paloalto TECHDOCS

安全策略最佳实践

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 5, 2023

Table of Contents

安全策略最佳实践

安全策略决定了您在网络上允许哪些流量以及如何处理这些流量。安全策略最佳实践将您允许的流量限制为仅限于您的业务所需的经批准的流量和员工允许的流量。这可以减少攻击面，并有助于保护您的网络和业务资产。本文档的观点是，无论您的业务是安全第一，还是将关键任务可用性放在首位，该如何才能获得最佳的网络安全。

安全策略最佳实践遵循最小权限原则，这意味着只有需要访问特定应用程序、数据和基础设施的人员才能获得访问权限，并对流量进行适当的解密、检查和记录，以保护资产、知识产权和其他对您的业务至关重要的资产。所有其他访问权限都会增加风险，而不会实现业务目标。

本书包含简化的分步最佳实践，介绍如何：

- Pod 安全策略
- 部署安全策略
- 维护安全策略

需要配置或有深入概念信息的步骤包括指向相应文档的链接，以获取详细信息。在产品管理员指南、版本说明、升级指南、互连指南等中了解 Palo Alto Networks 产品的特性、功能和操作，这些指南可在技术文档主页上找到：

- PAN-OS
- Panorama
- Panorama Managed Prisma Access（包括 GlobalProtect 应用文档）
- Cloud Managed Prisma Access
- Prisma SD-WAN
- 云端交付的安全服务
- 云身份引擎
- GlobalProtect
- VM-SERIES
- CN-Series
- Cortex 帮助中心
- 防火墙和设备硬件指南

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。

规划安全策略最佳实践

在创建最佳实践安全策略规则之前，请确保您了解规划安全网络的最佳实践，尤其是零信任网络访问 (ZTNA) 原则。安全策略定义您允许和阻止的流量。但是，需要一套全面的工具和服务来完全保护您的网络，包括提供以下功能的工具：

- 可见性，例如解密、App-ID、User-ID 和设备 ID。
- 高级威胁防护，例如漏洞防护、防病毒、反间谍软件、文件阻止、沙箱、数据丢失防护 (DLP)、DNS 安全等。
- 用于控制非托管设备的 IoT Security 和用于控制 SaaS 应用程序的 SaaS Security （下一代 CASB）。

确保您拥有适当的工具集来保护您的网络并在安全策略中使用。

STEP 1 | 您无法防御看不见的威胁。根据法律合规性、当地法规、隐私法规和业务考虑因素，尽可能解密所有流量，以获得流量可见性，从而检查流量并防止威胁。对于 SSL 转发代理（出站）解密，请先实现 User-ID 和 URL 过滤，以便您可以有效地定位解密。由于技术原因（例如固定证书、客户端身份验证和物联网设备中的嵌入式证书），某些流量无法解密。

如果不解密流量，防火墙就无法精细地识别应用程序。例如，防火墙可以看到容器应用程序是 facebook，但看不到功能应用程序，因此您不知道也无法控制用户是否在 Facebook 上上传、下载、发帖等。防火墙也无法查看和检查有效负载，因此您无法防御恶意内容。为了充分利用其他订阅并获得最佳保护，您必须解密流量以了解该流量。

解密不需要许可证，但要解密出站流量，请添加高级 URL 过滤许可证，以便您可以采用精细的解密方法，并轻松选择要解密和不解密的流量类型。URL 过滤使您能够排除因法律、个人信息、监管或其他原因而不应解密的类别。URL 过滤还使您能够阻止用户访问恶意网站。

此外，解密入站流量以保护关键服务器，并解密 SSH 代理流量以防止恶意管理流量。

遵循解密最佳实践来准备、部署和维护解密。

STEP 2 | 从最小权限访问和零信任网络访问的视角查看规划和部署流程。

了解谁需要使用哪些应用程序来访问哪些数据和哪些基础设施。这使您能够构建安全策略规则，仅允许出于业务目的需要访问的人员仅访问必要的数据和基础设施，同时阻止所有其他访问。

使用安全策略中可用的属性来定义最小权限访问：用户、设备、应用程序、源和目标、服务和 URL（对于出站流量，启用解密，以便防火墙可以查看每个功能应用程序，而不仅仅是容器应用）。

STEP 3 | 为您的企业获取适当的订阅，以实现最佳的威胁预防和安全态势。

- 高级 URL 过滤 - 云提供的服务，可实现安全的网站访问、保护用户免受危险网站的侵害，并帮助防止凭证网络钓鱼攻击。
- 高级威胁防护或有效的旧版威胁防护 - 云交付的高级威胁防护使用内联深度学习和机器学习模型来实时执行规避威胁和第 1 天命令与控制 (C2) 威胁，并包括标准威胁防护的所有功能。标准威胁防护可防止 C2、恶意软件和漏洞利用。

