paloalto
TECHDOCS

高级 URL 过滤管理

docs.paloaltonetworks.com

Contact Information

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

About the Documentation

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

Copyright

Last Revised

April 21, 2023

Table of Contents

URL 过滤基础知识

哪里可以使用？	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)	☐ 高级 URL 过滤许可证（或旧版 URL 过滤许可证） 注意： • 旧版 *URL* 过滤许可证已停用，但仍支持有效的旧版许可证。 • Prisma Access 许可证包括 *Advanced URL Filtering* 功能。

URL 过滤技术通过精细控制用户访问和与互联网内容的交互来保护用户免受基于 Web 的威胁。您可以制定 URL 过滤策略，根据 URL 类别、用户和群组限制对网站的访问。例如，您可以阻止访问已知存在恶意软件的站点，并阻止最终用户在特定类别的站点上输入公司证书。

为了精细控制用户对类别的访问权限，您可以创建 URL 过滤配置文件并为预定义和自定义 URL 类别定义网站访问权限；然后，将该配置文件应用于安全策略规则。您还可以在安全策略规则中使用 URL 类别作为匹配条件。有关高级 URL 过滤订阅可满足您组织的 Web 安全需求的方法列表，请参阅URL 过滤用例。

- Palo Alto Networks URL 过滤解决方案
- URL 过滤支持
- 本地内联分类
- 高级 URL 过滤的工作原理
- URL 过滤配置文件
- URL 分类
- URL 过滤用例

Palo Alto Networks URL 过滤解决方案

哪里可以使用？	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)	❑ 高级 URL 过滤许可证（或旧版 URL 过滤许可证） 注意： • 旧版 *URL* 过滤许可证已停用，但仍支持有效的旧版许可证。 • Prisma Access 许可证包括 *Advanced URL Filtering* 功能。

高级 URL 过滤（之前为 URL 过滤）是一项订阅服务，可保护您的网络及其用户免受已知和未知的恶意和规避的基于Web的威胁。该订阅提供与 URL 过滤相同的功能 — 粒度 URL 过滤控制、用户 Web 活动可见性、安全搜索实施和凭据钓鱼预防 — 并使用基于内联 ML 的 Web 安全引擎添加了完整的 Web 内容检查。内联 Web 安全引擎可以对 PAN-DB（Palo Alto Networks 基于云的 URL 数据库）中不存在的 URL 进行实时分析和分类。然后，引擎确定防火墙采取的操作。

高级 URL 过滤功能可防止在PAN-DB分析并将其添加到数据库之前更新或引入的恶意 URL。启用高级 URL 过滤后，URL 请求将：

- 使用基于云的高级 URL 过滤检测模块进行实时分析。这是除了将 URL 与 PAN-DB 中的条目进行比较之外的。ML 支持的 Web 保护引擎检测并阻止 PAN-DB 无法检测的恶意网站。
- 使用本地内联分类（这是一种基于防火墙的分析解决方案，可以实时阻止未知的恶意网络）检测网络钓鱼和恶意 JavaScript。

运行 PAN-OS 9.1 及更高版本的新一代防火墙支持高级 URL 过滤许可证。您可以在 PAN-OS 和 Panorama Web 界面、Prisma Access 和 Cloud NGFW 平台上管理 URL 过滤功能。但是，某些 URL 过滤功能并非在每个平台上都可用。

如果企业网络安全要求禁止防火墙直接访问互联网，Palo Alto Networks 可通过 PAN-DB 私有云提供离线 URL 过滤解决方案。您可以在一个或多个 M-600 设备上部署 PAN-DB 私有云，这些设备在您的网络中充当 PAN-DB 服务器；但是，它不支持高级 URL 过滤解决方案提供的任何基于云的 URL 分析功能。

旧版 URL 过滤订阅

URL 过滤会对存储在本地缓存或 PAN-DB 中的网站实施策略规则。当用户请求网站时，防火墙会检查本地缓存中的 URL 类别。如果网站不在缓存中，防火墙会查询 PAN-DB 以决定应用哪个操作。因此，攻击者能够更好地使用基于云的数据库中不存在的 URL 发起精确攻击活动。

旧版订阅持有者可以继续使用其 *URL* 过滤部署，直到许可期限结束。

URL 过滤支持

高级 URL 过滤功能可在新一代防火墙（虚拟和本地）、Prisma Access (Managed by Strata Cloud Manager)、Prisma Access (Managed by Panorama)、Cloud NGFW for AWS 和 Cloud NGFW for Azure 上使用。但是，新一代防火墙和 Cloud NGFW for Azure 需要订阅高级 URL 过滤，而所有 Prisma Access 以及 Cloud NGFW for AWS 许可证均包含高级 URL 过滤功能。

功能支持取决于 *URL* 过滤许可证的平台和类型。只有高级 *URL* 过滤许可证才能使用的功能由高级 *URL* 过滤标签指示。

下表显示了高级 URL 过滤功能与每个支持 URL 过滤的 Palo Alto 网络平台的兼容性。

功能	支持于						注意
	NGFW (Managed by Strata Cloud Manager)	**NGFW (Managed by PAN-OS or Panorama)**	**Prisma Access (Managed by Strata Cloud Manager)**	**Prisma Access (Managed by Panorama)**	**Cloud NGFW for AWS**	**Cloud NGFW for Azure**	
内联分类 • 本地内联分类（在 PAN-OS 10.2 之前称为内联 ML） • （高级 URL 过滤）云内联分类	是	是	是	是	是	是	VM-50 或 VM50L 设备不支持
自定义 URL 类别	是	是	是	是	是	是	
用户凭据检测	是	是	是	是	是	是	
自定义 URL 过滤响应页面	是	是	是	是	是	是	

功能	支持于						注意
	NGFW (Managed by Strata Cloud Manager)	NGFW (Managed by PAN-OS or Panorama)	Prisma Access (Managed by Strata Cloud Manager)	Prisma Access (Managed by Panorama)	Cloud NGFW for AWS	Cloud NGFW for Azure	
强制执行安全搜索 • 禁用“严格安全搜索”时阻止搜索结果 • 强制执行严格安全搜索	是	是	是	是	是	是	
URL 管理替代	是	是	是	是	是	是	
SSL/TLS 握手检测	是	是	是	是	是	是	
与远程浏览器隔离 (RBI) 集成	否	否	是	是	否	否	
仅记录容器页面（仅记录用户访问的页面）	否	是	是	是	是	是	

本地内联分类

哪里可以使用？	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)	❑ 高级 URL 过滤许可证 注意：Prisma Access 许可证包括 *Advanced URL Filtering* 功能。

通过 URL 过滤本地内联分类（以前称为内联 ML），防火墙数据平面可以在网页上使用机器学习，以在检测到网络钓鱼变体时警告用户，同时防止 JavaScript 漏洞利用的恶意变体进入您的网站。本地内联分类使用一系列 ML 模型评估各种网页的详细信息，从而动态分析并检测恶意内容。各个 ML 模型通过评估文件详细信息（包括解码器字段和模式），检测恶意内容，从而形成高概率分类和判定，然后将其用作更大型 Web 安全策略的组成部分。划分到恶意类的 URL 将被转发到 PAN-DB 进行其他分析和验证。您可以指定 URL 例外，以排除可能遇到的任何误报。这样，您就可以为配置文件创建更精细的规则，以满足特定安全需求。为了跟上威胁形势的最新变化，可以通过内容发布定期更新并添加内联 ML 模型。需要有效的高级 URL 过滤订阅才能配置内联分类。

作为配置防病毒配置文件的一部分，还可启用基于内联 ML 的保护，以实时检测恶意 PE（可迁移可执行文件）、ELF 和 MS Office 文件以及 PowerShell 和 Shell 脚本。有关详细信息，请参阅：高级 Wildfire 内联 ML。

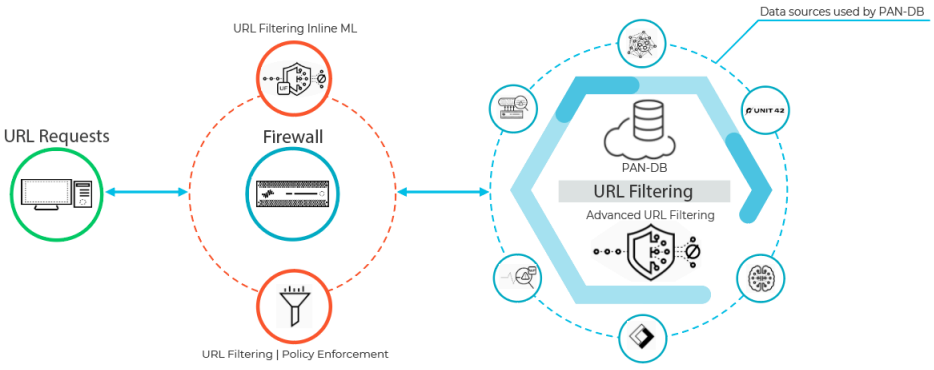
VM-50 或 *VM50L* 虚拟设备不支持本地内联分类。

高级 URL 过滤的工作原理

哪里可以使用？	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)	❑ 高级 URL 过滤许可证（或旧版 URL 过滤许可证） 注意： • 旧版 *URL* 过滤许可证已停用，但仍支持有效的旧版许可证。 • Prisma Access 许可证包括 *Advanced URL Filtering* 功能。

高级 URL 过滤功能会根据站点内容、功能和安全对网站进行分类。一个 URL 最多可以包含四个 URL 类别，以便指示该网站使您遭受威胁的可能性。随着 PAN-DB（高级 URL 过滤功能的 URL 数据库）对站点进行分类，启用了高级 URL 过滤的防火墙可利用该知识以实施您组织的安全策略。除了 PAN-DB 提供的保护之外，高级 URL 过滤还使用机器学习 (ML) 提供实时分析，以防御新的和未知的威胁。这提供了对在 URL 过滤数据库有机会分析和添加内容之前更新或引入的恶意 URL 的保护，为攻击者提供了一个开放的时间，他们可以在此期间发起精确攻击活动。高级 URL 过滤功能通过提供基于每个请求的实时 URL 分析来弥补数据库解决方案中固有的覆盖范围差距。高级 URL 过滤所使用的基于机器学习的模型已经过训练并不断更新，可检测各种恶意 URL、网络钓鱼网页以及命令与控制 (C2)。

通过基于云的内联深度学习系统，使用检测器和分析器来补充高级 URL 过滤功能使用的 ML 模型，对指示存在某些高级威胁的网站进行额外处理。深度学习探测器可以处理更大的数据集，并可以通过多层神经网络更好地识别复杂的恶意模式和行为。当高级 URL 过滤在收到可疑 Web 请求后、从防火墙接收 HTTP 响应数据时，将通过深度学习探测器对这些数据进行进一步分析，并提供内联保护，防止规避式样零日 Web 攻击。包括网页内容从未知网站秘密检索的隐蔽网站，这些未知网站可能包含 URL 数据库无法解释的恶意内容、多步攻击、CAPTCHA 质询以及先前未发现的一次性 URL。由于规避性恶意网站处于不断变化的状态，因此用于对网站进行分类的检测器和分析器会随着 Palo Alto Networks 威胁研究人员改进检测逻辑而自动更新和部署，而无需管理员下载更新包。



当用户请求网页时，防火墙会查询用户添加的例外和 PAN-DB，了解站点风险类别。PAN-DB 使用来自 Unit 42、WildFire、被动 DNS、Palo Alto Networks 遥测数据、来自 Cyber Threat

Alliance 的数据的 URL 信息，并应用各种分析器来确定类别。如果 URL 显示出危险或恶意特征，Web 有效负载数据也会提交到云端的高级 URL 过滤进行实时分析，并生成额外的分析数据。然后，由此生成的风险类别将由防火墙检索，并用于根据您的策略配置实施 Web 访问规则。此外，防火墙会缓存新条目的站点分类信息，以便快速检索后续请求，同时移除用户最近未访问的 URL，以便准确反映网络中的流量。此外，检查内置 PAN-DB 云查询，确保防火墙能够接收最新的 URL 分类信息。如果您没有互联网连接或活动的 URL 过滤许可证，则不会对 PAN-DB 进行查询。

防火墙通过将网站的 URL 类别与 1) 自定义 URL 类别、2) 外部动态列表 (EDL) 和 3) 预定义 URL 类别（按优先顺序）中的条目进行比较来确定网站的 URL 类别。

在数据面板上将防火墙配置为使用机器学习实时分析 URL 后，可提供另一层安全保护，防止网络钓鱼网站攻击和 JavaScript 漏洞利用。本地内联分类所使用的 ML 模型可识别当前未知以及未来可能会出现的基于 URL 的威胁（与 Palo Alto Networks 标识为恶意的特征相匹配）变体。为了跟上威胁形势的最新变化，可以通过内容发布添加或更新本地内联分类 ML 模型。

防火墙检查 PAN-DB 中的 URL 时，还会查找关键更新，例如之前被视为良性但现在被视为恶意的 URL。

如果您认为 PAN-DB 对站点的分类有误，您可以在浏览器中通过测试 A 站点提交更改请求，或者直接从防火墙日志中提交更改请求。

您知道吗？

从技术上而言，防火墙会将 *URL* 缓存在管理平面和数据平面上。

- *PAN-OS 9.0* 及后续版本不会下载 *PAN-DB* 种子数据库。相反，防火墙会在 *URL* 过滤许可证激活后，在执行 *URL* 查询时填充缓存。
- 管理平面会保留更多 *URL*，并直接与 *PAN-DB* 通信。如果防火墙无法在缓存中找到 *URL* 类别，并在 *PAN-DB* 中执行查找，则可以在管理平面上缓存检索到的类别信息。管理平面将此信息发送到数据平面，从而将其缓存，并用于实施策略。
- 数据平面保留的 *URL* 较少，可从管理平面接收信息。防火墙检查 *URL* 的 URL 类别例外列表（自定义 *URL* 类别和外部动态列表）后，接着会检查数据平面。如果防火墙在数据平面中找不到 *URL*，则会检查管理平面，如果不存在类别信息，则检查 *PAN-DB*。

URL 过滤配置文件

哪里可以使用？	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)	❑ 高级 URL 过滤许可证（或旧版 URL 过滤许可证） 注意： • 旧版 *URL* 过滤许可证已停用，但仍支持有效的旧版许可证。 • Prisma Access 许可证包括 *Advanced URL Filtering* 功能。

URL 过滤配置文件定义防火墙如何处理特定 URL 类别的流量。URL 过滤配置文件是可以应用到个别安全策略规则以执行 Internet 访问的一系列 URL 过滤控制集。您可以为 URL 类别配置站点访问权限、允许或不允许用户凭据提交、启用安全搜索实施以及各种其他设置。要强制执行 URL 过滤配置文件中定义的操作，请将配置文件应用于安全策略规则。防火墙会对匹配安全策略规则的流量实施配置文件操作（有关详细信息，请参阅配置 URL 过滤）。

防火墙配置了默认配置文件以阻止存在潜在威胁的类别，如恶意软件、网络钓鱼和成人类别。您可以使用安全策略规则中的默认配置文件，克隆此配置文件以用作新 URL 过滤配置文件的起点，或添加新 URL 过滤配置文件。您可以自定义新添加的 URL 过滤配置文件，并添加特定网站列表（应始终阻止或允许）。例如，您可以阻止社交网络类别，但允许访问该类别中的特定网站。默认情况下，创建基本 URL 过滤配置文件时，可将所有 URL 类别的站点访问设置为允许。这意味着，用户能够自由浏览所有站点且不会记录流量。

创建最佳实践 URL 过滤配置文件，以确保 *URL* 不受出现的托管恶意软件或破坏性内容的攻击。

URL 过滤配置文件策略操作

在 URL 过滤配置文件中，您可以为 URL 类别定义 **Site Access**（站点访问），根据 URL 类别允许或不允许 **User Credential Submissions**（用户凭据提交）（例如，您可以阻止中高风险网站的用户凭据提交），并启用强制执行安全搜索。

操作	说明
站点访问	
警报	允许网站且在 URL 过滤日志中生成日志条目。 设置 ***alert***（警报）作为您不会阻止记录的流量类别的操作，并提供流量的可见性。

操作	说明
允许	允许网站且不生成任何日志条目。 因为您无法查看未记录的流量，因此，请勿将 ***allow***（允许）设置作为您不会阻止的流量类别的操作。相反，应设置 ***alert***（警报）作为您不会阻止记录的流量类别的操作，并提供流量的可见性。
block	阻止网站，用户将会看到响应页面且无法继续访问网站。同时会在 URL 过滤日志中生成日志条目。 阻止 URL 类别的站点访问也会为该 URL 类别设置用户凭据提交，以进行阻止。
继续	系统会为用户提示表明因公司政策已阻止该网站的响应页面，但会提示用户选择继续访问网站。**continue**（继续）操作通常用于被视为良性的类别，并可在他们觉得此站点的分类不正确时，为其提供继续选项来提升用户体验。可以自定义响应页面消息以包含特定于贵公司的详细信息。同时会在 URL 过滤日志中生成日志条目。 继续页面不会正常显示在配置为使用代理服务器的客户端系统上。
替代	用户将会看到一个响应页面，表明允许访问指定类别中的网站需要密码。使用此选项，安全管理员或技术支持人员会提供密码，以授予对指定类别中所有网站的临时访问权限。同时会在 URL 过滤日志中生成日志条目。请参阅允许密码访问某些站点。 在早期发行版本中，URL 过滤类别替代可优先于自定义 URL 类别进行实施。升级到 PAN-OS 9.0 后，URL 类别替代项将转换为自定义 URL 类别，但不再优先于其他自定义 URL 类别实施。新的自定义 URL 类别采用最严格的 URL 过滤配置文件操作（而非在先前发行版本中为类别替代定义的操作）通过安全策略规则实施。可能的 URL 过滤配置文件操作从最严格到最不严格排序为：阻止、替代、继续、警报和允许。 这意味着，如果您的 URL 类别替代操作为允许，在 PAN-OS 9.0 中转换为自定义 URL 类别后，替代项可能会被阻止。 替代页面不会正常显示在配置为使用代理服务器的客户端系统上。

操作	说明
无	**none**（无）操作仅适用于自定义 URL 类别。选择 **none**（无）的目的是确保自定义类别将不会对其他配置文件产生任何影响（如果存在多个 URL 配置文件）。例如，如果您有两个 URL 配置文件，且一个配置文件中的自定义 URL 类别设置为 **block**（阻止），如果您不想阻止操作应用于另一个配置文件，您必须将此操作设置为 **none**（无）。 另外，要删除自定义 URL 类别，必须在使用该类别的任意配置文件中将其设置为 **none**（无）。
用户凭据权限 这些设置需要您首先设置凭据网络钓鱼防护。	
警报	允许用户向此 URL 类别的站点提交公司凭据，但在每次发生时都会生成 URL 过滤警报日志。
allow（允许）（默认）	允许用户向此 URL 类别的网站提交公司凭据。
block	阻止用户向此 URL 类别的网站提交公司凭据。当用户访问阻止公司凭据提交的站点时，将向用户显示默认反网络钓鱼响应页面。您可以自定义显示的阻止页面。
继续	向用户显示响应页面，提示他们选择继续以访问站点。默认情况下，当用户访问不鼓励凭据提交的站点时，将向用户显示反网络钓鱼继续页面。您可以自定义响应页面，以警告用户防范网络钓鱼尝试或在其他网站上重复使用其凭据。

URL 分类

哪里可以使用？	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)	❑ 高级 URL 过滤许可证（或旧版 URL 过滤许可证） 注意： • 旧版 *URL* 过滤许可证已停用，但仍支持有效的旧版许可证。 • Prisma Access 许可证包括 *Advanced URL Filtering* 功能。

Palo Alto Networks 根据网站的内容、功能和安全性对网站进行分类。每个 URL 类别对应于一组可用于创建策略规则的特征。用户在您的网络上访问的 URL 将添加到 Palo Alto Networks URL 过滤数据库 PAN-DB 中。PAN-DB 为这些网站分配最多四个 URL 类别，包括风险类别（高、中和低）。

URL 类别支持对 Web 流量进行基于类别的过滤，并对网站进行精细的策略控制。您可以配置 URL 过滤配置文件，以便为 URL 类别定义站点访问，并将配置文件应用于允许流量流向 Internet 的安全策略规则。您还可以将 URL 类别用作安全策略规则中的匹配标准，以确保这些规则仅适用于指定类别中的网站。例如，您可以配置一个解密策略规则，以防止解密流向 financial-services 类别的流量。

要检查特定 URL 的类别，请在我们的 URL 查找引擎测试 A 站点中输入 URL。如果您认为某个 URL 分类有误，请提交类别更改请求。

自定义 URL 类别

您可以创建自定义 URL 类别，以便将特定网站从基于类别的实施中排除。自定义 URL 类别可以基于特定 URL（URL 列表）或其他类别（类别匹配）。URL 列表类型的自定义 URL 类别用作阻止列表和允许列表。类别匹配类型的自定义 URL 类别允许对与定义为自定义类别一部分的所有类别匹配的网站进行定向实施。

预定义的 URL 类别

下表列出了 PAN-DB 用于过滤 URL 的预定义 URL 类别。某些条目描述从类别中排除的站点。以安全为中心的 URL 类别 描述风险类别，这些类别未分配给所有 URL。

URL 类别	说明
堕胎	与支持或反对堕胎的信息或团体相关的站点，有关堕胎手术的详细信息，与支持或反对堕胎的帮助或支持论坛相关的网站，或提供有关追求（或不追求）堕胎的后果或影响的信息的站点。

URL 类别	说明
滥用药物	宣传滥用合法和非法药物、使用和销售与毒品相关的用具或制造或销售毒品的网站。
成人	包含任何色情材料、媒体（包括语言、游戏或漫画）、艺术或产品的网站，具有色情性质的在线群组或论坛，以及宣传成人服务（如视频或电话会议、陪侍服务和脱衣舞俱乐部）的网站。
烟酒	与销售、制造或使用酒精或烟草产品以及相关用具相关的网站。包括与电子烟相关的网站。
人工智能	使用机器学习和深度学习模型（包括大语言模型）来提供通常需要人类智能的服务的网站。提供的服务包括但不限于聊天机器人、生产力、摘要、转录器、无代码以及音频或视频编辑相关服务。重点放在托管实际 AI 服务的网站上，而不是信息性 AI 内容上。
拍卖	促进个人之间商品销售的网站。 以捐赠为目的的拍卖被归类为社团。
商业与经济	包含与市场营销、管理、经济、创业或经营相关的内容的网站，包括以下内容： • 广告和营销公司的网站 • 运输服务网站，例如 fedex.com • 电话、有线电视和 Internet 服务提供商的网站 • 用于调查或投票的网站 • 商会网站 • 会议网站* • 公司网站可能按其技术而不是此类别进行分类。 • * 与会议相关的网站应根据内容进行分类。如果网站的内容不具体，则会将其归类为“商业和经济”。
命令和控件	恶意软件或受影响的系统使用命令和控制 (C2) URL 及域名与攻击者的远程服务器暗中通信，以接收恶意命令或泄露数据。

URL 类别	说明
计算机和互联网信息	提供有关计算机和 Internet 的一般信息的网站，包括有关以下主题的网站： • 计算机科学 • 工程 • 硬件和计算机零件 • 软件 • 安全 • 编程 “编程”可能与“参考和搜索”类别有一些重叠，但主要类别应该是“计算机和互联网信息”。
内容交付网络	主要关注向第三方提供内容（如广告、媒体、文件和图像服务器）的站点。
版权侵犯	包含非法内容的域，例如允许非法下载软件或其他知识产权的内容，这会带来潜在的责任风险。 提供对等文件交换服务或常规流媒体的站点属于各自的类别。
加密货币	推广加密货币的网站、加密挖矿（但不是嵌入式加密挖矿程序）网站、加密货币交易所和供应商，以及管理加密货币钱包和分类账的网站。 引用加密货币的网站或与加密货币相关的恶意网站将被单独分类。例如，解释加密货币和区块链技术如何运作的网站属于“计算机和互联网信息”。
交友	提供在线约会服务、建议或其他个人广告的网站。 提供性聊天室的约会网站属于成人类别。
动态 DNS	提供或利用动态 DNS 服务将域名与动态 IP 地址关联的站点。 动态 *DNS* 经常被攻击者用于命令和控制通信和其他恶意目的。

URL 类别	说明
教育机构	学校、学院、大学、学区、在线课程和其他学术机构的官方网站。还包括辅导学院的网站。 此类别是指规模较大的成熟教育机构，例如小学、高中和大学。
加密 DNS	DNS 解析器服务提供商的站点，通过使用 DNS over HTTPS (DoH) 等协议加密 DNS 请求和响应，为最终用户提供安全性和隐私性。
娱乐与艺术	电影、电视、广播、视频、节目指南或工具、漫画、表演艺术、博物馆、艺术画廊或图书馆的网站。包括以下站点： • 娱乐 • 名人娱乐行业新闻 • 小说 • 舞蹈课 • 活动场地 • 纹身艺术
极端主义	宣扬恐怖主义、种族主义、法西斯主义或其他歧视不同种族背景、宗教和其他信仰的人或群体的观点的网站。在某些地区，法律和法规可能会禁止访问极端主义站点，允许访问这些站点可能会带来责任风险。 讨论有争议的政治或宗教观点的网站分别属于“哲学”和“政治倡导”以及“宗教信仰”类别。
金融服务	与个人财务或建议相关的网站，例如网上银行、贷款、抵押贷款、债务管理、信用卡公司、外币兑换 (FOREX) 和保险公司。不包括与健康保险、股票市场、经纪公司或交易服务相关的网站。
赌博	通过彩票或赌博促进真实货币或虚拟货币交易的网站。包括提供有关赌博的信息、教程或建议的相关网站，例如，如何根据赔率和彩池下注。 不支持赌博的酒店和赌场的公司网站属于“旅行”类别。

URL 类别	说明
游戏	提供在线游戏或下载视频或计算机游戏、游戏评论、提示、作弊或相关出版物和媒体的网站。包括提供非电子游戏说明、促进棋盘游戏的销售或交易，或者支持或举办在线抽奖和赠品的网站。
政府	地方、州和国家政府以及相关机构、服务或法律的官方网站。 公共图书馆和军事机构的网站分别属于“参考和研究”以及“军事”类别。
灰色软件	网站的内容不构成直接安全威胁，但显示其他侵入性行为，并诱使最终用户授予远程访问或执行其他未经授权的操作。 灰色软件包括以下内容： • 被黑的网站 • 没有恶意行为且不属于目标域的拼写错误域名 • 包含流氓软件、广告软件或其他未经请求的应用程序的网站，例如嵌入式加密挖矿程序、点击劫持或更改 Web 浏览器元素的劫持程序 • 包含与非法或犯罪活动相关的内容的网站
黑客攻击	与非法或可疑地访问或使用通信设备或软件相关的网站，包括开发和分发可能导致网络和系统受损的此类程序、操作方法建议或提示。包括有助于绕过许可和数字版权系统的网站。
健康与医学	包含有关一般健康、问题以及传统和非传统提示、补救措施和治疗方法的信息的网站。包括各种医学专业、实践、设施（如健身房和健身俱乐部）和专业人士的场所。与医疗保险和整容手术相关的网站也包括在内。
家居和园艺	提供与家庭维修和保养、建筑、设计、施工、装饰和园艺相关的信息、产品和服务的网站。
狩猎和捕鱼	提供狩猎和钓鱼提示或说明，或为相关设备和用具的销售提供便利的营地。 主要销售枪支（即使用于狩猎）的网站属于武器类别。

URL 类别	说明
内容不足	显示测试页面的网站和服务，其中没有内容，提供的 API 访问不是供最终用户显示的，或者需要身份验证，而不显示任何其他建议不同分类的内容。
互联网通信和电话	支持或提供视频聊天、即时消息或其他电话服务的网站。
互联网门户	作为用户起点的网站，通常通过聚合一组广泛的内容和主题。
求职	为雇主和潜在求职者提供招聘信息、雇主评价、面试建议和提示或相关服务的网站。
法律	提供有关法律、法律服务、律师事务所或其他法律相关问题的信息、分析或建议的网站。
恶意软件	包含或已知托管恶意内容、可执行文件、脚本、病毒、特洛伊木马和代码的站点。
大麻	讨论、鼓励、推广、提供、销售、供应或以其他方式鼓吹使用、种植、制造或分销大麻及其各种别名的网站，无论是出于娱乐还是医疗目的。包含与大麻相关的用具内容的网站。
军事	包含有关军事部门、招募、当前或过去行动或任何相关用具的信息或评论的网站。包括军事和退伍军人协会的网站。
机动车	包含与汽车、摩托车、船只、卡车和休闲车 (RV) 的评论、销售、交易、修改、零件和其他相关讨论相关的信息的网站。
音乐	与音乐销售、发行或信息相关的网站。包括音乐艺术家、团体、唱片公司、活动、歌词和有关音乐业务的其他信息的网站。不包括音乐流媒体网站。
新注册域名	在过去 32 天内注册的网站。新注册的域通常是有意生成的，或者由域生成算法生成，可用于恶意活动。
新闻	在线出版物、新闻专线服务和其他汇总时事、天气或其他当代问题的网站。包括以下内容： • 报纸 • 电台 • 杂志

URL 类别	说明
	• 播客 • 专门报道新闻的电视节目 • 社交书签网站，例如 reddit.com 如果杂志或新闻网站专注于特定主题，如体育、旅行、时尚，它会根据网站上的主要内容进行分类。
未解决	此类别表示在本地 URL 过滤数据库中找不到该网站，并且防火墙无法连接到云数据库以检查类别。
裸体	包含人体裸体或半裸描写的网站，无论上下文或意图如何，例如艺术品。包括包含参与者图像的裸体主义者或裸体主义者网站。
在线存储和备份	免费或作为服务提供在线文件存储的网站。包括照片共享网站。
寄放	托管受限内容或点击后到达广告的 URL，这可能会为托管实体带来收入，但通常不包含对最终用户有用的内容。包括待售域名。 包含成人内容的停放网站属于“成人”类别。
点对点	提供对种子、下载程序、媒体文件或其他软件应用程序的对等共享的访问权限或客户端的站点。主要适用于具有 BitTorrent 下载功能的网站。不包括共享软件或免费软件网站。
个人网站和博客	个人或团体的个人网站和博客。如果此类网站具有与另一个类别关联的主导主题，则它们将被归类为两个类别。
哲学与治宣传	包含有关哲学或政治观点的信息、观点或活动的网站。
网络仿冒	秘密尝试使用社会工程技术主动或非自愿地从受害者那里收集信息（如登录凭据、信用卡信息、账号、PIN 和其他个人身份信息 (PII)）的 Web 内容。包括技术支持诈骗和恐吓软件。
专用 IP 地址	此类别包括 RFC 1918 “专用 Intranet 的地址分配”中定义的 IP 地址，如下所示：

URL 类别	说明
	• 10.0.0.0 - 10.255.255.255（10/8 前缀） • 172.16.0.0 - 172.31.255.255（172.16/12 前缀） • 192.168.0.0 - 192.168.255.255（192.168/16 前缀） 包括未使用公有 DNS 系统注册的域（如 *.local 和 *.onion）。
代理避免和匿名者	代理服务器和其他绕过 URL 过滤或监控的方法。 用于企业级别的 *VPN* 属于 *Internet* 通信和电话类别。
可疑	包含针对特定个人或人群的恶趣味和攻击性内容的网站。
勒索软件	已知托管勒索软件或恶意流量的网站，这些活动涉及进行勒索软件活动，这些活动通常威胁要发布私人数据或阻止对特定数据或系统的访问，通常是通过加密来阻止对特定数据或系统的访问，直到支付所要求的赎金。包括提供可能携带勒索软件负载的相关窃取程序、擦除程序和加载程序的 URL。
房地产	提供有关房产租赁、销售以及相关提示或信息的网站，包括以下网站： • 房地产公司和代理商 • 租赁服务 • 列表（和聚合） • 性能提升 • 房主协会 • 物业管理组或个人 抵押贷款和贷款服务商的网站属于 金融服务 类别。
实时检测（仅限高级 URL 过滤）	作为高级 URL 过滤的一部分，通过实时内联分析分析和检测的 URL。
娱乐和爱好	包含与娱乐活动和爱好相关的信息、论坛、协会、群组或出版物的网站。

URL 类别	说明
	销售与娱乐活动或爱好（如 *REI.com*）相关的商品的网站属于“购物”类别。
参考与研究	提供个人、专业或学术参考门户、资料或服务的网站，包括在线词典、地图、年鉴、人口普查信息、图书馆、家谱和科学信息。包括以下网站或与以下相关的网站： • 黄页 • 日历 • 公共图书馆 • 研究机构 • 灯光和车辆跟踪服务 • 与房地产、交通等相关的文件和记录（即使属于政府）
宗教	提供有关各种宗教、相关活动或事件信息的网站。包括宗教组织、宗教官员、礼拜场所、算命、占星术、星座运势和宗教用具的场所。 隶属于宗教组织的私立小学或中学（如天主教学校）的课程教授一般宗教教育和世俗科目的网站属于“教育机构”类别。
扫描活动（仅限高级 URL 过滤）	由攻击者执行的活动，这些活动可能表明遭到入侵，或者试图进行有针对性的攻击或探测现有漏洞。这些通常是对手进行的侦察活动的一部分。
搜索引擎	使用关键字、短语或其他参数提供搜索界面的网站，这些参数可能会将信息、网站、图像或其他文件作为结果返回。
性教育	提供有关生殖、性发育、安全性行为、性传播疾病、节育、改善性行为的提示以及任何相关商品或用具的信息的网站。包括相关组、论坛或组织的站点。
共享软件和免费软件	免费或捐赠提供软件、屏幕保护程序、图标、壁纸、实用程序、铃声、主题或小部件访问权限的网站。包括开源项目。
购物	促进商品和服务购买的网站。包括在线商家、百货公司网站、零售店、目录以及价格汇总或监控工具。此

URL 类别	说明
	类别中的网站应该是销售各种商品（或主要目的是在线销售）的在线商家。 恰好允许在线购买的化妆品公司的网站属于化妆品类别。
社交网络	用户社区或用户相互交互、发布消息、图片以及以其他方式与人群进行交流的站点。 个人网站、博客或论坛属于“个人网站和博客”类别。
社会	网站包含与普通人群相关的内容或影响大量人群（如时尚、美容、慈善团体、社团或儿童）的问题。包括餐厅网站。 与食品相关的公司网站（例如 *Burger King*）属于“商业和经济”类别。
运动	包含体育赛事、运动员、教练、官员、团队或组织、比分、赛程、相关新闻或体育用具信息的网站。包括幻想体育和虚拟运动联盟的网站。 以销售体育用品为主要目的的网站属于购物类别。
股票建议和工具	提供有关股票市场、股票或期权交易、投资组合管理、投资策略、报价或相关新闻信息的网站。
流媒体	免费或付费流式传输音频或视频内容的网站，包括在线广播电台、流媒体音乐服务和播客存档。
泳装和贴身衣服	包含有关泳装、贴身服装或其他性暗示服装的信息或图像的网站。
培训和工具	提供在线教育、培训和相关材料的站点。包括驾驶或交通学校、工作场所培训、游戏、应用程序、具有教育目的的工具以及辅导学院。 特定技能类根据其主题进行分类。例如，音乐课程的网站属于“音乐”类别。

URL 类别	说明
翻译	提供翻译服务（包括用户输入和 URL 翻译）的网站。这些网站还可以允许用户规避过滤，因为目标页面的内容显示在翻译人员 URL 的上下文中。
旅行	提供有关旅行信息（例如提示、交易、定价、目的地信息、旅游和相关服务（例如预订或价格监控工具）的网站。包括以下网站： • 当地景点 • 酒店 • 航空公司 • 邮轮公司 • 赌场（如果网站不允许在线赌博） • 旅行社 • 车辆租赁 • 停车设施
未知	Palo Alto Networks 尚未确定的站点。  如果此站点的可用性对您的业务至关重要，并且您必须允许流量、对未知站点发出警报、将最佳实践安全配置文件应用于流量并调查警报。  *PAN-DB* 实时更新在首次尝试访问未知站点后会学习这些站点，因此可以快速识别未知 *URL*，并成为防火墙可以根据实际 *URL* 类别处理的已知 *URL*。
武器	处理销售或提供有关武器、盔甲、防弹背心及其使用的评论、描述或说明的网站。 与粘土射击、射击场和射箭相关的网站分为“武器”主要类别和“运动”次要类别。
Web 广告	包含广告、媒体、内容和横幅的网站。包括用于订阅和取消订阅新闻稿或广告的页面。
基于 Web 的电子邮件	提供对电子邮件收件箱的访问以及发送和接收电子邮件的能力的任何网站。重点放在提供免费或付费公共访问此类服务的网站上。

URL 类别	说明
虚拟主机	为网页提供免费或付费托管服务的网站。包括提供有关 Web 开发、发布、促销和其他增加流量的方法的信息的网站。

以安全为中心的 URL 类别

对于未归类为恶意，或者因为在至少 30 天内仅显示良性活动而不再归类为恶意的 URL，PAN-DB 会自动评估并为 URL 分配风险类别（`high-risk`、`medium-risk`、和 `low-risk`）。每个风险类别都有特定的标准，URL 必须满足这些标准才能接收给定类别。随着网站内容的变化，风险类别和策略实施会动态调整。

如果 *PAN-DB* 确定某个 *URL* 属于恶意 URL 类别，则不会为站点分配风险类别。相反，防火墙会自动阻止该站点，因为它会给大多数环境带来不可接受的风险。

专用 *IP* 地址（和主机）对于主机环境是唯一的，对于 *PAN-DB* 不可见。因此，*Palo Alto Networks* 不会为此类别的网站指定风险评级。

以安全为中心的 URL 类别有助于有针对性地解密和策略实施，从而有助于减少攻击面。例如，您可以选择阻止用户访问高风险和中等风险网站和新注册的域，或者解密这些类别的流量。

下表列出了每个风险类别的描述以及默认和建议的策略操作。

您不能为以安全为中心的 *URL* 类别提交更改请求。

URL 类别	说明
高风险	• 其域被 ML 模型识别为具有先前链接到已知恶意域的属性或 Web 信誉信号较低的站点。 • 之前被确认为恶意软件、网上诱骗或命令与控制 (C2) 站点的网站。 • 与已确认的恶意活动相关联的站点，或与已知恶意站点共享域的站点。 • 防弹 ISP 托管站点 • 因存在活跃的动态 DNS 配置而被分类为 DDNS 的域。 • 源于已知允许恶意内容的 ASN 的 IP 托管站点。 • 分类为 *unknown* 的站点。 在 *PAN-DB* 完成站点分析和分类之前，这些站点仍然是高风险的。 • 这些站点仍将在该类别中保留至少 30 天。 默认和推荐策略操作：警报

URL 类别	说明
中等风险	• 先前已被确认为恶意和网络钓鱼的站点，或至少 30 天仅显示良性活动的 C2 站点。 • 所有云存储站点（分类为在线存储和备份）。 • 分类为 *unknown* 的 IP 地址。 在 *PAN-DB* 完成站点分析和分类之前，这些 *IP* 地址将保持中等风险。 • 这些站点将在该类别中额外保留 60 天。 默认和推荐策略操作：警报
低风险	非中等或高风险的网站。这些站点至少 90 天显示良性活动。 默认和推荐策略操作：允许
新注册域名	标识在过去 32 天内注册的站点。新域通常用作恶意活动中的工具。 新注册域通常是有目的地生成，或是通过域生成算法生成，专用于恶意活动。最佳做法是阻止此 *URL* 类别。 默认策略操作：警报 推荐策略操作：阻止

恶意 URL 类别

我们强烈建议您阻止以下 URL 类别，这些类别可识别恶意或剥削性内容和行为。

- **command-and-control**
- **copyright-infringement**
- **dynamic-dns**
- **extremism**
- **grayware**
- **malware**
- **newly-registered-domain**
- **parked**
- 网络仿冒
- **proxy-avoidance-and-anonymizers**
- **questionable**

- **ransomware**
- 扫描活动
- 未知

对于您发出警报（而非阻止）的类别，可以严格地控制用户与站点内容的交互方式。例如，允许用户访问他们需要的资源（例如，出于研究目的访问开发人员博客或云存储服务），但采取以下预防措施降低暴露于基于 Web 的威胁：

- 遵循防间谍软件、漏洞保护、和文件阻止最佳实践。采取的保护措施应该能阻止下载危险文件类型，并阻止您发出警报的站点使用混淆的 JavaScript。
- 基于 URL 类别的目标解密。解密高风险和中等风险站点就是一个良好的开端。
- 在用户访问高风险和中等风险站点时向其显示响应页面。警告用户，他们试图访问的站点可能存在恶意，并在其决定继续访问站点时建议用户如何采取预防措施。
- 防止凭据网络钓鱼，阻止用户向网站（包括高风险和中等风险的网站）提交其公司凭据。

下表列出了 PAN-DB 认为是恶意且默认阻止的类别，专用 IP 地址除外）。专用 IP 地址（和主机）对于主机环境是唯一的，对于 PAN-DB 不可见。因此，Palo Alto Networks 不会为此类别的网站指定风险评级。

类别	默认操作
命令和控件	阻止
灰色软件	
恶意软件	
网络仿冒	
勒索软件	
Scanning Activity	
专用 **IP** 地址	已允许（无默认操作）

URL 过滤用例

哪里可以使用？	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)	❑ 高级 URL 过滤许可证（或旧版 URL 过滤许可证） 注意： • 旧版 *URL* 过滤许可证已停用，但仍支持有效的旧版许可证。 • Prisma Access 许可证包括 *Advanced URL Filtering* 功能。

除了仅阻止和允许某些站点外，还有很多方法可以执行网页访问。例如，针对每个 URL 使用多个类别，以允许用户访问站点，但是阻止提交公司凭据或下载文件等某些特定功能。此外，还可使用 URL 类别实施不同类型的策略，例如，身份验证、解密、QoS 和安全策略。

请继续阅读以了解更多有关部署 URL 过滤的不同方法。

基于 **URL** 类别控制 **Web** 访问

您可以创建 URL 过滤配置文件以指定 URL 类别的操作，并将该配置文件附加到安全策略规则中。防火墙根据配置文件中的设置对流量实施策略。例如，要阻止所有游戏网站，您需要在 URL 过滤配置文件中为游戏类别配置阻止操作。之后，您将配置文件附加到允许 Web 访问的安全策略规则。

多类别 **URL** 过滤

每个 URL 最多可有 4 个类别，包括指示站点将您置于危险的可能性的 risk 类别。通过对 URL 更精细的分类，您可以超越基本的“阻止或允许”方法进行 Web 访问。相反，对于业务所需，但更有可能被用作网络攻击组成部分的在线内容，您可以控制用户与其交互。

例如，您可能认为某些 URL 类别对您的组织有害，但是，这些类别能提供有价值的资源或服务（例如，云存储服务或博客），因此，对于是否阻止他们，您很犹豫。现在，您可以允许用户访问属于这些类型类别的站点，同时，还能通过解密和检测流量并执行内容只读访问。

您还可以通过选择 **Category Match**（类别匹配）并指定新类别将包含的两个或多个 PAN-DB 类别来定义自定义 URL 类别。通过从多个类别创建自定义类别，您可以针对与自定义 URL 类别对象中指定的所有类别匹配的网站或页面执行操作。

