paloalto TECHDOCS

Internet 网关最佳实践安全策略

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

July 24, 2023

Table of Contents

最佳实践 Internet 网关安全策略

攻击者要获得对您的网络的访问权限，最便宜和最简单的方法之一是通过访问 Internet 的用户。通过成功利用端点，攻击者可以进入您的网络并横向移动以实现最终目标：窃取源代码、窃取客户数据或破坏基础设施。为了保护网络免受网络攻击并改进整体安全状况，请实施 Internet 网关安全策略最佳实践。利用最佳实践策略，您可以通过随时控制所有端口的所有流量，安全地启用应用程序、用户和内容。

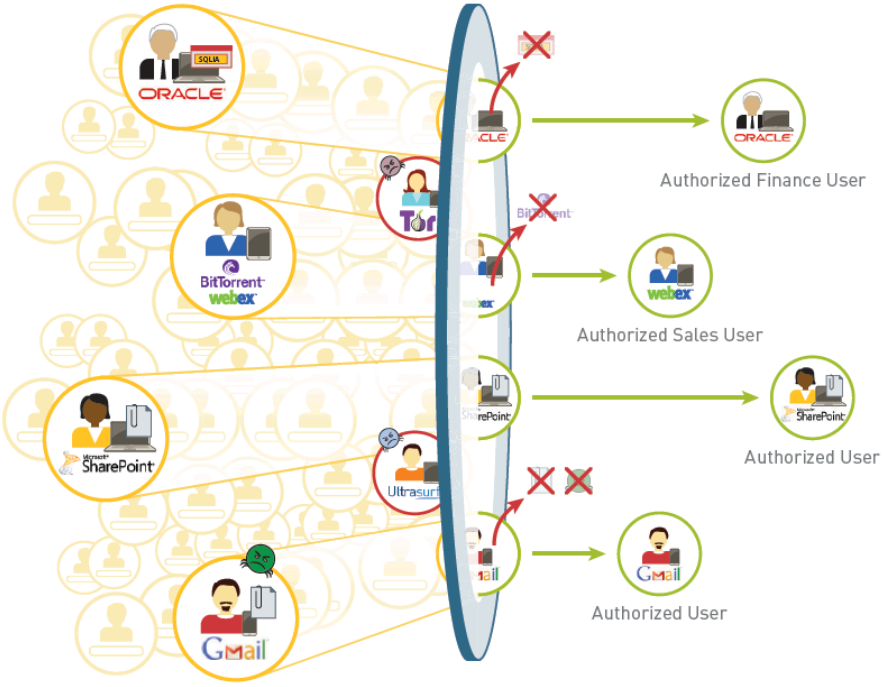
请参阅 Palo Alto Networks 最佳实践书籍系列，了解有关解密、DoS 和区域保护（包括数据包缓冲区保护）等主题的最佳实践建议。

最什么是最佳实践 Internet 网关安全策略？

最佳实践 Internet 网关安全策略主要有两个安全目标：

- 最大限度降低成功入侵的机会 - 传统的基于端口的安全策略会阻止可能影响网络安全的所有流量，或者启用与业务相关的所有流量，与之不同，最佳实践安全策略通过利用 App-ID、User-ID、Content-ID 和 Device-ID（对于 IoT Security，这超出了本书的范围）来确保所有用户可通过所有端口随时安全启用应用程序，并同步扫描所有流量，找出已知和未知威胁。
- 确定是否存在攻击者 - 最佳实践 Internet 网关安全策略提供内置机制来帮助识别规则库中的缺口和检测网络上的警报活动和潜在威胁。

为了实现这些目标，最佳实践 Internet 网关安全策略使用基于应用程序的规则来允许用户访问特定应用程序，扫描所有流量以检测和阻止所有已知威胁，并将未知文件发送到 WildFire，从而识别新威胁和生成阻止这些威胁的签名。



最佳实践策略基于以下方法，确保在攻击生命周期的多个阶段进行检测和预防。

最佳实践原则	为什么重要？
检查所有流量，提高可见度	由于您无法防御不可见的威胁，因此，请确保您能随时全面了解覆盖所有用户和应用程序的所有流量。 • 部署 GlobalProtect，扩展下一代安全平台至任何位置的用户和设备，

最佳实践原则	为什么重要？
	• 请启用解密功能，这样，防火墙就可以检查加密的流量（每年，加密的企业 Web 流量的比例越来越高，使用加密技术的恶意软件活动也越来越多）。 • 启用用户 ID 将应用程序流量和相关威胁映射到用户/设备，并启用策略跟踪用户，无论他们走到哪里。 • 如果公司策略允许用户设备（未配置 GlobalProtect 或未安装其他安全管理应用程序的自带设备或公司设备）位于网络上，则SaaS 安全 API 上的非托管设备访问控制允许用户在任意位置使用个人设备访问您的云 SaaS 应用程序，避免无意中将您的数据或组织置于危险之中。流量通过防火墙重定向，以执行策略和预防威胁。 凭借完全可见性，防火墙可检查所有流量，包括应用程序、威胁和内容，并采用本机 App-ID、Content-ID 和 User-ID 技术将其与用户绑定，无论处于何种位置或采用何种设备类型、端口、加密或规避技术。 全面监控网络上的应用程序、内容和用户是实现明智的策略控制的第一步。
缩小攻击范围	在获得网络上的应用程序、内容和用户的上下文后，创建基于应用程序的安全策略规则，以允许关键业务应用程序并阻止没有合法业务用例的高风险应用程序。 为了进一步减少攻击面，将文件传送阻止及 URL 筛选配置文件附加至所有允许应用程序流量的规则，防止用户访问容易被威胁攻击的网站，上传或下载危险的文件类型（不管是有意还是无意）。为了防止攻击者成功执行网络钓鱼攻击，请配置凭证网络钓鱼防护。
预防已知威胁	将安全配置文件附加到所有允许规则，以便防火墙可以检测并阻止网络和应用程序层漏洞利用、缓冲区溢出、DoS 攻击、端口扫描和已知的恶意软件变体（包括隐藏在压缩文件或压缩 HTTP/HTTPS 流量中的恶意软件变体）。激活加密流量检测，启动解密。 除了基于应用程序的安全策略规则之外，还可以根据 Palo Alto Networks 提供的威胁情报和信誉良好的第三方馈送创建规则，以阻止已知恶意 IP 地址。
检测未知威胁	转发所有文件至WildFire进行分析WildFire 在云中的虚拟环境中或通过 WildFire 设备直接观察并执行未知文件，识别文件中隐藏的未知或有针对性的恶意软件（也称为高级持续性威胁或 *APT*）。如果 WildFire 检测到恶意软件，它会自动开发签名，并可以实时或按照您选择的时间间隔将其传送给您。

我为什么需要最佳实践 Internet 网关安全策略？

最佳实践安全策略允许您通过始终对所有端口上的所有流量（包括加密流量）进行分类来安全地启用应用程序。确定每个应用程序的业务用例，以创建允许和保护对相关应用程序的访问的安全策略规则。对于 IoT 安全（这超出了本书的范畴），最佳实践安全策略利用 Palo Alto Networks 企业安全平台上的下一代技术 - App-ID，Content-ID，User-ID 和 Device-ID，并且：

- 确定除端口、协议、规避策略或加密之外的应用程序。
- 识别和控制用户，而不考虑 IP 地址、位置或设备。
- 防范已知和未知的应用程序传播威胁。
- 对应用程序访问和功能提供精细的可视性和策略控制。
- 如果您有 IoT 部署，请遵循 IoT 安全最佳做法。

最佳实践安全策略采用分层法，确保您不仅能启用认可的应用程序，而且能阻止无合法用途的应用程序。为了降低从基于端口的实施转向基于应用程序的强制时中断应用程序的风险，最佳实践规则库包括临时安全策略规则，用于识别规则库中的漏洞，检测警报活动和潜在威胁，确保应用程序在过渡期间不会中断，并使您能够监控应用程序使用情况，以便您可以制定适当的规则。基于端口的旧策略允许的某些应用程序可能是您不希望允许的应用程序，或者您希望限制为更精细的用户集的应用程序。

最佳实践安全策略更易于管理和维护，因为每个规则都满足特定的业务目标，并允许特定用户组访问应用程序或应用程序组。通过每个规则的应用程序和用户匹配条件，可以更轻松地了解规则强制实施的流量。最佳实践安全策略规则库利用标签和对象，使规则库更易于扫描，且更容易与您不断变化的环境保持同步。

我如何部署最佳实践 Internet 网关策略？

目标是构建基于应用程序的最佳实践安全策略，该策略应与您的业务目标和可接受的使用策略保持一致，简化管理，减少出错几率，并将零信任原则应用于网络接入。

与任何技术一样，通常采用渐进的方法来完成实施。仔细规划部署阶段，使过渡尽可能顺利，同时尽量减少对最终用户的影响。通常，实施最佳实践 Internet 网关安全策略的工作流程如下：

- 评估您的业务并确定需要保护的内容 - 部署安全架构的第一步是评估您的业务。确定您最有价值的资产以及这些资产面临的最大威胁。举个例子，假如您是一家技术公司，那么您最有价值的资产是知识产权。在这种情况下，最大的威胁为源代码盗窃。
- 使用接口和区域对网络进行分段 - 只有在安全策略规则允许的情况下，流量才能在区域之间流动。防止获得网络访问权限的攻击者在网络中横向移动的一种强有力的防御措施是定义精细区域，并且只允许需要访问每个区域中的应用程序或资源的特定用户组进行访问。将您的网络分段成细分区域后，可防止攻击者在您的网络上建立通信通道（通过恶意软件或对合法应用程序的漏洞利用），进而降低成功攻击的可能性。
- 确定您的应用程序允许列表 - 在创建 Internet 网关最佳实践安全策略之前，请先创建要在网络上允许的应用程序清单。单独列出您管理、正式批准的企业申请以及允许员工使用的应用程序。确定要允许的应用程序后，如果要从基于端口的规则库迁移，请将这些应用程序映射到基于端口的规则。如果基于端口的规则没有映射到它的应用程序，则可能不需要该规则。
- 为访问允许的应用程序创建用户组 - 确定您计划允许的应用程序后，您必须确定要求访问每个应用程序的用户组。入侵最终用户的系统是攻击者获取网络访问权限的最便宜、最简单的方法之一。要显著减少攻击面，请仅允许有合法业务需求的用户组访问应用程序。
- 为实现完全可视性和威胁检测解密流量 - 如果无法发现和检测，则无法为网络防御威胁。加密流量是攻击者传播威胁的常用方式。例如，攻击者可能会使用 Web 应用程序，如 Gmail （具有 TLS 加密），向正在访问公司网络上的应用程序的员工发送漏洞利用工具或恶意软件。或者，他会通过影响具有 TLS 加密的网站，悄悄地将漏洞或恶意软件下载至网站访问者的计算机上。
- 为 Internet 网关安全创建最佳实践配置文件 - 命令和控制流、CVE、偷渡式下载恶意内容、网络钓鱼攻击以及 APT 均可通过合法的应用程序传递。要防范已知和未知威胁，请在允许流量的所有安全策略规则中附加严格的安全配置文件。
- 定义初始 Internet 网关安全策略 - 使用创建的应用程序和用户组清单，定义允许用户或用户组访问应用程序的初始策略。初始策略规则库还包含阻止已知恶意 IP 地址的规则，以及防止您可能不知道的应用程序遭到破坏，并识别现有设计中的策略缺陷和安全漏洞的临时规则。
- 监控和微调策略规则库 - 临时规则就位后，您可以开始监视与其相匹配的流量，以便对您的策略进行微调。因为临时规则旨在发现网络上的突发流量，例如非默认端口运行的流量或未知用户产生的流量，因此，您必须评估这些流量是否与规则相匹配，并相应地调整您的应用程序允许规则。
- 移除临时规则 - 通过几个月的监控，您将会发现撞击临时规则的流量越来越少。当您达到不再有流量命中临时规则的点时，请移除临时规则以完成最佳实践 Internet 网关安全策略。
- 维护规则库 - 由于应用程序具有动态性，因此，您必须持续不断地监控您的应用程序允许列表，调整规则以适应新应用程序，并确定新的或修改后的 App-ID 如何影响策略。最佳实践规则

库中的规则与您的业务目标一致，并采用策略对象实现简单化管理，因此，为一个新应用程序或新的或修改后的 App-ID 添加支持的操作常常如同从应用程序组添加或删除一个应用程序或修改一个应用程序筛选器一样简单。

识别应用程序允许列表

应用程序允许列表包括您出于业务、基础设施和用户工作目的而配置和管理的认可应用程序以及您选择允许个人使用的容忍应用程序。在创建 Internet 网关安全策略之前，请创建要允许的应用程序的清单。

- 将应用程序映射到业务目标，简化规则库
- 使用临时规则优化允许列表
- 应用程序允许列表示例

将应用程序映射到业务目标，简化规则库

盘点网络上应用程序时，应考虑您的业务目标和可接受的使用策略，识别与此相对应的应用程序。这使您能够创建目标驱动的规则库。例如，业务目标可能会允许销售和支持组访问您的客户数据库。创建与每个目标对应的允许规则，并将与目标一致的所有应用程序分组到单个规则中。此方法使您能够创建具有较少数量的单个规则的规则库，并且每个规则都有明确的用途。

因为您创建的单个规则与您的业务目标相符，因此，您可通过应用程序对象组合允许的应用程序，以便进一步简化规则库的管理：

- 为每组批准的应用程序创建应用程序组 - 创建仅显式包含已批准应用程序集的应用程序组。应用程序组简化了策略的管理，因为它们使您能够添加和删除批准的应用程序，而无需修改单个安全策略规则。通常，如果映射至同一目标的应用程序的访问要求相同（例如，它们都有指向 Internet 的目的地址，都允许访问任何已知用户，并且您希望仅通过默认端口启用他们），则应将这些应用程序添加至同一应用程序组。

  使用预定义的已批准标签标记所有经批准的应用程序。*Panorama* 和防火墙认为不带批准标记的应用成为是未批准的应用程序。
- 创建应用程序过滤器以允许每种类型的常规应用程序 - 除了您正式批准的应用程序外，您还需要确定要允许用户访问的其他应用程序。通过应用程序筛选器，您可根据标记、类别、子类别、技术、风险因素或特征安全启用某些类别的应用程序。基于业务和个人使用目的划分不同类型的应用程序。为每种类型的应用程序创建单独的筛选器，以便理解每个策略规则。

使用临时规则优化允许列表

基于应用程序的安全策略的最终目标是显式允许您想要允许的应用程序流量并隐式拒绝您不想要的流量。但是，初始规则库需要一些临时规则，以确保您对网络上的所有应用程序具有完全可见性，以便您可以正确调整策略。初始规则库需要以下类型的规则：

- 允许您为业务目的正式批准和部署的应用程序的规则。
- 根据可接受的使用策略，用于安全访问您想要允许的容忍应用程序的允许规则。
- 阻止没有合法用例的应用程序的规则。这些规则可防止恶意流量进入您的网络，而临时规则会发现您的策略规则库尚未考虑的应用程序。

- 能让您了解网络上正在运行的所有应用程序的临时允许规则，方便调整规则库。

临时规则：

- 提供对网络上您不知道的应用程序的可见性。
- 防止您不知道的合法应用程序被阻止。
- 识别未知用户、未知应用程序以及在非标准端口上运行的应用程序（攻击者通常在非标准端口上使用标准应用程序作为恶意活动的规避技术）。

识别在非标准端口上运行的合法应用程序（例如，内部开发的应用程序），以便您可以修改应用程序使用的端口或创建要在策略中使用的自定义应用程序。

如果您创建了应用程序覆盖策略规则来定义一组端口的自定义会话超时，请通过配置基于服务的会话超时，将应用程序覆盖策略转换为基于应用程序的策略，以维护每个应用程序的自定义超时。然后将每个规则迁移到基于应用程序的规则。应用程序覆盖策略是基于端口的，并且不提供应用程序对流量的可见性，因此，您不知道使用端口的应用程序，也无法控制。基于服务的会话超时实现自定义超时，同时保持应用程序可见性。

应用程序允许列表示例

您并不需要捕获网络上的初始清单中可能正在使用的每个应用程序。请重点关注您想要允许的应用程序。临时规则会捕获网络上可能存在的其他应用程序，因此在过渡到基于应用程序的策略期间，有关遭到损坏的应用程序的投诉不至于让您焦头烂额。下表显示了企业网关部署的示例应用程序允许列表。

应用程序类型	以安全为目的的最佳实践
SaaS 应用程序	本软件和基础设施归SaaS 应用程序服务提供商所有和管理，但您拥有数据的完全控制权，包括确定谁可以创建、访问、共享和传输此数据。要控制 SaaS 应用程序，请使用 SaaS Security（需要订阅）。如果您使用 SaaS 安全性，请使用 SaaS 策略建议来控制防火墙上的 SaaS 应用程序。 如果您没有 SaaS 安全订阅，请生成 SaaS 应用程序使用报告，以便检查当前使用的 SaaS 应用程序是否有不适宜的托管特征，如过去的数据泄露或缺少应有的认证。基于业务需求和您可以接受的风险大小，使用此信息： • 立即拦截具备不适宜托管特征的现有应用程序。 • 创建更精准的策略拦截具备不适宜托管特征的应用程序，防止将来出现违规行为。 • 确定具备不适宜托管特征的上层应用程序的网络流量趋势，以便您可以对策略做出相应调节。 许多 SaaS 应用程序都有企业版和消费者（个人）版本，但不受限制的使用会增加泄露敏感数据的风险。HTTP 标头插入可让您控制网络上允许的

