迟而丢弃的连接

启用 DNS Security

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 DNS Security 许可证（用于增强功能支持）或 DNS Security 许可证 ❑ 高级威胁防护或威胁防护许可证

要启用 DNS Security，您必须创建（或修改）Anti-Spyware 安全配置文件以访问 DNS Security 服务，为 DNS 签名类别（或多个类别）配置日志严重性和策略设置，然后将该配置文件附加到安全策略规则。

- Strata Cloud Manager
- PAN-OS 和 Panorama

启用 DNS Security (Strata Cloud Manager)

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。

STEP 2 | 验证 DNS Security 和 Threat Prevention（或 Advanced Threat Prevention）许可证是否处于活动状态。选择 **Manage**（管理） > **Configuration**（配置） > **NGFW** 和 **Prisma Access** > **Overview**（概述），然后单击 **License**（许可证）面板中的许可证使用条款链接。您应该会在以下安全服务旁看到绿色复选标记：防病毒、防间谍软件、漏洞保护和 DNS Security。

STEP 3 | 验证您安全策略中的 *paloalto-dns-security* App-ID 是否配置为启用来自 DNS Security 云安全服务的流量。

如果您的防火墙部署通过面向互联网且配置为实施 *App-ID* 安全策略的外围防火墙路由您的管理流量，则您必须允许外围防火墙上的 *App-ID*；否则将阻止 *DNS Security* 连接。

STEP 4 | 配置 DNS Security 签名策略设置，以发送恶意软件 DNS 查询到定义的 Sinkhole。

如果您使用外部动态列表作为域允许列表，则其优先级不会高于 *DNS Security* 域策略操作。因此，当域匹配 *EDL* 中的条目和 *DNS Security* 域类别时，仍会应用在 *DNS Security* 下指定的操作，即使 *EDL* 明确配置了允许操作也是如此。如果要添加 *DNS* 域例外，请配置具有提醒操作的 *EDL*，或将其添加到位于 *DNS* 例外选项卡中的 *DNS* 域/*FQDN* 允许列表。

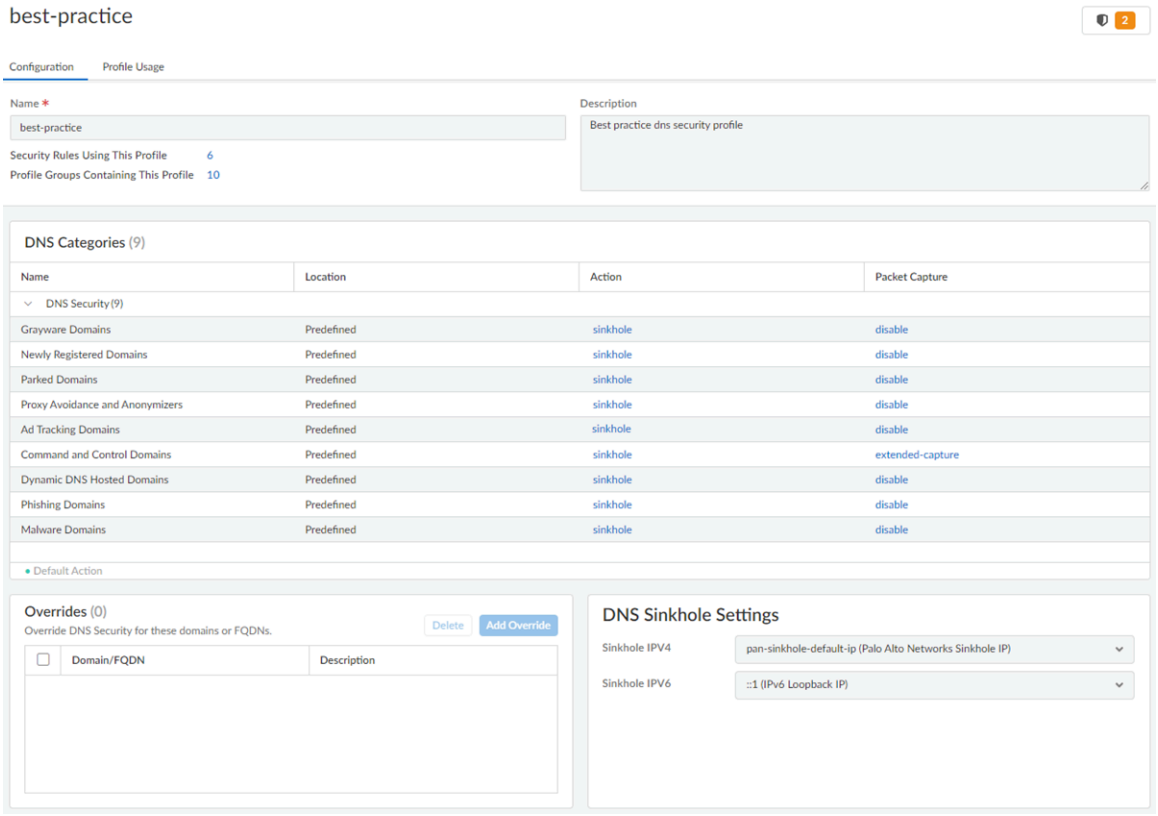
1. 选择 **Manage**（管理） > **Configuration**（配置） > **NGFW** 和 **Prisma Access** > **Security Services**（安全服务） > **DNS Security**。
2. 创建或修改现有的 DNS Security 配置文件。
3. 确定配置文件的**Name**（名称），或者提供描述。
4. 在 **DNS Categories**（**DNS** 类别）部分的 DNS Security 标题下，有单独可配置的 DNS 签名源，允许您定义单独的策略操作以及数据包捕获设置。

   Palo Alto Networks 建议对所有签名源使用默认操作设置，以确保最佳覆盖范围并为事件响应和补救提供协助。有关配置 *DNS Security* 设置的最佳实践，请参阅防止网络免遭第 4 层和第 7 层逃避的最佳实践。

   - 选择为 DNS Security 签名源的已知恶意软件站点执行 DNS 查找时采取的操作。可选操作为警报、允许、阻止或 sinkhole。Palo Alto Networks 建议将操作设置为 Sinkhole。
   - 通过为每个 DNS 签名源配置相应日志严重性为 **None**（无）的策略操作 **Allow**（允许），可以完全绕过 DNS 流量检查。
   - 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。
5. 在 **DNS Sinkhole Settings**（**DNS Sinkhole** 设置）部分，验证是否存在有效的 **Sinkhole** 地址。为了方便，默认设置 (pan-sinkhole-default-ip) 设置为访问 Palo Alto Networks sinkhole 服务器。Palo Alto Networks 可通过更新自动刷新此地址。

   对于与指定 *Sinkhole* 服务器的 *Sinkhole* 操作配置的 *DNS* 类别匹配的域的 *DNS* 查询，***Sinkhole*** 会伪造响应，以协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，如果客户端所在的网络没有内部 *DNS* 服务器，或者使用的软件或工具无法将 *CNAME* 正确解析为 *A* 记录响应，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。在这些情况下，您应该使用以下漏洞 *IP* 地址：*(72.5.65.111)*。

   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。



6. 单击 **OK**（确定）以保存 DNS Security 配置文件。

STEP 5 | 将 DNS Security 配置文件附加到安全策略规则。

STEP 6 | 测试是否实施了策略操作。

1. 访问 DNS Security 测试域以验证针对给定威胁类型的策略操作是否正在实施。
2. 监视活动：
   1. 查看活动日志并使用已 Sinkhole 的操作搜索 URL 域，从而查看您访问的测试域的日志条目。

STEP 7 | 可选 — 创建解密策略规则以解密 DNS-over-TLS/端口 853 流量。然后可以使用包含 DNS 策略设置的 DNS Security 配置文件配置来处理解密的 DNS 负载。当 DNS-over-TLS 流量被解密时，威胁日志中生成的 DNS 请求将显示为常规 **dns-base** 应用程序，其源端口为 853。

STEP 8 | 有关其他监控选项，请参阅 监控 DNS Security 订阅服务

启用 DNS Security (NGFW (Managed by PAN-OS or Panorama))

PAN-OS 10.0 及更高版本支持可单独配置的 DNS 签名源，这使您能够为给定签名源定义单独的策略操作以及日志严重性级别。这使您能够根据网络安全协议，根据域类型的威胁态势创建离散、精确的安全措施。DNS 签名源定义可通过 PAN-OS 内容版本进行扩展，因此，当引入新的 DNS Security 分析器时，您能够根据威胁的性质创建特定的策略。一旦升级到 PAN-OS 10.0 以及更高版本，DNS Security 源将被重新定义为新的类别，以提供扩展的粒度控制，这样，新类别就将替代先

前定义的操作，并获取默认设置。必须对新定义的 DNS Security 类别重新应用任何 sinkhole、日志严重性和相应的数据包捕获设置。

- PAN-OS 11.0 及更高版本
- PAN-OS 10.x
- PAN-OS 9.1

启用 DNS Security（PAN-OS 11.0 及更高版本）

STEP 1 | 登录 NGFW。

STEP 2 | 要利用 DNS Security，您必须拥有有效的DNS Security 和 Threat Prevention（或 Advanced Threat Prevention）订阅。

确认您拥有必要的订阅。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 3 | 验证您安全策略中的 *paloalto-dns-security* App-ID 是否配置为启用来自 DNS Security 云安全服务的流量。

如果您的防火墙部署通过面向互联网且配置为实施 *App-ID* 安全策略的外围防火墙路由您的管理流量，则您必须允许外围防火墙上的 *App-ID*；否则将阻止 *DNS Security* 连接。

STEP 4 | 配置 DNS Security 签名策略设置，以发送恶意软件 DNS 查询到定义的 Sinkhole。

如果您使用外部动态列表作为域允许列表，则其优先级不会高于 *DNS Security* 域策略操作。因此，当域匹配 *EDL* 中的条目和 *DNS Security* 域类别时，仍会应用在 *DNS Security* 下指定的操作，即使 *EDL* 明确配置了允许操作也是如此。如果要添加 *DNS* 域例外，请配置具有提醒操作的 *EDL*，或将其添加到位于 *DNS* 例外选项卡中的 *DNS* 域/*FQDN* 允许列表。

1. 选择 **Objects**（对象） > **Security Profiles**（安全配置文件） > **Anti-Spyware**（防间谍软件）。
2. 创建或修改现有配置文件，或者从现有的默认配置文件中选择一个并进行克隆。
3. 确定配置文件的**Name**（名称），或者提供描述。
4. 选择 **DNS Policies**（**DNS** 策略）选项卡。
5. 在“DNS Security ”标题下的 **Signature Source**（签名源）列中，存在可单独配置的 DNS 签名源，您可以通过该签名源定义单独的策略操作和日志严重性级别。

   Palo Alto Networks 建议更改签名源的默认 *DNS* 策略设置以确保最佳覆盖范围，并协助事件响应和修复。请遵循防止网络免遭第 4 层和第 7 层规避的最佳实践中概述的 *DNS Security* 设置配置最佳实践。

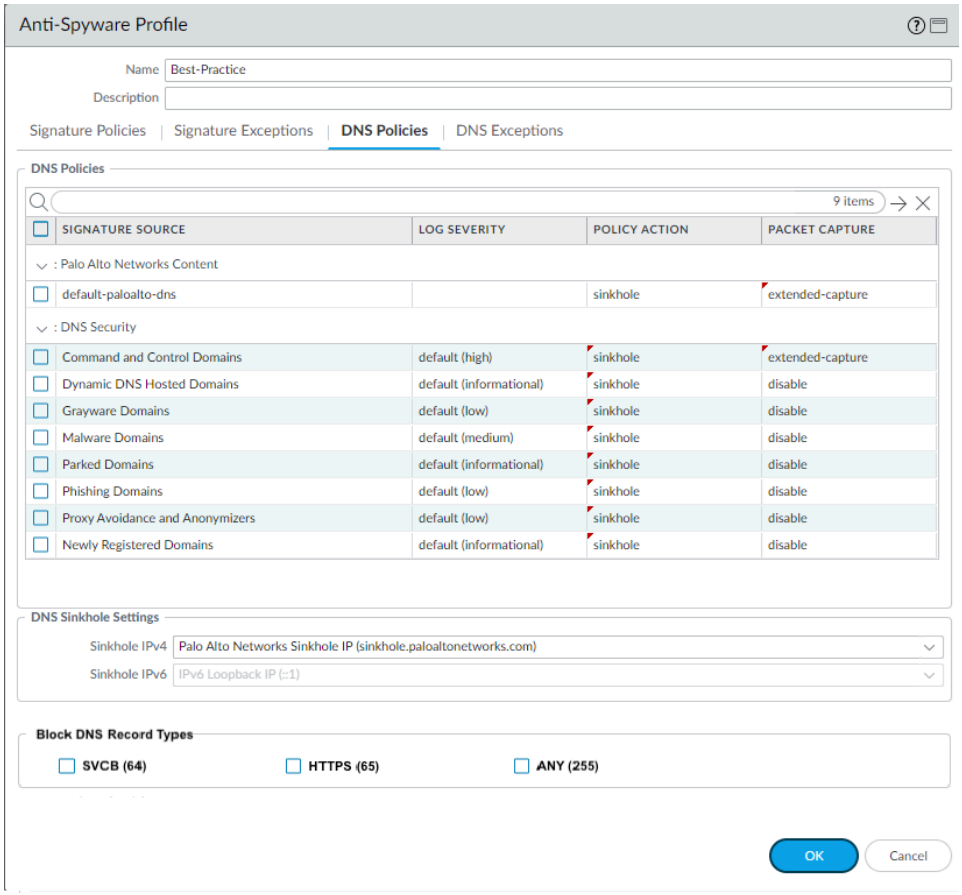
   - 指定防火墙检测到与 DNS 签名匹配的域时记录的日志严重性级别。更多有关各种日志严重性级别的信息，请参阅威胁严重性级别。
   - 选择为 DNS Security 签名源的已知恶意软件站点执行 DNS 查找时采取的操作。这些选项包括 Default、Allow、Block 或 Sinkhole。验证操作是否设为 sinkhole。
   - 通过为每个 DNS 签名源配置相应日志严重性为 **None**（无）的策略操作 **Allow**（允许），可以完全绕过 DNS 流量检查。
   - 在 **Packet Capture**（数据包捕获）下拉列表中，选择 **single-packet**（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。
6. 在 **DNS Sinkhole Settings**（**DNS Sinkhole** 设置）部分中，验证是否已启用 **Sinkhole**。为方便起见，已设置访问 Palo Alto Networks 服务器的默认 Sinkhole 地址 (sinkhole.paloaltonetworks.com)。Palo Alto Networks 可通过内容更新自动刷新此地址。

   对于与指定 *Sinkhole* 服务器的 *Sinkhole* 操作配置的 *DNS* 类别匹配的域的 *DNS* 查询，***Sinkhole*** 会伪造响应，以协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，以期将内部 *DNS* 服务器解析为 *CNAME* 记录，从而记录并标记从客户端到配置的 *Sinkhole* 服务器的恶意通信。但是，如果客户端所在的网络没有内部 *DNS* 服务器，或者使用的软件或工具无法将 *CNAME* 正确解析为 *A* 记录响应，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。在这些情况下，您应该使用以下漏洞 *IP* 地址：*(72.5.65.111)*。

   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。

7. （可选）屏蔽指定的 DNS 资源记录类型记录类型，这些记录类型用于在后续的 TLS 连接中加密客户端 hello 期间交换密钥信息。以下 DNS RR 类型可用：SVCB (64)、HTTPS (65) 和 ANY (255)。

   - 虽然没必要阻止 *ECH* 即可启用 *DNS Security over DoH*，但 *Palo Alto Networks* 目前建议阻止 *ECH* 使用的所有 *DNS* 记录类型，以实现最佳安全性。
   - *64* 和 *65* 类型的资源记录标准仍在不断修改（草案状态），可能会发生变化。有关 *DNS SVCB* 和 *HTTPS RR* 的更多信息，请参阅：通过 IETF 定义的 DNS（DNS SVCB 和 HTTPS RR）进行服务绑定和参数规范。



8. 单击 **OK**（确定）以保存防间谍软件配置文件。

STEP 5 | 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）。
2. 选择或创建 **Security Policy Rule**（安全策略规则）。
3. 在 **Actions**（操作）选项卡上，选中 **Log at Session End**（在会话结束时记录）复选框以启用日志记录。
4. 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或修改过的配置文件。
5. 单击 **OK**（确定）以保存策略规则。

STEP 6 | 测试是否实施了策略操作。

1. 访问 DNS Security 测试域以验证针对给定威胁类型的策略操作是否正在实施。
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。
   3. 有关更多监视选项，请参见监控 DNS Security 订阅服务

STEP 7 | 可选 — 创建解密策略规则以解密 DNS-over-TLS/端口 853 流量。然后，可以使用包含 DNS 策略设置的防间谍配置文件配置来处理解密的 DNS 有效负载。当 DNS-over-TLS 流量被解密时，威胁日志中生成的 DNS 请求将显示为常规 **dns-base** 应用程序，其源端口为 853。

STEP 8 | 可选 — 查看试图连接到恶意域的受感染主机

启用 DNS Security (PAN-OS 10.x)

STEP 1 | 登录 NGFW。

STEP 2 | 要利用 DNS Security，您必须拥有有效的DNS Security 和 Threat Prevention（或 Advanced Threat Prevention）订阅。

确认您拥有必要的订阅。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 3 | 验证您安全策略中的 *paloalto-dns-security* App-ID 是否配置为启用来自 DNS Security 云安全服务的流量。

如果您的防火墙部署通过面向互联网且配置为实施 *App-ID* 安全策略的外围防火墙路由您的管理流量，则您必须允许外围防火墙上的 *App-ID*；否则将阻止 *DNS Security* 连接。

STEP 4 | 配置 DNS Security 签名策略设置，以发送恶意软件 DNS 查询到定义的 Sinkhole。

如果您使用外部动态列表作为域允许列表，则其优先级不会高于 *DNS Security* 域策略操作。因此，当域匹配 *EDL* 中的条目和 *DNS Security* 域类别时，仍会应用在 *DNS Security* 下指定的操作，即使 *EDL* 明确配置了允许操作也是如此。如果要添加 *DNS* 域例外，请配置具有提醒操作的 *EDL*，或将其添加到位于 *DNS* 例外选项卡中的 *DNS* 域/*FQDN* 允许列表。

