迁移到基于应用程序的策略的最佳实践

Version 10.0 (EoL)

techDOCS paloalto NETWORKS

Contact Information

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

About the Documentation

- To ensure you are viewing the most current version of this document, or to access 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 15, 2020

Table of Contents

迁移到基于应用程序的策略的最佳实践

您不必为了应用程序可用性而牺牲更好的安全性。相反，使用 Expedition和策略优化器，您可以自动通过分阶段且安全的方式从旧版防火墙上基于端口的安全策略迁移到 Palo Alto Networks 下一代防火墙或 Panorama 设备上基于应用程序的安全策略，并减少迁移过程所需要的时间和精力。

- 使用分阶段转换安全地启用应用程序
- 使用 Expedition 将基于端口的策略迁移到 PAN-OS
- 使用策略优化器迁移到基于应用程序的策略
- 采用安全最佳实践的后续步骤

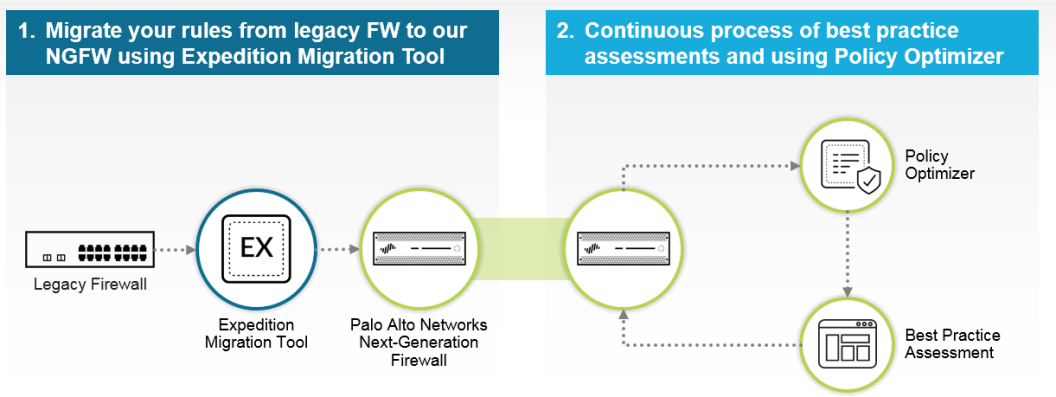
使用分阶段转换安全地启用应用程序

基于端口的安全策略的典型缺点众所周知：无法看到哪些应用程序使用端口，因此，任何恶意应用程序都可以在端口 80 (HTTP) 或端口 53 (DNS) 等开放端口上访问您的网络。这使攻击者更容易安装恶意软件，在网络中横向移动，泄露数据和破坏网络，因为您对网络上的应用程序一无所知，也无法阻止其流量中隐藏的威胁。

与之相反，无论端口、协议、加密（SSL 或 SSH）或规避策略如何，基于应用程序的安全策略使用 App-ID™ 都可以提供对应用程序的可见性，因此，您可以准确了解网络中有哪些应用程序，也可以检查其流量是否存在威胁。特定于应用程序的策略支持安全访问，因为您可以配置安全策略规则，从而只允许正确的用户访问正确位置的正确应用程序，并且可以将威胁防护配置文件应用于这些规则。使用 App-ID 对应用程序进行分类可以缩小攻击范围，因为网络上只允许支持业务的必要应用程序，并自动阻止不需要的应用程序。试图阻止您不想要的所有单个应用程序是一项永无止境的任务，相比之下，允许想要的应用程序而阻止其他一切更加容易和安全。

分阶段迁移到 App-ID：

Moving From Legacy Rules To App-ID Based Rules



1. 使用 Expedition 导入旧版规则库，进行清理，实现到 Palo Alto Networks 下一代防火墙或 Panorama 设备的类似迁移。Expedition 作为虚拟机 (VM) 分发。
2. 在网络生产环境中运行 PAN-OS 防火墙或设备，以便它开始学习和对网络上的应用程序分类。
3. 记录流量至少一周后，运行最佳实践评估 (BPA) 以设置基准，然后使用策略优化器开始安全地将基于端口的规则转换为基于应用程序的规则并保护您的网络。（您可以在大约一周后转换一些允许常见应用程序的简单规则；对于其他发现许多应用程序的规则，例如一般的出站 Internet 访问规则，请至少等待 30 天才能收集应用程序信息。）根据您的业务需求和优先级，采用分阶段方法安全地转换规则。
4. （可选）使用策略优化器将规则库转换为 App-ID 后，将配置重新导入 Expedition 并使用规则扩充功能进一步简化和优化规则库。
5. 向网络中引入新应用程序时，请维护 App-ID 部署。在第一次转换通过基于端口的规则后运行 BPA，然后定期测量进度并发现其他区域以提高安全性。

策略优化器从 *PAN-OS 9.0* 开始提供。如果您使用 *Panorama* 管理新一代防火墙，则不必将受管防火墙升级到 *PAN-OS 9.0*，即可使用策略优化器。您只需将 *Panorama* 升级到 *PAN-OS 9.0*，从受管防火墙将日志发送到运行 *PAN-OS 9.0* 的 *Panorama* 或日志收集器，并将策略从 *Panorama* 推送到防火墙。托管防火墙需要运行 *PAN-OS 8.1* 或更高版本，如果它们连接到日志收集器，则日志收集器必须运行 *PAN-OS 9.0*。这为资格认证提供了快速途径，因此，您可以使用策略优化器快速采用基于 *App-ID* 的策略。

PA-7000 系列防火墙支持两种日志记录卡，*PA-7000* 系列防火墙日志处理卡 *(LPC)* 和高性能 *PA-7000* 系列防火墙日志转发卡 *(LFC)*。与 *LPC* 不同，*LFC* 没有进行日志本地储存的磁盘空

间。取而代之的是，*LFC* 将所有日志转发至一个或多个日志记录系统，如 *Panorama* 或系统日志服务器。如果您使用 *LFC*，策略优化器的应用程序使用信息不会显示在防火墙上，因为流量日志并非本地储存。如果您使用 *LPC*，流量日志将本地存储到防火墙上，因此，策略优化器的应用程序使用信息会显示在防火墙上。在两种情况下，只要日志收集器和 *Panorama* 运行 *PAN-OS 9.0* 或更高版本，*PA-7000* 防火墙都可以运行 *PAN-OS 8.1*（或更高版本）。

使用 Expedition 将基于端口的策略迁移到 PAN-OS

使用 Expedition 导入旧版规则库，进行清理，并作为迁移到基于应用程序的安全策略的第一阶段，实现到 Palo Alto Networks 下一代防火墙或 Panorama 设备的类似迁移。Expedition 是在配置中对多个对象执行批量操作的绝佳工具，并支持从大多数主要防火墙供应商导入旧版配置。

本主题总结了 *Expedition* 工作流程。现场社区支持 *Expedition*，包括如何获取工具和关于如何使用工具的详细文档。

Palo Alto Networks 技术支持 *(TAC)* 不提供对 *Expedition* 的支持。

有关 Expedition 迁移工作流程的详细信息，请参阅“Expedition 用户指南”，其中还包含有关如何使用 CSV 文件将对象导入配置以及如何导入 Day 1 Iron-Skillet 配置的信息。

有关管理 Expedition 的信息，请参阅“Expedition 管理指南”，其中还包括一些用户界面信息，还可以参阅“Expedition 强化指南”，该指南提供了有关如何保护 Expedition VM 的建议。

在开始迁移之前，请确保满足以下先决条件：

- 将 Expedition 下载到支持运行 VM 的管理设备。
- 与要迁移到的 Palo Alto Networks Panorama 和防火墙建立 SSH 和/或 SSL 连接。SSH 访问用于 CLI 连接，SSL 访问用于 Web 界面连接和推送 API 命令。
- 要迁移到的 Palo Alto Networks Panorama 和防火墙的操作访问，以便您将类似配置推送到 PAN-OS 应用程序。