应用程序类型	以安全为目的的最佳实践
	SaaS 应用程序版本。例如，您可以允许企业版 Box 或 Office 365 并阻止消费者版本。通过仅允许您希望批准或容忍用户个人使用的每个 SaaS 应用程序的版本，HTTP 标头插入可减小了攻击面。

经批准的应用程序	IT 部门管理员专为您组织内业务使用，或为您的网络和应用程序提供基础结构而批准的应用程序。例如，在 Internet 网关部署中，这些程序可分为以下几类：
	• 基础设施应用程序 - 必须允许才能启用网络和安全性的应用程序，例如 ping、NTP、SMTP 和 DNS。
	• **IT** 认可的应用程序 - 为用户配置和管理的的应用程序。分为两类：
	  • **IT** 认可的本地应用程序 - 在数据中心安装和托管的供业务使用的应用程序。通过IT批准的预置应用程序，程序基础结构和数据可保存在企业拥有的设备上。例子包括 Microsoft Exchange 和动态同步，以及 Kerberos 和 LDAP 等身份验证工具。
	  • **IT** 认可的 **SaaS** 应用程序 - IT 部门出于业务目的认可的 SaaS 应用程序，例如 Salesforce、Box 和 GitHub。
	• 管理应用程序 — 仅供特定管理用户组使用的应用程序，目的是管理应用程序和支持用户（例如，远程桌面应用程序）。
	使用预定义的已批准标签标记所有经批准的应用程序。全景图和防火墙认为不带批准标记的应用成为是未批准的应用程序。

允许的应用程序类型	除了正式批准的应用程序之外，您还需要允许用户安全地访问其他类型的可容忍应用程序： • 通用商务应用程序 - 例如，允许访问容忍应用程序的软件更新和 Web 服务，如 WebEx、Adobe 在线服务和 Evernote。 • 个人应用程序 - 例如，您可能允许用户浏览网页或安全使用基于 Web 的邮件、即时消息或社交网络应用程序，包括某些消费者版本的 SaaS 应用程序。 从广泛的应用程序过滤器开始，了解您的网络上有哪些应用程序。确定您愿意承担多少风险并缩减应用程序允许列表。例如，您可能有多个消息应用程序，每个应用程序都有固有的数据泄露，还可能传输被恶意软件感染的文件等风险。 最佳方法是批准单个消息应用程序，然后逐渐从允许策略过渡到警报策略，并在向用户发出充分警告后，过渡到阻止策略以逐步淘汰其他消息应用程序。您也可以选择一小部分用户继续使用额外的消息应用程序，以便与同事一起完成相应的工作。

应用程序类型	以安全为目的的最佳实践
专用于您的环境的自定义应用程序	为专有应用程序或在非标准端口上运行的应用程序创建自定义应用程序。这样，您可以将这些程序定义为认可的应用程序（并应用预定义的已认可标签），并将其锁定至默认端口。否则，您必须打开额外的端口（对于在非标准端口上运行的应用程序）或允许未知流量进入（对于专有应用程序）。这两种方式都不符合最佳实践安全策略的建议。 如果您有现用的应用程序替代策略，该策略是专门为定义端口集合的自定义会话超时而单独创建的，则通过将基于服务的会话超时配置为维护每个应用的自定义超时，将现有的应用程序替代策略转换为基于应用程序的策略。然后将每个规则迁移到基于应用程序的规则。应用程序覆盖策略是基于端口的，并且不提供应用程序对流量的可见性，因此，您不知道使用端口的应用程序，也无法控制。基于服务的会话超时实现自定义超时，同时保持应用程序可见性。

创建可访问允许的应用程序的用户组

安全启用应用程序意味着定义要允许的应用程序列表，并仅允许有合法业务需求的用户访问权限。例如，一些应用程序，如软件即服务应用程序，可访问人力资源服务（如工作日或现时服务），仅能提供给网络上任何已知用户访问。但是，对于更敏感的应用程序，可以仅允许出于业务目的需要这些应用程序的用户访问权限，从而减少攻击面。例如，IT 支持人员可能合法需要访问远程桌面应用程序，但大多数用户不需要。限制用户对应用程序的访问可防止攻击者可能利用潜在安全漏洞来访问和控制您网络上的系统。

激活基于用户访问的应用程序：

- 激活您用户启用流量的区中的 User-ID。
- 对于定义的每个应用程序允许列表规则，识别对应用程序访问具有合法业务需求的用户组。与将基于端口的规则映射到用户相比，将应用程序映射到业务目标（包括考虑哪些用户对特定类型的应用程序有业务需求）可以减少需要管理的规则数量。
- 如果您的 Active Directory (AD) 服务器上没有现有的用户组，也可以创建自定义 LDAP 组以匹配需要访问特定应用程序的用户组。
- 只要有一名最终用户点击网络钓鱼链接并提供其凭据，攻击者就能访问您的网络。为了防御这种简单而有效的攻击技术，在所有允许用户访问 Internet 的安全策略规则上设置网络凭据钓鱼保护。使用基于 Windows 的 User-ID 代理配置凭据检测，以确保您可以检测用户何时向未授权类别的网站提交公司凭证。

解密流量，实现完全可视性，检测威胁

解密除敏感类别之外的所有流量，敏感类别包括 URL 类别，例如金融服务、健康和医疗、政府以及出于业务、法律或监管原因不解密的其他流量。使用 URL 类别、自定义 URL 类别和 External Dynamic Lists (EDLs) 来指定不解密的流量。

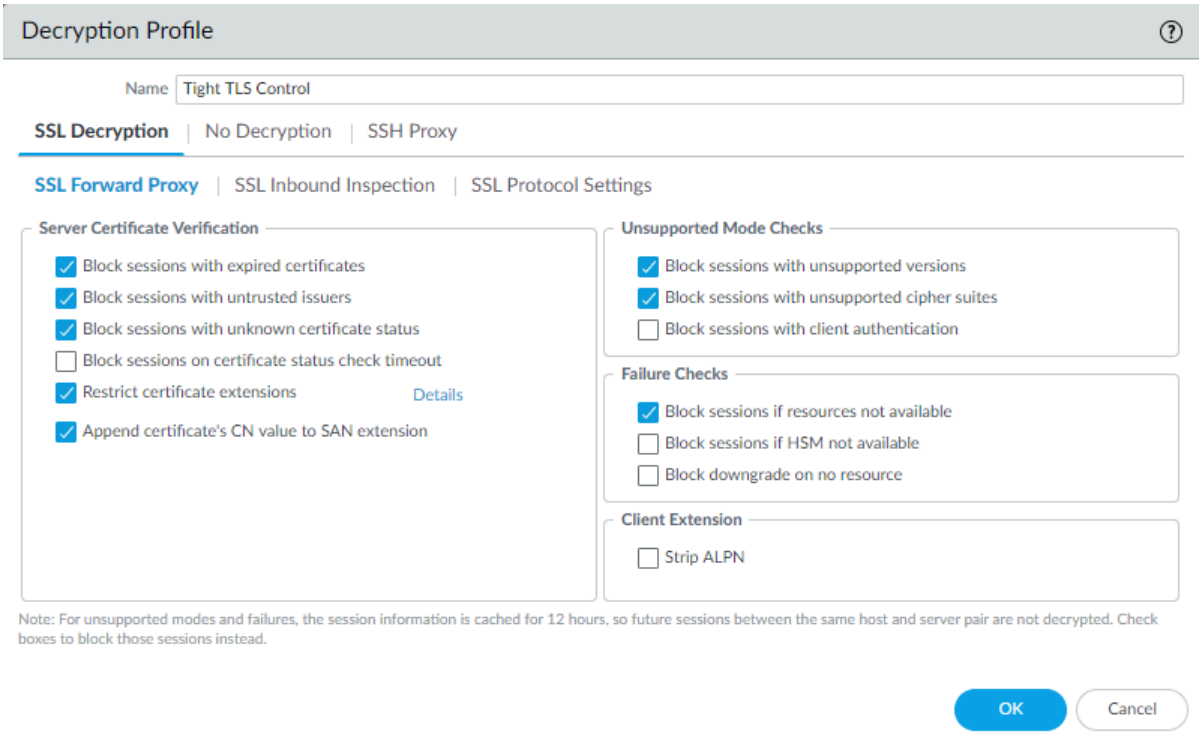
仅在需要时使用解密异常。精确地确保您根据需要限制特定应用程序或用户的例外情况：

- 如果解密损坏了重要的应用程序，在程序关联的证书中为特定的 IP 地址，域名，或公用名创建一个例外。
- 如果您由于法规、业务或法律原因而需将特定用户排除在外，只为该用户创建一个例外。

为了确保解密期间提供的证书有效，请执行 CRL/OCSP 检查。

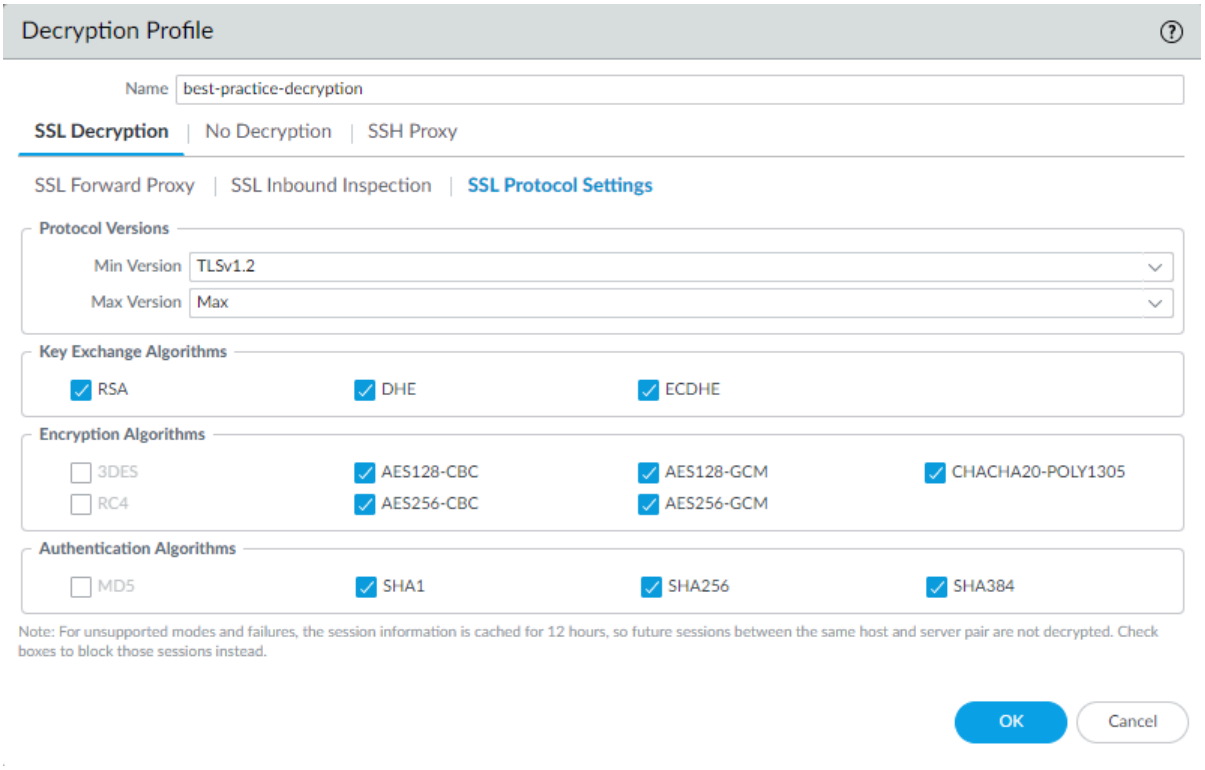
将严格的解密配置文件添加到解密策略规则中。在配置 SSL 转发代理之前，创建一个最佳实践解密配置文件（**Objects**（对象）> **Decryption Profile**（解密配置文件）），并将其附加到解密策略规则中，同时遵循一般解密最佳实践操作：

STEP 1 | 配置 **SSL Decryption**（**SSL** 解密）> **SSL Forward Proxy**（**SSL** 转发代理）设置，阻止 TLS 协商过程中的异常和无法解密的会话：



Block sessions if resources not available（如果资源不可用，则阻止会话）可防止在防火墙没有执行解密的资源时允许潜在危险的连接，但阻止因此无法解密的流量可能会影响用户体验。

STEP 2 | 配置 **SSL Decryption**（**SSL** 解密）> **SSL Protocol Settings**（**SSL** 协议设置），阻止使用易受攻击的 SSL/TLS 版本（TLS 1.0、TLSv1.1 和 SSLv3），并避免使用脆弱的算法（MD5、RC4 和 3DES）：

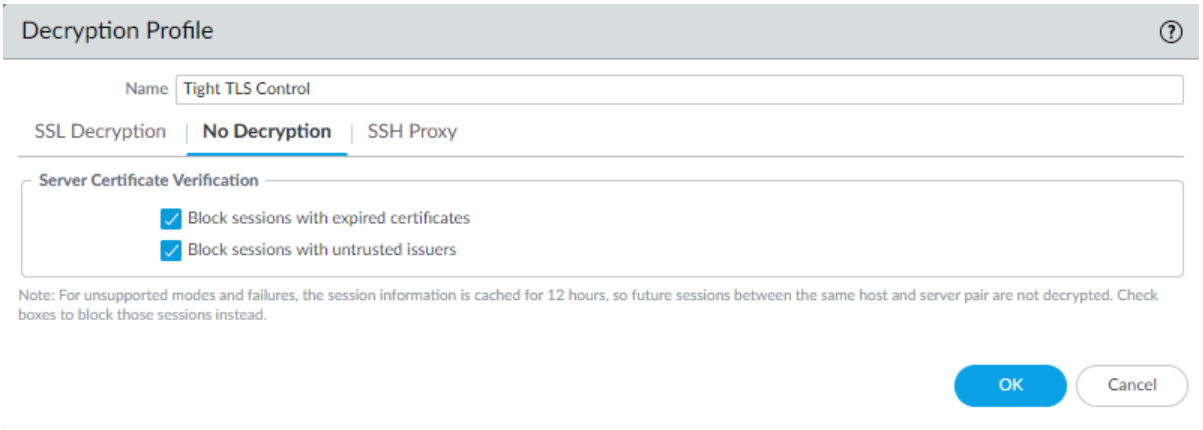


如果可能，请使用 TLSv1.3（最安全的协议）。许多移动应用程序使用证书固定来防止解密并导致防火墙丢弃流量。对于该流量，请使用 TLSv1.2。

审查您需要进行商业目的的访问的站点。如果其中任何一个使用 TLSv1.1，请为这些站点创建单独的解密策略和配置文件，以便只有出于业务目的必须访问的站点才能使用安全性较低的协议。

除非必须，否则不要允许 SHA1 身份验证算法。为使用 SHA1 的站点创建单独的解密策略规则和配置文件，您必须出于业务目的访问这些站点。

STEP 3 | 对于不解密的流量，配置 **No Decryption**（不解密）设置，阻止证书过期或不受信任发行者的加密会话访问站点：



仅对 *TLSv1.2* 和更早的版本使用“不解密”配置文件。不要将“不解密”配置文件附加到未解密的 *TLSv1.3* 通信。*TLSv1.3* 对以前版本中未加密的证书信息进行加密，因此，防火墙无法阻止基于证书信息的会话。

安全转换为最佳实践安全配置文件

利用安全配置文件，您可以检查网络流量是否存在漏洞利用、恶意软件、命令和控制 (C2) 通信以及未知威胁等，并防止它们使用各种类型的威胁签名、机器学习和 AI 来破坏您的网络（某些保护措施需要订阅）。

最终目标是让所有安全配置文件达到最佳实践状态。但是，为了确保业务关键型应用程序的可用性，从一开始就实施完整的最佳实践安全配置文件配置可能并不可行。在大多数情况下，您可以安全地阻止某些签名、文件类型或协议，同时为其他项目提供警告，在充分了解信息后，您可以胸有成竹地安全过渡到最佳实践安全配置文件，而不影响可用性。

实施最佳实践安全配置文件的路径是：

1. 使用 AIOps 生成有关安全状况的按需最佳实践评估 (BPA) 报告。查看最佳做法采用情况，确定采用方面的差距，并查看安全配置文件配置。
2. 使用以下安全过渡步骤将您的安全配置文件转换到最佳实践状态。