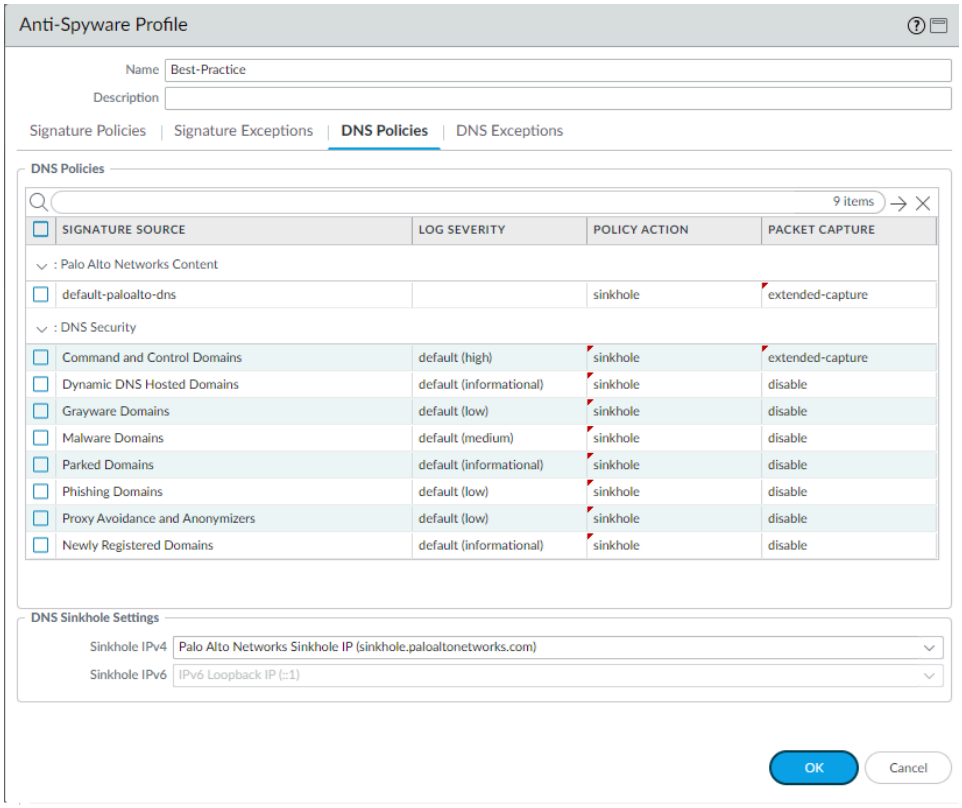
1. 选择 **Objects**（对象） > **Security Profiles**（安全配置文件） > **Anti-Spyware**（防间谍软件）。
2. 创建或修改现有配置文件，或者从现有的默认配置文件中选择一个并进行克隆。
3. 确定配置文件的**Name**（名称），或者提供描述。
4. 选择 **DNS Policies**（**DNS** 策略）选项卡。
5. 在“DNS Security ”标题下的 **Signature Source**（签名源）列中，存在可单独配置的 DNS 签名源，您可以通过该签名源定义单独的策略操作和日志严重性级别。

   Palo Alto Networks 建议更改签名源的默认 *DNS* 策略设置以确保最佳覆盖范围，并协助事件响应和修复。请遵循防止网络免遭第 4 层和第 7 层规避的最佳实践中概述的 *DNS Security* 设置配置最佳实践。

   - 指定防火墙检测到与 DNS 签名匹配的域时记录的日志严重性级别。更多有关各种日志严重性级别的信息，请参阅威胁严重性级别。
   - 选择为 DNS Security 签名源的已知恶意软件站点执行 DNS 查找时采取的操作。这些选项包括 Default、Allow、Block 或 Sinkhole。验证操作是否设为 sinkhole。
   - 通过为每个 DNS 签名源配置相应日志严重性为 **None**（无）的策略操作 **Allow**（允许），可以完全绕过 DNS 流量检查。
   - 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。
6. 在 **DNS Sinkhole Settings**（**DNS Sinkhole** 设置）部分中，验证是否已启用 **Sinkhole**。为方便起见，已设置访问 Palo Alto Networks 服务器的默认 Sinkhole 地址 (sinkhole.paloaltonetworks.com)。Palo Alto Networks 可通过内容更新自动刷新此地址。

   对于与指定 *Sinkhole* 服务器的 *Sinkhole* 操作配置的 *DNS* 类别匹配的域的 *DNS* 查询，***Sinkhole*** 会伪造响应，以协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，以期将内部 *DNS* 服务器解析为 *CNAME* 记录，从而记录并标记从客户端到配置的 *Sinkhole* 服务器的恶意通信。但是，如果客户端所在的网络没有内部 *DNS* 服务器，或者使用的软件或工具无法将 *CNAME* 正确解析为 *A* 记录响应，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。在这些情况下，您应该使用以下漏洞 *IP* 地址：*(72.5.65.111)*。

   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。



7. 单击 **OK**（确定）以保存防间谍软件配置文件。

STEP 5 | 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）。
2. 选择或创建 **Security Policy Rule**（安全策略规则）。
3. 在 **Actions**（操作）选项卡上，选中 **Log at Session End**（在会话结束时记录）复选框以启用日志记录。
4. 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或修改过的配置文件。
5. 单击 **OK**（确定）以保存策略规则。

STEP 6 | 测试是否实施了策略操作。

1. 访问 DNS Security 测试域以验证针对给定威胁类型的策略操作是否正在实施。
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。
    3. 有关更多监视选项，请参见监控 DNS Security 订阅服务

STEP 7 | 可选 — 创建解密策略规则以解密 DNS-over-TLS/端口 853 流量。然后，可以使用包含 DNS 策略设置的防间谍配置文件配置来处理解密的 DNS 有效负载。当 DNS-over-TLS 流量被解密时，威胁日志中生成的 DNS 请求将显示为常规 **dns-base** 应用程序，其源端口为 853。

STEP 8 | 可选 — 查看试图连接到恶意域的受感染主机

启用 DNS Security (PAN-OS 9.1)

STEP 1 | 登录 NGFW。

STEP 2 | 要利用 DNS Security，您必须拥有活动的 DNS Security 和 Threat Prevention 订阅。

确认您拥有必要的订阅。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 3 | 验证您安全策略中的 *paloalto-dns-security* App-ID 是否配置为启用来自 DNS Security 云安全服务的流量。

如果您的防火墙部署通过面向互联网且配置为实施 *App-ID* 安全策略的外围防火墙路由您的管理流量，则您必须允许外围防火墙上的 *App-ID*；否则将阻止 *DNS Security* 连接。

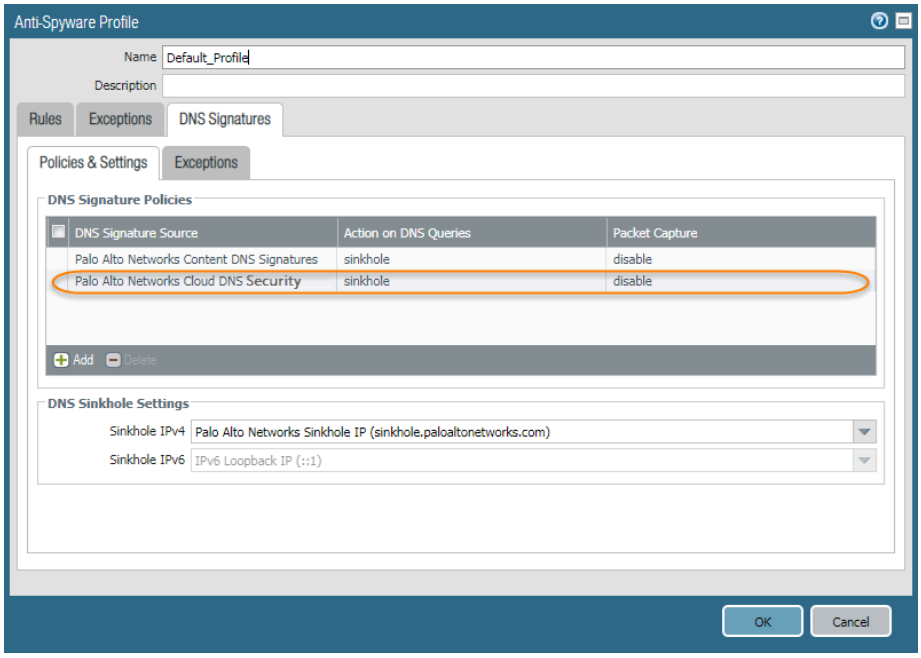
STEP 4 | 配置 DNS Security 签名策略设置，以发送恶意软件 DNS 查询到定义的 sinkhole。

如果您使用外部动态列表作为域允许列表，则其优先级不会高于 *DNS Security* 域策略操作。因此，当域匹配 *EDL* 中的条目和 *DNS Security* 域类别时，仍会应用在 *DNS Security* 下指定的操作，即使 *EDL* 明确配置了允许操作也是如此。如果要添加 *DNS* 域例外，可以配置具有警报操作的 *EDL*。

1. 选择 **Objects**（对象） > **Security Profiles**（安全配置文件） > **Anti-Spyware**（防间谍软件）。
2. 创建或修改现有配置文件，或者从现有的默认配置文件中选择一个并进行克隆。
3. 确定配置文件的**Name**（名称），或者提供描述。
4. 选择 **DNS Signatures**（**DNS** 签名） **> Policies & Settings**（策略和设置）选项卡。
5. 如果不存在 **Palo Alto Networks DNS Security**（**DNS Security** ）源，则单击 **Add**（添加），并从列表中进行选择。
6. 选择为 DNS Security 签名源的已知恶意软件站点执行 DNS 查找时采取的操作。可选操作为警报、允许、阻止或 sinkhole。验证操作是否设为 sinkhole。
7. （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。
8. 在 **DNS Sinkhole Settings**（**DNS Sinkhole** 设置）部分中，验证是否已启用 **Sinkhole** 。为方便起见，已设置访问 Palo Alto Networks 服务器的默认 Sinkhole 地址 (sinkhole.paloaltonetworks.com)。Palo Alto Networks 可通过内容更新自动刷新此地址。

   对于与指定 *Sinkhole* 服务器的 *Sinkhole* 操作配置的 *DNS* 类别匹配的域的 *DNS* 查询，***Sinkhole*** 会伪造响应，以协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，以期将内部 *DNS* 服务器解析为 *CNAME* 记录，从而记录并标记从客户端到配置的 *Sinkhole* 服务器的恶意通信。但是，如果客户端所在的网络没有内部 *DNS* 服务器，或者使用的软件或工具无法将 *CNAME* 正确解析为 *A* 记录响应，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。在这些情况下，您应该使用以下漏洞 *IP* 地址：*(72.5.65.111)*。

   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。
9. 单击 **OK**（确定）以保存防间谍软件配置文件。



STEP 5 | 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）。
2. 选择或创建 **Security Policy Rule**（安全策略规则）。
3. 在 **Actions**（操作）选项卡上，选中 **Log at Session End**（在会话结束时记录）复选框以启用日志记录。
4. 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或修改过的配置文件。
5. 单击 **OK**（确定）以保存策略规则。

STEP 6 | 测试是否实施了策略操作。

1. 访问 DNS Security 测试域以验证针对给定威胁类型的策略操作是否正在实施。
2. 监控防火墙上的活动：
   1. 查看威胁活动并搜索您访问的域名的 URL 测试域和阻止的活动。
   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。
   3. 有关更多监视选项，请参见监控 DNS Security 订阅服务

STEP 7 | 可选 — 创建解密策略规则以解密 DNS-over-TLS/端口 853 流量。然后，可以使用包含 DNS 策略设置的防间谍配置文件配置来处理解密的 DNS 有效负载。当 DNS-over-TLS 流量被解密时，威胁日志中生成的 DNS 请求将显示为常规 **dns-base** 应用程序，其源端口为 853。

STEP 8 | 可选 — 查看试图连接到恶意域的受感染主机

启用 Advanced DNS Security

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 DNS Security 许可证（用于增强功能支持） ❑ 高级威胁防护或威胁防护许可证

Advanced DNS Security 是对您现有的 DNS Security 配置的补充，它通过检查 DNS 响应的变化来提供额外的保护，从而防止 DNS 劫持。在继续执行此步骤之前，您应该已完全配置 DNS Security 设置。

要启用 Advanced DNS Security，必须创建（或修改）防间谍软件安全配置文件以访问 Advanced DNS Security 服务，配置 DNS 签名类别（或类别）的日志严重性和策略设置，然后将配置文件附加到安全策略规则。

- PAN-OS 11.2 及更高版本
- 云端管理

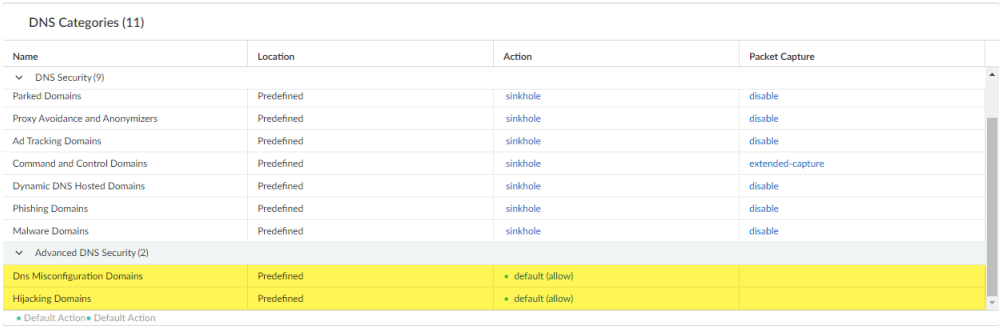
启用 Advanced DNS Security (Strata Cloud Manager)

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。

STEP 2 | 确认 DNS Security 和 Threat Prevention 许可证处于活动状态。选择 **Manage**（管理）> **Configuration**（配置）> **NGFW** 和 **Prisma Access** > **Overview**（概述），然后单击 **License**（许可证）面板中的许可证使用条款链接。您应该会在以下安全服务旁看到绿色复选标记：防病毒、防间谍软件、漏洞保护和 DNS Security。

STEP 3 | 更新或创建新的 DNS Security 配置文件，以便启用实时 Advanced DNS Security 查询。通常，这是用于 DNS Security 配置的现有 DNS Security 配置文件。

1. 选择现有 DNS Security 配置文件，或 **Add**（添加）一个新配置文件，导航路径为 **Manage**（管理） > **Configuration**（配置） > **NGFW** 和 **Prisma Access** > **Security Services**（安全服务） > **DNS Security**。
2. 选择您的 DNS Security 配置文件，然后转到 **DNS Categories**（**DNS** 类别）。



3. 对于每个 Advanced DNS Security 域类别，指定检测到相应域类型时要采取的策略 **Action**（操作）。目前有两个可用的分析引擎：**DNS Misconfiguration Domains**（**DNS** 错误配置域）和 **Hijacking Domains**（劫持域）。

   策略操作选项：

   - **Allow**（允许）— 允许 DNS 查询。

     通过将操作设置为允许，将日志严重性设置为参考，可以将 *Strata Cloud Manager* 配置为在检测到适用的域类型时生成警报。

   - **Block**（阻止）— 阻止 DNS 查询。
   - **Sinkhole** — 针对检测到的恶意域为 DNS 查询伪造 DNS 响应。这会将恶意域名的解析定向到一个特定的 IP 地址（称为 Sinkhole IP），该地址作为响应嵌入。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。

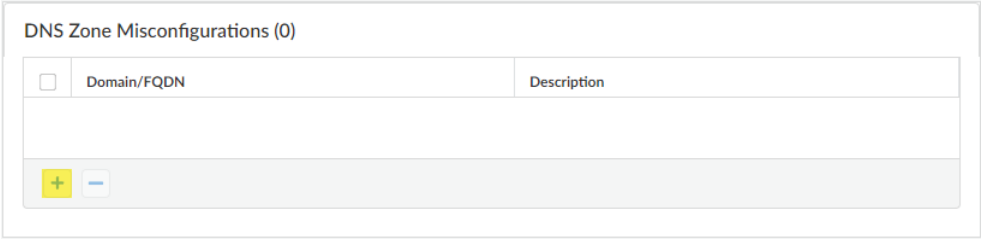
STEP 4 | （可选）指定您的组织内任何面向公共的父域，您希望 Advanced DNS Security 分析并监视其中是否存在错误配置的域。错误配置的域是由域所有者无意中造成的，他们使用

CNAME、MX、NS 记录类型将别名记录指向第三方域，并使用不再有效的条目，使得攻击者能够通过注册过期或未使用的域来接管原来的域。

TLD（顶级域）和根级域无法添加到 *DNS* 区域错误配置列表中。

1. 选择包含 Advanced DNS Security 配置的 DNS Security 配置文件，导航路径为 **Manage**（管理）> **Configuration**（配置）> **NGFW** 和 **Prisma Access** > **Security Services**（安全服务）> **DNS Security**。
2. 在 **DNS Zone Misconfigurations**（**DNS** 区域错误配置）部分，添加面向公众的父域，并添加可选说明，以帮助您识别组织内的域使用情况或所有权。

   条目必须按以下格式（例如 *paloaltonetworks.com*）在域中包含一个“.”，否则会被解析为主机名，而主机名会被视为私有域。



3. 单击 **OK**（确定）以退出并保存 DNS Security 配置文件。

STEP 5 | （可选）监控在 Strata Cloud Manager 上使用 Advanced DNS Security 检测到的 DNS 查询的活动。使用 Advanced DNS Security 实时分析 DNS 响应数据包分析的 DNS Security 类别具有前缀“adns”，后跟类别。例如，adns-dnsmisconfig，其中“dnsmisconfig”表示支持的 DNS 类别类型。如果 DNS 域类别是通过分析 DNS 请求数据包确定的，则会显示指定的类别，前缀为“DNS”，后跟类别。例如，“dns-grayware”。

1. 访问 Advanced DNS Security 测试域，以验证是否针对给定威胁类型实施了策略操作。
2. 选择 **Incidents & Alerts**（事件和警报）> **Log Viewer**（日志查看器）。您可以根据 Advanced DNS Security 域类别的特定类型筛选威胁日志，例如 `threat_category.value = 'adns-hijacking'`，其中变量 `adns-hijacking` 表示已被 Advanced DNS Security 归类为恶意 DNS 劫持尝试的 DNS 查询。日志中提供以下 Advanced DNS Security 威胁类别：

   Advanced DNS Security 类别

   - **DNS** 劫持 — `adns-hijacking`

     DNS 劫持域的威胁 ID 为（UTID：109,004,100）。

   - **DNS** 错误配置 — `adns-dnsmisconfig`

     DNS 错误配置域有三个威胁 ID，它们对应于 DNS 错误配置域类型的三种变体：dnsmisconfig_zone（UTID：109,004,200）、dnsmisconfig_zone_dangling（UTID：109,004,201）和 dnsmisconfig_claimable_nx（UTID：109,004,202）。您可以通过交叉

引用对应于特定 DNS 错误配置域类型的 Threat-ID 值来约束搜索。例如，`threat_category.value = 'adns-dnsmisconfig'` 和 `Threat ID = 109004200`，其中 109004200 表示由于 DNS 服务器配置问题而无法将流量路由到活动域的 DNS 配置错误域的威胁 ID。

使用 Advanced DNS Security 增强响应分析来分析的 DNS 类别。

- **DNS** — `adns-benign`
- 恶意软件域 — `adns-malware`
- 命令和控制域 — `adns-c2`
- 网络钓鱼域 — `adns-phishing`
- 动态 **DNS** 托管域 — `adns-ddns`
- 新注册域 — `adns-new-domain`
- 灰色软件域 — `adns-grayware`
- 寄放域 — `adns-parked`
- 代理规避和匿名程序 — `adns-proxy`
- 广告跟踪域 — `adns-proxy`

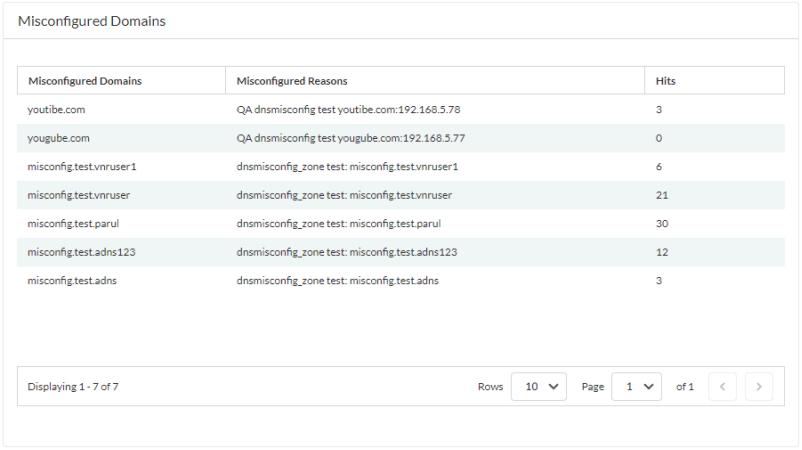
如果 *DNS* 查询在 *Advanced DNS Security* 的指定超时期限内未完成，将尽可能使用 *DNS Security* 分类。在这些情况下，使用类别的传统表示法，例如，它将被归类为 *`dns-malware`*，而不是 *`adns-malware`*，表明使用了 *DNS Security* 分类值。