阻止或允许基于 **URL** 类别的公司凭据提交

通过启用防火墙检测站点的公司凭据提交情况预防凭据网络钓鱼，然后基于 URL 类别控制这些提交。阻止用户将凭据提交到恶意和不受信任的站点、警告用户不要在未知站点输入公司凭据或警告用户不要在非公司站点重复使用公司凭据，以及明确允许用户向公司和经批准的站点提交凭据。

实施安全搜索设置

很多搜索引擎都有安全搜索设置，用以过滤搜索结果中的成人图像和视频。如果最终用户未使用最严格的安全搜索设置，您可以启用防火墙来阻止搜索结果，还可以透明地启用用户安全搜索。防火墙可以针对以下搜索提供商执行安全搜索：Google、Yahoo、Bing、Yandex 和 YouTube。请参阅如何开始使用强制执行安全搜索。

对某些站点实施密码访问权限

您可以阻止大多数用户访问站点，同时允许某些用户访问此站点。请参阅如何允许密码访问某些站点。

阻止某些 URL 类别的高风险文件下载

您可以通过创建具有文件阻止配置文件的安全策略规则阻止特定 URL 类别的高风险文件下载。

基于 URL 类别实施安全、解密、身份验证和 QoS 策略

您可以基于 URL 类别实施不同类型的防火墙策略。例如，假定您已启用解密，但不想解密某些个人信息。在这种情况下，您可以创建解密策略规则，从解密中将与 URL 类别 *financial-services* 和 *health-and-medicine* 匹配的网站排除。又如，您可以在 QoS 策略中使用 URL 类 别*streaming-media*，以便对属于此类别的网站应用带宽控制。

下表介绍了接受 URL 类别作为匹配条件的策略：

策略类型	说明
解密	您还可以使用 URL 类别逐步实施解密，从解密中排除可能包含敏感信息或个人信息的 URL 类别（例如，financial-services 和 health-and-medicine）。 计划先对最危险的流量进行解密（URL 类别最有可能包含恶意流量，如赌博或高风险），然后在获得经验时进行解密。或者，先解密不影响业务的 URL 类别（如果出现错误，也不会影响业务），例如，新闻推送。考虑用户反馈，在这两种情况下，解密一些 URL 类别，运行报告，确保解密按预期进行，然后，逐步解密更多的 URL 类别等等。如果由于技术原因或因为选择不解密而不能对站点进行解密，则计划排除解密，将站点排除在解密之外。 *URL* 过滤和解密的最佳实践是基于 *URL* 类别解密流量。
身份验证	要确保在允许用户访问特定类别之前对其进行身份验证，可以附加 URL 类别作为身份验证策略规则的匹配条件。

策略类型	说明
QoS	使用 QoS 策略来分配特定网站类别的吞吐量水平。例如，您可能想要允许 *streaming-media* 类别，但通过添加 URL 类别到 QoS 策略规则可以限制吞吐量。

安全	您可以使用 URL 类别作为匹配条件，或者创建为每个类别指定操作并将其附加到安全策略规则的 URL 过滤配置文件。
	
	使用 ***URL*** 类别作为匹配标准与将 ***URL*** 过滤配置文件应用于安全策略规则
	• 在以下情况下使用 *URL* 类别作为匹配标准：
	  • 创建 URL 类别实施的例外
	  • 将特定操作分配给自定义或预定义的 *URL* 类别。例如，您可以创建允许访问个人站点和博客类别中的站点的安全策略规则。
	• 在以下情况下使用 *URL* 过滤配置文件：
	  • 在 *URL* 过滤日志中记录到 *URL* 类别的流量
	  • 您还可以指定更详细的操作，例如针对特定类别的流量发出警报。
	  • 配置在用户访问被阻止或阻止继续网站时显示的响应页面。
	在 *URL* 过滤配置文件中，为每个 *URL* 类别指定的操作仅适用于发往安全策略规则中指定的 *URL* 类别的流量。您还可以将特定配置文件应用于多个规则。
	
	例如，贵公司的 IT 安全组需要访问 *hacking* 类别，但要拒绝其他所有用户访问此类别，您必须创建以下规则：
	• 允许 IT 安全组访问分类为 *hacking* 的内容的安全策略规则。此安全策略规则引用 **Services/URL**

策略类型	说明
	Category（服务/**URL** 类别）选项卡中的 *hacking* 类别和 **Users**（用户）选项卡中的 IT 安全组。 • 另一个允许用户进行常规 Web 访问的安全策略规则。将用于阻止 *hacking* 类别的 URL 过滤配置文件附加到此规则。 在策略阻止 *hacking* 之前，必须列出允许访问 *hacking* 的策略。这是因为防火墙会对安全策略规则进行从上到下评估，因此当属于安全组的用户尝试访问 *hacking* 站点时，防火墙会先评估允许访问的策略规则，从而允许用户访问。防火墙会针对阻止访问 *hacking* 站点的常规 Web 访问规则评估其他所有组中的用户。

配置 URL 过滤

哪里可以使用？	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)	☐ 高级 URL 过滤许可证（或旧版 URL 过滤许可证） 注意： • 旧版 *URL* 过滤许可证已停用，但仍支持有效的旧版许可证。 • Prisma Access 许可证包括 *Advanced URL Filtering* 功能。

熟悉 URL 过滤基础知识中的概念后，您就可以 开始使用 URL 过滤了。从激活 Advanced URL Filtering 许可证（如果适用）到测试您的配置，本章介绍了有效 URL 过滤部署所需的内容。为了充分利用部署，请遵循 URL 过滤最佳实践。

- 激活高级 URL 过滤许可证
- URL 过滤入门
- 配置 URL 过滤
- 配置内联分类
- URL 类别例外
- URL 过滤最佳实践
- 测试 URL 过滤配置

激活 Advanced URL Filtering 许可证

哪里可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Advanced URL Filtering 许可证（或旧版 URL 过滤许可证） 注意： • 旧版 *URL* 过滤许可证已停用，但仍支持有效的旧版许可证。 • Prisma Access 许可证包括 *Advanced URL Filtering* 功能。

Advanced URL Filtering 订阅可提供实时 URL 分析和恶意软件预防。除了 PAN-DB 访问（Palo Alto Networks 开发的用于高性能 URL 查找的 URL 过滤数据库），它还可以提供针对恶意 URL 和 IP 地址的防护。

新一代防火墙（虚拟和本地）、Strata Cloud Manager、Prisma Access (Managed by Panorama)、Cloud NGFW for AWS 和 Cloud NGFW for Azure 上提供 Advanced URL Filtering 功能。但是，新一代防火墙和 Cloud NGFW for Azure 需要 Advanced URL Filtering 订阅，而所有 Prisma Access 和 Cloud NGFW for AWS 许可证包括 Advanced URL Filtering 功能。

检查 Advanced URL Filtering 功能与每个支持 URL 过滤的 Palo Alto Networks 平台的兼容性，请查看 URL 过滤支持。

- Strata Cloud Manager
- PAN-OS 和 Panorama

激活高级 URL 过滤许可证 (Strata Cloud Manager)

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

切换到 **PAN-OS & Panorama**（**PAN-OS** 和 **Panorama**）选项卡，然后按照其中的指导激活许可证。

如果您使用的是 **Strata Cloud Manager**：

❑ 验证 URL 过滤许可证。

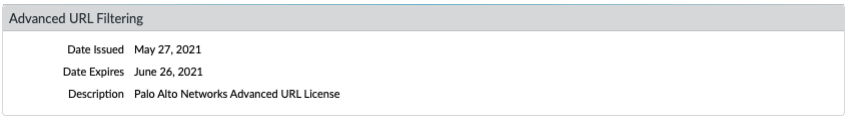
❑ 高级 URL 过滤入门。

激活高级 URL 过滤许可证（PAN-OS 和 Panorama）

STEP 1 | 获取并安装 Advanced URL Filtering 许可证。

Advanced URL Filtering 许可证包括对 *PAN-DB* 的访问；如果许可证过期，则防火墙将停止执行所有 *URL* 过滤功能、*URL* 类别实施和 *URL* 云查找。此外，在您安装有效许可证之前，所有其他基于云的更新都将无法运行。

1. 选择 **Device**（设备） > **Licenses**（许可证），然后在“许可证管理”部分中选择许可证安装方法：
   - **Retrieve license keys from license server**（从许可证服务器检索许可证密钥）
   - **Activate feature using authorization code**（使用授权代码激活功能）
2. 确认 Advanced URL Filtering 部分的 **Date Expires**（过期日期）字段显示了有效的日期。



当您激活 *Advanced URL Filtering* 许可证时，您的 *PAN-DB* 和 *Advanced URL Filtering* 的许可证权利可能无法在防火墙上正确显示 — 这属于显示例外，而非许可问题，不会影响对服务的访问。您可以使用以下 *CLI* 命令更新防火墙上的许可证以纠正显示问题：***request license fetch***。

STEP 2 | 下载并安装 PAN OS 的最新内容版本。PAN-OS 应用程序和威胁内容版本 8390-6607 及更高版本允许运行 PAN-OS 9.x 及更高版本的防火墙，以便识别已使用通过 Advanced URL Filtering 引入的实时检测类别进行分类的 URL。有关更新的详细信息，请参阅应用程序和威胁内容版本说明。您还可以在 Palo Alto Networks 支持门户上查看应用和威胁内容发布说明，或者直接在防火墙 Web 界面中查看：选择 **Device**（设备） > **Dynamic Updates**（动态更新），打开特定内容发布版本的发布说明。

更新至最新内容发布版本时，请遵循应用程序和威胁内容更新的最佳实践。

STEP 3 | 为防火墙制定应用程序和威胁的相关动态更新下载计划。

接收内容更新需要威胁防御许可证，其中涵盖抗病毒以及应用程序和威胁。

1. 选择**Device**（设备） > **Dynamic Updates**（动态更新）。
2. 在“应用程序和威胁”部分的“计划”字段中，单击 **None**（无）链接以计划定期更新。

如果防火墙拥有直接互联网访问权限，那么您只能计划动态更新。如果已在某个部分中计划过更新，那么链接文本会显示计划设置。

应用程序和威胁更新有时包含与强制执行安全搜索相关的 URL 过滤更新。

后续步骤：

1. 配置 URL 过滤配置文件以定义您组织的 Web 使用策略。
2. 测试您的 URL 过滤配置。

URL 过滤入门

哪里可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Advanced URL Filtering 许可证（或旧版 URL 过滤许可证） 注意： • 旧版 *URL* 过滤许可证已停用，但仍支持有效的旧版许可证。 • Prisma Access 许可证包括 *Advanced URL Filtering* 功能。

开始使用 URL 过滤的第一步是了解网络上用户的 Web 活动模式。

为了安全观察这些模式，我们建议：

- ❑ 查看 Palo Alto Networks 预定义的 URL 类别。
- ❑ 将 URL 输入到我们的测试 A 站点引擎中，以查看 PAN-DB 如何对其进行分类。
- ❑ 大多数时候，创建一个对大部分类别发出警报的被动 URL 过滤配置文件。当您为 URL 类别选择 `alert` 设置时，防火墙将记录该类别的通信。然后，您可以查看用户正在访问的站点，并为 URL 类别和特定站点决定适当的站点访问权限。

  对所有 *Web* 活动发出警报可能会产生大量日志文件。因此，您可能只希望将此操作作为初始部署的一部分。此时，您也可以通过启用 *URL* 过滤配置文件中的 ***Log container page only***（仅记录容器页面）选项来减少 *URL* 过滤日志，这样就只会记录与类别匹配的主页面，而非可能已在容器页面中加载的后续页面/类别。
- ❑ 阻止我们知道有错误的 URL 类别：恶意软件，命令和控制以及网络钓鱼。

- Strata Cloud Manager
- PAN-OS 和 Panorama

Advanced URL Filtering 入门 (Strata Cloud Manager)

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

切换到 ***PAN-OS & Panorama***（***PAN-OS*** 和 ***Panorama***）选项卡，然后按照其中的指导操作。

如果您正在使用 ***Strata Cloud Manager***，请在此处继续。

STEP 1 | 使用测试 A 站点检查 PAN-DB 如何对特定网站进行分类。

您也可以使用该平台为您认为分类有错误的任何网站请求更改分类。

STEP 2 | 创建对所有类别发出 *Alerts*（警报）的被动 URL 访问管理配置文件。

防火墙会为 URL 类别中具有除允许之外的操作的网站生成 URL 过滤日志条目。

1. 选择 **Manage**（管理） > **Configuration**（配置） > **Security Services**（安全服务） > **URL Access Management**（URL 访问管理）。
2. 在 URL 访问管理配置文件下，选中最佳实践配置文件旁的复选框，然后 **Clone**（克隆）该配置文件。

   克隆的配置文件会出现在名为 `best-practices-1` 的配置文件下。
3. 选择 **best-practices-1** 配置文件并重命名。例如，将其重命名为 `URL-Monitoring`。

STEP 3 | 对除恶意软件、命令与控制以及网络钓鱼之外的所有类别发出 **Alerts**（警报），这些类别应保持被阻止的状态。

1. 在 **Access Control**（访问控制）下，选择所有类别，然后排除 `Malware`（恶意软件）、`Command-and-Control`（命令与控制）以及 `Phishing`（网络钓鱼）。
2. 对于仍突出显示的类别，请单击 **Set Access**（设置访问权限），然后选择 **Alert**（警报）。
3. **Block**（阻止）访问 `Malware`（恶意软件）、`Command-and-Control`（命令与控制）和 `Phishing`（网络钓鱼），以及其他已知有危险的 URL 类别：
   - phishing
   - dynamic-dns
   - unknown
   - extremism
   - copyright-infringement
   - proxy-avoidance-and-anonymizers
   - newly-registered-domain
   - grayware
   - parked
4. **Save**（保存）配置文件。

STEP 4 | 将 URL 访问管理配置文件应用到安全策略规则，这些规则允许从信任区域中的客户端到 Internet 的通信。

仅当包含在安全策略规则引用的配置文件组中时，URL 访问管理配置文件才会处于活动状态。

按照步骤激活 URL 访问管理配置文件（和任何安全配置文件）。

确保您应用于 *URL* 访问管理配置文件的安全策略规则中的 *`Source Zone`* 设置为受保护的内部网络。

STEP 5 | **Push Config**（推送配置）以提交配置。

STEP 6 | 检查 URL 日志以了解用户正在访问哪些类别的网站。被阻止的网站也会被记录。

有关查看日志和生成报告的信息，请参阅监控 Web 活动。

选择 **Activity**（活动） > **Log Viewer**（日志查看器） > **URL**。URL 过滤报告会提供 24 小时内 Web 活动的视图。

STEP 7 | 后续步骤：

- 对于不允许或阻止的所有内容，请使用风险类别来根据网站安全性编写简单的策略。PAN-DB 按风险等级（高、中、低）分类每个 URL。虽然高风险和中风险站点未被证实是恶意的，但他们与恶意站点密切关联。例如，他们可能与恶意站点位于同一域中，或可能直到最近他们才托管有恶意内容。

  您可以采取预防措施限制高风险的用户交互站点，尤其是在您想授予用户访问存在安全隐患的站点之权限的某些情况下（例如，您可能想让开发人员使用开发者微博进行研究，但是，已知微博通常是托管恶意软件的类别。）
- URL 过滤与 User-ID 配对后，可对基于组织或部门的 Web 访问进行控制，并阻止将公司凭据提交至未经批准的站点：
  - URL 过滤根据站点类别检测公司凭据提交到站点的情况，从而防止凭据被盗。阻止用户将凭据提交到恶意和不受信任的站点、警告用户不要在未知站点输入公司凭据或警告用户不要在非公司站点重复使用公司凭据、并明确允许用户向公司站点提交凭据。
  - 使用被动 URL 访问管理配置文件添加或更新安全策略规则，使其适用于营销或工程等部门用户组。 监控部门活动，并向部门成员获得反馈，以了解对他们的工作至关重要的网络资源。
- 考虑所有利用 URL 过滤的方法来减小攻击面。例如，学校可能会使用 URL 过滤对学生强制执行严格安全搜索。或者，如果您有安全运营中心，则可能仅向威胁分析师提供密码访问权限，以便他们对受感染或有危险的站点进行研究。
- 请遵循 URL 过滤最佳实践。

Advanced URL Filtering 入门（PAN-OS 和 Panorama）

STEP 1 | 使用测试 A 站点检查 PAN-DB 如何对特定网站进行分类。

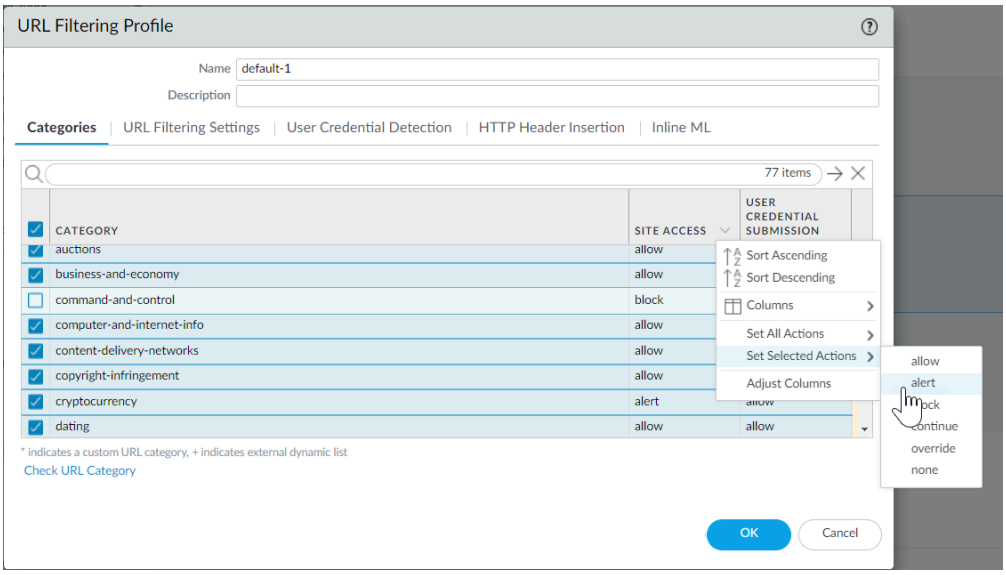
您也可以使用该平台为您认为分类有错误的任何网站请求更改分类。

STEP 2 | 创建被动 URL 过滤配置文件，该配置文件会对所有类别发出 *Alerts*（警报）。

1. 选择 **Objects**（对象） > **Security Profiles**（安全配置文件） > **URL Filtering**（**URL** 过滤）。
2. 选择默认配置文件，然后单击 **Clone**（克隆）。新的配置文件将命名为 **default-1**。
3. 选择 **default-1** 配置文件并重命名。例如，将其重命名为 URL-Monitoring。

STEP 3 | 除应保持阻止状态的恶意软件、命令和控制、以及网络钓鱼外，请将所有类别的操作配置为 **alert**（警报）。

1. 在列出所有 URL 类别的部分，选择所有类别，然后取消选择恶意软件、命令和控制以及网络钓鱼。
2. 在操作列标题右侧，鼠标悬停在上方并选择向下箭头，然后依次选择 **Set Selected Actions**（设置选定操作）和 **alert**（警报）。



3. **Block**（阻止）访问已知的危险 URL 类别。

   阻止访问恶意软件、网络钓鱼、动态 *DNS*、未知、命令和控制、极端主义、版权侵犯、回避代理和匿名者、新注册域、灰色软件以及寄放等 *URL* 类别。

4. 单击 **OK**（确定）保存配置文件。

STEP 4 | 将 URL 过滤配置文件应用于允许从信任区域中的客户端到 Internet 的通信的安全策略规则。

确保您添加 *URL* 访问管理配置文件的安全策略规则中的 *Source Zone* 设置为受保护的内部网络。

1. 选择 **Policies**（策略） > **Security**（安全）。然后，选择要修改的安全策略规则。
2. 在 **Actions**（操作）选项卡上，编辑“配置文件设置”。
3. 对于 **Profile Type**（配置文件类型），选择 **Profiles**（配置文件）。随即将显示配置文件列表。
4. 对于 **URL Filtering**（URL 过滤）配置文件，选择刚才创建的配置文件。
5. 单击 **OK**（确定）保存更改。

STEP 5 | **Commit**（提交）配置。

STEP 6 | 查看 URL 过滤日志以查看用户访问的所有网站类别。此外还会记录您已设为阻止的类别。

有关查看日志和生成报告的信息，请参阅监控 Web 活动。

选择 **Monitor**（监控） > **Logs**（日志） > **URL Filtering**（**URL** 过滤）。将会为 URL 过滤数据库中存在的所有网站创建日志条目，该数据库属于设置为任何操作（非 **allow**（允许））的类别。您可以通过 URL 过滤报告查看 24 小时内的 Web 活动。[**Monitor**（监控） > **Reports**（报告）]。

STEP 7 | 后续步骤：

- PAN-DB 最多可将每个 URL 分为四个类别，且每个 URL 都存在一个风险类别（高、中、低）。虽然高风险和中风险站点未被证实是恶意的，但他们与恶意站点密切关联。例如，他们可能与恶意站点位于同一域中，或可能直到最近他们才托管有恶意内容。对于您不允许或阻止的任何事件，可以使用风险类别，根据网站安全性写入简单的策略规则。

  您可以采取预防措施限制高风险的用户交互站点，尤其是在您想授予用户访问存在安全隐患的站点之权限的某些情况下（例如，您可能想让开发人员使用开发者微博进行研究，但是，已知微博通常是托管恶意软件的类别。）

- URL 过滤与 User-ID 配对后，可对基于组织或部门的 Web 访问进行控制，并阻止将公司凭据提交至未经批准的站点：

  - URL 过滤根据站点类别检测公司凭据提交到站点的情况，从而防止凭据被盗。阻止用户将凭据提交到恶意和不受信任的站点、警告用户不要在未知站点输入公司凭据或警告用户不要在非公司站点重复使用公司凭据、并明确允许用户向公司站点提交凭据。
  - 使用被动 URL 过滤配置文件添加或更新安全策略规则，以便将其应用到市场部或工程部等部门用户组，导航路径为 **Policies**（策略） > **Security**（安全） > **User**（用户）。监视部门活动，获得部门成员反馈，从而了解对部门工作必不可少的 Web 资源。

- 考虑所有利用 URL 过滤的方法来减小攻击面。例如，学校可能会使用 URL 过滤对学生强制执行严格安全搜索。或者，如果您有一个安全运营中心，则可能仅授予威胁分析师密码访问权限，以便他们研究已遭到入侵或有危险的站点。
- 请遵循 URL 过滤最佳实践。

配置 URL 过滤

哪里可以使用？	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)	❑ 高级 URL 过滤许可证（或旧版 URL 过滤许可证） 注意： • 旧版 *URL* 过滤许可证已停用，但仍支持有效的旧版许可证。 • Prisma Access 许可证包括 *Advanced URL Filtering* 功能。

在规划 URL 过滤部署后，您应该对用户正在访问的网站类型有了基本的了解。请使用此信息创建 URL 过滤配置文件，定义防火墙如何处理指向特定 URL 类别的流量。您还可以限制用户可提交公司证书的网站或强制执行严格的安全搜索。要激活这些设置，请将 URL 过滤配置文件应用于允许 Web 访问的安全策略规则。

- Strata Cloud Manager
- PAN-OS 和 Panorama

配置 URL 过滤 (Strata Cloud Manager)

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

切换到 ***PAN-OS & Panorama***（***PAN-OS*** 和 ***Panorama***）选项卡，然后按照其中的指导操作。

如果您正在使用 ***Strata Cloud Manager***，请在此处继续。

URL 过滤在 Strata Cloud Manager 中称为*URL* 访问管理

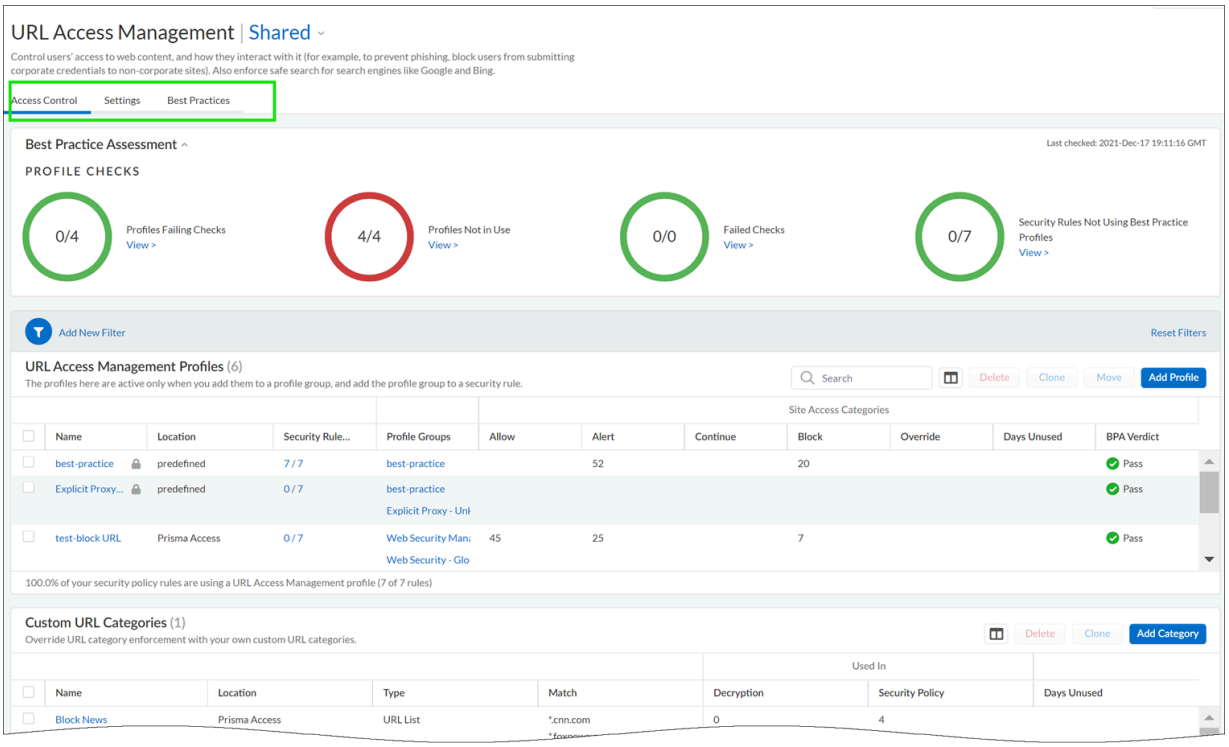
STEP 1 | 检查您的 Prisma Access 订阅是否包含高级 URL 过滤。

- 转至“管理”>“服务设置”>“概述”>“许可证”，以确认您的订阅中包含的功能。

STEP 2 | 浏览 URL 访问管理指示板。

转到 **Manage**（管理）> **Configuration**（配置）> **Security Services**（安全服务）> **URL Access Management**（**URL** 访问管理）。

浏览 **Access Control**（访问控制）、**Settings**（设置）和 **Best Practices**（最佳实践）选项卡，探索可用的 URL 过滤功能。



STEP 3 | 查看和自定义“常规 URL 过滤设置”。

在指示板上，转到 **Settings**（设置），查看适用于您的 Prisma Access 环境的默认 URL 过滤设置，包括：

- URL 过滤超时和查找设置
- 某些管理员的 URL 过滤覆盖
- URL 过滤响应页面
- 远程浏览器隔离 (RBI) 设置

自动向自定义 ***URL*** 类别或外部动态列表中的 ***URL*** 附加结束令牌

（*PAN-OS 10.1* 及更低版本）如果您将 *URL* 添加到 *URL* 列表类型的自定义 *URL* 类别或外部动态列表 *(EDL)*，并且不在末尾添加斜杠 *(/)*，则可能阻止或允许超出预期的的网址数量。例如，如果输入 ***example.com*** 而不是 ***example.com/***，则会将匹配的 *URL* 会扩展到 *example.com.website.info* 或 *example.com.br*。*Prisma Access* 可以自动为自定义 *URL* 类别或 *EDL* 中的网址添加末尾的斜线，这样，如果您输入 ***example.com***，则 *Prisma Access* 会将其视为 ***example.com/*** 进行处理，也就是说，只考虑该域及其子目录匹配。转到 ***Settings***（设置） ***> General Settings***（常规设置），并启用 ***Append End Token to Entries***（将结束令牌添加到条目）选项。

（*PAN-OS 10.2* 及更高版本）*Prisma Access* 会自动在域条目中添加末尾的斜杠。

您可以为每种部署类型（移动用户、远程网络或服务连接）自定义这些设置。

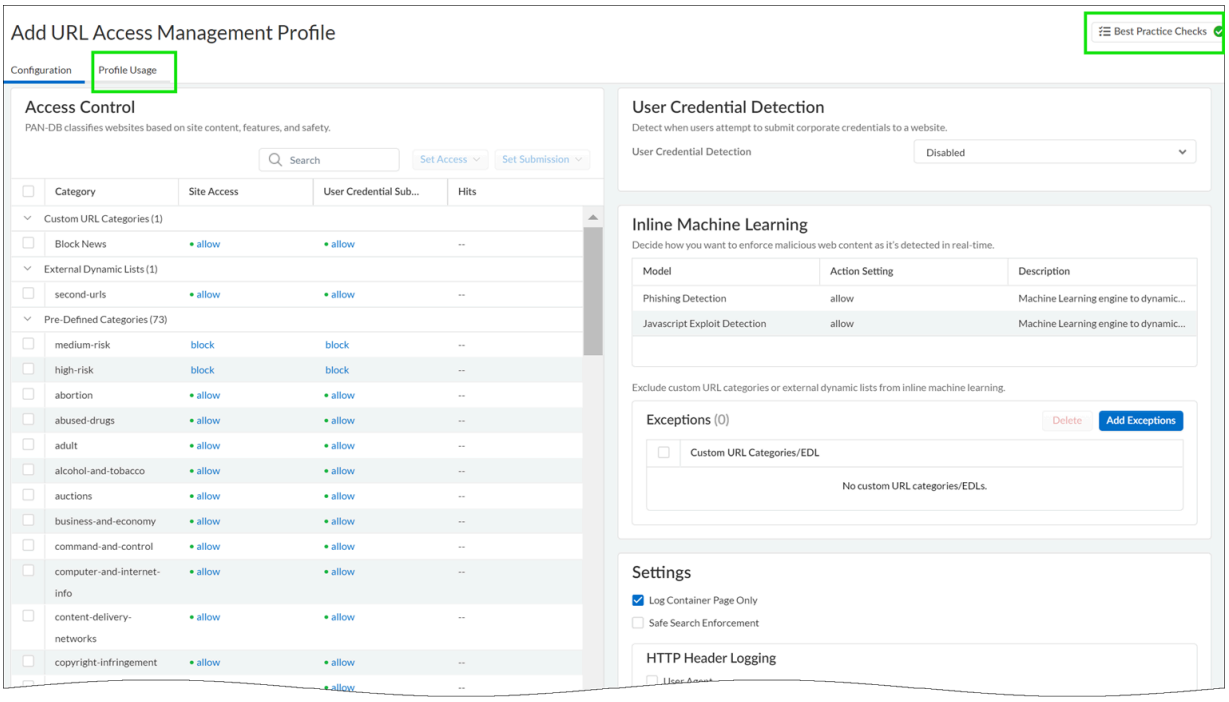
STEP 4 | 创建 URL 访问管理配置文件。

在 URL 访问管理指示板上，**Add Profile**（添加配置文件）并继续指定 Web 访问设置：

- **Access Control**（访问控制）显示您可以为其定义 Web 访问权限和使用策略的 URL 类别和列表。默认情况下，所有类别的 **Site Access**（站点访问）和 **User Credential Submission**（用户凭据提交）权限设置为 **Allow**（允许）。
- 对于每个 URL 类别，配置 **User Credential Detection**（用户凭据检测），从而使用户只能向指定 URL 类别的网站提交证书。
- 启用 **Safe Search Enforcement**（强制执行安全搜索），以便强制执行严格的安全搜索过滤。
- 启用 **Log Container Page Only**（仅记录容器页面），以便仅记录与指定内容类型匹配的 URL。
- 启用 **HTTP Header Logging**（**HTTP** 标头日志记录），则可以查看 HTTP 请求中发送到服务器的属性。
- 使用 **Advanced URL Inline Categorization**（高级 **URL** 内联分类），以便启用和配置实时网页分析和管理 URL 例外。
  - **Enable local Inline Categorization**（启用本地内联分类）— 使用机器学习模型对 URL 流量进行实时分析，以检测和防止恶意网络钓鱼变体和 JavaScript 漏洞进入您的网络。
  - **Enable cloud inline categorization**（启用云内联分类）— 使用基于机器学习的检测器对本地内联 ML 使用的分析引擎进行补充，将可疑网页内容转发到云进行补充分析，从而对 URL 进行实时分析。
  - 您可以为特定网站定义 URL **Exceptions**（例外），将其排除在内联 ML 操作之外。

请注意：

- 配置文件中内置了最佳实践检查功能，可以实时评估您的配置。
- 启用配置文件后，您可以检查配置文件的使用情况，以查看是否有任何安全策略规则引用该配置文件。



STEP 5 | 将 URL 访问管理配置文件应用到安全策略规则。

仅当包含在安全策略规则引用的配置文件组中时，URL 访问管理配置文件才处于活动状态。

按照步骤激活 URL 访问管理配置文件（和任何安全配置文件）。请确保 **Push Config**（推送配置）

配置 URL 过滤（PAN-OS 和 Panorama）

STEP 1 | 创建 URL 过滤配置文件。

如果尚未执行该操作，请配置最佳实践 URL 过滤配置文件，以确保 *URL* 不受托管恶意软件或破坏性内容的攻击。

选择 **Objects**（对象） > **Security Profiles**（安全配置文件） > **URL Filtering**（**URL** 过滤），并 **Add**（添加）URL 过滤配置文件。

STEP 2 | 为每个 URL 类别定义站点访问。

选择 **Categories**（类别），并为每个 URL 类别设置站点访问：

- **allow**（允许）发往该 URL 类别的流量；允许流量未被记录。
- 选择 **alert**（警报）以查看用户访问的网站。允许与此类别匹配的流量，但应生成 URL 过滤日志以记录用户访问此类别中站点的时间。
- 选择 **block**（阻止）以拒绝访问与此类别匹配的流量，并启用已阻止流量的日志记录。
- 选择 **continue**（继续）可以向带有警告的用户显示一个页面，并要求他们单击 **Continue**（继续）以继续进入此类别的站点。
- 如仅允许在用户有提供配置密码的情况下进行访问，请选择 **override**（替代）。更多详细信息，请参阅允许密码访问某些站点。

STEP 3 | 配置 URL 过滤配置文件以检测提供给允许的 URL 类别的网站的公司凭据。

即使启用相应类别中的检查，防火墙仍会自动跳过检查与从未出现托管恶意软件或破坏性内容的站点相关的任何 *App-ID™* 凭据提交情况，以确保最佳性能和低误报率。防火墙跳过凭据检查的站点列表通过应用程序和威胁内容更新自动更新。

1. 选择 **User Credential Detection**（用户凭据检测）。
2. 从 **User Credential Detection**（用户凭据检测）下拉列表的网页中选择一个检查公司凭据提交方法：
   - **Use IP User Mapping**（使用 **IP** 用户映射）— 检查有效的公司用户名提交，并验证用户名是否与登录至会话源 IP 地址的用户相匹配。防火墙根据其 IP 地址到用户名的映射表匹配提交的用户名。您可使用将 IP 地址映射到用户中描述的任何用户映射方法。
   - **Use Domain Credential Filter**（使用域凭据过滤器）— 检查有效的公司用户名和密码提交，并验证用户名是否映射到用户登录的 IP 地址。有关如何设置 User-ID 以启用此方法的说明，请参阅使用基于 Windows 的 User-ID 代理配置凭据检测。
   - **Use Group Mapping**（使用组映射）— 当防火墙配置为将用户映射到组时，根据用户到组映射表检查有效的用户名提交。

     使用组映射，您可以将凭据检测应用于目录的任何部分或特定组，例如可以访问最敏感应用程序的 IT 组。

     在用户名结构不是唯一的环境中，这种方法容易产生误报，因此，应仅使用此方法保护高价值用户账户。
3. 设置防火墙用于记录公司凭据提交检测的 **Valid Username Detected Log Severity**（有效用户名检测到的日志严重性）（默认为中等）。

STEP 4 | 配置 URL 过滤配置文件，以使用本地内联分类实时检测网络钓鱼和恶意 JavaScript。

STEP 5 | 允许或阻止用户根据 URL 类别将公司凭据提交到站点，以便阻止凭据网络钓鱼。

即使启用相应类别中的检查，防火墙仍会自动跳过检查与从未出现托管恶意软件或破坏性内容的站点相关的 *App-ID* 凭据提交情况，以确保最佳性能和低误报率。防火墙跳过凭据检查的站点列表通过应用程序和威胁内容更新自动更新。

1. 对于允许 **Site Access**（站点访问）的每个 URL 类别，选择要处理 **User Credential Submissions**（用户凭据提交）的方法：
   - **Alert**（警报）— 允许用户向站点提交凭据，但每次用户在该 URL 类别中向站点提交凭据时生成 URL 过滤警报日志。
   - **Allow**（允许）（默认）— 允许用户向网站提交凭据。
   - **Block**（阻止）— 显示防网络钓鱼阻止页面，以阻止用户将凭据提交到网站。
   - **Continue**（继续）— 显示防网络钓鱼继续页面，要求用户单击 **Continue**（继续）以访问网站。
2. 配置 URL 过滤配置文件以检测向允许的 URL 类别中的网站提交的公司凭据。

STEP 6 | 定义 URL 类别例外以指定不管 URL 类别如何，应始终阻止或允许的网站。

例如，要减少“URL 过滤”日志，您可能想将公司网站加入到允许列表中，这样，这些站点就不会生产任何日志；或者，如果某个与工作无关的网站使用极度频繁，您可以将此站点添加到阻止列表。

为自定义 URL 类别配置的策略操作优先于外部动态列表中的匹配 URL。

无论相关类别的操作怎样，都将始终阻止阻止列表中的网站流量，始终允许允许列表中的 URL 流量。

有关格式和通配符正确使用方法的详细信息，请参阅 URL 类别例外列表。

STEP 7 | 启用 Safe Search Enforcement（强制执行安全搜索）。

STEP 8 | 对于 URL 过滤事件，仅记录用户访问的页面。

1. 选择 **URL Filtering Settings**（**URL** 过滤设置）并启用 **Log container page only**（仅记录容器页面）（默认），以便防火墙只记录与此类别匹配的主页面，而非已在容器页面中加载的后续页面或类别。
2. 要为所有页面和类别启用日志记录，请禁用 **Log container page only**（仅记录容器页面）选项。

STEP 9 | 为一个或多个受支持 HTTP 标头字段启用 HTTP 标头日志记录。

选择 **URL Filtering Settings**（**URL** 过滤设置），然后选择一个或多个以下字段进行记录：

- **User-Agent**（用户代理）
- **Referer**（推荐人）
- **X-Forwarded-For**

STEP 10 | 保存 URL 过滤配置文件。

单击 **OK**（确定）。

STEP 11 | 将 URL 过滤配置文件应用于允许从信任区域中的客户端到 Internet 的通信的安全策略规则。

请确保在安全策略规则中添加 *URL* 过滤配置文件的 *Source Zone* 设置为受保护的内部网络。

1. 选择 **Policies**（策略） > **Security**（安全）。然后，选择要修改的安全策略规则。
2. 在 **Actions**（操作）选项卡上，编辑“配置文件设置”。
3. 对于 **Profile Type**（配置文件类型），选择 **Profiles**（配置文件）。随即将显示配置文件列表。
4. 对于 **URL Filtering**（**URL** 过滤）配置文件，选择刚才创建的配置文件。
5. 单击 **OK**（确定）保存更改。

STEP 12 | **Commit**（提交）配置。

STEP 13 | 测试您的 URL 过滤配置。

STEP 14 | （最佳实践）在防火墙执行 URL 类别查找时，启用 **Hold client request for category lookup**（保持客户端类别查找请求）以阻止客户端请求。

1. 选择 **Device**（设备） > **Setup**（设置） > **Content - ID**（内容 **ID**）。
2. 选择 **Hold client request for category lookup**（保持客户端类别查找请求）。
3. **Commit**（提交）更改。

STEP 15 | 设置 URL 类别查找超时之前的时间量，以秒计。

1. 选择 **Device**（设备） > **Setup**（设置） > **Content-ID** > **gear icon**（齿轮图标）。
2. 输入 **Category lookup timeout (sec)**（类别查找超时（秒））的秒数。
3. 单击 **OK**（确定）。
4. **Commit**（提交）更改。

配置内联分类

哪里可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Advanced URL Filtering 许可证（或旧版 URL 过滤许可证） 注意： • 旧版 *URL* 过滤许可证已停用，但仍支持有效的旧版许可证。 • Prisma Access 许可证包括 *Advanced URL Filtering* 功能。

要启用内联分类，请将配置有内联分类设置的“URL 过滤”配置文件附加到安全策略规则（参阅设置基本安全策略）。

VM-50 或 *VM50L* 虚拟设备当前不支持“*URL* 过滤”本地内联分类。

- Strata Cloud Manager
- PAN-OS 和 Panorama

配置内联分类 (Strata Cloud Manager)