专业服务团队有着丰富的迁移经验。您可以聘请专业服务团队来帮助您将配置从旧版设备迁移到 *Palo Alto Networks* 下一代防火墙和 *Panorama* 设备。

STEP 1 | 查看旧版防火墙配置。

了解旧版规则库的目标。记录迁移时需要了解的项目，例如 Juniper SRX 设备上已禁用的接口，或验证具有相同安全级别的接口之间是否允许通信，验证 IPSec 隧道的状态并收集 Cisco ASA 设备上的预共享密钥。

STEP 2 | 将旧版配置导入 Expedition，并对配置进行任何必要的修改。

STEP 3 | 在 Expedition 中创建一个新的 **Project**（项目）。

STEP 4 | 将迁移的源（旧版）配置导入到 **Project**（项目）并进行检查。

检查文件格式，确保包含所有必需文件，并检查 Expedition 日志和事件，确保正确加载迁移的配置文件。如有必要，请修改迁移的源文件以修复问题，然后再次检查。重复此步骤，直到解决所有问题。

STEP 5 | 将 PAN-OS 配置导入到 **Project**（项目），作为迁移的基本配置。

获取最新的内容更新，然后从现有 PAN-OS 设备（现有配置文件或出厂默认 PAN-OS 配置文件）导入基本配置。

配置文件应与要使用的 *PAN-OS* 版本匹配。例如，要运行 *PAN-OS 9.0*，请导入 *PAN-OS 9.0* 配置文件。

STEP 6 | 清理迁移的配置，以准备将其与 PAN-OS 基本配置合并。

- 删除或替换无效的服务对象。PAN-OS 只能识别 TCP 和 UDP 服务端口，Expedition 会自动将 TCP 和 UDP 服务对象迁移到应用程序。搜索非基于 IP 的应用程序和服务，例如 Ping 和 ICMP，某些旧版设备将其视为服务而非应用程序。将它们替换为 App-ID，以便将其归类为应用程序并获得对流量检查和控制的可见性。
- 要简化配置并减小大小，请删除或替换其他无效对象和未使用的对象，并合并重复的对象。
- 查找并删除已禁用的规则，避免它们导致配置混乱。
- 重命名接口以匹配 PAN-OS 设备上的接口。从旧版设备导入的接口名称通常与 PAN-OS 命名约定不匹配。
- 导入旧版配置时，Expedition 会自动分配区域名称。重命名区域，使其名称可以描述将配置迁移到 PAN-OS 设备时需要实现的目的。确保将区域正确映射到接口。

  另外，检查虚拟路由器是否有静态路由。如果存在许多静态路由，请使用 Expedition 将路由迁移到 PAN-OS 配置。如果只有少量静态路由，请记下它们，然后在迁移配置后手动创建。

STEP 7 | 通过将迁移的配置中的对象拖放到基本配置中，将迁移的配置与 PAN-OS 基本配置合并。

STEP 8 | 检查合并配置以查找合并可能已创建的重复对象，然后删除或合并它们。

STEP 9 | 将合并配置导出到 PAN-OS 设备之前，请清除连接到 PAN-OS 设备和 PAN-OS 设备的交换机和路由器上的 ARP 缓存，以更新 ARP 表。

在 PAN-OS 设备上，使用 **`clear arp all`** CLI 命令。（如有必要，您可以使用 **`clear arp <interface>`** CLI 命令按每个接口清除 ARP 缓存。）

STEP 10 | 将合并的配置导出到 PAN-OS 设备并加载合并的配置。

要使用的方法取决于您希望如何迁移合并配置：

- 对于 PAN-OS 设备上的新安装，**Generate XML & Set Output**（生成 **XML** 并设置输出），导入 XML 文件（配置），然后将其加载到 PAN-OS 设备上。
- 对于现有 PAN-OS 安装，或者如果一次只迁移配置的一个部分而不是全部，则 **Generate XML & Set Output**（生成 **XML** 并设置输出），导入 XML 文件（配置），然后使用 **`load config partial`** CLI 命令选择要加载的配置的特定部分。您需要 SSH 访问权限才能在 PAN-OS 设备上使用 CLI。
- 如果 PAN-OS 设备已连接到 Expedition，则还可以使用 API 调用将部分或整个配置发送到设备。

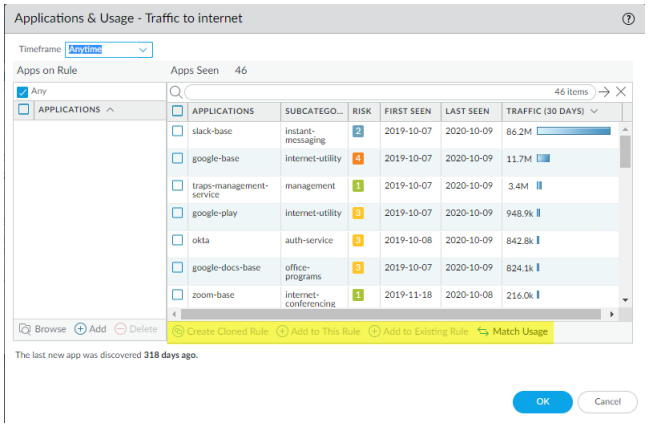
STEP 11 | 将合并的配置导出到 PAN-OS 设备并加载配置后，使用策略优化器将基于端口的策略转换为基于应用程序的策略。

使用策略优化器迁移到基于应用程序的策略

使用 Expedition 将类似的配置迁移到 PAN-OS 设备后，下一阶段是使用策略优化器简化向基于 App-ID 的安全策略规则的迁移。策略优化器使基于端口的旧版规则的转换变得更加容易，因为它可以自动显示每个规则的应用程序信息，并提供了理解信息所需的上下文，同时在单个视图中创建基于应用程序的智能规则。策略优化器：

- 学习并记住每个规则在流量中自动发现的所有应用程序，这消除了整理和分析大量日志数据的需要。即使日志滚动，策略优化器也会保留应用程序信息，因此您可以确信看到了规则中的所有应用程序。
- 可让您安全地迁移到基于 App-ID 的规则，而不会有应用程序可用性的风险。
- 是 PAN-OS 设备的原生工具且受支持，因此，无需在设备和非原生工具之间迁移配置和数据。
- 提供简单而直观的排序和筛选选项，帮助您确定转换哪些规则最容易和最安全，并确定优先转换哪些规则。
- 在 Panorama 设备和各个下一代防火墙上运行。如果使用 Panorama 管理运行 PAN-OS 8.1 的下一代防火墙，则只需将 Panorama（以及连接到托管防火墙的任何日志收集器）升级到 PAN-OS 9.0 即可使用和获得策略优化器的优势，因此，与必须获得所有防火墙的资格相比，您可以更快地获得资格并采用策略优化器。

这些功能为您提供了一款简单易用的工具，可以为您节省时间，并防止在将基于端口的规则转换为基于 App-ID 的规则时出错。策略优化器提供了几种转换规则的方法：



- **Create Cloned Rule**（创建克隆规则）— 克隆规则会保留基于端口的原始规则，并将新的基于 App-ID 的规则置于克隆规则之上。您可以从一个基于端口的规则克隆多个基于 App-ID 的规则。例如，您可以根据常规 Web 浏览规则中的应用程序子类别克隆多个 App-ID 规则，以对需要类似访问和威胁处理的应用程序进行分组，而不是尝试在一个常规的非安全规则中控制所有位置的所有用户的所有 Web 访问。