  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。

  遵循威胁内容更新的最佳实践，以确保您拥有最新的保护。

- DNS 安全 -（必须购买高级威胁防护或拥有有效的旧版威胁防护许可证和 DNS 安全许可证才能激活）云提供的服务，可识别和阻止 DNS 流量中的威胁，并防止连接到恶意 DNS 站点，并不断更新为防止基于 DNS 的新型攻击。
- 企业数据丢失防护 (DLP) - 云交付的服务，可保护所有企业网络、云和用户中的数据，并确保遵守数据安全法规。
- Cortex Data Lake (CDL) - 基于云的日志存储，可根据日志量进行扩展，并从下一代防火墙、Panorama、Prisma Access 和 Cortex XDR 中提取日志。大多数 Cortex 应用程序使用 CDL 来访问、分析和报告记录的网络数据。
- WildFire - 基于云的分析环境或私有分析环境，可识别已知和未知（新）恶意软件并生成防火墙用于识别和阻止恶意流量的签名。
- SaaS Security - 云交付的服务，可使用独立或捆绑的许可证来保护您认可的 SaaS 应用程序：
  - 数据安全许可证包括 SaaS Security API 和企业 DLP。
  - SaaS Security Inline 附加许可证与 CDL 配合使用，可以发现和控制网络上的所有 SaaS 应用程序（包括遮蔽 IT 应用程序），并向防火墙管理员启用 SaaS 策略建议。
  - 企业 DLP 可防止 SaaS 应用程序中的数据丢失。
- IoT Security - 发现并保护网络上的 IoT 设备，并向防火墙管理员启用自动 IoT 策略规则建议。遵循 IoT Security 最佳实践进行规划、部署和监控。
- GlobalProtect - 提供免费 VPN 功能之外的功能，包括 GlobalProtect 移动应用程序、HIP 检查、无客户端 VPN等。

STEP 4 | 检查网络分段计划。

对于 Panorama Managed Prisma Access，实际上只有两个区域：信任区域和不信任区域，并且会将所有 Panorama 区域映射到 Prisma 信任区域或 Prisma 不信任区域。

在 Panorama 和防火墙上，如果区域不够详细并且包含需要不同安全处理的设备、用户和应用程序，请考虑重新架构您的区域，以更详细的方式对网络进行分段。将需要类似处理的用户、应用程序和设备放置在同一区域中。小区域比大区域更容易防御。

在某些云环境中，架构可能会限制您可以配置的区域数量。

遵循 DoS 和区域保护最佳实践来防止泛洪攻击并保护每个区域中的设备和防火墙缓冲区。

对于Cloud Managed Prisma Access，基于身份进行微分段。

STEP 5 | 定义您需要允许哪些应用程序用于商业目的（认可的应用程序）以及允许哪些应用程序用于其他目的（容忍的应用程序）。

在安全策略中使用 App-ID（无需订阅）来识别容器应用程序及其功能应用程序（例如，不仅是“facebook”，还包括“facebook-post”、“facebook-download”等）。如果您使用 SaaS Security，请使用 App-ID Cloud Engine (ACE) 来识别云应用程序（需要 SaaS Security 订阅）。

基于规则的条件，防火墙允许在安全策略规则中指定的应用程序，这些应用程序的 **Action**（操作）为 **Allow**（允许）；以及在规则中阻止的应用程序，这些应用程序的 **Action**（操作）会拒绝、丢弃或重置流量。流量必须满足规则的所有条件才能匹配该规则。如果应用程序没有匹配任何规则，则安全策略规则库底部的两个默认规则将控制流量。区域间（源和目标位于不同区域）流量默认被拒绝。默认情况下允许区域内（源和目标位于同一区域）流量。

传达访问策略，以便员工了解为什么他们无法访问某些应用程序。

STEP 6 | 识别所有用户。在安全策略中控制谁有权访问哪些应用程序和设备，以确保一致的策略遵循网络中任何位置的每个用户。

User-ID（无需订阅）结合多个来源的用户信息来识别网络上的所有用户。为了帮助确保用户标识一致并在整个网络中扩展，请使用 Cloud Identity Engine (CIE)（无需订阅）作为 User-ID 的聚合单一源。CIE 从整个网络的来源收集并同步用户数据。所有防火墙都从 CIE 提取完全相同的用户信息，无论它们是在园区内还是在云中。CIE 还与大多数主要身份提供商 (IdP)（例如 Okta、Azure AD、PingID 等）结合提供身份验证。

在 *PAN-OS 10.2* 及更早版本中，*CIE* 提供目录同步 *(DSS)* 和云身份验证 *(CAS)* 服务。从 *PAN-OS 11.0* 开始，您还可以使用 *CIE* 作为重新分发点。

配置用户组时，请考虑谁需要出于相同的业务目的以相同的方式访问相同的资源，并遵循用户组映射的最佳实践和动态用户组 (DUG) 的最佳实践。

如果可能，请在始终开启模式下使用 GlobalProtect VPN，以实现最高的安全性和可靠的用户识别。使用 GlobalProtect 进行远程访问并通过内部网关收集 User-ID 信息，无论您的用户位于何处。

STEP 7 | 计划将适当的安全配置文件或安全配置文件组附加到允许流量的每个安全策略规则。（如果规则阻止流量，防火墙不会检查被阻止的流量。）

安全配置文件组是为特定目的而调整的配置文件组，您可以将其应用于安全策略规则，而不是单独应用每个配置文件。这可以节省时间并有助于防止意外的错误配置。

STEP 8 | 规划如何存储日志（在 CDL 中，在日志收集器上等），以及针对不同类型和严重性的日志事件通知哪些管理员。规划足够的日志存储容量，以便能够在事件发生后对其进行调查。

STEP 9 | 使用单一管理窗格（例如 Panorama 或 Cloud Managed Prisma Access） 来管理部署，以实现更轻松、更一致的安全性。