3. 选择一个日志条目以查看 DNS 查询的详细信息。
4. DNS 类别显示在详细日志视图的 **General**（常规）窗格中。此外，您可以查看威胁的其他方面，包括来源 URL、特定威胁类型和相关特征。

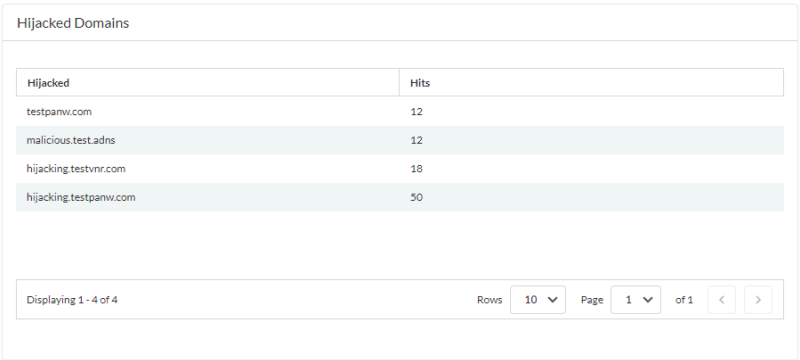
STEP 6 | （可选）检索 Advanced DNS Security 服务检测到的错误配置域和被劫持域的列表。配置错误的域基于添加到 **DNS Zone Misconfigurations**（**DNS** 区域错误配置）的面向公众的父级域条目。

从网络中删除的错误配置的域条目不会立即反映在 *Advanced DNS Security* 指示板的统计信息中。

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。
2. 选择 **Dashboards**（指示板） > **More Dashboards**（更多指示板） > **DNS Security**，以便打开 DNS Security 指示板。
3. 从 DNS Security 指示板中，参考以下小部件：
   - **Misconfigured Domains**（配置错误的域）— 查看与用户指定的面向公众的父级域关联的不可解析域列表。对于每个条目，都有一个错误配置原因和基于源 IP 的流量命中计数。



   - **Hijacked Domains**（被劫持的域）— 查看由 Advanced DNS Security 确定的被劫持域列表。对于每个条目，都有一个分类原因和基于源 IP 的流量命中计数。



启用 Advanced DNS Security（PAN-OS 11.2 及更高版本）

Palo Alto Networks 建议在设置 Advanced DNS Security 之前启用 DNS Security 功能。

STEP 1 | 登录 NGFW。

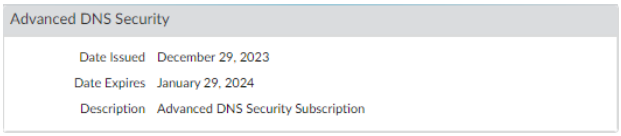
STEP 2 | 更新内容发布版本至 8832 或更高版本。

STEP 3 | 要防止使用 Advanced DNS Security 访问已知和未知的恶意域，您必须拥有有效的 Advanced DNS Security 许可证。只有在升级到 PAN-OS 11.2 后，才应安装此软件。

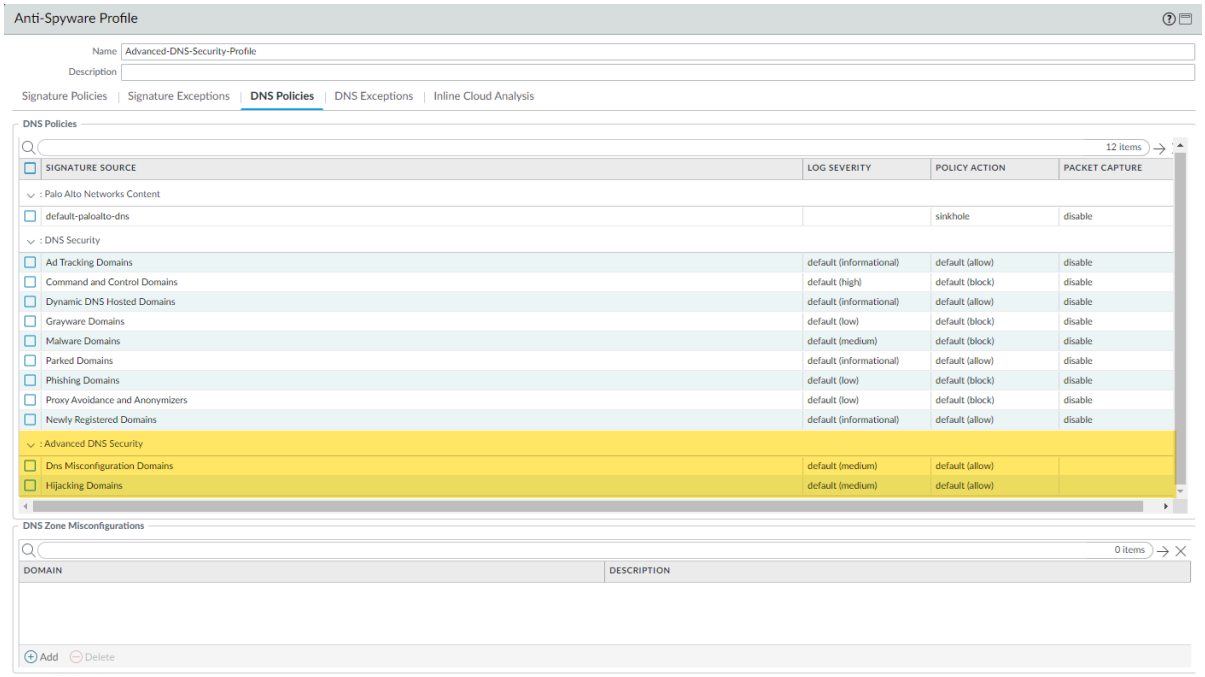
Advanced DNS Security 支持一种许可模式，当安装在以前未获得许可的防火墙上时，它将 *DNS Security* 功能归入 *Advanced DNS Security* 许可证。如果您从具有现有 *DNS Security* 许可证的防火墙进行升级，将显示表明存在单独的 *DNS Security* 和 *Advanced DNS Security* 许可证的条目。在这种情况下，*DNS Security* 许可证是被动条目，将通过 *Advanced DNS* 许可证授予所有 *DNS Security* 和 *Advanced DNS Security* 功能，包括相关的到期日期。以前没有安装 *DNS Security* 许可证的防火墙会显示 *Advanced DNS Security* 许可证，但是，它同时提供 *DNS Security* 和 *Advanced DNS Security* 功能。

因此，如果您从运行 *Advanced DNS Security* 许可证的 *PAN-OS* 版本降级为不支持 *Advanced DNS Security* 的版本，防火墙将继续通过 *Advanced DNS Security* 许可证显示和授予 *DNS Security* 功能，但是，它仅限于基本的 *DNS Security* 功能。

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。



STEP 4 | 更新或创建新的反间谍软件安全配置文件以启用实时 Advanced DNS Security 查询。通常，这是您现有的用于 DNS Security 配置的反间谍软件安全配置文件。



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，导航路径为 **Objects**（对象） > **Security Profiles**（安全配置文件） > **Anti-Spyware**。
2. 选择您的反间谍软件安全配置文件，然后转到 **DNS Policies**（**DNS** 策略）。
3. 对于每个 Advanced DNS Security 域类别，指定使用相应的分析引擎检测到域类型时要采取的 **Log Severity**（日志严重性）和 **Policy Action**（策略操作）。目前有两个可用的分析引擎：**DNS Misconfiguration Domains**（**DNS** 错误配置域）和 **Hijacking Domains**（劫持域）。

   策略操作选项：

   - **Allow**（允许）— 允许 DNS 查询。

     您可以将防火墙配置为在检测到适用的域类型时生成警报，方法是将操作设置为允许，将日志严重性设置为参考。

   - **Block**（阻止）— 阻止 DNS 查询。
   - **Sinkhole** — 针对检测到的恶意域为 DNS 查询伪造 DNS 响应。这会将恶意域名的解析定向到一个特定的 IP 地址（称为 Sinkhole IP），该地址作为响应嵌入。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。

日志严重性选项：

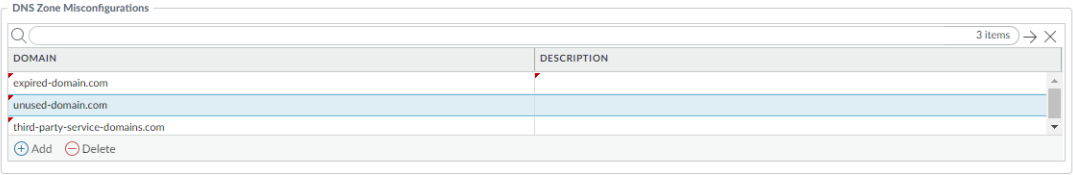
- **None**（无）— 事件没有关联的日志严重级别。
- **Low**（低） — 警告级别的威胁，对组织的基础设施的影响非常小。它们通常需要本地或物理系统访问权限，并且可能经常会导致受害者隐私或 DoS 问题及信息遭到泄漏。
- **Informational**（参考） — 不会立即构成威胁，但是会报告，以提醒相关人员注意可能存在更深层次问题的可疑事件。
- **Medium**（中等） — 影响力最低的小威胁，例如不会危害目标的 DoS 攻击或如下攻击：需要攻击者与受害者驻留在同一 LAN 中，仅会影响非标准配置或不知名应用程序，或者提供的访问权限有限。
- **High**（高）— 能够演变为关键威胁，但有抑制因素的威胁；例如，可能难以利用，不会导致攻击者的权限得到提升，或者受害者群体不会很大。
- **Critical**（严重）— 严重威胁，如对广泛部署的软件的默认安装产生影响的威胁，这些威胁会导致服务器的超级用户权限被窃取，使得攻击者有机会广泛窃用漏洞利用代码。攻击者通常不需要任何特别的身份验证凭据，或者无需知道各个受害人，也不需要操纵目标，即可执行所有特定功能。

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

STEP 5 | （可选）指定您的组织内任何面向公共的父域，您希望 Advanced DNS Security 分析并监视其中是否存在错误配置的域。错误配置的域是由域所有者无意中造成的，他们使用

CNAME、MX、NS 记录类型将别名记录指向第三方域，并使用不再有效的条目，使得攻击者能够通过注册过期或未使用的域来接管原来的域。

TLD（顶级域）和根级域无法添加到 *DNS* 区域错误配置列表中。



1. 选择反间谍软件安全配置文件，导航路径为 **Objects**（对象） > **Security Profiles**（安全配置文件） > **Anti-Spyware**，然后转到 **DNS Policies**（**DNS** 策略）。
2. 在 **DNS Zone Misconfigurations**（**DNS** 区域错误配置）部分，添加面向公众的父域，并添加可选说明，以帮助您识别组织内的域使用情况或所有权。

   条目必须按以下格式（例如 *paloaltonetworks.com*）在域中包含一个“.”，否则会被解析为主机名，而主机名会被视为私有域。
3. 单击 **OK**（确定）以退出防间谍软件安全配置文件的配置对话框，然后 **Commit**（提交）更改。

STEP 6 | （可选）配置 Advanced DNS 签名查找超时设置的最大值。如果超过该值，DNS 响应会通过，而不使用 Advanced DNS Security 进行分析。

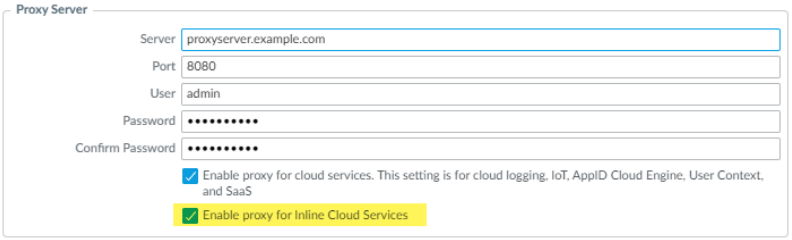
STEP 7 | （可选 [如果您没有最新的设备证书]）安装用于向 Advanced Threat Prevention 内联云分析服务进行身份验证的更新防火墙设备证书。对为内联云分析启用的所有防火墙重复此操作。

如果您已经在 IoT Security、Device Telemetry、Advanced Threat Prevention 或 Advanced URL Filtering 初始设置过程中安装更新的防火墙设备证书，则无需执行此步骤。

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）。

STEP 9 | （可选） 验证防火墙与 Advanced DNS Security 云服务的连接状态。

STEP 10 | （可选）监视防火墙上使用 Advanced DNS Security 检测到的 DNS 查询的活动。使用 Advanced DNS Security 实时分析 DNS 响应数据包分析的 DNS Security 类别具有前缀“adns”，后跟类别。例如，adns-dnsmisconfig，其中“dnsmisconfig”表示支持的 DNS 类别类型。如果 DNS 域类别是通过分析 DNS 请求数据包确定的，则会显示指定的类别，前缀为“DNS”，后跟类别。例如，“dns-grayware”。

1. 访问 Advanced DNS Security 测试域，以验证是否针对给定威胁类型实施了策略操作。
2. 选择 **Monitor**（监控）> **Logs**（日志）> **Threat**（威胁）。您可以根据特定类型的 Advanced DNS Security 域类别过滤日志，例如 `(category-of-threatid eq adns-hijacking)`，其中变量 `adns- hijack` 表示已被 Advanced DNS Security 归类为恶意 DNS 劫持尝试的 DNS 查询。日志中提供以下 Advanced DNS Security 威胁类别：

   Advanced DNS Security 类别

   - **DNS** 劫持 — `adns-hijacking`

     DNS 劫持域的威胁 ID 为（UTID：109,004,100）。

   - **DNS** 错误配置 — `adns-dnsmisconfig`

     DNS 错误配置域有三个威胁 ID，它们对应于 DNS 错误配置域类型的三种变体：dnsmisconfig_zone（UTID：109,004,200）、dnsmisconfig_zone_dangling（UTID：109,004,201）和 dnsmisconfig_claimable_nx（UTID：109,004,202）。您可以通过交叉引用对应于特

定 DNS 错误配置域类型的 Threat-ID 值来约束搜索。例如 (category-of-threatid eq adns-dnsmisconfig) 和 (threatid eq 109004200)，其中 109004200 表示由于 DNS 服务器配置问题而没有将流量路由到活动域的 DNS 错误配置域的威胁 ID。

使用 Advanced DNS Security 增强响应分析来分析的 DNS 类别。

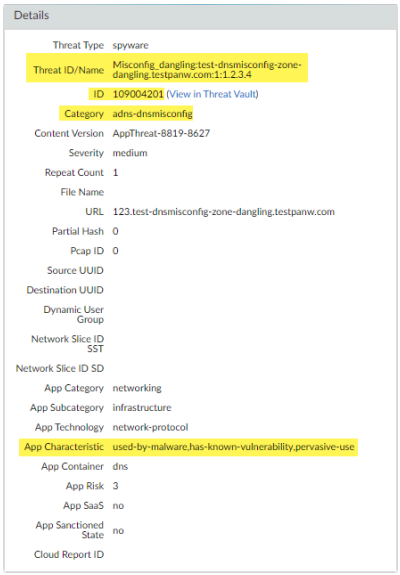
> 您必须运行使用 *PAN-OS 11.2* 或更高版本的防火墙，才能利用增强的 *Advanced DNS Security* 实时分析。

- **DNS** — `adns-benign`
- 恶意软件域 — `adns-malware`
- 命令和控制域 — `adns-c2`
- 网络钓鱼域 — `adns-phishing`
- 动态 **DNS** 托管域 — `adns-ddns`
- 新注册域 — `adns-new-domain`
- 灰色软件域 — `adns-grayware`
- 寄放域 — `adns-parked`
- 代理规避和匿名程序 — `adns-proxy`
- 广告跟踪域 — `adns-proxy`

> 如果 *DNS* 查询在 *Advanced DNS Security* 的指定超时期限内未完成，将尽可能使用 *DNS Security* 分类。在这些情况下，使用类别的传统表示法，例如，它将被归类为 *`dns-malware`*，而不是 *`adns-malware`*，表明使用了 *DNS Security* 分类值。

3. 选择一个日志条目以查看 DNS 查询的详细信息。
4. DNS **Category**（类别）显示在详细日志视图的 **Details**（详细信息）窗格中。此外，您还可以看到威胁的其他方面，包括威胁 ID，其中包括源域、特定威胁类别和其他相关特征，以及关联的 Q 类型，以及使用以下格式的 R 数

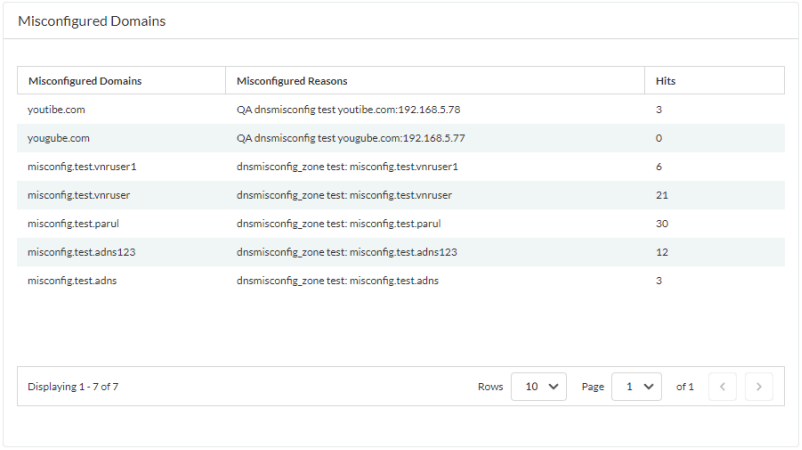
据：hijacking:<FQDN>:<QTYPE>:<RDATA>，其中 <QTYPE> 表示 DNS 资源记录类型，<RDATA> 表示被劫持的 IP 地址。



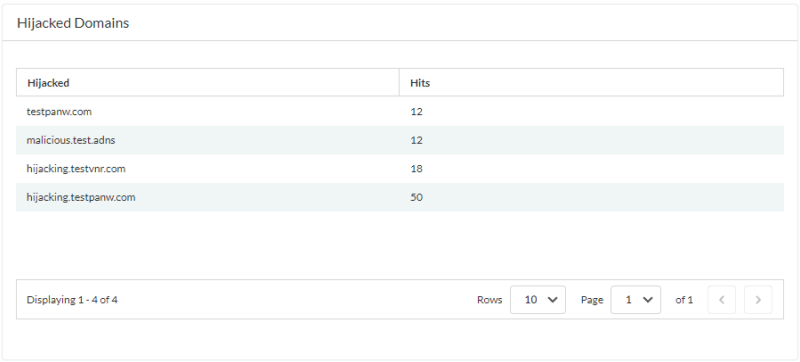
STEP 11 | （可选）检索 Advanced DNS Security 服务检测到的错误配置域和被劫持域的列表。配置错误的域基于添加到 **DNS Zone Misconfigurations**（**DNS** 区域错误配置）的面向公众的父级域条目。