  这样，应用程序可用性就没有风险，因为克隆规则下面的基于端口的规则就像一个安全网。如果基于克隆 (App-ID) 的规则与需要允许的所有应用程序不匹配，您会看到这些应用程序匹配克隆规则下面的基于端口的规则，因此，您可以进行调整。如果在一段合理的时间内，没有您希望允许的流量与基于端口的规则匹配，则可以删除该基于端口的规则，从而完成将规则转换为基于 App-ID 的规则。
- **Add to This Rule**（添加到此规则）— 将应用程序添加到规则会将基于端口的规则替换为基于 App-ID 的规则，这会导致从规则库中删除基于端口的规则，并且不会提供克隆规则所具有的安全网。只有当您确定知道您希望规则控制的所有应用程序时，才使用 **Add to This Rule**（添加到此规则）。对于只发现了少量应用程序的规则，并且您确信自己了解您的业务所需的应用程序，才能将其作为 **Add to This Rule**（添加到此规则）的候选项。克隆已经发现了许多应用程序和规则是最安全的，这些规则发现的应用程序可能比您需要允许的更多。如果您没有将应用程序添加到规则，则会丢失该应用程序的可用性，除非另一个规则允许，而克隆规则会保留基于端口的规则，以作为安全网。
- **Add to Existing Rule**（添加到现有规则）— 将应用程序添加到现有规则不会替换基于端口的原始规则（包含在规则库中）。**Add to Existing Rule**（添加到现有规则）支持选择之前配置的任何规则以及将应用程序添加到该规则中。

当您将应用程序添加到基于应用程序的现有规则中时，防火墙会从基于端口的规则中移除这些应用程序，并将其添加到所选应用程序规则中。添加的应用程序与基于应用程序的规则中的其他应用程序使用相同的来源、目的和服务等。

当您将应用程序添加到基于端口的另一个现有规则中时，防火墙会从基于端口的原始规则中移除这些应用程序，并将其添加到其他基于端口的规则中。这会将基于端口的规则转换为基于应用程序的规则，而后者仅控制添加到该规则的应用程序。如果以这种方式转换基于端口的规则的一部分，请前往规则，并将服务更改为 application-default，以防止应用程序使用非标准端口（此外，在规则上配置的服务可能与应用程序不匹配）。

- **Match Usage**（匹配使用情况）— 匹配基于端口的规则的使用情况会将基于端口的规则替换为基于 App-ID 的规则，其中包含该规则发现的所有应用程序。仅在规则发现少数具有合法商业目的的常见应用程序时才使用 **Match Usage**（匹配使用情况）。一个很好的例子是 TCP 端口 22，它只应允许 SSH 流量。如果 SSH 是在端口 22 的基于端口的规则上发现的唯一应用程序，则可以安全地 **Match Usage**（匹配使用情况）并将规则转换为 App-ID 规则。

对于 **Create Cloned Rule**（创建克隆规则）、**Add to This Rule**（添加到此规则）或 **Add to Existing Rule**（添加到现有规则），您必须从中 **Apps Seen**（发现的应用程序）中选择至少一个应用程序。

如果历史记录不足以捕获应用程序的最新活动，则仅用于季度或年度事件的应用程序可能不会出现在应用程序信息中。转换规则时要注意这些类型的应用程序。

将基于端口的规则转换为基于应用程序的规则时，策略优化器除了将服务转换为 App-ID 之外，不会对规则进行任何其他更改。在大多数情况下，转换规则后，您需要将 **Service**（服务）更改为 **application-default**，因此，只有合法使用该端口的应用程序才能访问该端口，并且会阻止规避应用程序通过使用非标准端口获取网络访问权限。

如果业务需求要求在特定客户端和服务器之间的非标准端口上允许应用程序（如内部自定义应用程序），请将例外限制为仅包含所需的应用程序、源和目标。考虑重写自定义应用程序以使用应用程序默认端口。

在使用策略优化器将基于端口的规则转换为基于 App-ID 的规则之前：

1. 完成将旧版配置从 Expedition 到 Palo Alto Networks 下一代防火墙或 Panorama 设备的类似迁移。
2. 开始将规则转换到 App-ID 之前，在生产网络中运行 PAN-OS 9.0 设备大约一周时间，以便设备开始学习和对网络上的应用程序分类。您可以快速转换一些简单的规则（例如，端口 22 规则应该仅允许 SSH 流量且易于转换），而对于其他规则，您需要允许防火墙花更长的时间从流量中收集应用程序数据，例如您的 Internet 访问（端口 80/433）规则。
3. 运行最佳实践评估https://docs.paloaltonetworks.com/best-practices/10-0/best-practices-getting-started/get-started-with-best-practices/access-and-run-the-bpa.html (BPA) 以设置用于比较进度的基准。
4. 设定现实目标。想一想您想要怎样的最终结果。实现目标后，再次运行 BPA 以确认您已达到目标，然后重新评估是否可以更进一步改善网络安全性。利用策略优化器，您不需要为了安全性而牺牲可用性，您只会提高安全性。

分阶段转换规则。在 PAN-OS 设备只有一周的日志之后（策略优化器通过读取日志发现规则监视的应用程序），您可以将一些允许常见应用程序的基于端口的简单规则转换为基于 App-ID 的规则。对于监视许多应用程序的其他规则（例如常规 Web 访问规则），请至少等待 30 天来收集应用程序信息。

专业服务团队有着丰富的迁移经验。您可以聘请专业服务团队来帮助您将配置从旧版设备迁移到 *Palo Alto Networks* 下一代防火墙和 *Panorama* 设备。

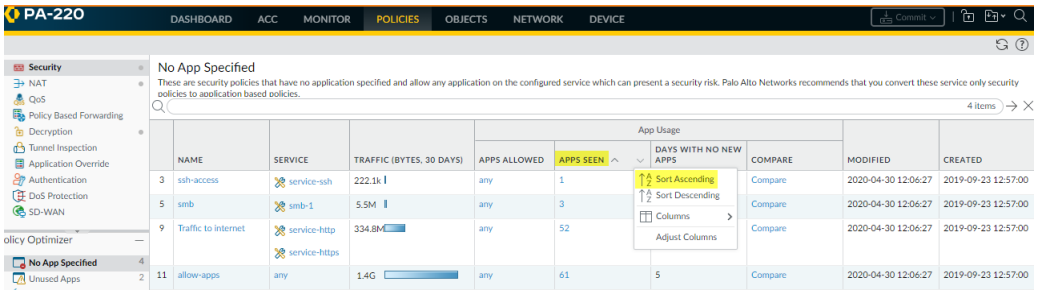
- 转换监控一周后常见应用程序的简单规则
- 30 天后开始转换的规则

转换监控一周后常见应用程序的简单规则

在监控生产流量一周后，您可以安全地开始将基于端口的简单规则转换为基于 App-ID 的规则。一些不错的候选项是包括仅允许一个或少量常见应用程序合法使用该端口的规则，因为这样很容易确定您想要在简单规则中允许的应用程序。示例包括端口 21 (FTP)、端口 22 (SSH) 和端口 53 (DNS)。

在开始转换规则之前先安装最新的内容更新，确保 PAN-OS 设备上具有最新的应用程序签名。本示例介绍如何对基于端口的规则进行排序，以查找安全转换的候选项以及将这些基于端口的规则直接转换为基于 App-ID 的规则的选项。

STEP 1 | 在 **Policies**（策略）> **Security**（安全）> **Policy Optimizer**（策略优化器）> **No App Specified**（未指定应用程序）中，选择 **Apps Seen**（发现的应用程序）和 **Sort Ascending**（升序排序）（或单击 **Apps Seen**（发现的应用程序）以恢复当前显示顺序），从而找到发现最少应用程序的基于端口的规则。

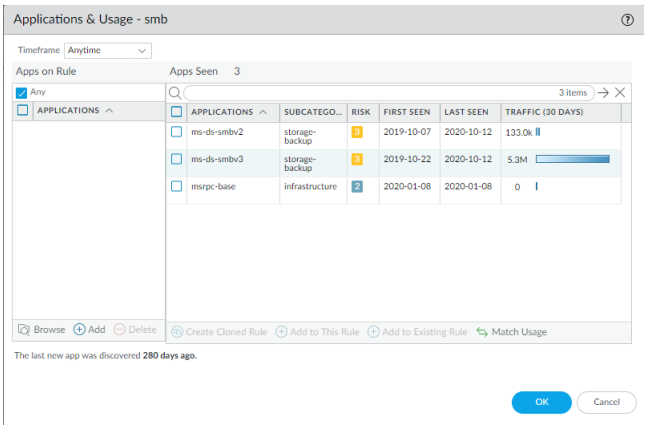


发现最少应用程序的基于端口的规则显示在 **No App Specified**（未指定应用程序）列表的顶部。您可以安全地将特定服务（例如 SSH）的规则直接转换为基于应用程序的规则，并且可以检查发现少量应用程序的规则，以了解是否可以安全转换。