STEP 10 | 遵循管理访问最佳实践，确保 Panorama 和防火墙管理员的最小权限访问。

STEP 11 | 第 1 天配置可在 客户支持门户（工具 > 运行第 **1** 天配置）上找到，并且需要支持登录，这些模板提供与用例无关的配置模型，以启动您的最低权限访问路径。第 1 天配置可帮助您立即实施基本网络安全最佳实践，包括动态更新、安全配置文件、日志记录等关键元素。

部署安全策略最佳实践

部署安全策略最佳实践包括：

- 安全策略规则最佳实践 - 专注于安全策略规则构建的各个方面，从哪些用户可以以何种方式访问哪些应用程序和资源，到应用有助于保护流量免受恶意软件侵害的威胁配置文件。
- 安全策略规则库最佳实践 - 重点关注规则库中安全策略规则的顺序以及它如何影响您允许和阻止的流量。
- Policy Optimizer 最佳实践 - 专注于使用 Policy Optimizer 来加强和维护规则库。
- App-ID Cloud Engine 最佳实践 - 重点介绍如何在安全策略中使用云 App-ID 以及如何自动将新的云 App-ID 添加到规则库。（App-ID Cloud Engine 需要 SaaS Security Inline 订阅。）
- 策略建议最佳实践 - 重点关注 SaaS 策略推荐和 IoT 策略推荐。（SaaS 策略建议需要 SaaS Security Inline 订阅，而 IoT 策略建议需要 IoT Security 订阅。）

在规划和部署时，请记住以下原则：

- 最小权限访问原则；仅使用正确的应用程序将访问限制为正确的人员，仅从正确的来源到正确的目的地。
- 遵循解密最佳实践。根据您的业务考虑、本地和隐私法规以及法律合规性允许解密尽可能多的流量，以获得流量的最大可见性，以便您可以检查和控制它。对于 SSL 转发代理（出站）解密，请先实现 User-ID 和 URL 过滤，以便您可以有效地定位解密。

  对于出站解密，请获取高级 *URL* 过滤许可证，以便当解密暴露恶意网站时，*URL* 过滤可以阻止对其的访问。

  由于固定证书、客户端身份验证、物联网设备中的嵌入证书等技术原因，某些流量无法解密。
- 检查两个方向的所有流量是否存在威胁。绝对不信任任何流量。
- 使用动态地址组 (DAG)、外部动态列表 (EDL)和虚拟机监控功能尽可能实现自动化，以帮助确保安全策略保持最新状态。

  对于基于日志事件的用户和设备，使用自动标记自动执行安全操作。自动标记使您能够在日志事件发生时自动执行操作，例如，隔离可能受感染的设备或强制用户使用 MFA 身份验证。

- 避免配置膨胀：
  - 重用安全配置文件和配置文件组、标签、应用程序组、应用程序过滤器、用户组和地址组等对象。在 Panorama 上，使用共享对象以避免为多个设备组配置相同的对象。
  - 在将新策略规则添加到规则库之前，请检查现有规则，看看是否可以将新应用程序、用户或设备添加到现有规则，而不是创建多个类似规则。

    查看现有规则是否相同，除了以下对象之一：源区域、目标区域、源 IP 地址、目标 IP 地址、应用程序、服务端口或用户。如果这些对象中只有一个不同，请将新对象添加到现有规则，而不是创建新规则。

    例如，您想要允许新的会计应用程序。当您查看现有规则库时，您会发现不同会计应用程序的规则，该规则允许相同的用户组使用应用程序的默认端口从相同的源访问相同的目标。无需为新应用程序编写新规则，只需将新应用程序添加到现有规则即可。

    

    此方法对于巩固现有规则也很有效。
  - 对于出站流量，根据 URL 类别为需要相同安全处理的多个应用程序创建一条规则。例如，要允许所有低风险金融服务流量（假设您希望以相同方式检查和记录流量），请创建指定 **financial-services**（金融服务）和 **low-risk**（低风险）URL 类别的允许规则。
  - 使用 Policy Optimizer 删除未使用的规则。
- 使用 Panorama 或 Cloud Managed Prisma Access 管理防火墙部署，以便您可以使用设备组将一致的安全策略应用于单个或一组防火墙。

  适当使用前置规则和后置规则：
  - 前置规则 - 防火墙在本地定义的规则和后置规则之前评估前置规则。（各个防火墙上本地定义的规则仅适用于这些防火墙。） 在预规则中放置适用于所有防火墙部署的策略，例如允许 DNS 和其他关键服务以及使用预定义的威胁 EDL 来阻止已知的恶意和高风险 IP 地址。
  - 后置规则 - 防火墙在预规则和本地定义的规则之后评估这些规则。

  

  在 *Panorama* 安全策略规则中，使用 ***Target***（目标）选项卡从规则中排除特定防火墙或设备组子集（***Target to all but these specified devices***（目标指向除这些指定设备之外的所有设备））。这使您能够在层次结构中的较高位置创建一个广泛的规则，而不是在层次结构的较低位置创建多个类似的规则来例外。
- 应用程序覆盖策略与第 7 层安全策略不同。除非必须，否则不要使用它，因为应用程序覆盖会删除 Palo Alto Networks 平台固有的许多安全控制。应用程序覆盖无法让您检查第 7 层流量、使用安全配置文件来保护流量免受威胁或使用 App-ID，因此会增加风险。在大多数情况下，创建自定义应用程序或使用自定义服务超时 比使用应用程序覆盖更好。