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

切换到 ***PAN-OS & Panorama***（***PAN-OS*** 和 ***Panorama***）选项卡，然后按照其中的指导操作。

如果您正在使用 ***Strata Cloud Manager***，请在此处继续。

STEP 1 | 更新或创建 URL 访问管理配置文件。

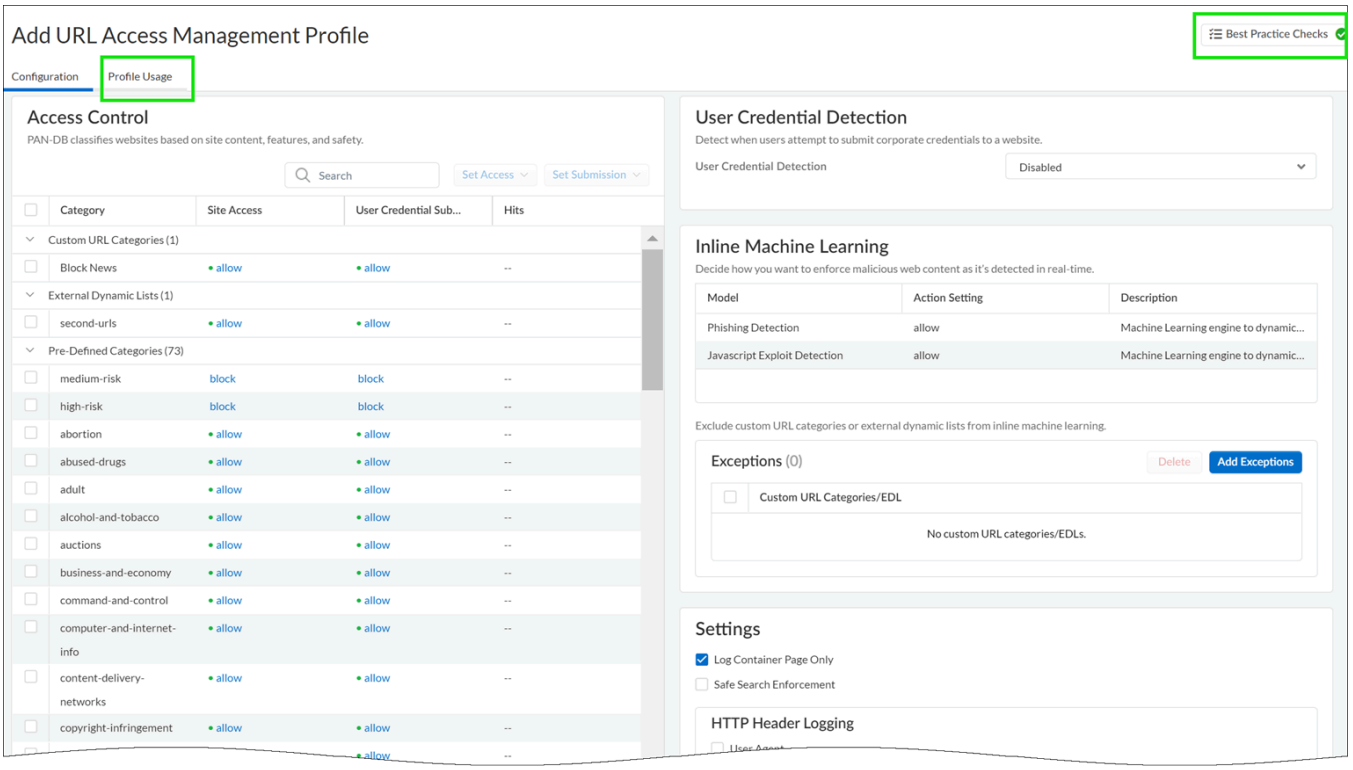
1. 转到 **Manage**（管理）> **Configuration**（配置）> **Security Services**（安全服务）> **URL Access Management**（URL 访问管理）。
2. 在 URL 访问管理指示板上，选择 URL 访问管理配置文件或 **Add Profile**（添加配置文件）。

   如果您创建新的配置文件，请在配置文件中配置设置，例如 URL 类别的网站访问权限 [**Access Control**（访问控制）]。配置 URL 过滤（云管理）介绍了可用设置。
3. 在 **Advanced URL Inline Categorization**（高级 URL 内联分类）下，选择一种内联分类类型。

   这两个选项都支持实时网页分析和 URL 例外管理。

   - **Enable cloud inline categorization**（启用云内联分类）— 使用基于机器学习的检测器对本地内联 ML 使用的分析引擎进行补充，将可疑网页内容转发到云进行补充分析，从而对 URL 进行实时分析。

- **Enable local Inline Categorization**（启用本地内联分类）— 使用机器学习模型对 URL 流量进行实时分析，以检测和防止恶意网络钓鱼变体和 JavaScript 漏洞进入您的网络。
- 您还可以定义 URL **Exceptions**（例外），将特定网站排除在内联 ML 操作之外。



4. **Save**（保存）配置文件。

STEP 2 | 将 URL 访问管理配置文件应用到安全策略规则。

要激活 URL 访问管理配置文件（以及任何安全配置文件），请将其添加到 `profile group`，并在安全策略规则中引用该配置文件组。

配置内联分类（PAN-OS 和 Panorama）

在 *PAN-OS 10.2* 中，*URL* 过滤内联 *ML* 功能已重命名为内联分类。因此，*PAN-OS 10.1* 任务使用短语“*URL* 过滤内联 *ML*”，而 *PAN-OS 10.2* 及更高版本任务使用“内联分类”。有关详细信息，请查看 PAN-OS 10.2 升级/降级注意事项中的 *URL* 过滤内联 *ML* 条目。

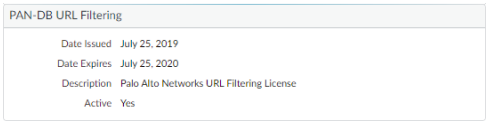
- PAN-OS 10.1
- PAN-OS 10.2 及更高版本

配置内联分类（**PAN-OS 10.1**）

STEP 1 | 登录 PAN-OS Web 界面。

STEP 2 | 确认您拥有有效的旧版 URL 过滤或高级 URL 过滤订阅。

选择 **Device**（设备） > **Licenses**（许可证），并确认 URL 过滤许可证可用且未过期。

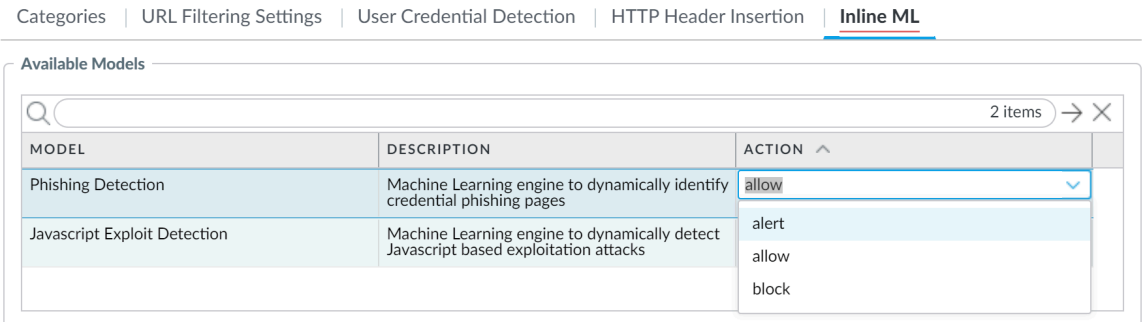


STEP 3 | 在 URL 过滤配置文件中配置 URL 过滤内联 ML 设置。

1. 选择 **Objects**（对象） > **Security Profiles**（安全配置文件） > **URL Filtering**（URL 过滤），然后 **Add**（添加）或选择一个 URL 过滤配置文件。
2. 选择 **Inline ML**（内联 ML），并定义每个内联 ML 模型的 **Action**（操作）。

   对于每种类型的恶意网页内容，有两个分类引擎可用：**Phishing**（网络钓鱼）和 **JavaScript Exploit**（**JavaScript** 漏洞利用）。

   - 阻止 — 防火墙检测网页上的网络钓鱼内容时，会生成 URL 过滤日志条目。
   - 警报 — 防火墙允许访问网站，但还是会生成 URL 过滤日志条目。
   - 允许— 防火墙允许访问网站，但不生成 URL 过滤日志条目。



3. 单击 **OK**（确定）保存更改。
4. **Commit**（提交）更改。

STEP 4 | （可选）如果遇到误报，请将 URL 例外添加到 URL 过滤配置文件中。

您还可以在 URL 过滤配置文件中指定外部动态列表，或者从 URL 过滤日志中添加网页条目到自定义 URL 类别，从而添加例外。

1. 选择 **Objects**（对象） **> Security Profiles**（安全配置文件） **> URL Filtering**（**URL** 过滤）。
2. 选择要排除特定 URL 的 URL 过滤配置文件，然后选择 **Inline ML**（内联 **ML**）。
3. **Add**（添加）预先存在的 URL 类型的外部动态列表。如果没有可用列表，请创建一个新的外部动态列表。
4. 单击 **OK**（确定）保存更改。
5. **Commit**（提交）更改。

从 URL 过滤日志条目添加文件例外。

1. 选择 **Monitor**（监控） **> Logs**（日志） **> URL Filtering**（**URL** 过滤），并使用内联 ML 判定 **malicious-javascript**（恶意 **javascript**）或 **phishing**（网络钓鱼）过滤日志中的URL 条目。为要创建例外的 URL 选择一个 URL 过滤日志。
2. 转到 **Detailed Log View**（详细日志视图），然后向下滚动至 **Details**（详细信息）窗格，并选择 **Inline ML Verdict**（**Inline ML** 判定）旁边的 **Create Exception**（创建例外）。
3. 选择自定义 URL 例外类别，然后单击 **OK**（确定）。

   新的 URL 例外将添加到 **Objects**（对象） **> Custom Objects**（自定义对象） **> URL Category**（**URL** 类别）下的列表中。

STEP 5 | （可选）检验防火墙与内联 ML 云服务的连接状态。

在防火墙上使用以下 CLI 命令查看连接状态。

```
show mlav cloud-status
```

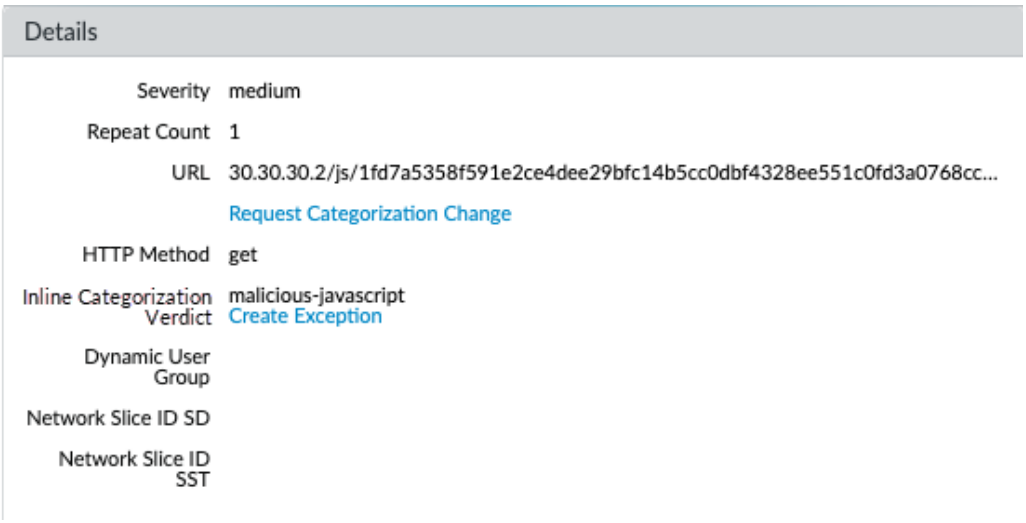
例如：

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

如果您无法连接到内联 ML 云服务，请验证 ML 域 ml.service.paloaltonetworks.com 是否未被阻止。

STEP 6 | 测试 URL 过滤部署。

要查看已使用 URL 过滤内联 ML 处理过的网页的相关信息，请根据 **Inline ML Verdict**（**Inline ML** 判定）过滤日志，导航路径为 **Monitor**（监控） **> Logs**（日志） **> URL Filtering**（**URL** 过滤）。已判定为包含危险的网页将按 **phishing**（网络钓鱼） 或 **malicious-javascript**（恶意 **javascript**）判定进行分类。例如：



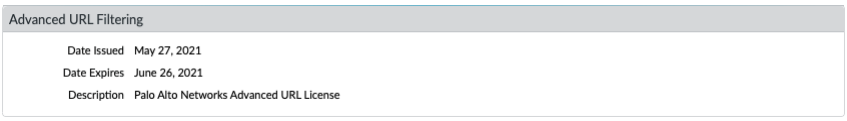
配置内联分类（PAN-OS 10.2 及更高版本）

STEP 1 | 登录 PAN-OS Web 界面。

STEP 2 | 要利用内联分类，您必须拥有有效的高级 URL 过滤订阅。

如果您有旧版 *URL* 过滤订阅，则可以启用本地内联分类。

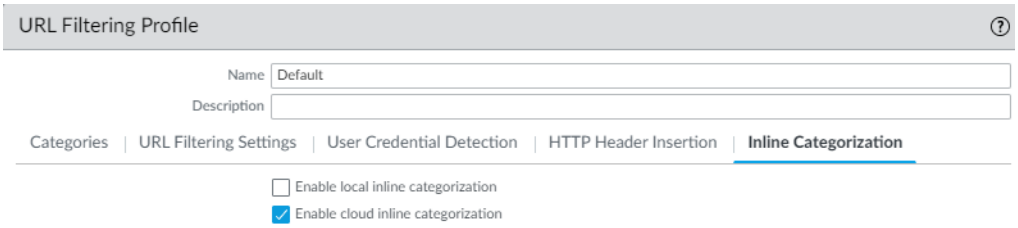
确认您是否有“高级 URL 过滤”订阅。若要检查您是否拥有当前有效的许可证订阅，请选择 **Device**（设备） > **Licenses**（许可证），确认是否有相应的许可证以及许可证是否已过期。



STEP 3 | 更新或创建新的 URL 过滤配置文件以启用云内联分类。

本地和云内联分类使用的策略操作取决于 ***Categories***（类别）选项卡中配置的设置。

1. 选择现有 **URL Filtering Profile**（URL 过滤配置文件）或 **Add**（添加）一个新的配置文件，导航路径为 **Objects**（对象） > **Security Profiles**（安全配置文件） > **URL Filtering**（URL 过滤）。
2. 选择 URL 过滤配置文件，然后转到 **Inline Categorization**（内联分类）并启用您要部署的内联分类方法。
   - **Enable cloud inline categorization**（启用云内联分类）— 一种基于云的内联深度学习引擎，可实时分析可疑网页内容，以保护用户免受零日网络攻击，包括针对性的网络钓鱼攻击和其他使用高级规避技术的网络攻击。
   - **Enable local inline categorization**（启用本地内联分类）— 基于防火墙的检测引擎，使用机器学习技术来防御 JavaScript 漏洞的恶意变体和嵌入网页中的网络钓鱼攻击。



3. 单击 **OK**（确定）并 **Commit**（提交）更改。

STEP 4 | （可选）如果遇到误报，请将 URL 例外添加到 URL 过滤配置文件中。可以通过在 URL 过滤配置文件中指定外部动态列表或自定义 URL 类别列表来添加例外。指定的例外适用于云和本地内联分类。

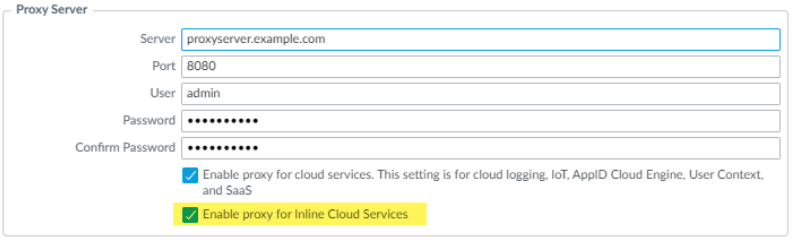
通过将条目添加到自定义 *URL* 类别（***Objects***（对象） > ***Custom Objects***（自定义对象） > ***URL Category***（***URL*** 类别））的其他机制创建的 *URL* 例外也可以用作内联分类的例外。

1. 选择 **Objects**（对象） > **Security Profiles**（安全配置文件） > **URL Filtering**（URL 过滤）。
2. 选择您想要排除特定 URL 的 URL 过滤配置文件，然后选择 **Inline Categorization**（内联分类）。
3. 单击 **Add**（添加），以选择一个预先存在的基于 URL 的外部动态列表或自定义 URL 类别。如果没有列表或类别可用，请分别创建一个新的外部动态列表或自定义 URL 类别。
4. 单击 **OK**（确定）以保存 URL 过滤配置文件，并 **Commit**（提交）更改。

STEP 5 | （当防火墙已部署显式代理服务器时必需）配置用于访问服务器的代理服务器，以便处理所有配置的内联云分析功能生成的请求。可以指定单个代理服务器，并将其应用于所有 Palo Alto Networks 更新服务，包括所有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**（为内联云服务启用代理）。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六个字符。

   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六个字符。

   3. 使用以下 CLI 命令，使代理服务器可以向内联云服务服务器发送请求：

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

   4. 使用以下 CLI 命令查看内联云服务的代理支持的当前运行状态：

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

      例如：

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

STEP 6 | （可选）设置防火墙用来处理内联分类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：

- 美国 — **us.hawkeye.services-edge.paloaltonetworks.com**
- 欧洲 — **eu.hawkeye.services-edge.paloaltonetworks.com**
- 英国 — **uk.hawkeye.services-edge.paloaltonetworks.com**

  英国云内容 *FQDN* 通过连接到位于欧盟的后端服务来提供高级 *URL* 过滤内联分类服务支持 *(eu.hawkeye.services-edge.paloaltonetworks.com)*。
- 亚太地区 — **apac.hawkeye.services-edge.paloaltonetworks.com**

STEP 7 | （可选）检查防火墙与内联分类服务器的连接状态。

1. ml.service.paloaltonetworks.com 服务器为与云操作和本地内联分类相关的基于防火墙的组件提供定期更新。

   在防火墙上使用以下 CLI 命令查看连接状态。

   ```
   show mlav cloud-status
   ```

   例如：

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

   如果无法连接到内联 ML 云服务，请检查以下域是否被阻止：ml.service.paloaltonetworks.com。

2. 云内联分类使用 hawkeye.services-edge.paloaltonetworks.com 服务器处理服务请求。

   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 URL 过滤云服务，请确认以下域是否被阻止：hawkeye.services-edge.paloaltonetworks.com。

STEP 8 | 安装用于向高级 URL 过滤云服务进行身份验证的更新防火墙设备证书。对为云内联分类启用的所有防火墙重复此操作。

STEP 9 | 测试 URL 过滤部署。

URL 类别例外

哪里可以使用？	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)	❑ 高级 URL 过滤许可证（或旧版 URL 过滤许可证） 注意： • 旧版 *URL* 过滤许可证已停用，但仍支持有效的旧版许可证。 • Prisma Access 许可证包括 *Advanced URL Filtering* 功能。

您可以将特定网站排除在 URL 类别实施之外，以确保无论与其 URL 类别关联的策略操作如何，都将阻止或允许这些网站。例如，您可能会阻止社交网络 URL 类别，但允许访问 LinkedIn。为 URL 类别策略的实施创建例外情况：

- 将要阻止或允许的网站的 IP 地址或 URL 添加到 **URL List**（**URL** 列表）类型的自定义 URL 类别中。然后，在 URL 过滤配置文件中定义该类别的站点访问。最后，将配置文件附加到安全策略规则。

  您还可以在安全策略规则中使用自定义 *URL* 类别作为匹配条件。确保将例外规则置于任何阻止或允许 *URL* 例外所属的类别的规则之上。
- 将要阻止或允许的网站的 URL 添加到 **URL List**（**URL** 列表）类型的 外部动态列表中。然后，在 URL 过滤配置文件中使用外部动态列表或作为安全策略规则中的匹配条件。使用外部动态列表的好处是，您无需在防火墙上执行配置更改或提交即可更新列表。

不要将 ***URL List***（***URL*** 列表）类型的外部动态列表与域列表的外部动态列表或 IP 地址列表类型混淆。虽然 *URL* 的外部动态列表允许域和 *IP* 地址，但反之则不然，会导致条目无效。

- URL 类别例外指南
- 创建自定义 URL 类别
- 使用 URL 过滤配置文件中的外部动态列表

URL 类别例外指南

哪里可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager)	❑ 高级 URL 过滤许可证（或旧版 URL 过滤许可证） 注意： • 旧版 *URL* 过滤许可证已停用，但仍支持有效的旧版许可证。

哪里可以使用？	需要提供什么？
• NGFW (Managed by PAN-OS or Panorama)	• Prisma Access 许可证包括 *Advanced URL Filtering* 功能。

以下指南介绍了如何填充 URL 类别例外列表 — 自定义 URL 类别或 URL 的外部动态列表：我们提供了有关如何使用通配符和特定条目的示例。

URL 类别例外列表的基本指南

在将条目添加到 URL 类别例外列表之前，请考虑该条目可能有的匹配项。以下指南介绍了如何创建阻止或允许您想要访问的网站和页面的条目。

防火墙默认自动将尾斜杠 (/) 附加到不以尾斜杠 (/) 或星号 (*) 结尾的域条目。添加尾斜杠会更改防火墙认为匹配并对其实施策略的 URL。在非通配符域条目中，尾斜杠会限制与给定域及其子目录匹配。例如，**example.com**（处理后的 **example.com/**）与自身和 **example.com/search** 相匹配。

在通配符域条目（带星号或插入符号的条目）中，尾斜杠限制与符合指定模式的 URL 相匹配。例如，要匹配条目 ***.example.com**，URL 必须至少包含一个子域名并以根域 **example.com** 结尾。具体模式为：**<subdomain>.example.com**；**news.example.com** 是匹配项，但 **example.com** 不是，因为它缺少子域名。

我们建议您手动添加尾斜杠，以向检查该条目的人员阐明该条目的预期匹配行为。如果尾斜杠是由防火墙添加，则该尾斜杠不可见。

运行 PAN-OS® 10.2 的 Panorama™ 管理服务器只能为同一软件版本的防火墙启用此功能。要为运行 PAN-OS 10.1 或更早版本的防火墙启用此功能，请在每个防火墙上使用以下 CLI 命令：

```
admin@PA-850> debug device-server append-end-token on
```

```
admin@PA-850> configure
```

```
admin@PA-850# commit
```

要禁用此功能，请选择 **Device**（设备）> **Setup**（设置）> **Content-ID** > **URL Filtering**（URL 过滤）。然后，取消选择 **Append Ending Token**（附加结束令牌）。但是，如果禁用此功能，则可能会阻止或允许访问超出预期数量的 URL。对于不以 / 或 * 结尾的域条目，防火墙将在其末尾添加隐式星号。例如，如果您将 **example.com** 添加到允许的网站的 URL 列表中，防火墙会将该条目解释为 **example.com.***。因此，防火墙允许访问诸如 **example.com.domain.xyz** 之类的站点。URL 类别例外（PAN-OS 10.1 及更早版本）描述了禁用此功能时防火墙的行为。

- 列表条目不区分大小写。
- 忽略 URL 条目中的 `http` 和 `https`。
- 每个 URL 条目的最大长度为 255 个字符。

- 输入与要阻止或允许的 IP 地址或 URL 完全匹配的内容，或者使用通配符创建模式匹配。

  不同的条目会导致不同的完全匹配项。如果您输入特定网页 (***example.com/contact***) 的 URL，则防火墙会限制仅与该网页匹配。完全匹配域会将匹配限制为域本身及其子目录。
- 如果原始条目可以通过多个 URL 访问，请考虑将最常用于访问网站或网页的 URL 添加到例外列表（例如 **blog.paloaltonetworks.com** 和 **paloaltonetworks.com/blog**）中。
- 条目 **example.com** 与 **www.example.com** 不同。虽然二者的域名相同，但第二个条目包含 *www* 子域。

Palo Alto Networks 不支持在自定义 *URL* 类别或外部动态列表条目中使用正则表达式。您必须知道特定 *URL*，或必须使用通配符和以下字符构造要匹配的 *URL* 模式：**. / ? & = ; +**。

URL 类别例外列表的通配符指南

您可以在 URL 类别例外列表中使用星号 (*) 和插入符号 (^) 来配置单个条目，从而匹配多个子域、域、顶级域 (TLD) 或页面，而无需指定具体的 URL。

如何使用星号 (*) 和插入符号 (^) 通配符

以下字符为令牌分隔符：**. / ? & = ; +**。由一个或两个这种字符分隔的每个字符串就是一个令牌。使用通配符作为令牌占位符，表明特定令牌可以包含任何值。在 **docs.paloaltonetworks.com** 条目中，令牌为“docs”、“paloaltonetworks”和“com”。

下表描述了星号和插入符号的工作原理并提供了示例。

*	^
表示一个或多个可变子域、域、TLD 或子目录。 可以在尾斜杠后使用星号，例如 **example.com/***。 例如：***.domain.com** 与 **docs.domain.com** 和 **abc.xyz.domain.com** 匹配。	表示一个可变的子域、根域或 TLD。 不能在尾斜杠后使用插入符号。以下条目无效：**example.com/^**。 例如：**^.domain.com** 与 **docs.domain.com** 和 **blog.domain.com** 匹配。
：星号比插入符号匹配的 URL 范围更大。星号对应任意数量的连续令牌，而插入符号恰好对应一个令牌。 类似于 **xyz.*.com** 的条目比 **xyz.^.^.com** 匹配的网站更多；**xyz.*.com** 可以匹配字符串之间具有任意数量令牌的站点，而 **xyz.^.^.com** 则匹配具有两个令牌的站点。	

- 通配符必须是令牌中的唯一字符。例如，**example*.com** 是一个无效条目，因为 **example** 和 ***** 位于同一个令牌中。但是，一个条目可以在多个令牌中包含通配符。
- 可以在同一条目中使用星号和插入符号（例如，***.example.^**）。

不要创建带有连续星号 (*) 或九个以上连续插入符号 (^) 的条目，因为这些条目可能会影响防火墙的性能。

例如，请勿添加诸如 ***mail.*.*.com*** 之类的条目。而应该根据想要控制其访问的网站范围，输入 ***mail.*.com*** 或 ***mail.^.^.com***。

URL 类别例外列表 — 示例

下表列出了示例 URL 列表条目、匹配站点以及关于防火墙自动附加尾斜杠时匹配行为的说明。

此表中的条目不包含尾斜杠，以反映防火墙在后台将斜杠附加到适用条目。此外，例外列表可能包含在看到尾斜杠指引之前添加的条目。URL 类别例外 — 示例 *(PAN-OS 10.1)* 显示防火墙默认不附加末尾斜杠时的匹配行为。

我们建议您手动添加尾斜杠，以向检查该条目的人员阐明该条目的预期匹配行为。如果尾斜杠是由防火墙添加，则该尾斜杠不可见。

URL 例外列表条目	匹配网站	说明
示例集 **1**		
paloaltonetworks.com	paloaltonetworks.com paloaltonetworks.com/network-security/security-subscriptions	防火墙会为条目附加一个尾斜杠，将匹配项限制为确切的域及其子目录。
paloaltonetworks.com/example	paloaltonetworks.com/example	防火墙不会为此条目附加尾斜杠，因为域后面跟着子目录 **example**。输入特定网页的 URL 时，防火墙会将例外操作应用于指定的网页。
示例集 **2** — 星号		
*.example.com	www.example.com docs.example.com support.tools.example.com	星号将匹配项扩展到所有 **example.com** 子域。 防火墙为条目附加一个尾斜杠，不包括根域 **example.com** 右侧的匹配项。
mail.example.* 无论是否启用尾斜杠功能，此条目都会产生相同的匹配项。	mail.example.com mail.example.co.uk mail.example.com/#inbox	星号将匹配项扩展到 **mail.example** 之后的任何 **URL**。***<TLD>*** 模式。

URL 例外列表条目	匹配网站	说明
example.*.com	example.yoursite.com example.es.domain.com example.abc.xyz.com	星号将匹配扩展到最左边子域名为 **example**、顶级域名为 **com** 的 URL。此时的尾斜杠排除了 TLD 右侧的匹配项。
example.com/*	example.com/photos example.com/blog/latest 任何 example.com 子目录	域后跟一个 / 和一个星号，表示一定有子目录。星号可以用作任何 **example.com** 子目录的令牌占位符。 防火墙不会为以星号结尾的条目附加尾斜杠。
示例集 **3** — 插入符号		
google.^ 诸如 *example.co.^* 之类的模式通常用于匹配特定国家/地区的域名，例如 ***example.co.jp***。但是，通用顶级域 *(gTLD)* 会产生例如 *example.co.^* 匹配 *example.co.info* 或 *example.co.amzn* 之类的模式，这些模式可能属于不同组织。	google.com google.info google.com/search?q=paloaltonetworks	插入符号将匹配项扩展到以 **google** 开头并以单个 TLD 结尾的 URL。此时的尾斜杠排除了最后一个令牌右侧的匹配项。
^.google.com	www.google.com news.google.com	插入符号将匹配项扩展到 **google.com** 的单级子域名。防火墙会为条目附加一个尾斜杠，排除根域右侧的匹配项。
^.^.google.com	www.maps.google.com support.tools.google.com	两个插入符号将匹配项扩展到在 **google.com** 前面包含两个连续子域的 URL。防火墙会

URL 例外列表条目	匹配网站	说明
		为条目添加一个尾斜杠，排除根域右侧的匹配项。
google.^.com	google.example.com google.company.com	插入符号将匹配扩展到 **google** 为最左边的子域名、后跟一个令牌和 **.com** 的 URL。 防火墙会为条目添加一个尾斜杠，排除 TLD 右侧的匹配项。

创建自定义 URL 类别

哪里可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Advanced URL Filtering 许可证（或旧版 URL 过滤许可证） 注意： • 旧版 *URL* 过滤许可证已停用，但仍支持有效的旧版许可证。 • Prisma Access 许可证包括 *Advanced URL Filtering* 功能。

您可以创建一个自定义 URL 类别，以便定义 URL 类别实施的例外情况，或者从多个类别中定义新的 URL 类别。

定义 **URL** 类别实施的例外（**URL** 列表）

指定您希望独立于预定义的 URL 类别来实施的 URL 列表（分组在单个自定义类别下）。您可以在应用于安全策略规则的 URL 过滤配置文件中控制对此类别的访问，或者将该类别用作安全策略规则中的匹配标准。例如，您可以阻止社交网络类别，但允许访问 LinkedIn。

根据多个 **PAN-DB** 类别定义自定义 **URL** 类别（类别匹配）

创建新类别以针对匹配的网站或页面执行，这些网站或页面与自定义类别包含的所有类别都匹配。例如，PAN-DB 可能会将工程师用于研究的开发人员博客分类为 `personal-sites-and-blogs`、`computer-and-internet-info` 和 `high-risk`。要允许工程师访问博客和类似网站，并且可查看这些网站，可以根据这三个类别创建自定义 URL 类别，并在 URL 过滤配置文件中设置要报警的类别的站点访问权限。

PAN-DB 在外部动态列表和预定义 *URL* 类别之前根据自定义 *URL* 类别评估 *URL*。因此，防火墙对自定义 *URL* 列表中的 *URL* 实施安全策略规则，而不是与该 *URL* 所在的各个 *URL* 类别关联的策略规则。

如果多个安全策略规则包括一个自定义 *URL* 类别，则防火墙会对匹配流量使用最严格的 *URL* 过滤配置文件操作来实施安全策略规则。

- Strata Cloud Manager
- PAN-OS 和 Panorama

创建自定义 URL 类别 (Strata Cloud Manager)

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

切换到 ***PAN-OS & Panorama***（***PAN-OS*** 和 ***Panorama***）选项卡，然后按照其中的指导操作。

如果您正在使用 ***Strata Cloud Manager***，请在此处继续。

STEP 1 | 选择 **Manage**（管理） > **Configuration**（配置） > **Security Services**（安全服务） > **URL Access Management**（**URL** 访问管理） > **Access Control**（访问控制）。

STEP 2 | 在“自定义 URL 类别”下，选择 **Add Category**（添加类别）。

输入类别的描述性 **Name**（名称）。

STEP 3 | 将自定义 URL 类别的 **Type**（类型）设置为 **URL List**（**URL** 列表）或 **Category Match**（类别匹配）。

- **URL List**（**URL** 列表）— 使用此列表类型来添加要以不同于其所属的 URL 类别的方式强制执行的 URL，或者将 URL 列表定义为属于自定义类别。创建 URL 列表条目时，请参阅 URL 类别例外指南。
- **Category Match**（类别匹配）— 针对符合类别集的网站实施。网站或网页必须与在自定义类别中定义的所有类别相符。

STEP 4 | 在 **Items**（项目）下，**Add**（添加）URL 或现有类别。

STEP 5 | **Save**（保存）自定义 URL 类别。

STEP 6 | 为自定义 URL 类别定义站点访问权限和用户凭据提交设置。

1. 选择 **Manage**（管理） > **Configuration**（配置） > **Security Services**（安全服务） > **URL Access Management**（**URL** 访问管理） > **URL Access Management Profiles**（**URL** 访问管理配置文件）。
2. 选择要修改的现有配置文件，或者单击 **Add Profile**（添加配置文件）。
3. 在访问控制下，选择之前创建的自定义 URL 类别。该类别位于 `Custom URL Categories`（自定义 URL 类别）之下和 `Pre-Defined Categories`（预定义类别）之上。
4. 为类别设置 **Site Access**（站点访问权限）。
5. 为类别设置 **User Credential Submissions**（用户凭据提交）。
6. **Save**（保存）配置文件。

STEP 7 | 将 URL 访问管理配置文件应用到安全策略规则。

仅当包含在安全策略规则引用的配置文件组中时，URL 访问管理配置文件才处于活动状态。

按照步骤激活 URL 访问管理配置文件（和任何安全配置文件）。确保 **Push Config**（推送配置）。

您还可以使用自定义 URL 类别作为安全策略规则匹配条件。在这种情况下，您没有在 URL 过滤配置文件中为 URL 类别定义站点访问权限。相反，在创建自定义 URL 类别后，选择要将自定义 URL 类别添加到的安全策略规则，访问路径为 **Manage**（管理）> **Configuration**（配置）> **Security Services**（安全服务）> **Security Policy**（安全策略）。在 **Applications, Services and URLs**（应用程序、服务和 **URL**）以及 URL 类别实体下，单击 **Add URL Categories**（添加 **URL** 类别）。选择您创建的自定义 URL 类别，然后 **Save**（保存）安全策略规则。

创建自定义 URL 类别（PAN-OS 和 Panorama）

STEP 1 | 选择 **Objects**（对象）> **Custom Objects**（自定义对象）> **URL Category**（**URL** 类别）。

STEP 2 | **Add**（添加）或修改自定义 URL 类别，并为类别提供描述性 **Name**（名称）。

STEP 3 | 将类别 **Type**（类型）设置为 **Category Match**（类别匹配）或 **URL List**（**URL** 列表）：

- **URL List**（**URL** 列表）— 添加您想要实施且与其所属 URL 类别不同的 URL。使用此列表类型以定义 URL 类别实施的例外情况，或定义属于自定义类别的 URL 列表。有关创建 URL 列表条目的准则，请参阅 URL 类别例外。

  防火墙默认自动将末尾的斜杠 (/) 附加到末尾不以斜杠或星号 (*) 结尾的域名条目 (**example.com**)。尾斜杠可防止防火墙在域的右侧使用隐式星号。在非通配符域条目中，尾斜杠将匹配项限制为给定域及其子目录。例如，**example.com**（处理后为 **example.com/**）与 **example.com/search** 会被视为相同。

  在通配符域条目（带星号或插入符号的条目）中，尾斜杠限制与符合指定模式的 URL 相匹配。例如，如要匹配条目 ***.example.com**，URL 必须严格地以一个或多个子域开头，并以根域 **example.com** 结束；**news.example.com** 为匹配项，但 **example.com** 不是，因为它缺少子域。

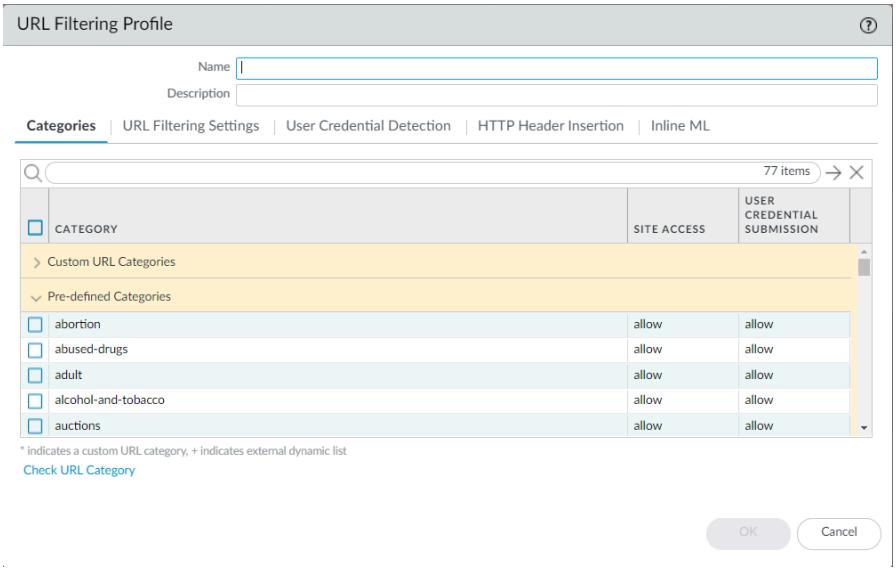
  我们建议您手动添加尾斜杠，以向检查 URL 列表的人阐明该条目的预期匹配行为。如果尾斜杠是由防火墙添加，则该尾斜杠不可见。“URL 类别例外”部分进一步介绍了尾斜杠和匹配行为。

  要禁用此功能，请转到 **Device**（设备）> **Setup**（设置）> **Content-ID** > **URL Filtering**（**URL** 过滤）。然后，取消选择 **Append Ending Token**（附加结束令牌）。如果禁用此功能，可能会阻止或允许访问超出预期数量的 URL。URL 类别例外（*PAN-OS 10.1* 及更早版本）描述了禁用此功能时防火墙的行为。
- **Category Match**（类别匹配）— 针对符合类别集的网站实施。网站或网页必须与在自定义类别中定义的所有类别相符。

STEP 4 | 单击 **OK**（确定）以保存自定义 URL 类别。

STEP 5 | 选择 **Objects**（对象） > **Security Profiles**（安全配置文件） > **URL Filtering**（**URL** 过滤），并 **Add**（添加）或修改 URL 过滤配置文件。

新的自定义类别显示在 **Custom URL Categories**（自定义 **URL** 类别）下：



STEP 6 | 决定您如何为自定义 URL 类别实施 **Site Access**（站点访问）和 **User Credential Submissions**（用户凭据提交）。（要控制用户可提交企业凭据的站点，请参阅预防凭据网络钓鱼）。

STEP 7 | 将 URL 过滤配置文件附加到安全策略规则，以实施与该规则相符的流量。

选择 **Policies**（策略） > **Security**（安全） > **Actions**（操作）并指定安全策略规则，以根据刚才更新的 URL 过滤配置文件执行流量。确保 **Commit**（提交）您的更改。

您也可以使用自定义 *URL* 类别作为安全策略规则匹配条件。在这种情况下，不要在 *URL* 过滤配置文件中定义该 *URL* 类别的站点访问。创建自定义类别后，转到要向其添加自定义 *URL* 类别的安全策略规则，导航路径为 ***Policies***（策略） > ***Security***（安全）。之后，选择 ***Service/URL Category***（服务/*URL* 类别），以使用自定义 *URL* 类别作为规则的匹配条件。

使用 URL 过滤配置文件中的外部动态列表

哪里可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Advanced URL Filtering 许可证（或旧版 URL 过滤许可证） 注意： • 旧版 *URL* 过滤许可证已停用，但仍支持有效的旧版许可证。 • Prisma Access 许可证包括 *Advanced URL Filtering* 功能。

外部动态列表是一个托管在外部 Web 服务器上的文本文件。您可使用此列表导入 URL 并对这些 URL 实施策略。防火墙会以配置的间隔动态导入列表，并为列表中的 URL（IP 地址或域将被忽略）实施策略。更新 web 服务器上的列表时，防火墙检索更改，并对修改过的列表实施策略，而无需在防火墙上进行提交。

为保护您的网络免遭新发现的威胁和恶意软件的威胁，您可以使用 URL 过滤配置文件中的 External Dynamic Lists（外部动态列表）。有关 URL 格式化指南，请参见URL 类别例外指南。

- Strata Cloud Manager
- PAN-OS 和 Panorama

使用 URL 过滤配置文件中的外部动态列表 (Strata Cloud Manager)。

如果您使用 *Panorama* 管理 *Prisma Access*：

切换到 ***PAN-OS & Panorama***（***PAN-OS*** 和 ***Panorama***）选项卡，然后按照其中的指导操作。

如果您正在使用 ***Strata Cloud Manager***，请在此处继续。

STEP 1 | 启用 Prisma Access 来引用外部动态列表。

外部动态列表允许您定义一个导入的 IP 地址、URL 或域名列表，您可以在策略规则中使用这些列表来阻止或允许流量。

要设置外部动态列表，请转到 **Manage**（管理） > **Configuration**（配置） > **Objects**（对象） > **External Dynamic Lists**（外部动态列表）：

- 确保此列表不包括 IP 地址或域名；防火墙跳过非 URL 条目。
- 使用自定义 URL 列表指南来验证列表的格式。
- 将 **List Type**（列表类型）指定为 **URL List**（**URL** 列表）。

STEP 2 | 将外部动态列表与 URL 过滤结合使用。

转到 **Manage**（管理） > **Configuration**（配置） > **Security Services**（安全服务） > **URL Access Management**（**URL** 访问管理）。

- 为外部动态列表中的 URL 指定 **Site Access**（站点访问）。
- 从高级内联分类中排除外部动态列表中的 URL。

您还可以使用外部动态列表来创建自定义 *URL* 类别（返回 *URL* 访问管理指示板来执行此操作）。

如果外部动态列表中包含的 *URL* 也包含在自定义 URL 类别或阻止和允许列表中，则在自定义类别中指定的操作优先于外部动态列表。

STEP 3 | 测试是否实施了策略操作。

1. 查看外部动态列表条目，导航路径为 **Manage**（管理） > **Configuration**（配置） > **Objects**（对象） > **External Dynamic Lists**（外部动态列表），并尝试从列表中访问 URL。
2. 验证您定义的操作在浏览器中实施。

使用 **URL** 过滤配置文件中的外部动态列表（**PAN-OS** 和 **Panorama**）。

STEP 1 | 将防火墙配置为访问外部动态列表。

- 确保此列表不包括 IP 地址或域名；防火墙跳过非 URL 条目。
- 使用自定义 URL 列表指南来验证列表的格式。
- 从类型下拉列表中选择 **URL List**（**URL** 列表）。

STEP 2 | 使用 URL Filtering（URL 过滤）配置文件中的外部动态列表。

1. 选择 **Objects**（对象） > **Security Profiles**（安全配置文件） > **URL Filtering**（**URL** 过滤）。
2. **Add**（添加）或修改现有的 URL Filtering（URL 过滤）配置文件。
3. **Name**（命名）配置文件，并在 **Categories**（类别）选项卡中从“Category（类别）”列表中选择外部动态列表。
4. 单击“Action（操作）”，为外部动态列表中的 URL 选择更精细的操作。

   如果外部动态列表中包含的 *URL* 也包含在自定义 URL 类别或阻止和允许列表中，则在自定义类别中指定的操作优先于外部动态列表。
5. 单击 **OK**（确定）。
6. 将 URL 过滤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 **Actions**（操作）选项卡，并在“Profile Setting（配置文件设置）”部分中，从 **URL Filtering**（**URL** 过滤）下拉列表中选择新的配置文件。
   3. 单击 **OK**（确定）并 **Commit**（提交）更改。

STEP 3 | 测试是否实施了策略操作。

1. 查看外部动态列表条目并尝试访问列表中的 URL。
2. 验证您定义的操作在浏览器中实施。
3. 监控防火墙上的活动：
   1. 选择 **ACC** 并添加 URL 域作为查看访问 URL 的 Network Activity（网络活动）和 Blocked Activity（阻止的活动）的全局过滤器。
   2. 选择 **Monitor**（监控） > **Logs**（日志） > **URL Filtering**（**URL** 过滤）访问详细的日志视图。

STEP 4 | 验证外部动态列表中的条目已忽略或跳过。

在 URL 类型的列表中，防火墙跳过非 URL 的无效条目，并忽视超过防火墙型号最大限制的条目。

要检查是否已达到外部动态列表类型的限制，请选择 ***Objects***（对象） ***> External Dynamic Lists***（外部动态列表），然后单击 ***List Capacities***（列表容量）。

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 url name <list_name>
```

例如：