旨在允许 Server Message Block（服务器消息块 - SMB）流量的基于端口的规则在将配置迁移到 PAN-OS 设备后仅发现了三个应用程序，因此是转换的候选项。

STEP 2 | 点击 **Apps Seen**（发现的应用程序）数字或 **Compare**（比较）以检查按规则发现的应用程序。

Applications & Usage（应用程序和使用情况）显示在流量中实际发现的与规则匹配的应用程序。



STEP 3 | 对于按该规则发现的应用程序，评估是要允许其中的全部、部分，还是全部不允许，并选择要允许的应用程序。

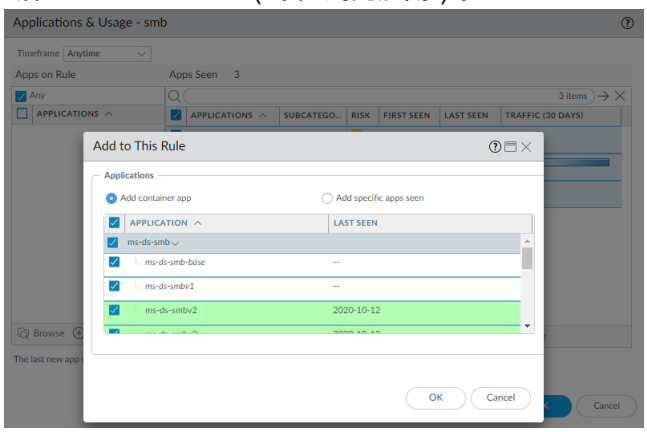
您可以通过添加容器应用程序来匹配规则的确切使用方法，在将来对规则进行证明，或选择要添加到规则的单个应用程序。

- 如果您希望规则允许与规则完全匹配的所有应用程序：

1. 在 **Apps Seen**（发现的应用程序）中选定所有 **Applications**（应用程序）。
2. 单击 **Match Usage**（匹配使用情况）。
3. 点击 **OK**（确定），将基于端口的规则转换为基于 App-ID 的规则。
4. 将 **Service**（服务）设置为 **application-default**，从而禁止所有规避和恶意应用程序使用此端口。

- 如果您允许按规则发现的所有或部分应用程序，或通过将其添加容器应用程序，以便在未来证明该规则（从而允许每个容器中的所有应用程序，并且自动允许以后添加到容器的应用程序）：

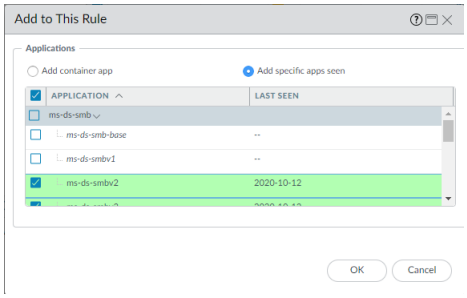
1. 选择所有应用程序，然后 **Add to This Rule**（添加到此规则）。



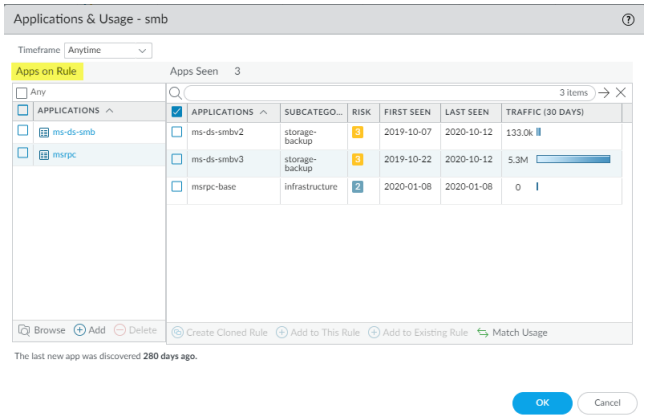
带灰色阴影的应用程序是容器应用程序。带绿色阴影的应用程序是规则中发现的应用程序。无阴影的应用程序属于同一容器应用程序，但没有在规则中发现。

默认已选中 **Add container app**（添加容器应用），因此，在默认情况下，已选中容器中的所有应用程序。

2. 如果您仅希望规则包含与规则匹配的应用程序，请选择 **Add container app**（添加容器应用）。这样就只会将该规则发现的应用程序添加到规则中。不会选中容器应用和规则中与规则不匹配的应用程序。单击 **OK**（确定）以仅选择规则中发现的应用程序。



如果您希望在规则中包含容器应用及其所有应用程序，请将选择保留为 **Add container app**（添加容器应用），然后点击 **OK**（确定）。只有容器应用会显示在 **Apps on Rule**（规则上的应用）中，因为其中包含（允许）所有应用程序，而且也会通过允许在未来将应用程序添加到容器，从而“在未来验证”规则：

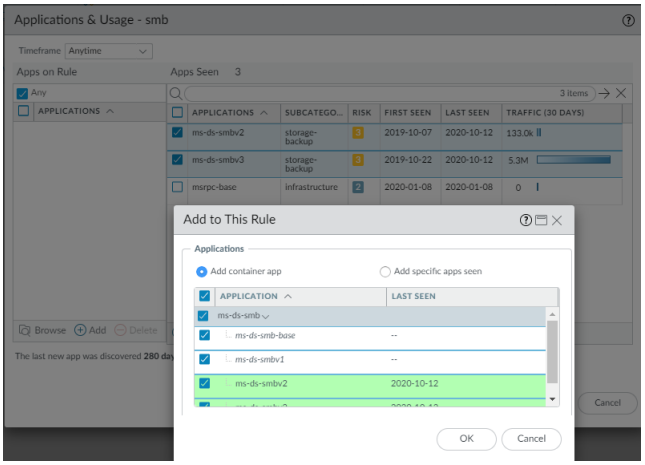


3. 在 **Usage**（使用情况）上单击 **OK**（确定）以转换规则。
4. 将 **Service**（服务）设置为 **application-default**，从而禁止所有规避和恶意应用程序使用此端口。

- 如果您希望选择在容器应用中允许的应用程序，请选择这些应用程序，然后单击 **Add to This Rule**（添加到此规则）。例如，如果您决定不允许 msrpc-base，而仅选择 ms-ds-smbv2 和 ms-ds-smbv3 并 **Add to Rule**（添加到规则），策略优化器会在容器应用程序中显示相关应用程序（ms-ds-smb，带灰色阴影），并通过添加这些应用程序提供未来证明规则的机会：

  1. 选择要允许的应用程序，然后单击 **Add toThis Rule**（添加到此规则）。

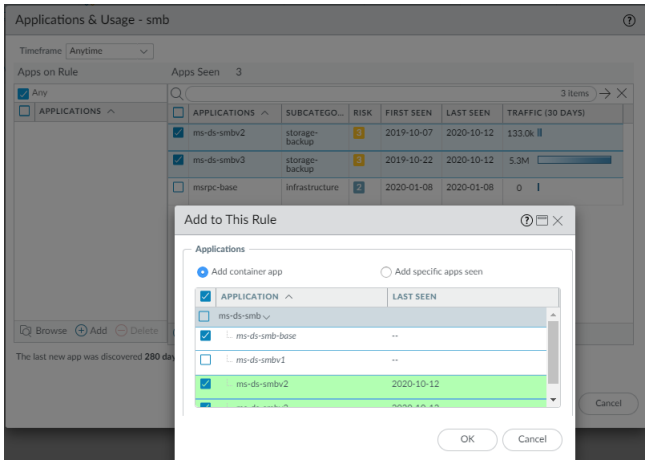
     例如，如果您决定不允许 msrpc-base，而仅选择 ms-ds-smbv2 和 ms-ds-smbv3 并 **Add to This Rule**（添加到此规则），策略优化器会在容器应用程序中显示相关应用程序（ms-ds-smb，带灰色阴影），并通过添加添加容器应用及其所有当前和未来的应用程序，提供未来证明规则的机会：