  检查现有规则库。如果您对除 SMB 或 SIP 之外的流量有应用程序覆盖规则，请将该规则转换为基于 App-ID 的规则，以便能解密和检查第 7 层的流量并预防威胁。如果规则适用于 SMB 或 SIP 流量，请确保其遵循最小权限访问原则并尽可能具有限制性。

安全策略规则最佳实践

本节介绍安全策略规则的构建，从谁可以访问哪些应用程序和资源，到应用威胁配置文件，帮助保护流量免受恶意软件的攻击。

安全策略规则定义通信匹配标准，包括应用程序、用户、设备、源和目标、URL 和服务（端口）。组合匹配条件可以为规则添加更细粒度的上下文，缩小规则的范围，并减少攻击面。匹配条件使您能够定义要使用规则控制的确切流量，并遵守零信任网络访问 (ZTNA) 原则。

安全策略规则还定义了对符合规则标准的流量采取的操作，包括是否允许或拒绝流量、日志记录和日志转发、威胁检查和调度。

创建尽可能具体的安全策略规则，以应用最低权限访问原则并对网络进行分段。

- 安全策略的关键概念 - 安全策略规则如何工作。
- 规则名称、描述、审核注释和标记 - 管理安全策略规则的最佳实践。
- 源和目的地 - 应用最低权限访问原则以锁定通信源和目的地的最佳实践。
- 应用和服务- 将应用程序添加到规则的最佳实践。
- 网站访问（URL 过滤） - 如何允许用户访问外部网站的最佳实践。
- 策略操作和其他设置 - 关于如何允许或拒绝流量以及应用 QoS 的最佳实践。
- 日志记录和日志转发 - 记录流量和转发日志以进行长期存储和分析的最佳实践。
- 安全配置文件 - 将安全配置文件应用于安全策略规则的最佳实践。

安全策略的关键概念

要创建有效的安全策略，它有助于了解有关安全策略规则的作用、它们在安全策略规则库中的工作方式、流量如何匹配规则以及规则构建的最佳实践的关键概念。

- 解密本地法规、合规性、业务要求和隐私考虑允许的所有流量。对于 SSL 转发代理（出站）解密，请先实现 User-ID 和 URL 过滤，以便您可以有效地定位解密。解密流量提供了可见性，因此防火墙可以识别功能应用程序（例如，不仅是 facebook，还有 facebook-post、facebook-download、facebook-file-sharing 等），识别网站，并应用威胁配置文件来检查和防止流量中的威胁。解密通信使您能够从威胁订阅中获得最大程度的保护和防范。
- 允许与阻止规则 - Palo Alto Networks 防火墙上的安全策略基于策略规则中的明确允许流量，并拒绝您不明确允许的所有流量（允许列表）。您不显式允许的流量将被隐式拒绝。目标是只允许您想要的应用程序、用户和设备进入网络，并让防火墙自动阻止您不想要的内容。

  当您转向基于允许列表的安全策略时，请使用阻止规则来阻止访问有风险的IP地址、网站和应用程序。基于预定义的外部动态列表 (EDL) 创建和测试阻止规则，以阻止防弹IP地址、高风

险IP地址和潜伏在其他良性应用程序类别中的已知恶意 IP 地址，并防止对恶意 URL 或域进行身份验证。使用 高级 URL 过滤功能阻止访问有风险的网站。

要特别小心文件共享应用程序，因为坏人可以使用它们来泄露数据。阻止大多数文件共享应用程序。对于您需要用于业务目的的文件共享应用程序，仅允许需要这些应用程序用于业务目的的用户访问。

为了最严格的安全性，只允许用于商业目的的应用程序。但是，大多数企业需要允许员工使用一些非业务应用程序（容忍应用程序）。考虑允许哪些可容忍的应用程序，并问问自己这些应用程序是否对组织构成任何威胁，例如上传或下载数据的能力。解密和检查尽可能多的流量，您可以为威胁。

- 安全策略规则是特定的。如果通信不符合安全策略规则中指定的所有条件，则通信不符合该规则。例如，如果规则指定了特定用户、应用程序以及源和目标，则流量必须符合所有这些条件才能与规则匹配。如果用户、源和目标匹配，但应用程序不匹配，则流量与规则不匹配。
- 安全策略规则通过定义谁有权访问哪些应用程序和基础架构来划分网络。规则通过定义源、目标、用户、设备、服务和URL来划分网络。
- 安全策略规则将所有附加的威胁防御配置文件应用于与规则匹配的通信。
- 安全策略规则位于有序规则库中（您可以选择规则的顺序）。防火墙将通信与安全策略规则进行比较，从安全策略规则库中的第一个规则开始，一直到规则库中的最后一个规则。当流量符合规则的条件时，防火墙会对流量执行规则的“操作”，而不会将流量与任何其他规则进行比较。如果没有规则与流量匹配，防火墙将丢弃该流量（隐式拒绝）。
- 在规则库中，将更具体、更精细的安全策略规则置于一般规则之上，以避免遮蔽规则。4是指包含与特定规则相同的匹配条件的广义规则在规则库中的位置高于特定规则。在这种情况下，旨在匹配特定规则的流量将首先匹配一般规则。
- 如果流量不匹配任何其他规则，则规则库底部的两个默认安全策略规则会自动丢弃不同区域之间的所有流量 (**interzone-default**)，并自动允许同一区域之间的所有流量 (**intrazone-default**)。您可以修改 interzone-default 和 intrazone-default 规则来记录流量、应用威胁检测等。如果您在规则库中较早的位置添加了拒绝所有通信的规则（本地防火墙规则或 Panorama 前置规则和后置规则），则没有通信与默认规则匹配。
- 将最低权限访问原则应用于安全策略规则构造（粒度、精确）：
  - 控制哪些管理员有权管理哪些防火墙和 Panorama 设备的哪些部分。遵循安全管理访问权限最佳实践。
  - 识别所有用户（您的网络上不应有未知用户），识别您希望允许在网络上使用的应用程序，并了解您的基础架构（用户和应用程序访问的资源）。映射出于业务目的需要访问哪些应用