问自己以下问题来帮助确定为指定网段或安全策略规则组启用安全配置文件的正确方法：

1. 我在保护类似应用程序或网段的规则上是否已启用安全配置文件？如果答案是肯定的，则您可以复制这些配置文件设置，包括您认为可以安全启用的阻止操作。
2. 我保护的网段是否对我的业务至关重要？如果答案是肯定的，并且您没有在类似细分中启用经过验证的配置文件，则您可能更愿意先发出警报，检查导致警报的流量以确保配置文件不会阻止关键应用程序，然后在您满意时阻止。
3. 我是不是在部署安全配置文件来应对即时威胁？如果答案是肯定的，您可能希望将阻止作为初始操作（而不是警报）。
4. 是否存在防火墙更改流程，以便及时调查和纠正误报？如果答案是肯定的，您可以将阻止作为初始操作（而不是警报）。

> 大多数“误报”都是尝试对网络中不存在的漏洞发起的攻击行为。攻击是真实的，但没有危险，因为漏洞不存在，所以攻击通常被视为误报。如果攻击阈值设置得太低，暴力攻击签名也可能导致误报。

考虑您当前的安全状态，并结合每种类型的安全配置文件的指导，决定刚开始如何部署配置文件，然后转到最佳实践指南。

- 安全转换漏洞保护配置文件为最佳实践
- 安全转换防间谍软件配置文件为最佳实践
- 安全转换防病毒配置文件为最佳实践
- 安全转换 WildFire 配置文件为最佳实践
- 安全转换 URL 筛选配置文件为最佳实践
- 安全转换文件阻止配置文件为最佳实践

安全转换漏洞保护配置文件为最佳实践

首次将漏洞防护配置文件应用到流量时，采用阻止或警告的决策取决于您在安全性与可用性方面的当前安全状况和业务需求。以下指南可帮助您确定在开始过渡到最佳实践漏洞防护配置文件时是否开始阻止或警报操作。

漏洞防护需要高级威胁防护或有效的旧版威胁防护订阅。

为了识别和防止威胁，防火墙必须能够了解应用程序流量。在当地法规、业务考虑、隐私考虑和技术能力允许的情况下解密尽可能多的流量。如果您不解密流量，防火墙将无法分析加密的标头和有效负载信息。

此外，请遵循威胁内容更新最佳实践，以确保您的安全配置文件签名是最新的。

- 业务关键型应用程序 - 通常最好将初始规则 **Action**（操作）设置为 **alert**（警报）以确保应用程序可用性。但是，在某些情况下，您可以从一开始就使用阻止操作。例如，如果您已使用阻止漏洞签名的漏洞防护配置文件保护类似的应用程序，并且您确信配置文件满足您的业务和安全需求时，则可以使用类似的配置文件来阻止漏洞并保护类似的应用程序。

  警报使您能够在开始阻止流量之前分析威胁日志并在必要时创建异常。在转向阻止之前发出警报和监控可以让您确信：

  - 当您部署初始配置文件时，它不会阻止关键业务应用程序。
  - 当您转换到阻塞状态时，您可以创建必要的异常以维持应用程序可用性。

  将保持初始警报操作的时间保持在最短，以减少出现安全漏洞的可能性。一旦您觉得已经确定了需要添加的任何例外情况并相应地配置配置文件后，就可以开始转换到阻止状态了。
- 关键和高严重性签名 - 关键和高严重性签名的误报率通常比较低，而且一般表示攻击者对您的网络中不存在的漏洞发起了攻击。对于非业务关键型应用程序（例如 Internet 访问），可以从一开始就阻止（**reset-both**（重置两者））关键和高严重性签名。
- 中等严重性签名 - 可能会产生误报且需要初始监控。首先通过得对中等严重性签名发出警告并监控威胁日志（**Monitor**（监视） > **Logs**（日志） > **Threat**（威胁）），以查看是否需要阻止收到警报的应用程序，还是需要允许它们。
- 微调在转换为阻止之前发出警报的配置文件规则，尤其是面向互联网和数据中心的流量。当您感觉舒服的时候，尽快转移到阻塞状态。
- 将暴力类别中的签名设置为警报，然后尽快转为阻止。暴力事件是当某个操作在短时间内多次发生时触发的聚合事件。例如，一次 SSH 登录尝试是一个信息事件，但 10 秒内 100 次登录尝试会触发暴力签名。尽管调整配置文件可能需要一些时间，以便正常的网络流量不会触发暴力签名，但请根据您的舒适度，尽快安全地过渡到阻止这些签名。

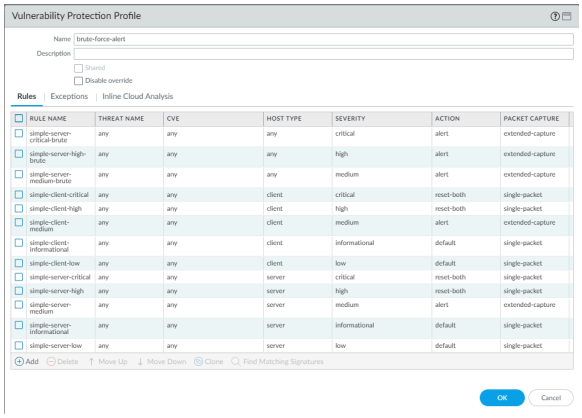


图 **1:** 暴力破解警报漏洞保护配置文件

- 大多数低严重性和信息严重性签名的默认操作是警告或允许。除非您有特定需要对所有低签名和信息签名发出警报，否则请将 **Action** 配置为 **default**。
- 如果资源可用，请针对您发出警报的关键、高和中严重性签名启用扩展数据包捕获。对被阻止的签名以及低严重性和信息性严重性签名启用单个数据包捕获。启用数据包捕获可让您在必要时更详细地调查事件。当您转到最佳实践配置文件时，如果信息性事件创建太多数据包捕获活动（流量过大），而信息又不是特别有用，则可以转换为禁用信息性事件的数据包捕获。

  数据包捕获会消耗管理平面资源。检查系统资源（例如，***Dashboard***（仪表板）> ***System Resources***（系统资源）），以了解实施数据包捕获之前和之后的使用情况，从而确保您的系统有足够的资源来捕获所有数据包。
- 对于内联云分析，请使用与安全漏洞防护规则相同的标准来发出警报和阻止业务应用程序。如果您有现有的控制措施，则可以复制它们以阻止流量。对于新的控制措施，在过渡到阻止之前至少警告一周。尽快转向阻止。

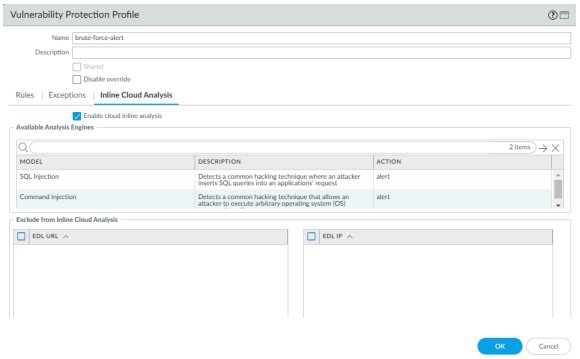


图 **2:** 内联云分析警报漏洞保护配置文件

如果有初始配置文件，请监控威胁日志足够长的时间，以便确信您已了解是否有任何业务关键型应用程序会导致警报或阻止。在转换到完整的漏洞防护最佳实践配置文件之前，根据需要在每个配置文件中创建例外（如有必要，打开支持票证）以修复已确认的误报。完成向最佳实践配置文件过渡的速度取决于您的业务、应用程序和兼容程度 - 请注意，某些应用程序仅每周、每月、每季度或每年用于审核、定期活动和会议等。

安全转换防间谍软件配置文件为最佳实践

在定义初始防间谍软件配置文件并开始过渡到最佳实践配置文件时，以下指南可帮助确定是否以阻止或警报操作开始。

反间谍软件需要高级威胁防护或有效的旧版威胁防护订阅。

为了识别和防止威胁，防火墙必须能够了解应用程序流量。在当地法规、业务考虑、隐私考虑和技术能力允许的情况下解密尽可能多的流量。如果您不解密流量，防火墙将无法分析加密的标头和有效负载信息。

此外，请遵循威胁内容更新最佳实践，以确保您的安全配置文件签名是最新的。

- 业务关键型应用程序 - 设置警报的初始操作以确保应用程序可用性。但是，在某些情况下，您可以从一开始就使用阻止操作。例如，如果您已使用阻止关键、高和/或中等严重性签名的防间谍软件配置文件保护应用程序，并且您确信配置文件满足您的业务和安全需求时，则可以使用类似的配置文件来阻止间谍软件并保护这些应用程序。

  警报操作让您可以分析威胁日志并在必要时创建例外，然后再转到阻止操作。在进行阻止之前发出警报和监控可以让您确信：

  - 当您部署配置文件时，它不会阻止关键业务应用程序。
  - 当您转换到阻塞状态时，您可以创建必要的异常以维持应用程序可用性。

  一旦您觉得已经确定了需要进行的任何例外处理并相应地配置了配置文件，就可以转换到最佳实践状态。
- 关键和高严重性签名 - 误报率通常比较低。对于非业务关键型应用程序，可以从一开始就阻止关键和高严重性签名。
- 中等严重性签名 - 可能会产生误报且需要初始监控。首先针对内部流量的中等严重性签名发出警报，并针对面向外部的流量阻止中等严重性签名。监视威胁日志（**Monitor**（监视） > **Logs**（日志） > **Threat**（威胁））以查看是否应该阻止收到警报的应用程序，或者是否需要允许它们。
- 低严重性和信息性严重性签名 - 大多数这些签名的默认操作是警报或允许。除非您特别需要警告所有低严重性和信息性签名，否则请从默认操作开始。
- 如果您有这些资源，请在过渡期间为所有严重性签名启用单一数据包捕获。启用数据包捕获可让您在必要时更详细地调查事件。当您转到最佳实践配置文件时，如果低严重性或信息性事件创建太多数据包捕获活动（流量过大），而信息又不是特别有用，则可以转换为禁止对这些严重性级别捕获数据包。

  数据包捕获会消耗管理平面资源。检查系统资源（例如，***Dashboard***（仪表板） > ***System Resources***（系统资源））以了解实施数据包捕获之前和之后的使用情况，从而确保系统有足够的资源来捕获所有数据包。
- 如果将内部应用程序与外部应用程序区别对待，则可能需要针对面向 Internet 的流量使用反间谍软件配置文件，对内部通信使用另一个反间谍软件配置文件。

- **DNS** 政策：
  - 将 DNS 签名的 策略操作 设置为 **Sinkhole**，以识别尝试访问可疑域的潜在受感染主机。DNS Sinkhole 使您能够跟踪主机并阻止它们访问这些域。（立即启用 DNS Sinkhole 是最佳实践。） 将 **Packet Capture**（数据包捕获）设置为 **extended-capture**（扩展捕获）
  - Sinkhole 所有 **DNS Security**（**DNS** 安全）域类型，并设置 **Packet Capture**（数据包捕获），如图 1（PAN-OS 10.0 及更高版本）所示。
  - 此外，阻止所有 DNS 记录类型，因为它们由加密的 DNS 查询使用。这可以防止客户端在 DNS 解析过程中对客户端 Hello 信号进行加密，从而阻止密钥信息的交换。

仅允许流量流向经批准的 *DNS* 服务器。使用 DNS 安全服务阻止恶意 *DNS* 服务器连接。

在基于 *PAN-OS* 的系统上，将 *DNS* 接收器地址设置为 *FQDN*，例如，*sinkhole.paloaltonetworks.com*，这样，如果 *IP* 地址发生更改，该设置仍然有效。对于 *Prisma Access*，请使用 *Sinkhole IP* 地址。

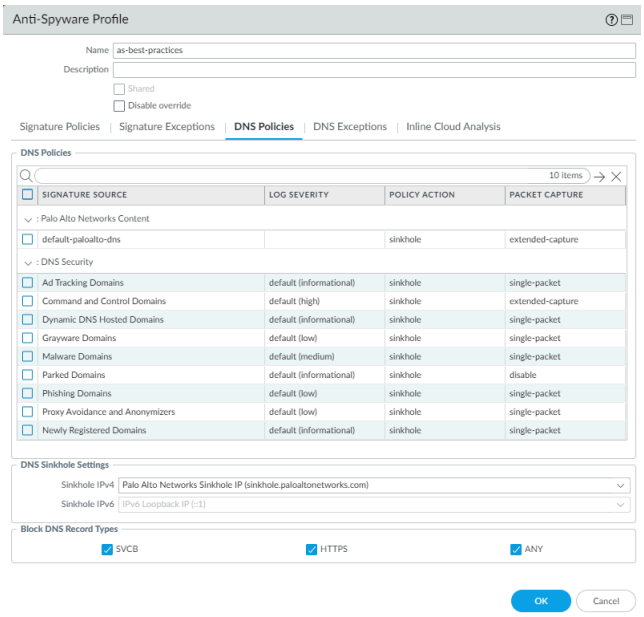


图 **3:** 反间谍软件配置文件 **DNS** 策略

- 内联云分析（需要高级威胁防护订阅和 PAN-OS 10.2 或更高版本）- 对所有出站流量启用云内联分析。为所有模型将 **Action**（操作）设置为 **reset-both**（重置两者）。

气隙环境无法使用高级威胁防护，因为它是云服务并且需要云连接。

如果有初始配置文件，请监控威胁日志足够长的时间，以便确信您已了解是否有任何业务关键型应用程序会导致警报或阻止。只要您愿意，请立即过渡到最佳实践反间谍软件配置文件。根据需要在每个配置文件中创建例外（必要时开立支持票据），以便在实施完整的最佳实践防间谍软件配置文件之前修复任何已确认的误报。

安全转换防病毒配置文件为最佳实践

在克隆默认防病毒配置文件，对其进行修改以定义初始配置文件，并开始过渡到最佳实践配置文件时，以下指南可帮助您确定是否开始阻止或警报操作。

防病毒软件需要高级威胁防护或有效的旧版威胁防护订阅。

为了识别和防止威胁，防火墙必须能够了解应用程序流量。在当地法规、业务考虑、隐私考虑和技术能力允许的情况下解密尽可能多的流量。如果您不解密流量，防火墙将无法分析加密的标头和有效负载信息。

此外，请遵循威胁内容更新最佳实践，以确保您的安全配置文件签名是最新的。

- 业务关键型应用程序 - 设置警报的初始操作以确保应用程序可用性。但是，在某些情况下，您可以从一开始就阻止防病毒签名。例如，如果您已使用防病毒配置文件保护类似的应用程序，并且您确信该配置文件符合您的业务和安全需求，则可以使用类似的配置文件来保护类似的应用程序，因为您已经了解了要阻止的对象。

  警报操作让您可以分析威胁日志（***Monitor***（监控） > ***Logs***（日志） > ***Threat***（威胁））并在必要时创建例外，然后再转到阻止操作。在转向阻止之前发出警报和监控可以让您确信：

  - 当您部署配置文件时，它不会阻止关键业务应用程序。
  - 当您转换到阻塞状态时，您可以创建必要的异常以维持应用程序可用性。

  将维持初始警报操作的时间保持在最低限度，以减少发生安全事件的可能性。一旦您觉得已经确定了需要进行的任何例外处理并相应地配置了配置文件，就可以转换到最佳实践状态。
- 关键和高严重性签名 - 部署最佳实践防病毒配置文件来阻止对您的业务不重要的应用程序的恶意流量是安全的，因为误报率很少，因此很少发生不必要的阻止。
- 如果将内部应用程序与外部应用程序区别对待，则可能需要针对面向 Internet 的流量使用防病毒配置文件，为内部流量使用另一个防病毒配置文件。
- 在设备上和防病毒配置文件中全局启用实时签名查找以保留文件，直到防火墙从云端收到最新的实时防病毒签名：
  - 全局启用 - **Device**（设备） > **Setup**（设置） > **Content-ID** > **Content-ID Settings**（**Content-ID** 设置） > **Realtime Signature Lookup**（实时签名查找），启用 **Hold for WildFire Real Time Signature Look Up**（为 **WildFire** 实时签名查找保留），并将 **Action On Real Time Signature Timeout**（实时签名超时后的操作）设置为 **Reset Both**（重置两者）。您必须全局启用实时签名查找才能在防病毒配置文件中启用。
  - 在防病毒配置文件中启用 - **Objects**（对象） > **Security Profiles**（安全配置文件） > **Antivirus**（防病毒），并启用 **Hold for WildFire Real Time Signature Look Up**（为 **WildFire** 实时签名查找保留）。

保留文件以确保 WildFire 获得最新的防病毒签名，从而保护您免受零日恶意软件和过时的防病毒签名的侵害，如果您转发文件而不保留文件以获取最新签名，则可能会暴露给这些恶意软件和过时的防病毒签名。

- 如果流量生成的 WildFire 签名会导致重置或丢弃操作，那么防病毒软件配置文件内的 WildFire 操作设置可能会影响该流量。

如果有初始配置文件，请监控威胁日志足够长的时间，以便确信您已了解是否有任何业务关键型应用程序会导致警报或阻止。还要监控 WildFire 提交日志（**Monitor**（监控）> **Logs**（日志）> **WildFire Submissions**（**WildFire** 提交））足够长的时间，以便确信您已了解是否有任何业务关键型应用程序因防病毒配置文件 WildFire 操作而导致产生警报或阻止。根据需要在每个配置文件中创建例外（必要时开立支持票据），以便在实施完整的最佳实践防病毒软件配置文件之前修复任何已确认的误报。过渡到最佳实践配置文件的速度取决于您的业务、应用程序和舒适度 - 请注意，某些应用程序仅每周、每月、每季度或每年用于审核、定期活动和会议等。