```
request system external-list show type url name My_URL_List
 vsys5/My_URL_List:Next update at:Tue Jan 3 14:00:00 2017 Source:
 http://example.com/My_URL_List.txt Referenced:Yes Valid:Yes Auth-
Valid:Yes Total valid entries:3 Total invalid entries:0 Valid urls:
 www.URL1.com www.URL2.com www.URL3.com
```


URL 过滤最佳实践

哪里可以使用？	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)	❑ 高级 URL 过滤许可证（或旧版 URL 过滤许可证） 注意： • 旧版 *URL* 过滤许可证已停用，但仍支持有效的旧版许可证。 • Prisma Access 许可证包括 *Advanced URL Filtering* 功能。

Palo Alto Networks URL 过滤解决方案可保护您免遭基于 Web 的威胁，并为您提供一种监视和控制 Web 活动的简单方法。若要最大化地利用 URL 过滤部署，您应先为您开展业务所需的应用程序创建允许规则。然后，查看划分为恶意和攻击性内容的 URL 类别，我们建议您阻止这些类别。接下来，对其他方面而言，此最佳实践可指导您如何在不限制用户访问所需 Web 内容的情况下减少暴露于基于 Web 的威胁。

- 开始之前，请确定您要允许的应用程序，然后创建应用程序允许规则，将其作为最佳实践互联网网关安全策略的组成部分。

  允许的应用程序不仅包括您出于业务和基础结构目的而提供和管理的应用程序，还包括您的用户为完成工作所需的其他应用程序，以及您允许用于个人目的的应用程序。

  标识完这些经过批准的应用程序后，您可以使用 URL 过滤控制和保护未列入到允许列表中的所有 Web 活动。
- 了解用户的网络活动，以便为您的组织规划最有效的 URL 过滤策略。这包括：
  - 使用测试站点了解 PAN-DB（Palo Alto Networks URL 过滤云数据库）如何对特定 URL 进行分类，并了解所有可能的 URL 类别。
  - 从发出 URL 类别警报的（大多数）被动 URL 过滤配置文件开始。这样，您可以看到用户正在访问的站点，从而决定您想要允许、限制和阻止的内容。
  - 监控 Web 活动以评估用户正在访问的站点，并查看这些站点如何与您的业务需求保持一致。
- 阻止划分为恶意和攻击性 Web 内容的 URL 类别。虽然我们知道这些类别很危险，但是请始终记住，您可能需要根据您的业务需求确定要阻止的 URL 类别。
- 使用 URL 类别逐步实施解密，从解密中排除敏感信息或个人信息（例如，financial-services 和 health-and-medicine）。

  计划先对最危险的流量进行解密（URL 类别最有可能包含恶意流量，如赌博或高风险），然后在获得经验时进行解密。或者，先解密不影响业务的 URL 类别（如果出现错误，也不会影响业务），例如，新闻推送。考虑用户反馈，在这两种情况下，解密一些 URL 类别，运行报告，确

保解密按预期进行，然后，逐步解密更多的 URL 类别等等。如果由于技术原因或您选择不解密网站而无法解密，请计划将网站排除在解密之外。

根据 *URL* 类别进行有针对性的解密也是一种解密最佳实践。

- 通过启用防火墙检测站点的公司凭据提交情况阻止凭据被盗，然后基于 URL 类别控制这些提交。阻止用户将凭据提交到恶意和不受信任的站点、警告用户不要在未知站点输入公司凭据或警告用户不要在非公司站点重复使用公司凭据，以及明确允许用户向公司和经批准的站点提交凭据。
- 实时阻止 JavaScript 漏洞利用和网络钓鱼攻击的恶意变体。启用本地内联分类可允许您使用防火墙上的机器学习动态分析网页。
- 配置内联分类以启用内联深度学习、基于 ML 的检测引擎，以便分析可疑网页内容并保护用户免受零日网络攻击。云内联分类可以检测并阻止有针对性的高级网络钓鱼攻击，以及其他使用高级规避技术（如掩蔽、多步攻击、CAPTCHA 挑战和以前未发现过的一次性 URL）的 Web 页面攻击。
- 解密、检查并严格限制用户与高风险和中风险内容（如果您出于业务原因而不阻止任何恶意 URL 类别，则应严格限制用户与这些类别的交互）的交互。

  您批准的 Web 内容和您完全阻止的恶意 URL 类别都只是您整个 Web 流量的一部分。用户访问的其他内容包括良性内容（低风险）和风险内容（高风险和中风险）。高风险和中风险内容未被证实是恶意的，但他们与恶意站点密切关联。例如，高风险 URL 可能与恶意网站位于同一域中，或者可能在过去托管过恶意内容。

  但是，很多对您组织构成风险的站点还能为您的用户提供有价值的资源和服务（云存储服务就是其中一个很好的示例）。尽管这些资源和服务是业务所必需的，但是，他们也很容易成为网络攻击的一部分。以下介绍了如何在确保用户良好体验的同时控制用户与这些存在潜在危险内容进行交互的方式：

  - 在 URL 过滤配置文件中，设置高风险和中风险类别，以继续显示响应页面，从而警告用户，他们正在访问存在潜在危险的站点。如果用户决定继续前往该站点，请告知他们如何采取预防措施。如果您不想通过响应页面提示用户，可发出高风险和中风险类别警报。
  - 解密高风险和中风险站点。
  - 遵循高风险和中风险站点的防间谍软件、漏洞保护和文件阻止最佳实践。采取的保护措施应能阻止下载危险文件类型，并能阻止混淆的 JavaScript。
  - 通过阻止用户向高风险和中风险站点提交其公司凭据，可防止凭据被盗。
- 学校或教育机构应使用强制执行安全搜索，确保搜索引擎将搜索结果中的成人图像和视频筛除。
- 在 URL 类别查找期间保留初始 Web 请求。

  当用户访问网站时，Advanced URL Filtering 会检查缓存的 URL 类别来对网站进行分类。如果在缓存中找不到该 URL 的类别，它会在 PAN-DB（Palo Alto Networks URL 数据库）中执行查找。默认情况下，在此云查找期间允许用户的网络请求。

  但是，当您选择保留 Web 请求时，则可以阻止请求，直到 Advanced URL Filtering 找到 URL 类别或超时。如果查找超时，则防火墙认为 URL 类别是未解析的。在您的 URL 过滤设置中找到此功能，保留客户端对类别查找的请求。

测试 URL 过滤配置

哪里可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Advanced URL Filtering 许可证（或旧版 URL 过滤许可证） 注意： • 旧版 *URL* 过滤许可证已停用，但仍支持有效的旧版许可证。 • Prisma Access 许可证包括 *Advanced URL Filtering* 功能。

要测试您的 URL 过滤策略配置，请使用 Palo Alto Networks URL 过滤测试页面。这些页面是为了对所有预定义的 URL 类别和 Advanced URL Filtering 实时检测类别进行安全测试而创建的。

测试页面可通过 *HTTP* 和 *HTTPS* 连接访问。但是，您必须启用 *SSL* 解密才能通过 *HTTPS* 查看测试页面。

您可以使用 *Palo Alto Networks URL* 类别查找工具测试站点来检查特定网站的分类。

按照与您的 URL 过滤订阅相对应的程序进行操作：

验证 URL 过滤

如果您有旧版 URL 过滤订阅，请测试和验证防火墙的分类是否正确、实施和记录最终用户访问的类别中的 URL。

STEP 1 | 访问感兴趣的 URL 类别中的网站。

考虑在被阻止的 URL 类别中测试站点。您可以使用测试页 (urlfiltering.paloaltonetworks.com/test-<*url-category*>) 来避免直接访问站点。例如，要测试恶意软件的阻止策略，请访问 https://urlfiltering.paloaltonetworks.com/test-malware。

STEP 2 | 查看流量和 URL 过滤日志以验证您的防火墙能否正确处理该站点。

例如，如果您将阻止页面配置为在有人访问违反您组织策略的站点时显示，请检查在您访问测试站点时是否显示该页面。

验证 Advanced URL Filtering

如果您有 Advanced URL Filtering 订阅，请测试并验证提交给 Advanced URL Filtering 的 URL 得到了正确分析。

Palo Alto Networks 建议设置实时检测（云内联分类）操作设置，以对活动的 *URL* 过滤配置文件发出 ***Alert***（警报）。这有助于实时了解分析的 *URL*，并将根据为特定 *Web* 威胁配置的类别设置阻止（或允许，取决于您的策略设置）。

防火墙会实施为给定 *URL* 检测到的 *URL* 类别配置的操作中最严重的操作。例如，假设 *example.com* 被分类为实时检测、命令和控制和购物 — 分别配置了警报、阻止和允许操作的类别。防火墙阻止该 *URL*，因为阻止是检测到的类别中最严格的操作。

STEP 1 | 访问以下每个测试 URL 来验证 Advanced URL Filtering 服务对 URL 分类正确：

- 恶意软件 — http://urlfiltering.paloaltonetworks.com/test-inline-url-analysis-malware
- 网络钓鱼 — http://urlfiltering.paloaltonetworks.com/test-inline-url-analysis-phishing
- **C2** — http://urlfiltering.paloaltonetworks.com/test-inline-url-analysis-command-and-control
- 灰色软件 — http://urlfiltering.paloaltonetworks.com/test-inline-url-analysis-grayware

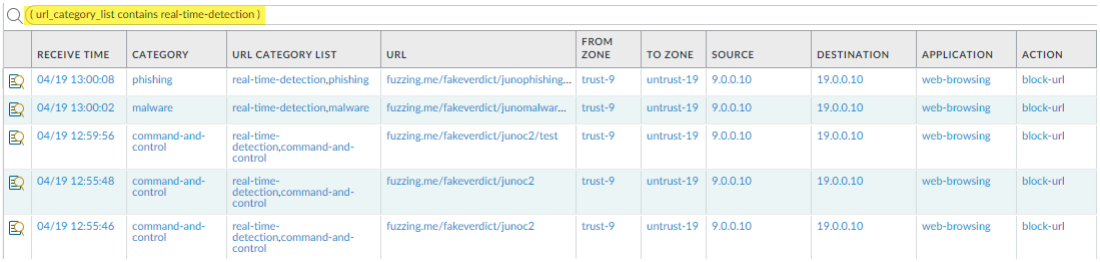
如果已启用云内联分类，请使用以下 URL 测试该功能的运行：

- 恶意软件 — http://urlfiltering.paloaltonetworks.com/test-inline-content-analysis-malware
- 网络钓鱼 — http://urlfiltering.paloaltonetworks.com/test-inline-content-analysis-phishing
- 灰色软件 — http://urlfiltering.paloaltonetworks.com/test-inline-content-analysis-grayware
- 寄放 — http://urlfiltering.paloaltonetworks.com/test-inline-content-analysis-parked
- 成人 — http://urlfiltering.paloaltonetworks.com/test-inline-content-analysis-adult

STEP 2 | 监控 Web 活动，以验证 Advanced URL Filtering 是否已正确分类测试 URL：

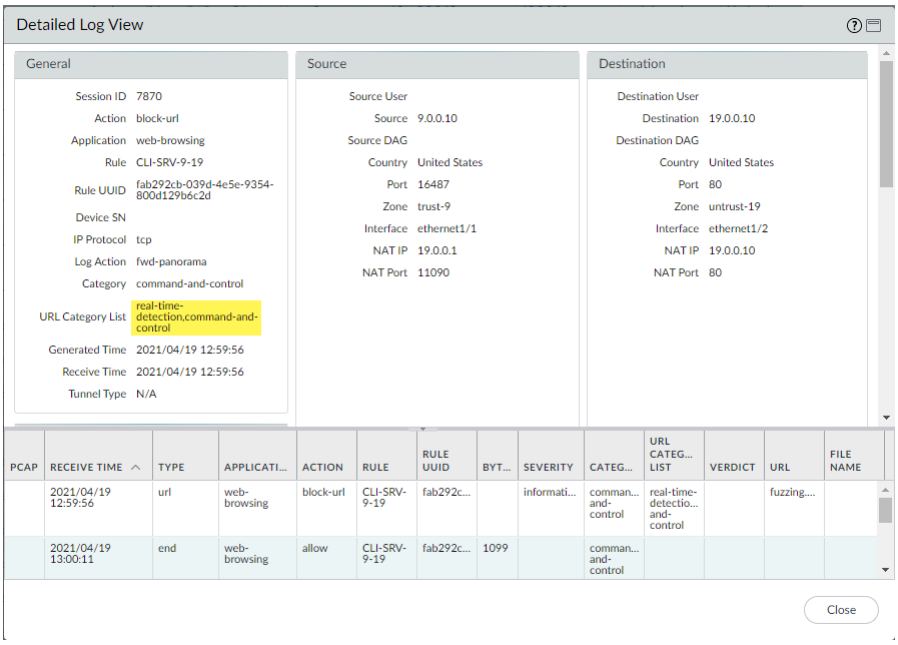
1. 使用以下条件过滤您的 URL 过滤日志：`(url_category_list contains real-time-detection)`。

   其他网页类别匹配也会显示出来，并对应于 PAN-DB 定义的类别。



2. 详细查看日志，以验证是否正确分析和分类了每种类型的 Web 威胁。

   在下个示例中，URL 被归类为已进行实时分析，具有将其定义为命令和控制 (C2) 的特性。因为与实时检测相比，C2 类别的操作更加严重（将阻止而不是警报），因此，该 URL 已被归类为命令和控制，并将被阻止。



URL 过滤功能

哪里可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Advanced URL Filtering 许可证（或旧版 URL 过滤许可证） 注意： • 旧版 *URL* 过滤许可证已停用，但仍支持有效的旧版许可证。 • Prisma Access 许可证包括 *Advanced URL Filtering* 功能。

配置 URL 过滤部署的基本组件后，请考虑配置以下功能：

- 内联分类
- SSL/TLS 握手检测
- URL 管理替代
- 凭据网络钓鱼防护
- URL 过滤响应页面
- 强制执行安全搜索
- （仅限 Prisma Access）远程浏览器隔离 (RBI) 集成

检查 SSL/TLS 握手情况

哪里可以使用？	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)	❑ 高级 URL 过滤许可证（或旧版 URL 过滤许可证） 注意： • 旧版 *URL* 过滤许可证已停用，但仍支持有效的旧版许可证。 • Prisma Access 许可证包括 *Advanced URL Filtering* 功能。

检查 SSL/TLS 握手可提高网络安全，并优化传统和高级 URL 过滤订阅。当您启用 SSL/TLS 握手检查时，高级 URL 过滤将使用握手中的数据来识别通信量，并尽早实施适用的安全策略规则。

下面是它的工作原理

首先，它会扫描客户端 Hello 消息中的服务器名称指示 *(SNI)* 字段，这是一个包含所请求网站的主机名的 TLS 协议扩展。然后，根据主机名确定流量的 URL 类别和服务器目的地。接下来，根据其 URL 类别强制检查流量。如果检测到威胁，例如 SNI 字段中的恶意 Web 服务器，或者安全策略规则阻止了网站，则握手将终止，Web 会话将立即结束。如果未检测到威胁并且每个策略允许流量，则完成 SSL/TLS 握手并通过安全连接交换应用程序数据。

对于在 *SSL/TLS* 握手检查期间被阻止的网站，*URL* 过滤响应页面不会显示，因为防火墙重置了 *HTTPS* 连接。连接重置结束 *SSL/TLS* 握手，并阻止通过响应页面通知用户。相反，浏览器会显示标准的连接错误消息。

您可以在流量和解密日志中找到成功的 *SSL/TLS* 握手和会话的详细信息。失败会话的详细信息可在 *URL* 过滤日志中找到；*SSL/TLS* 握手期间阻止的网页会话不会生成解密日志。

- Strata Cloud Manager
- PAN-OS 和 Panorama

检查 SSL/TLS 握手 (Strata Cloud Manager)

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

切换到 ***PAN-OS & Panorama***（***PAN-OS*** 和 ***Panorama***）选项卡，然后按照其中的指导操作。

如果您正在使用 ***Strata Cloud Manager***，请在此处继续。

检查 SSL 握手的要求是，通过 SSL 转发代理或 SSL 入站检查解密 SSL/TLS 流量。

STEP 1 | 确认您的 Prisma Access 许可证包括高级 URL 过滤订阅。

1. 选择 **Manage**（管理） > **Service Setup**（服务设置） > **Overview**（改述），然后单击带超链接的 Quantity 值。此时将显示包含“安全服务”的信息。

2. 在“安全服务”下，确认 URL 过滤旁有复选标记。

STEP 2 | 验证您是否通过 SSL 转发代理或 SSL 入站检测解密 SSL/TLS 流量。

STEP 3 | 启用 CTD 检查 SSL/TLS 握手。默认情况下，此选项处于禁用状态。

1. 选择 **Manage**（管理） > **Configuration**（配置） > **Security Services**（安全服务） > **Decryption**（解密）。
2. 通过“解密设置”，选择设置图标。然后，选择 **Inspect TLS Handshake Messages**（检查 **TLS** 握手消息）。

   或者，您可以使用 **`set deviceconfig setting ssl-decrypt scan-handshake <yes|no>`** CLI 命令。
3. **Save**（保存）更改。在“解密设置”下，“检查 TLS 握手消息”设置应显示“已启用”。

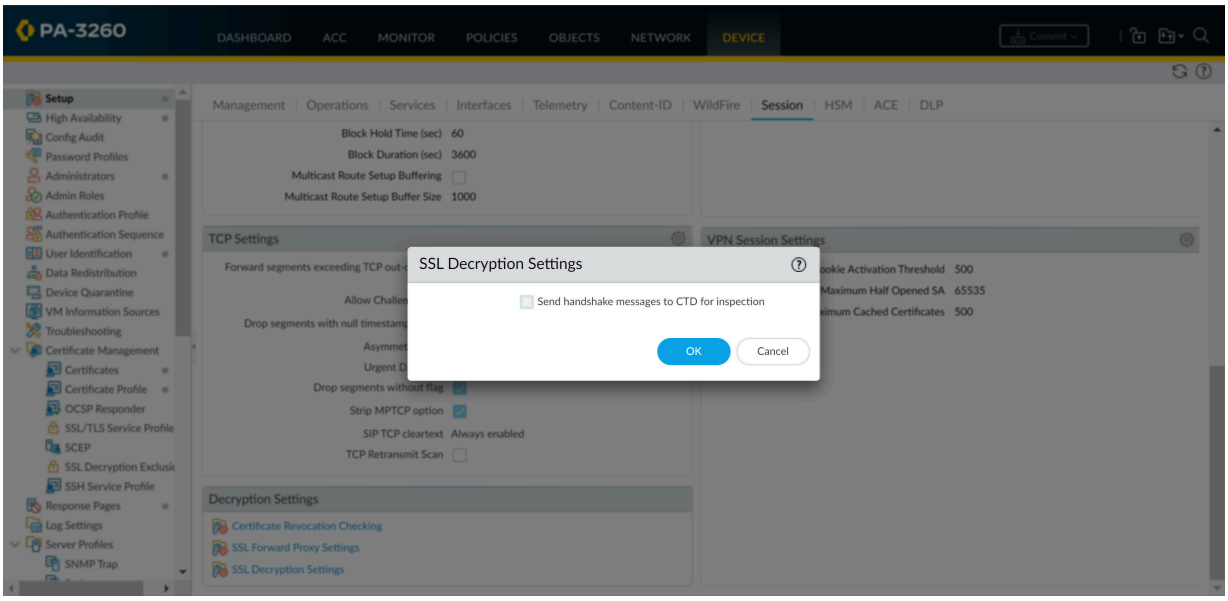
STEP 4 | **Push Config**（推送配置）以保存并提交更改。

检查 SSL/TLS 握手（PAN-OS 和 Panorama）

STEP 1 | 选择 **Device**（设备）> **Licenses**（许可证），以确认您拥有有效的高级 URL 过滤或旧版 URL 过滤许可证。

STEP 2 | 验证您是否通过 SSL 转发代理或 SSL 入站检测解密 SSL/TLS 流量。

STEP 3 | 启用 CTD 检查 SSL/TLS 握手。默认情况下，该选项处于禁用状态。



1. 选择 **Device**（设备） > **Setup**（设置） > **Session**（会话） > **Decryption Settings**（解密设置） > **SSL Decryption Settings**（**SSL** 解密设置）。
2. 选择 **Send handshake messages to CTD for inspection**（将握手消息发送到 **CTD** 进行检测）。

   或者，您可以使用 **`set deviceconfig setting ssl-decrypt scan-handshake <yes|no>`** CLI 命令。
3. 单击 **OK**（确定）。

STEP 4 | **Commit**（提交）配置更改。

允许密码访问某些站点

哪里可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Advanced URL Filtering 许可证（或旧版 URL 过滤许可证） 注意： • 旧版 *URL* 过滤许可证已停用，但仍支持有效的旧版许可证。 • Prisma Access 许可证包括 *Advanced URL Filtering* 功能。

在某些情况下，可能需要密码才能访问某些类别的网站。例如，贵公司可能会阻止威胁员工安全和福祉的 URL 类别。但是，某些员工可能需要为进行研究或其他合法目的访问这些类别。为了平衡安全性和业务需求，实施 URL 管理员覆盖可能是一种有效的解决方案。

要创建 URL 管理员覆盖，请将类别的操作设置为 **Override**（覆盖）。然后，创建一个密码，用户必须输入该密码才能访问此类别的站点。当用户试图访问您覆盖的类别中的网站时，将显示继续和覆盖响应页面。此页面会通知用户某个网站已被阻止，并提示他们输入密码来继续访问该网站。

- Strata Cloud Manager
- PAN-OS 和 Panorama

允许使用密码访问某些站点 (Strata Cloud Manager)

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

切换到 ***PAN-OS & Panorama***（***PAN-OS*** 和 ***Panorama***）选项卡，然后按照其中的指导操作。

如果您正在使用 ***Strata Cloud Manager***，请在此处继续。

STEP 1 | 转到 URL 访问管理指示板。

选择 **Manage**（管理）> **Configuration**（配置）> **Security Services**（安全服务）> **URL Access Management**（**URL** 访问管理）。

STEP 2 | 选择 **Settings**（设置）。

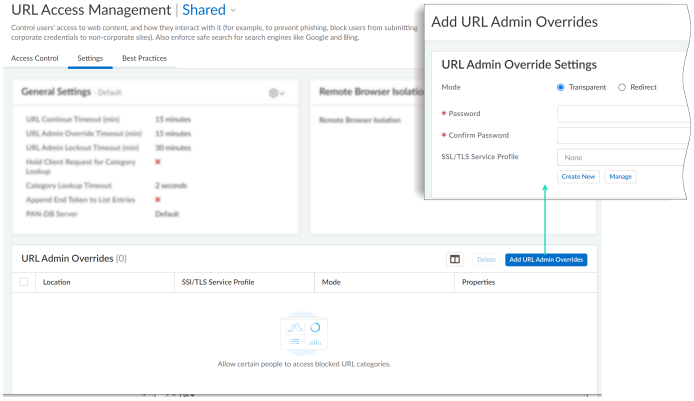
STEP 3 | 创建 URL 管理员覆盖密码。

1. 转到 URL 管理员覆盖，然后 **Add URL Admin Overrides**（添加 **URL** 管理员覆盖）。
2. （可选）选择提示用户输入密码的 **Mode**（模式）：
   - **Transparent**（透明）— 密码提示似乎源自原始目标 URL。防火墙拦截发送到设置为覆盖的 URL 类别中网站的浏览器流量，并发出 HTTP 302 来提示输入密码，该密码适用于 vsys 级别。

- **Redirect**（重定向）— 密码提示从您指定的 **Address**（地址）（IP 地址或 DNS 主机名）出现。防火墙拦截发送到设置为覆盖的 URL 类别的 HTTP 或 HTTPS 流量，并使用 HTTP 302 重定向将请求发送到防火墙上的第 3 层接口。

3. 输入 **Password**（密码），然后再次输入以 **Confirm Password**（确认密码）。
4. （可选）选择 **SSL/TLS Service Profile**（**SSL/TLS** 服务配置文件）。

   您可以通过分别单击 **Create New**（新建）和 **Manage**（管理）来创建和管理 SSL/TLS 服务配置文件。
5. **Save**（保存）更改。



STEP 4 | （可选）设置覆盖访问和密码锁定的持续时间。

默认情况下，对于成功输入覆盖密码的类别中的网站，用户可以访问 15 分钟。在默认或自定义间隔过后，用户必须重新输入密码。

默认情况下，用户可以尝试输入密码三次，三次都失败后，用户会被阻止 30 分钟。在默认或自定义锁定时间过后，用户可以尝试再次访问网站。

1. 自定义常规设置。
2. 对于 **URL Admin Override Timeout**（**URL** 管理员覆盖超时），请输入一个介于 1 到 86,400 之间的值（以分钟为单位）。
3. 对于 **URL Admin Lockout Timeout**（**URL** 管理员锁定超时），请输入介于 1 到 86,400 之间的值（以分钟为单位）。
4. **Save**（保存）更改。

STEP 5 | 指定需要使用密码访问的 URL 类别。

1. 在“URL 访问管理”指示板上的 **Access Control**（访问控制）选项卡下，转到“URL 访问管理配置文件”并修改或 **Add Profile**（添加配置文件）。
2. 在“访问控制”下，选择需要使用密码访问的类别。
3. 选择所有类别后，单击 **Set Access**（设置访问权限），然后选择 **Override**（覆盖）。

   突出显示的类别的站点访问权限现在应该会显示为 `Override`（覆盖）。
4. **Save**（保存）更改。

STEP 6 | 将 URL 访问管理配置文件应用到安全策略规则。

仅当包含在安全策略规则引用的配置文件组中时，URL 访问管理配置文件才处于活动状态。

按照步骤激活 URL 访问管理配置文件（和任何安全配置文件）。完成后，请确保 **Push Config**（推送配置）。

允许使用密码访问某些站点（PAN-OS 和 Panorama）

STEP 1 | 设置 URL 管理员覆盖密码。

1. 选择 **Device**（设备） > **Setup**（设置） > **Content - ID**（内容 **ID**）。
2. 在 **URL Admin Override**（**URL** 管理替代）部分中，单击 **Add**（添加）。
3. 在 **Location**（位置）字段中，选择要应用该密码的虚拟系统。
4. 输入 **Password**（密码），然后再次输入以 **Confirm Password**（确认密码）。
5. 选择 **SSL/TLS Service Profile**（**SSL/TLS** 服务配置文件）。

   当具有覆盖权限的站点是 HTTPS 站点时，SSL/TLS 服务配置文件用于指定防火墙向用户提供的证书。
6. 选择提示用户输入密码的 **Mode**（模式）：
   - **Transparent**（透明）— 密码提示似乎源自原始目标 URL。防火墙拦截发送到设置为覆盖的 URL 类别中网站的浏览器流量，并发出 HTTP 302 来提示输入密码，该密码适用于 vsys 级别。

     如果客户端浏览器不信任证书，将会显示证书错误。
   - **Redirect**（重定向）— 密码提示从您指定的 **Address**（地址）（IP 地址或 DNS 主机名）出现。防火墙拦截发送到设置为覆盖的 URL 类别的 HTTP 或 HTTPS 流量，并使用 HTTP 302 重定向将请求发送到防火墙上的第 3 层接口。
7. 单击 **OK**（确定）。

STEP 2 | （可选）设置覆盖访问和密码锁定的持续时间。

默认情况下，对于成功输入覆盖密码的类别中的网站，用户可以访问 15 分钟。在默认或自定义间隔过后，用户必须重新输入密码。

默认情况下，用户可以尝试输入密码三次，三次都失败后，用户会被阻止 30 分钟。在默认或自定义锁定时间过后，用户可以尝试再次访问网站。

1. 编辑 URL 过滤部分。
2. 对于 **URL Admin Override Timeout**（**URL** 管理员覆盖超时），输入介于 1 到 86,400 之间的值（以分钟为单位）。---默认情况下，用户无需重新输入密码即可访问该类别中的站点 15 分钟。
3. 对于 **URL Admin Lockout Timeout**（**URL** 管理员锁定超时），请输入介于 1 到 86,400 之间的值（以分钟为单位）。
4. 单击 **OK**（确定）。

STEP 3 | （仅重定向模式）创建要将针对替代配置类别中站点的 Web 请求重定向至的第 3 层接口。

1. 创建管理配置文件，以启用接口显示“URL 过滤继续和替代页面”响应页面：
   1. 选择 **Network**（网络） > **Interface Mgmt**（接口管理），然后单击 **Add**（添加）。
   2. 输入配置文件的 **Name**（名称），选择 **Response Pages**（响应页），然后单击 **OK**（确定）。
2. 创建第 3 层接口。确保附加您刚创建的管理配置文件（在“Ethernet 接口”对话框的 **Advanced**（高级） > **Other Info**（其他信息）选项卡上）。

STEP 4 | （仅重定向模式）若要透明地重定向用户而不显示证书错误，请安装与您要将针对替代配置 URL 类别中站点的 Web 请求重定向至的接口的 IP 地址匹配的证书。您可以生成自签名证书，也可以导入外部 CA 签名的证书。

若要使用自签名证书，必须先创建一个根 CA 证书，然后使用该 CA 签名您将用于 URL 管理替代的证书，步骤如下：

1. 若要创建根 CA 证书，请选择 **Device**（设备） > **Certificate Management**（证书管理） > **Certificates**（证书） > **Device Certificates**（设备证书），然后单击 **Generate**（生成）。输入 **Certificate Name**（证书名称），例如 RootCA。不要选择 **Signed By**（签名者）字段中的值（此值表示自签名）。请确保选中 **Certificate Authority**（证书授权机构）复选框，然后单击 **Generate**（生成）证书。
2. 若要创建用于 URL 管理替代的证书，请单击 **Generate**（生成）。输入 **Certificate Name**（证书名称），并输入接口的 DNS 名称或 IP 地址作为 **Common Name**（通用名）。在 **Signed By**（签名者）字段中，选择您在上一步中创建的 CA。添加 IP 地址属性，并指定您要将针对拥有替代操作的 URL 类别的 Web 请求重定向至的第 3 层接口的 IP 地址。
3. **Generate**（生成）证书。
4. 要配置客户端信任该证书，请在 **Device Certificates**（设备证书）选项卡上选择 CA 证书，然后单击 **Export**（导出）。然后，必须通过手动配置浏览器，或者通过将证书添加到 Active Directory 组策略对象 (GPO) 的可信根中，将该证书作为可信的根 CA 导入到所有客户端浏览器。

STEP 5 | 指定需要替代密码才能启用访问权限的 URL 类别。

1. 选择 **Objects**（对象） > **URL Filtering**（**URL** 过滤），然后选择现有 URL 过滤配置文件或 **Add**（添加）新配置文件。
2. 在 **Categories**（类别）选项卡上，针对需要密码的各个类别将“操作”设置为 **override**（替代）。
3. 完成 URL 过滤配置文件中的所有剩余部分，然后单击 **OK**（确定）保存该配置文件。

STEP 6 | 将 URL 过滤配置文件应用到安全策略规则，以允许访问需要进行密码替代才能访问的站点。

1. 选择 **Policies**（策略） > **Security**（安全），然后选择相应的安全策略以进行修改。
2. 选择 **Actions**（操作）选择卡，然后在 **Profile Setting**（配置文件设置）部分中，单击 **URL Filtering**（**URL** 过滤）下拉列表，并选择该配置文件。
3. 单击 **OK**（确定）以保存。

STEP 7 | **Commit**（提交）配置。

凭据网络钓鱼防护

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)	❑ 高级 URL 过滤许可证（或旧版 URL 过滤许可证） 注意： • 旧版 *URL* 过滤许可证已停用，但仍支持有效的旧版许可证。 • Prisma Access 许可证包括 *Advanced URL Filtering* 功能。

网络钓鱼站点是攻击者伪装成合法网站的站点，目的是窃取用户信息，尤其是可访问您网络的凭据。当网络钓鱼电子邮件进入网络时，只需一名用户点击链接并输入凭据，攻击就会发生。您可以通过控制用户根据站点的 URL 类别提交公司凭据的站点，来检测和阻止进行中的网络钓鱼攻击，从而放置凭据被盗。此操作允许您阻止用户将凭据提交给不可信站点，同时允许用户继续向公司和受约束的站点提交凭据。

通过扫描提交给网站的用户名和密码，并将这些提交内容与有效的公司凭据进行比较，以阻止凭据网络钓鱼。可以根据网站的 URL 类别选择要允许或阻止公司凭据提交的网站。当用户尝试向您限制的类别中的站点提交凭据时，阻止响应页面会阻止用户提交凭据，或者继续页面会警告用户不要向某些 URL 类别中的站点提交凭据，但仍允许他们继续提交。您可以自定义响应页面，针对用户如何重复使用公司凭据提供指导，即使在合法的非网络钓鱼站点上，他们也应按照您的指导操作。

以下主题介绍了您可以选择的不同凭据检测方法，并提供了配置凭据网络钓鱼防御的说明。

- 检查公司凭据提交的方法
- 使用基于 Windows 的 User-ID 代理配置凭据检测
- 启用凭据网络钓鱼防御

检查公司凭据提交的方法

哪里可以使用？	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)	❑ 高级 URL 过滤许可证（或旧版 URL 过滤许可证） 注意： • 旧版 *URL* 过滤许可证已停用，但仍支持有效的旧版许可证。 • Prisma Access 许可证包括 *Advanced URL Filtering* 功能。

在启用凭据网络钓鱼防护之前，请确定要使用哪种方法来检查有效的公司凭据是否已提交至网页。

检查已提交凭据的方法	User-ID 配置要求	该方法将如何检测用户提交给网站的公司用户名和/或密码？
组映射	防火墙上的组映射	防火墙通过检查确定用户提交至受限站点的用户名是否匹配任何有效的公司用户名。 为此，防火墙将提交的用户名与其用户到组映射表中的用户名列表相匹配，以在用户向受限类别中的站点提交公司用户名时进行检测。 该方法仅根据 LDAP 组成员身份检查公司用户名提交，让配置更简单，但是更容易发生误报。
IP 用户映射	通过用户映射、GlobalProtect 或身份验证策略和身份验证门户识别的 IP 地址到用户名映射	防火墙通过检查确定用户提交至受限站点的用户名是否映射到登录用户名的 IP 地址。 为此，防火墙将登录用户名的 IP 地址和提交给网站的用户名与其 IP 地址到用户映射表相匹配，以在用户将公司用户名提交给受限类别中的站点时进行检测。 因为这种方法将与会话相关联的登录用户名的 IP 地址与 IP 地址到用户名映射表相匹配，因此它是检测公司用户名提交的有效方法，但不会检测公司密码提交。如果要检测公司用户名和密码提交，则必须使用域凭据过滤器方法。
域凭据过滤器	已配置 User-ID 凭据服务插件的 Windows User-ID 代理 - 和 - 通过用户映射、GlobalProtect 或身份验证策略和身份验证门户识别的 IP 地址到用户名映射	防火墙通过检查确定用户提交的用户名和密码是否与同一用户的公司用户名和密码相匹配。 为此，防火墙必须能够将凭据提交与有效的公司用户名和密码相匹配，并验证提交的用户名是否映射至登录用户名的 IP 地址，如下所示： • 要检测公司用户名和密码 — 防火墙从配备有 User-ID 凭据服务插件的 Windows User-ID 代理中检索一个名为 *bloom* 过滤器的安全位掩码。该插件服务扫描您的目录以获取用户名和密码哈希，将其解构为安全位掩码（即 bloom 过滤器），并将其传递到 Windows User-ID 代理。防火墙定期从 Windows User-ID 代理中检索bloom 过滤器。只要检测到用户将凭据提交到受限类别，就会重建 bloom 过滤器并查找匹配的用户名和密码哈希。防火墙只能连接一个正在运行 User-ID 凭据服务插件的 Windows User-ID 代理。 • 要验证凭据是否属于登录用户名 — 防火墙在其 IP 地址到用户名映射表中查找登录用户名的 IP 地址与检测到的用户名之间的映射关系。 要了解有关域凭据方法的更多信息，请参阅使用基于 Windows 的 User-ID 代理配置凭据检测。

使用 Windows User-ID 代理配置凭据检测

哪里可以使用？	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)	❑ 高级 URL 过滤许可证（或旧版 URL 过滤许可证） 注意： • 旧版 *URL* 过滤许可证已停用，但仍支持有效的旧版许可证。 • Prisma Access 许可证包括 *Advanced URL Filtering* 功能。

域凭据过滤器检测使防火墙能够检测提交至 Web 页面的密码。该凭据检测方法需要 Windows User-ID 代理和 User-ID 凭据服务（User-ID 代理的一种插件，安装在只读域控制器 *(RODC)* 上）。

Windows User-ID 代理仅支持域凭据过滤检测方法。您不能使用 集成有 *PAN-OS* 的 *User-ID* 代理来配置此凭据检测方法。

RODC 是一个 Microsoft Windows 服务器，用于维护域控制器托管的 Active Directory 数据库的只读副本。例如，当域控制器位于公司总部时，RODC 可以部署在远程网络位置，以提供本地身份验证服务。在 RODC 上安装 User-ID 代理可能有用，原因如下：不需要访问域控制器目录来启用凭据检测，并且可支持有限的或有针对性的一组用户的凭据检测。因为 RODC 托管的目录为只读，因此，目录内容的安全性在域控制器上可得到保证。

因为您必须在 *RODC* 上安装 *Windows User-ID* 代理以进行凭据检测，因此最佳做法是为此目的部署单独的代理。请勿使用 *RODC* 上安装的 *User-ID* 代理将 *IP* 地址映射到用户。

在 RODC 上安装 User-ID 代理后，User-ID 凭据服务将在后台运行并扫描目录，找出 RODC 密码复制策略 (PRP) 中列出的组成员的用户名和密码哈希。您可以定义您在该列表中的角色。然后，User-ID 凭据服务将获取收集到的用户名和密码哈希，并将数据解构为一种名为 *bloom* 过滤器的位掩码。Bloom 过滤器的数据结构紧凑，提供一种检查元素（用户名或密码哈希）是否是元素集（您已批准用于复制到 RODC 的凭据集）成员的安全方法。User-ID 凭据服务将 bloom 过滤器转发给 Windows User-ID 代理；防火墙定期从 User-ID 代理中检索最新的 bloom 过滤器，并用其来检测用户名和密码哈希提交。然后，防火墙根据您的设置阻止、提醒或允许向 Web 页面提交有效的密码，或向用户显示响应页面，警告他们网络钓鱼的危险，但允许其继续提交。

在此过程中，User-ID 代理不会存储或公开任何密码哈希，也不会将密码哈希转发给防火墙。一旦密码哈希被解构成一个 bloom 过滤器，就无法再次恢复。

STEP 1 | 使用 Windows User-ID 代理配置用户映射。

要启用凭据检测，必须在 *RODC* 上安装 *Windows User-ID* 代理。有关受支持的服务器列表，请参阅兼容性矩阵。为此，请安装单独的 *User-ID* 代理。

设置 User-ID 以启用域凭据过滤器检测时要记住的重要事项：

- 凭据网络钓鱼检测的有效性取决于您的 RODC 设置。确保查看 RODC 管理的最佳实践和建议。
- 下载 User-ID 软件更新 ：
  - User-ID 代理 Windows 安装程序 — UaInstall-x.x.x-x.msi。
  - User-ID 代理凭据服务 Windows 安装程序 — UaCredInstall64-x.x.x-x.msi。
- 使用具有通过 LDAP 读取 Active Directory 之权限的帐户（User-ID 代理也需要此权限），在 RODC 上安装 User-ID 代理和用户代理凭据服务。
  - User-ID 代理凭据服务需要使用本地系统帐户进行登录的权限。有关详细信息，请参阅为 User-ID 代理创建专用服务帐户。
  - 服务帐户必须是 RODC 上本地管理员组成员。

STEP 2 | 启用 User-ID 代理和用户代理凭据服务（在后台运行以扫描允许使用的凭据）以共享信息。

1. 在 RODC 服务器上，启动 User-ID 代理。
2. 选择 **Setup**（设置），然后编辑设置部分。
3. 选择 **Credentials**（凭据）选项卡。仅在您已经安装 User-ID 代理凭据服务时，才会显示此选项卡。
4. 选择 **Import from User-ID Credential Agent**（从 **User-ID** 凭据代理导入）。这使得 User-ID 代理可以导入 User-ID 凭据代理创建的 bloom 过滤器来呈现用户和相应的密码哈希。
5. 单击 **OK**（确定），**Save**（保存）您的设置，并 **Commit**（提交）。

STEP 3 | 在 RODC 目录中，定义要为其支持凭据提交检测的用户组。

- 确认将应接收凭据提交执行的组添加到“允许的 RODC 密码复制组”。
- 检查在默认情况下，“允许的 RODC 密码复制组”中的任何组都不在“拒绝的 RODC 密码复制组”中。两者中列出的组均不会受到凭据网络钓鱼执行的影响。

STEP 4 | 继续下一个任务。

在防火墙上设置凭据网络钓鱼防护。

设置凭据网络钓鱼防护

哪里可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Advanced URL Filtering 许可证（或旧版 URL 过滤许可证） 注意：

哪里可以使用？	需要提供什么？
• NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	• 旧版 *URL* 过滤许可证已停用，但仍支持有效的旧版许可证。 • Prisma Access 许可证包括 *Advanced URL Filtering* 功能。

决定配置哪种用户凭据检测方法后，请按照以下步骤防止凭据网络钓鱼攻击成功。

在启用凭据网络钓鱼防护之前，请验证您在防火墙上配置的 Primary Username（主用户名）是否使用了 *samAccountName* 属性。凭据网络钓鱼防护不支持备用属性。

- Strata Cloud Manager
- PAN-OS 和 Panorama

设置凭据网络钓鱼防护 (Strata Cloud Manager)

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

切换到 ***PAN-OS & Panorama***（***PAN-OS*** 和 ***Panorama***）选项卡，然后按照其中的指导操作。

如果您正在使用 ***Strata Cloud Manager***，请在此处继续。

STEP 1 | 配置要使用的用户凭据检测方法。

查看检查公司凭据提交的方法，了解有关每种方法的详细信息。

- 对于 IP 用户映射，设置本地用户和组、身份重分发或使用 Prisma Access 进行身份验证。
- 要使用域凭据过滤器，请设置身份重新分发以及本地用户和组或身份验证。
- 要使用组映射，请设置本地用户和组或身份验证。

STEP 2 | 创建解密策略规则，这将解密要监控的用户凭据提交的流量。

STEP 3 | 创建或修改 URL 访问管理配置文件。

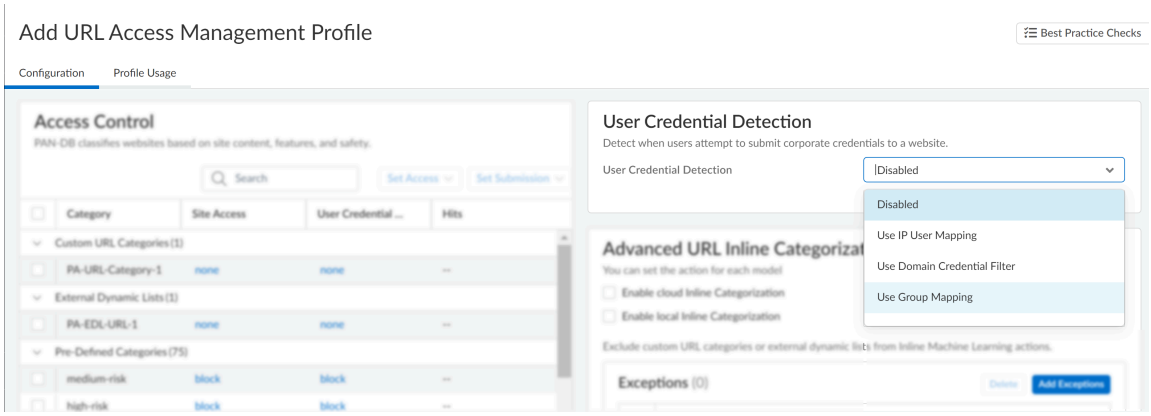
1. 选择 **Manage**（管理） > **Configuration**（配置） > **NGFW and Prisma Access**（**NGFW 和 Prisma Access**） > **Security Services**（安全服务） > **URL Access Management**（**URL 访问管理**）。
2. 在“URL 访问管理配置文件”下，单击 **Add Profile**（添加配置文件）或选择现有配置文件。

STEP 4 | 配置“用户凭据检测”设置。

1. 在“用户凭据检测”下，选择一种 **User Credential Detection**（用户凭据检测）方法。
   - **Use IP User Mapping**（使用 **IP** 用户映射）— 检查有效的公司用户名提交，并验证用户名是否已映射到会话的源 IP 地址。为此，Prisma Access 根据其 IP 地址到用户名的映射表匹配提交的用户名和会话的源 IP 地址。
   - **Use Domain Credential Filter**（使用域凭据过滤器）— 检查提交的有效公司用户名和密码，并验证用户名是否映射到登录用户的 IP 地址。

- **Use Group Mapping**（使用组映射）— 根据将用户映射到组时填充的用户到组映射表，检查提交的用户名是否有效。您可以将凭据检测应用于目录的任何部分，也可以应用于有权访问您最敏感的应用程序（如 IT）的特定组。

  在没有唯一结构化用户名的环境中，此方法容易出现误报。因此，您只能使用此方法来保护您的高价值用户帐户。



2. 对于 **Valid Username Detected Log Severity**（检测到有效用户名日志严重性），选择防火墙在检测到公司凭据提交时，在日志中记录的严重性级别：
   - 高
   - （默认）**Medium**（中等）
   - 低

STEP 5 | 配置防火墙检测到公司凭据提交时采取的操作。

1. 在“访问控制”下，对于每个 URL 类别及其设置为“允许”或“警报”的 **Site Access**（站点访问），为 **User Credential Submission**（用户凭据提交）选择一个操作。

   您可以从以下操作中进行选择：
   - （推荐）**Alert**（警报）— 允许用户向给定 URL 类别中的网站提交凭据，但每次发生这种情况时都会生成 URL 过滤日志。
   - （默认）**Allow**（允许）— 允许用户向网站提交凭据。
   - （推荐）**Block**（阻止）— 阻止用户向给定 URL 类别中的网站提交凭据。当用户尝试提交凭据时，防火墙会显示防网络钓鱼阻止页面。
   - **Continue**（继续）— 当用户尝试提交凭据时显示的防网络钓鱼继续页面。用户必须在响应页面上选择“继续”，才能继续访问网站。
2. **Save**（保存）配置文件。

STEP 6 | 将 URL 访问管理配置文件应用于您的安全策略规则。

1. 选择 **Manage**（管理） > **Configuration**（配置） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Security Services**（安全服务） > **Security Policy**（安全策略）。
2. 在 Security Policy Rules（安全策略规则）下，创建或选择一条安全策略规则。
3. 选择 **Actions**（操作） > **Profile Group**（配置文件组），然后选择“URL 访问管理”配置文件组。
4. **Save**（保存）规则。

STEP 7 | 单击 **Push Config**（推送配置）。

设置凭据网络钓鱼防护（PAN-OS 和 Panorama）

STEP 1 | 启用 User-ID.

每种检查公司凭据提交的方法都需要不同的 User-ID 配置：

- 群组映射 — 检测用户提交的企业用户名是否有效，并要求您将用户映射到群组。
- IP 用户映射 — 检测用户提交的企业用户名是否有效，以及用户名是否与登录用户名相匹配，需要您将 IP 地址映射到用户。
- 域凭据过滤器 — 检测用户是否正在提交有效的用户名和密码，以及这些凭据是否属于登录用户 — 要求您使用基于 Windows 的 User-ID 代理配置凭据检测并将 IP 地址映射到用户。

STEP 2 | 请配置最佳实践 URL 过滤配置文件，以确保 URL 不受出现的托管恶意软件或破坏性内容的攻击。

1. 选择 **Objects**（对象） > **Security Profiles**（安全配置文件） > **URL Filtering**（**URL** 过滤），并 **Add**（添加）或修改 URL 过滤配置文件。
2. 阻止访问所有已知的危险 URL 类别：恶意软件、网络钓鱼、动态 DNS、未知、命令和控制、极端主义、版权侵犯、回避代理和匿名者、新注册域、灰色软件以及寄放。

STEP 3 | 创建解密策略规则，对要监控的用户凭据提交的流量进行解密。

STEP 4 | 检测向允许的 URL 类别的网站提交的公司凭据。

为了提供最佳性能，防火墙不会检查为可信站点提交的凭据，即使您为这些站点启用 *URL* 类别检查，也是如此。可信站点是指 *Palo Alto Networks* 尚未观察到任何恶意攻击或网络钓鱼攻击的站点。此可信站点列表的更新通过应用程序和威胁内容更新提供。

1. 选择要修改的 URL 过滤配置文件，导航路径为 **Objects**（对象） > **Security Profiles**（安全配置文件） > **URL Filtering**（**URL** 过滤）。
2. 选择 **User Credential Detection**（用户凭据检测），并选择一种用户凭据检测方法。

   确定主用户名的格式与 *User-ID* 源提供的用户名格式一致。

   - **Use IP User Mapping**（使用 **IP** 用户映射）— 检查有效的公司用户名提交，并验证用户名是否已映射到会话的源 IP 地址。为此，防火墙根据其 IP 地址到用户名的映射表

匹配提交的用户名和会话的源 IP 地址。要使用此方法，您可使用将 IP 地址映射到用户中列出的任何用户映射方法。

- **Use Domain Credential Filter**（使用域凭据过滤器）— 检查有效的公司用户名和密码提交，并验证用户名是否映射到用户登录的 IP 地址。有关如何设置此方法的说明，请参阅使用基于 Windows 的用户 ID 代理配置凭据检测。
- **Use Group Mapping**（使用组映射）— 当防火墙配置为将用户映射到组时，根据用户到组映射表检查有效的用户名提交。

  使用组映射，您可以将凭据检测应用于目录的任何部分，或可以访问最敏感应用程序的特定组，例如 IT 组。

该方法在没有唯一结构化用户名的环境中容易出现误报。因此，您只能使用此方法来保护您的高价值用户帐户。

3. 设置防火墙用于记录公司凭据提交检测的 **Valid Username Detected Log Severity**（有效用户名检测到的日志严重性）。默认情况下，防火墙将这些事件记录为中等严重性。

STEP 5 | 阻止（或警报）允许站点的凭据提交。

1. 选择 **Categories**（类别）。
2. 对于允许 **Site Access**（站点访问）的每个类别，选择要处理 **User Credential Submissions**（用户凭据提交）的方式方法：
   - **alert**（警报）— 允许用户向网站提交凭据，但是每次用户在该 URL 类别中向站点提交凭据时生成 URL 过滤日志。
   - **allow**（允许）—（默认）允许用户向网站提交凭据。
   - **block**（阻止）— 阻止用户向网站提交凭据。当用户尝试提交凭据时，防火墙会显示防网络钓鱼阻止页面，从而阻止提交。
   - **Continue**（继续）— 当用户尝试提交凭据时显示的防网络钓鱼继续页面。用户必须在响应页面上选择“继续”以继续提交。
3. 选择 **OK**（确定）以保存 URL 过滤配置文件。

STEP 6 | 将设置有凭据检测功能的 URL 过滤配置文件应用于您的安全策略规则。

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）选项卡中，将 **Profile Type**（配置文件类型）设置为 **Profiles**（配置文件）。
3. 选择新的或已更新的 **URL Filtering**（**URL** 过滤）配置文件，将其附加到安全策略规则。
4. 选择 **OK**（确定）以保存安全策略规则。

STEP 7 | **Commit**（提交）配置。

STEP 8 | 监控防火墙检测到的凭据提交。

选择 ***ACC > Hosts Visiting Malicious URLs***（访问恶意 ***URL*** 的主机）可查看访问过恶意软件和网络钓鱼站点的用户数。

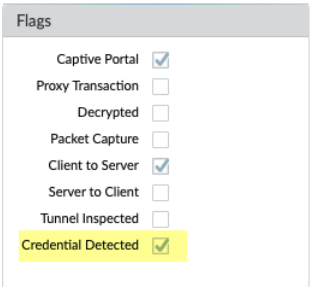
选择 **Monitor**（监控） **> Logs**（日志） **> URL Filtering**（**URL** 过滤）。

新的 **Credential Detected**（检测到的凭据）列显示防火墙检测到包含有效凭据的 HTTP 发布请求的事件：

	CATEGORY	APPLICATION	ACTION	CREDENTIAL DETECTED
	streaming-media		block-url	yes
	streaming-media		block-url	yes
	streaming-media		block-url	yes
	streaming-media		block-url	yes
	streaming-media		block-url	yes

要显示此列，将鼠标悬停在任何列标题上，然后单击箭头以选择要显示的列。

日志条目详细信息还显示凭据提交：



STEP 9 | 验证和解决凭据提交检测问题。

- 使用以下 CLI 命令查看凭据检测统计信息：