程序和资源的人员，以便您的安全策略规则不允许不必要的访问。仅允许出于业务目的需要访问的用户访问业务资源和认可的应用程序，并且仅允许最低限度的访问权限。

- 允许访问您为了员工的利益而容忍的非业务应用程序。
- 在大多数情况下，使用允许规则而不是阻止规则 - 定义您希望在网络上允许哪些应用程序并隐式拒绝其余应用程序比显式阻止您不希望在网络上出现的不断增加的应用程序更准确，也更容易。
- 优化规则库以编辑未使用的应用程序的规则，并删除或禁用未使用的规则。

规则名称、描述、审核注释和标记

名称、说明、审核注释和标记字段使管理和导航安全策略规则库以及了解每个规则的作用变得更加容易。它们还可以帮助新的和有经验的管理员了解何时向现有规则添加新的应用程序、用户或用户组，以及何时创建新规则。

STEP 1 | **Name**（名称）- 说明每个规则的作用。

制定一个标准的命名约定，使用术语来方便搜索规则库。清楚地向管理员显示每个规则的功能的名称可以更容易地理解每个规则控制的流量，并使搜索任何特定规则更容易和更直观。

STEP 2 | **Description**（描述）- 描述规则的用途，以便检查规则库的任何人都能理解创建规则的原因和预期结果。

要确保所有策略都在 PAN-OS 和 Panorama Managed Prisma Access 中有描述，请在 **Panorama** > **Setup**（设置） > **Management**（管理） > **Policy Rulebase Settings**（策略规则库设置）（各个防火墙上的 **Device**（设备） > **Setup**（设置） > **Management**（管理） > **Policy Rulebase Settings**（策略规则库设置））中启用 **Require description on policies**（要求关于策略的描述）。对于没有说明的现有规则，请在下次编辑规则时添加说明。

在 Cloud Managed Prisma Access 中，确保管理员输入描述。

STEP 3 | **Tags**（标记） - 用于描述基于流的组件、基于应用程序的策略、内部服务、特定用户组的高级描述符 - 任何对您的业务有意义的内容。

标记将策略组织到组中，这使您能够基于标记筛选和搜索策略。

例如，如果创建名为 **`disabled`** 的标记并将其应用于所有禁用的规则，则可以筛选规则库并查看基于该标记的所有禁用的规则。使用相同的标记，您可以在规则库中搜索标记为 **`disabled`** 但已通过筛选 **`disabled`** 标记和 **`disabled eq no`** 重新激活的规则。

要确保所有策略在 PAN-OS 和 Panorama Managed Prisma Access 中都有标记，请在 **Panorama** > **Setup**（设置） > **Management**（管理） > **Policy Rulebase Settings**（策略规则库设置）（各个防火墙上的 **Device**（设备） > **Setup**（设置） > **Management**（管理） > **Policy Rulebase Settings**（策略规则库））中启用 **Require Tag on policies**（要求关于策略的标记）。对于没有标记的现有规则，请在下次编辑规则时添加标记。

STEP 4 | 如果策略没有标记或描述，则禁止管理员提交策略。

在 PAN-OS 和 Panorama Managed Prisma Access 中，请在 **Panorama** > **Setup**（设置） > **Management**（管理） > **Policy Rulebase Settings**（策略规则库设置）（各个防火墙上的 **Device**（设备） > **Setup**（设置） > **Management**（管理） > **Policy Rulebase Settings**（策略规则库设置））中启用 **Fail commit if policies have no tags or description**（如果策略没有标记或描述，则提交失败）。对于现有规则，如果您在下次编辑规则时未添加标记和描述，则提交将失败。

STEP 5 | **Audit Comments**（审核备注） - 跟踪规则的更改以及更改原因，以便您了解规则更改的历史记录以及更改的理由。这对于记录仅在灾难恢复情况下或在有限的基础上使用的规则特别有用。

在 PAN-OS 和 Panorama Managed Prisma Access 中，确保所有策略都包括审核备注，请在 **Panorama** > **Setup**（设置） > **Management**（管理） > **Policy Rulebase Settings**（策略规则库设置）（各个防火墙上的 **Device**（设备） > **Setup**（设置） > **Management**（管理） > **Policy Rulebase Settings**（策略规则库设置））中启用 **Require audit comment on policies**（要求关于策略的审核备注）并 specify an audit comment format（指定审核备注格式）。对于没有审核注释的现有规则，下次编辑规则时必须添加这些注释。