安全转换 WildFire 配置文件为最佳实践

以下指南有助于定义 WildFire 分析配置文件的初始配置。

Palo Alto Networks 下一代防火墙包括基本 WildFire 服务，不需要高级 WildFire（或有效的旧版 WildFire）订阅。基本服务使防火墙能够转发 PE 文件进行分析，并仅通过每 24-48 小时更新一次防病毒和/或威胁防护来检索高级 WildFire 签名。高级 WildFire 订阅（PAN-OS 10.0 或更高版本）或旧版 WildFire 订阅包含更多功能，例如实时接收更新、支持更多文件类型和 API。

为了识别和防止威胁，防火墙必须能够了解应用程序流量。在当地法规、业务考虑、隐私考虑和技术能力允许的情况下解密尽可能多的流量。如果您不解密流量，防火墙将无法分析加密的标头和有效负载信息。

WildFire 签名生成非常准确，误报也很少。部署默认 WildFire 分析配置文件（这是最佳实践配置文件）不会影响网络流量。（但是，如果流量生成的 WildFire 签名会导致重置或丢弃操作，那么防病毒软件配置文件内的 WildFire 操作设置可能会影响该流量。

如果有初始配置文件，请监控 WildFire 提交日志（**Monitor**（监控）> **Logs**（日志）> **WildFire Submissions**（**WildFire** 提交））足够长的时间，以便确信您已了解是否有任何业务关键型应用程序因防病毒配置文件 WildFire 操作而导致产生警报或阻止。根据需要在防病毒配置文件中创建例外（必要时开立支持票据）以修复任何确认的误报。

安全转换 URL 筛选配置文件为最佳实践

在定义初始 URL 过滤配置文件并开始过渡到最佳实践配置文件时，以下指南有助于确定是从屏蔽操作还是警报操作开始。将 URL 筛选文件应用于 Internet 流量（不要将 URL 筛选配置文件应用于内部流量）。

您必须启用解密才能利用 *URL* 过滤，因为您必须解密流量以显示确切的 *URL*，以便防火墙可以采取适当的操作。至少解密高风险和中等风险流量。

高级 URL 过滤需要订阅。

- 预定义的 URL 类别是准确的，因此根据允许或拒绝访问不同类型的站点的公司策略，可以利用配置的类别操作安全地实施 URL 筛选配置文件。
- 从一开始就屏蔽已知错误的 URL 类别的网站访问和用户凭证提交，包括：恶意软件、命令和控制、版权侵权、极端主义、网络钓鱼、勒索软件、动态 dns、黑客攻击（但内部的 PEN 测试人员除外）以及代理避开和匿名器。
- 对于未知（尚未识别站点 PAN-DB）、已寄放的（通常用于凭据网络钓鱼）URL 类别、灰色软件（恶意或存疑），以及新注册的域名（通常用于恶意活动），先要提醒，以便在迁移到阻止这些类别的最佳实践之前，如果合法网站触发警报，则可以监控 URL 筛选日志（**Monitor**（监视）> **Logs**（日志）> **URL Filtering**（**URL** 筛选））。
- 将所有其他 URL 类别设置为 **alert**（警报）以生成流量日志。当访问设置为 **allow**（允许）时，防火墙不会记录流量。监视 URL 过滤日志，看看是否要屏蔽任何其他类别。

  您可以将高风险、中等风险和低风险类别与其他类别结合起来，以确定允许、屏蔽和解密哪些流量。例如，您可以屏蔽所有既有高风险又有金融服务的网站的访问权限。或者，如果您的防火墙需要节省资源，则可以解密某些类别的所有高风险和中等风险流量，而不是解密这些类别的低风险流量。

如果您有初始配置文件，请监控 URL 筛选日志足够长的时间，以便确信您已了解在从警报过渡到阻止以及过度到最佳实践 URL 筛选配置文件时，是否会阻止任何关键业务站点。如果您认为指定 URL 未正确分类，可请求重新分类 URL，将 URL 放到正确的类别中。过渡到最佳实践档案的速度取决于您的业务、应用程序和舒适程度。

安全转换文件阻止配置文件为最佳实践

以下指南可帮助您在定义初始文件阻止配置文件并开始过渡到最佳实践配置文件时确定是否从阻止或警报操作开始。发出警报，而不是允许文件类型生成日志并获得流量可见性。

- 最佳实践文件阻止配置文件通常对于不同类型的应用程序是不同的，并且对于入站、出站和内部流量也可能不同。例如：
  - 如果内部应用程序依赖于最佳实践文件阻止配置文件建议阻止的文件类型传输，请为这些内部应用程序允许这些文件类型；dll 文件就是一个典型的例子。仅允许必要的内部应用程序而不是所有应用程序使用这些文件传输类型。
  - 对于基于 Internet 的流量，请采取更严格的方法，以防止攻击者传递恶意文件并缩小攻击范围。
  - 对于数据中心流量，则采取更严格的方法（除依赖于您将阻止的文件传输类型的内部应用程序外）以缩小攻击范围和保护最宝贵的资产。
  - 当您制定例外时，请遵循最小权限原则，并将例外仅应用于出于业务目的需要访问文件类型的应用程序和用户。
- 业务关键型应用程序 - 从针对所有文件类型的警报操作开始，并尽快转向最佳实践文件阻止配置文件。如果您已经设置了阻止控制措施，请复制它们并继续阻止您已经知道要阻止的流量。

- 对于非业务关键型应用程序，开始过渡到最佳实践文件阻止配置文件：
  - 入站和出站流量 - 将 **Action**（操作）设置为 **block**（阻止）7z、bat、chm、class、cpl、dll、dlp、hta、jar、ocx、pif、scr、torrent、vbe 和 wsf 文件。将 **Action**（操作）设置为针对所有其他文件发出 **alert**（警报）。
  - 内部流量 - 阻止 7z、bat、chm、class、cpl、dlp、hta、jar、ocx、pif、scr、torrent、vbe 和 wsf 文件（这与入站/出站配置文件相同，但它会对 .dll 文件发出警报，而不是阻止它们）。对所有其他文件发出警报。
  - 您可以为不需要用于商业目的的用户阻止以下所有文件类型：cab、exe、flash、msi、多级编码、PE、rar、tar、加密的 rar 和加密的 zip。

如有必要，请为 *IT* 团队和其他需要合法业务访问任何这些文件类型的人创建例外。如果您已阻止任何其他文件类型，请继续阻止它们。

只要您愿意，即可尽快过渡到最佳实践文件阻止配置文件。

微调配置文件规则，以便在您方便的情况下尽快发出警报并将其转换为阻止状态，特别是对于面向互联网和数据中心的流量。监控数据筛选日志（**Monitor**（监控）> **Logs**（日志）> **Data Filtering**（数据筛选）），在为特定文件类型配置阻止操作之前了解文件类型使用情况。当您了解关键业务应用程序和内部自定义应用程序需要哪些文件类型时，请过渡到最佳实践文件阻止配置，并根据需要进行修改以支持您的业务需求。

创建 Internet 网关最佳实践安全配置文件

大多数恶意软件都是通过合法应用程序或服务潜入网络。要安全地启用应用程序，您必须扫描所有允许的流量以查找威胁。将安全配置文件附加到允许流量的所有安全策略规则，以便可以检测网络流量中的威胁（已知和未知）。以下最佳实践建议主要针对最严格的安全性。将 URL 过滤配置文件附加到允许 Internet 绑定流量的所有规则，并将其他配置文件附加到所有允许规则。

超过 90% 的网络流量是加密的。启用解密以了解流量，使用安全配置文件检查有效负载，并防止恶意事件。

请考虑将最佳做法安全配置文件添加到默认安全配置文件组。将安全配置文件组命名为默认值时，防火墙会自动将其附加到您创建的每个新安全策略规则，并确保防火墙检查流量是否存在恶意活动。

此外，请考虑为不同类型的流量创建专用的安全配置文件组。安全配置文件组使将所有必要的配置文件应用于安全策略规则变得容易，并确保不会忘记任何关键配置文件。

- 最佳实践 Internet 网关文件阻止配置文件
- 最佳实践 Internet 网关文件防病毒文件
- 最佳实践 Internet 网关漏洞保护配置文件
- 最佳实践 Internet 网关防间谍配置文件
- 最佳实践 Internet 网关 URL 筛选配置文件
- 最佳实践 Internet 网关 WildFire 分析配置文件

最佳实践 Internet 网关文件阻止配置文件

使用预定义的 **strict file blocking**（严格文件阻止）配置文件阻止恶意软件攻击活动中通常包含的文件，以及不属于上传/下载的真实用例的文件。阻止这些文件类型可减少攻击面。预定义的严格配置文件会阻止批处理文件、DLL、Java 类文件、帮助文件、Windows 快捷方式 (.lnk)、BitTorrent 文件、压缩文件、tar 文件、解密的压缩文件、多级编码文件（加密或压缩多达四次的文件）、hta 文件和 Windows Portable Executable (PE) 文件（包括 .exe、cpl、dll、ocx、sys、scr、drv、efi、fon 和.pif 文件）。最后，预定义的严格配置文件警示所有其他类型的文件传输，让您了解其他文件传输会发生什么，以便您确定是否需要修改策略。

某些情况下，支持关键型应用程序的需求可能会妨碍您阻止所有类型的严格配置文件。按照安全转换文件阻止配置文件为最佳实践的建议，帮助确定是否需要在网络的不同区域设置例外。审查数据筛选日志（***Monitor***（监视） > ***Logs***（日志） > ***Data Filtering***（数据筛选））以识别文件类型，并与企业利益相关者交流，了解他们的应用程序对文件类型的要求。基于此信息，克隆严格配置文件并视需要修改此文件，以允许仅一种您需要用于支持关键型应用程序的其他文件类型。还可使用方向 ***(Direction)*** 设置来限制文件类型双向流动，或阻止一个方向的文件。

NAME	LOCATION	RULE NAME	APPLICATIONS	FILE TYPES	DIRECTION	ACTION
basic file blocking	Predefined	Block high risk file types	any	7z, bat, chm, class, cpl, dll, exe, hlp, hta, jar, ocx, PE, pif, rar, scr, torrent, vbe, wsf	both	block
		Continue prompt encrypted files	any	encrypted-rar, encrypted-zip	both	continue
		Log all other file types	any	any	both	alert
strict file blocking	Predefined	Block all risky file types	any	7z, bat, cab, chm, class, cpl, dll, exe, flash, hlp, hta, jar, msi, Multi-Level-Encoding, ocx, PE, pif, rar, scr, tar, torrent, vbe, wsf	both	block
		Block encrypted files	any	encrypted-rar, encrypted-zip	both	block
		Log all other file types	any	any	both	alert

您可能还需要一些通常用于恶意目的的协议，以便进行 Windows 更新等活动。严格文件阻止配置文件阻止 .exe、.dll、.pe 和 .cab 文件。要设置例外以允许特定活动（如 Windows 更新）的协议，请执行以下操作：

1. 创建特定的安全策略规则，该规则仅允许使用要阻止其他流量的协议的所需用户和业务应用程序。
2. 克隆严格的文件阻止配置文件，对其进行修改以允许所需的协议，然后将其附加到规则。
3. 将规则放在具有文件阻止配置文件的安全策略规则之上，该配置文件阻止所有其他流量的协议。

此方法使您能够以安全的方式使用潜在的恶意文件类型，从而在阻止恶意流量的同时启用业务应用程序。微调配置文件和规则库以允许任何所需的例外情况。

我为什么需要该配置文件？

攻击者可以通过多种方式传递恶意文件：

- 公司或个人电子邮件中的附件或链接。
- 社交媒体和其他来源中的链接或即时消息。
- 漏洞利用工具包
- 文件共享应用程序（如 FTP、Google 云端硬盘或 Dropbox）。
- U 盘。
-

附加严格文件阻止配置文件可防止这些类型的攻击并减少攻击面。

如果选择不阻止所有 PE 文件，则发送所有未知文件到 WildFire 进行分析。另外，设置“操作”以 **continue**（继续）以阻止偷渡式下载，这是指最终用户在没有意识到的情况下下载安装有恶意文件（如 Java 小程序或执行文件）的内容。最终用户访问误导性网站，查看电子邮件信息，或点击弹出式窗口时，都有可能发生偷渡式下载。告诉用户，如果他们被提示继续进行不是他们有意识发起的文件传输，就可能会下载恶意文件。此外，如果必须允许可能带有威胁的文件类型，请使用文件阻止和 URL 筛选来限制用户可以传输文件的类别，以减少攻击面。

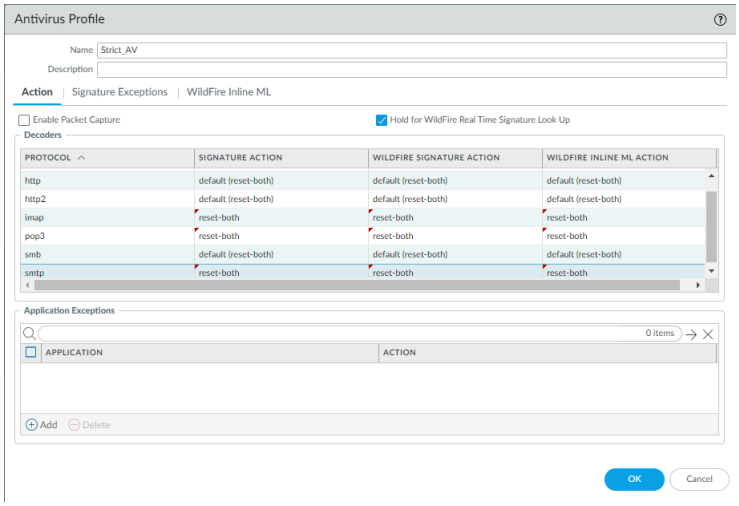
最佳实践 Internet 网关文件防病毒文件

要确保业务关键型应用程序的可用性，从当前状态转移到最佳实践配置文件时，请遵循安全转换防病毒配置文件为最佳实践的建议。目标是转换为配置文件，如下所示，并将其附加到允许流量的所有安全策略规则。防病毒配置文件包含协议解码器，该解码器会检测并预防病毒和恶意软件通过以下七种协议传输：FTP、HTTP、HTTP2、IMAP、POP3、SMB 和 SMTP。

为所有七种协议设置 WildFire 签名和 WildFire 内联 ML 操作（防病毒配置文件还根据 WildFire 签名强制执行操作），如果尚未执行此操作，请启用实时特征码查找，如安全转换防病毒配置文件为最佳实践 所示。

配置克隆的防病毒配置文件以重置所有七个协议解码器和 WildFire 操作的客户端和服务器，然后将配置文件附加到安全策略允许规则。

如果将内部应用程序与外部应用程序区别对待，则可能需要针对面向 *Internet* 的流量使用防病毒配置文件，为内部流量使用不同的防病毒配置文件。



在全局和防病毒配置文件中启用实时签名查找以保留文件，直到防火墙从云收到最新的实时防病毒签名：

- 全局启用：**Device**（设备）> **Setup**（设置）> **Content-ID** > **Content-ID Settings**（**Content-ID** 设置）> **Realtime Signature Lookup**（实时签名查找），启用 **Hold for WildFire Real Time Signature Look Up**（为 **WildFire** 实时签名查找保留），并将 **Action on Real Time Siganture Timeout**（实时签名超时后的操作）设置为 **Reset Both**（重置二者）。您必须全局启用实时签名查找才能在防病毒配置文件中启用它。
- 在防病毒配置文件中启用 **Hold for WildFire Real Time Signature Lookup**（为 **WildFire** 实时签名查找保留）。保留文件以确保 WildFire 获得最新的防病毒签名，从而保护您免受零日恶意软件和过时的防病毒签名的侵害，如果您转发文件而不保留文件以获取最新签名，则可能会暴露给这些恶意软件和过时的防病毒签名。

我为什么需要该配置文件？

通过为所有安全规则附加防病毒配置文件，您可以在所有已知恶意文件（恶意软件，勒索机器人程序和病毒）进入网络时阻止它们。通常用户收到恶意文件的途径包括电子邮件附件中的恶意附件，定向到恶意文件的链接，或渗透代码工具包的静态攻击，找到漏洞，然后自动下载恶意负载到最终用户设备的服务。

最佳实践 Internet 网关漏洞保护配置文件

为所有允许的流量附加漏洞保护配置文件，防止缓冲区溢出，不合法的代码执行，以及其他试图探测客户端和服务器端漏洞的行为。要确保业务关键型应用程序的可用性，请按照安全转换漏洞保护配置文件为最佳实践的建议从当前状态转移到最佳实践配置文件。克隆预定义的严格漏洞防护配置文件并对其进行编辑以创建最佳实践配置文件：