从网络中删除的错误配置的域条目不会立即反映在 *Advanced DNS Security* 指示板的统计信息中。

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。
2. 选择 **Dashboards**（指示板） > **More Dashboards**（更多指示板） > **DNS Security**，以便打开 DNS Security 指示板。
3. 从 DNS Security 指示板中，参考以下小部件：
   - **Misconfigured Domains**（配置错误的域）— 查看与用户指定的面向公众的父级域关联的不可解析域列表。对于每个条目，都有一个错误配置原因和基于源 IP 的流量命中计数。



   - **Hijacked Domains**（被劫持的域）— 查看由 Advanced DNS Security 确定的被劫持域列表。对于每个条目，都有一个分类原因和基于源 IP 的流量命中计数。



配置 DNS Security Over TLS

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 DNS Security 许可证（用于增强功能支持）或 DNS Security 许可证 ❑ 高级威胁防护或威胁防护许可证

您可以通过解密加密 DNS 请求中包含的 DNS 有效负载，获得对 TLS 请求的 DNS Security 的可见性和控制能力。然后可以使用包含 DNS 策略设置的安全配置文件配置来处理解密的 DNS 负载。已确定来自 TLS 源的 DNS 请求在威胁日志中的源端口为 853。

- Strata Cloud Manager
- PAN-OS 和 Panorama

配置 DNS Security Over TLS (Strata Cloud Manager)

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 应用程序。

STEP 2 | 启用 DNS Security 已配置为检查 DNS 请求。如果您想对 TLS 流量的 DNS Security 使用相同的 **DNS Policies**（**DNS** 策略）设置，则可以使用现有的安全配置文件。

STEP 3 | 创建一条解密策略规则，该规则包含解密端口 853 上 HTTPS 流量的操作，其中包括 DNS Security over TLS 流量（有关更多信息，请参阅解密最佳实践）。当 DNS Security over TLS 浏览量已解密时，日志中生成的 DNS 请求将显示为常规的 **dns-base** 应用程序。

STEP 4 | （可选）在防火墙上搜索活动，查找已使用 DNS Security 处理的已解密 TLS 加密 DNS 查询。

1. 选择 **Activity**（活动）> **Log Viewer**（日志查看器），然后选择 **Threat**（威胁）日志。使用查询生成器根据使用 **dns-base** 和端口 853（专用于 DNS Security over TLS 事务）的应用程序进行过滤，例如，`app = 'dns-base' AND source_port = 853`。
2. 选择日志条目以查看检测到的 DNS 威胁的详细信息。
3. **Application**（应用程序）应在日志详细信息视图的 **General**（常规）窗格中显示 **dns-base**，并在 **Source**（源）窗格中显示 **Port**（端口）。有关威胁的其他相关详细信息显示在相应的选项卡中。

配置 DNS Security Over TLS (NGFW (Managed by PAN-OS or Panorama))

STEP 1 | 登录 NGFW。

STEP 2 | 启用 DNS Security 已配置为检查 DNS 请求。如果您想对 TLS 流量的 DNS Security 使用相同的 **DNS Policies**（**DNS** 策略）设置，则可以使用现有的安全配置文件。

STEP 3 | 创建解密策略规则（类似于以下示例），该规则包含对端口 853 上的 HTTPS 流量进行解密的操作，其中包括基于 TLS 流量的 DNS Security（有关更多信息，请参阅解密最佳实践）。对 DNS Security over TLS 流量解密时，日志中生成的 DNS 请求将显示为 **DNS-Base**（基于 **TLS**）的常规应用程序。

		Source				Destination					Decrypt Options					
	NAME	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	URL CATEGORY	SERVICE	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSSL HAN
1	Decrypt Port 853	any	any	any	any	any	any	any	any	Port 853	decrypt	ssl-forward-proxy	default	none	false	true

STEP 4 | （可选）在防火墙上搜索活动，查找已使用 DNS Security 处理的已解密 TLS 加密 DNS 查询。

1. 选择 **Monitor**（监控）> **Logs**（日志）> **Traffic**（流量），然后使用 **dns-base** 和端口 853（专门用于 DNS Security over TLS 事务）根据应用程序进行过滤，例如，`(app eq dns-base)` 和 `(port.src eq 853)`。
2. 选择日志条目以查看检测到的 DNS 威胁的详细信息。
3. **Application**（应用程序）应在日志详细信息视图的 **General**（常规）窗格中显示 **dns-base**，并在 **Source**（源）窗格中显示 **Port**（端口）。有关威胁的其他相关详细信息显示在相应的窗口中。

配置 DNS Security Over DoH

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 DNS Security 许可证（用于增强功能支持）或 DNS Security 许可证 ❑ 高级威胁防护或威胁防护许可证

您可以使用 HTTPS (DoH—[DNS-over-HTTPS]) 对加密 DNS 流量请求中包含的 DNS 负载进行分析和分类。如果您的组织当前按照 Palo Alto Networks 的建议阻止所有 DoH 请求，则可以脱离该策略，因为 DNS Security 现在允许您从加密请求中提取 DNS 主机名并应用组织的现有 DNS Security 策略。随着对 DoH 支持的范围不断扩大，这可以让您安全地访问更多网站。通过配置防火墙来解密源自用户指定的 DNS 解析器列表的 DNS 请求的有效负载，从而启用对 DoH 的 DNS Security 支持，从而提供对一系列服务器选项的支持。然后，您可以使用包含 DNS 策略配置的反间谍软件配置文件配置来处理解密的 DNS 负载。已确定为 DoH 的 DNS 请求在流量日志中标记为 **dns-over-https**。

- Strata Cloud Manager
- PAN-OS 11.0 及更高版本

配置 DNS Security Over DoH (Strata Cloud Manager)

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。

STEP 2 | 创建自定义 URL 类别列表，其中包括您要启用流入/传出流量的所有 DoH 解析器（您需要 DNS 服务器 URL）。

STEP 3 | 创建一条解密策略规则，该规则引用您在上一步中创建的自定义 URL 类别列表。

STEP 4 | 更新或创建用于检查 DoH 请求的新防间谍软件安全配置文件。

STEP 5 | 创建或更新安全策略规则，并引用 DNS Security 配置文件和自定义 URL 类别列表（**Manage**（管理） > **Configuration**（配置） > **PAN-OS** 和 **Prisma Access** > **Security Services**（安全服务） > **URL Access Management**（**URL** 访问管理）），其中包含 DoH 服务器的已批准列表。

STEP 6 | 通过使用 App-ID: **dns-over-https** 和以下 URL 类别：**encrypted-dns**，创建对解密 HTTPS 流量的阻止策略，并阻止自定义 URL 类别列表（在第 5 步中引用）未明确允许的所有剩余未经批准的 DoH 流量。

如果您已经有阻止 *DoH* 流量的现有阻止策略，请验证该规则是否位于先前的安全策略规则下，后者用于匹配自定义 *URL* 类别列表对象中列出的特定 *DoH* 解析器。

STEP 7 | （可选）在防火墙上搜索已使用 DNS Security 处理的 HTTPS 加密 DNS 查询的活动。

1. 选择 **Activity**（活动） > **Logs**（日志） > **Log Viewer**（日志查看器），然后选择 **Threat**（威胁）。
2. 使用 **dns-over-https** 提交基于应用程序的日志查询，例如 `app = 'dns-over-https'`。
3. 选择日志条目以查看检测到的使用 DoH 的 DNS 威胁的详细信息。
4. 威胁 **Application**（应用程序）将显示在详细日志视图的 **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。

配置 DNS Security Over DoH（PAN-OS 11.0 及更高版本）

STEP 1 | 登录 PAN-OS Web 界面。

STEP 2 | 创建自定义 URL 类别列表，其中包括您要启用流入/传出流量的所有 DoH 解析器（您需要 DNS 服务器 URL）。

STEP 3 | 创建一条解密策略规则，该规则引用您在上一步中创建的自定义 URL 类别列表。

STEP 4 | 更新或创建用于检查 DoH 请求的新防间谍软件安全配置文件。

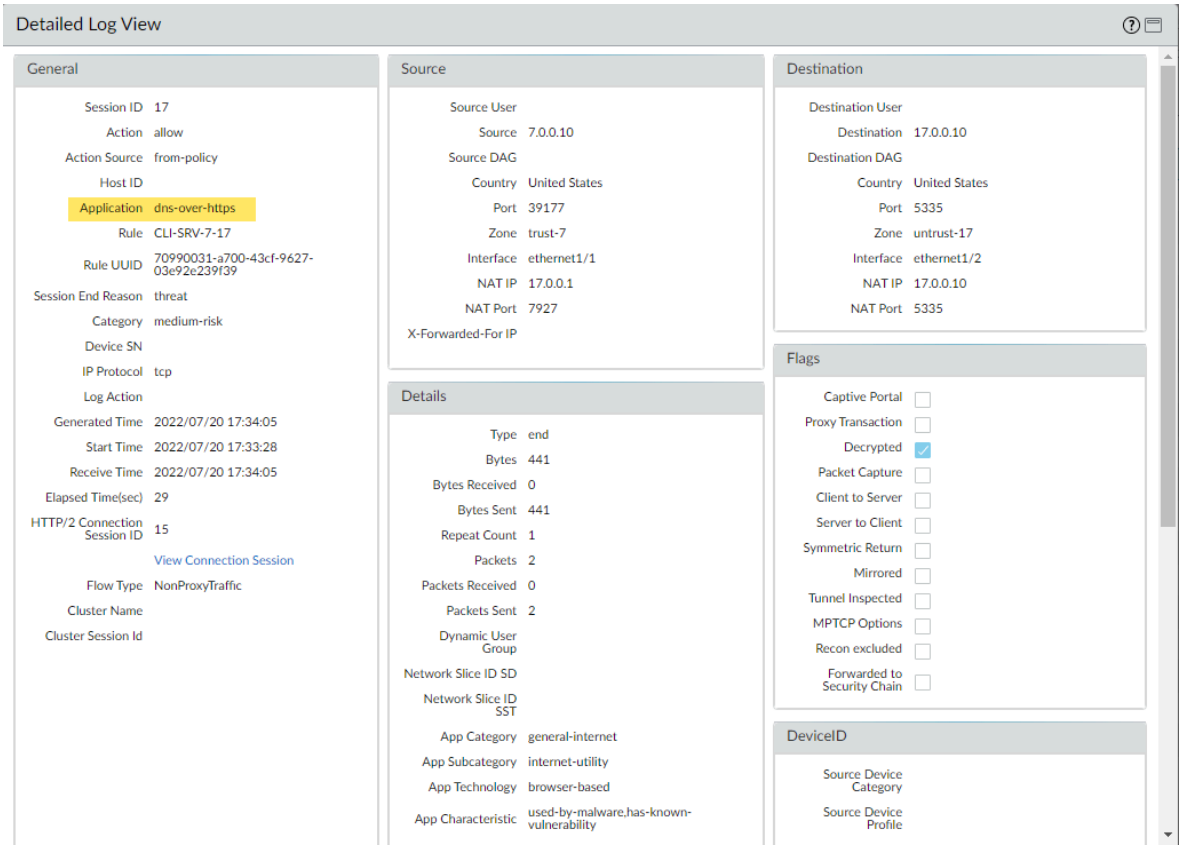
STEP 5 | 创建或更新安全策略规则，并引用反间谍软件配置文件和包含已批准 DoH 服务器列表的自定义 URL 类别列表（**Objects**（对象） > **Custom Objects**（自定义对象） > **URL Category**（**URL** 类别））。

STEP 6 | 通过使用 App-ID: **dns-over-https** 和以下 URL 类别：**encrypted-dns**，创建对解密 HTTPS 流量的阻止策略，并阻止自定义 URL 类别列表（在第 5 步中引用）未明确允许的所有剩余未经批准的 DoH 流量。

如果您已经有阻止 *DoH* 流量的现有阻止策略，请验证该规则是否位于先前的安全策略规则下，后者用于匹配自定义 *URL* 类别列表对象中列出的特定 *DoH* 解析器。

STEP 7 | （可选）在防火墙上搜索已使用 DNS Security 处理的 HTTPS 加密 DNS 查询的活动。

1. 选择 **Monitor**（监控） > **Logs**（日志） > **Traffic**（流量），并使用 **dns-over-https** 根据应用程序进行筛选，例如 `(app eq dns-over-https)`。
2. 选择日志条目以查看检测到的 DNS 威胁的详细信息。
3. **Application**（应用程序）应在详细日志视图的 **General**（常规）窗格中显示 dns-over-https，表明这是使用 DNS Security 处理的 DoH 流量。有关威胁的其他相关详细信息显示在相应的窗口中。



创建域例外和允许 | 阻止列表

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 DNS Security 许可证（用于增强功能支持）或 DNS Security 许可证 ❑ 高级威胁防护或威胁防护许可证

DNS Security 将为已由 DNS Security 服务分析的域创建威胁签名。对于这些已知域，收到 DNS 查询时会引用签名。在某些情况下，由于域中存在某些特征或域的质量问题，签名可能会错误地将域归类为威胁。在这种情况下，您可以添加签名例外来绕过这些误报。如果存在被归类为恶意的已知安全域（例如内部域），您可以添加将绕过任何 DNS 分析的域列表。如果您的组织使用第三方威胁源作为综合威胁情报解决方案的一部分，则还可以在 DNS Security 配置文件中以外部动态列表 (EDL) 的形式引用这些源。

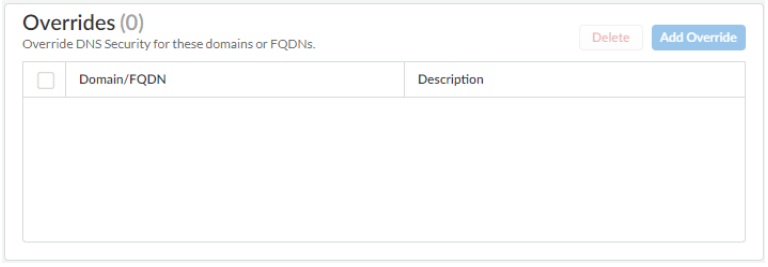
- Strata Cloud Manager
- PAN-OS 和 Panorama

创建域例外和允许 | 阻止列表 (Strata Cloud Manager）

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。

STEP 2 | 在出现误报的情况下添加域覆盖。

1. 选择 **Manage**（管理） > **Configuration**（配置） > **NGFW** 和 **Prisma Access** > **Security Services**（安全服务） > **DNS Security**，并选择要修改的 DNS Security 配置文件。
2. **Add Override**（添加覆盖）或 **Delete**（删除）以根据需要修改域列表条目。每个附加条目都需要域和描述。



3. 单击 **OK**（确定）以保存修改的 DNS Security 配置文件。

STEP 3 | 引用外部动态列表 (EDL) 作为 DNS Security 配置文件的一部分，以导入第三方威胁源。

1. 创建基于域的外部动态列表（**Manage**（管理） > **Configuration**（配置） > **NGFW** 和 **Prisma Access** > **Objects**（对象） > **External Dynamic Lists**（外部动态列表））。有关 EDL 的更多信息，请参阅外部动态列表。
2. 选择 **Manage**（管理） > **Configuration**（配置） > **NGFW** 和 **Prisma Access** > **Security Services**（安全服务） > **DNS Security**。
3. 在 **External Dynamic Lists**（外部动态列表）面板中，选择域列表 EDL 并提供 **Policy Action**（策略操作）和 **Packet Capture**（数据包捕获）设置。在 **Apply to Profiles**（应用到配置文件）中，选择您想要应用 EDL 域列表的 DNS Security 配置文件。
4. 完成更新后，**Save**（保存）更改。

创建域例外和允许 | 阻止列表 (NGFW (Managed by PAN-OS or Panorama)）

PAN-OS 10.0 及更高版本提供了附加选项，可以通过反间谍软件安全配置文件明确添加允许的域。如果已批准的域来源触发 DNS Security 的误报响应，您可以添加域/FQDN 条目。

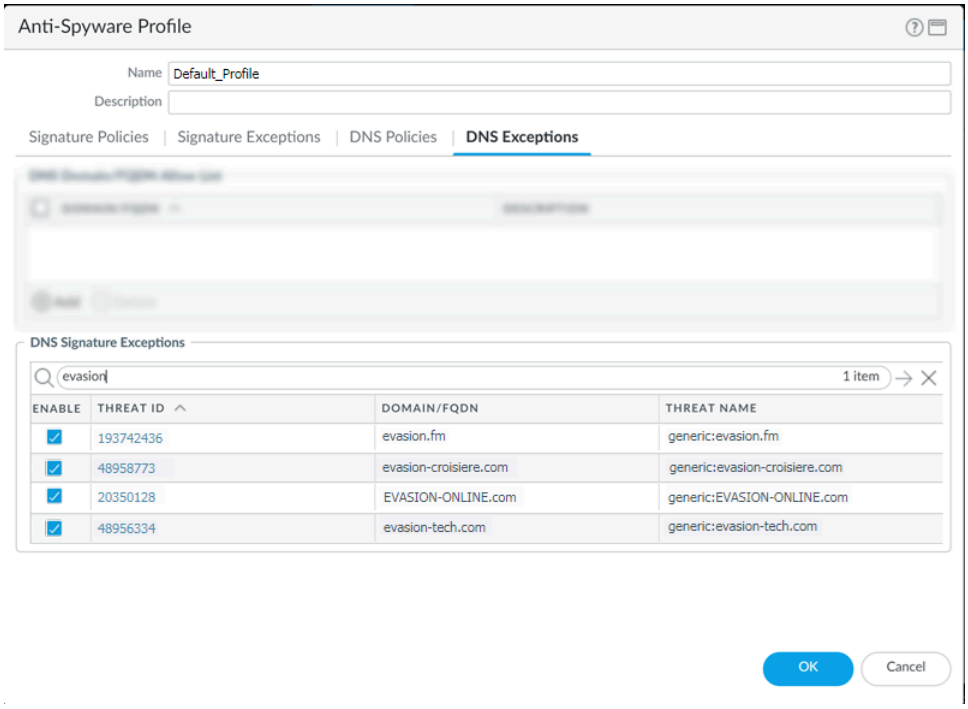
- PAN-OS 10.0 及更高版本
- PAN-OS 9.1

创建域缓存和允许 | 阻止列表（**PAN-OS 10.0** 及更高版本）

登录 NGFW。

（可选）在发生误报时添加域签名例外。

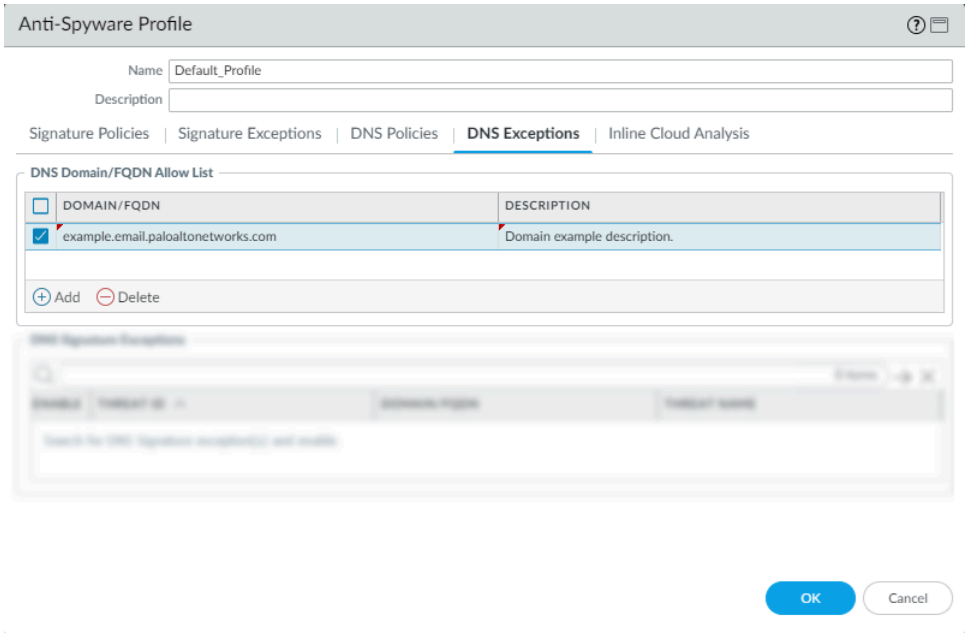
1. 选择 **Objects**（对象） > **Security Profiles**（安全配置文件） > **Anti-Spyware**（防间谍软件）。
2. 选择要修改的配置文件。
3. **Add**（添加）或修改要从中排除威胁签名的防间谍软件配置文件，然后选择 **DNS Exceptions**（**DNS** 例外）。
4. 通过输入名称或 FQDN 搜索要排除的 DNS 签名。
5. 选中要从执行中排除的 DNS 签名的各 **Threat ID**（威胁 **ID**）复选框。