```
> show user credential-filter statistics
```

该命令的输出可能会有所不同，取决于为防火墙配置的用于检测凭据提交的方法。例如，如果在任何 URL 过滤配置文件中配置域凭据过滤器，则会显示将 bloom 过滤器转发到防火墙的 User-ID 代理列表，以及包含在 bloom 过滤器的凭据数。

- （仅限组映射法）使用以下 CLI 命令查看组映射信息，包括启用组映射凭据检测的 URL 过滤配置文件数，以及已尝试将凭据提交到受限站点的组成员的用户名。

```
> show user group-mapping statistics
```

- （仅限域凭据过滤器法）使用以下 CLI 命令查看正在向防火墙发送映射信息的所有基于 Windows 的 User-ID 代理：

```
> show user user-id-agent state all
```

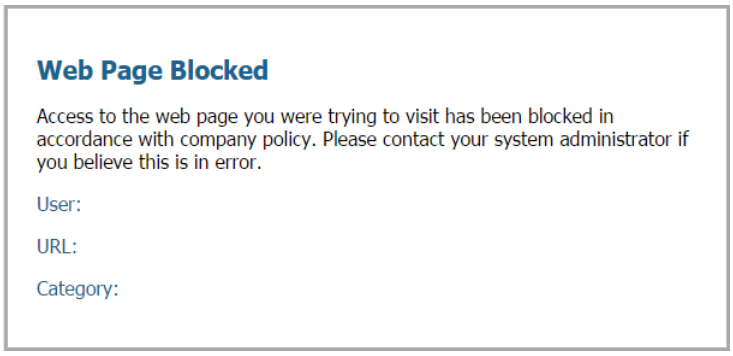
此命令的输出显示 bloom 过滤器计数情况，包括防火墙从每个代理接收到的 bloom 过滤器更新次数，以及自上次 bloom 过滤器更新以来过去的时间长度（以秒计算）（前提是任何 bloom 过滤器更新失败）。

- （仅限域凭据过滤器法）基于 Windows 的 User-ID 代理显示引用 BF（bloom 过滤器）推送到防火墙的日志消息。在 User-ID 代理界面中，选择 **Monitoring**（监控） > **Logs**（日志）。

URL 过滤响应页面

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)	❑ 高级 URL 过滤许可证（或旧版 URL 过滤许可证） 注意： • 旧版 *URL* 过滤许可证已停用，但仍支持有效的旧版许可证。 • Prisma Access 许可证包括 *Advanced URL Filtering* 功能。

当对请求的 URL 的访问受到限制时，URL 过滤响应页面会通知用户。如果某个站点属于已配置阻止、继续或覆盖操作的类别，或者对该站点或类别的凭据提交已被阻止，则访问可能会受到限制。如果用户没有为搜索引擎配置最严格的安全搜索设置，并且安全策略规则强制执行安全搜索，则访问也会受到限制。出于这些原因，共有五个预定义响应页面。一些回应页面直接阻止访问，而其他回应页面则允许有条件访问。例如，如果出现“URL 过滤继续和覆盖页面”或“反网络钓鱼继续页面”，则用户可以单击“继续”进入网站（除非启用了“URL 管理员覆盖”）。



一般情况下，响应页面会说明页面无法访问的原因，并列出用户、URL 和 URL 类别。但是，您可以自定义响应页面的内容和外观。例如，您可以更改通知消息、链接到可接受使用政策或添加企业品牌。

您可能会发现不同 *PAN-OS* 软件版本的响应页面外观有所不同。但其功能保持不变。

请记住，您可以自定义响应页面以满足您的特定需求。

如果启用了 SSL/TLS 握手检查，则浏览器不会显示响应页面。

- 预定义的 URL 过滤响应页面
- URL 过滤响应页面对象
- 自定义 URL 过滤响应页面

预定义的 URL 过滤响应页面

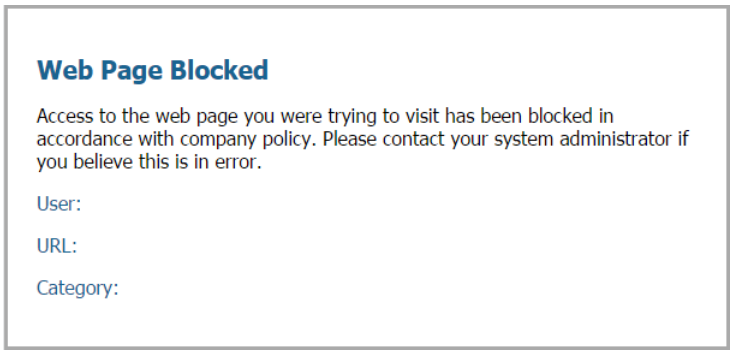
哪里可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ 高级 URL 过滤许可证（或旧版 URL 过滤许可证） 注意： • 旧版 *URL* 过滤许可证已停用，但仍支持有效的旧版许可证。 • Prisma Access 许可证包括 *Advanced URL Filtering* 功能。

当对请求的 URL 的访问受到限制时，Web 浏览器上会显示URL 过滤响应页面。每个响应页面都会解释为什么无法访问该页面，并且大多数页面会列出有关用户、请求的 URL 以及触发阻止操作的 URL 类别的信息。

您可能会发现不同 *PAN-OS* 软件版本的响应页面外观有所不同。但其功能保持不变。请记住，您可以自定义响应页面以满足您的特定需求。

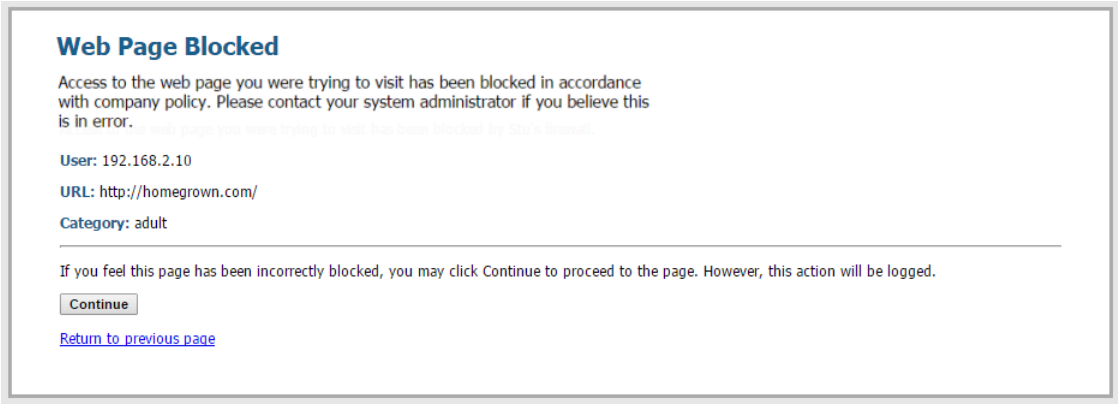
- **URL** 过滤和类别匹配阻止页面

  URL 过滤配置文件阻止访问，或因安全策略规则阻止 URL 类别而阻止访问。



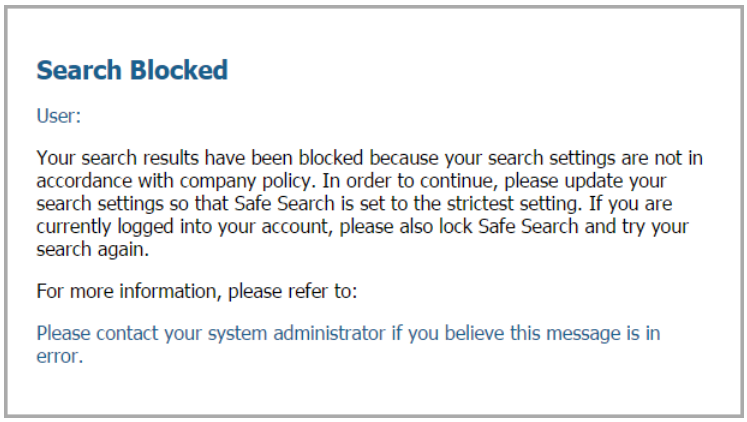
- **URL** 过滤继续和替代页面

  包含可使用户通过单击 **Continue**（继续）以绕过阻止的初始阻止策略的页面。如果启用 URL 管理替代（允许密码访问某些站点），单击 **Continue**（继续）后，用户必须提供密码才能替代阻止此 URL 的策略。



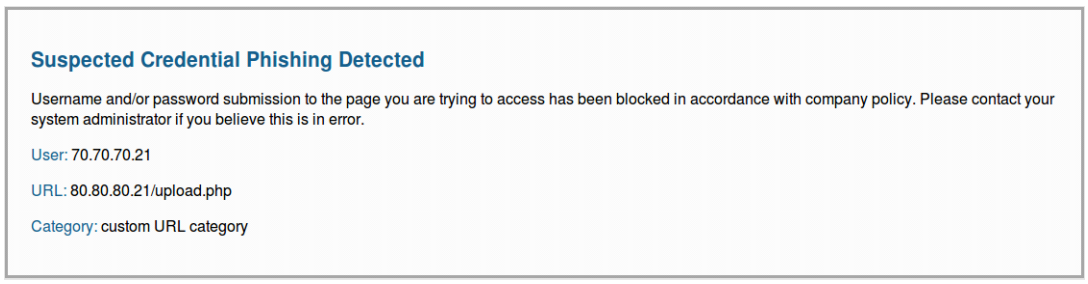
- **URL** 过滤安全搜索块页

  安全策略规则会阻止访问，该策略中的 URL 过滤配置文件已启用 Safe Search Enforcement（强制执行安全搜索）选项（参阅强制执行安全搜索）。如果使用 Google、Bing、Yahoo 或 Yandex 执行搜索，且其浏览器或搜索引擎帐户的安全搜索设置未设置为严格，则用户将看到此页面。



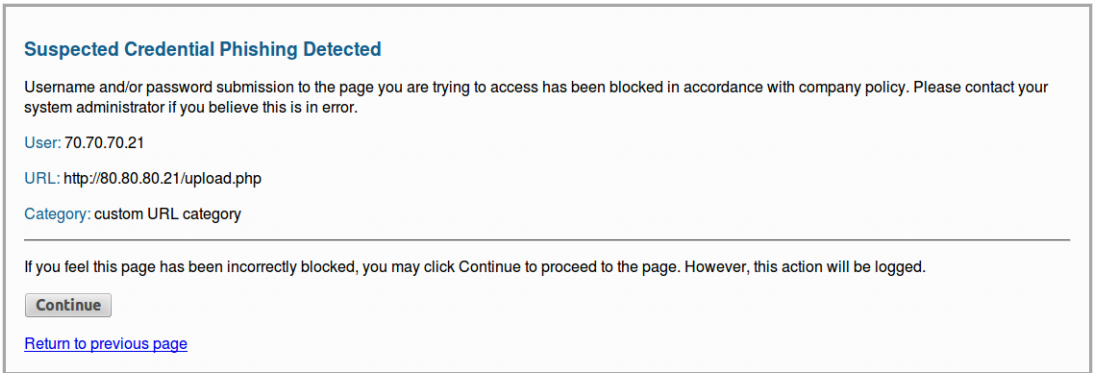
- 防钓鱼阻止页面

  当用户尝试在阻止凭据提交的类别中的网页上输入公司凭据（用户名或密码）时，向用户显示该页面。用户可以继续访问该站点，但仍然无法向任何关联的网络表单提交有效的公司凭据。要控制用户可以提交公司凭据的站点，您必须配置 User-ID 并启用基于 URL 类别的凭据网络钓鱼防护。



- 防钓鱼继续页面

  此页面警告用户不要将凭据（用户名和密码）提交到网站。警告用户不要提交凭据可以帮助阻止他们重复使用公司凭据，并向他们讲解有关可能的网络钓鱼尝试的风险。他们必须选择继续才能在站点上输入凭据。要控制用户可以提交公司凭据的站点，您必须配置 User-ID 并启用基于 URL 类别的凭据网络钓鱼防护。



URL 过滤响应页面对象

哪里可以使用？	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)	☐ 高级 URL 过滤许可证（或旧版 URL 过滤许可证） 注意： • 旧版 *URL* 过滤许可证已停用，但仍支持有效的旧版许可证。 • Prisma Access 许可证包括 *Advanced URL Filtering* 功能。

使用以下部分介绍的变量和引用来自定义 URL 过滤响应页面。响应页面变量显示有关 URL 请求的不同信息。例如，对于请求的 URL 的 URL 类别，防火墙取代了响应页面的 HTML 代码中的 `<category/>` 变量。响应页面引用使您能够添加外部图像、声音、样式表和链接。

响应页面变量

下表列出了响应页面变量以及系统在阻止事件期间替换每个变量的信息或对象。每个 URL 过滤响应页面默认使用以下变量：user、url、category。但是，响应页面是可定制的。例如，您可以修改变量的顺序或为特定的 URL 类别添加不同的消息。

变量	使用情况
<user/>	在显示响应页面时，防火墙会使用用户的用户名（如果可以通过 User-ID 加以使用）或 IP 地址来代替该变量。
<url/>	在显示响应页面时，防火墙会使用所请求的 URL 来代替该变量。

变量	使用情况
<category/>	防火墙会使用被阻止请求的 URL 过滤类别来代替该变量。
<pan_form/>	用于在“URL 过滤继续和替代”页面上显示 **Continue**（继续）按钮的 HTML 代码。

您还可以添加代码，以触发防火墙根据用户尝试访问的 URL 类别来显示不同的消息。例如，响应页面中的以下代码片段可指定在 URL 类别为 games 时显示消息 1，在类别为 travel 时显示消息 2，或在类别为 kids 时显示消息 3：

```
var cat = "<category/>"; switch(cat) { case 'games':
 document.getElementById("warningText").innerHTML = "Message 1";
 break; case 'travel':
 document.getElementById("warningText").innerHTML = "Message 2";
 break; case 'kids': document.getElementById("warningText").innerHTML
 = "Message 3"; break; }
```

响应页面引用

对于每个阻止页面类型，只能为每个虚拟系统加载一个 *HTML* 页面。但是，当浏览器中显示响应页面时，可以从其他服务器加载其他资源，如图像、声音和级联样式表（*CSS* 文件）。所有引用都必须包含完全限定 *URL*。

引用类型	示例 **HTML** 代码
映像	`<img src="http://virginiadot.org/images/Stop-Sign-gif.gif">`
声音	`<embed src="http://simplythebest.net/sounds/WAV/WAV_files/ movie_WAV_files/ do_not_go.wav" volume="100" hidden="true" autostart="true">`
样式表	`<link href="http://example.com/style.css" rel="stylesheet" type="text/css" />`
超链接	`<a href="http://en.wikipedia.org/wiki/Acceptable_use_policy">查看公司政策</a>`

自定义 URL 过滤响应页面

哪里可以使用？	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)	❑ 高级 URL 过滤许可证（或旧版 URL 过滤许可证） 注意： • 旧版 *URL* 过滤许可证已停用，但仍支持有效的旧版许可证。 • Prisma Access 许可证包括 *Advanced URL Filtering* 功能。

默认情况下，URL 过滤响应页面解释无法访问请求的 URL 的原因，并显示用户的 IP 地址、请求的 URL 和 URL 类别。您可以自定义响应页面以满足企业需求。例如，您可以更改向用户显示的消息、添加公司品牌或链接到可接受的使用政策。

要自定义页面，请将其从平台导出并在文本编辑器中进行修改。您可以使用提供的响应页面变量和引用进行更新。响应页面变量对应被阻止的特定用户、URL 和类别。响应页面引用允许使用图像、声音、样式表和链接。

Panorama™ Web 界面不支持导出响应页面。

大于最大支持大小的自定义响应页面不会被解密或向用户显示。在 *PAN-OS 8.1.2* 及更早的 *PAN-OS 8.1* 版本中，解密站点上的自定义响应页面不会超过 *8191* 字节；在 *PAN-OS 8.1.3* 及更高版本中，最大大小为 *17,999* 字节。

- Strata Cloud Manager
- PAN-OS 和 Panorama

自定义 URL 过滤响应页面 (Strata Cloud Manager)

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

切换到 ***PAN-OS*** 选项卡并遵循相应的指导。

如果您正在使用 ***Strata Cloud Manager***，请在此处继续。

STEP 1 | 导出您要自定义的默认响应页面。

1. 选择 **Manage**（管理） > **Configuration**（配置） > **NGFW** 和 **Prisma Access** > **Security Services**（安全服务） > **URL Access Management**（**URL** 访问管理） > **Settings**（设置）。
2. 在"响应页面"窗格中，单击要编辑的每个响应页面的 **Export HTML Template**（导出 **HTML** 模板）。
3. 将文件保存到您的系统。

STEP 2 | 编辑导出的响应页面。

1. 使用所选 HTML 文本编辑器编辑该页面：
   - 要显示与已阻止的特定用户、URL 或类别相关的自定义信息，请添加一个或多个响应页变量。
   - 要包括自定义图像、声音、样式表或链接，请包括一个或多个响应页面引用。
2. 使用新文件名保存编辑后的页面。

   确保该页面保持其 *UTF-8* 编码。例如，在“记事本”的“另存为”对话框中，从 *“Encoding*（编码）”下拉列表中选择 *UTF-8*。

STEP 3 | 导入自定义响应页面。

1. 选择 **Manage**（管理） > **Configuration**（配置） > **NGFW** 和 **Prisma Access** > **Security Services**（安全服务） > **URL Access Management**（**URL** 访问管理） > **Settings**（设置）。
2. 在“响应页面”窗格中，单击自定义的响应页面类型。随即出现文件选择对话框。

   例如，如果您自定义了 URL 访问管理阻止页面，则会单击 **URL Access Management Block Page**（**URL** 访问管理阻止页面）。
3. 单击 **Choose File**（选择文件），然后选择自定义的文件。
4. 单击 **Save**（保存）。

STEP 4 | 单击 **Push Config**（推送配置）。

STEP 5 | 验证是否显示自定义响应页面。

从 Web 浏览器访问将触发响应页面的网址。例如，要验证自定义的 URL 访问管理阻止页面，请访问被安全策略规则阻止的 URL。

防火墙使用以下端口显示 URL 访问管理响应页面：

- **HTTP**—6080
- **Default TLS with firewall certificate**（带防火墙证书的默认 **TLS**）—6081
- **Custom SSL/TLS profile**（自定义 **SSL/TLS** 配置文件）—6082

自定义 URL 过滤响应页面（PAN-OS 和 Panorama）

STEP 1 | 导出要自定义的预定义响应页面。

> *Panorama Web* 界面不支持导出响应页面。您可以直接从特定防火墙的 *Web* 界面导出响应页面，或使用 *Panorama Web* 界面上的 上下文下拉菜单 快速切换到托管防火墙的 *Web* 界面。

1. 选择 **Device**（设备） > **Response Pages**（响应页面）。
2. 选择要编辑的响应页面 **Type**（类型）。此时将显示特定响应页面的对话框。
3. 选择 **Predefined**（预定义），然后选择 **Export**（导出）。
4. **Close**（关闭）对话框。

   （可选）对于其他响应页面，请重复第 2 步到第 4 步。
5. 将文件保存到您的系统。

STEP 2 | 自定义导出的 HTML 响应页面。

1. 在首选文本编辑器中打开文件。
   - 要显示有关特定用户、请求的 URL 或阻止的 URL 类别的自定义信息，请使用响应页面变量。
   - 要集成自定义图像、声音、样式表或链接，请使用响应页面引用。
2. 使用新名称保存编辑的文件。

> 确保该页面保持其 *UTF-8* 编码。例如，在“记事本”的“另存为”对话框中，从 ***Encoding***（编码）下拉列表中选择 ***UTF-8***。

STEP 3 | 导入自定义响应页面。

1. 选择 **Device**（设备） > **Response Pages**（响应页面）。
2. 选择您编辑的响应页面 **Type**（类型）。此时将显示特定响应页面的对话框。
3. 选择 **Predefined**（预定义），然后选择 **Import**（导入）。此时将显示“导入文件”对话框。

   对于 **Import File**（导入文件），请 **Browse**（浏览）编辑的响应页面。
4. （可选）对于 **Destination**（目标），请选择将使用响应页面的虚拟系统，或者选择 **Shared**（共享）以使其对所有虚拟系统可用。
5. 单击 **OK**（确定），然后 **Close**（关闭）对话框。

STEP 4 | **Commit**（提交）更改。

STEP 5 | 测试自定义响应页面。

从 Web 浏览器访问触发特定响应页面的 URL。例如，要验证 URL 过滤和类别匹配响应页面，请访问安全策略规则中阻止的 URL。验证您的更改是否显示。

防火墙使用以下端口显示 URL 过滤响应页面：

- **HTTP**—6080
- **Default TLS with firewall certificate**（带防火墙证书的默认 **TLS**）—6081
- **Custom SSL/TLS profile**（自定义 **SSL/TLS** 配置文件）—6082

强制执行安全搜索

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)	❑ 高级 URL 过滤许可证（或旧版 URL 过滤许可证） 注意： • 旧版 *URL* 过滤许可证已停用，但仍支持有效的旧版许可证。 • Prisma Access 许可证包括 *Advanced URL Filtering* 功能。 • 透明安全搜索需要 Prisma Access 许可证（最低运行版本 4.1）。

许多搜索引擎都提供了安全搜索设置，使您可以从搜索结果中过滤掉成人内容。过滤器设置通常包括 `Moderate`、`Strict` 和 `Off`。您可以使用中等设置来仅过滤掉成人图像和视频，或者使用严格设置来过滤掉露骨的文字。教育机构、工作场所、儿童和成人均可受益于此安全搜索功能。但是，允许网络中的用户配置安全搜索设置并不总能提供您所需的保护。

为了保护您的网络免受成人内容的侵害，您可以对所有最终用户强制实施最严格的安全搜索设置，而不管他们当前的个人设置如何。最严格的安全搜索设置可提供最安全的浏览体验。首先，在 URL 过滤配置文件中选择 **Safe Search Enforcement**（强制执行安全搜索）选项。然后，将该配置文件应用于允许从信任区域中的客户端到互联网的流量的任何安全策略规则。

无论是搜索引擎提供商，还是 *Palo Alto Networks*，都无法保证完全的过滤准确性。搜索引擎将网站分为安全或不安全两类。因此，被归类为安全的网站可能包含露骨内容。*Palo Alto Networks* 仅根据搜索引擎的过滤机制强制进行过滤。

当用户使用 Bing、Yahoo、Yandex 或 YouTube 进行搜索，并且未将这些引擎的安全搜索设置设为最严格级别时，防火墙可以强制执行以下选项：

- 严格安全搜索关闭时阻止搜索结果（默认）— 防火墙会阻止最终用户查看搜索结果，直到他们将安全搜索设置设为最严格的可用选项。在这种情况下，浏览器会显示 URL 过滤安全搜索阻止页面。此响应页面让最终用户知道他们的搜索结果被阻止的原因，并包含用于搜索的搜索引擎的搜索设置的链接。

  由于 *Google* 安全搜索实施发生了变化，*Palo Alto Networks* 无法再检测 *Google SafeSearch* 是否已启用。因此，阻止方法不适用于 *Google* 搜索。相反，您可以使用 搜索提供商的安全搜索设置 中介绍的方法配置 *Google* 安全搜索。
- 强制严格安全搜索（仅支持 Yahoo 和 Bing 搜索引擎）— 防火墙自动且透明地强制执行最严格的安全搜索设置。具体来说，防火墙将搜索查询重定向到返回严格过滤的搜索结果的 URL，并更改所用搜索引擎的安全搜索偏好。要启用此功能，请将 URL 过滤安全搜索阻止页面文本替换

为过程中指定的文本。替换文本包含 JavaScript 代码，该代码使用用于搜索的搜索引擎的严格安全搜索参数重写搜索查询 URL。

使用此方法时，浏览器不会显示 *URL* 过滤安全搜索阻止页面。

- 透明安全搜索（仅限 Prisma Access 部署）— 在无法解密流量的情况下（例如，在提供访客互联网访问的商店），并且您想要阻止使用非托管设备（包括显示设备）的用户搜索受限、不适当或令人反感的材料，您可以在 Prisma Access 中使用透明安全搜索，它通过执行 FQDN 到 IP 映射将移动用户的搜索引擎查询解析到引擎的安全搜索门户。

通过查看每个受支持的搜索引擎的安全搜索设置，开始强制执行安全搜索。然后，决定哪种执行方法最适合您的情况。

- 搜索提供商的安全搜索设置
- 禁用“严格安全搜索”时阻止搜索结果
- 强制执行严格安全搜索
- 在 Prisma Access 中使用透明安全搜索

搜索提供商的安全搜索设置

哪里可以使用？	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)	☐ 高级 URL 过滤许可证（或旧版 URL 过滤许可证） 注意： • 旧版 *URL* 过滤许可证已停用，但仍支持有效的旧版许可证。 • Prisma Access 许可证包括 *Advanced URL Filtering* 功能。

每个搜索提供商的安全搜索设置各不相同，请查看以下设置了解详情。

搜索提供商	安全搜索设置说明
Google/YouTube	通过 Google 安全搜索虚拟 IP 地址在各台计算机上或整个网络中提供安全搜索： 针对个人计算机上的 **Google** 搜索的安全搜索强制执行 在 Google 搜索设置中，**Filter explicit results**（过滤显式结果）设置可启用安全搜索功能。启用后，该设置会以 FF= 的形式存储在浏览器 Cookie 中，并会在每次用户执行 Google 搜索时传递到服务器。 将 **safe=active** 附加到 Google 搜索查询 URL 还会启用最严格安全搜索设置。

搜索提供商	安全搜索设置说明
	针对使用虚拟 **IP** 地址的 **Google** 和 **YouTube** 搜索的安全搜索强制执行 在每次 Google 和 YouTube 搜索中，Google 提供的服务器会锁定安全搜索 (forcesafesearch.google.com) 设置。通过为 **`www.google.com`** 和 **`www.youtube.com`**（以及其他相关 Google 和 YouTube 国家/地区子域）添加 DNS 条目以将指向 **`forcesafesearch.google.com`** 的 CNAME 记录包含在您的 DNS 服务器配置中，您可以确保网络上的所有用户在每次执行 Google 或 TouTube 搜索时都会使用严格的安全搜索设置。但请记住，此解决方案与防火墙上的强制执行安全搜索不兼容。因此，如果您正在使用此选项在 Google 上执行安全搜索，最佳做法是通过创建自定义 URL 类别并将其添加到 URL 过滤配置文件中的阻止列表来阻止访问防火墙上的其他搜索引擎。 • *PAN-OS* 支持通过 *HTTP* 标头插入实施 *YouTube* 安全搜索。*HTTP/2* 当前不支持 *HTTP* 标头插入。要对 *YouTube* 强制执行安全搜索，App-ID 和 HTTP/2 检查 会在适当的解密配置文件中使用 ***Strip ALPN***（剥离 ***ALPN***）功能，将 *HTTP/2* 连接降级为 *HTTP/1.1*。 • 如果您计划使用 *Google Lock SafeSearch* 解决方案，请考虑配置 *DNS* 代理，导航路径为 ***Network***（网络）> ***DNS Proxy***（***DNS*** 代理），并将继承源设置为第 *3* 层接口，防火墙会在该接口上通过 *DHCP* 从服务提供商处接收 *DNS* 设置。您应使用 *www.google.com* 和 *www.youtube.com* 的 ***Static Entries***（静态条目）配置 *DNS* 代理，以便为 *forcesafesearch.google.com* 服务器使用本地 *IP* 地址。
Yahoo	仅在各台计算机上提供安全搜索。Yahoo 搜索首选项包含三个安全搜索设置：**Strict**（严格）、**Moderate**（中

搜索提供商	安全搜索设置说明
	等）或 **Off**（关闭）。启用后，该设置会以 `vm=` 的形式存储在浏览器 Cookie 中，并会在每次用户执行 Yahoo 搜索时传递到服务器。 将 `vm=r` 附加到 Yahoo 搜索查询 URL 还会启用最严格安全搜索设置。 如果在登录 *Yahoo* 帐户后在 *Yahoo Japan* (***yahoo.co.jp***) 执行搜索，终端用户还必须启用 ***SafeSearch***（安全搜索）***Lock***（锁定）选项。
Bing	在个人计算机上提供安全搜索。Bing 设置包含三个安全搜索设置：**Strict**（严格）、**Moderate**（中等）或 **Off**（关闭）。启用后，该设置会以 `adtl=` 的形式存储在浏览器 Cookie 中，并会在每次用户执行 Bing 搜索时传递到服务器。 将 **`adlt=strict`** 附加到 Bing 搜索查询 URL 还会启用最严格安全搜索设置。 Bing SSL 搜索引擎不会执行安全搜索 URL 参数，因此您应该考虑阻止基于 SSL 的 Bing，以便全面强制执行安全搜索。

禁用“严格安全搜索”时阻止搜索结果

哪里可以使用？	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)	❑ 高级 URL 过滤许可证（或旧版 URL 过滤许可证） 注意： • 旧版 *URL* 过滤许可证已停用，但仍支持有效的旧版许可证。 • Prisma Access 许可证包括 *Advanced URL Filtering* 功能。

如果启用强制执行安全搜索，则防火墙的默认行为是阻止最终用户在 Bing、Yahoo、Yandex 或 Youtube 搜索引擎上的搜索结果，直到他们将安全搜索设置为最严格的可用选项。默认情况下，URL 过滤安全搜索会阻止页面显示在浏览器中。预定义阻止页面提供指向所用搜索引擎的搜索设置的链接，以便用户可以调整安全搜索设置。您可以自定义安全搜索阻止页面以满足您组织的特定需求。

如果您计划使用此方法来强制执行安全搜索，请在实施之前将其告知您的最终用户。如果您希望自动将最终用户的搜索查询 URL 重定向到严格的安全搜索版本，请启用以透明方式执行严格安全搜索。

由于 *Google* 实施方式的变化，*Palo Alto Networks* 无法再检测 *Google* 安全搜索是否处于开启状态。因此，防火墙无法使用此方法强制实施安全搜索。您仍然可以透明地实施安全搜索。但是，我们无法保证 *Google* 会过滤掉露骨的图片和内容。

- Strata Cloud Manager
- PAN-OS 和 Panorama

阻止未启用严格安全搜索时的搜索结果 (Strata Cloud Manager)

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

切换到 ***PAN-OS*** 选项卡并遵循相应的指导。

如果您正在使用 ***Strata Cloud Manager***，请在此处继续。

STEP 1 | 在 URL 访问管理配置文件中启用安全搜索实施。

1. 选择 **Manage**（管理） > **Configuration**（配置） > **Security Services**（安全服务） > **URL Access Management**（URL 访问管理）。
2. 在 URL 访问管理配置文件下，选择现有配置文件或 **Add Profile**（添加配置文件）以创建新配置文件。随即会显示配置选项。
3. 在 **Settings**（设置）下，选择 **Safe Search Enforcement**（强制执行安全搜索）.
4. **Save**（保存）配置文件。

STEP 2 | （可选）限制最终用户可以访问的搜索引擎。

1. 选择 **Manage**（管理） > **Configuration**（配置） > **Security Services**（安全服务） > **URL Access Management**（URL 访问管理）。
2. 在 **Access Control**（访问控制）下，**Search**（搜索）（ ）**search-engines** 类别。
3. 将 **search-engines** 类别的站点访问设置为 **Block**（阻止）。

   在后续步骤中，将使用您想要允许的搜索引擎创建自定义 URL 类别（URL 列表类型）。
4. **Save**（保存）配置文件。

STEP 3 | 将 URL 访问管理配置文件应用到安全策略规则，这些规则允许从信任区域中的客户端到 Internet 的通信。

要激活 URL 访问管理配置文件（以及任何安全配置文件），请将其添加到 `profile group`，并在安全策略规则中引用该配置文件组。

STEP 4 | 为支持的搜索引擎创建自定义 URL 类别。

在下一步中，您将配置防火墙来解密到该自定义类别的通信。

1. 选择 **Manage**（管理） > **Configuration**（配置） > **Security Services**（安全服务） > **URL Access Management**（URL 访问管理）。

2. 在 **Access Control**（访问控制）下，对于自定义 URL 类别，请 **Add Category**（添加类别）。
3. 输入类别 **Name**（名称），如 **`SearchEngineDecryption`**。
4. 对于自定义 URL 类别的 **Type**（类型），请选择 **URL List**（**URL**列表）。
5. 在 **Items**（项目）下，将以下项目 **Add**（添加）到 URL 列表中：
   - **`www.bing.*`**
   - **`search.yahoo.*`**
   - **`yandex.com.*`**
6. **Save**（保存）自定义类别。
7. 为新自定义 URL 类别配置站点访问。
   1. 在“URL 访问管理配置文件”下，选择之前配置的配置文件。
   2. 在“访问控制”下，选择新的自定义 URL 类别。它会显示在外部动态 URL 列表和预定义类别上方的自定义 URL 类别部分中。
   3. 将 **Site Access**（站点访问）设置为 **Allow**（允许）。
   4. **Save**（保存）更改。

STEP 5 | 配置 SSL 转发代理解密。

由于大多数搜索引擎都会对其搜索结果进行加密，因此您必须启用 SSL 转发代理解密，以便防火墙能够检查搜索流量并检测安全搜索设置。

在解密策略规则的 **Services and URLs**（服务和 **URL**）部分下，单击 **Add URL Categories**（添加 **URL** 类别）。然后，选择您之前创建的自定义 URL 类别。新的自定义类别位于列表顶部。

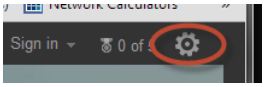
Save（保存）解密策略规则。

STEP 6 | 选择 **Push Config**（推送配置）以激活更改。

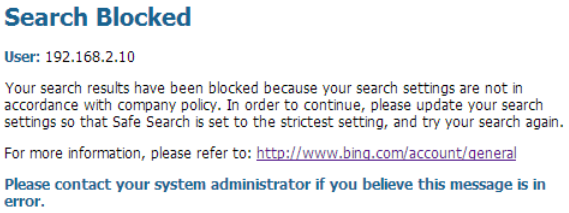
STEP 7 | 验证强制执行安全搜索配置。

仅当您正使用阻止页面执行安全搜索时，该验证步骤才会执行。如果您以透明方式启用安全搜索，则存在另一个验证步骤。

1. 从防火墙后面的计算机中，为受支持的搜索提供商禁用严格搜索设置。例如，在 bing.com 中，单击 Bing 菜单栏中的 **Preferences**（首选项）图标。



2. 将 **SafeSearch**（安全搜索）选项设置为 **Moderate**（中等）或 **Off**（关闭），然后单击 **Save**（保存）。
3. 执行 Bing 搜索（或使用其他提供商进行搜索），查看是否显示 URL 访问管理安全搜索阻止页面，而不是搜索结果：



4. 使用阻止页面上的链接将安全搜索设置更新为最严格的设置 [对于 Bing，设置为 **Strict**（严格）]，然后单击 **Save**（保存）。
5. 再次从 Bing 执行搜索，并验证显示的是经过筛选的搜索结果，而非阻止页面。

阻止未启用严格安全搜索时的搜索结果（PAN-OS 和 Panorama）

STEP 1 | 在 URL 过滤配置文件中启用强制执行安全搜索。

1. 选择 **Objects**（对象） > **Security Profiles**（安全配置文件） > **URL Filtering**（URL 过滤）。
2. 选择要修改的现有配置文件，或克隆默认配置文件以创建新配置文件。
3. 在 **URL Filtering Settings**（URL 过滤设置）选项卡上，选择 **Safe Search Enforcement**（安全实施）。

STEP 2 | （可选）限制最终用户在同一 URL 过滤配置文件中可以访问的搜索引擎。

1. 在 **Categories**（类别）选项卡中，将 **search-engines** 类别设置为 **Search**（搜索）（ ）。
2. 将 **search-engines** 类别的站点访问设置为 **Block**（阻止）。

   在后续步骤中，将使用您想要允许的搜索引擎创建自定义 URL 类别（URL 列表类型）。
3. 单击 **OK**（确定）保存配置文件。

STEP 3 | 将 URL 过滤配置文件应用到安全策略规则中，以允许来自互联网信任区域内客户端的流量。

1. 选择 **Policies**（策略） > **Security**（安全）。然后，单击要应用 URL 过滤配置文件的规则。
2. 在 **Actions**（操作）选项卡上，找到“配置文件设置”。对于 **Profile Type**（配置文件类型），选择 **Profiles**（配置文件）。随即将显示配置文件列表。
3. 对于 **URL Filtering**（**URL** 过滤）配置文件，请选择您之前创建的配置文件。
4. 单击 **OK**（确定）以保存安全策略规则。

STEP 4 | 为支持的搜索引擎创建自定义 URL 类别。

在下面的步骤中，您将指定想要解密自定义类别中网站的流量。

1. 选择 **Objects**（对象） > **Custom Objects**（自定义对象） > **URL Category**（**URL** 类型）并 **Add**（添加）自定义类别。
2. 输入类别 **Name**（名称），如 **`SearchEngineDecryption`**。
3. 将以下内容 **Add**（添加）到 **Sites**（站点）列表中：
   - **`www.bing.*`**
   - **`search.yahoo.*`**
   - **`yandex.com.*`**
4. 单击 **OK**（确定）以保存自定义类别。
5. 为新自定义 URL 类别配置站点访问。
   1. 转到 **Objects**（对象） > **Security Profiles**（安全配置文件） > **URL Filtering**（**URL** 过滤），然后选择之前配置的 URL 过滤配置文件。
   2. 在 **Category**（类别）选项卡上，选择新的自定义 URL 类别。它显示在外部动态 URL 列表和预定义类别上方的自定义 URL 类别部分。
   3. 将 **Site Access**（站点访问）设置为 **Allow**（允许）。
   4. 单击 **OK**（确定）保存更改。

STEP 5 | 配置 SSL 转发代理解密。

由于大多数搜索引擎都会对其搜索结果进行加密，因此您必须启用 SSL 转发代理解密，以便防火墙能够检查搜索流量并检测安全搜索设置。

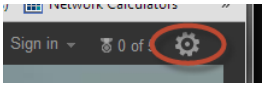
在解密策略规则的 **Service/URL Category**（服务/**URL** 类别）选项卡中，**Add**（添加）刚才创建的自定义 URL 类别。然后单击 **OK**（确定）。

STEP 6 | **Commit**（提交）更改。

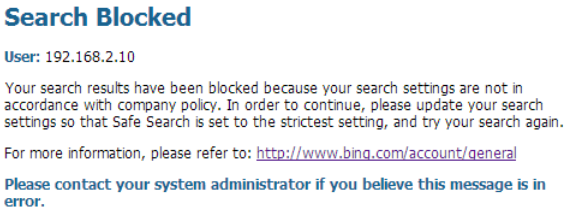
STEP 7 | 验证强制执行安全搜索的配置。

仅当您正使用阻止页面执行安全搜索时，该验证步骤才会执行。如果您以透明方式启用安全搜索，则存在另一个验证步骤。

1. 从防火墙后面的计算机中，为受支持的搜索提供商禁用严格搜索设置。例如，在 bing.com 中，单击 Bing 菜单栏中的 **Preferences**（首选项）图标。



2. 将 **SafeSearch**（安全搜索）选项设置为 **Moderate**（中等）或 **Off**（关闭），然后单击 **Save**（保存）。
3. 执行 Bing 搜索（或使用其他提供程序搜索），以查看是否显示 URL 过滤安全搜索阻止页面，而不是搜索结果：



4. 使用阻止页面上的链接将安全搜索设置更新为最严格的设置 [对于 Bing，设置为 **Strict**（严格）]，然后单击 **Save**（保存）。
5. 再次从 Bing 执行搜索，并验证经过过滤的搜索结果，而非验证阻止页面。

强制执行严格安全搜索

哪里可以使用？	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)	❑ 高级 URL 过滤许可证（或旧版 URL 过滤许可证） 注意： • 旧版 *URL* 过滤许可证已停用，但仍支持有效的旧版许可证。 • Prisma Access 许可证包括 *Advanced URL Filtering* 功能。

通过透明启用严格的安全搜索，您可以为 Bing 和 Yahoo 最终用户提供安全无缝的搜索体验。当最终用户在没有启用严格安全搜索的情况下进行搜索时，防火墙不会阻止搜索结果，而是会自动打开严格安全搜索，并且仅返回严格过滤的搜索结果。例如，学校和图书馆可以受益于自动执行，以确保一致的学习体验。

要激活以透明方式强制执行安全搜索，您需要在 URL 过滤配置文件中启用安全搜索实施，并使用以下过程中提供的文本替换 URL 过滤安全搜索阻止页面文件中的文本。替换文本包含 JavaScript，从而为用于搜索的搜索引擎附加具有严格安全搜索参数的搜索查询 URL。

浏览器中不显示 *URL* 过滤安全搜索阻止页面。

完成这些步骤后，防火墙将在终端用户进行搜索时执行 JavaScript。例如，假设学生在研究可能产生不适当结果的概念时，将 Bing SafeSearch 首选项设置为 `Off`（关）。防火墙检测到安全搜索首选项后，会将 `&adlt=strict` 附加到搜索查询 URL。然后，搜索引擎显示适当的结果，SafeSearch 首选项更改为 `Strict`（严格）。

- Strata Cloud Manager
- PAN-OS 和 Panorama

强制执行严格安全搜索 (Strata Cloud Manager)

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

切换到 ***PAN-OS & Panorama***（***PAN-OS*** 和 ***Panorama***）选项卡，然后按照其中的指导操作。

如果您正在使用 ***Strata Cloud Manager***，请在此处继续。

STEP 1 | 在 URL 访问管理配置文件中启用安全搜索实施。

1. 选择 **Manage**（管理）> **Configuration**（配置）> **Security Services**（安全服务）> **URL Access Management**（**URL** 访问管理）。
2. 在 URL 访问管理配置文件下，选择现有配置文件或 **Add Profile**（添加配置文件）以创建新配置文件。随即会显示配置选项。
3. 在 **Settings**（设置）下，选择 **Safe Search Enforcement**（强制执行安全搜索）.
4. **Save**（保存）配置文件。

STEP 2 | （可选）限制最终用户可以访问的搜索引擎。

1. 选择 **Manage**（管理）> **Configuration**（配置）> **Security Services**（安全服务）> **URL Access Management**（**URL** 访问管理）。
2. 在 **Access Control**（访问控制）下，**Search**（搜索）（ ）**search-engines** 类别。
3. 将 **search-engines** 类别的站点访问设置为 **Block**（阻止）。

   在后续步骤中，将使用您想要允许的搜索引擎创建自定义 URL 类别（URL 列表类型）。
4. **Save**（保存）配置文件。

STEP 3 | 将 URL 访问管理配置文件应用到安全策略规则，这些规则允许从信任区域中的客户端到 Internet 的通信。

要激活 URL 访问管理配置文件（以及任何安全配置文件），请将其添加到 `profile group`，并在安全策略规则中引用该配置文件组。

STEP 4 | 编辑 URL 访问管理安全搜索阻止页面，使用 JavaScript 替换现有代码，以便重写搜索查询 URL。

1. 选择 **Manage**（管理）> **Configuration**（配置）> **Security Services**（安全服务）> **URL Access Management**（**URL** 访问管理）> **Response Pages**（响应页面）。
2. 为 URL 访问管理阻止页面 **Export HTML Template**（导出 **HTML** 模板）。

3. 使用 HTML 编辑器将所有现有的阻止页面文本替换为以下文本。然后，保存该文件。