- 将三个暴力破解规则中的 **Action**（操作）更改为 **reset-both**（重置两者），将 **Packet Capture**（数据包捕获）更改为 **single-packet**（单一数据包），以便从暴力攻击事件警报转换为阻止它们。
- 将服务器和客户端的关键、高和中等严重性事件整合到一个规则中。将 **Action**（操作）设置为 **reset-both**（重置两者），并将 **Packet Capture**（数据包捕获）设置为 **single-packet**（单一数据包）。这简化了配置文件且会起作用，因为配置文件对这些严重性使用相同的操作和相同的数据包捕获设置。

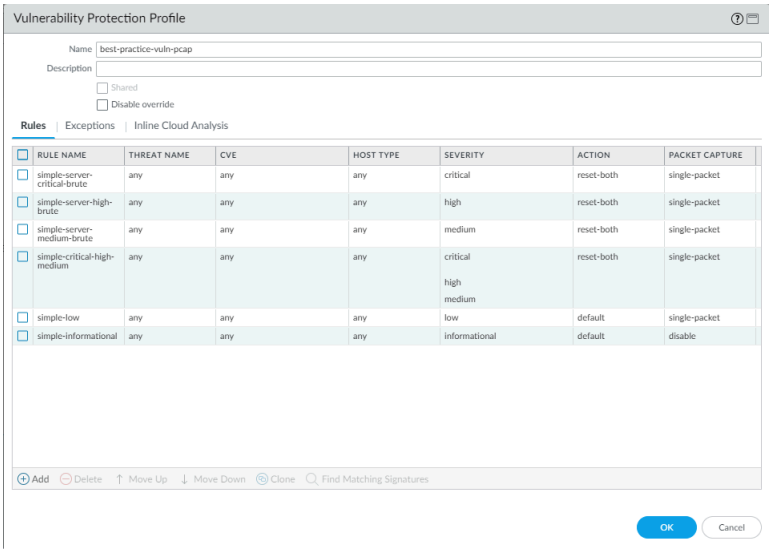
  对于控制内部（东西向）流量的配置文件，阻止中等严重性事件可能会影响业务应用程序。如果阻止影响业务应用程序，请在配置文件中为中等严重性事件创建单独的规则，并将 ***Action***（操作）设置为 ***alert***（警报）。仅将配置文件应用于内部流量。
- 要简化配置文件，请将服务器和客户端的低严重性事件合并到一个规则中。将 **Action**（操作）设置为 **default**（默认值），并将 **Packet Capture**（数据包捕获）设置为 **single-packet**（单一数据包）。
- 将服务器和客户端的信息事件合并到一个规则中。将 **Action**（操作）设置为 **default**（默认值），并将 **Packet Capture**（数据包捕获）设置为 **disable**（禁用）。

  信息事件的 PCAP 生成相对较高的流量，与有关潜在威胁的捕获相比，这些流量通常没有用。
- 将扩展的 PCAP（而不是单一 PCAP）应用到您应用**alert**（警报）操作的高价值流量。使用用于确定要记录的流量的相同逻辑应用 PCAP，并获取所记录流量的 PCAP。将单一 PCAP 应用到您阻止的流量。超出 PCAP 记录且发送到管理平面的默认数据包数量为 5 个，这也是推荐值。在大多数情况下，捕获五个数据包可提供足够的信息来分析威胁。如果将太多 PCAP 流量发送至管理平面，捕获的数据包数量超过五个时，将导致 PCAP 被丢弃。

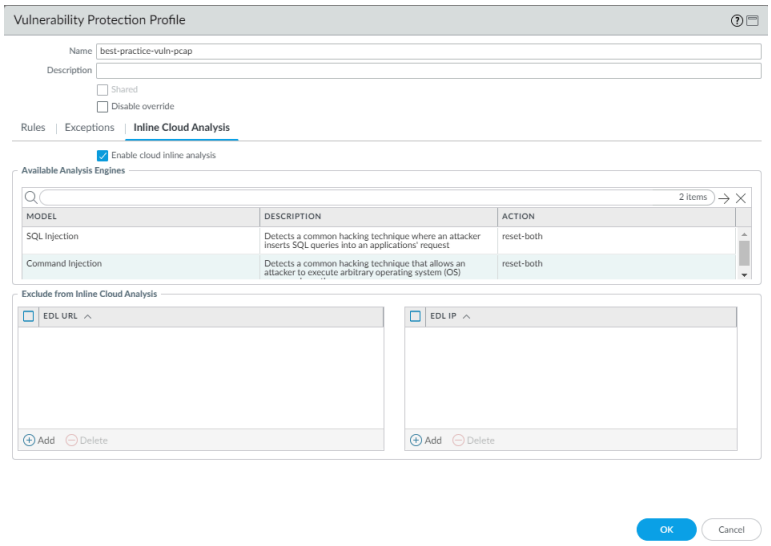
如果您希望更精细地微调配置文件，请使用 ***Action***（操作）和 ***Packet Capture***（数据包捕获）设置单独的规则，如前所述。例如，为服务器创建严重、高和中等严重性规则，为客户端创建另一个类似规则，或者为客户端和服务器的每个严重性创建单独的规则，以实现所需的粒度和控制级别。

数据包捕获会消耗管理平面资源。检查系统资源（例如，***Dashboard***（仪表板） > ***System Resources***（系统资源））以了解实施数据包捕获之前和之后的使用情况，从而确保系统有足够的资源来捕获所需的数据包。

为每个规则启用数据包捕获 (PCAP)，以便跟踪潜在攻击的来源。自动下载并尽快安装内容更新，以便保持签名集始终处于最新状态。



对于 **Inline Cloud Analysis**（内联云分析），将 **Action**（操作）设置为 **reset-both**（重置两者），以便阻止常见黑客技术。



我为什么需要该配置文件？

如果没有严格的漏洞保护，攻击者就可以利用客户端和服务器端的漏洞，攻陷终端用户。例如，攻击者可以利用漏洞在客户端系统上安装恶意代码，或使用漏洞利用工具包自动向最终用户传递恶意负载。漏洞防护配置文件可防止攻击者利用内部主机上的漏洞在网络中横向移动。

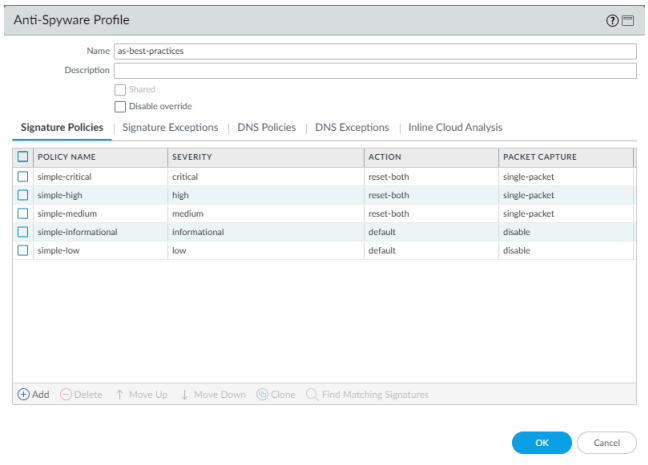
最佳实践 Internet 网关防间谍配置文件

为所有允许的流量附加防间谍配置文件，检测命令，控制由服务器或端点上运行的恶意代码发起的流量 (C2)，防止受影响的系统与您的网络建立导出连接。克隆并编辑预定义的严格防间谍软件配置文件。为确保业务关键型应用程序的可用性，请将反间谍软件配置文件安全地过渡到最佳实践。编辑配置文件以启用 DNS Sinkhole 和数据包捕获 (PCAP)，帮助您跟踪试图解析恶意域名的端点。

保留默认 **Action**（操作），以便在防火墙检测到中等、高度或严重严重性威胁时重置连接，并为这些威胁启用单个 PCAP。

仅允许流量流向批准的 *DNS* 服务器。使用 DNS 安全服务阻止恶意 *DNS* 服务器连接。

如果将内部应用程序与外部应用程序区别对待，则可能需要针对面向 *Internet* 的流量使用反间谍软件配置文件，对内部通信使用不同的反间谍软件配置文件。



请勿为信息活动启用 PCAP，因为这将产生相对较高的流量，对于潜在威胁而言，它所起的作用不如 PCAP。将扩展的 PCAP（而不是单一 PCAP）应用到您应用**alert**（警报）操作的高价值流量。使用用于确定要记录的流量的相同逻辑应用 PCAP，并获取所记录流量的 PCAP。将单一 PCAP 应用到您阻止的流量。超出 PCAP 记录且发送到管理平面的默认数据包数量为 5 个，这也是推荐值。在大多数情况下，捕获五个数据包可提供足够的信息来分析威胁。如果将太多 PCAP 流量发送至管理平面，捕获的数据包数量超过五个时，将导致 PCAP 被丢弃。

数据包捕获会消耗管理平面资源。检查系统资源（例如，***Dashboard***（仪表板） > ***System Resources***（系统资源））以了解实施数据包捕获之前和之后的使用情况，从而确保系统有足够的资源来捕获所需的所有数据包。

配置 DNS 策略，以防止网络遭到 DNS 查询和恶意域攻击等。为了获得最佳安全性，请使用 DNS 安全服务来保护 DNS 流量。否则，请使用本地可用的可下载 DNS 签名集（与防病毒和 WildFire 更新一起打包）。

Sinkhole 恶意流量而不是阻止它，以通过跟踪主机并阻止它们访问可疑域来识别尝试访问可疑域的潜在受损主机。对于构成更大威胁的域类别，请配置更高的日志严重性级别和/或数据包捕获设置，以帮助确定攻击是否成功、识别攻击方法并提供更好的整体上下文。

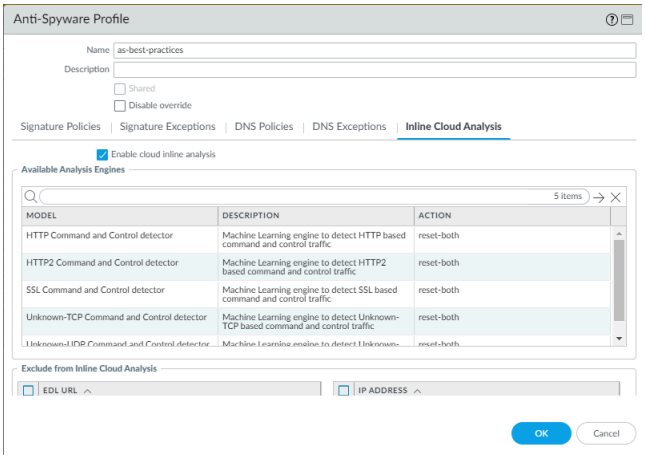
配置默认的Palo Alto NetworksDNS 和各个 DNS 签名源类别（PAN-OS 10.0 及更高版本）：

DNS 签名源	日志严重性	策略操作	数据包捕获
Palo Alto Networks 内容			

DNS 签名源	日志严重性	策略操作	数据包捕获
default-paloalto-dns	默认	Sinkhole	extended-capture
DNS 安全			
命令和控制域	高（默认）	Sinkhole	extended-capture
动态 DNS 托管域	参考（默认）	Sinkhole	单一数据包
灰色软件域	低（默认）	Sinkhole	单一数据包
恶意软件域	中（默认）	Sinkhole	单一数据包
寄放域	参考（默认）	Sinkhole	禁用（默认）
网络钓鱼域	低（默认）	Sinkhole	单一数据包
代理避免和匿名者	低（默认）	Sinkhole	单一数据包
新注册域名	参考（默认）	Sinkhole	单一数据包
广告跟踪域	参考（默认）	Sinkhole	单一数据包

对于 **Inline Cloud Analysis**（内联云分析）（需要高级威胁防护订阅），请对所有出站流量 **Enable cloud inline analysis**（启用云内联分析）。为所有模型将 **Action**（操作）设置为 **reset-both**（重置两者）。

气隙环境无法使用高级威胁防护，因为它是云服务，需要云连接。



最佳实践 Internet 网关 URL 筛选配置文件

使用高级 URL 过滤来防止恶意活动访问高风险的 Web 内容。对允许访问基于 Web 的应用程序的所有规则附加 URL 筛选配置文件，从而防范 Palo Alto Networks 已观察到具有恶意软件、潜在恶意软件、责任风险或漏洞利用内容的 URL。

您必须启用解密才能利用 *URL* 过滤，因为您必须解密流量以显示确切的 *URL*，以便防火墙可以采取适当的操作。至少解密高风险和中等风险流量。

为确保业务关键型应用程序的可用性，安全转换 URL 筛选配置文件为最佳实践。最佳做法 URL 筛选配置文件将所有已知的危险 URL 类别和凭据提交设置为阻止。目标是阻止以下类别：

- 设置恶意 URL 类别的所有操作，以阻止站点访问和用户凭据提交。根据需要为 PEN 测试、威胁研究和信息安全设置适当的例外情况：
  - **command-and-control**（命令和控制） - 恶意软件或受感染系统用于与攻击者的远程服务器通信的 URL 和域。
  - **grayware**（灰色软件）- 这些站点不符合病毒的定义或构成直接安全威胁，但它们会影响用户授予远程访问权或执行其他未经授权的操作。灰色软件网站包括诈骗、非法活动、犯罪活动、广告软件以及其他不需要的和未经请求的应用程序，包括“域名仿冒”域名。
  - **Malware**（恶意软件） - 已知具有恶意软件或用于命令和控制活动的站点。
  - **phishing**（网络钓鱼） - 已知托管凭据和个人信息网上诱骗页面（包括技术支持诈骗和恐吓软件）的网站。
  - **ransomware**（勒索软件） - 已知会分发勒索软件的网站。
  - **scanning-activity**（扫描活动） - 探测现有漏洞或进行针对性攻击的站点。

- 某些 URL 类别具有很强的恶意潜力，但并非绝对是恶意的。设置这些 URL 类别的所有操作以阻止站点访问和用户凭据提交。根据需要为 PEN 测试、威胁研究和信息安全设置适当的例外情况：
  - **dynamic-dns**（动态 **DNS**） - 具有动态分配的 IP 地址的系统，通常用于传递恶意软件有效负载或命令和控制恶意软件。

    如果您的动态 *DNS* 域名用于业务目的，请确保在 *URL* 筛选配置文件中将这些 *URL* 列入允许列表。
  - **hacking**（黑客攻击） - 与非法或可疑地访问或使用设备和软件相关的网站。包括有助于绕过许可和数字版权系统的网站。

    为相应的 *PEN* 测试和威胁研究用户设置此类别的例外情况。
  - **insufficient-content**（内容不足） - 提供测试页面、无内容、提供不用于最终用户显示的 API 访问权限或要求在不显示任何其他内容的情况下进行身份验证的网站和服务。
  - **newly-registered-domains**（新注册的域） - 域生成算法经常生成的域或恶意行为者生成的域。
  - **not-resolved**（未解析） - 如果无法访问 PAN-DB 云，并且 URL 不在防火墙的 URL 筛选缓存中，则防火墙无法解析和识别 URL 类别。

    为了获得最高安全性，请启用 ***Hold client request for category lookup***（为类别查找保留客户端请求），以便防火墙有更多时间来解析 *URL* 类别。这延长了防火墙从云查询类别类型的时间，从而提高了安全性，但可能会增加延迟。
  - **parked**（已寄放） - 经常用于凭据网络钓鱼或个人信息盗窃的域。
  - **Proxy-avoidance-and-anonymizers**（回避代理和匿名者可疑的） - 常用来绕开内容筛选产品的 URL 和服务。
  - **unknown**（未知） - Palo Alto Networks (PAN-DB) 尚未识别的站点。

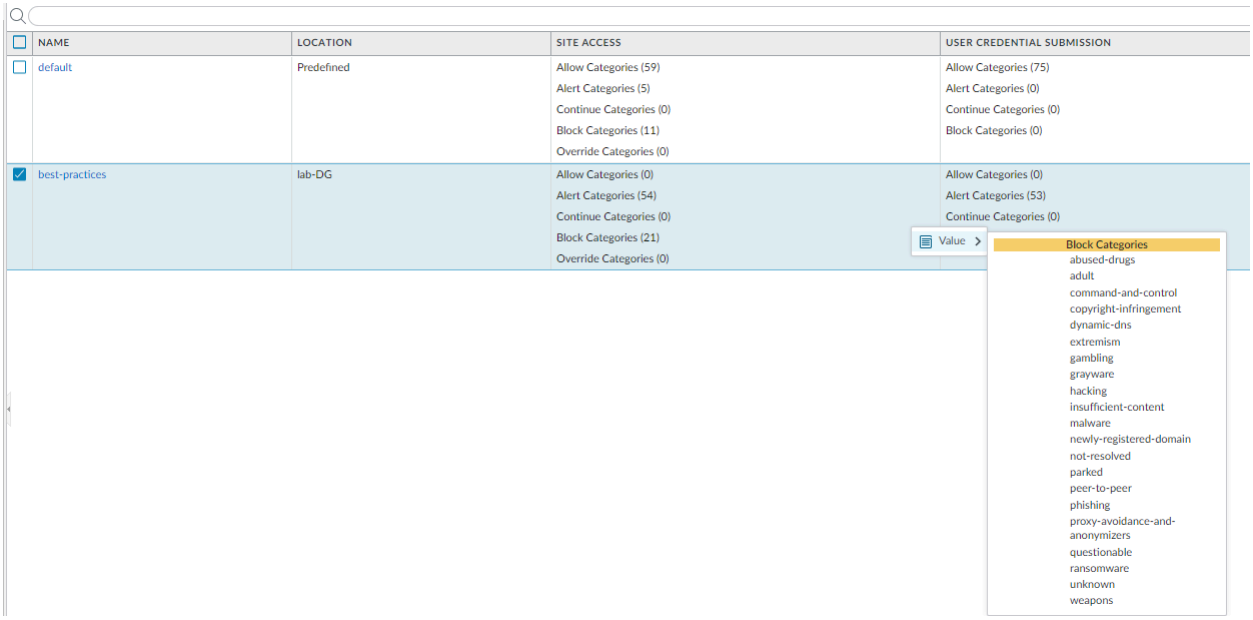
    PAN-DB 实时更新在首次尝试访问未知站点后会学习未知站点，因此防火墙可以快速识别未知 *URL*，然后根据站点的实际 *URL* 类别进行处理。