6. 单击 **OK**（确定）以保存新的或修改过的反间谍软件配置文件。

添加允许列表以指定要明确允许的 DNS 域/FQDN 的列表。

1. 选择 **Objects**（对象） > **Security Profiles**（安全配置文件） > **Anti-Spyware**（防间谍软件）。
2. 选择要修改的配置文件。
3. **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）。
4. 要 **Add**（添加）新的 FQDN 允许列表条目，请提供 DNS 域或 FQDN 位置和说明。



5. 单击 **OK**（确定）以保存新的或修改过的反间谍软件配置文件。

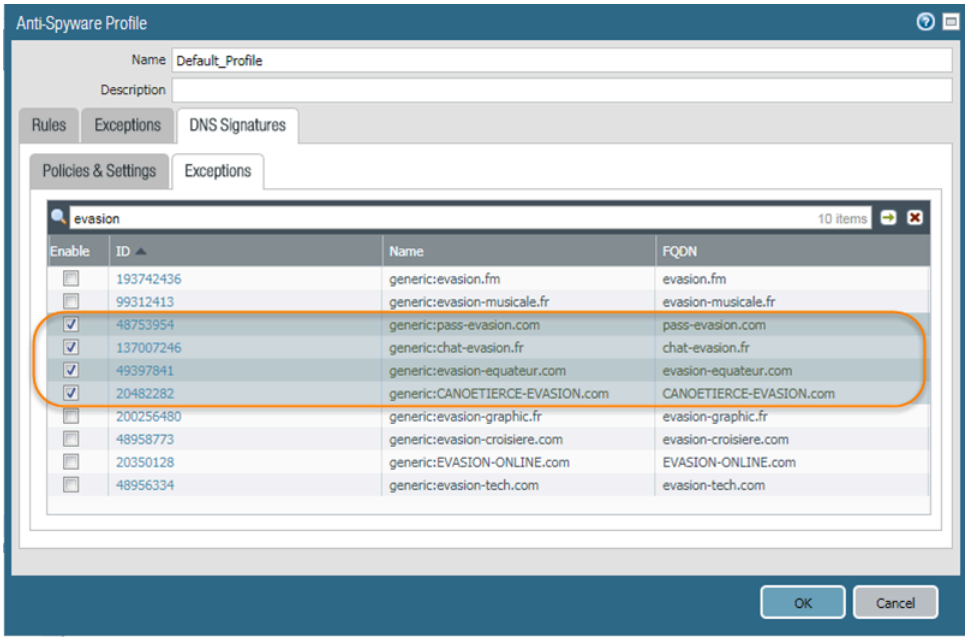
创建域缓存和允许 | 阻止列表 (PAN-OS 9.1)

PAN-OS 9.1 中不提供允许和阻止列表。

登录 NGFW。

（可选）在发生误报时添加域签名例外。

1. 选择 **Objects**（对象） > **Security Profiles**（安全配置文件） > **Anti-Spyware**（防间谍软件）。
2. 选择要修改的配置文件。
3. **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 Signatures > Exceptions**（**DNS** 签名 > 例外）。
4. 通过输入名称或 FQDN 搜索要排除的 DNS 签名。
5. 选择要从执行中排除的 DNS 签名的 **DNS Threat ID**（**DNS** 威胁 **ID**）。



6. 单击 **OK**（确定）以保存新的或修改过的反间谍软件配置文件。

测试域

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 DNS Security 许可证（用于增强功能支持）或 DNS Security 许可证 ❑ 高级威胁防护或威胁防护许可证

Palo Alto Networks 提供以下 DNS Security 测试域，以根据 DNS 类别验证您的策略配置。

STEP 1 | 访问以下测试域，以验证是否针对给定威胁类型实施了策略操作：

DNS Security

- C2 — test-c2.testpanw.com
- DNS 隧道 — test-dnstun.testpanw.com
- DGA — test-dga.testpanw.com
- 动态 DNS* — test-ddns.testpanw.com
- 恶意软件 — test-malware.testpanw.com
- 新注册域* — test-nrd.testpanw.com
- 网络钓鱼* — test-phishing.testpanw.com
- 灰色软件* — test-grayware.testpanw.com
- 寄放域* — test-parked.testpanw.com
- 代理规避和匿名程序* — test-proxy.testpanw.com
- Fast Flux* — test-fastflux.testpanw.com
- 恶意 NRD* — test-malicious-nrd.testpanw.com
- NXNS 攻击* — test-nxns.testpanw.com
- Dangling* — test-dangling-domain.testpanw.com
- DNS 重新绑定* — test-dns-rebinding.testpanw.com
- DNS 渗透* — test-dns-infiltration.testpanw.com
- 通配符滥用* — test-wildcard-abuse.testpanw.com
- 策略性过期* — test-strategicly-aged.testpanw.com
- 被入侵的 DNS* — test-compromised-dns.testpanw.com
- 广告跟踪* — test-adtracking.testpanw.com
- CNAME 隐藏* — test-cname-cloaking.testpanw.com
- 勒索软件* — test-ransomware.testpanw.com
- Stockpile * — test-stockpile-domain.testpanw.com
- 域名抢注* — test-squatting.testpanw.com
- 子域名信誉* — test-subdomain-reputation.testpanw.com

PAN-OS 9.1 中不支持带有 * 的测试域。

Advanced DNS Security

访问以下测试域，以验证是否针对给定威胁类型实施策略操作：

- **DNS** 错误配置域（可声明）— http://test-dnsmisconfig-claimable-nx.testpanw.com

在访问域之前，应将以下测试域测试用例添加到 testpanw.com 的 DNS 服务器区域文件中。这些测试用例与 Advanced DNS Security 签名匹配，并将生成相应的日志。验证针对给定威胁类型的策略操作是否正在执行。

表 **1: DNS** 错误配置域（区域无关联）测试用例

主机	记录类型	记录数据
*.test-dnsmisconfig-zone-dangling.testpanw.com	A	1.2.3.4

表 **2:** 劫持域测试用例

主机	记录类型	记录数据
test-ipv4.hijacking.testpanw.com	A	1.2.3.5
*.test-ipv4-wildcard.hijacking.testpanw.com	A	1.2.3.6
test-ipv6.hijacking.testpanw.com	AAAA	2607:f8b0:4005:80d::2005
test-cname-rrname.hijacking.testpanw.com	CNAME	1.test-cname-wc.hijacking.testpanw.com
test-cname-rrname-wc.hijacking.testpanw.com	CNAME	1.test-cname-wildcard-1.hijacking.testpanw.com
*.test-cname-rrname-sub-wc.hijacking.testpanw.com	CNAME	2.test-cname-wc.hijacking.testpanw.com
test-ns-rrname.hijacking.testpanw.com	NS	test-ns.hijacking.testpanw.com
test-ns-rrname-rdata-wc.hijacking.testpanw.com	NS	1.test-ns-wc.hijacking.testpanw.com
1.test-ns-rrname-sub-wc.hijacking.testpanw.com	NS	test-ns.hijacking.testpanw.com
test-rrname-wc.hijacking.testpanw.com	NS	test-ns-2.hijacking.testpanw.com

对于 *NS* 记录，必须使用以下选项： ***“dig +trace NS”***

STEP 2 | 通过监视活动验证 DNS 查询请求是否已由 DNS Security 处理。

测试与 DNS Security 云服务的连接

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

DNS Security

验证您的防火墙与 DNS Security 服务的连接。如果无法访问该服务，请验证以下域是否被阻止：dns.service.paloaltonetworks.com。

STEP 1 | 访问防火墙 CLI。

STEP 2 | 使用以下 CLI 命令验证您的防火墙与 DNS Security 服务的连接可用性。

```
show dns-proxy dns-signature info
```

例如：

```
show dns-proxy dns-signture info Cloud URL:
 dns.service.paloaltonetworks.com:443 Telemetry URL:
 io.dns.service.paloaltonetworks.com:443 Last Result:None Last
 Server Address:Parameter Exchange:Interval 300 sec Allow List
 Refresh:Interval 43200 sec Request Waiting Transmission:0 Request
 Pending Response:0 Cache Size:0
```

如果您的防火墙与 DNS Security 服务建立了有效连接，则服务器详细信息将显示在响应输出中。

STEP 3 | 检索指定域的事务详细信息，例如延迟、TTL 和签名类别。

在防火墙上使用以下 CLI 命令查看有关域的详细信息：

```
test dns-proxy dns-signature fqdn
```

例如：

```
test dns-proxy dns-signature fqdn www.yahoo.com DNS
 Signature Query [ www.yahoo.com ] Completed in 178 ms
 DNS Signature Response Entries:2 Domain Category GTID TTL
```

```
 ----------------------------------------------------------------------------
 *.yahoo.com Benign 0 86400 www.yahoo.com Benign 0 3600
```

Advanced DNS Security

验证您的防火墙与 Advanced DNS Security 服务的连接。如果您无法访问该服务，请确认以下域名未被阻止：adv-dns.service.paloaltonetworks.com。如果您手动配置区域 Advanced DNS Security 服务器，则可能需要验证特定的区域域名也已解除阻止。

验证防火墙与 Advanced DNS Security 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 ADNS(1)
 Current cloud server: qa.adv-dns.service.paloaltonetworks.com:443
 Cloud connection: connected Config:Number of gRPC connections:2,
 Number of workers:8 Debug level:2, Insecure connection: false,
 Cert valid: true, Key valid: true, CA count:306 Maximum number
 of workers:12 Maximum number of sessions a worker should process
 before reconnect:10240 Maximum number of messages per worker:0
 Skip cert verify: false Grpc Connection Status:State Ready
 (3), last err rpc error: code = Unavailable desc = unexpected
 HTTP status code received from server:502 (Bad Gateway);
 transport: received unexpected content-type "text/html" Pool
 state:Ready (2) last update:2024-01-24 11:15:00.549591469
 -0800 PST m=+1197474.129493596 last connection retry:2024-01-23
 00:03:09.093756623 -0800 PST m=+1070762.673658768 last pool
 close:2024-01-22 14:15:50.36062031 -0800 PST m=+1035523.940522446
 Security Client AdnsTelemetry(2) Current cloud server: io-qa.adv-
dns.service.paloaltonetworks.com:443 Cloud connection: connected
 Config:Number of gRPC connections:2, Number of workers:8 Debug
 level:2, Insecure connection: false, Cert valid: true, Key valid:
 true, CA count:306 Maximum number of workers:12 Maximum number of
 sessions a worker should process before reconnect:10240 Maximum
 number of messages per worker:0 Skip cert verify: false Grpc
 Connection Status:State Ready (3), last err rpc error: code
 = Internal desc = stream terminated by RST_STREAM with error
 code:PROTOCOL_ERROR Pool state:Ready (2) last update:2024-01-24
 11:25:58.340198656 -0800 PST m=+1198131.920100772 last connection
 retry:2024-01-23 00:03:36.78141425 -0800 PST m=+1070790.361316421
 last pool close:2024-01-22 14:24:26.954340157 -0800 PST m=
+1036040.534242289 ...
```

验证 `Security Client AdnsTelemetry(2)` 和 `Security Client ADNS(1)` 的云连接状态是否显示活动连接。

为简洁起见，上述 *CLI* 输出进行了截短。

如果您无法连接到 Advanced DNS Security 云服务，请确认高级 DNS 服务器未被阻止：dns.service.paloaltonetworks.com。

配置查找超时

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

DNS Security

如果防火墙因连接问题无法在指定时间内检索到签名裁决，则包含所有后续 DNS 响应在内的请求都将通过。您可以通过检查平均延迟时间来验证这些请求是否都在配置时段内。如果平均延迟时间超出配置时段，请考虑更新设置，设置一个比平均延迟时间更大的值，从而阻止请求超时。

STEP 1 | 在 CLI 中，发出以下命令以查看平均延迟时间。

```
show dns-proxy dns-signature counters
```

默认超时为 100 毫秒。

STEP 2 | 向下滚动输出到签名请求 API 标题下的延迟部分，验证平均延迟时间是否在定义的超时时段内。此延迟时间表示 DNS Security 服务检索签名裁决所花费的平均时间量。关于各延迟时段的其他延迟统计数据可能低于平均值。

```
Signature query API: . . . [latency ] : max 1870 (ms) min 16(ms)
 avg 27(ms) 50 or less :47246 100 or less :113 200 or less :25 400
 or less :15 else :21
```

STEP 3 | 如果平均延迟时间一律高于默认超时值，您可以增加设置，使请求位于规定时段内。选择 **Device**（设置）> **Content-ID**，并更新 **Realtime Signature Lookup**（实时签名查询）设置。

STEP 4 | 提交更改。

Advanced DNS Security

STEP 1 | 使用以下调试 CLI 命令查看 Advanced DNS Security 请求的往返时间记录（以毫秒为单位）。它们分布在 0ms 到 450ms 的延迟范围内。您可以使用它来确定 NGFW 理想的最大延迟设置。

```
admin@PA-VM debug dataplane show ctd feature-forward stats
```

在响应输出中，导航到 `PAN_CTDF_DETECT_SERVICE_ADNS` 部分。

```
PAN_CTDF_DETECT_SERVICE_ADNS cli_timeout:1 req_total:2
 req_timed_out:0 Hold: adns rtt>=0ms:0 adns rtt>=50ms:2 adns
 rtt>=100ms:0 adns rtt>=150ms:0 adns rtt>=200ms:0 adns rtt>=250ms:0
 adns rtt>=300ms:0 adns rtt>=350ms:0 adns rtt>=400ms:0 adns
 rtt>=450ms:0
```

STEP 2 | 配置 Advanced DNS 签名的查找超时设置最大值。如果超过该值，DNS 响应会通过，而不使用 Advanced DNS Security 进行分析。仍应用通过定期内容更新传递的 DNS 签名（及其相关策略），或属于配置的 EDL（外部动态列表）或 DNS 例外的 DNS 签名（及其相关策略）。

1. 选择 **Device**（设备） > **Setup**（设置） > **Content-ID** > **Advanced DNS Security**。
2. 指定更新的 Advanced DNS 签名的查找超时设置最大值（毫秒）。默认值为 100ms，这是推荐设置。
3. 单击 **OK**（确定） 以确认您的更改。

或者，您可以使用以下 CLI 命令配置 Advanced DNS Security 超时值。您可以按 100ms 的增量设置 100-15,000ms 范围内的值。默认值为 100ms，这是推荐设置。

```
admin@PA-VM#set deviceconfig setting adns-setting max-latency
 <timeout_value_in_milliseconds>
```

例如：

```
admin@PA-VM# set deviceconfig setting adns-setting max-latency 500
```

您可以使用以下 CLI 命令检查当前超时配置（请参阅输出中的 **max-latency** 条目）。