```
<html> <head> <title>Search Blocked</title> <meta http-
equiv="Content-Type" content="text/html; charset=utf-8">
 <meta http-equiv="pragma" content="no-cache"> <meta
 name="viewport" content="initial-scale=1.0"> <style> #content
 { border:3px solid#aaa; background-color:#fff; margin:1.5em;
 padding:1.5em; font-family:Tahoma,Helvetica,Arial,sans-serif;
 font-size:1em; } h1 { font-size:1.3em; font-weight:bold;
 color:#196390; } b { font-weight:normal; color:#196390; }
 </style> </head> <body bgcolor="#e7e8e9"> <div id="content">
 <h1>Search Blocked</h1> <p> <b>User:</b><user/> </p> <p>由
于搜索设置不符合公司政策，搜索结果已被阻止。如要继续，请更新搜索设置，以
将 Safe Search（安全搜索）设置为最严格的设置。如果您当前已登录帐户，请
同时锁定“安全搜索”，然后尝试重新搜索。</p><p> 有关更多信息，请参阅：<a
 href="<ssurl/>"> <ssurl/> </a> </p> <p id="java_off"> 请在浏览
器中启用 JavaScript。<br></p><p><b>如果您认为此消息有误，请联系系统管
理员。</b></p></div></body><script>//抓取浏览器中的网址。var s_u =
 location.href; //bing //匹配开头的正斜杠，任何内容，然后是“.bing.”，
再是任何内容，最后是非穷尽斜杠。Hopefully the first forward slash.
 var b_a = /^.*\/\/(.+\.bing\..+?)\//.exec(s_u); if (b_a)
 { s_u = s_u + "&adlt=strict"; window.location.replace(s_u);
 document.getElementById("java_off").innerHTML = 'You
 are being redirected to a safer search!'; } //yahoo //
 Matches the forward slashes in the beginning, anything,
 then ".yahoo."" then anything followed by a non greedy
 slash.希望是第一个正斜杠。var y_a = /^.*\/\/(.+\.yahoo\..
+?)\//.exec(s_u); if (y_a) { s_u = s_u.replace(/&vm=p/
ig,""); s_u = s_u + "&vm=r"; window.location.replace(s_u);
 document.getElementById("java_off").innerHTML =
 'You are being redirected to a safer search!'; }
 document.getElementById("java_off").innerHTML = ' '; </
script> </html>
```

STEP 5 | 将经过编辑的 URL 访问管理安全搜索阻止页面导入防火墙。

1. 选择 **Manage**（管理） > **Configuration**（配置） > **Security Services**（安全服务） > **URL Access Management**（URL 访问管理） > **Response Pages**（响应页面）。
2. 单击 URL 访问管理安全搜索阻止页面。此时将显示一个对话框，其中包含 **Choose File**（选择文件）选项。
3. 选择之前编辑的安全搜索阻止页面文件，然后单击 **Save**（保存）。

STEP 6 | 为支持的搜索引擎创建自定义 URL 类别。

在下一步中，您将配置防火墙来解密到该自定义类别的通信。

1. 选择 **Manage**（管理） > **Configuration**（配置） > **Security Services**（安全服务） > **URL Access Management**（**URL** 访问管理）。
2. 在 **Access Control**（访问控制）下，对于自定义 URL 类别，请 **Add Category**（添加类别）。
3. 输入类别 **Name**（名称），如 **`SearchEngineDecryption`**。
4. 对于自定义 URL 类别的 **Type**（类型），请选择 **URL List**（**URL**列表）。
5. 在 **Items**（项目）下，将以下项目 **Add**（添加）到 URL 列表中：
   - **`www.bing.*`**
   - **`search.yahoo.*`**
   - **`yandex.com.*`**
6. **Save**（保存）自定义类别。
7. 为新自定义 URL 类别配置站点访问。
   1. 在“URL 访问管理配置文件”下，选择之前配置的配置文件。
   2. 在“访问控制”下，选择新的自定义 URL 类别。它会显示在外部动态 URL 列表和预定义类别上方的自定义 URL 类别部分中。
   3. 将 **Site Access**（站点访问）设置为 **Allow**（允许）。
   4. **Save**（保存）更改。

STEP 7 | 配置 SSL 转发代理解密。

由于大多数搜索引擎都会对其搜索结果进行加密，因此您必须启用 SSL 转发代理解密，以便防火墙能够检查搜索流量并检测安全搜索设置。

在解密策略规则的 **Services and URLs**（服务和 **URL**）部分下，单击 **Add URL Categories**（添加 **URL** 类别）。然后，选择您之前创建的自定义 URL 类别。新的自定义类别位于列表顶部。

Save（保存）解密策略规则。

STEP 8 | 选择 **Push Config**（推送配置）以激活更改。

STEP 9 | 验证强制执行安全搜索的配置。

从位于防火墙后面的计算机中，打开浏览器并使用 Bing、Yahoo 或 Yandex 执行搜索。然后，使用以下方法之一验证您的配置：

- 检查 URL 的查询字符串以获取安全的搜索参数。搜索提供商的安全搜索设置列出了附加到每个搜索查询 URL 的安全搜索参数。
- 转到受支持的搜索引擎的安全搜索设置，并验证所选的 SafeSearch 首选项是否为最严格级别 [大多数情况下为 **Strict**（严格）级别]。

强制执行严格安全搜索（PAN-OS 和 Panorama）

STEP 1 | 确保防火墙正在运行 Content Release V475 或更高版本。

1. 选择 **Device**（设备） > **Dynamic Updates**（动态更新）。
2. 检查 **Applications and Threats**（应用程序和威胁）部分以确定当前正在运行的更新。
3. 如果防火墙并未运行所需更新或更高版本，请单击 **Check Now**（立即检查）以检索可用更新列表。
4. 找到所需更新并单击 **Download**（下载）。
5. 下载完成后，单击 **Install**（安装）。

STEP 2 | 在 URL 过滤配置文件中启用强制执行安全搜索。

1. 选择 **Objects**（对象） > **Security Profiles**（安全配置文件） > **URL Filtering**（URL 过滤）。
2. 选择要修改的现有配置文件，或克隆默认配置文件以创建新配置文件。
3. 在 **URL Filtering Settings**（URL 过滤设置）选项卡上，选择 **Safe Search Enforcement**（安全实施）。

STEP 3 | （可选）限制最终用户在同一 URL 过滤配置文件中可以访问的搜索引擎。

1. 在 **Categories**（类别）选项卡中，将 **search-engines** 类别设置为 **Search**（搜索）（ ）。
2. 将 **search-engines** 类别的站点访问设置为 **Block**（阻止）。

   在后续步骤中，将使用您想要允许的搜索引擎创建自定义 URL 类别（URL 列表类型）。
3. 单击 **OK**（确定）保存配置文件。

STEP 4 | 将 URL 过滤配置文件应用到安全策略规则中，以允许来自互联网信任区域内客户端的流量。

1. 选择 **Policies**（策略） > **Security**（安全）。然后，单击要应用 URL 过滤配置文件的规则。
2. 在 **Actions**（操作）选项卡上，找到“配置文件设置”。对于 **Profile Type**（配置文件类型），选择 **Profiles**（配置文件）。随即将显示配置文件列表。
3. 对于 **URL Filtering**（URL 过滤）配置文件，选择您之前创建的配置文件。
4. 单击 **OK**（确定）以保存安全策略规则。

STEP 5 | 编辑 URL 过滤安全搜索阻止页面，将现有代码替换为 JavaScript 以重写搜索查询 URL。

1. 选择 **Device**（设备） > **Response Pages**（响应页面） > **URL Filtering Safe Search Block Page**（URL 过滤安全搜索阻止页面）。
2. 选择 **Predefined**（预定义），然后单击 **Export**（导出）以将文件保存在本地。
3. 使用 HTML 编辑器将所有现有的阻止页面文本替换为以下文本。然后，保存该文件。

```
<html> <head> <title>Search Blocked</title> <meta http-
equiv="Content-Type" content="text/html; charset=utf-8">
 <meta http-equiv="pragma" content="no-cache"> <meta
 name="viewport" content="initial-scale=1.0"> <style> #content
 { border:3px solid#aaa; background-color:#fff; margin:1.5em;
 padding:1.5em; font-family:Tahoma,Helvetica,Arial,sans-serif;
```