    如果可用性对您的业务至关重要，您必须允许来自未知站点的流量，请对流量应用最严格的安全配置文件并对流量的所有警报进行调查。

- 设置“站点访问”和“用户凭据提交”操作，以根据法律或业务要求以及潜在的责任风险阻止以下 URL 类别。如果不阻止这些站点，请发出警报并对流量应用严格的安全配置文件。
  - **abused-drugs**（滥用药物）- 宣传非法和合法药物滥用的网站。
  - **adult**（成人）- 包含任何类型的成人内容（包括游戏和漫画以及露骨色情材料、媒体、艺术、论坛和服务）的所有网站。
  - **copyright-infringement**（侵犯版权）- 包含非法内容且存在责任风险的域名。
  - **extremism**（极端主义）- 宣扬恐怖主义、种族主义、剥削儿童内容等的网站。
  - **gambling**（赌博）- 彩票和赌博网站。
  - **peer-to-peer**（点对点）- 种子、下载程序、媒体文件或其他软件应用程序的点对点共享。（不包括共享软件或免费软件网站。
  - **questionable**（可疑）- 宣传无味幽默、针对特定受众特征的冒犯性内容的网站。
  - **weapons**（武器）- 出售、审查、描述或说明武器及其使用。

  还要考虑如何处理加密货币和烟酒 URL 类别。根据业务需求，对它们发出警报并将严格的安全配置文件应用于流量或阻止它们。
- 阻止高风险类别的用户凭据提交。（不要阻止高风险类别的站点访问。）

除阻止已知的恶意类别外，还要警告其他所有类别，以便监控用户访问的站点。如果您需要分阶段实施阻止策略，请设置类别以继续，并创建自定义响应页面，告知客户可接受的使用策略，并警告他们正在访问的站点可能有威胁。这样，您就可以在监控期结束后顺利地阻止该类别。



在配置文件中禁用 **Log Container Page Only**（仅日志容器页面），该页面默认情况下处于启用状态。如果仅记录容器页面，则会失去对功能应用程序的可见性，例如发布、上传、下载等。禁用 **Log Container Page Only**（仅日志容器页面）以查看完整日志，以便您看到真正的功能应用程序。

如果您的环境是接受联邦资助的学校，请启用 **Safe Search Enforcement**（安全搜索强制要求）（法律要求）。

如果运行的是 PAN-OS 9.0.4 或更高版本，请启用保留客户端请求的选项（输入 **config**，然后输入 **set deviceconfig setting ctd hold-client-request yes**），从而确保让防火墙尽可能安全地处理用户 Web 请求。默认情况下，当防火墙在 PAN-DB 中查找未缓存的 URL 类别时，它会允许请求，然后在服务器响应时强制执行适当的策略。在此查找期间保留请求以最大程度地提高安全性（这可能会增加延迟，但是最安全的选项）。有关详细信息，请参阅配置 URL 筛选。

如果我不能阻止所有的建议类别，怎么办？

如果用户出于业务目的需要访问阻止类别中的站点，请在规则中仅为特定站点创建允许列表，该规则仅允许必要的用户和应用程序（如果您认为风险是合理的）。请了解当地规定您可以屏蔽、不能屏蔽和必须屏蔽的网站类型的法律法规。在决定允许访问的风险类别上，请设置凭据网络钓鱼防护，以确保用户不会向可能托管网络钓鱼攻击的站点提交公司凭据。

如果您允许流量流向恶意和潜在恶意 URL 类别或存在潜在责任问题的网站，则风险包括：

- 恶意 URL 类别
  - **Command-and-control**（命令和控制） - - 恶意软件和/或受影响的系统使用命令和控制 URL 及域名与攻击者的远程服务器暗中交流，以接收恶意软件指令或泄露数据。
  - **grayware**（灰色软件） - 不符合病毒定义、但有恶意或可疑且可能会降低设备性能和导致安全风险的网站和服务。在内容发布版本 8206 之前，防火墙将灰色软件列入到恶意软件或可疑 URL 类别中。如果您不确定是否阻止灰色软件，请先发出灰色软件警报，然后调查警报，最后决定是阻止灰色软件还是继续发出灰色软件警报。
  - **malware**（恶意软件） - 已知托管恶意软件或用于命令和控制 (C2) 流量且可能显示漏洞利用工具包的站点。
  - **Phishing**（钓鱼） - 已知有认证钓鱼页面，或钓鱼获取个人身份信息。
  - **ransomware**（勒索软件） - 已知会分发勒索软件的网站。
  - **scanning-activity**（扫描活动） - 探测现有漏洞或进行针对性攻击的站点。

- 潜在恶意网址类别：
  - **Dynamic-dns**（动态 **DNS**） - 动态指定 IP 地址的系统主机和域名，常常被用来传送恶意负荷或 C2 流量。而且动态 DNS 域名不会像由信誉良好的域名注册公司注册的域名那样通过审批流程，因此也不那么值得信赖。
  - **hacking**（黑客攻击） - 与非法或可疑地访问或使用设备和软件相关的网站。包括有助于绕过许可和数字版权系统的网站。

    为相应的 *PEN* 测试和威胁研究用户设置此类别的例外情况。

  - **insufficient-content**（内容不足） - 提供测试页面、无内容、提供不用于最终用户显示的 API 访问权限或要求在不显示任何其他内容的情况下进行身份验证的网站和服务。
  - **Newly-registered-domains**（新注册域） - 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。
  - **not-resolved**（未解析） - 如果无法访问 PAN-DB 云，并且 URL 不在防火墙的 URL 筛选缓存中，则防火墙无法解析和识别 URL 类别。

    为了获得最高安全性，请启用 ***Hold client request for category lookup***（为类别查找保留客户端请求），以便防火墙有更多时间来解析 *URL* 类别。这延长了防火墙从云查询类别类型的时间，从而提高了安全性，但可能会增加延迟。

  - **Parked**（寄放的） - 由个人注册的域名，后来常常会发现用作认证钓鱼。这些域名可能与合法域名很相似，如 pal0alto0netw0rks.com，就会试图钓鱼获取认证或个人身份信息。或者可能是个人购买，希望有一天会有价值的域名，如 panw.net。
  - **Proxy-avoidance-and-anonymizers**（回避代理和匿名者可疑的） - 常用来绕开内容筛选产品的 URL 和服务。
  - **Unknown**（未知） - PAN-DB 尚未标识的站点。如果可用性对您的业务至关重要，您必须允许流量、对未知站点发出警报、针对流量应用最佳实践安全配置文件，并对警报进行调查。

    PAN-DB 实时更新可在首次尝试访问未知站点后了解该未知站点，这样，就可快速标识未知 *URL*，并将未知 *URL* 变为已知 *URL*，以便防火墙在以后可根据实际的 *URL* 类别对其进行处理。

- 具有潜在责任风险的网址类别：
  - **abused-drugs**（滥用药物） - 宣传滥用合法和非法药物、销售和使用吸毒用具以及制造或销售毒品的网站。
  - **adult**（成人） - 可能不适合工作场所的网站。
  - **copyright-infringement(**版权侵权**)** - 具有非法内容的域名，例如允许非法下载可带来潜在责任风险的软件或其他知识产权的内容。介绍此类别以遵守教育领域要求的儿童保护法，及要求 Internet 提供商预防用户通过其服务共享受版权保护的资料的国家的法律。
  - **extremism**（极端主义） - 宣扬恐怖主义、种族主义、法西斯主义或歧视不同种族背景、宗教或其他信仰的个人或群体的其他极端主义观点。介绍此类别旨在遵守教育行业要求的儿童保

护法。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。

- **gambling**（赌博）- 促进真实和/或虚拟货币交换的彩票或赌博网站。还包括提供有关赌博的教程、建议或其他信息的网站，包括投注赔率和彩池。
- **peer-to-peer**（点对点）- 客户端访问或访问种子、下载程序、媒体文件或其他软件应用程序的点对点共享的网站，主要用于防止 bitTorrent 下载功能。不包括共享软件或免费软件站点。
- **questionable**（可疑）- 包含针对个人或团体的特定人口统计数据、犯罪活动、非法活动和快速致富计划的潜在冒犯性内容的网站。
- **weapons**（武器）- 销售、评论、描述或提供有关武器及其使用说明的网站，这些网站可能不适合工作场所。

默认 *URL* 过滤配置文件会阻止恶意软件、网络钓鱼和命令和控制 *URL* 类别，但不会阻止建议阻止的其他类别。此外，默认 *URL* 筛选配置文件还可以阻止滥用药物、成人、赌博、可疑的和武器类 *URL* 类别。是否阻止这些 *URL* 类别取决于您的业务要求。例如，大学可能不会限制学生访问大多数此类网站，因为可用性很重要，但重视安全性的企业可能会阻止全部网站。

URL 筛选示例

URL 筛选与文件阻止、解密、外部动态列表 (EDL)、日志记录和其他安全功能配合使用，可创建比简单阻止或允许整个 URL 类别更严格的精细策略。按照 URL 筛选安全转换步骤评估要允许和要阻止的站点，然后实施符合业务需求的策略。例如：

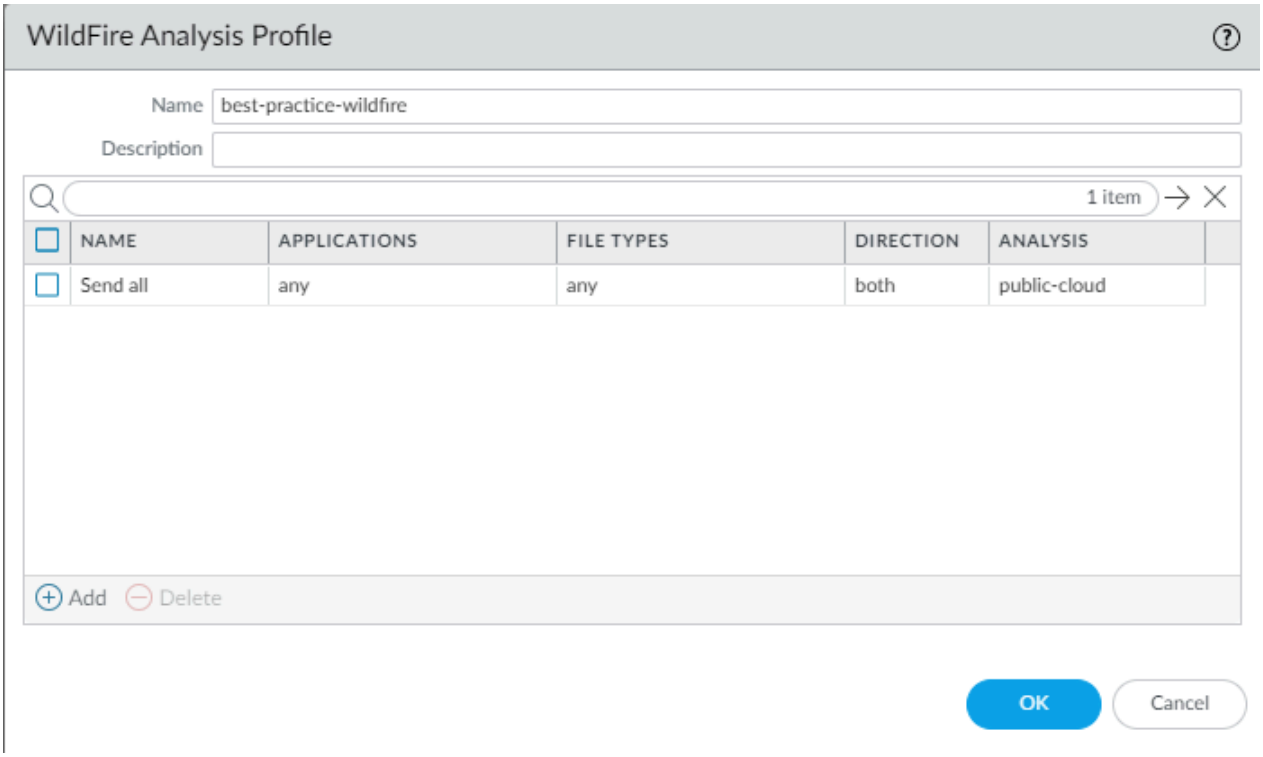
- 将基于风险的 URL 类别（高风险、中等风险和低风险）与其他 URL 类别结合使用，以定向解密或定位阻止流量。例如，您可以：
  - 阻止流向金融服务类别中高风险网站的流量。
  - 解密所有高风险和中风险 Web 流量。
  - 如果防火墙没有足够的资源来解密要解密的所有流量，请将高风险和中等风险流量解密到特定 URL 类别。
- 记录高风险和中等风险类别域的所有用户代理和引用网站、所有 URL 和所有文件下载，以提高可见性。
- 允许访问个人网站和博客等类别，同时将文件阻止配置文件应用于流量，以防止下载有风险的内容，如 .exe、.scr 和其他潜在恶意文件。
- 使用预定义的 **Palo Alto Networks - Bulletproof IP addresses**（**Palo Alto Networks -** 防护 **IP** 地址）EDL 来防止访问 Bulletproof ISP 上托管的站点，尤其是在您允许访问高风险或中等风险金融站点的情况下。
- 使用 URL 类别组合来简化策略。

最佳实践 Internet 网关 WildFire 分析配置文件

将文件转发到 WildFire 进行分析，以保护您的网络免受未知威胁。没有这一层保护，攻击者就会渗入您的网络，攻击您的雇员每天使用的应用程序中的漏洞。WildFire 防护未知威胁，所以是您用来抵御高持续性威胁 (APT) 的最佳防护。

设置 WildFire 设备内容更新以实时自动下载和安装，让您始终拥有最新的支持。

最佳实践 WildFire 分析配置文件将双向传输（上传和下载）的所有文件发送到 WildFire 进行分析。特别是，确保发送所有的 PE 文件（如果您没有根据文件阻止最佳实践将其阻止）、Adobe Flash 和 Reader 文件（PDF、SWF）、Microsoft Office 文件（PowerPoint，Excel，Word，RTF），Java 文件（Java、.CLASS）和 Android 文件 (.APK)。



通过电子邮件，SNMP 或系统日志服务器设置恶意软件警报，以便防火墙在遇到潜在问题时立即通知您。隔离受感染主机的速度越快，以前未知的恶意软件传播到其他数据中心设备的可能性就越低，修复问题就越容易。

必要时，可以根据流量方向限制发送用于分析的应用程序和文件类型。

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

定义初始 Internet 网关安全策略

最佳实践 Internet 网关安全策略的目标是积极利用允许的应用程序实施方法。但是，确定网络上运行的确切应用程序、哪些应用程序对您的业务至关重要，以及谁需要访问每个应用程序需要时间。要根据应用程序允许规则创建安全策略，请从一个规则库开始，该规则库允许用户使用您正式批准的应用程序，并允许使用一般业务应用程序和个人应用程序（如果适合您的业务）。

最初的策略包括明确阻止已知的恶意 IP 地址和应用程序的规则，以及临时允许规则，这些规则有助于在过渡到最佳实践策略时完善策略并保持应用程序可用性。

为了在多个位置应用一致的安全策略，您可以重复使用模板和模板栈，从而可以在每个位置的每个 *Internet* 网关防火墙应用相同的策略。模板使用变量来应用设备特定的值，例如 *IP* 地址、*FQDN* 等，同时维护全球安全策略并减少需要管理的模板和模板堆栈的数量。

以下主题介绍如何创建初始规则库，描述每条规则为何必要，并阐明忽略最佳实践建议的风险：

- 第 1 步：基于可信任的威胁情报源创建规则
- 第 2 步：创建应用程序允许规则
- 第 3 步：创建应用程序阻止规则
- 第 4 步：创建临时调整规则
- 第 5 步：启用日志，记录不匹配任何规则的流量

第 1 步：基于可信任的威胁情报源创建规则

屏蔽来自 Palo Alto Networks 和可信第三方来源已被证明是恶意的主机的流量。高级威胁防护许可证（或有效的传统威胁防护许可证）包括包含已知恶意 IP 地址的内置外部动态列表 (EDL)。在策略中使用 EDL 来阻止恶意流量。Palo Alto Networks 根据最新的威胁情报编译和动态更新列表。防火墙无需重启即可接收和实施动态更新。