```
admin@PA-VM show config pushed-template ... }
 deviceconfig { setting { dns { dns-cloud-server dns-
qa.service.paloaltonetworks.com; } adns-setting { max-latency
 100; } } } ...
```

绕过 DNS Security 订阅服务

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	❑ Advanced DNS Security 许可证（用于增强功能支持）或 DNS Security 许可证 ❑ 高级威胁防护或威胁防护许可证

在存在延迟问题或其他网络问题的情况下，可以绕过 DNS Security 查询。

在发生误报的情况下，*Palo Alto Networks* 建议创建特定的例外，而不是绕过 *DNS Security* 查询。

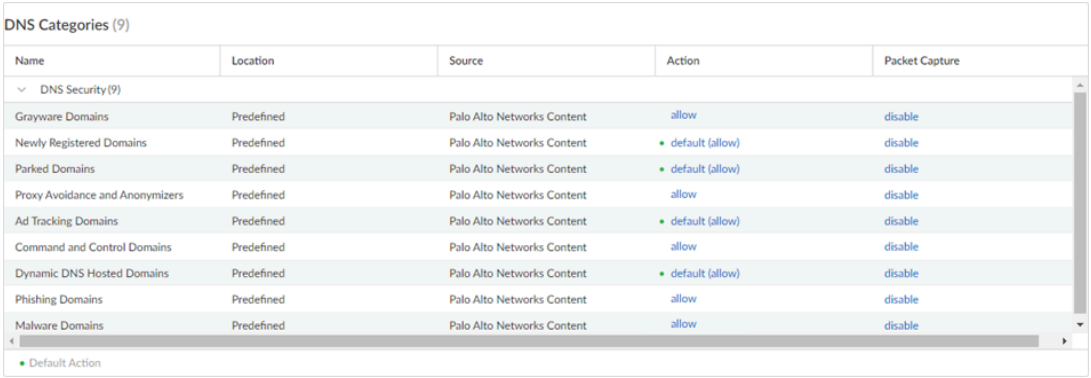
- 云端管理
- PAN-OS 和 Panorama

绕过 DNS Security 订阅服务 (Strata Cloud Manager)

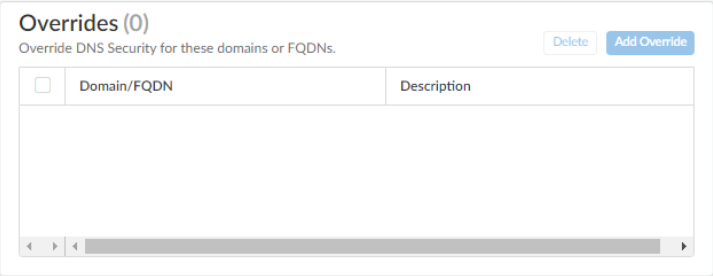
STEP 1 | 使用与 Palo Alto Networks 支持帐户关联的凭据，登录到中心的 Strata Cloud Manager。

STEP 2 | 转到 **Manage**（管理）> **Configuration**（配置）> **NGFW** 和 **Prisma Access** > **Security Services**（安全服务）> **DNS Security**（**DNS** 安全），并选择相关的 DNS Security 配置文件。

STEP 3 | 配置 DNS Security 签名策略设置以绕过 DNS Security 查询。对于每个 DNS 类别，将 **Action**（操作）设置为 **Allow**（允许），将 **Packet Capture**（数据包捕获）设置为 **Disabled**（禁用）。下面，DNS Security 类别已配置为绕过 DNS Security 查询。



STEP 4 | 在 **Overrides**（覆盖）部分，验证是否不存在任何条目；如有必要，请删除所有 **Domain/FQDN**（域/**FQDN**）覆盖。



STEP 5 | 单击 **OK**（确定）以保存 DNS Security 配置文件。

绕过 DNS Security 订阅服务 (NGFW (Managed by PAN-OS or Panorama))

PAN-OS 10.0 及更高版本支持可单独配置的 DNS 签名源，这使您能够为给定签名源定义单独的策略操作以及日志严重性级别。这要求您为每个可用的 DNS 签名源配置策略操作和日志严重性，以绕过 DNS Security。此外，您还必须删除 DNS 例外条目，才能完全绕过 DNS Security。在 PAN-OS 9.1 上，您只需将 Palo Alto Networks DNS Security 的策略操作设置为“允许”操作。

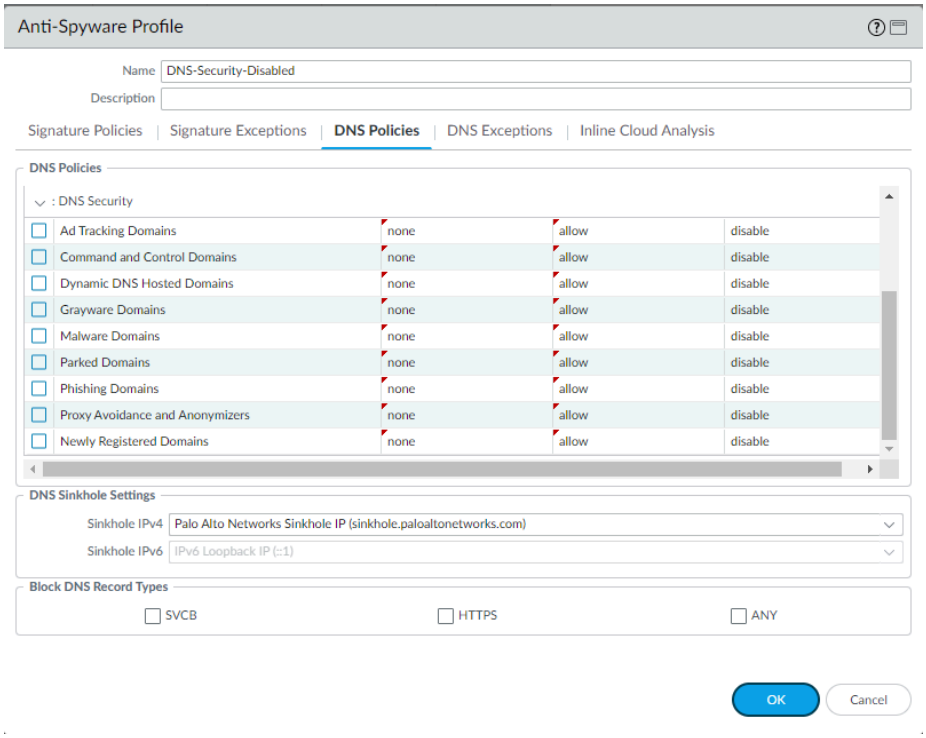
- PAN-OS 10.0 及更高版本
- PAN-OS 9.1

绕过 **DNS Security** 订阅服务（**PAN-OS 10.0** 及更高版本）

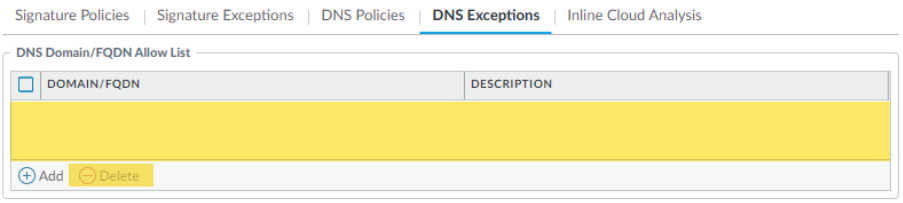
STEP 1 | 登录 NGFW。

STEP 2 | 配置 DNS Security 签名策略设置以绕过 DNS Security 查询。

1. 选择 **Objects**（对象） > **Security Profiles**（安全配置文件） > **Anti-Spyware**（防间谍软件）。
2. 选择包含活动 DNS Security 策略设置的配置文件。
3. 选择 **DNS Policies**（**DNS** 策略）选项卡。
4. 对于每个 DNS 类别，将日志严重性设置为 **None**（无），将策略操作设置为 **Allow**（允许），并将数据包捕获设置为 **Disable**（禁用）。下面，DNS Security 类别已配置为绕过 DNS Security 查询。



STEP 3 | 选择 **DNS Exceptions**（**DNS** 例外）并删除所有 **DNS Domain/FQDN Allow List**（**DNS** 域/**FQDN** 允许列表）条目。



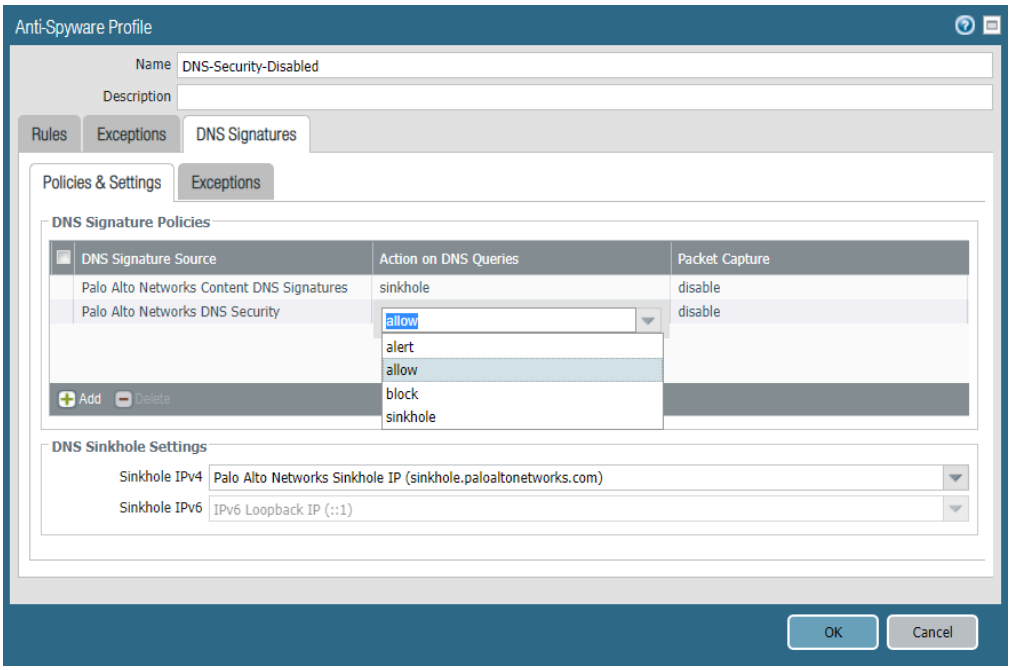
STEP 4 | 单击 **OK**（确定）以保存防间谍软件配置文件。

绕过 DNS Security 订阅服务 (PAN-OS 9.1)

STEP 1 | 登录 NGFW。

STEP 2 | 配置 DNS Security 签名策略设置以绕过 DNS Security 查找。

1. 选择 **Objects**（对象） > **Security Profiles**（安全配置文件） > **Anti-Spyware**（防间谍软件）。
2. 选择包含活动 DNS Security 策略设置的配置文件。
3. 选择 **DNS Signatures**（**DNS** 签名）选项卡。
4. 在 **Policies & Settings**（策略和设置）下，将 **Palo Alto Networks DNS Security** 的策略操作设置为 **Allow**（允许）操作。



STEP 3 | 单击 **OK**（确定）以保存防间谍软件配置文件。

监控 DNS Security 订阅服务

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	❑ Advanced DNS Security 许可证（用于增强功能支持）或 DNS Security 许可证 ❑ 高级威胁防护或威胁防护许可证

Palo Alto Networks 提供了几个选项来监控 DNS Security 和 Advanced DNS Security 活动，以适应一系列依赖 DNS Security 订阅服务和相关流量数据的产品的情报检索。根据产品平台的不同，您可以访问提供 DNS 请求统计信息和使用趋势（包括网络活动上下文）的高级指示板，以日志数据的形式访问特定用户的特定 DNS 请求详细信息。

您还可以通过 Strata Cloud Manager 命令中心查看 DNS Security 订阅服务如何与其他 Palo Alto Networks 应用程序和安全服务集成，以保护组织免受威胁，并全面了解部署的整体运行状况。命令中心就是您的 NetSec 主页，在交互式可视指示板中全面概述您的网络运行状况、安全性和效率，具有多个数据方面，以便您进行一目了然地评估。

有关 DNS Security 订阅服务操作的更多具体细节，指示板提供对网络 DNS 查询数据的查看，以及深入查看各种 DNS 趋势的能力。每个指示板卡都以图形报告格式提供了 DNS 请求和响应处理和分类的独特视图。这使您可以一目了然地看到贵组织的 DNS 使用情况统计信息的高级视图。它还提供 Advanced DNS Security 服务检测到的错误配置域和被劫持域的列表，使您能够更正任何 DNS 配置错误。配置错误的域基于添加到 **DNS** 区域配置错误列表中面向公众的父级域条目。

您还可以查看处理 DNS 请求时自动生成的日志。这些事件文件带有时间戳，在配置为执行时，根据 DNS 类别日志配置提供审计跟踪。DNS 日志条目可以包含有关 DNS 请求的各种详细信息，包括关联域构成的 DNS 威胁的性质，以及检测到威胁时采取的行动。

Palo Alto Networks 提供了几种方法，用于根据您的平台监控 DNS Security 活动。

- Strata Cloud Manager 命令中心
- 查看 DNS Security 指示板
- 查看通过我的网络的 DNS 查询的 DNS Security 日志

查看 DNS Security 指示板

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 DNS Security 许可证（用于增强功能支持）或 DNS Security 许可证 ❑ 高级威胁防护或威胁防护许可证

DNS Security 指示板显示 Advanced DNS Security 和 DNS Security 订阅服务生成的统计数据，以快速、直观的方式评估您组织的 DNS 使用情况。查看并深入了解您网络中发现的各种 DNS 趋势。每个指示板卡片都提供了一个独特的视图，以了解如何处理和分类 DNS 请求。选择指示板卡片可更改指示板的上下文或查看有关特定趋势、域或统计数据的更多信息。

DNS Security 指示板可在 Prisma Access 和 AIOps for NGFW 上使用。您可以与 DNS Security 指示板卡片 交互以更改指示板的上下文或查看有关特定趋势、域或统计数据的更多信息。您还可以自定义格式，以显示相关数据点的当前趋势或历史数据。

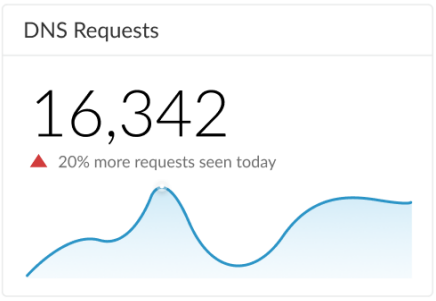
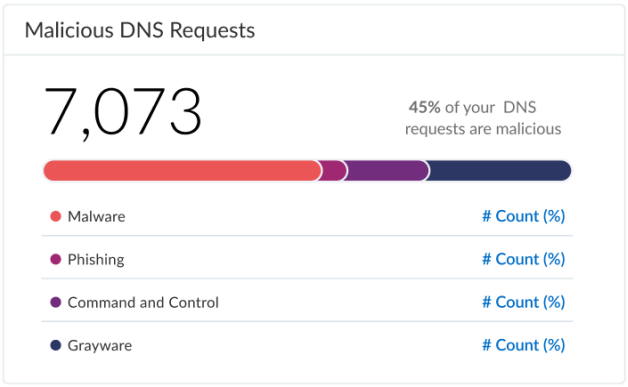
- Strata Cloud Manager
- AIOps for NGFW 免费版

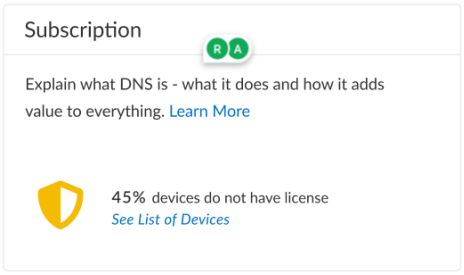
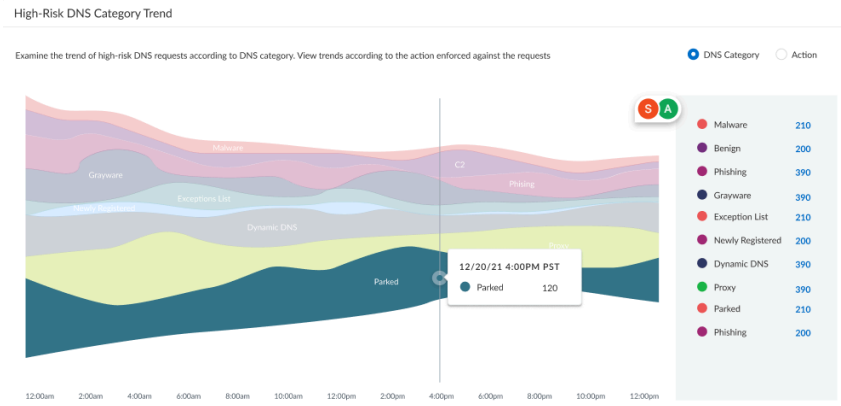
DNS Security 指示板卡片

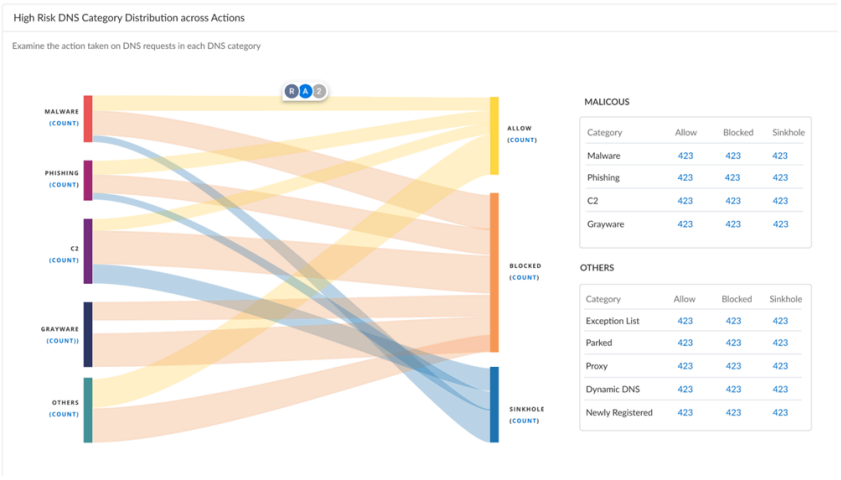
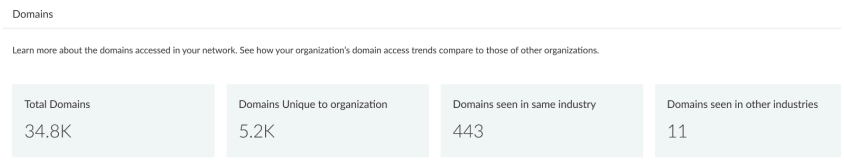
在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Advanced DNS Security 许可证（用于增强功能支持）或 DNS Security 许可证 ❑ 高级威胁防护或威胁防护许可证

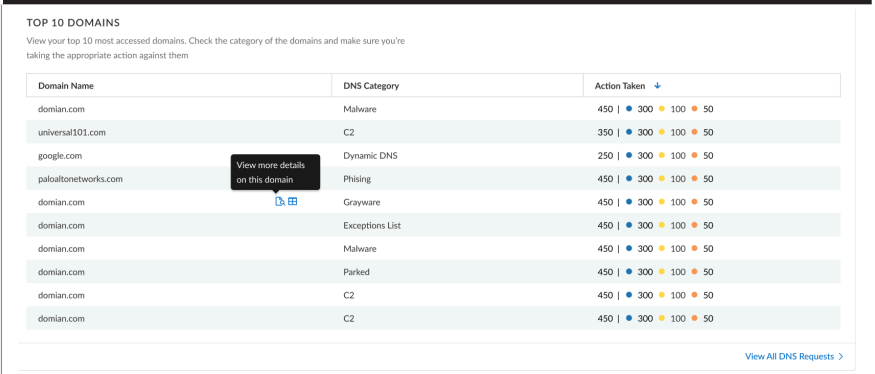
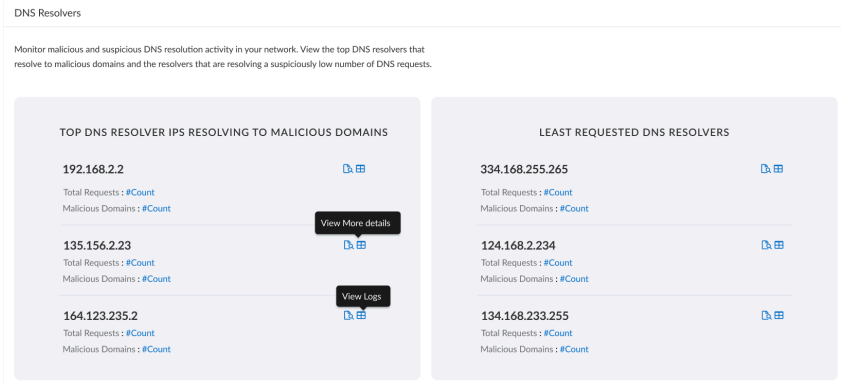
填充 DNS Security 指示板的卡片是交互式的，允许您查看其他详细信息，或转到特定请求、事件和域的列表，因为它与内容的显示方式有关。

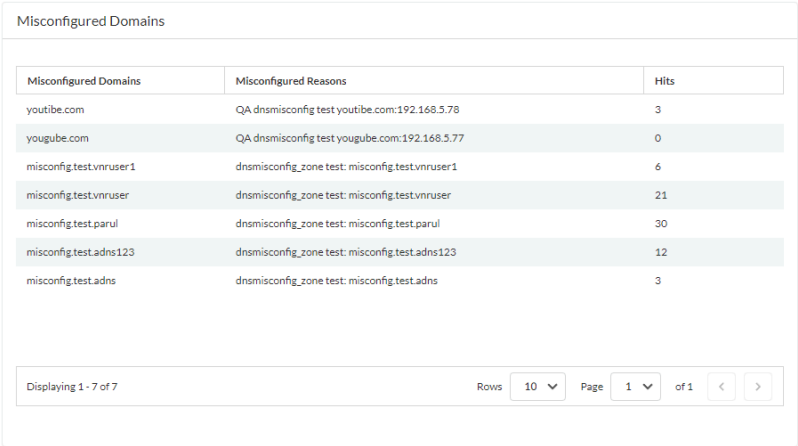
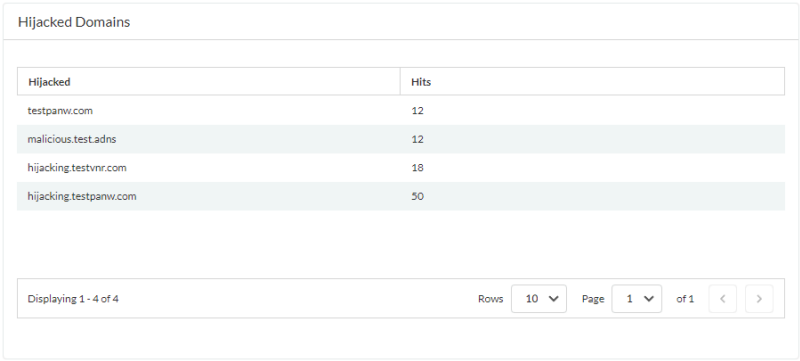
以下列表提供了 DNS Security 指示板卡片的概述：

卡片名称	说明