审核注释将永久保留在规则中。单击规则中的 **Audit Comment Archive**（审核备注存档）以查看历史记录，该历史记录无法删除。

源和目的地

控制流量来源和目的地是关于遵循最小权限访问的原则。创建安全策略规则，指定要与规则匹配的应用程序通信的确切来源和目标。允许来自应用程序不需要用于业务目的的源和目的地的规则流量增加了攻击面，从而增加了风险。将源和目的地严格限制在业务目的所需的范围内，可以减少攻击面并降低风险。

精细的源和目标控制可帮助您实现最低权限访问：

- 源区域 - 区域、地址、用户和设备、5G 安全、订户、设备和网络切片。
- 目标 - 区域、地址和设备。

尽可能使用地址组和用户组对象，而不是单个地址和用户，以减少源对象和目标对象的数量。这简化了策略，使其更容易理解。限制源对象和目标对象的总数以使规则库清晰。

STEP 1 | 在 PAN-OS 中，尽可能窄地指定源区域和目标区域，以防止对数据和应用程序进行不必要的访问。

将区域专用于特定用途（例如所有 Web 服务器的区域）可以更轻松地创建粒度策略，因为区域中的所有服务器通常都需要相同的安全策略。

Panorama Managed Prisma Access 使用两个区域：信任和不信任。将 Panorama 区域映射到 *Prisma*信任区域或 *Prisma* 非信任区域。

Cloud Managed Prisma Access 使用三个区域：信任、不信任和无客户端 *VPN*，默认情况下映射到信任区域。在许多第三方 *SD-WAN* 集成中，在日志查看器中，源区域使用远程网络的名称。

STEP 2 | 尽可能严格地指定源地址和目标地址，以防止对数据和应用程序进行不必要的访问。尽可能使用地址组而不是单个地址来简化策略。如果规则适用于区域中的所有设备，则对于入站流量，将目标地址指定为 **any**（任何），对于出站流量，将源地址指定为 **any**（任何）。

- 使用IP地址对象来引用内部系统，这样当系统IP地址更改时，更改不会影响策略。
- 在策略中使用动态地址组 (DAG)，根据日志事件和自动标记自动适应服务器角色或安全状态的更改。考虑如何对服务器进行分组并制定对您的业务有意义的标记策略。

  当发生指定的日志事件时，防火墙会根据自动标记将IP地址从一个 DAG 移动到另一个 DAG。DAG 会自动更新，不需要提交操作。这使您能够采取自动化的安全操作，例如将可能受感染的服务器或端点从允许访问关键资源的策略规则中的 DAG 移动到阻止该访问的策略规则中的 DAG（阻止设备）。
- 在具有自动化功能的数据中心环境中，当数据中心启动和关闭虚拟化服务器时，使用 DAG 控制虚拟机的访问。使用本机 XML API 或防火墙上的 VM Monitoring 代理动态注册标记。
- 在数据中心环境中，分段与自动化相结合可能会使管理单个 IP 地址变得困难。如果环境太难管理，作为最后的手段可以使用 MySQL，但这是一种不太安全的方法。
- 使用 Palo Alto Networks 预定义的外部动态列表 (EDL) 作为源或目的地，以阻止来自高风险、防弹和其他恶意 IP 地址的流量。
- 如果法规遵从性、业务策略或其他原因要求您阻止地理区域，请指定一个或多个区域作为地址。（对于入站流量，指定地理区域作为源，并指定 **any**（任何）作为目的地。对于出站流量，请指定 **any**（任何）作为源，指定地理区域作为目标。）

STEP 3 | 使用 User-ID 指定源用户，以便安全策略对本地和远程访问都有效。一致的用户标识对于确保一致的策略至关重要，无论用户的位置和连接方法如何。

- 根据以下上下文创建用户组：需要为业务部门做什么 - 常见的访问要求是什么？此观点按用户需要访问的资源和需要使用的应用程序对用户进行分组，以便您可以创建逻辑组并对其应用策略。

  让网络安全团队与控制用户组的团队合作，以帮助确保分组对安全控制有意义。

  仅当无法使用组时才在策略中指定单个用户。例如，您的 CEO 和其他少数高管可能需要其他用户和组不应该拥有的各种访问权限。

- 如果您的部署允许，请使用 Cloud Identity Engine (CIE)：
  - 聚合网络中的所有 User-ID 源，包括云和内部部署。
  - 搜索目录源。
  - 在整个网络中提供一致的 User-ID 信息。

  一致的 User-ID 使策略能够在网络中的任何位置跟踪用户。

  CIE 通过与 *Okta*、*Azure AD* 等身份提供程序集成来提供身份验证。

- GlobalProtect 是 User-ID 映射源，具有最准确、最全面的用户信息和最高的准确性（还有许多其他可能的 User-ID 映射源）。
- 在策略中使用 动态用户组 (DUG)，根据日志事件和自动标记自动修复异常用户行为和恶意活动。DUG 的工作方式与 DAG 类似。考虑哪些活动需要禁止或限制访问，并制定对您的业务有意义的标记策略。