STEP 1 | 阻止往来于 Palo Alto Networks 认定为恶意的 IP 地址的流量。

为什么需要这些规则？	规则亮点
❑ 该规则保护您免受已被 Palo Alto Networks 证明是专用于分发恶意软件、启动命令和控制活动以及启动攻击的 IP 地址的攻击。	• 一个规则阻止已知恶意 IP 地址的出站流量，而另一个规则阻止前往这些地址的入站流量。 • 将外部动态列表 **Palo Alto Networks - Known malicious IP addresses**（**Palo Alto Networks -** 已知恶意 **IP** 地址）设置为用于出站流量规则的目标地址，以及入站流量规则的源地址。 • 拒绝符合这些规则的流量。

为什么需要这些规则？	规则亮点
	• 启用日志，记录匹配这些规则的流量，便于您调查网络上的潜在威胁。 • 由于这些规则可以阻止恶意流量，因此它们可以保护流量免受在任何端口上运行的任何用户的攻击。

		Source				Destination							
NAME	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Drop Outbound Malicious IP	universal	any	any	any	any	any	Palo Alto Networks - Known malicio...	any	any	any	Deny	none	
Drop Inbound Malicious IP	universal	any	Palo Alto Networks - Known malic...	any	any	any	any	any	any	any	Deny	none	

STEP 2 | 阻止进出 Bulletproof 托管提供商的流量。

为什么需要这些规则？	规则亮点
❑ 该规则可防范 Palo Alto Networks 已证实属于 Bulletproof 托管提供商的 IP 地址。 Bulletproof 托管提供商对内容没有限制或限制有限，也不会记录事件。Bulletproof 站点是发起命令和控制 (C2) 攻击以及非法活动的理想场所，因为它毫无限制，也不会跟踪任何行为。	• 一个规则阻止已知 Bulletproof 托管 IP 地址的出站流量，另一个规则传输到这些地址的入站流量。 • 将外部动态列表 **Palo Alto Networks - Bulletproof IP addresses**（**Palo Alto Networks - Bulletproof IP** 地址）设置为出站流量规则的目标地址，以及入站流量规则的源地址。 • 拒绝符合这些规则的流量。 • 启用日志，记录匹配这些规则的流量，便于您调查网络上的潜在威胁。 • 由于这些规则可以阻止恶意流量，因此它们可以保护流量免受在任何端口上运行的任何用户的攻击。

		Source				Destination							
NAME	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Drop Outbound Bulletproof IP	universal	any	any	any	any	any	Palo Alto Networks - Bulletproof IP ...	any	any	any	Deny	none	
Drop Inbound Bulletproof IP	universal	any	Palo Alto Networks - Bulletproof I...	any	any	any	any	any	any	any	Deny	none	

STEP 3 | 屏蔽和记录来自可信威胁公告的高风险 IP 地址的流量。

为什么需要这些规则？	规则亮点
虽然 Palo Alto Networks 没有证据能直接证明高风险 IP 地址源中 IP 地址的恶意性，但威胁公告已将其与恶意行为相关联。 ❑ 屏蔽并记录流量，如本示例所示。 ❑ 如果您出于业务原因必须允许高风险 IP 地址，请创建具有严格安全配置文件的安全策略规则，该规则仅允许该 IP 地址，并将其置于规则库中高风险 IP 地址屏蔽规则的前面。密切监视并记录您选择允许的任何高风险 IP 地址。	• 一条规则记录阻止的高风险 IP 地址的出站流量，另一条规则记录阻止的前往这些地址的入站流量。 • 将外部动态列表 **Palo Alto Networks - High risk IP addresses**（**Palo Alto Networks -** 高风险 **IP** 地址）设置为用于出站流量规则的目标地址，以及入站流量规则的源地址。 • 如果允许流量，请应用最佳实践安全配置文件。 • 由于这些规则可以阻止恶意流量，因此它们可以保护流量免受在任何端口上运行的任何用户的侵害，适用于任何应用程序。

		Source				Destination							
NAME	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Block Outbound High Risk IPs	universal	any	any	any	any	any	Palo Alto Networks - High risk IP addresses	any	any	any	Deny	none	
Block Inbound High Risk IPs	universal	any	Palo Alto Networks - Known malicious IP addresses	any	any	any	any	any	any	any	Deny	none	

STEP 4 | 同样，使用 **Palo Alto Networks - Tor** 退出 **IP** 地址外部动态列表，创建两条规则，阻止和记录进出 Tor 出口节点的流量，这些流量经常（但并非总是）与恶意活动有关，尤其是在企业环境中。

第 2 步：创建应用程序允许规则

在创建应用程序允许规则之前确定应用程序允许列表。基于应用程序而不是端口创建允许规则。除了某些需要用户访问才能让防火墙识别用户的基础设施应用程序之外，仅允许已知用户访问。创建用户组以访问允许的应用程序，并将用户访问权限仅限于有业务需要访问每个应用程序的特定用户或用户组。

要将基于端口的规则转换为基于应用程序的规则或基于端口的防火墙迁移，请遵循迁移到基于应用程序的策略的最佳实践中的建议，该策略利用 策略优化器。策略优化器可帮助您分析基于端口的规则并向您显示与这些规则匹配的确切应用程序。它还可以帮助您查找未使用的规则、具有未使用的应用程序的规则（过度配置的规则）以及基于端口的现有规则。

在安全策略规则库中，将特定规则置于一般规则之上。否则，一般规则可能会掩盖特定规则。（隐藏是指您放置一个广泛的规则，其中包含与规则库中比特定规则更高的更具体的规则相同的匹配条件，因此旨在匹配特定规则的流量而不是匹配一般规则。）

规则库的这一部分包含识别为应用程序允许列表部分的应用程序的允许规则，包括：

- 以业务和基础架构为目的，您提供和管理的经批准的应用程序
- 一般业务应用程序用户可能需要完成他们的工作。
- 您选择允许个人使用的容忍应用程序。

使用预定义的已批准标签标记所有经批准的应用程序。全景图和防火墙认为不带批准标记的应用成为是未批准的应用程序。

附加最佳实践安全配置文件以扫描所有允许的流量是否存在已知和未知威胁。如果尚未创建这些配置文件，则创建 Internet 网关最佳实践安全配置文件。由于您无法检查看不到的内容，因此请将防火墙配置为解密流量以实现完全可见性和威胁检查。

STEP 1 | 允许访问您的企业 DNS 服务器。

仅允许流量流向批准的 *DNS* 服务器。使用 DNS 安全服务阻止恶意 *DNS* 服务器连接。

我为什么需要该规则？	规则亮点
❑ 对 DNS 的访问提供了网络基础设施服务，并且经常被攻击者利用。 ❑ 只允许访问您的内部 DNS 服务器可以降低攻击面。	• 由于此规则非常具体，因此请将其放置在规则库顶部附近。 • 创建地址对象，作为目的地址，保证用户只能访问您的数据中心的 DNS 服务器。 • 由于用户在登录之前需要访问这些服务，因此允许任何用户访问。

			Source				Destination							
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
IT DNS Services	Best Practice	universal	Users	any	any	any	IT Infrastructure	DNS Servers	any	dns	application-default	Allow		

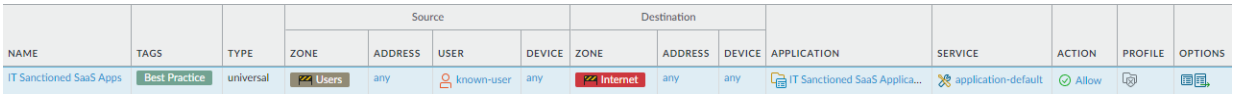
STEP 2 | 允许访问其他需要的 IT 基础架构资源。

我为什么需要该规则？	规则亮点
❑ 启用提供网络基础设施和管理功能的应用程序，例如 NTP、OCSP、STUN 和 Ping。 ❑ 前述规则将允许的 DNS 流量限制为数据中心的目标地址，但这些应用程序可能不在数据中心内，所以需要单独的规则。	• 因为这些应用程序在默认端口运行，允许访问任何用户（需要这些服务时，用户可能还未登录或不是已知用户），并且具有 **any**（任何）目标地址，请将他们包含在一个应用程序组中，并创建一个单独的规则来允许访问它们。

			Source				Destination							
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Required Infrastructure	Best Practice	universal	Users	any	any	any	Internet	any	any	Required Infrastructure	application-default	Allow		

STEP 3 | 允许访问 IT 批准的 SaaS 应用程序。

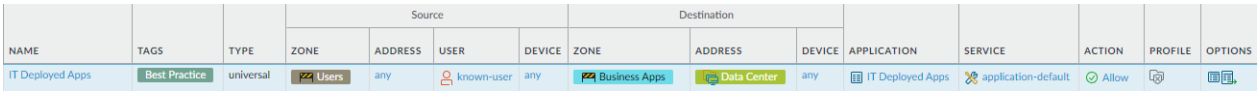
我为什么需要该规则？	规则亮点
❑ 对于 SaaS 应用程序，专有数据驻留在云中。此规则确保只有已知用户才能访问这些应用程序（以及底层数据）。 ❑ 允许扫描 SaaS 流量，检测威胁。	• 创建应用程序组以控制所有认可的 SaaS 应用程序。 • SaaS 应用程序应始终在应用程序默认端口上运行。 • 限制已知用户的访问。请参阅为允许的应用程序访问权限创建用户组。



NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE					
IT Sanctioned SaaS Apps	Best Practice	universal	Users	any	known-user	any	Internet	any	any	IT Sanctioned SaaS Applica...	application-default	Allow		

STEP 4 | 允许访问 IT 配置的本地应用程序。

我为什么需要该规则？	规则亮点
❑ 攻击通常在渗透阶段使用 FTP 等关键业务数据中心应用程序，或利用应用程序漏洞进行横向移动。 ❑ 许多数据中心应用程序使用多个端口。将服务设置为 **application-default**（应用程序默认值）可以安全地在其标准端口上启用应用程序。不允许在非标准端口上运行应用程序，这通常与规避行为相关。	• 创建应用程序组集合所有数据中心应用程序。 • 为您的数据中心服务器地址创建一个地址组。 • 限制已知用户的访问。请参阅为允许的应用程序访问权限创建用户组。

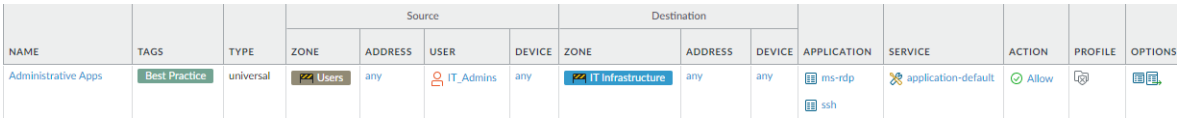


NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE					
IT Deployed Apps	Best Practice	universal	Users	any	known-user	any	Business Apps	Data Center	any	IT Deployed Apps	application-default	Allow		

STEP 5 | 允许访问您的管理用户所需的应用程序。

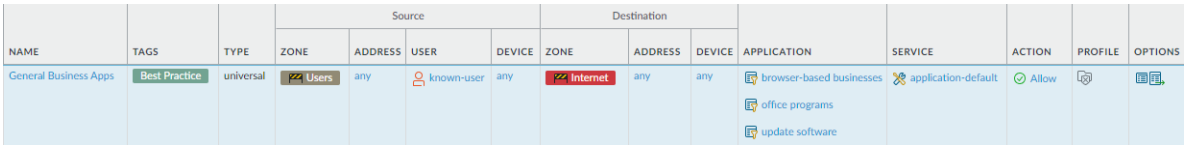
我为什么需要该规则？	规则亮点
❑ 为缩小攻击面，请为允许的应用程序访问权限创建用户组。 ❑ 因为管理员常常需要访问敏感的帐户数据和远程访问其他系统（如 RDP），从而减小您的攻击面，因此，您可以仅授予有业务需要的管理员访问权限。	• 该规则限制访问 IT 管理组的用户。 • 为每个内部应用程序或非标准端口上运行的应用程序创建自定义应用程序，使您在网络上打开多余的端口，而是在默认端口上实施这些应用程序。

我为什么需要该规则？	规则亮点
	• 如果不同的应用程序有不同的用户组，则设置分离的规则，实现粒度控制。



STEP 6 | 允许访问常规业务应用程序。

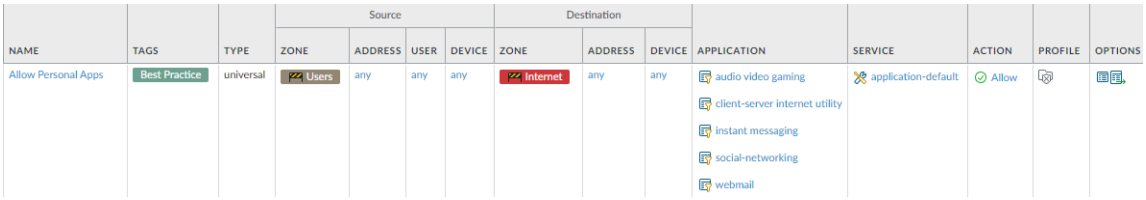
我为什么需要该规则？	规则亮点
❑ 除了您为用户批准和管理的应用程序之外，用户通常还需要访问其他业务应用程序，例如 Zoom、Adobe 在线服务或 G Suite。 ❑ 此规则使您能够在扫描威胁的同时安全地允许 Web 浏览。请参阅创建 Internet 网关最佳实践安全配置文件。	• 仅限制已知用户的访问。请参阅为允许的应用程序访问权限创建用户组。 • 考虑到可视性，为您想要允许的每种类型的应用程序创建应用程序筛选器。 • 附加最佳实践安全配置文件以防止所有流量中的已知和未知威胁。



STEP 7 | （可选）允许访问个人应用程序。

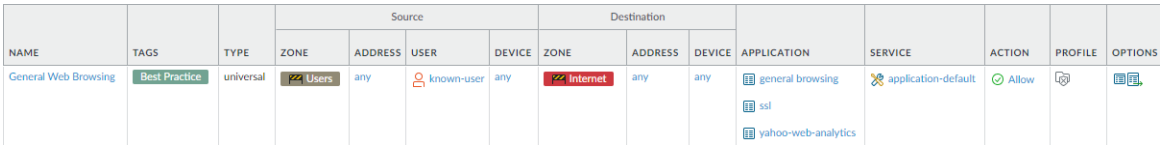
我为什么需要该规则？	规则亮点
❑ 由于工作和个人设备之间界线很模糊，所以，您的用户访问的所有应用程序都会安全启用，并且没有威胁。 ❑ 创建此初始规则库时，使用应用程序过滤器可以安全地启用对个人应用程序的访问。评估正在使用的应用程序之后，您可以利用信息决定是否移除筛选器，并且允许适合您的	• 仅限制已知用户的访问。请参阅为允许的应用程序访问权限创建用户组。 • 考虑到可视性，为您想要允许的每种类型的应用程序创建应用程序筛选程序。 • 附加最佳实践安全配置文件以防止所有流量中的已知和未知威胁。

我为什么需要该规则？	规则亮点
可接受使用策略的更小的个人应用程序子集。	



STEP 8 | 允许常规 web 浏览。

我为什么需要该规则？	规则亮点
❑ 之前的规则允许访问个人应用程序（其中许多是基于浏览器的）。此规则允许一般网页浏览。 ❑ 常规 web 浏览比其他类型的应用程序流量风险更大。创建最佳实践安全配置文件并将其附加到此规则，以便安全地启用 Web 浏览。 ❑ 由于威胁常常隐藏在加密流量中，因此，要安全启用 Web 浏览，您要解密流量以获得完全可视性和威胁检测。	• 使用与其他规则相同的最佳实践安全配置文件，并尽可能收紧 URL 过滤配置文件。 • 为了帮助防止带有恶意软件或嵌入式设备的设备访问互联网，请仅允许已知用户。 • 使用应用程序筛选程序，允许访问通用类应用程序。 • 要允许用户浏览您选择从解密排除的 HTTPS 站点，则要明确允许 SSL 作为应用程序。 • 将服务设置为 **application-default**。



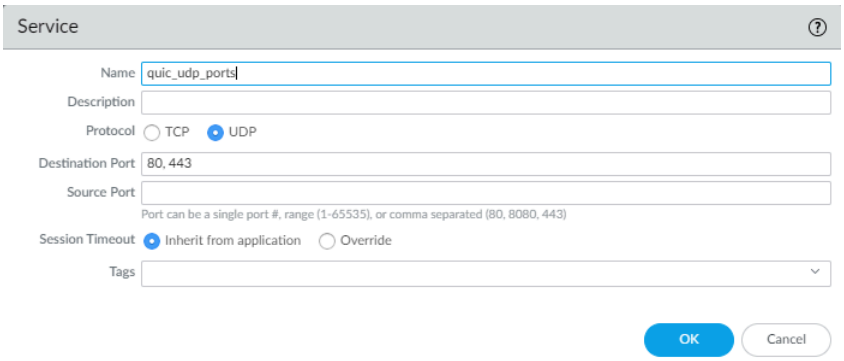
第 3 步：创建应用程序阻止规则

在您开发和调整安全策略规则库时，应用程序阻止规则可保护您免受规避和经常被利用的应用程序的侵害。临时调整规则有助于查找策略中的漏洞并识别可能的攻击。由于它们捕获您不知道网络上正在运行的应用程序流量，因此它们允许可能带来安全风险的流量。以下阻止规则显式阻止攻击者常用的潜在恶意应用程序和协议，例如公共 DNS 和 SMTP、加密隧道、远程访问和未经批准的文件共享应用程序。