     带绿色阴影的应用程序是规则中发现的应用程序。无阴影的应用程序属于同一容器应用程序，但没有在规则中发现。
  2. 您可以允许所有应用程序或选择要允许的应用程序。

     要允许所有容器应用及其所有当前和未来的应用程序，请单击 **OK**（确定）。**Apps on Rule**（规则中的应用程序）显示所选的应用程序。单击 **OK**（确定）以转换规则。

     要仅允许所选的应用程序，请取消选择不需要的应用程序。如果取消选择容器中的应用程序，则也会取消选择容器应用程序，因此，它不会自动允许其子应用。



3. 单击 **OK**（确定）。**Apps on Rule**（规则中的应用程序）显示所选的应用程序。
4. 单击 **OK**（确定）以转换规则。
5. 将 **Service**（服务）设置为 **application-default**，从而禁止所有规避和恶意应用程序使用此端口。

30 天后开始转换的规则

在监控生产流量 30 天后，您可以安全地开始将基于端口的其他规则转换为基于 App-ID 的规则，同时清理规则库。一个好的起点是清理未使用的规则以缩小攻击范围。然后，开始在外围使用出站 Internet 访问（端口 80/443）规则将规则转换为基于 App-ID 的规则，因为该规则可能会比任何其他规则发现更多应用程序的更多流量，这也意味着它具有最大的风险。

在开始转换规则之前先安装最新的内容更新，确保 PAN-OS 设备上具有最新的应用程序签名。

策略优化器提供了很多直观的方法来对要转换的规则进行排序、筛选和确定转换优先级。删除未使用的规则并将 Web 访问规则转换为基于 App-ID 的规则后，您选择优先转换的规则取决于业务和安全要求。以下部分提供了使用简单但功能强大的排序和筛选选项来识别在前 30 天之后要转换和确定优先级的规则的思路和方法：

- 移除未使用的规则
- 转换最稳定的规则
- 转换 Internet 访问规则
- 转换监控最多流量的规则
- 转换在一段时间内发现的少数应用程序的规则

移除未使用的规则

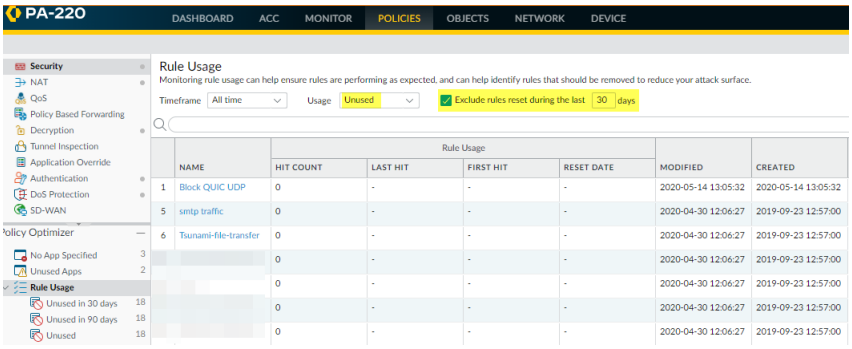
迁移的规则库通常包含不使用的规则，因为没有应用程序流量与这些规则匹配。不使用的规则会使规则库混乱并为攻击者提供攻击途径。请删除这些规则，以便清理规则库和缩小攻击范围，或对其进行修改，以便将其应用于应用程序流量并在规则库中提供合法用途。

由于各种原因，可能存在不使用的规则。例如，企业曾经用来监管服务和应用程序的规则在被其他应用程序替换后，可能仍位于规则库中。位于未使用的规则之前的规则可能会控制应用程序，否则该应用程序可能与未使用的规则匹配。在某些情况下，未使用的规则是由已从公司离职的管理员创建的旧规则，而当前管理员并不了解规则的意图。

查看您选择的任何 **Timeframe**（时间范围）内的规则（**Policies**（策略）> **Security**（安全）> **Policy Optimizer**（策略优化器）> **Rule Usage**（规则使用情况））。将 **Usage**（使用情况）设置为 **Unused**（未使用）以筛选出发现了应用程序流量的规则。

STEP 1 | 确定未使用的规则。

在 **Policies**（策略）> **Security**（安全）> **Policy Optimizer**（策略优化器）> **Rule Usage**（规则使用情况）中，将 **Timeframe**（时间范围）设置为 **All time**（全部），将 **Usage**（使用方法）设置为 **Unused**（未使用）（仅显示命中计数为零的规则），并 **Exclude rules reset during the last 30 days**（排除最后 30 天内重置的规则）（防止显示最近重置的规则，这些规则可能在过去几天内没有发现流量，但可能会在较长的时间段内发现流量）。结果是未在所选 **Timeframe**（时间范围）内未发现应用程序流量的规则列表。



STEP 2 | 评估没有发现流量的规则，并确定是否需要这些规则，或者是否可以将其禁用。

在本例中，该企业过去使用 Tsunami 传输文件，但调查显示该企业不再使用 Tsunami，因此，没有理由继续允许网络上的 Tsunami 应用程序流量。

STEP 3 | 请 **Disable**（禁用）（或 **Delete**（删除））该规则。

在 **Policies**（策略）> **Security**（安全）中，选择 Tsunami 文件传输规则，并 **Disable**（禁用）或 **Delete**（删除）该规则。

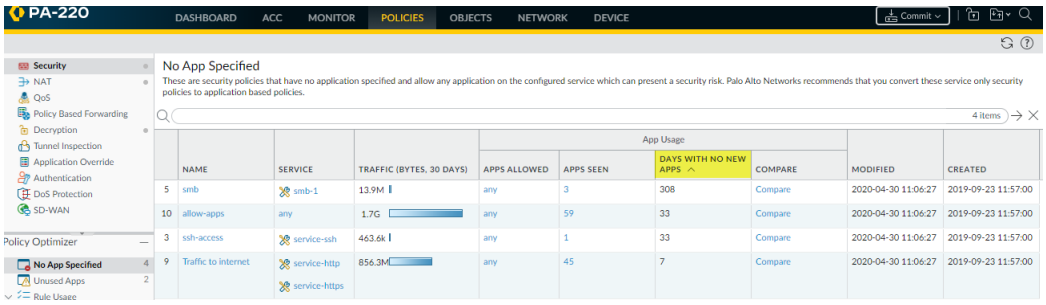
禁用该规则更加安全，即使它不会发现任何流量，但这样可以防止万一最后发现您的企业需要该应用程序。（如果您在调查企业是否使用某个应用程序时没有考虑季度或年度事件，或者如果仅定期访问网络的承包商或合作伙伴的流量需要该应用程序，也可能会发生这种情况。）经过一段合理的时间后，请删除之前禁用的未使用规则。

转换最稳定的规则

转换在合理的时间段内没有发现新应用程序的基于端口的规则，这意味着规则已稳定，并且不太可能发现新的应用程序。克隆这些规则，确保以后有更多应用程序与规则匹配时，基于端口的规则在必要时作为安全保障保留在规则库中。

当您评估是否认为新应用程序符合规则时，请考虑仅用于季度、年度和其他定期事件的应用程序。

STEP 1 | 在 **Policies**（策略）> **Security**（安全）> **Policy Optimizer**（策略优化器）> **No App Specfied**（未指定应用程序）中，对规则进行排序（降序），将 **Days with No New Apps**（无新应用的天数）的数量最大的规则排在列表的顶部。