  还可以使用 DUG 来允许定期访问用户组。例如，DUG 可以在审计期间允许季度审计员（由审计员用户组定义）访问，并在所有其他时间阻止访问。
- 在安全策略规则配置中，除了指定特定用户和组之外，还可以指定规则是否应用于 **any**（任何）用户、**pre-logon**（登录前）用户、**known-user**（已知用户）（已验证）或 **unknown**（未知）用户（未验证）：
  - 使用 **any**（任何）表示适用于所有网络用户的规则，例如，访问 DNS、NTP、OCSP 等基本服务。
  - 允许您的网络上没有 **unknown**（未知）用户。创建规则以阻止未知用户。或者，如果您不允许访问您的公司网络，则使用 **unknown**（未知）作为访客访问权限。
  - 具有登录前访问权限的远程访问 VPN 专用于 GlobalProtect 用户。它在用户登录到设备之前建立 VPN 隧道，以验证端点并启用对特定服务（如 DHCP、DNS 等）的访问，并要求

在每个端点上安装机器证书。允许登录前用户访问的策略规则必须只允许访问用于计算机身份验证的服务和必要的网络服务。拒绝登录前用户的所有其他访问。

首要原则是最小权限访问。仅允许出于业务目的需要访问应用程序和资源的用户和组访问。

- 遵循 User-ID 最佳实践。

STEP 4 | 在管理 IoT 设备的安全策略规则（IoT Security 需要订阅）中，使用 Device-ID 指定 IoT 设备（PAN-OS 10.0 及更高版本）。

设备对象定义 IoT 设备的 Device-ID，并以与 User-ID 标识源用户相同的方式标识源设备。设备对象有六个度量用作匹配标准。设备必须匹配所有配置的指标才能匹配 Device-ID 。在大多数情况下，定义一个或两个指标就足够了。您定义的指标越多，筛选器过于具体而无法匹配您想要匹配的设备的可能性就越大。了解设备发送到防火墙的信息，以了解要配置哪些指标来定义设备对象（并非所有设备都传输所有指标）。以下操作命令显示IoT设备发送到防火墙的信息：

- **`> show iot ip-device-mapping-mp all`** - 查看防火墙上的所有IP地址到设备的映射。
- **`> show iot ip-device-mapping-mp ip <ip-address>`** - 查看指定IP地址的IP地址到设备的映射。

遵循 IoT Security 最佳实践。

应用和服务

默认情况下，位于安全策略规则库底部的隐式拒绝规则会阻止您在安全策略规则中未明确允许的应用程序。要强制最低权限访问，请细化安全策略规则，直到它们仅指定您希望允许用于业务目的（认可的应用程序）和员工（允许的应用程序）的确切应用程序。基于应用程序的规则提供了对谁使用每个功能应用程序以及他们如何使用它的精细控制，因此您可以在迈向https://docs.paloaltonetworks.com/best-practices/zero-trust-best-practices网络访问环境时创建精确的安全策略规则。基于端口的规则允许在开放端口上的任何应用程序；请避开这些规则。

您必须启用https://docs.paloaltonetworks.com/best-practices/10-2/decryption-best-practices/decryption-best-practices，防火墙才能看到功能应用程序，而不仅仅是“*-base*”应用程序。查看功能应用程序使您能够精细地控制应用程序。例如，防火墙可以看到“*facebook-posting*”、“*facebook-downloading*”、“*facebook-file-sharing*”等，而不是只看到容器应用程序“*facebook*”。这使您能够根据最低权限访问配置安全策略;您可以限制或阻止适当用户访问特定功能应用程序，而不是让所有员工访问所有*Facebook* 功能应用程序。

将容器应用程序添加到规则时，其所有功能应用程序都将隐式添加到规则中。指定您希望允许的确切功能应用程序，以便对您允许的应用程序以及允许使用它们的人员进行更精细的控制。

如何为应用程序应用最佳实践建议取决于您的环境是新环境、现有环境还是迁移环境。许多建议反映了最后的最佳实践状态。在某些情况下，我们提供过渡建议或有关不同环境的建议。然而，每个

环境都是独一无二的。目标是了解哪些应用程序会遍历您的网络，您希望遍历您的网络的应用程序是经过批准和允许的，并使用这些信息安全地过渡到安全策略规则库，该规则库仅允许您批准用于业务目的并允许员工访问的应用程序。

安全策略规则库最佳实践 介绍了在安全策略规则库中放置规则的位置。

1. 尽可能多地使用应用程序组来简化和加强安全策略规则的创建，并减少规则库的大小。

   应用程序组是用户定义的应用程序集，需要类似的安全处理。通过将应用程序组添加到安全策略规则，您可以使用一个规则控制多个应用程序，而无需为每个应用程序创建单独的规则。如果您需要将应用程序添加到组中或进行任何其他更改，则只需进行一次更改，而不是在每个规则中进行更改，因为当您更新应用程序组时，引用它的规则会自动更新。
2. 无论是将应用程序添加到应用程序组还是单个安全策略规则，都要指定所需的确切功能应用程序，除非您使用组来阻止容器应用程序（这会阻止其所有功能应用程序），或者您希望允许访问容器应用程序的所有功能应用程序。
3. 当应用程序需要其他应用程序（依赖应用程序）才能正常工作时，就会出现应用程序依赖性。应用程序依赖关系只对您允许的应用程序有影响，而对您阻止的应用程序没有影响。有两种类型的依赖应用程序：

   - 显式应用程序，当您将应用程序添加到规则时防火墙会显示这些应用程序，您可以手动添加这些应用程序，以便应用程序正常工作。例如，facebook-chat 应用程序依赖于手动添加 facebook-base 和 mqtt-base 应用程序。
   - 隐式应用程序，防火墙自动允许其支持指定的应用程序，并且不需要显式添加到规则中。例如，除了facebook-chat 正常工作所需的显式应用程序外，当您将 facebook-chat 添加到规则中