DNS 请求	显示 DNS Security 处理过的 DNS 请求总数。  • 该折线图根据用户定义的时间范围图示 DNS 请求的数量。指定自定义时间范围将相应地更新折线图。 • DNS 类别和操作过滤器不会改变卡片内容。
恶意 DNS 请求	显示堆叠条形图，其中显示已根据当前可用的恶意类型进行分类的 DNS 请求。总数显示在左上角，而分类变量的细目如下所示。  • 该折线图根据用户定义的时间范围图示 DNS 请求的数量。指定自定义时间范围将相应地更新折线图。 • DNS 类别和操作过滤器不会改变卡片内容。
订阅	显示网络中具有活动 DNS Security 订阅的设备数量。还会显示未配备 DNS Security 或具有已过期订阅的设备百分比，并且包含完整列表的链接。

卡片名称	说明
	 • 您可以选择 **See a List of Devices**（查看设备列表）以查看完整列表。 • 此卡片显示当前订阅状态的快照 — 过滤器选项没有任何影响。
高风险 DNS 类别趋势	显示趋势图，其中显示基于 DNS 类别或在可观察时间范围内应用于 DNS 请求的操作的 DNS 请求细分。  • 使用单选按钮选择 DNS 类别或操作趋势图。 • 将鼠标悬停在表示数据类型的蒸汽图中的线段上，以隔离并打开一个显示 DNS 请求数或执行的操作类型的弹出窗口。 • 指定自定义时间范围将相应地更新趋势图。 • DNS 类别和操作过滤器突出显示卡片中的选定变量，但不会将其从图表中删除。
不同操作的 DNS 类别分布	显示一个流程图，其中提供了针对高风险 DNS 类别所采取操作的分布可视化图表。次级表显示对低优先级 DNS 类别执行的操作。 • 将鼠标悬停在特定流上可打开一个弹出式窗口，显示指定类型的操作数。 指定自定义时间范围会相应地更新流程图。

卡片名称	说明
	• DNS 类别和操作过滤器不会改变卡片内容。  • 顶级域列表是根据指示板顶部应用的过滤器设置生成的。影响整体页面设置的小部件还决定显示哪些域。 • 将鼠标悬停在条形图上可查看使用情况统计信息。 • 单击域可查看 DNS 分析详细信息。
域	根据所选 DNS 类别，显示在您的网络、行业，以及在其他行业内看到的域数量以及总数。允许您将您组织的 DNS 使用情况与行业内的其他组织以及全球收集的数据进行比较，包括仅在您的网络中发现的域请求的列表。  • 此卡片中列出的域包括所有 DNS 类别，而不考虑 DNS 类别和操作过滤器。只有时间范围会更新卡片内容。
前 10 个域	提供从您网络请求最多的前 10 个域的列表，以及 DNS 类别和采取的行动。您可以通过单击相应的图标来查看域的更多详细信息和相关日志。选择 **View All DNS Requests**（查看所有 **DNS** 请求）以查看已访问域的完整列表。

卡片名称	说明
	 • 此卡片中列出的域包括所有 DNS 类别，而不考虑 DNS 类别和操作过滤器。只有时间范围会更新卡片内容。 • 单击域可查看 DNS 分析详细信息。
DNS 解析器	提供两个列表，分别显示网络中解析度最高的恶意域和解析度最低的域。  • 单击 DNS 解析器以查看 DNS 分析详细信息。

卡片名称	说明
配置错误的域 (Advanced DNS Security)	提供与用户指定的面向公众的父级域关联的不可解析域的列表。对于每个条目，都有一个错误配置原因和基于源 IP 的流量命中计数。 
被劫持的域 (Advanced DNS Security)	提供由 Advanced DNS Security 确定的被劫持域列表。对于每个条目，都有一个分类原因和基于源 IP 的流量命中计数。 

查看 DNS Security 指示板 (Strata Cloud Manager)

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。

STEP 2 | 选择 **Dashboards**（指示板） > **More Dashboards**（更多指示板） > **DNS Security**，以便打开 DNS Security 指示板。

STEP 3 | 从指示板中，使用可用的下拉列表配置过滤器选项。

1. 按时间范围筛选 — 选择 **Last hour**（前一个小时）、**Last 24 hours**（过去 **24** 小时）、**Last 7 days**（过去 **7** 天）或 **Last 30 days**（过去 **30** 天），以便显示特定时间范围内的数据。
2. 按 DNS 类别过滤 — 选择 **Select All**（全选）、**Malware**（恶意软件）**Command and Control**（命令和控制）、**Phishing**（网络钓鱼）、**Grayware**（灰色软件）、**Exceptions List**（例外列表）、**Newly Registered**（新注册）、**Dynamic DNS**（动态 **DNS**）、**Proxy**（代理）、**Parked**（寄放）、**Benign**（良性）和 **Ad Track**（广告跟踪），以便根据 DNS 类型过滤数据集。

   Palo Alto Networks 根据 *PAN-DB* 和 *Alexa* 的指标维护的明确允许域的列表。可以经常访问这些允许域列表，且该列表已知没有恶意内容。
3. 按 DNS 操作筛选 — 选择 **Allow**（允许）、**Block**（阻止）和 **Sinkhole**，以便根据 DNS Security 配置文件操作设置对 DNS 查询执行的操作进行筛选。

STEP 4 | （可选）您还可以下载、共享和计划活动报告。

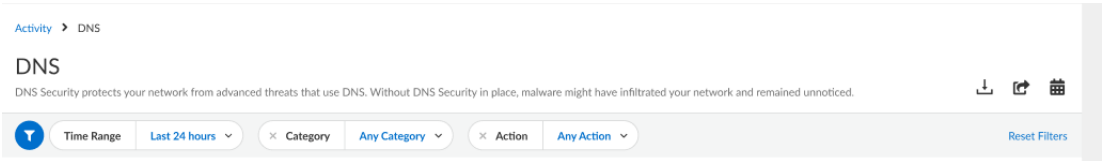
STEP 5 | 您可以从指示板卡片提供的数据中重新设置上下文、进行交互和旋转。有关每个 DNS Security 指示板卡片的概述，请参阅 DNS Security 指示板卡片。

查看 DNS Security 指示板 (AIOps for NGFW Free)

STEP 1 | 使用与 Palo Alto Networks 支持帐户关联的凭据，登录到中心的 AIOps for NGFW Free 应用程序。

STEP 2 | 选择 **Dashboards**（指示板） > **More Dashboards**（更多指示板） > **DNS Security**，以便打开 DNS Security 指示板。

STEP 3 | 从指示板中，使用可用的下拉列表配置过滤器选项。



1. 按时间范围筛选 — 选择 **Last hour**（前一个小时）、**Last 24 hours**（过去 **24** 小时）、**Last 7 days**（过去 **7** 天）或 **Last 30 days**（过去 **30** 天），以便显示特定时间范围内的数据。
2. 按 DNS 类别筛选 — 选择 **C2 (DGA, Tunneling, other C2)**（**C2 [DGA**、隧道、其他 **C2]**）、**Malware**（恶意软件）、**Newly Registered Domain**（新注册的域）、**Phishing**（网络钓鱼）、**Dynamic DNS**（动态 **DNS**）、**Allow List**（允许列

表）、**Benign**（良性）、**Grayware**（灰色软件）、**Parked**（寄放）、**Proxy**（代理）和 **Any Category**（任何类别），以便根据 DNS 类型筛选数据集。

允许列表类别是由 *Palo Alto Networks* 维护的基于 *PAN-DB* 和 *Alexa* 指标的明确允许域列表。可以经常访问这些允许域列表，且该列表已知没有恶意内容。

3. 按 DNS 操作筛选 — 选择 **Allow**（允许）、**Block**（阻止）和 **Sinkhole**，以便根据 DNS Security 配置文件操作设置对 DNS 查询执行的操作进行筛选。

STEP 4 | （可选）您还可以下载、共享和计划活动报告。

STEP 5 | 您可以从指示板卡片提供的数据中重新设置上下文、进行交互和旋转。有关每个 DNS Security 指示板卡片的概述，请参阅 DNS Security 指示板卡片。

查看 DNS Security 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	❑ Advanced DNS Security 许可证（用于增强功能支持）或 DNS Security 许可证 ❑ 高级威胁防护或威胁防护许可证

您可以浏览、搜索和查看 DNS Security 遇到合格事件时自动生成的 DNS Security 日志。通常，这包括 DNS Security 分析的任何域类别，除非它专门将日志严重性级别配置为“无”。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。

DNS Security 日志可直接在防火墙上或通过基于 Strata Logging Service 的日志查看器（AIOps for NGFW Free、Cloud Management、Strata Logging Service 等）访问。虽然防火墙允许您访问用户进行 DNS 查询时生成的恶意威胁日志条目，但不会记录良性的 DNS 请求。DNS Security 数据也会通过日志转发（作为威胁日志）和 DNS Security 遥测（作为 DNS Security 日志）转发至 Strata Logging Service，然后由各种活动日志查看器应用程序引用。DNS Security 遥测以最小的开销运行，从而限制发送到 Strata Logging Service 的数据量；其结果是，只有一部分 DNS 查询作为 DNS Security 日志条目转发到 Strata Logging Service，无论严重程度、威胁类型或类别如何。可完整提供使用日志转发为恶意 DNS 请求转发到 Strata Logging Service 的威胁日志。因此，Palo Alto Networks 建议将恶意 DNS 请求的日志视为威胁日志，而不是 DNS Security 日志。

- Strata Cloud Manager
- PAN-OS 和 Panorama
- AIOps for NGFW 免费版
- Strata 日志记录服务

查看 DNS Security 日志 (Strata Cloud Manager)

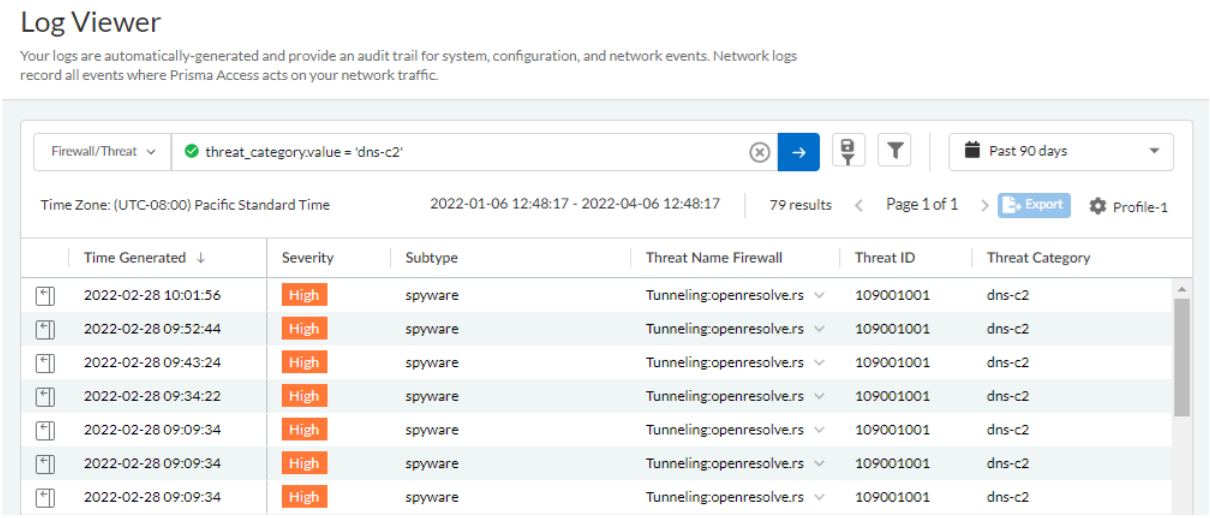
日志查看器中不会显示已由 *DNS Security* 分析的良性 *DNS* 查询。登录到您的 *Strata Logging Service* 应用可访问良性 *DNS* 日志条目。

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。

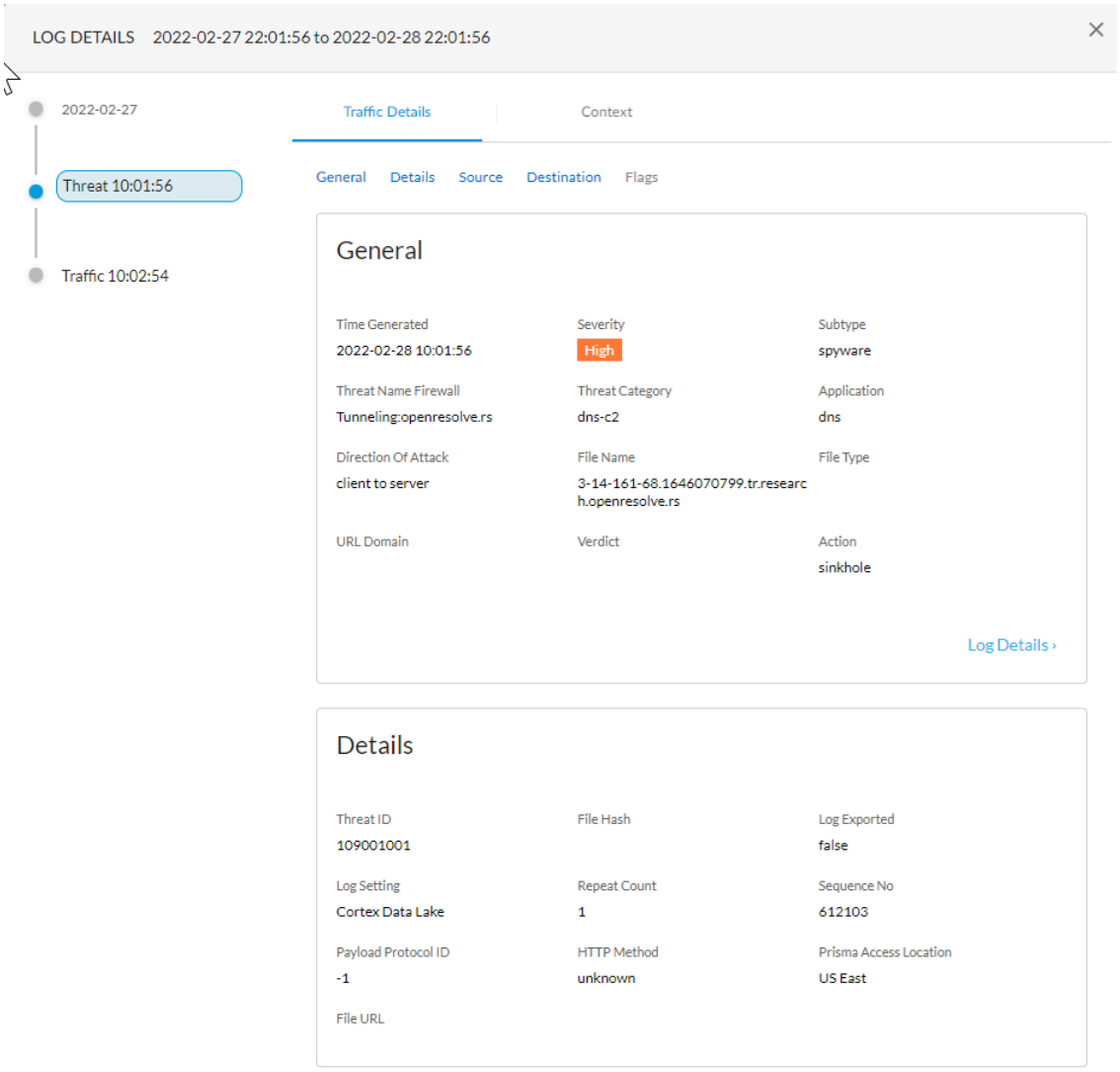
STEP 2 | 搜索已使用 DNS Security 处理的 DNS 查询。