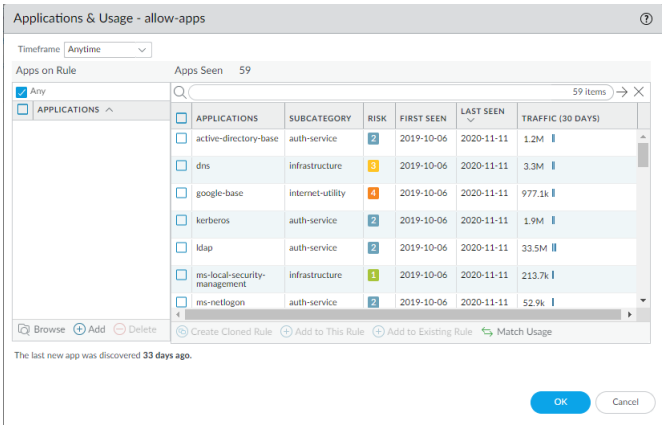


前三个规则已经超过 30 天没有发现新的应用程序，并且是转换为 App-ID 的候选项。（转换监控一周后常见应用程序的简单规则介绍具有少量 **Apps Seen**（发现的应用程序）的转换规则，如 SMB 规则，因此，该示例主要讲解允许应用规则。）

检查 *Modified*（修改）日期，因为长时间未修改的规则也可能更稳定。最近修改的规则可能没有发现可能匹配规则的所有应用程序。

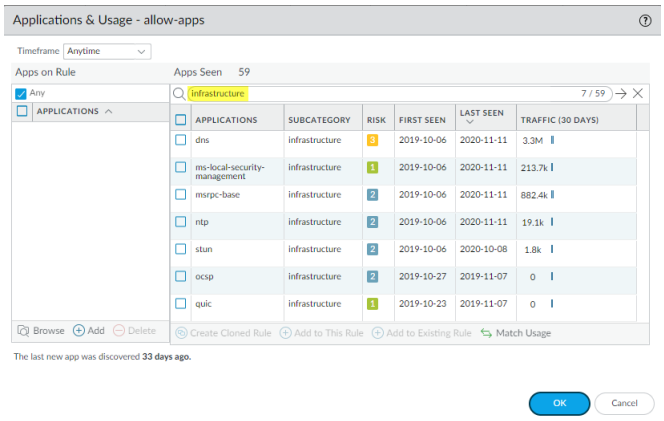
由于在规则中发现多个应用程序，因此要克隆规则，而不是将其直接转换为基于 App-ID 的规则。

STEP 2 | 单击 **Apps Seen**（发现的应用程序）的数字，打开 **Applications & Usage**（应用程序和使用情况）对话框。



STEP 3 | 排序并筛选在规则中 **Apps Seen**（发现的应用程序），以确定如何处理应用程序。

按子类别排序或筛选有助于了解在发现多个应用程序的规则监控的流量。例如，您可以按基础架构子类别进行筛选，以查看所有基础架构应用程序并克隆基于 App-ID 的规则来控制它们。



STEP 4 | 按照转换 Internet 访问规则中的步骤 4 到步骤 7 创建克隆规则，以控制要以类似方式处理的应用程序的每个子类别（或相关子类别）。

转换 *Internet* 访问规则

Internet 访问规则控制端口 80 (HTTP) 和端口 443 (HTTPS) 的流量。该规则通常会发现最大数量的应用程序以及最大的流量（以字节计）。基于端口的 Internet 访问规则可能允许您不希望在网络上出现的应用程序，并将其暴露给攻击。通过将基于端口的 Internet 访问规则转换为一组基于应用程序的规则，控制并安全地启用在这些端口上允许的应用程序。为此，您需要了解公司为业务用途而阻止哪些应用程序以及为其他目的而容忍哪些应用程序。

一种良好的转换方法是将需要在同一规则中进行类似处理的应用程序分组，而不是为每个应用程序创建单独的规则，这样有助于防止规则库变得臃肿。使用策略优化器按应用程序子类别对规则中发现的应用程序进行排序，以便您可以查看特定子类别的规则中的所有应用程序，选择您的业务使用的应用程序，然后克隆规则以控制这些应用程序。策略优化器提供了许多排序和筛选选项来组织和分析在规则中发现的应用程序。

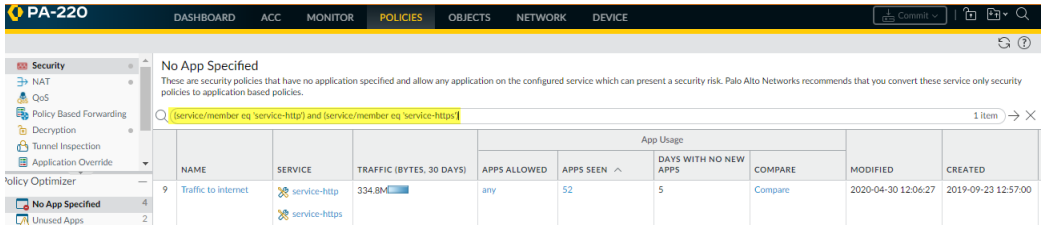
克隆规则（而不是直接转换）可确保应用程序可用性。克隆规则会保留基于端口的原始规则，并将克隆的基于应用程序的规则直接放在安全规则库中基于端口的规则之上。从基于端口的原始规则为需要以不同方式处理的应用程序组创建不同的 Internet 访问规则，而不会有应用程序可用性的风险。轻松查看哪些应用程序与克隆规则匹配，以及哪些应用程序筛选到基于端口的原始规则，然后根据需要调整规则。如果时间足够长，您确信已经考虑了业务所需的所有应用程序，但您希望允许的应用程序中没有一个与基于端口的规则匹配，则可以禁用（或删除）该基于端口的规则，这样可以完成转换，同时也没有应用程序可用性风险。

使用相同的方法转换发现更多常见应用程序的其他规则。在转换 Internet 访问规则后，使用 **Policies**（策略）> **Security**（安全）> **Policy Optimizer**（策略优化器）> **No App Specified**（未指定应用程序）信息帮助确定要转换的规则的优先级。例如，您可以按过去 30 天内 **Apps Seen**（发现的应用程序）最多和流量最大（**Traffic (Bytes, 30 days) [流量（字节，30天）]**）的组合来优先转换最常用的规则，也可以看一下 **Days with No New Apps**（无新应用的天数）和 **Modified**（修改）日期，以查找发现了很多应用程序，但也更稳定的规则。

该示例介绍如何克隆从基于端口的 Internet 访问规则控制常规业务应用程序的基于应用程序的规则。使用同一克隆过程为任何基于端口的规则发现的不同子目录和单个应用程序安全地创建基于应用程序的规则。

STEP 1 | 导航至 **Policies**（策略）> **Security**（安全）> **Policy Optimizer**（策略优化器）> **No App Specfied**（未指定应用程序）并找到控制 Internet 访问权限的基于端口的规则。

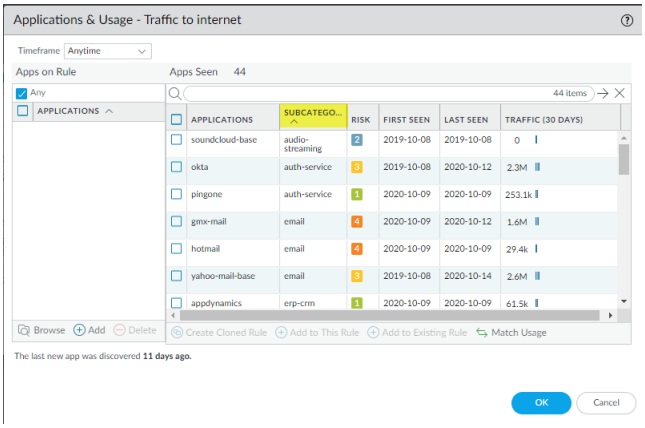
使用筛选器 **(service/member eq 'service-http') and (service/member eq 'service-https')** 找到使用 **service-http** 和 **service-https**配置的基于端口的规则，即 Internet 访问权限规则。