```
 font-size:1em; } h1 { font-size:1.3em; font-weight:bold;
 color:#196390; } b { font-weight:normal; color:#196390; }
 </style> </head> <body bgcolor="#e7e8e9"> <div id="content">
 <h1>Search Blocked</h1> <p> <b>User:</b><user/> </p> <p>由
于搜索设置不符合公司政策，搜索结果已被阻止。如要继续，请更新搜索设置，以
将 Safe Search（安全搜索）设置为最严格的设置。如果您当前已登录帐户，请
同时锁定“安全搜索”，然后尝试重新搜索。</p><p> 有关更多信息，请参阅：<a
 href="<ssurl/>“> <ssurl/> </a> </p> <p id="java_off"> 请在浏览
器中启用 JavaScript。<br></p><p><b>如果您认为此消息有误，请联系系统管
理员。</b></p></div></body><script>//抓取浏览器中的网址。var s_u =
 location.href; //bing //匹配开头的正斜杠，任何内容，然后是“.bing.”，
再是任何内容，最后是非穷尽斜杠。Hopefully the first forward slash.
 var b_a = /^.*\/\/(.+\.bing\..+?)\//.exec(s_u); if (b_a)
 { s_u = s_u + "&adlt=strict"; window.location.replace(s_u);
 document.getElementById("java_off").innerHTML = 'You
 are being redirected to a safer search!'; } //yahoo //
 Matches the forward slashes in the beginning, anything,
 then ".yahoo."" then anything followed by a non greedy
 slash.希望是第一个正斜杠。var y_a = /^.*\/\/(.+\.yahoo\..
+?)\//.exec(s_u); if (y_a) { s_u = s_u.replace(/&vm=p/
ig,""); s_u = s_u + "&vm=r"; window.location.replace(s_u);
 document.getElementById("java_off").innerHTML =
 'You are being redirected to a safer search!'; }
 document.getElementById("java_off").innerHTML = ' '; </
script> </html>
```

STEP 6 | 将经过编辑的 URL 过滤安全搜索阻止页面导入到防火墙。

1. 选择 **Device**（设备） > **Response Pages**（响应页面） > **URL Filtering Safe Search Block Page**（**URL** 过滤安全搜索阻止页面）。
2. 单击 **Import**（导入）。然后，**Browse**（浏览）阻止页文件或在 **Import File**（导入文件）字段中输入路径和文件名。
3. （可选）对于 **Destination**（目标），选择将使用登录页面的虚拟系统或 **Shared**（共享）登录页面，以使其可供所有虚拟系统使用。
4. 单击 **OK**（确定）以导入文件。

STEP 7 | 为支持的搜索引擎创建自定义 URL 类别。

在下一步中，您将配置防火墙来解密到该自定义类别的通信。

1. 选择 **Objects**（对象） > **Custom Objects**（自定义对象） > **URL Category**（**URL** 类型）并 **Add**（添加）自定义类别。
2. 输入类别 **Name**（名称），如 **SearchEngineDecryption**。
3. 将以下内容 **Add**（添加）到 **Sites**（站点）列表中：
   - **www.bing.***
   - **search.yahoo.***
   - **yandex.com.***
4. 单击 **OK**（确定）以保存自定义 URL 类别。

STEP 8 | 配置 SSL 转发代理解密。

由于大多数搜索引擎都会对其搜索结果进行加密，因此您必须启用 SSL 转发代理解密，以便防火墙能够检查搜索流量并检测安全搜索设置。

在解密策略规则的 **Service/URL Category**（服务/URL 类别）选项卡中，**Add**（添加）刚才创建的自定义 URL 类别。然后单击 **OK**（确定）。

STEP 9 | **Commit**（提交）更改。

STEP 10 | 验证强制执行安全搜索的配置。

在防火墙后的计算机上，打开浏览器并使用 Bing 或 Yahoo 进行搜索。然后，使用以下方法之一来验证您的配置是否按预期运行：

- 检查 URL 的查询字符串以获取安全的搜索参数。搜索提供商的安全搜索设置列出了附加到每个搜索查询 URL 的安全搜索参数。
- 转到搜索引擎的安全搜索设置，验证所选的安全搜索首选项是否为最严格的级别 [Bing 为 **Strict**（严格）]。

在 Prisma Access 中使用透明安全搜索

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) 如果您想在 Prisma Access 环境中使用此功能，请与客户团队联系以了解更多信息。	❑ 运行最低版本 4.1 的 Prisma Access 部署 ❑ Prisma Access 许可证

Prisma Access 允许您通过执行 FQDN 到 IP 映射将移动用户的搜索引擎查询解析到引擎的安全搜索门户。当无法解密流量（例如，在提供访客互联网访问的商店），并且您想要阻止使用非托管设备（包括显示设备）的用户搜索受限制、不适当或令人反感的材料时，使用透明安全搜索作为实施严格安全搜索的替代方案。

- Strata Cloud Manager
- Panorama

在 Prisma Access 中使用透明安全搜索 (Strata Cloud Manager)

在 Strata Cloud Manager 中，要为 Prisma Access 配置透明安全搜索支持，请完成以下步骤。您可以为远程网络或 GlobalProtect 移动用户配置透明安全搜索。

STEP 1 | 选择您想要配置安全搜索的部署类型（移动用户或远程网络）。

- 对于移动用户 — GlobalProtect 部署，请转到 **Manage**（管理） > **Service Setup**（服务设置） > **Mobile Users**（移动用户）；然后，选择 **GlobalProtect Setup**（**GlobalProtect** 设置） > **Infrastructure Settings**（基础架构设置）。

  如果使用 Strata Cloud Manager，请转到 **Workflows**（工作流程） > **Prisma Access Setup**（**Prisma Access** 设置） > **Mobile Users**（移动用户）；然后，选择 **GlobalProtect Setup**（**GlobalProtect** 设置） > **Infrastructure Settings**（基础架构设置）。

- 对于 Remote Network（远程网络）部署，请转到 **Manage**（管理） > **Service Setup**（服务设置） > **Remote Networks**（远程网络）。

  如果使用 Strata Cloud Manager，请转到 **Workflows**（工作流） > **Prisma Access Setup**（**Prisma Access** 设置） > **Remote Networks**（远程网络）。

STEP 2 | 选择 **Advanced Settings**（高级设置）。

STEP 3 | 使用 **Static Entries**（静态条目）以将 FQDN 解析为特定的 IP 地址。

STEP 4 | 输入静态条目规则的唯一 **Name**（名称）、搜索引擎的 **FQDN** 以及应定向 FQDN 请求的搜索引擎的安全搜索 IP **Address**（地址）。

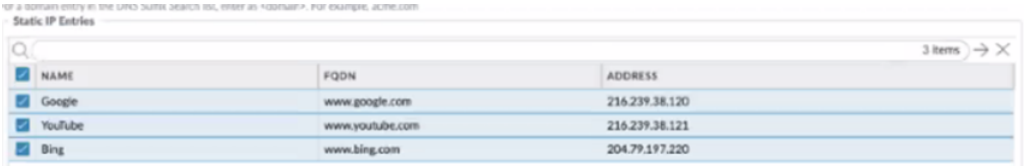
在 Prisma Access 中使用透明安全搜索 (Panorama)

在 Panorama 中，要为 Prisma Access 配置透明安全搜索支持，请完成以下步骤。您可以为远程网络或 GlobalProtect 移动用户配置透明安全搜索。

STEP 1 | 选择要为其配置 SafeSearch 的部署类型（远程网络或移动用户）。

- 对于移动用户 — GlobalProtect部署，请转到 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > 移动用户 — **GlobalProtect**，在 **Onboarding**（初始配置）区域选择 **Configure**（配置）；然后，选择 **Network Services**（网络服务）。
- 对于远程网络部署，请转到 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Remote Networks**（远程网络），请单击齿轮图标以编辑 **Settings**（设置）；然后选择 **DNS Proxy**（**DNS** 代理）。

STEP 2 | 通过输入静态输入规则的的唯一 **Name**（名称）、搜索引擎的 **FQDN** 和搜索引擎的 SafeSearch IP **Address**（地址）来输入 **Static IP Entries**（静态 **IP** 条目）。



与第三方远程浏览器隔离提供商集成

哪里可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager)	❑ 高级 URL 过滤许可证 注意：Prisma Access 许可证包括 *Advanced URL Filtering* 功能。

虽然这是最安全的操作，但阻止未知和有风险的网站可能会破坏用户的体验和工作效率。远程浏览器隔离 (RBI) 将用户从未知或有危险的站点重定向到由 RBI 提供商托管的隔离环境。该网站为用户呈现，他们可以查看所需的资源，而无需从他们的终端直接访问未知或有风险的网站。

Prisma Access 可轻松与 RBI 提供商集成，以便实现此类浏览器重定向。只需一两步，您就可以选择要集成的 RBI 提供商，然后选择要定向到 RBI 提供商托管环境的 URL 类别。

除了第三方 *RBI* 提供商外，*Palo Alto Networks* 的远程浏览器隔离 (RBI) 功能也可以与 *Prisma Access* 集成。与其他隔离解决方案不同，*RBI* 使用新一代隔离技术，为访问网站的用户提供近乎原生的体验，同时又不影响安全性。

以下是 Prisma Access 可集成的 RBI 提供商 — 某些提供商可能要求您添加 RBI 环境详细信息（例如，没有实名地址的 URL 或租户 ID）到 Strata Cloud Manager，以便设置集成：

- ❑ **Palo Alto Networks** 的 **RBI**

  要与 *Palo Alto Networks* 的 *RBI* 集成，您需要配置远程浏览器隔离。
- ❑ **Authentic8**

  要与 *Authentic8* 集成，请准备好 *Authentic8 RBI* 环境没有实名地址的 *URL*。
- ❑ **Proofpoint**

  要与 *Proofpoint* 集成，请准备好选择使用适用于 *RBI* 的 *Proofpoint* 生产或 *PoC* 环境。
- ❑ **Ericom**

  要与 *Ericom* 集成，请准备好 *Ericom RBI* 环境的租户 *ID*。
- ❑ **Menlo Security**

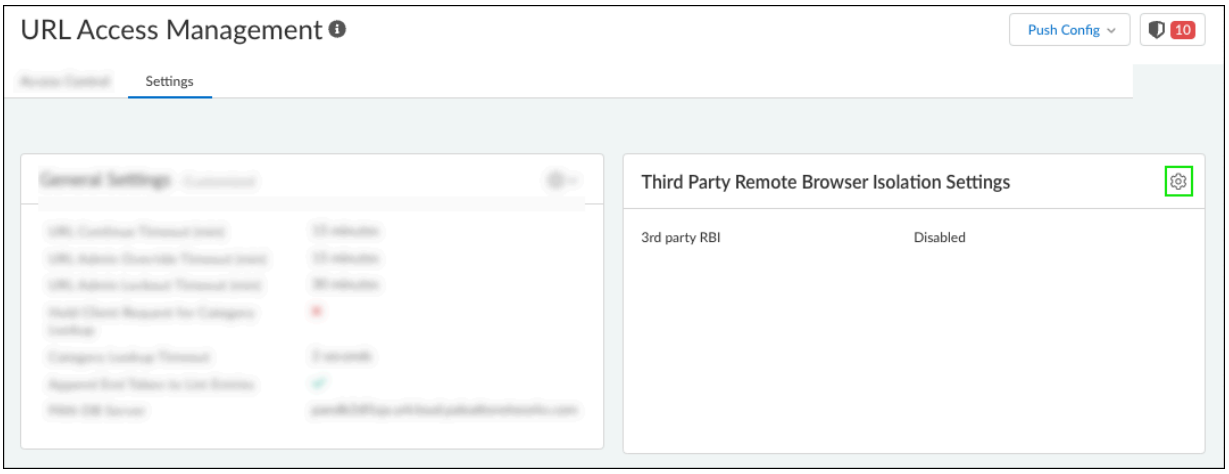
  您不需要为 *Menlo Security RBI* 环境配置任何设置；您只需要启用集成。

以下介绍如何将第三方 RBI 提供商添加到 Strata Cloud Manager，以及如何指定将用户重定向到 RBI 环境的 URL 类别。

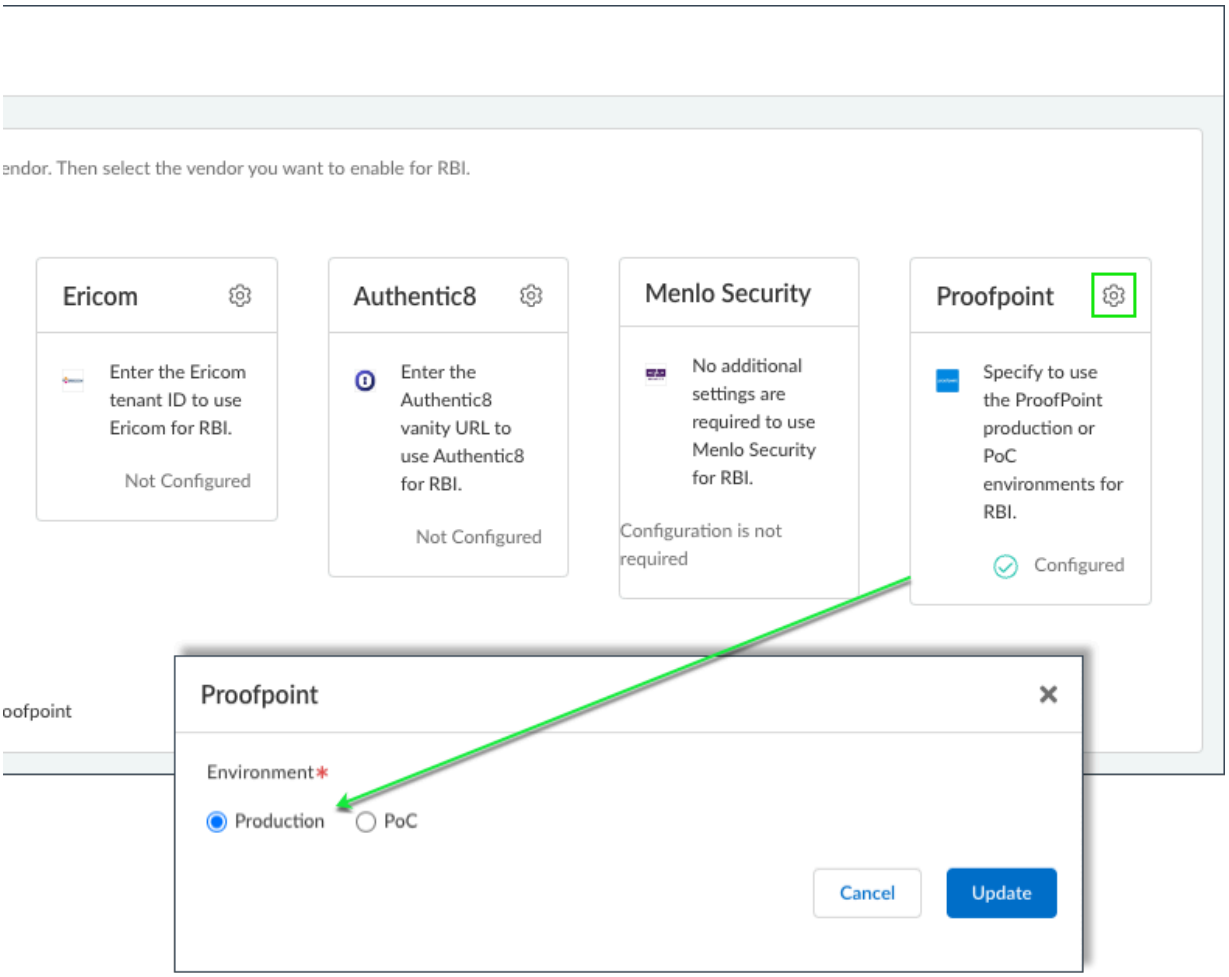
STEP 1 | 设置远程浏览器隔离 (RBI)。

- 转到 **Manage**（管理） > **Configuration**（配置） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Security Services**（安全服务） > **URL Access Management**（**URL** 访问管理） > **Settings**（设置），并打开 **Third Party Remote Browser Isolation Settings**（第三方远程浏览器隔离设置）。

- 如果您的 **Web** 安全管理员：导航至 **Manage**（管理） > **Configuration**（配置） > **Web Security**（**Web** 安全） > **Threat Management**（威胁管理），并打开 **Third Party Remote Browser Isolation Settings**（第三方远程浏览器隔离设置）。

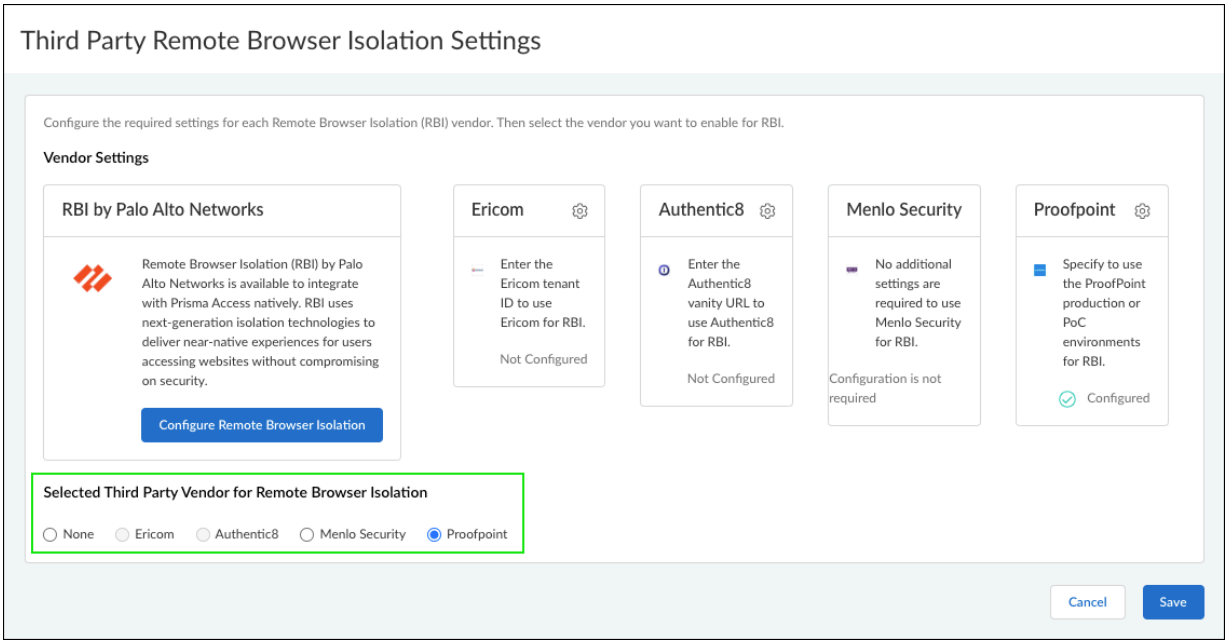


STEP 2 | 检查您的 RBI 是否要求您指定要使用的 RBI 环境；如果是，请输入所需的设置。



STEP 3 | 然后，选择您想要启用的第三方 RBI 提供商并 **Save**（保存）。就是这样#当您下次 **Push Config**（推送配置）时，您的 RBI 提供商将与 Prisma Access 集成。

如果您已经购买并激活 Palo Alto Networks 的 RBI 许可证，则还可以配置远程浏览器隔离。但是，您不能同时使用 *Palo Alto Networks* 的 *RBI* 和第三方 *RBI* 供应商进行隔离。如果选择使用 *Palo Alto Networks* 的 *RBI*，请选择 ***None***（无），否则，请从 ***Selected Third Party Vendor for Remote Browser Isolation***（为远程浏览器隔离选择的第三方供应商）中选择第三方 *RBI* 供应商。

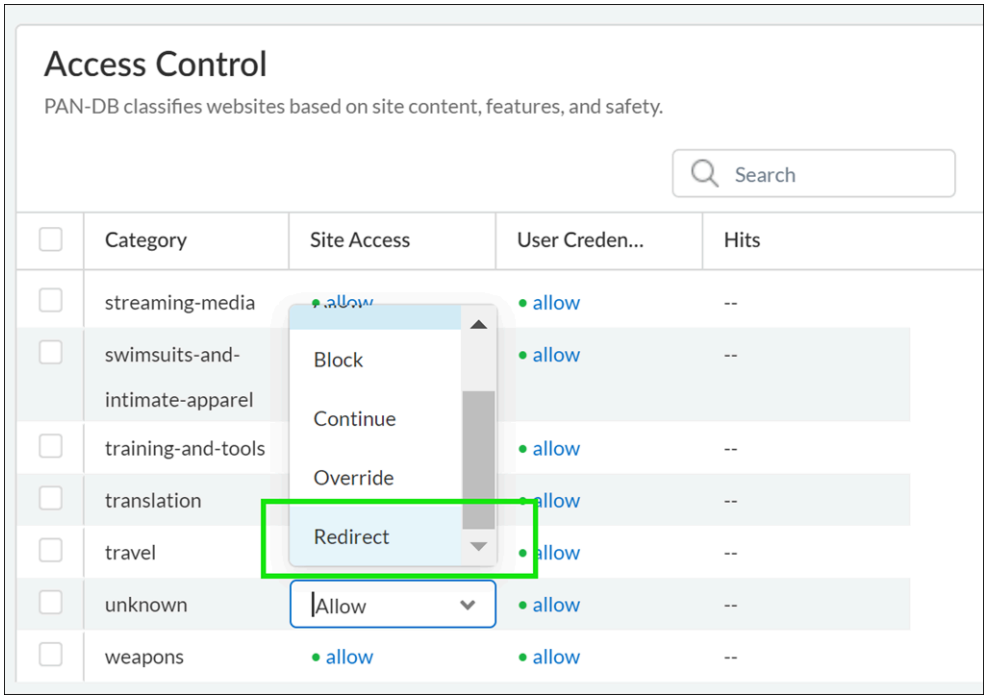


STEP 4 | 现在，指定将用户重定向到 RBI 环境的 URL 类别。

转到 **URL Access Management**（**URL** 访问管理）**> Access Control**（访问控制），并添加或编辑 **URL Access Management Profile**（**URL** 访问管理配置文件）。

在 **Access Control**（访问控制）设置中，将 **Site Access**（站点访问）更新为 **Redirect**（重定向）。

新的 **Redirect**（重定向）操作将用户重定向到 RBI 环境，而不是向他们显示阻止页面。



监控

哪里可以使用？	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)	❑ 高级 URL 过滤许可证（或旧版 URL 过滤许可证） 注意： • 旧版 *URL* 过滤许可证已停用，但仍支持有效的旧版许可证。 • Prisma Access 许可证包括 *Advanced URL Filtering* 功能。

监控网络上的 Web 活动对于保护组织和确保 URL 过滤策略的有效性至关重要。Palo Alto Networks 平台会生成详细的日志，这些日志用作指示板和报告的来源。您可以自定义日志、指示板和报告，以满足您的特定监控和报告需求。如有必要，您可以从 URL 过滤日志请求 URL 类别更改。使用我们的监控工具提供的见解来微调 Web 访问策略规则，分析任何可疑活动并采取相应措施。

HTTP 标头日志记录和仅记录容器页面功能提供对日志详细信息和数量的控制。HTTP 标头日志记录增加了日志的粒度。仅记录用户访问的主页可以减少生成的日志数量。

浏览以下主题以了解有关 Web 活动监控工具和功能的更多信息。

- 监视 Web 活动
- 仅记录用户访问页面
- HTTP 标头日志记录
- 请求更改 URL 类别

监视 Web 活动

哪里可以使用？	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)	❑ 高级 URL 过滤许可证（或旧版 URL 过滤许可证） 注意： • 旧版 *URL* 过滤许可证已停用，但仍支持有效的旧版许可证。 • Prisma Access 许可证包括 *Advanced URL Filtering* 功能。

您可以查看各种指示板、报告和日志，以查看和分析网络上的网络活动。例如，在 PAN-OS 新一代防火墙上，应用程序命令中心 (ACC)、URL 过滤日志和报告会显示设置为 **Alert**（警报）、**Block**（阻止）、**Continue**（继续）或 **override**（覆盖）的 URL 类别的所有用户 Web 活动。通过使用以下工具监控用户活动，您可以更好地了解用户群的网络活动并确定适当的网络访问策略规则。

平台	查看用户 **Web** 活动的方法
PAN-OS 和 Panorama	• 应用程序命令中心 (ACC) • 网络活动小部件 • URL 过滤日志 • URL 过滤报告
Prisma Access	• 日志 • 见解 • 自主 DEM • 活动

- Strata Cloud Manager
- PAN-OS 和 Panorama

监控 Web 活动 (Strata Cloud Manager)

无论您使用何种界面管理 Prisma Access（Panorama 或 Strata Cloud Manager），Strata Cloud Manager 的“活动”窗格都会提供网络中所发生情况的全面视图。“活动”窗格中包含各种指示板，该窗格位于 Strata Cloud Manager 和 Device Insights 应用程序中。您还可以与组织中的其他用户共享活动数据。

以下交互式指示板可帮助您监控和分析网络上的 Web 活动：

- 威胁见解 — 高级 URL 过滤和其他 Palo Alto Networks 安全服务在您的网络中检测到并阻止的所有威胁的整体视图。您可以查看威胁趋势、受影响的应用程序、用户以及允许或阻止威胁的安全策略规则。
- 日志查看器 — 日志提供系统、配置和网络事件的审计跟踪。从活动指示板跳转到日志，以获取详细信息并调查结果。
- 应用程序使用情况 — 查看网络上的应用程序概述，包括其风险、批准状态、消耗的带宽以及这些应用程序的顶级用户。
- 执行摘要（**URL** 过滤）— 查看在您的网络中执行最多 Web 活动的 URL 类别、前 10 个恶意 URL 和前 10 个高风险 URL。
- 用户活动 — 查看单个用户的浏览模式：他们最常访问的网站、他们与之传输数据的网站，以及访问高风险网站的尝试。URL 过滤日志和 Cloud Identity 引擎提供的数据可实现此可见性。

  - 为了轻松安全地访问用户活动数据并共享报告，我们建议激活并配置 Cloud Identity 引擎.

其他可见性和监控方法：

- “报告”窗格包含用于计划报表传递或随时下载和共享报告以供离线查看的选项。
- 您还可以搜索安全构件（IP 地址、域名、URL 或文件哈希），以便与仅针对该构件的数据进行交互，这些数据来自您的网络和全球威胁情报调查结果。

打开“活动”指示板。

- 选择 **Activity**（活动） > 威胁见解 | 应用程序使用情况 | 用户活动 | 执行摘要。

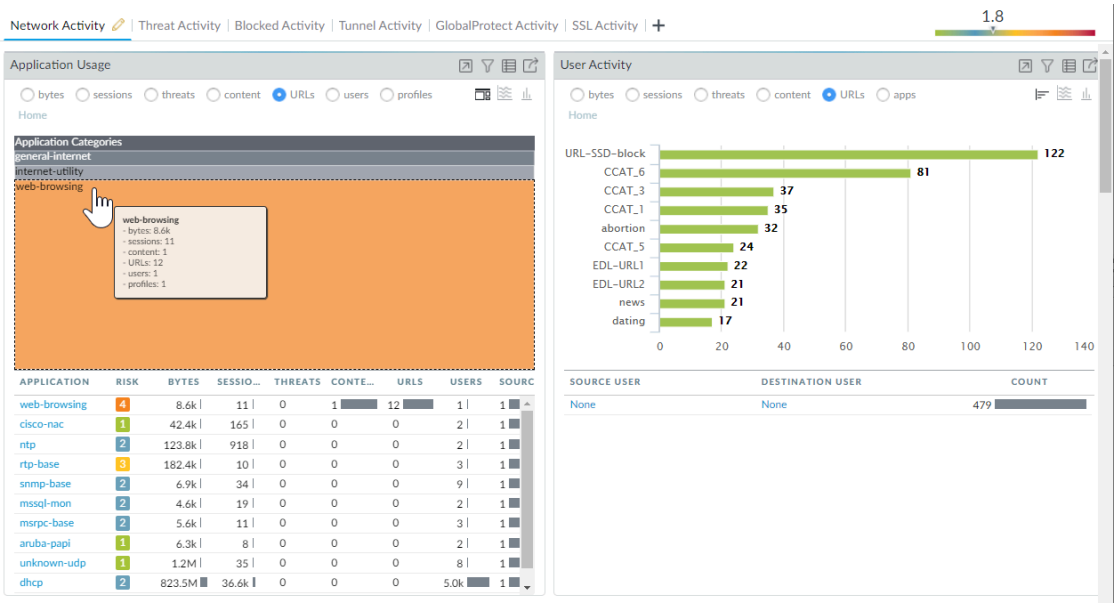
  要查看 URL 过滤的执行摘要，您需要在登陆指示板时单击 URL 过滤选项卡。
- 要访问日志查看器，请选择 **Activity**（活动） > **Logs**（日志） > **Log Viewer**（日志查看器）。

下载、共享和安排活动报告。

监视 Web 活动（PAN-OS 和 Panorama）

要快速查看环境中最常见的类别用户访问，请选中 **ACC** 小部件。**Network Activity**（网络活动）选项卡中大部分小部件允许您对 URL 进行排序。例如，在“应用程序使用”小部件中，您

可以看到网络类别是最常访问的类别，随后是加密隧道和 SSL。您还可以查看按照 URL 排序的 **Threat Activity**（威胁活动）和 **Blocked Activity**（阻止的活动）列表。



查看日志并配置日志选项：

可以从 ACC 直接跳转到日志 () 或选择 **Monitor**（监控） > **Logs**（日志） > **URL Filtering**（URL 过滤）。

每个条目的日志操作取决于您为相应类别定义的站点访问设置：

- **Alert log**（警报日志）— 在此示例中，computer-and-internet-info 类别设置为警报。

RECEIVE TIME	CATEGORY	URL	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	DESTINATION	APPLICATION	ACTION
2020/04/16 14:10:53	computer-and-internet-info	outlook.office36...	pm wifi	UNTRUST	[redacted]	[redacted]	[redacted]	outlook-web-online	alert

- **Block log**（阻止日志）— 在此示例中，insufficient-content 类别设置为继续。相反，如果该类别被设置为阻止，则日志操作将是 block-url。

RECEIVE TIME	CATEGORY	URL	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	DESTINATION	APPLICATION	ACTION
2020/04/08 18:47:49	insufficient-content	munchkin.mark...	pm wifi	UNTRUST	[redacted]	[redacted]	[redacted]	ssl	block-continue

- **Alert log on encrypted website**（加密网站上的警报日志）— 在此示例中，类别是 private-ip-addresses，应用程序是 web-browsing。该日志还显示防火墙已解密此流量。

RECEIVE TIME	CATEGORY	URL	DECRYPTED	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	DESTINATION	APPLICATION	ACTION
2020/04/09 14:11:29	private-ip-addresses	[redacted]/Updates/Updat...	yes	TRUST	UNTRUST	192.168.58.3	[redacted]	[redacted]	web-browsing	alert

[本地] 内联 ML 判定 (PAN-OS 10.0/10.1) 以及 [本地和云] 内联分类判定（PAN-OS 10.2 及更高版本）指示基于内联 ML 的分析器确定的判定。

- 内联 ML 判定适用于在 PAN-OS 10.0/10.1 上使用本地操作的 URL 过滤内联 ML 进行分类的 URL。

RECEIVE TIME	CATEGORY	URL CATEGORY LIST	INLINE ML VERDICT	ACTION	URL
10/11 17:32:10	malware	malware	phishing	block	hisperfectlight.com/downloads/etipa/login.php?cmd=login_submit&id=2cf35df3...
10/11 14:15:14	malware	malware	phishing	block	hisperfectlight.com/downloads/etipa/login.php?cmd=login_submit&id=2cf35df3...
04/30 15:19:30	medium-risk	medium-risk,unknown	malicious-javascript	block	130.127.24.16/0x39814f84/448d21c8e396e8f4e0eb75de69d6473e033422b...

现提供以下判定：

- 网络钓鱼 — 本地内联 ML 检测到的网络钓鱼攻击内容。
- 恶意 **javascript** — 本地内联 ML 检测到的恶意 javascript 内容。
- 未知 — URL 被分类，内容被确定为良性。

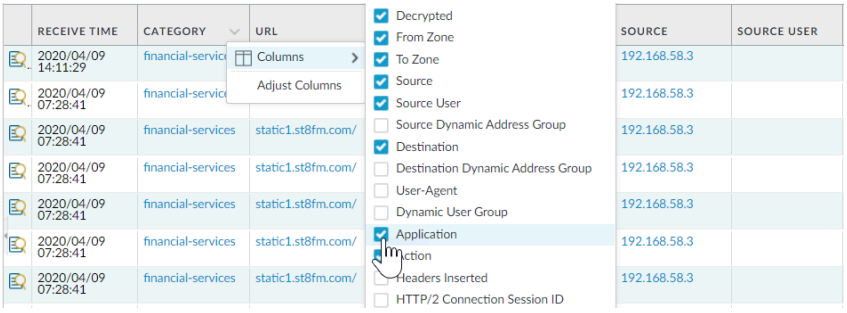
- 内联分类判定适用于使用本地操作的 URL 过滤内联 ML（在 PAN-OS 10.2 中重命名为本地内联分类）和云内联分类（在高级 URL 过滤云中操作）进行分类的 URL。特定的攻击类型在日志的类别列下指定。

RECEIVE TIME	CATEGORY	URL CATEGORY LIST	INLINE CATEGORIZATI... VERDICT	ACTION	URL
08/16 15:16:58	computer-and-internet-info	computer-and-internet-info,high-risk	N/A	alert	mlav.testpanw.com/js.html
08/16 15:16:58	phishing	computer-and-internet-info,high-risk	local	block	mlav.testpanw.com/phishing.html
08/16 15:14:58	phishing	phishing,real-time-detection	cloud	block-url	urlfiltering.paloaltonetworks.com/test-inline-content-analysis-phishing
08/16 15:14:58	phishing	phishing,real-time-detection	cloud	block-url	urlfiltering.paloaltonetworks.com:80/test-inline-content-analysis-phishing

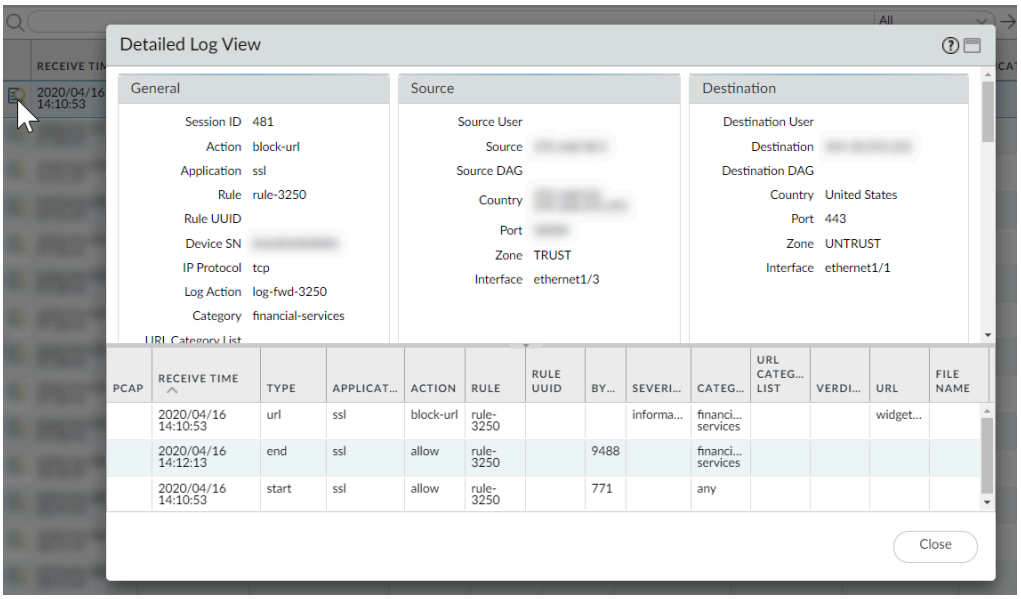
现提供以下判定：

- 本地 — 使用本地内联分类检测到的恶意内容。
- 云端 — 使用位于高级 URL 过滤云端的云端内联分类引擎检测到恶意内容。
- 不适用 — URL 未被本地或云内联分类引擎分析。

也可以将多个其他列添加到 URL 过滤日志视图，如到区域和从区域、内容类型、以及是否执行数据包捕获。要修改显示的列，单击任何一列中的向下箭头，然后选择要显示的属性。

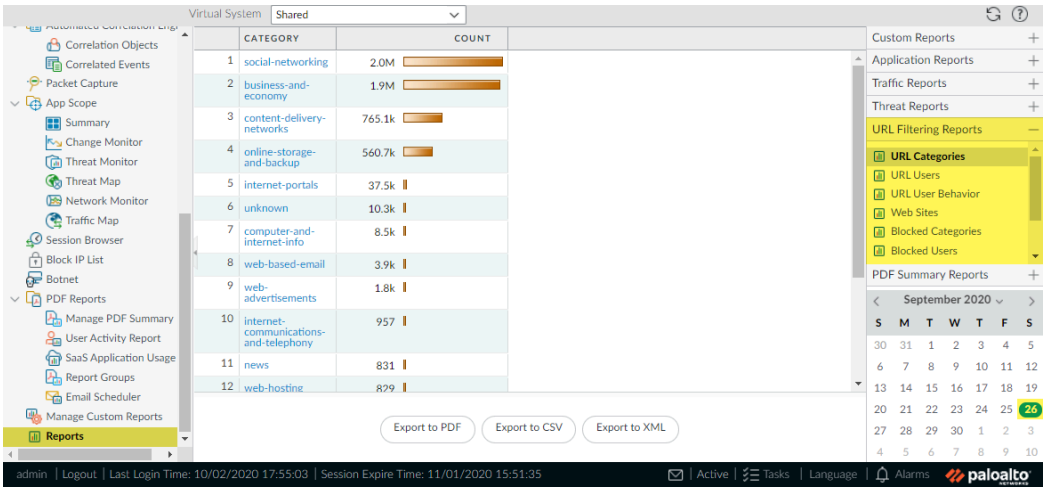


要查看完整的日志详细信息和/或请求访问的指定 URL 的类别更改，单击日志的第一列中的日志详细信息图标。



生成关于 URL 类别、URL 用户、访问的网站、已阻止类别等的预定义 URL 过滤报告。

选择 **Monitor**（监控） > **Reports**（报告）并在 **URL Filtering Reports**（**URL** 过滤报告）部分下，选择其中一个报告。报告涵盖您在日历上选择的日期的 24 小时时段。也可以将报告导出为 PDF、CSV 或 XML 格式。



查看用户活动报告

哪里可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	☐ 高级 URL 过滤许可证（或旧版 URL 过滤许可证） 注意：

哪里可以使用？	需要提供什么？
• NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	• 旧版 *URL* 过滤许可证已停用，但仍支持有效的旧版许可证。 • Prisma Access 许可证包括 *Advanced URL Filtering* 功能。

此报告提供了查看用户或组活动的快速方法，并且也提供了用于查看浏览时间活动的选项。

- Strata Cloud Manager
- PAN-OS 和 Panorama

查看用户活动报告 (Strata Cloud Manager)

无论您是使用 Panorama 还是 Strata Cloud Manager 来管理 Prisma Access，都可以转到 Strata Cloud Manager 应用来生成用户活动报告。在应用中，转到 **Activity**（活动）以找到 **User Activity Report**（用户活动报告）指示板。访问用户活动数据需要有效的云身份引擎租户。

STEP 1 | 激活云身份引擎。

STEP 2 | 设置云身份引擎。

STEP 3 | 配置用户活动报告。

1. 选择 **Activity**（活动） > **User Activity**（用户活动）。
2. **Enter Username**（输入用户名），从而为用户生成报告。
3. 选择报告 **Type**（类型）：
   - 选择 **User**（用户）为其中一名用户生成报告。
   - 为一组用户选择 **Group**（组）。

   您必须启用 User-ID，才能选择用户名或组名。如果没有配置 *User-ID*，可选择类型 ***User***（用户），然后输入用户计算机的 *IP* 地址。
4. 输入用户报告的 **Username/IP Address**（用户名/IP 地址），或输入用户组报告的组名。
5. 选择时段。可以选择现有时段，或选择 **Custom**（自定义）。
6. 选中 **Include Detailed Browsing**（包括详细浏览）复选框，这样可在报告中包括浏览信息。

STEP 4 | 运行报告。

1. 单击 **Run Now**（立即运行）。
2. 防火墙完成生成报告时，单击其中一个链接下载报告：
   - 单击 **Download User Activity Report**（下载用户活动报告）可下载 PDF 版本的分析报告。
   - 单击 **Download URL Logs**（下载 **URL** 日志）可下载相应日志条目的 CSV 文件。
3. 下载报告后，单击 **Cancel**（取消）。
4. 如果要保存用户活动报告设置，以便稍后再次运行相同的报告，请单击 **OK**（确定）；否则请单击 **Cancel**（取消）。

STEP 5 | 通过打开下载的文件查看用户活动报告。PDF 版本的报告显示您基于报告的用户或组、报告时间框架和目录：

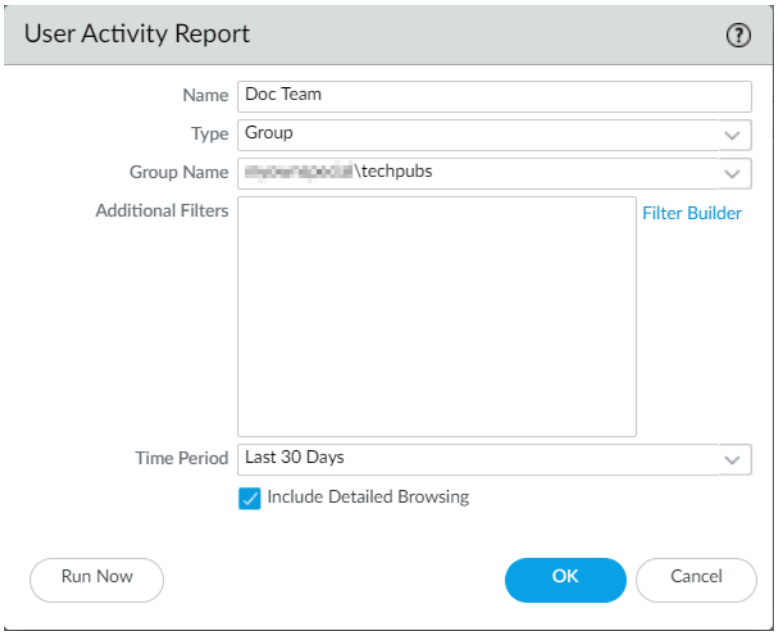
STEP 6 | 单击目录中的项目以查看报告详细信息。例如，单击 **Traffic Summary by URL Category**（按 **URL** 类别的流量摘要）可查看选定用户或组的统计信息。

查看用户活动报告（PAN-OS 和 Panorama）

STEP 1 | 配置用户活动报告。

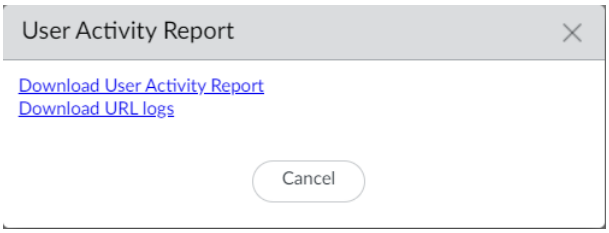
1. 选择 **Monitor**（监控） > **PDF Reports**（PDF 报告） > **User Activity Report**（用户活动报告）。
2. **Add**（添加）报告，然后输入报告的 **Name**（名称）。
3. 选择报告 **Type**（类型）：
   - 选择 **User**（用户）为其中一名用户生成报告。
   - 为一组用户选择 **Group**（组）。

   您必须启用 User-ID 才能选择用户名或组名。如果没有配置 *User-ID*，可选择类型 ***User***（用户），然后输入用户计算机的 *IP* 地址。
4. 输入用户报告的 **Username/IP Address**（用户名/IP 地址），或输入用户组报告的组名。
5. 选择时段。可以选择现有时段，或选择 **Custom**（自定义）。
6. 选中 **Include Detailed Browsing**（包括详细浏览）复选框，这样可在报告中包括浏览信息。



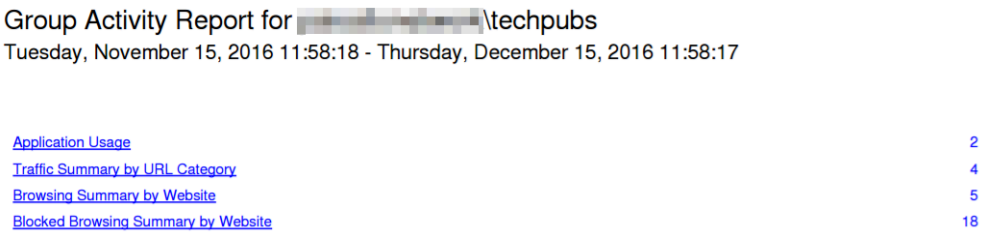
STEP 2 | 运行报告。

1. 单击 **Run Now**（立即运行）。
2. 防火墙完成生成报告时，单击其中一个链接下载报告：
   - 单击 **Download User Activity Report**（下载用户活动报告）可下载 PDF 版本的分析报告。
   - 单击 **Download URL Logs**（下载 **URL** 日志）可下载相应日志条目的 CSV 文件。

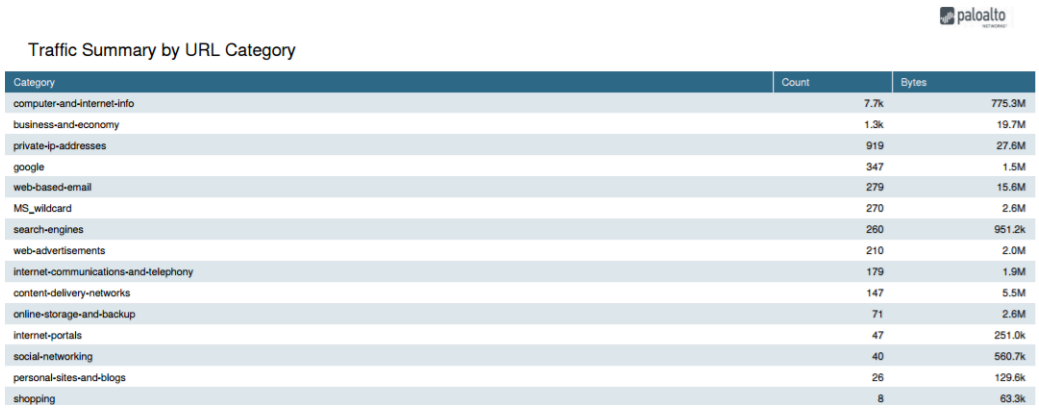


3. 下载报告后，单击 **Cancel**（取消）。
4. 如果要保存用户活动报告设置，以便稍后再次运行相同的报告，请单击 **OK**（确定）；否则单击 **Cancel**（取消）。

STEP 3 | 通过打开下载的文件查看用户活动报告。PDF 版本的报告显示您基于报告的用户或组、报告时间框架和目录：



STEP 4 | 单击目录中的项目以查看报告详细信息。例如，单击 **Traffic Summary by URL Category**（按 **URL** 类别的流量摘要）可查看选定用户或组的统计信息。



Category	Count	Bytes
computer-and-internet-info	7.7k	775.3M
business-and-economy	1.3k	19.7M
private-ip-addresses	919	27.6M
google	347	1.5M
web-based-email	279	15.6M
MS_wildcard	270	2.6M
search-engines	260	951.2k
web-advertisements	210	2.0M
internet-communications-and-telephony	179	1.9M
content-delivery-networks	147	5.5M
online-storage-and-backup	71	2.6M
internet-portals	47	251.0k
social-networking	40	560.7k
personal-sites-and-blogs	26	129.6k
shopping	8	63.3k

计划和共享 URL 过滤报告

哪里可以使用？	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)	❑ 高级 URL 过滤许可证（或旧版 URL 过滤许可证） 注意： • 旧版 *URL* 过滤许可证已停用，但仍支持有效的旧版许可证。 • Prisma Access 许可证包括 *Advanced URL Filtering* 功能。

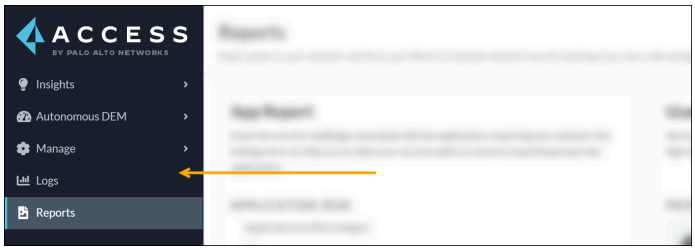
您可以安排、生成和共享与 URL 过滤和 Web 活动相关的各种报告。

- Strata Cloud Manager
- PAN-OS 和 Panorama

计划和共享 URL 过滤报告 (Strata Cloud Manager)

无论您使用 Panorama 还是 Strata Cloud Manager 来管理 Prisma Access，您都可以为 URL 过滤报告使用 Strata Cloud Manager。在 Strata Cloud Manager 中，转至“活动”以了解交互式 URL 过滤数据和报告。您可以在组织内共享活动报告，并安排定期更新。以下是 Prisma Access 利用 URL 过滤且与其最相关的指示板和工具：

- 执行摘要 — 查看在您的网络中占有最多网络活动的 URL 类别、排名前 10 的恶意 URL，以及排名前 10 的高风险 URL。
- 用户活动 — 查看个人用户的浏览模式：他们最常访问的网站，正在传输数据的网站，以及尝试访问的高风险网站。URL 过滤日志和 Cloud Identity 引擎提供的数据可实现此可见性。
- 搜索安全工件（IP 地址、域名、URL 或文件哈希），以便与仅针对该工件的数据进行交互，这些数据来自您的网络和全球威胁情报调查结果。



为了轻松安全地访问用户活动数据并共享报告，我们建议激活并配置 Cloud Identity 引擎.

STEP 1 | 下载、共享和安排活动报告。

STEP 2 | 访问 URL 过滤执行摘要。

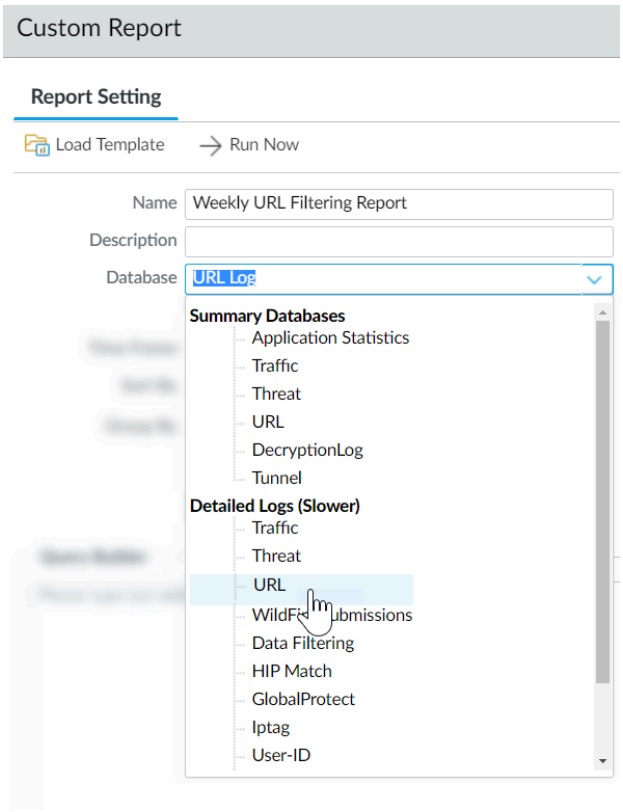
选择 **Activity**（活动） > **Executive Summary**（执行摘要），然后单击“URL 过滤”选项卡。

STEP 3 | 搜索安全工件。

计划和共享 URL 过滤报告（PAN-OS 和 Panorama）

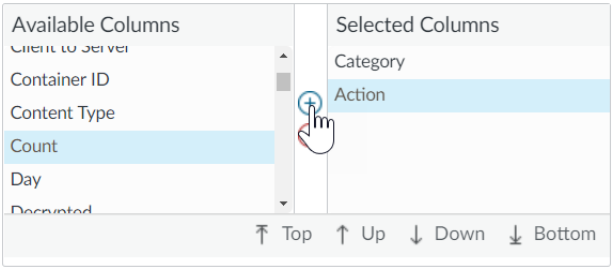
STEP 1 | 添加新的自定义报告。

1. 选择 **Monitor**（监控） > **Manage Custom Reports**（管理自定义报告），然后 **Add**（添加）报告。
2. 给予报告一个唯一的 **Name**（名称）和 **Description**（说明）（可选）。
3. 选择用于生成报告的 **Database**（数据库）。要生成详细的 URL 过滤报告，请从“详细日志”部分中选择 **URL**：

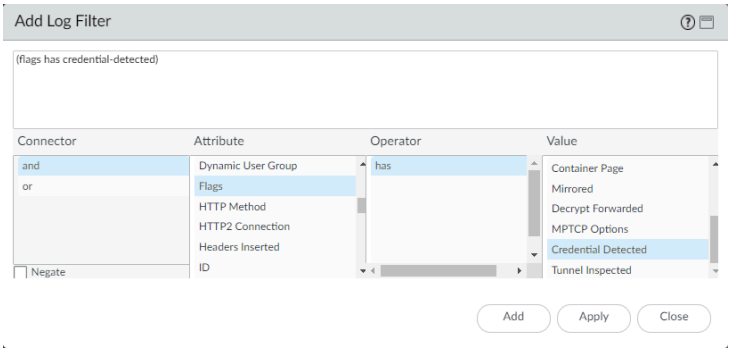


STEP 2 | 配置报告选项。

1. 选择预先定义的 **Time Frame**（时间框架）或选择 **Custom**（自定义）。
2. 从“可用列”列表中选择要包含在报告中的日志列，将其 (+) 添加到“选定列”中。例如，对于 URL 过滤报告，您可以选择：
   - 操作
   - 应用程序类别
   - 类别
   - 目标国家/地区
   - 源用户
   - 网址

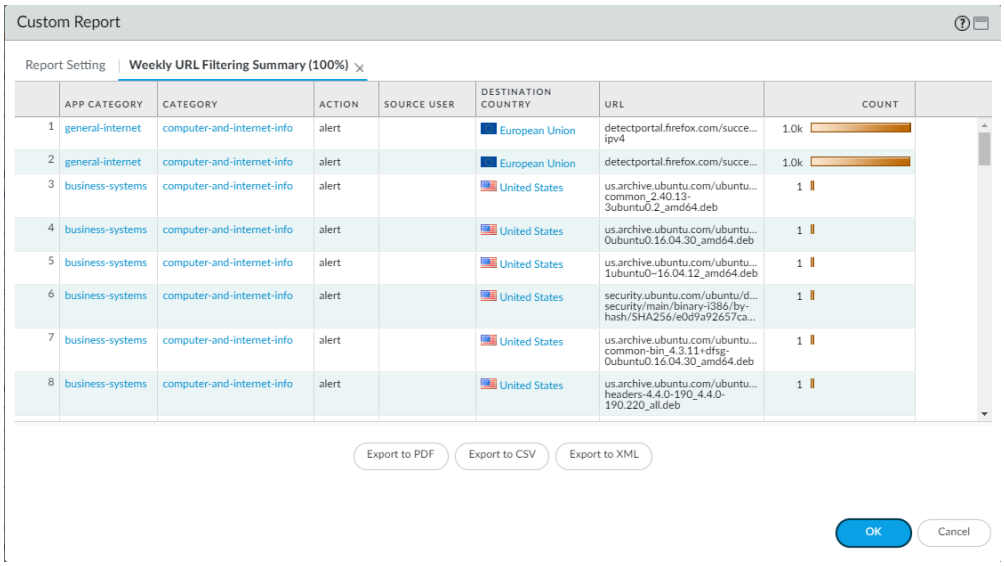


3. 如果防火墙启用阻止凭据网络钓鱼，请选择属性 **Flags**（标志），操作员 **has**（拥有）和值 **Credential Detected**（检测到的凭据），还应包括用户向站点提交有效公司凭据时在报告中记录的事件。



4. （可选）选择 **Sort By**（排序方式）选项，以设置用于汇总报告详细信息的属性。如果您未选择排序属性，报告则会返回前面 N 个结果，不进行任何聚合。选择 **Group By**（分组方式）属性，以用作分组数据的锚点。以下示例显示了将 **Group By**（分组方式）设

置成 **App Category**（应用程序类别），将 **Sort By**（排序方式）设置成 **Top 5**（前 5 组）**Count**（计数）的一份报告。



STEP 3 | 运行报告。

1. 单击 **Run Now**（立即运行）图标可立即生成报告，该报告将在新选项卡中打开。
2. 完成报告审查后，返回 **Report Setting**（报告设置）选项卡，然后调整设置并再次运行报告，或继续下一步来安排报告。
3. 选择 **Schedule**（时间表）复选框以每天运行一次报告。这将生成每日报告，其中详细记录了过去 24 小时的 Web 活动。

STEP 4 | **Commit**（提交）配置。

STEP 5 | 查看自定义报告。

1. 选择 监视器 > 报告.
2. 展开右列的 **Custom Reports**（自定义报告）窗格，然后选择要查看的报告。最新报告会自动显示。
3. 要查看以前日期的报告，请从日历中选择日期。也可以将报告导出为 PDF、CSV 或 XML 格式。

仅记录用户访问页面

哪里可以使用？	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)	❑ 高级 URL 过滤许可证（或旧版 URL 过滤许可证） 注意： • 旧版 *URL* 过滤许可证已停用，但仍支持有效的旧版许可证。 • Prisma Access 许可证包括 *Advanced URL Filtering* 功能。

容器页面是用户在访问网站时访问的主页，但在此主页内可以加载其他页面。如果已在 URL 过滤配置文件（Prisma Access 的 URL 访问管理配置文件）中启用 **Log Container page only**（仅记录容器页面）选项，则只记录主容器页面，而不会记录容器页面中可能加载的后续页面。因为 URL 过滤可能会生成大量的日志条目，且您可能想要启用此选项，因此日志条目将只包含请求页面文件名与特定 MIME 类型匹配时的 URI。默认设置包括以下 MIME 类型：

- application/pdf
- application/soap+xml
- application/xhtml+xml
- text/html
- text/plain
- text/xml

如果已启用 ***Log container page only***（仅记录容器页面）选项，则抗病毒或漏洞防护可能并不能总是检测到与威胁的相关 *URL* 日志条目。

- Strata Cloud Manager
- PAN-OS 和 Panorama

仅记录用户访问的页面 (Strata Cloud Manager)

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

切换到 ***PAN-OS & Panorama***（***PAN-OS*** 和 ***Panorama***）选项卡，然后按照其中的指导操作。

如果您正在使用 ***Strata Cloud Manager***，请在此处继续。

STEP 1 | 在 URL 访问管理配置文件中，选择 **Log Container Page Only**（仅记录容器页面）。

STEP 2 | 将 URL 访问管理配置文件应用到安全策略规则。

仅当包含在安全策略规则引用的配置文件组中时，URL 访问管理配置文件才处于活动状态。

按照步骤激活 URL 访问管理配置文件（和任何安全配置文件）。确保 **Push Config**（推送配置）。

仅记录用户访问的页面（PAN-OS 和 Panorama）

STEP 1 | 创建或选择要修改的 URL 过滤配置文件。

选择 **Objects**（对象） > **Security Profiles**（安全配置文件） > **URL Filtering**（URL 过滤）。

STEP 2 | 启用 **Log container page only**（仅记录容器页面）。

STEP 3 | 单击 **OK**（确定）保存配置文件。

STEP 4 | **Commit**（提交）更改。

HTTP 标头日志记录

哪里可以使用？	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)	❑ 高级 URL 过滤许可证（或旧版 URL 过滤许可证） 注意： • 旧版 *URL* 过滤许可证已停用，但仍支持有效的旧版许可证。 • Prisma Access 许可证包括 *Advanced URL Filtering* 功能。

URL 过滤提供监视和控制网络上的 Web 通信的功能。为了改善 Web 内容的可见性，您可以将 URL 过滤配置文件配置为记录 Web 请求中所含的 HTTP 标头属性。当客户端请求 Web 页面时，HTTP 标头会包含用户代理、推荐人和 x-forwarded-for 字段作为属性值对并将其转发给 Web 服务器。启用 HTTP 标头日志记录后，防火墙会在 URL 过滤日志中记录以下属性值对。

此外，您还可以使用 *HTTP* 标头管理对 *SaaS* 应用程序的访问。要执行此操作，无需获取 *URL* 过滤许可证，但必须使用 *URL* 过滤配置文件打开此功能。

属性	说明
User-Agent（用户代理）	用户用于访问 URL 的 Web 浏览器，如互联网Explorer。此信息在 HTTP 请求中发送到服务器。 HTTP 标头不包含用户代理的完整字符串。在包含标头端的数据包之前的数据包记录的最大字节数为 36 个字节。
Referer（推荐人）	用户链接到其他网页的网页的 URL；它是用户重定向（引用）到所请求的网页的源。
X-Forwarded-For (XFF)	用于保留请求此网页的用户 IP 地址的 HTTP 请求标头字段中的选项。如果您的网络上有代理服务器，XFF 能让您识别请求此内容的用户的 IP 地址，而不是仅将代理服务器的 IP 地址记录为请求此网页的源 IP 地址。
已插入标头	防火墙插入的标头类型和标头文本。

请求更改 URL 的类别

哪里可以使用？	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)	❑ 高级 URL 过滤许可证（或旧版 URL 过滤许可证） 注意： • 旧版 *URL* 过滤许可证已停用，但仍支持有效的旧版许可证。 • Prisma Access 许可证包括 *Advanced URL Filtering* 功能。

如果您认为某个域或 URL 的分类不正确，您可以通过防火墙或我们的 URL 类别查找工具测试 A 站点提交重新分类请求。您还可以通过测试 A 站点提交批量重新分类请求。这两种方法都要求您为要查看的网址建议至少一个新类别。

您无法请求更改 *URL* 接收到的风险类别，也无法请求将 *URL* 分类为 *`insufficient content`* 或 *`new-registered domains`*。

在防火墙上，您可以从 URL 过滤日志条目的详细日志视图中请求更改 URL 类别。在测试 A 站点上，您必须输入要重新分类的网站才能查看其 PAN-DB 分类。搜索结果后跟请求表单链接。同样，在 Strata Cloud Manager 中，测试 A 站点表单的链接会显示在编辑 URL 访问管理配置文件时可用的内部测试 A 站点工具的查询结果。要访问批量更改请求表单，您需要登录到测试 A 站点。登录后，网页会显示批量请求表单的链接。

在提交更改请求后，自动爬虫会立即分析 URL。如果爬虫验证您的类别建议，Palo Alto Networks会批准您的请求，并立即用新类别更新 PAN-DB。如果没有，Palo Alto Networks 威胁研究和数据科学团队的人工编辑会审核您的请求。他们可以决定保留原来的类别，同意你建议的类别，或者更改类别（如果他们不同意原来的和建议的类别）。

提交更改请求后，您将收到一封确认电子邮件。调查完成后，您将收到第二封附有调查结果的电子邮件。

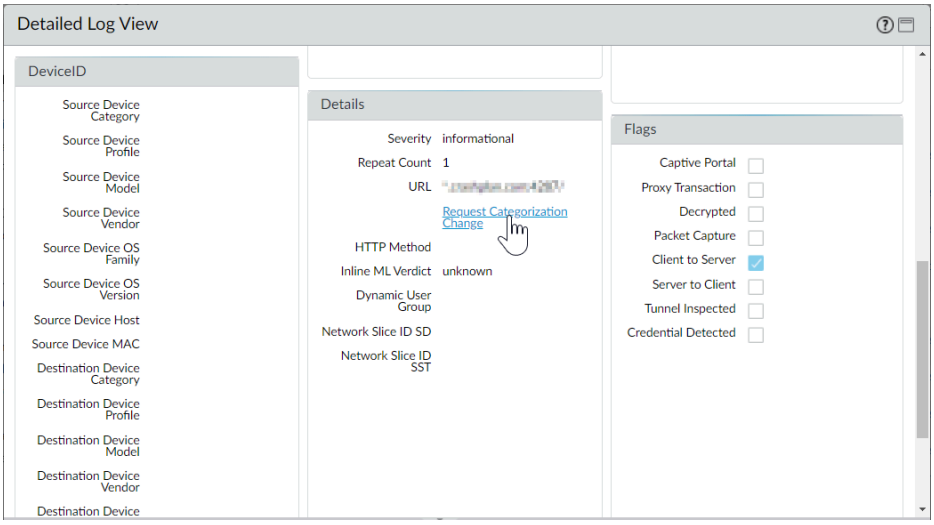
- PAN-OS 和 Panorama
- 测试 A 站点

请求更改 URL 类别（PAN-OS 和 Panorama）

STEP 1 | 访问 URL 过滤日志，导航路径为 **Monitor**（监控） > **Logs**（日志） > **URL Filtering**（**URL** 过滤）。

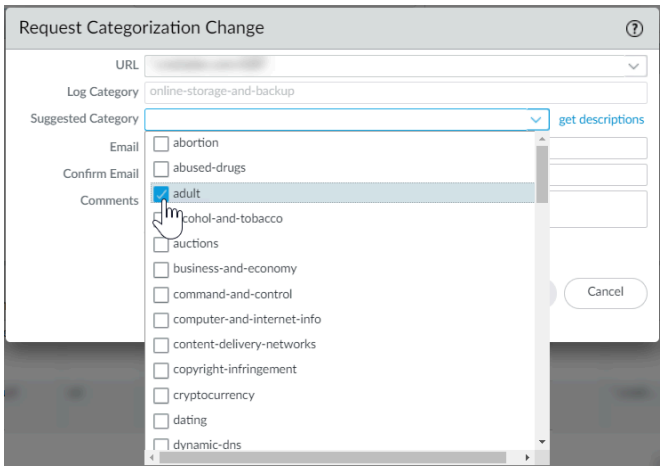
STEP 2 | 打开详细日志视图，查看包含要更改的 URL 分类的 URL 过滤日志条目。

1. 单击日志条目对应的望远镜图标 ( )。此时将显示详细日志视图。



STEP 3 | 在详细信息下，单击 **Request Categorization Change**（请求更改分类）。

STEP 4 | 填写并提交申请表。



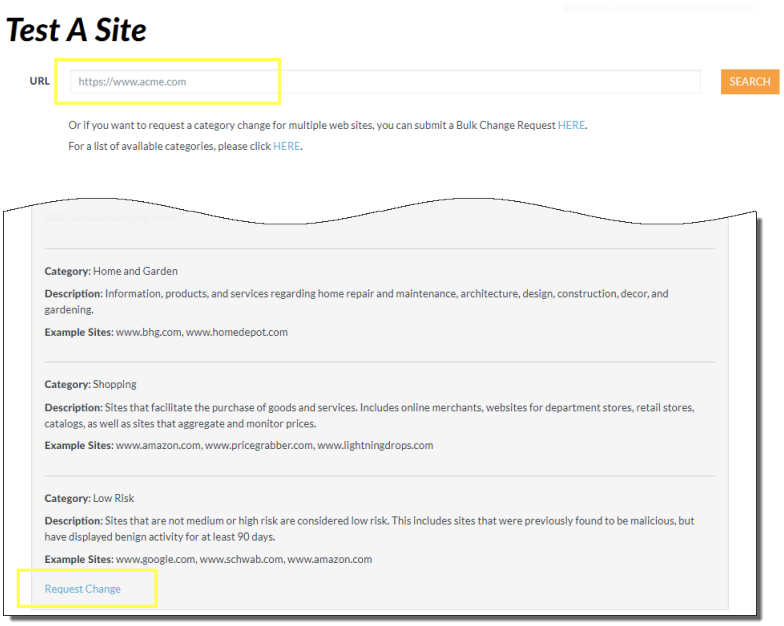
请求更改 URL 的类别（测试 A 站点）

STEP 1 | 前往 Test A Site（测试站点）。

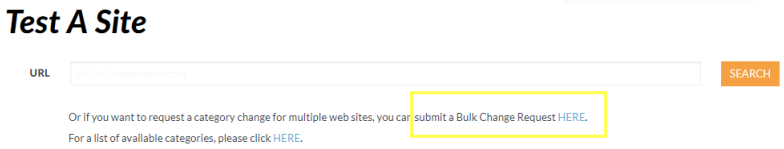
Log in（登录）以避免完成 *CAPTCHA* 测试，并在更改申请表上输入您的电子邮件地址。请注意，登录后才能访问批量更改申请表。

STEP 2 | 选择要填写的更改申请表。

- 更改单个 **URL** 的请求 — 输入要重新分类的 **URL**，然后单击 **Search**（搜索）。在 URL 类别结果下面，单击 **Request Change**（请求更改）。

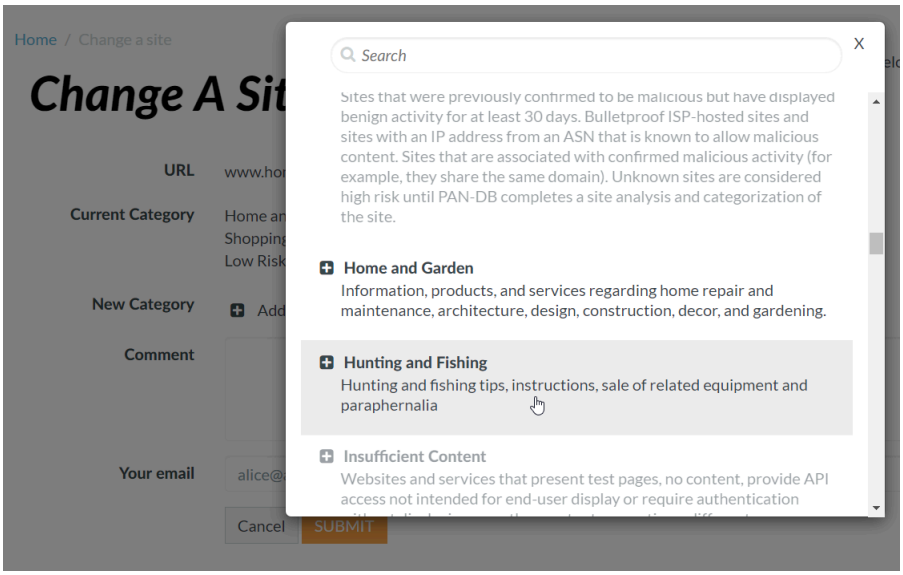


- 批量更改请求 — **Log-in**（登录）测试 A 站点。然后在此处单击提交批量更改请求。



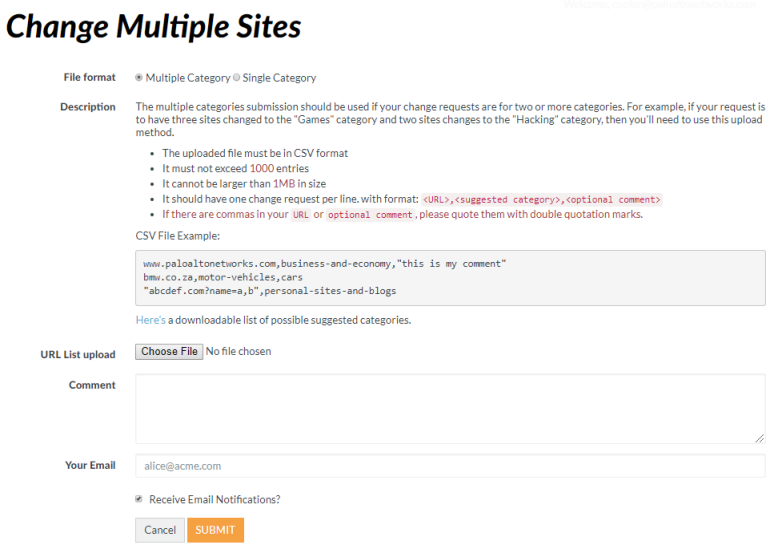
STEP 3 | 填写更改申请表。

- 更改单个 **URL** 的请求 — 建议最多为 URL 添加两个新类别。单击 **Select category (from a list)**（选择类别 [从列表中]），一次选择一个类别。（可选）提供关于请求的 **Comment**（备注）。例如，您可以解释为什么您的建议合适。



- 批量更改请求 — 选择 **File Format**（文件格式）。如果您的更改请求包括两个或多个类别，请选择多个类别。例如，如果您要将列表中一半的 URL 重新分类为 `business-and-economy`，将另一半分类为 `personal-sites-and-blogs`。

  然后，单击 **Choose File**（选择文件），然后选择要上载的 CSV 文件。此格式的文件每行应有一个更改请求：`<URL>`、`<first suggested category>`、`<second suggested category>`、`<(optional) comment>`。该文件不能包含超过 1000 个条目或大于 1MB。（可选）提供关于请求的 **Comment**（备注）。



STEP 4 | **Submit**（提交）表单。

故障排除

哪里可以使用？	需要提供什么？
• NGFW (Managed by PAN-OS or Panorama)	☐ 高级 URL 过滤许可证（或旧版 URL 过滤许可证） 注意：旧版 *URL* 过滤许可证已停用，但仍支持有效的旧版许可证。

本章介绍诊断和解决 Palo Alto Networks 新一代防火墙常见 URL 过滤问题的任务。在就这些问题联系 Palo Alto Networks 支持团队之前，请完成相关任务中的步骤。如果您仍然需要联系支持人员，请确保提供您在执行故障排除任务时了解到的所有信息。

故障排除和监控 *Web* 活动通常息息相关。经常利用监视和日志工具来识别和解决本章没有明确讨论的问题。熟悉监视一章介绍的监视工具和任务。

- 激活高级 URL 过滤功能时出现问题
- PAN-DB 云连接问题
- 将 URL 分类为未解析
- 分类不正确
- 解决网站访问问题
- 排除 URL 过滤响应页面显示问题

激活高级 URL 过滤功能时出现问题

哪里可以使用？	需要提供什么？
• NGFW (Managed by PAN-OS or Panorama)	❑ 高级 URL 过滤许可证（或旧版 URL 过滤许可证） 注意：旧版 *URL* 过滤许可证已停用，但仍支持有效的旧版许可证。

使用以下工作流程来解决高级 URL 过滤功能的激活问题。

STEP 1 | 访问 PAN-OS CLI。

STEP 2 | 通过运行以下命令验证高级 URL 过滤功能是否已激活：