1. 选择 **Incidents and Alerts**（时间和警报）> **Log Viewer**（日志查看器）。
2. 使用威胁过滤器限制搜索，并根据 DNS 类别提交日志查询，例如，使用 `threat_category.value = 'dns-c2'`可查看已确定为 C2 域的日志。要搜索其他

DNS 类型，请将 c2 替换为另一个受支持的 DNS 类别（ddns、parked、malware 等）。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。



3. 选择日志条目以查看检测到的 DNS 威胁的详细信息。
4. 威胁 **Category**（类别）显示在详细日志视图的 **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。



5. 对于库存域和 DNS 隧道域，包括基于隧道的 APT（高级持续威胁），可以查看攻击中使用的各种工具以及与域相关的攻击活动。这反映在给定域的日志条目的威胁 ID/名称字段中。具有属性的 DNS 域的威胁 ID/名称使用以下格式；在本示例中，对于 DNS 隧道域：`Tunneling:<tool_name>,<tool_name>,<tool_name>,...:<domain_name>`，其中 `tool_name` 是指用于将数据嵌入 DNS 查询和响应的 DNS 隧道工具，也是网络威胁活动名称，以逗号分隔列表。这些活动可以是业界认可的事件，使用相同的命名约定，也可以是 Palo Alto Networks 确定和命名的事件，并在 Unit 42 Threat Research 博客中进行了介绍。一篇关于此类攻击活动的博客，本例中是利用 DNS 隧道技术的活动，可在这里找到：利用 DNS 隧道进行跟踪和扫描。

   在初始检测完成后，相关工具和活动属性可能需要一段时间才能在日志以及 *Palo Alto Networks ThreatVault* 和 *Test-A-Site* 中查看。当属性组件完成并经过验证后，完整的 *DNS* 隧道工具和活动详细信息将如预期显示在威胁 *ID*/名称和活动字段中。

查看 DNS Security 日志 (NGFW (Managed by PAN-OS or Panorama))

STEP 1 | 登录 PAN-OS Web 界面。

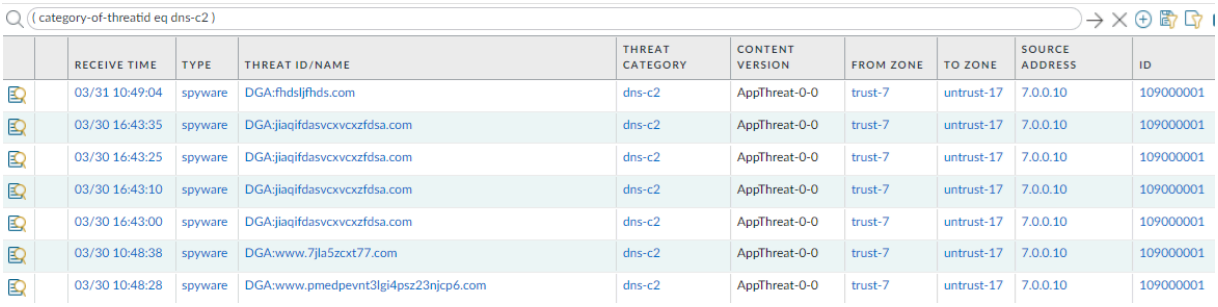
STEP 2 | 在防火墙上搜索已使用 DNS Security 处理的查询的活动。

1. 选择 **Monitor**（监视） > **Logs**（日志） > **Threat**（威胁），并根据 DNS 类别进行过滤。

   请考虑以下示例：

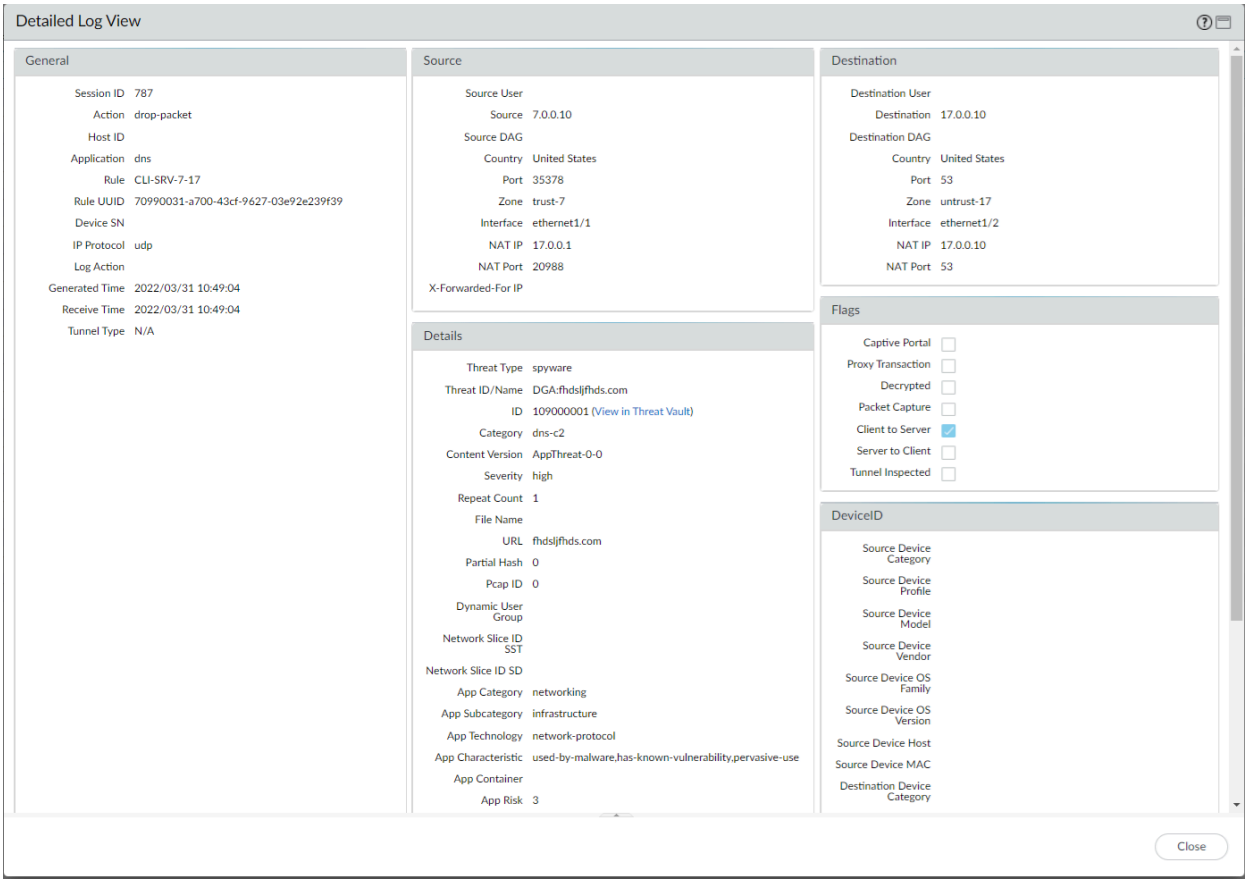
   - `(category-of-threatid eq dns-c2)`，以查看被 DNS Security 确定为 C2 域的日志。
   - `(category-of-threatid eq adns-hijacking)`，其中变量 `adns-hijacking` 表示已被 Advanced DNS Security 归类为恶意 DNS 劫持尝试的 DNS 查询。

   要搜索其他 DNS 类型，请将 c2 替换为另一个受支持的 DNS 类别（ddns、parked、malware 等）。



	RECEIVE TIME	TYPE	THREAT ID/NAME	THREAT CATEGORY	CONTENT VERSION	FROM ZONE	TO ZONE	SOURCE ADDRESS	ID
	03/31 10:49:04	spyware	DGA:fhdsljfhds.com	dns-c2	AppThreat-0-0	trust-7	untrust-17	7.0.0.10	109000001
	03/30 16:43:35	spyware	DGA:jiaqifdasvcxvcxzfdsa.com	dns-c2	AppThreat-0-0	trust-7	untrust-17	7.0.0.10	109000001
	03/30 16:43:25	spyware	DGA:jiaqifdasvcxvcxzfdsa.com	dns-c2	AppThreat-0-0	trust-7	untrust-17	7.0.0.10	109000001
	03/30 16:43:10	spyware	DGA:jiaqifdasvcxvcxzfdsa.com	dns-c2	AppThreat-0-0	trust-7	untrust-17	7.0.0.10	109000001
	03/30 16:43:00	spyware	DGA:jiaqifdasvcxvcxzfdsa.com	dns-c2	AppThreat-0-0	trust-7	untrust-17	7.0.0.10	109000001
	03/30 10:48:38	spyware	DGA:www.7jla5zcxt77.com	dns-c2	AppThreat-0-0	trust-7	untrust-17	7.0.0.10	109000001
	03/30 10:48:28	spyware	DGA:www.pmedpevnt3lgi4psz23njcp6.com	dns-c2	AppThreat-0-0	trust-7	untrust-17	7.0.0.10	109000001

2. 选择日志条目以查看检测到的 DNS 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。有关威胁的其他相关详细信息显示在相应的窗口中。



4. 对于库存域和 DNS 隧道域，包括基于隧道的 APT（高级持续威胁），可以查看攻击中使用的各种工具以及与域相关的攻击活动。这反映在给定域的日志条目的威胁 ID/名称字段中。具有属性的 DNS 域的威胁 ID/名称使用以下格式；在本示例中，对于 DNS 隧道域：`Tunneling:<tool_name>,<tool_name>,<tool_name>,...:<domain_name>`，其中 `tool_name` 是指用于将数据嵌入 DNS 查询和响应的 DNS 隧道工具，也是网络威胁活动名称，以逗号分隔列表。这些活动可以是业界认可的事件，使用相同的命名约定，也可以是 Palo Alto Networks 确定和命名的事件，并在 Unit 42 Threat Research 博客中进行了介绍。一篇关于此类攻击活动的博客，本例中是利用 DNS 隧道技术的活动，可在这里

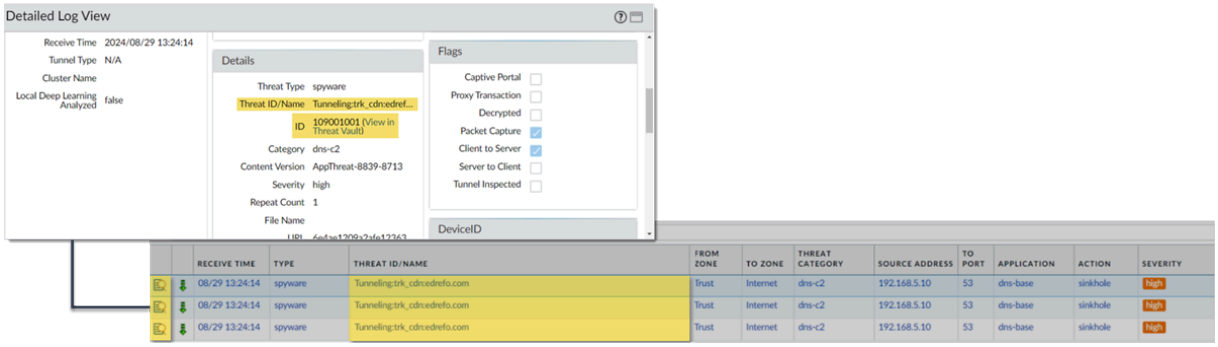
找到：利用 DNS 隧道进行跟踪和扫描。或者，您也可以从 Palo Alto Networks ThreatVault 和 URL 过滤测试 A 站点查看归属信息。

在初始检测完成后，相关工具和活动属性可能需要一段时间才能在日志以及 *Palo Alto Networks ThreatVault* 和 *Test-A-Site* 中查看。当属性组件完成并经过验证后，完整的 *DNS* 隧道工具和活动详细信息将如预期显示在威胁 *ID*/名称和活动字段中。

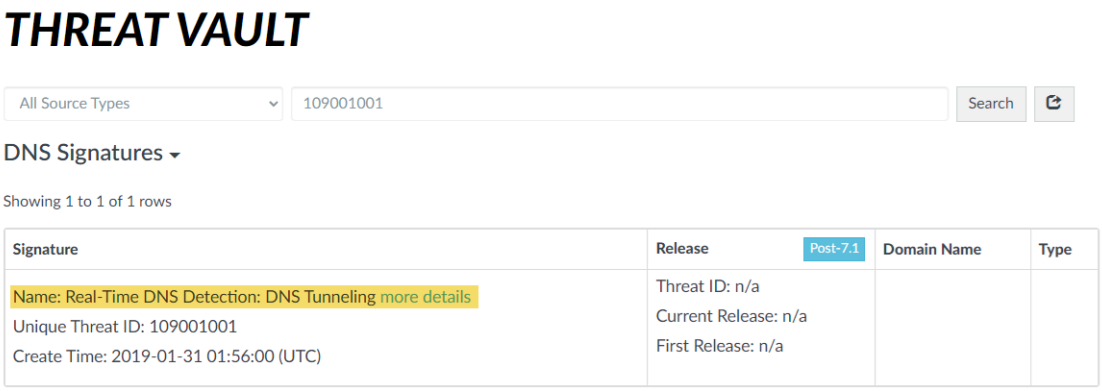
请考虑以下示例：

- **DNS** 隧道域 **APT** 属性

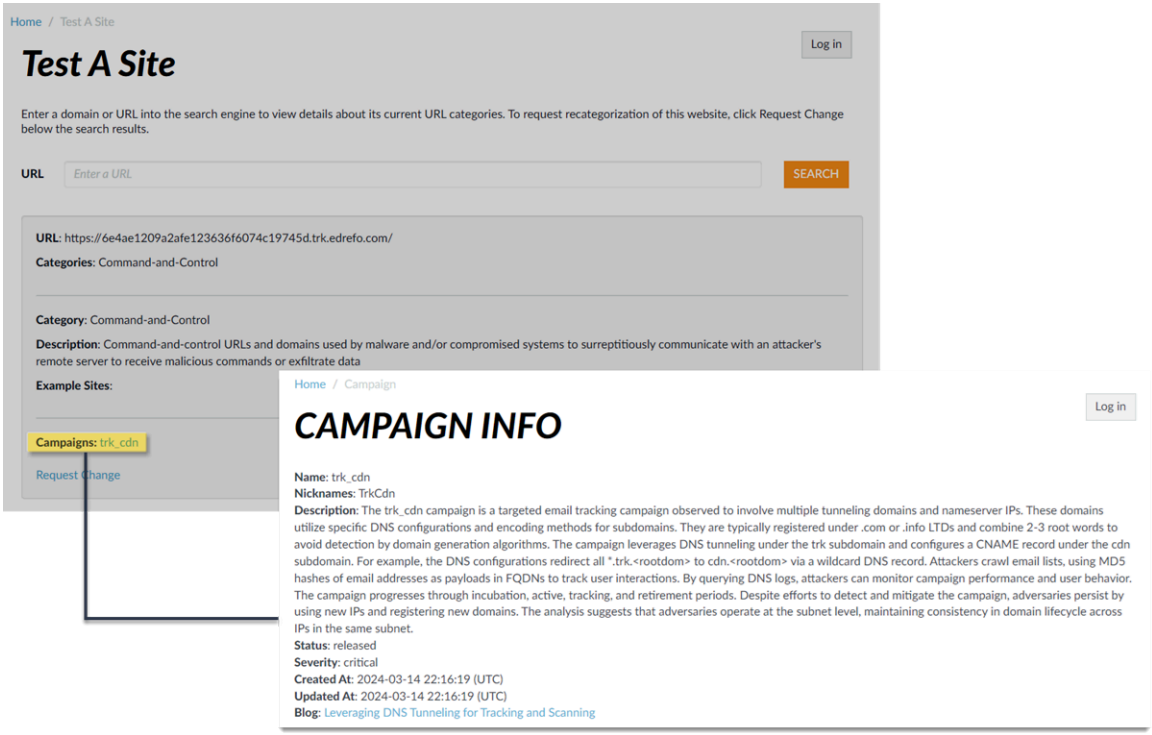
  1. PAN-OS



  2. ThreatVault

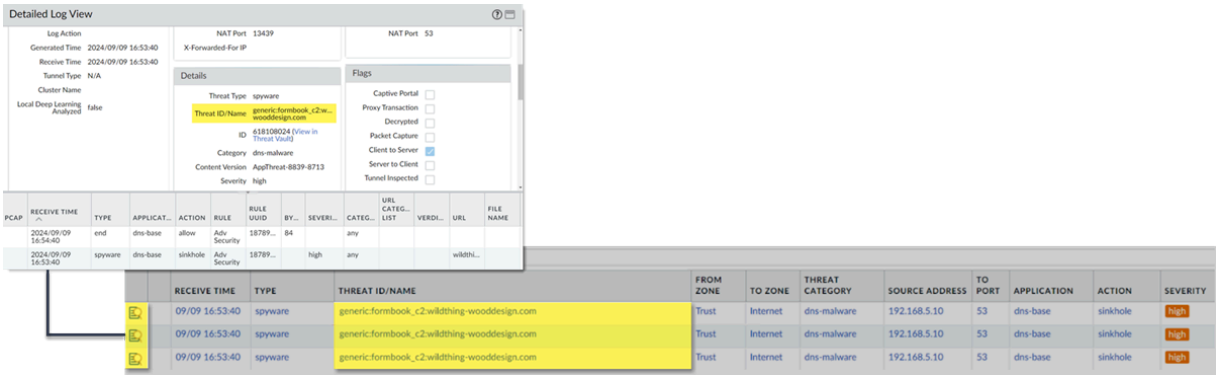


  3. URL 过滤 Test-A-Site

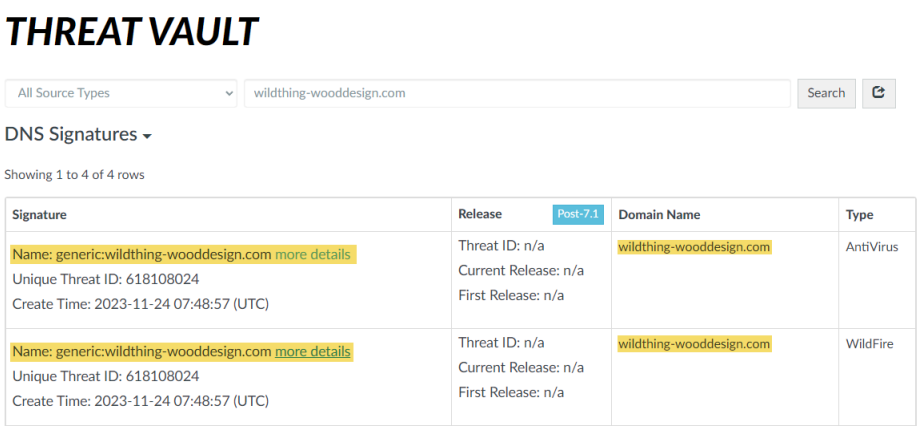


- 库存域 **APT** 属性

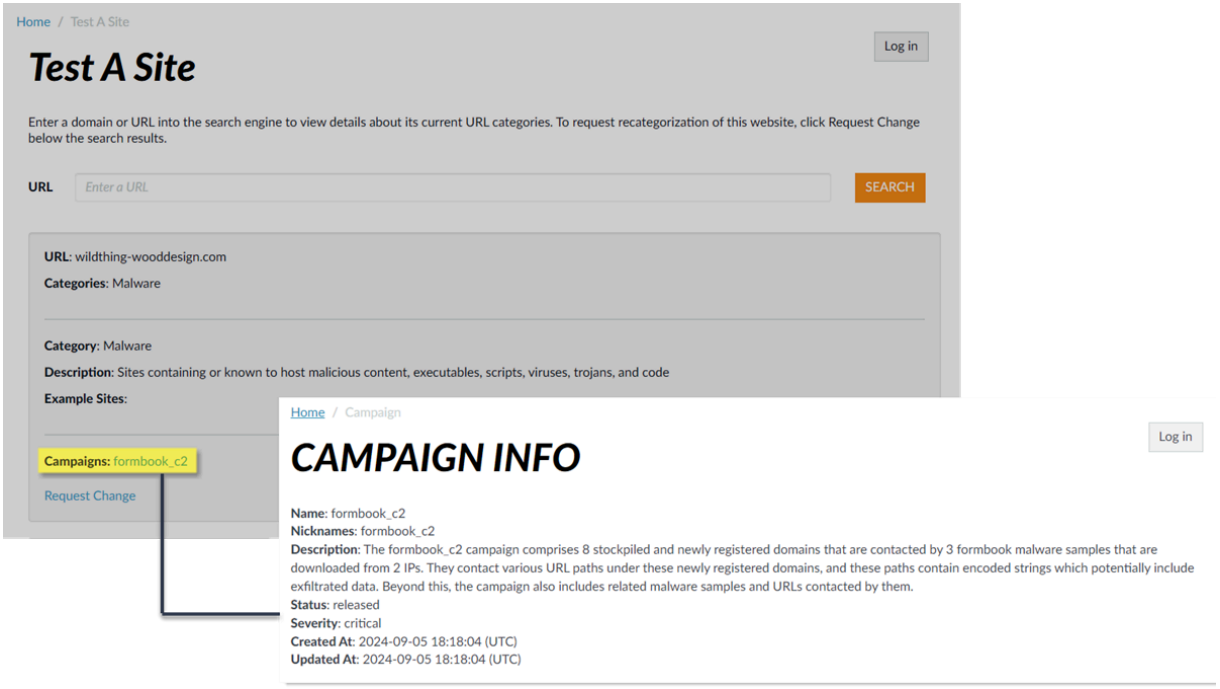
  1. PAN-OS



  2. ThreatVault



3. URL 过滤 Test-A-Site



查看 DNS Security 日志 (AIOps for NGFW Free)

DNS Security 分析的良性 *DNS* 查询不会显示在 *AIOps for NGFW Free* 日志查看器中。登录到您的 *Strata Logging Service* 应用可访问良性 *DNS* 日志条目。

STEP 1 | 使用与 Palo Alto Networks 支持帐户关联的凭据，登录到中心的 AIOps for NGFW Free 应用程序。

STEP 2 | 在 AIOps for NGFW Free 中搜索已使用 DNS Security 处理的 DNS 查询。

1. 选择 **Incidents and Alerts**（时间和警报）> **Log Viewer**（日志查看器）。
2. 使用威胁过滤器限制搜索，并根据 DNS 类别提交日志查询，例如，使用 `threat_category.value = 'dns-c2'` 可查看已确定为 C2 域的日志。要搜索其他 DNS 类型，请将 c2 替换为另一个受支持的 DNS 类别（ddns、parked、malware 等）。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。
3. 选择日志条目以查看检测到的 DNS 威胁的详细信息。
4. 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。

查看 DNS Security 日志 (Strata Logging Service)

STEP 1 | 使用与 Palo Alto Networks 支持帐户关联的凭据，登录到中心的 Strata Logging Service 应用程序。

STEP 2 | 根据日志类型分配存储。如果尚未在 Strata Logging Service 上为 DNS Security 日志分配存储空间，则无法通过 Strata Logging Service 查看日志条目.

STEP 3 | 在 Strata Logging Service 中搜索已使用 DNS Security 处理的 DNS 查询。

1. 选择**Explore**（浏览）以打开 Strata Logging Service 日志查看器。
2. 使用威胁过滤器限制搜索，并根据 DNS 类别提交日志查询，例如，使用 `threat_category.value = 'dns-c2'`可查看已确定为 C2 域的日志。要搜索其他 DNS 类型，请将 c2 替换为另一个受支持的 DNS 类别（ddns、parked、malware 等）。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。
3. 选择日志条目以查看检测到的 DNS 威胁的详细信息。
4. 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。