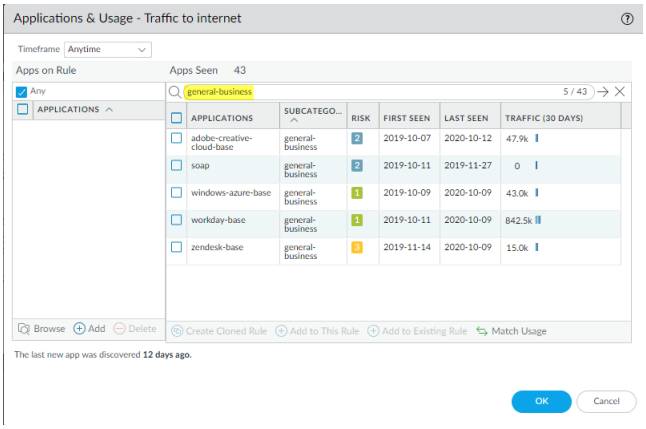
STEP 2 | 单击 **Compare**（比较）或 **Apps Seen**（发现的应用程序）的数字，打开 **Applications & Usage**（应用程序和使用情况）对话框。

STEP 3 | 按应用程序子类别对 **Apps Seen**（发现的应用程序）排序，以便将可能适合在同一安全策略规则中控制的类似应用程序进行分组。

按 **Subcategory**（子类别）排序，以便对规则发现的应用程序分组：

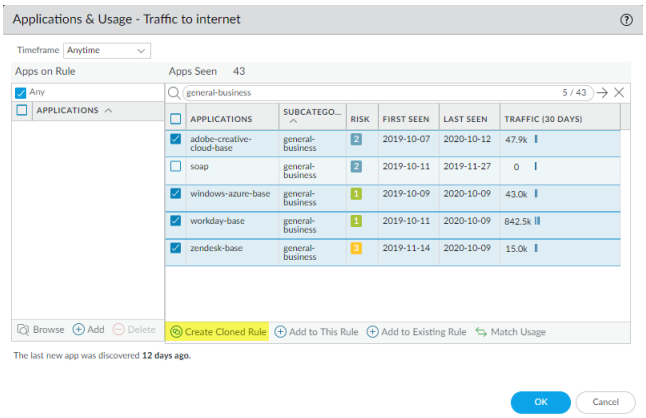


您还可以按特定子类别进行筛选，以便仅查看属于该子类别的应用程序。在本示例中，要创建基于 App-ID 的规则来控制常规业务应用程序，请筛选以仅查看该规则发现的常规业务应用程序：



STEP 4 | 选择要允许的应用程序，然后选择 **Create Cloned Rule**（创建克隆规则），以便从基于端口的规则克隆新的基于应用程序的规则。

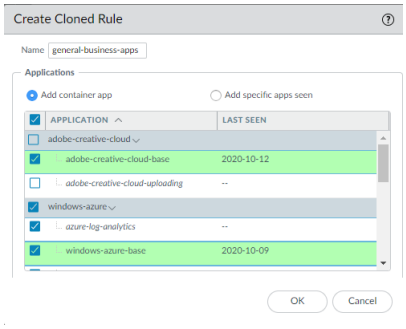
在本示例中，该公司使用了四个应用程序，但其中任何一个应用程序的使用时间都不够长。您可以在 **Last Seen**（上次查看）和 **Traffic (30 Days)**（流量（30 天））列中查看。基于使用情况和公司认可的应用程序，该公司选择不允许不需要使用的应用程序。



STEP 5 | 在 **Clone**（克隆）对话框中，选择与要允许的与每个容器应用关联的应用程序。

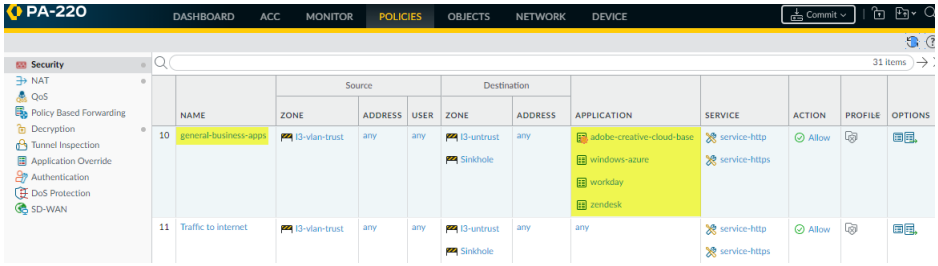
为新规则指定一个描述其用途的 **Name**（名称）— 本例中为 general-business-apps。确定是否只允许每个容器应用中的特定应用程序，或者是否要允许容器应用。如果允许容器应用，则会允许容器中的所有应用程序。如果将新应用程序添加到容器应用，则可以通过自动允许新应用程序，在未来验证规则，这有助于确保应用程序可用性。默认情况下会选择所有应用程序。容器应用带灰色阴影，规则发现的应用程序带有绿色阴影，容器应用中规则未发现的应用程序用斜体显示（没有阴影）。

在本示例的示意图中，您可以看到带灰色阴影的容器应用“adobe-creative-cloud”和“windows-azure”，在此规则中发现的带绿色阴影的应用程序（“adobe-creative-cloud-base”和“windows-azure-base”），以及以斜体显示的在规则中未发现的两个应用程序（“adobe-creative-cloud-uploading”和“azure-log-analytics”）。该示例表明，已取消选中应用程序“adobe-creative-cloud-uploading”，这也会自动取消选中其容器应用（“adobe-creative-cloud”），而保持选中所有“windows-azure”应用程序，因此会保持选中“windows-azure”容器应用。



如果不希望用户访问特定应用程序，则取消选中该应用程序。但是，如果将新应用程序添加到“adobe-creative-cloud”容器应用中，防火墙将不会自动允许它们，因为不会选中容器应用。相反，如果将新应用程序添加到“windows-azure”容器应用中，防火墙将自动允许它们，而这会在未来验证规则。

STEP 6 | 单击 **OK**（确定）以返回“安全策略规则使用情况”选项卡，然后再次单击 **OK**（确定）以创建规则。在安全策略规则库（**Policies**（策略）> **Security**（安全））中，防火墙将规则置于基于端口的规则上。



如果选择容器应用，则策略优化器仅将容器应用添加到规则中，因为它们包含所有应用程序。“adobe-creative-cloud-base”的红色齿轮表示这是个别应用程序，而不是容器应用。

STEP 7 | 单击规则 **Name**（名称）或 **Service**（服务）并将 **Service**（服务）更改为 **application-default**（应用程序默认），以防止规避应用程序在非标准端口上获取访问权限。

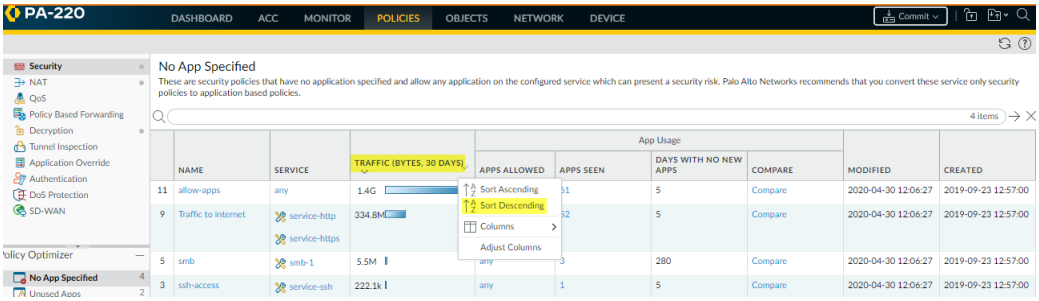
STEP 8 | 当您需要允许其他认可的常规业务应用程序时，请将其添加到 general-business-apps 规则中，如果您不再需要使用它们，则从该规则中将其删除。