```
show system setting url-database
```

如果响应是 `paloaltonetworks`，则 PAN-DB（即 Palo Alto Networks URL 过滤数据库）是当前的供应商。

STEP 3 | 验证防火墙是否具有有效的高级 URL 过滤许可证。

运行 **`request license info`** CLI 命令。

应该能够看到许可证条目 `Feature`：高级 URL 过滤。如果未安装许可证，将需要获取并安装许可证。请参阅配置 URL 过滤。

STEP 4 | 检查 PAN-DB 云连接状态。

PAN-DB 云连接问题

哪里可以使用？	需要提供什么？
• NGFW (Managed by PAN-OS or Panorama)	❑ 高级 URL 过滤许可证（或旧版 URL 过滤许可证） 注意：旧版 *URL* 过滤许可证已停用，但仍支持有效的旧版许可证。

为了确保与 *PAN-DB* 云的连接，请创建专用的安全策略规则，以允许所有 *Palo Alto* 管理服务流量。这可以避免管理流量被归类为 *not-resolved*，同时防止流量在通过数据平面进行路由时被阻止。

要检查防火墙与 PAN-DB 云之间的连接：

```
show url-cloud status
```

如果云可访问，则预期响应类似如下：

```
show url-cloud status PAN-DB URL Filtering License : valid Current
 cloud server : serverlist.urlcloud.paloaltonetworks.com Cloud
 connection : connected Cloud mode : public URL database version -
 device :20200624.20296 URL database version - cloud :20200624.20296
 ( last update time 2020/06/24 12:39:19 ) URL database status : good
 URL protocol version - device : pan/2.0.0 URL protocol version -
 cloud : pan/2.0.0 Protocol compatibility status : compatible
```

如果云不可访问，则预期响应类似如下：

```
show url-cloud status PAN-DB URL Filtering License : valid
 Cloud connection : not connected URL database version -
 device :0000.00.00.000 URL protocol version - device : pan/0.0.2
```

使用以下清单来识别和解决连接问题：

- ❑ PAN-DB URL 过滤许可证字段是否显示为无效？获取并安装有效的 PAN-DB 许可证。
- ❑ URL 协议版本是否显示为不兼容？将 PAN-OS 升级到最新版本。

- 您是否可以从防火墙 ping PAN-DB 云服务器？运行以下命令以检查：

  ```
  ping source <ip-address> host
   serverlist.urlcloud.paloaltonetworks.com <
  ```

  例如，如果管理接口 IP 地址为 10.1.1.5，请运行以下命令：

  ```
  ping source 10.1.1.5 host serverlist.urlcloud.paloaltonetworks.com
  ```

- 防火墙是否在 HA 配置中？验证防火墙的 HA 状态是处于主动、主动-主要或主动-辅助状态。如果防火墙处于不同的状态，将阻止对 PAN-DB 云的访问。在对中每个防火墙上运行以下命令以查看状态：

  ```
  show high-availability state
  ```

如果防火墙和 PAN-DB 云之间仍存在连接问题，请联系 Palo Alto Networks 获得支持。

将 URL 分类为未解析

哪里可以使用？	需要提供什么？
• NGFW (Managed by PAN-OS or Panorama)	❑ 高级 URL 过滤许可证（或旧版 URL 过滤许可证） 注意：旧版 *URL* 过滤许可证已停用，但仍支持有效的旧版许可证。

如果您的防火墙无法连接到 PAN-DB URL 过滤云服务来执行查找，或者 PAN-DB 响应 URL 查询的时间过长，则 URL 将被归类为 `not-resolved`。云连接状态和 URL 分类不适用于过期的订阅许可证或未经许可的用户。有关 URL 分类过程的详细说明，请参阅 URL 过滤的工作原理。

使用以下工作流程来进行故障排除：PAN-DB 所识别的部分或所有 URL 被分类为未解析的原因：

STEP 1 | 通过运行 **`show url-cloud status`** CLI 命令检查 PAN-DB 云连接。

`Cloud connection:` 字段会显示 `.connected`。如果您看到除 `connected` 之外的任何类别，则管理平面缓存中不存在的任何 URL 都将被归类为 未解析。要解决这一问题，请参阅 PAN-DB 云连接问题。

STEP 2 | 如果云连接状态显示 `connected`，请检查防火墙的当前利用率。

如果防火墙的利用率突然上升，URL 请求可能会被丢弃（可能无法到达管理面板），并被分类为 `not-resolved`。

要查看系统资源，请运行 **`show system resources`** CLI 命令。然后，查看 `%CPU` 和 `%MEM` 列。

您还可以在 Web 界面的 **Dashboard**（指示板）上的“系统资源”小部件上查看系统资源。

STEP 3 | 考虑增加**Category lookup timeout (sec) [**类别查找超时（秒）**]** 值。

增加类别查找超时值可提高 URL 类别得到解析的可能性，并减少日志中 `not-resolved` URL 的频率。

1. 选择 **Device**（设备） > **Setup**（设置） > **Content-ID**，并编辑 URL 过滤设置。
2. 单击 **OK**（确定）并 **Commit**（提交）更改。

   您还可以使用 **`set deviceconfig setting ctd url-wait-timeout`** CLI 命令更新该值。

STEP 4 | 如果问题仍然存在，请联系 Palo Alto Networks 技术支持部门。

分类不正确

哪里可以使用？	需要提供什么？
• NGFW (Managed by PAN-OS or Panorama)	❑ 高级 URL 过滤许可证（或旧版 URL 过滤许可证） 注意：旧版 *URL* 过滤许可证已停用，但仍支持有效的旧版许可证。

有时可能会遇到您认为分类不正确的网址。使用以下工作流程来确定站点的 URL 分类，并在适当时请求类别更改。

STEP 1 | 通过运行以下命令验证数据面板中的类别：

```
show running url <URL>
```

例如，要查看 Palo Alto Networks 网站的类别，请运行以下命令：

```
show running url paloaltonetworks.com
```

如果对存储在数据面板缓存中的 URL 分类正确（在本例中为“计算机和互联网信息”），则分类正确且无需执行进一步操作。如果类别不正确，请继续执行下一步。

STEP 2 | 通过运行以下命令验证管理面板中的类别是否正确：

```
test url-info-host <URL>
```

例如：

```
test url-info-host paloaltonetworks.com
```

如果对存储在管理面板缓存中的 URL 分类正确，请通过运行以下命令从数据面板缓存中移除该 URL：

```
clear url-cache url <URL>
```

下一次防火墙请求此 URL 的类别时，请求将会转发到管理面板。这样应该可以解决问题，且无需执行进一步操作。如果这样都无法解决问题，请转到下一步检查云系统中的 URL 类别。

STEP 3 | 通过运行以下命令验证云中的类别：

```
test url-info-cloud <URL>
```


STEP 4 | 如果对存储在云中的 URL 分类正确，请从数据面板和管理面板缓存中移除该 URL。

运行以下命令以从数据面板缓存中删除 URL：

```
clear url-cache url <URL>
```

运行以下命令以从管理面板缓存中删除 URL：

```
delete url-database url <URL>
```

下一次防火墙请求给定 URL 的类别时，请求将会转发到管理面板，然后再转发到云。这样应该可以解决类别查询问题。如果问题仍然存在，请参阅下一步提交分类更改请求。

STEP 5 | 要从 Web 界面提交更改请求，请转到 URL 日志，然后选择想要更改的 URL 的日志条目。

STEP 6 | 单击 **Request Categorization**（请求分类）更改链接，然后按照以下说明进行操作。通过搜索 URL，然后单击 **Request Change**（请求更改）图标，也可以从 Palo Alto Networks 测试 A 站点网站请求更改类别。要查看每个类别的描述，请参阅预定义的 URL 类别。

如果更新请求获批，您将收到电子邮件通知。然后，您可以通过两种方式确保 URL 类别在防火墙上得到更新：

- 等到缓存中的 URL 过期，然后当有用户再访问该 URL 时，新分类更新就会进入缓存。
- 运行以下命令强制更新进入缓存：

```
request url-filtering update url <URL>
```


解决网站访问问题

哪里可以使用？	需要提供什么？
• NGFW (Managed by PAN-OS or Panorama)	❑ 高级 URL 过滤许可证（或旧版 URL 过滤许可证） 注意：旧版 *URL* 过滤许可证已停用，但仍支持有效的旧版许可证。

由于各种原因，最终用户可能在访问网站时遇到问题，包括缺少 URL 过滤许可证、策略规则配置错误、PAN-DB 连接问题或网站分类错误。按照以下步骤诊断并解决网站访问问题。

该问题可能与 *URL* 过滤无关。此任务中步骤后面的“下一步做什么”部分列出了需要重点关注的其他故障排除方面。

STEP 1 | 验证您是否拥有有效的高级 URL 过滤或旧版 URL 过滤许可证。

新一代防火墙需要有效的 *URL* 过滤许可证才能对网站和应用程序进行准确分类。如果您没有 *URL* 过滤许可证，则网站访问问题与 *URL* 过滤无关。

选择 **Device**（设备） > **Licenses**（许可证），并查找高级 URL 过滤（或 PAN-DB URL 过滤）许可证。有效许可证显示的到期日期晚于当前日期。

或者，使用 **`request license info`** CLI 命令。如果许可证有效，该界面将显示许可证信息，包括到期状态：`Expired?: no`。

STEP 2 | 在 CLI 上验证 PAN-DB 云连接状态。

`Cloud connection:` 字段会显示 `connected`。否则，任何管理平面 (MP) 缓存中不存在的 URL 都会归类为 `not-resolved`，并且可能会被安全策略规则中的 URL 过滤配置文件设置阻止。

STEP 3 | 清除特定 URL 的 MP 和数据平面 (DP) 缓存。

清除缓存可能会耗费大量资源。请考虑在维护期间清除缓存。

1. 要清除 MP 缓存，请使用 **`delete url-database url <affected url>`** CLI 命令。
2. 要清除 DP 缓存，请使用 **`clear url-cache url <affected url>`** CLI 命令。

STEP 4 | 查看 URL 过滤日志，验证该网站所属的 URL 类别是否已被阻止。

1. 选择 **Monitor**（监控） > **URL Filtering**（**URL** 过滤）。
2. 搜索受影响的 URL，然后选择最近的日志条目。
3. 查看类别和操作列。

   URL 的分类是否正确？通过测试 A 站点（Palo Alto Networks URL 类别查找工具）验证其类别。如果您仍认为分类不正确，请提交更改请求。

   如果操作列显示 `block-url`，请记下与日志条目关联的安全策略规则的名称。

STEP 5 | 检查安全策略规则，并根据需要进行更新。

1. 选择 **Policies**（策略） > **Security**（安全），然后选择您在上一步中记下名称的策略规则。
2. 验证安全策略规则是否允许访问请求的 URL 或其 URL 类别。

   查找以下两种配置之一：

   - **URL** 类别作为匹配条件：在 **Service/URL Category**（服务/**URL** 类别）下，指定的类别之一包含所请求的 URL。在 **Actions**（操作）下，将“操作设置”设置为 **Allow**（允许）。
   - **URL** 过滤配置文件：在 **Actions**（操作）下，“配置文件设置”设置为允许访问所请求的 URL 的 URL 过滤配置文件。

STEP 6 | 测试安全策略规则。

如果通过以上步骤未能发现或解决问题，则可能需要进行额外的故障排除以进一步区分问题。重点方面包括：

- 基本 IP 地址连接
- 路由配置
- DNS 解析
- 代理配置
- 数据包路径中的上游防火墙或检查设备

对于间歇性或复杂的问题，请联系 Palo Alto Networks 支持团队，以获得进一步帮助。

排除 URL 过滤响应页面显示问题

哪里可以使用？	需要提供什么？
• NGFW (Managed by PAN-OS or Panorama)	❑ 高级 URL 过滤许可证（或旧版 URL 过滤许可证） 注意：旧版 *URL* 过滤许可证已停用，但仍支持有效的旧版许可证。

URL 过滤响应页面可能由于各种原因而无法显示，包括：

- SSL/TLS 握手检查已启用。
- 该网站在检查 SSL/TLS 握手时被封锁。在这种情况下，URL 过滤响应页面不显示，因为防火墙会重置 HTTPS 连接。
- 该网站使用 HTTPS 协议或包含通过 HTTPS 提供的内容（例如广告），但网站或 URL 类别未解密。
- 自定义响应页面大于支持的最大大小。

使用以下步骤作为起点，对无法显示的 URL 过滤响应页面进行故障排除。如果问题仍然存在，请联系 Palo Alto Networks 技术支持部门。

STEP 1 | 确定问题的范围。

该问题是特定网站还是特定网页的子集？检查当您访问网站上的其他页面时是否显示回复页面。

STEP 2 | 识别网站的协议（HTTP 或 HTTPS）。

这种区分有助于进一步隔离和诊断问题。

STEP 3 | （HTTPS 站点或包含 HTTPS 内容的 HTTP 站点）验证 SSL/TLS 解密策略规则是否对访问该网站或 URL 类别的流量进行解密。

通常，除非可以解密网站，否则防火墙无法在 *HTTPS* 网站上提供响应页面。

一些网站可能通过 *HTTP* 提供其主页面，但通过 *HTTPS* 提供广告或其他内容。还应对这些网站进行解密，以确保显示响应页面。

1. 登录到 Web 界面。
2. 选择 **Policies**（策略） > **Decryption**（解密），然后验证相关规则是否解密了特定网站或 URL 类别的流量。

   如果不是，请更新解密策略规则以解密网站或 URL 类别。

- 如果已启用 SSL/TLS 解密，但仍未显示响应页面，则启用对 SSL/TLS 握手的检查。
- 在未启用 SSL/TLS 解密的情况下，要通过 HTTPS 会话提供 URL 过滤响应页面，请按照以下步骤操作。

STEP 4 | 确认该网站所属的 URL 类别已被阻止。

如果该类别已在应用于安全策略规则的 URL 过滤配置文件中被阻止，或者已被以特定 URL 类别作为匹配条件的安全策略规则阻止，则给定条目的操作列中的值将显示 `block-url`。

1. 选择 **Monitor**（监控） > **URL Filtering**（URL 过滤）。
2. 搜索受影响的网站，然后选择最新的日志条目。
3. 检查“类别”和“操作”列。

   分配给网站的类别是否准确？通过测试 A 站点（Palo Alto Networks URL 类别查找工具）验证其类别。如果您仍然认为该网站的分类不正确，请提交更改请求。

   操作值是 `block-url` 吗？如果不是，请更新 URL 过滤配置文件或安全策略规则。
4. 记下与此日志条目相关的规则，以备将来参考。

STEP 5 | 确定自定义回复页面是否是导致此问题的原因。

1. 选择 **Device**（设备） > **Response Pages**（响应页面）。
2. 确认仅选择 **Predefined**（预定义）。

   除 **Predefined**（预定义）外，如果在以下任一位置列出了 **Shared**（共享），则自定义响应页面处于活动状态：

   - **Device**（设备） > **Response Pages**（响应页面）：在与给定响应页面对应的“位置”列下。
   - **Device**（设备） > **Response Pages**（响应页面） > ***Type***（类型）：在“位置”下。
3. （如果列出了 **Shared**（共享））将自定义页面恢复到其默认状态，以确认自定义响应页面是问题所在。

   1. **Delete**（删除）自定义页面。
   2. **Commit**（提交）更改。
   3. 访问受影响的网站，查看是否显示默认回复页面。

   如果问题仍然存在，请致电支持部门进行进一步调查。

如果上述步骤无法纠正问题，请联系 Palo Alto Networks 支持人员。可能需要进行其他故障排除才能查明问题。例如，如果响应页面无法在某些网页上运行但适用于其他网页，则通过数据包捕获 (pcap) 工具分析流量以及支持可能会很有帮助。

PAN-DB 私有云

哪里可以使用？	需要提供什么？
• NGFW (Managed by PAN-OS or Panorama)	☐ 高级 URL 过滤许可证（或旧版 URL 过滤许可证） 注意：旧版 *URL* 过滤许可证已停用，但仍支持有效的旧版许可证。

PAN-DB 私有云为限制使用公有云服务的组织提供本地解决方案。值得注意的是，防火墙在 URL 查找期间查询 PAN-DB 私有云服务器，而不是 PAN-DB 公共云服务器。要实施此解决方案，您需要将一个或多个 M-600 或M-700 设备部署为网络或数据中心内的 PAN-DB 服务器。只有运行 PAN-OS 9.1 或更高版本的防火墙才能与 PAN-DB 私有云通信。

PAN-DB 私有云部署不支持 *Advanced URL Filtering* 订阅基于云的分析功能。

下表介绍了 PAN-DB 公有云和 PAN-DB 私有云之间的区别。

表 **1: PAN-DB** 公共云和 **PAN-DB** 私有云之间的差别

差别	PAN-DB 公共云	PAN-DB 私有云
内容更新和数据库更新	每天会多次发布内容（常规和关键）更新和完整数据库更新。PAN-DB 公有云每 5 分钟更新一次恶意软件和网络钓鱼 URL 类别。只要防火墙查询云服务器进行 URL 查找，就会检查关键更新。	工作日的某一天可一次性获取内容更新和完整 URL 数据库更新。
URL 分类请求	您可以通过以下途径请求更改 URL 类别： • Palo Alto Networks 测试站点网站。 • URL 过滤配置文件。 • URL 过滤日志。	您可以通过 Palo Alto Networks 测试 A 站点网站请求更改 URL 类别。
未解析的 **URL** 查询	如果防火墙无法解析 URL 查询，则会将请求发送到公有云中的服务器。	如果防火墙无法解析查询，则会将请求发送到 PAN-DB 私有云中的设备。如果 URL 不匹配，PAN-DB 私有云会向防火墙发送 *unknown* 类别响应；除非您已将设备配置为访问 PAN-DB

差别	PAN-DB 公共云	PAN-DB 私有云
		公有云，否则该请求不会发送到公有云。 如果 PAN-DB 私有云中的设备完全离线运行，则防火墙不会将任何数据或分析发送到公有云。

- PAN-DB 私有云的工作原理
- PAN-DB 私有云设备
- 设置 PAN-DB 私有云

PAN-DB 私有云的工作原理

哪里可以使用？	需要提供什么？
• NGFW (Managed by PAN-OS or Panorama)	❑ 高级 URL 过滤许可证（或旧版 URL 过滤许可证） 注意：旧版 *URL* 过滤许可证已停用，但仍支持有效的旧版许可证。

设置 PAN-DB 私有云时，您可以将 M-600 或 M-700 设备配置为可以直接访问互联网或保持离线状态。设备需要更新数据库和内容才能执行 URL 查询。如果设备没有有效的互联网连接，则必须手动将更新下载到网络上的服务器，并使用 SCP 将更新导入到 PAN-DB 私有云中的每个 M-600 或 M-700 设备中。此外，该设备必须能够为其服务的防火墙获取种子数据库和其他任何正常或关键内容更新。

私有云和公有云部署中的防火墙的 URL 查询过程是相同的。但是，在私有云部署中，防火墙会查询 PAN-DB 私有云中的服务器。您需要指定他们可以查询的每台 M-600 或 M-700 服务器的 IP 地址或 FQDN，以授予防火墙访问私有云服务器的权限。

M-600 和 M-700 设备使用预打包的服务器证书对连接到 PAN-DB 私有云的防火墙进行身份验证。您无法导入或使用其他服务器证书进行身份验证。如果您更改设备的主机名，设备会自动生成一组新的证书来对防火墙进行身份验证。

PAN-DB 私有云设备

哪里可以使用？	需要提供什么？
• NGFW (Managed by PAN-OS or Panorama)	❑ 高级 URL 过滤许可证（或旧版 URL 过滤许可证） 注意：旧版 *URL* 过滤许可证已停用，但仍支持有效的旧版许可证。

要部署 PAN-DB 私有云，您需要一个或多个 M-600 或 M-700 设备。两种设备均采用 Panorama 模式，但要部署为 PAN-DB 私有云，必须将它们配置为在 PAN-URL-DB 模式下运行。在 PAN-URL-DB 模式中，此设备为不想使用 PAN-DB 公共云的企业提供 URL 分类服务。

M-600 设备部署为 PAN-DB 私有云时，可使用两个端口 — MGT (Eth0) 和 Eth1，不能使用 Eth2。管理端口用于对设备的管理访问权，并从 PAN-DB 公共云或网络上的服务器获取最新内容更新。对于 PAN-DB 私有云和网络上的防火墙之间的通信，您可以使用 MGT 端口或 Eth1。

M-200 设备不能部署为 *PAN-DB* 私有云。

PAN-URL-DB 模式下的 M-600 和 M-700 设备：

- 没有 Web 接口，只支持命令行接口 (CLI)。
- 不能由 Panorama 管理。
- 不能部署在高可用性对中。
- 不需要使用 URL 过滤许可证。防火墙必须有有效的 PAN-DB URL Filtering 许可证才能连接到 PAN-DB 私有云并在其中进行查询。
- 随一组默认服务器证书一起提供，这组证书用于对要连接到 PAN-DB 私有云的防火墙进行身份验证。您不能导入或使用其他服务器证书对防火墙进行身份验证。如果您更改 M-600 设备上的主机名，设备将自动生成一组新的证书来对其服务的防火墙进行身份验证。
- 只能重置为 Panorama 模式。如果您想将此设备部署为专用日志收集器，请切换到 Panorama 模式，然后在日志收集器模式中对其进行设置。

设置 PAN-DB 私有云

哪里可以使用？	需要提供什么？
• NGFW (Managed by PAN-OS or Panorama)	❑ 高级 URL 过滤许可证（或旧版 URL 过滤许可证） 注意：旧版 *URL* 过滤许可证已停用，但仍支持有效的旧版许可证。

要在网络或数据中心内将一台或多台 M-600 或 M-700 设备部署为 PAN-DB 私有云，必须完成以下任务：

- 配置 PAN-DB 私有云
- 配置防火墙以访问 PAN-DB 私有云
- 在 PAN-DB 私有云上使用自定义证书配置身份验证

配置 PAN-DB 私有云

哪里可以使用？	需要提供什么？
• NGFW (Managed by PAN-OS or Panorama)	❑ 高级 URL 过滤许可证（或旧版 URL 过滤许可证） 注意：旧版 *URL* 过滤许可证已停用，但仍支持有效的旧版许可证。

STEP 1 | 在机架中安装 M-600 或 M-700 设备。

请参阅相关硬件参考指南中的机架安装说明。

STEP 2 | 注册设备。

STEP 3 | 执行设备的初始配置。

PAN-DB 模式下的 *M-600* 和 *M-700* 设备使用两个端口 — *MGT (Eth0)* 和 *Eth1*；*PAN-DB* 模式下不使用 *Eth2*。管理端口用于对设备的管理访问权以及从 *PAN-DB* 公共云获取最新内容更新。对于设备（*PAN-DB* 服务器）和网络上的防火墙之间的通信，您可以使用 *MGT* 端口或 *Eth1*。

1. 通过以下方式之一连接到设备：
   - 使用串行电缆将计算机连接到设备上的控制台端口，并使用终端模拟软件 (9600-8-N-1) 进行连接。
   - 使用 RJ-45 以太网电缆从计算机连接到设备上的 MGT 端口。从浏览器中访问 https://192.168.1.1。访问此 URL 可能需要将计算机的 IP 地址更改为 192.168.1.0 网络中的地址（如 192.168.1.2）。
2. 收到提示时，登录到设备。使用默认用户名和密码 (admin/admin) 登录。设备将开始初始化。
3. 配置 MGT 接口的网络访问设置（包括 IP 地址）。

   使用以下 CLI 命令：**set deviceconfig system ip-address *<server-IP>* netmask *<netmask>* default-gateway *<gateway-IP>* dns-setting servers primary *<DNS-IP>***。

   变量说明：
   - *<server-IP>* 是要分配给服务器管理接口的 IP 地址
   - *<netmask>* 是子网掩码
   - *<gateway-IP>* 是网络网关的 IP 地址，*<DNS-IP>* 是主 DNS 服务器的 IP 地址
   - *<DNS-IP>* 是 DNS 服务器的 IP 地址
4. 配置网络访问设置，包括 Eth1 接口的 IP 地址。

   使用以下命令：**set deviceconfig system eth1 ip-address *<server-IP>* netmask *<netmask>* default-gateway *<gateway-IP>* dns-setting servers primary *<DNS-IP>***.
5. 将您的更改保存到 PAN-DB 服务器。

   使用 **commit** 命令。

STEP 4 | 切换到 PAN-DB 私有云模式。

您可以在 *Panorama* 模式和 *PAN-DB* 模式之间以及Panorama 模式和日志收集器模式之间来回切换。不支持 *PAN-DB* 模式和日志收集器模式之间的直接切换。切换操作模式会触发数据重置。除“管理访问”设置外，重新启动时会删除所有现有配置和日志。

1. 要切换到 PAN-DB 模式，请使用 **request system system-mode pan-url-db** 命令。
2. 要验证模式切换，请使用 **show system info** 命令。

   如果您已成功切换到 PAN-DB 私有云模式，则 system-mode 字段会显示 PAN-URL-DB。

```
admin@M-600> show system info  hostname:M-600 ip-
address:1.2.3.4 public-ip-address: netmask:255.255.255.0
 default-gateway:1.2.3.1 ipv6-address: unknown ipv6-
link-local-address: fe80:00/64 ipv6-default-gateway:
 mac-address:00:56:90:e7:f6:8e time:Mon Apr 27 13:43:59
 2015 uptime:10 days, 1:51:28 family: m model:M-600
 serial:0073010000xxx sw-version:7.0.0 app-version:492-2638
 app-release-date:2015/03/19 20:05:33 av-version:0 av-release-
date: unknown wf-private-version:0 wf-private-release-date:
 unknown wildfire-version:0 wildfire-release-date: logdb-
version:7.0.9 platform-family: m pan-url-db:20150417-220
 system-mode:Pan-URL-DB operational-mode: normal licensed-
device-capacity:0 device-certificate-status:None
```

3. 要检查设备上的云数据库版本，请使用 **show pan-url-cloud-status** 命令。

   system-info 中的 *pan-url-db* 字段包含相同的信息。

STEP 5 | 安装内容和数据库更新。

设备仅存储当前正在运行的内容版本和一个早期版本。

选择以下安装方法之一：

- 如果 PAN-DB 服务器拥有直接互联网访问权限，请使用以下命令：
  - 检查是否已发布新版本：**request pan-url-db upgrade check**
  - 检查服务器上当前安装的版本：**request pan-url-db upgrade info**。
  - 下载最新版本：**request pan-url-db upgrade download latest**.

    安装最新版本：**request pan-url-db upgrade install <*version latest* | *file*>**.
  - 安排设备自动检查更新：**set deviceconfig system update-schedule pan-url-db recurring weekly action download-and-install day-of-week <*day of week*> at <*hr:min*>**。
- 如果 PAN-DB 服务器处于离线状态，请访问 Palo Alto Networks 客户支持网站，将内容更新下载并保存到您网络上的 SCP 服务器上。然后，您可以使用以下命令导入并安装这些更新：
  - **scp import pan-url-db remote-port <*port-number*> from username@host:path**
  - **request pan-url-db upgrade install file <*filename*>**

STEP 6 | 设置对 PAN-DB 私有云的管理访问

设备有一个默认 *admin* 帐户。您创建的其他任何管理用户可以是超级用户（具有完全访问权）或拥有只读访问权的超级用户。

PAN-DB 私有云不支持使用 *RADIUS VSA*。如果防火墙或 *Panorama* 上使用的 *VSA* 用于支持访问 *PAN-DB* 私有云，将出现身份验证失败。

- 要在 PAN-DB 服务器上设置本地管理用户，请使用以下命令：
  1. **configure**
  2. **set mgt-config users <*username*> permissions role-based <superreader | superuser> yes**
  3. **set mgt-config users <*username*> password**
  4. Enter password:**xxxxx**
  5. Confirm password:**xxxxx**
  6. **commit**
- 要使用 RADIUS 身份验证设置管理用户，请使用以下命令：
  1. 创建 RADIUS 服务器配置文件：**set shared server-profile radius <*server_profile_name*> server <*server_name*> ip-address <*ip_address*> port <*port_no*> secret <*shared_password*>**。
  2. 创建身份验证配置文件：**set shared authentication-profile <*auth_profile_name*> user-domain <*domain_name_for_authentication*> allow-list <all> method radius server-profile <*server_profile_name*>**。
  3. 将身份验证配置文件附加到用户：**set mgt-config users <*username*> authentication-profile <*auth_profile_name*>**。
  4. 提交更改：**commit**.
- 要查看用户列表，请使用 **show mgt-config users** 命令。

STEP 7 | 将防火墙配置为访问 PAN-DB 私有云。

配置防火墙以访问 PAN-DB 私有云

哪里可以使用？	需要提供什么？
• NGFW (Managed by PAN-OS or Panorama)	☐ 高级 URL 过滤许可证（或旧版 URL 过滤许可证） 注意：旧版 *URL* 过滤许可证已停用，但仍支持有效的旧版许可证。

在使用 PAN-DB 公共云时，各防火墙访问 AWS 云中的 PAN-DB 服务器来下载合格服务器列表，防火墙可连接这些服务器进行 URL 查询。使用 PAN-DB 私有云，您必须使用将用于 URL 查询的

（静态）PAN-DB 私有云服务器列表来配置防火墙。此列表最多可包含 20 个条目，支持 IPv4 地址、IPv6 地址和 FQDN。列表中的每个条目（IP 地址或 FQDN）都必须分配给 PAN-DB 服务器的管理接口和/或 eth1。

STEP 1 | 在 PAN-OS CLI 中，添加用于 URL 查找的静态 PAN-DB 私有云服务器列表。

- 使用以下 CLI 命令添加私有 PAN-DB 服务器的 IP 地址：

```
> configure
```

```
# set deviceconfig setting pan-url-db cloud-static-list <IP addresses>
```

或者，在每个防火墙的 Web 界面中，选择 **Device**（设备）> **Setup**（设置）> **Content-ID**，编辑 URL 过滤部分，然后输入 PAN-DB 服务器的 IP 地址或 FQDN。该列表必须以逗号分隔。

- 要删除私有 PAN-DB 服务器的条目，请使用以下 CLI 命令：

```
# delete deviceconfig setting pan-url-db cloud-static-list <IP addresses>
```

删除私有 PAN-DB 服务器列表会触发防火墙上的重新选择过程。防火墙会先检查 PAN-DB 私有云服务器列表，如果找不到条目，防火墙会访问 AWS 云中的 PAN-DB 服务器来下载可连接的合格服务器列表。

STEP 2 | 输入 **# commit** 以保存更改。

STEP 3 | 要验证更改是否生效，请在防火墙上使用以下 CLI 命令：

```
> show url-cloud status Cloud status:Up URL database version:20150417-220
```

在 PAN-DB 私有云上使用自定义证书配置身份验证

哪里可以使用？	需要提供什么？
• NGFW (Managed by PAN-OS or Panorama)	☐ 高级 URL 过滤许可证（或旧版 URL 过滤许可证） 注意：旧版 *URL* 过滤许可证已停用，但仍支持有效的旧版许可证。

默认情况下，PAN-DB 服务器使用预定义证书进行相互身份验证，以建立用于管理访问和设备间通信的 SSL 连接。但是，您可以使用自定义证书配置身份验证。自定义证书允许您建立唯一的信任链，以确保您的 PAN-DB 服务器和防火墙之间的相互身份验证。对于 PAN-DB 专有云，防火墙充当客户端，PAN-DB 服务器充当服务器。

STEP 1 | 获取密钥对和证书颁发机构 (CA) 颁发的用于 PAN-DB 服务器和防火墙的证书。

STEP 2 | 导入 CA 证书以验证防火墙证书。

1. 登录到 PAN-DB 服务器上的 CLI，并进入配置模式。

```
admin@M-600> configure
```

2. 使用 TFTP 或 SCP 导入 CA 证书。

```
admin@M-600# {tftp | scp} import certificate from <value>
 file <value> remote-port <1-65535> source-ip <ip/netmask>
 certificate-name <value> passphrase <value> format {pkcs12 |
 pem}
```

STEP 3 | 使用 TFTP 或 SCP 导入密钥对，该密钥对包含用于私有云设备的服务器证书和私钥。

```
admin@M-600# {tftp | scp} import keypair from <value> file <value>
 remote-port <1-65535> source-ip <ip/netmask> certificate-
name <value> passphrase <value> format {pkcs12 | pem}
```

STEP 4 | 配置包含根 CA 和中间 CA 的证书配置文件。此证书定义 PAN-DB 服务器和防火墙之间的设备身份验证。

1. 从 PAN-DB 服务器上的 CLI 进入配置模式。

```
admin@M-600> configure
```

2. 命名证书配置文件。

```
admin@M-600# set shared certificate-profile <name>
```

3. （可选）设置用户域。

```
admin@M-600# set shared certificate-profile <name>
 domain <value>
```

4. 配置 CA。

Default-ocsp-url *and* ***ocsp-verify-cert*** *are optional parameters.*

admin@M-600# **set shared certificate-profile <*name*> CA <*name*>**

```
admin@M-600# set shared certificate-profile <name> CA <name>
 [default-ocsp-url <value>]
```

```
admin@M-600# set shared certificate-profile <name> CA <name>
 [ocsp-verify-cert <value>]
```


STEP 5 | 为设备配置 SSL/TLS 服务配置文件。该配置文件定义 PAN-DB 设备和客户端设备用于 SSL/TLS 服务的证书和协议范围。

1. 确定 SSL/TLS 服务配置文件。

```
admin@M-600# set shared ssl-tls-service-profile <name>
```

2. 选择证书。

```
admin@M-600# set shared ssl-tls-service-profile <name>
 certificate <value>
```

3. 定义 SSL/TLS 范围。

   PAN-OS 8.0 和更高版本仅支持 *TLS1.2* 和更高版本的 *TLS*。您必须将最高版本设置为 ***TLS 1.2*** 或 ***max***（更高版本）。

```
admin@M-600# set shared ssl-tls-service-profile <name>
 protocol-settings min-version {tls1-0 | tls1-1 | tls1-2
```

```
admin@M-600# set shared ssl-tls-service-profile <name>
 protocol-settings max-version {tls1-0 | tls1-1 | tls1-2 | max
```

STEP 6 | 在 PAN-DB上配置安全服务器通信。

1. 设置 SSL/TLS 服务配置文件。此配置文件适用于 PAN-DB 和防火墙之间的所有 SSL 连接。

```
admin@M-600# set deviceconfig setting management secure-conn-
server ssl-tls-service-profile <ssltls-profile>
```

2. 设置证书配置文件。

```
admin@M-600# set deviceconfig setting management secure-conn-
server certificate-profile <certificate-profile>
```

3. 设置断开等待时间。这是 PAN-DB 在中断和重新建立与其防火墙的连接之前等待的分钟数（范围为 0 到 44,640）。

```
admin@M-600# set deviceconfig setting management secure-conn-
server disconnect-wait-time <0-44640
```

STEP 7 | 导入 CA 证书以验证设备的证书。

1. 登录到防火墙 Web 界面。
2. 导入 CA 证书。

STEP 8 | 配置防火墙的本地或 SCEP 证书。

1. 如果您正在配置本地证书，请导入防火墙的密钥对。
2. 如果您正在配置 SCEP 证书，请配置 SCEP 配置文件。

STEP 9 | 配置防火墙的证书配置文件。您可以单独在每个防火墙上配置此配置，或者您可以将此配置从 Panorama 推送到防火墙作为模板的一部分。

1. 选择防火墙的 **Device**（设备） > **Certificate Management**（证书管理） > **Certificate Profile**（证书配置文件）或 Panorama 的 **Panorama** > **Certificate Management**（证书管理） > **Certificate Profile**（证书配置文件）。
2. 配置证书配置文件。

STEP 10 | 在每个防火墙上部署自定义证书。您可以从 Panorama 集中部署证书，也可以在每个防火墙上手动配置。

1. 登录到防火墙 Web 界面。
2. 为防火墙选择 **Device**（设备） > **Setup**（设置） > **Management**（管理），为 Panorama 选择 **Panorama** > **Setup**（设置） > **Management**（管理），并 **Edit**（编辑）安全通信设置。
3. 从相应的下拉列表中选择 **Certificate Type**（证书类型）、**Certificate**（证书）和 **Certificate Profile**（证书配置文件）。
4. 从“自定义通信”设置中选择 **PAN-DB Communication**（**PAN-DB** 配置）。
5. 单击 **OK**（确定）。
6. **Commit**（提交）更改。

   提交更改后，在 **Disconnect Wait Time**（断开连接等待时间）结束后，防火墙才会终止与 PAN-DB 服务器的当前会话。断开连接等待时间将在您于下一步骤中，使用自定义证书后开始倒计时。

STEP 11 | 强制执行自定义证书身份验证。

1. 登录到 PAN-DB 服务器上的 CLI，并进入配置模式。

   ```
   admin@M-600> configure
   ```

2. 使用自定义证书。

   ```
   admin@M-600# set deviceconfig setting management secure-conn-
   server disable-pre-defined-cert yes
   ```

提交更改后，如果您已在 PAN-DB 上完成此设置的配置，断开连接等待时间会开始倒计时。等待时间结束后，PAN-DB 及其防火墙仅使用已配置证书进行连接。

STEP 12 | 您可以通过两种方式将新的防火墙或 Panorama 添加至您的 PAN-DB 专有云部署。

- 如果您没有启用 **Custom Certificates Only**（仅允许自定义证书），则可以向 PAN-DB 私有云添加新防火墙，然后部署自定义证书。
- 如果已在 PAN-DB 私有云上启用 **Custom Certificates Only**（仅允许自定义证书），则必须在将其连接至 PAN-DB 私有云之前，在防火墙上部署自定义证书。