STEP 1 | 阻止快速 UDP Internet 连接 (QUIC) 协议。

我为什么需要该规则？	规则亮点
❑ Chrome 和其他一些浏览器使用 QUIC 而不是 TLS 建立会话。QUIC 使用防火墙无法解密的专有加密，因此潜在危险的加密流量可能会进入网络。 ❑ 阻止 QUIC 会强制浏览器退回到 TLS，使防火墙解密流量。	• 创建指定 UDP 端口 80 和 443 的服务（**Objects**（对象）> **Services**（服务））。 • 第一条规则在其 UDP 服务端口（80 和 443）上阻止 QUIC，并使用您创建的服务来指定这些端口。 • 第二条规则阻止 QUIC 应用程序。

该服务指定要阻止 QUIC 的 UDP 端口。



第一条规则指定您为 QUIC 配置的服务，第二条规则阻止 QUIC 应用程序：

			Source				Destination							
	NAME	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
1	Block QUIC UDP	universal	l3-vlan-trust	any	any	any	l3-untrust	any	any	any	quic_udp_ports	Deny	none	
2	Block QUIC	universal	l3-vlan-trust	any	any	any	l3-untrust	any	any	quic	application-default	Deny	none	

STEP 2 | 阻止没有合法用例的应用程序。

我为什么需要该规则？	规则亮点
❑ 阻止潜在的恶意应用程序，例如 IT 未批准的加密隧道、点对点文件共享和基于 Web 的文件共享应用程序。 ❑ 由于临时优化规则可能允许具有恶意意图的流量以及与策略规则不匹配的合法流量，因此它们可能会允许有风险或恶意的流量。此规则阻止没有合法用例且攻击者或疏忽用户可以使用的流量。	• 采用 **Drop**（丢弃）操作默默地丢弃流量，不用发送信号到客户或服务器。 • 为匹配此规则的流量启用日志记录，以便您调查网络上应用程序的潜在威胁和错误使用。

我为什么需要该规则？	规则亮点
	• 由于此规则旨在捕获恶意流量，因此它会匹配来自在任何端口上运行的任何用户的流量。

NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE					
Block Bad Apps	Best Practice	universal	Users	any	any	any	Internet	any	any	encrypted tunnels file sharing remote access	any	Drop	none	

STEP 3 | 阻止公用 DNS 和 SMTP 应用程序。

仅允许流量流向批准的 *DNS* 服务器。使用 DNS 安全服务阻止恶意 *DNS* 服务器连接。

我为什么需要该规则？	规则亮点
❑ 阻止公共 DNS/SMTP 应用程序，以避免 DNS 隧道、命令和控制流量以及远程管理应用程序。	• 使用 **Reset both client and server**（重置客户端和服务器端）操作，向客户端设备和服务器端设备发送 TCP 重置信息。 • 为与此规则匹配的流量启用日志记录，以便您可以调查潜在威胁。

NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE					
Block Public DNS and SMTP	Best Practice	universal	Users	any	any	any	Internet	any	any	dns smtp	any	Reset Both	none	

第 4 步：创建临时调整规则

临时调整规则来帮助您监控初始最佳实践规则库缺陷，并在出现预警行为时发出警告。

例如，临时规则可识别来自未知用户或在意外端口上运行的应用程序的流量。监视与临时规则匹配的流量，以全面了解网络上使用的所有应用程序（并在过渡到最佳实践规则库时确保应用程序可用性）。使用此信息可以帮助您微调允许列表，方法是为您不知道需要的应用程序添加新的允许规则，或者缩小允许规则并用应用程序组或特定应用程序替换应用程序过滤器。当流量不再匹配这些规则时，您可以移除临时规则。

一些临时调整规则的优先级高于阻止不良应用程序的规则，而另一些则确保目标流量与适当的规则匹配，同时确保不良流量不会进入您的网络。

STEP 1 | 允许已知用户的web 浏览和非标准端口的 SSL，确定是否有合法应用程序在非标准端口运行。

我为什么需要该规则？	规则亮点
❑ 此规则有助于确定您的策略中是否存在漏洞，导致用户无法访问合法应用程序，因为它们在非标准端口上运行。 ❑ 监控所有符合此规则的流量。对于合法流量，请将适当的应用程序添加到适当的允许规则中。如果合适，请创建自定义应用程序。	• 不像只允许默认端口上的应用程序的允许规则，此规则允许所有端口上的 Web 浏览和 SSL 流量，以便发现允许列表中的缺陷。 • 由于此规则会发现策略中的漏洞，因此请将其限制为网络上的已知用户。 • 要允许用户浏览未解密的 HTTPS 站点（例如，财务服务和健康护理站点），则要在此规则中明确允许 SSL 作为应用程序。 • 附加最佳实践安全配置文件以扫描威胁。 • 将此规则添加到应用程序阻止规则之上，否则任何流量都不会与此规则匹配。

			Source				Destination							
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Unexpected Port SSL and Web	Best Practice	universal	Users	any	known-user	any	Internet	any	any	ssl web-browsing	any	Allow		

STEP 2 | 允许来自未知用户的非标准端口上的web 浏览和 SSL 流量，标出所有未知用户，无论端口是多少。

我为什么需要该规则？	规则亮点
❑ 此规则可帮助您确定用户 ID 覆盖范围内是否有缺陷。 ❑ 此规则有助于识别尝试访问互联网的受损或嵌入式设备。 ❑ 阻止非标准端口的使用很重要，即使对于 Web 浏览流量，因为这是一种逃逸技术。	• 大部分应用程序允许规则适用于已知用户或特定的用户组，而该规则明确匹配来自 **Unknown**（未知）客户的流量。 • 该规则必须置于应用程序阻止规则之上，否则流量永远不会触犯到它。 • 附加最佳实践安全配置文件以扫描威胁。

			Source				Destination							
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Unknown User SSL and Web	Best Practice	universal	Users	any	unknown	any	Internet	any	any	ssl web-browsing	any	Allow		

STEP 3 | 允许应用程序默认端口上的所有应用程序，识别预期以外的应用程序。

我为什么需要该规则？	规则亮点
❑ 该规则为您不知道在网络中运行的应用程序提供了可见性，从而让您可以微调应用程序允许列表。 ❑ 监视与此规则匹配的所有流量，以确定它是否代表潜在威胁，或者是否需要修改允许规则以允许访问更多应用程序。	• 因为该规则允许所有应用程序，所以您必须将其添加在应用程序阻止规则之后，防止坏应用程序在网络中运行。 • 如果您运行 PAN-OS 7.0.x 或更早版本，为了正确识别不可预知的应用程序，请创建包含所有应用程序的应用程序筛选器，而不是将规则设为允许 **any**（任何）应用程序。

			Source				Destination							
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Unexpected Traffic	Best Practice	universal	Users	any	any	any	Internet	any	any	All apps	application-default	Allow		

STEP 4 | 允许任何端口上的任何应用程序识别在非标准端口上运行的应用程序。

我为什么需要该规则？	规则亮点
❑ 此规则有助于识别在未知端口上运行的合法、已知应用程序。 ❑ 该规则可帮助您识别需要创建自定义应用程序的未知应用程序，以将其添加到应用程序允许规则中。 ❑ 符合此规则的流量是可操作的。追踪流量来源并确保不允许未知的 tcp、udp 或非 syn-tcp 流量。	• 因为这是一条非常通用的规则，允许任何用户在任何端口上使用任何应用程序，因此将其放在规则库的底部。 • 为与此规则匹配的流量启用日志记录，以便您可以调查应用程序的滥用和潜在威胁，或识别需要自定义应用程序的合法应用程序。

			Source				Destination							
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Unexpected Port Usage	Best Practice	universal	Users	any	any	any	Internet	any	any	any	any	Allow		

第 5 步：启用日志，记录不匹配任何规则的流量

与您定义的规则不匹配的 Internet 网关流量与规则库底部的预定义区域间默认规则相匹配，因此会被拒绝。为了查看不匹配您创建的规则的流量，对“区域间默认”规则启用日志记录：

STEP 1 | 在规则库中选择区域间默认规则的行，然后 **Override**（覆盖）该规则以进行编辑。

STEP 2 | 选择 **interzone-default**（区间-默认）规则名称，打开要编辑的规则。

STEP 3 | 在 **Actions**（操作）选项卡中，选择 **Log at Session End**（结束时记录）并点击 **OK**（确定）。

STEP 4 | 创建自定义报告以监控符合规则的流量：

1. 选择 **Monitor**（监控） > **Manage Custom Reports**（管理自定义报告）。
2. **Add**（添加）一个报告，并为其指定描述性 **Name**（名称）。
3. 将 **Database**（数据库）设为 **Traffic Summary**（流量统计）。
4. 选中 **Scheduled**（已调度）复选框。
5. 将 **Rule**（规则）、**Application**（应用程序）、**Bytes**（字节）、**Sessions**（会话）添加到“所选列列表“中。
6. 设置期望的 **Time Frame**（时间框架）、**Sort By**（排序方式）和 **Group By**（分组方式）字段。
7. 定义查询，以匹配与区域间默认规则匹配的流量：

   ```
   (rule eq 'interzone-default')
   ```

STEP 5 | 将所做更改 **Commit**（提交）至规则库。

监控和微调策略规则库

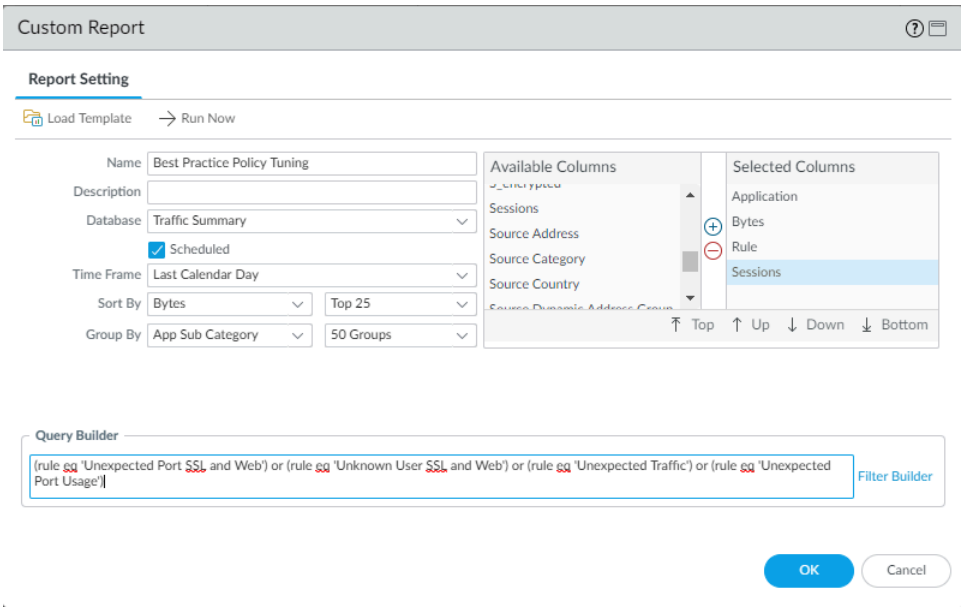
创建最佳实践安全策略是一个迭代过程。您定义初始 Internet 网关安全策略后，可以监控匹配临时规则的流量，这些临时规则用于识别策略缺陷和警报行为，然后对您的策略进行相应调整。通过监控符合这些规则的流量，您可以对永久规则进行适当的调整，确保所有流量都与您的应用程序允许规则相匹配，或者评估是否应允许不匹配任何规则的应用程序。

在调整规则库时，您应该看到允许与临时规则匹配的流量越来越少。当您不再看到想要允许与这些规则匹配的流量时，您的强制执行允许规则已完成，您可以删除临时规则（区域间默认拒绝规则会自动拒绝任何规则明确允许的流量）。

由于每月发布的内容会添加新的应用程序 *ID*，因此，请查看应用程序 ID 更改对您的安全政策的影响。

STEP 1 | 创建自定义报告以监控与识别策略差距的规则相匹配的流量。

1. 选择 **Monitor**（监控） > **Manage Custom Reports**（管理自定义报告）。
2. **Add**（添加）报告并为其指定一个描述性 **Name**（名称），以表明您正在调查的政策差距。
3. 将 **Database**（数据库）设为 **Traffic Summary**（流量统计）。
4. 选择 **Scheduled**（调度）。
5. 将 **Rule**（规则）、**Application**（应用程序）、**Bytes**（字节）、**Sessions**（会话）添加到“所选列列表“中。
6. 设置期望的 **Time Frame**（时间框架）、**Sort By**（排序方式）和 **Group By**（分组方式）字段。
7. 定义查询以匹配与发现政策差距和警报行为的规则相匹配的流量。您可以使用 **or**（或）运算符为匹配任何规则的流量创建单个详细报告，或是创建单个报告以监控每个规则。以下示例查询使用示例策略中定义的规则名称：
   - `(rule eq 'Unexpected Port SSL and Web')`
   - `(rule eq 'Unknown User SSL and Web')`
   - `(rule eq 'Unexpected Traffic')`
   - `(rule eq 'Unexpected Port Usage')`



STEP 2 | 定期查看报告，了解流量与每条调整规则相匹配的原因。要么更新规则以包括合法的应用程序和用户，要么使用报告中的信息来评估应用程序的风险并实施政策改革。

移除临时规则

经过几个月的监视您的初始互联网网关最佳实践安全策略和调整规则库，您应该看到更少的和您想要允许的流量匹配临时规则。当您看不到有任何您希望允许的流量匹配这些规则时，就已经达到了转换到完全基于应用程序的安全策略规则库的目的。您现在可以删除临时规则，包括不具有合法用例的应用程序以及公共DNS和SMTP应用程序的应用程序阻止规则，因为默认的区域间默认拒绝规则会自动阻止该通信，因为它不匹配任何显式的允许规则。（保留 QUIC 的规则。）

STEP 1 | 选择 **Policies**（策略） > **Security**（安全）。

STEP 2 | 选中规则，然后单击 **Delete**（删除）。

也可以在删除规则之前，**Disable**（禁用）一段时间。如果流量日志显示您要允许的流量与区域间默认拒绝规则相匹配，则可以再次 **Enable**（启用）它们。

STEP 3 | **Commit**（提交）更改。

维护规则库

业务和应用程序不断发展，因此您的安全策略规则库也需要不断发展。当批准的应用程序发生更改时，请尽可能对与应用程序的业务用例一致的现有策略规则进行相应的更改，而不是添加新规则。通常，更改非常简单，只需将新应用程序添加到应用程序组或从应用程序组中删除已弃用的应用程序即可。

在 *Panorama* 或独立防火墙上，使用策略规则匹配计数器分析规则库发生的变化。例如，添加新应用程序时，先将允许规则添加至规则库，再允许应用程序的网络流量。如果流量触发规则，且计数器递增，则表示即使您尚未激活应用程序，与规则匹配的流量也已存在于网络上，或者您需要调整此规则。接着检查 ***ACC*** > ***Threat Activity***（威胁活动） > ***Applications Using Non Standard Ports***（使用非标准端口的应用程序）和***ACC*** > ***Threat Activity***（威胁活动） > ***Rules Allowing Apps On Non Standard Ports***（允许非标准端口上的应用程序的规则）小组件，查看是否是非标准端口上的流量导致触发非预期的规则。

使用策略规则计数器的关键在于执行更改时重置计数器，如引入新应用程序或更改规则的定义。重置计数器时确保您看到更改后的结果，结果不包括更改前所做的更改和发生的事件。

如果使用 *Panorama* 管理防火墙，则可以监视防火墙运行状况，以便对比设备的基准性能，并将设备相互对比来确定与正常行为的偏差。

设置 Palo Alto Networks 内容更新，以便在防火墙上自动下载和安排安装。每当安全配置文件签名需要更新时，都会更新应用程序和威胁内容。每月第三个星期二发送的内容更新还包含新的和修改的应用 ID（应用程序更新；在极少数情况下，应用程序更新可能会延迟一到两天）。评估新的和修改的应用 ID 如何影响非生产环境中的安全策略规则库，并根据需要修改规则。

遵循内容更新最佳实践，尽快安装更新以保护您的互联网网关，并为所有内容更新配置日志转发。

STEP 1 | 安装新的内容更新之前，请检查新的和修改的 App-ID，确定更改是否影响策略。

STEP 2 | 如有必要，修改现有的安全策略规则，以适应 App-ID 的更改。如果有些 App-ID 要求执行更多测试并安装剩下的新的和修改的 App-ID，您可以禁用选择的 App-ID。完成最终测试和所有必要的策略修改，再在收到新 App-ID（每个月第三个星期二）后发布下个月的内容更新，避免重叠。

STEP 3 | 准备策略更新，以便解释内容更新中包含的 App-ID 更改，将新的经批准的应用程序添加至允许列表规则，或者从允许列表规则移除应用程序。