转换监控最多流量的规则

对过去 30 天内监控的流量最多的规则（**Traffic (Bytes, 30 days)** [流量（字节，30天）]）进行排序，以显示当前最活跃的规则。（时间范围较长可能会产生误导，因为它们具有较大的累积总数，即使没有再监控到很多流量，它们也会排在列表的顶部。）将这些规则转换为基于 App-ID 的规则可以保护您所需的最大流量。

如果有多个规则看到大量流量，请使用 **Policies**（策略）> **Security**（安全）> **Policy Optimizer**（策略优化器）> **No App Specified**（未指定应用程序）信息帮助确定优先转换哪些规则。例如，您可以优先排列 **Apps Seen**（发现的应用程序）最多的规则（可能是风险最大的规则）或 **Days with No New Apps**（无新应用的天数）最多的规则，以及 **Modified**（修改）日期最近的规则（最稳定的高流量规则）。

STEP 1 | 在 **Policies**（策略）> **Security**（安全）> **Policy Optimizer**（策略优化器）> **No App Specified**（未指定应用程序）中，按 **Traffic (Bytes, 30 days)**（流量（字节，30天））的降序排列规则，将最近的活跃规则放在列表顶部。



STEP 2 | 选择要开始转换的规则并单击 **Apps Seen**（发现的应用程序）的数字。

STEP 3 | 在 **Applications & Usage**（应用程序和使用情况）对话框中，排序并筛选通过该规则 **Apps Seen**（发现的应用程序），以确定如何处理应用程序。

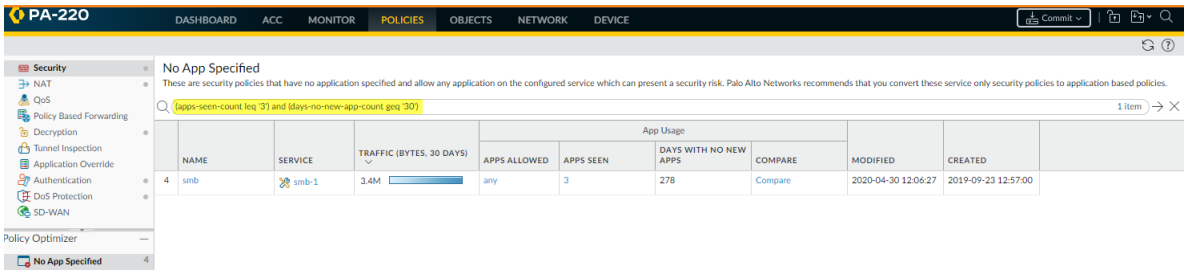
按应用程序子类别排序或筛选，以对可能需要类似处理且可在一个基于应用程序的规则中控制的应用程序进行分组。按 **Traffic (30 days)**（流量（30天））排序，查看各个应用程序的最新流量，以确定当前最活跃的应用程序的优先级。

STEP 4 | 按照转换 Internet 访问规则中的步骤 4 到步骤 7 创建克隆规则，以控制要以类似方式处理的应用程序的每个子类别（或相关子类别）。

转换在一段时间内发现的少数应用程序的规则

Apps Seen（发现的应用程序）相对较少以及在足够长的时间内未发现新应用程序的规则可能很容易转换，相对稳定且易于使用筛选器识别。

STEP 1 | 在 **Policies**（策略）> **Security**（安全）> **Policy Optimizer**（策略优化器）> **No App Specfied**（未指定应用程序）中，筛选规则以仅显示 **Apps Seen**（发现的应用程序）数量较少的规则以及在特定时间段内没有发现任何应用程序的规则。



以下示例筛选发现了三个或更少应用程序的规则：`apps seen count leq` ‘3’；至少至少 30 天未发现任何应用程序的规则：`days no new app count geq` ‘30’。

STEP 2 | 选择要转换的规则并单击 **Apps Seen**（发现的应用程序）的数字。

STEP 3 | 在 **Applications & Usage**（应用程序和使用情况）对话框中，决定是否要允许所有应用程序以及它们是否应该在同一规则中 — 即，确定应用程序在访问权限和安全性方面是否需要类似的处理。

如果您想要允许所有应用程序且这些应用程序需要类似的处理，则可以 **Match Usage**（匹配使用情况）并使用新的基于 App-ID 的规则替换基于端口的规则。

如果要允许所有应用程序，但这些应用程序需要不同的处理，则为需要不同处理的每一组应用程序克隆规则。例如，如果基于端口的规则允许三个应用程序，其中两个是电子邮件应用程序，另一个是基础架构应用程序，则可能需要为电子邮件应用程序克隆一个规则，为基础架构应用程序克隆另一个规则。

如果您想要允许某些应用程序并拒绝其他应用程序：

- 为想要保留的应用程序克隆一个或多个规则，并监视基于端口的原始规则，以确保您不想保留的应用程序是仅有的符合该规则的应用程序。如果经过足够长的时间后，您确信没有要允许的应用程序与基于端口的规则匹配，则可以将其禁用或删除。转换 Internet 访问规则中的步骤 4 到步骤 7 显示了如何创建克隆规则。
- 如果您确信自己知道要允许哪些应用程序以及要阻止哪些应用程序：
  - 如果您想要允许的应用程序需要类似的处理，请通过 **Add to This Rule**（添加到此规则），使用仅允许添加到规则中的应用程序的基于应用程序的规则来替换基于端口的规则。除非在其他规则中允许，否则未添加到此规则的应用程序将被阻止。
  - 如果要允许的应用程序需要不同的处理，请从基于端口的规则克隆要允许的应用程序的基于应用程序的规则。如果您仍然确信可以阻止剩余的应用程序，则可以禁用（或删除）基于端口的规则。

采用安全最佳实践的后续步骤

完成第一步后，也就是将基于端口的规则转换为基于应用程序的规则后，请考虑按照以下步骤来加强安全策略规则库和提高网络安全性：

- 使用 Expedition 的规则扩充功能，它使用机器学习来检查和合并策略配置。
- 定期运行最佳实践评估 (BPA) 来测量实现 App-ID 采用目标的进度并确定其他弱点。实现目标后，使用 BPA 来确定可以继续提高采用率并进一步保护网络的区域。
- 策略优化器将基于端口的规则转换为基于 App-ID 的规则，但不会更改有关规则的任何其他内容。将旧版规则转换为基于 App-ID 的规则后，请收紧规则以缩小攻击范围和提高可见性：
  - 将 **Service**（服务）设置为 **application-default**（应用程序默认）以防止应用程序使用非标准端口。对于内部自定义应用程序，请定义默认端口，然后应用 **application-default**（应用程序默认）。
  - 对于 Web 应用程序，请在外围（Internet 网关）使用 URL 筛选类别来防止访问风险网站。
  - 配置 User-ID 以控制可访问应用程序的用户。
  - 配置日志转发以集中来自多个 PAN-OS 设备的日志，对于特定警报，向特定管理员或组发送电子邮件警报，并保留日志以进行历史分析。
  - 为防病毒软件、反间谍软件、漏洞保护、文件阻止和 WildFire 分析配置最佳实践安全配置文件，并将它们应用于 App-ID 安全策略规则。
  - 考虑使用 Iron-Skillet 模板（从 GitHub 上下载）作为开始，并引导最初的最佳实践配置。
- 维护 App-ID 部署。为新应用程序（包括内部自定义应用程序）添加规则时，请创建基于 App-ID 的规则，以帮助保持网络安全。不要恢复使用基于端口的规则，这些规则不会让您了解应用程序流量，也不会允许您检查和控制它们。在 PAN-OS 管理员指南中了解关于 App-ID 的更多信息。
- 在收紧安全策略规则库时，请考虑对网络应用其他保护措施，例如解密流量以及 DoS 和区域保护的最佳实践。

如果您需要关于将旧版设备配置迁移到 Palo Alto Networks 设备的帮助，请联系 Palo Alto Networks 专业的服务小组，他们有着丰富的迁移经验，可以帮助您实现成功迁移并成功转换为 App-ID。