时，防火墙会自动允许应用程序 jabber 和 web 浏览。（除非您明确地将它们添加到规则中，否则 jabber 和网页浏览并不适用于所有流量，只适用于 facebook-chat 流量。）

在允许应用程序时，请注意隐式允许哪些应用程序。

您可以通过以下几种方式查看应用程序的依赖项：

- **Applications**（应用程序）对象提供了一个可搜索的应用程序数据库。选择一个应用程序以查看其显式应用程序依赖项（**Depends on**（依赖于））和隐式应用程序依赖项（**Implicitly Uses**（隐式使用））。
- Palo Alto Networks applipedia 是一个可搜索的内容交付 App-ID 数据库。搜索并选择应用程序以查看其显式应用程序依赖项（**Depends on Applications**（依赖于应用程序））和隐式应用程序依赖项（**Implicit use Applications**（隐式使用应用程序））。
- 将应用程序添加到安全策略规则时，防火墙会显示显式依赖应用程序，但不会显示隐式依赖应用程序。
- 根据整个安全策略规则库而不是仅根据一个规则 **Commit Validate**（提交验证）以查看应用程序依赖项。

每个网络环境和业务都是不同的，因此如何处理应用程序依赖关系并不是一个一刀切的建议。根据您的业务和安全要求，有两种方法可以处理应用程序依赖关系：

- 关注可用性 - 将安全策略规则中显示的所有依赖应用程序添加到规则中，以确保应用程序正常运行。例如，对于控制 facebook-chat 的规则，将 facebook-base 和 mqtt-base 添加到规则中。

  但是，这可能会导致一些常见的依赖应用程序（如 ssl）被添加到许多规则中，而不是仅添加到一个规则中，这会增加规则库的混乱。(即使规则库已经允许 ssl，ssl 也会显示为许多其他应用程序的依赖应用程序。） 缓解此问题的一个好方法是使用 Policy Optimizer 来删除依赖应用程序的重复出现。
- 关注安全性 - 要允许尽可能少的应用程序，请运行 **Commit Validate**（提交验证）命令以查看安全策略规则库中的所有应用程序依赖项。根据提交命令的输出添加所需的依赖项。考虑为不同的应用程序依赖项集（例如，VMware依赖项、软件更新依赖项等）创建应用程序组，这些应用程序组包含您希望允许的所有依赖应用程序，以便您可以根据用户控制访问。

4. 在新的和现有的部署中，立即阻止已知的恶意和危险流量。

   - 基于可信威胁情报源,阻止潜在恶意流量，包括 Palo Alto Networks 内置的外部动态列表 (EDL)，这需要高级威胁预防或威胁预防订阅，并阻止防弹 IP 地址、高风险 IP 地址、已知恶意 IP 地址和称为 Tor 出口节点的 IP 地址。
   - 阻止加密的DNS以保持流量的可见性，并使用威胁配置文件检查流量中的威胁。攻击者使用 DNS 进行多种类型的攻击，因此您必须检查 DNS 流量。阻止 DNS-over-HTTPS (DoH) 和

DNS-over-TLS (DoT)，并使用 Palo Alto Networks DNS 服务。如果您无法立即阻止加密的 DNS，请查看流量并过渡到阻止 DoH 和 (DoT) 流量。

由于 *App-ID* 的粒度，您可以在一个规则中允许常规 *DNS* 流量，而在另一个规则中阻止 *DoT* 和 *DoH* 流量，因为每种流量都有不同的 *App-ID*，您可以在安全策略规则中指定这些流量。

- 不良行为者经常使用文件共享应用程序来泄露数据。阻止大多数文件共享应用程序，仅允许需要这些应用程序用于业务目的的用户访问业务文件共享应用程序。一个简单的方法是创建一个规则，指定用户，并创建一个应用程序过滤器，其中包括子类别 **file-sharing**（文件共享）和/或标记 **Uploading**（正在上传）。

构建基于允许列表的安全策略会隐式地阻止大多数不需要的应用程序，因此您不需要很多阻止规则。根据您的业务需求进行阻止，只允许您希望的应用程序流量进入网络，并考虑谁需要使用每个应用程序。

5. 在大多数情况下，将 **Service**（服务）设置为 **application-default**（应用程序默认值）。由于 App-ID 基于签名而不是端口和协议（可以欺骗），因此 App-ID 非常准确，因此您不需要指定端口。使用应用程序默认值可防止合法应用程序以外的任何应用程序使用该端口，并阻止规避应用程序使用非标准端口。如果将来应用程序的默认端口发生更改，application-default 会自动应用新端口，因此您不必重新配置服务端口设置。

   只有在您有自定义应用程序、特殊体系结构要求或公司安全要求时才指定服务端口。

6. 对于内部应用程序和没有App-ID的应用程序，创建自定义应用程序以获得第 7 层流量可见性。不要使用应用程序防火墙策略，因为它会绕过第 7 层处理和威胁检查。应用程序身份验证的用例是 SMB 或 SIP 流量的异常情况。

7. 使用应用程序过滤器发现网络上的流量并处理新应用程序。

   应用程序筛选器是应用程序的动态集。应用程序根据您定义的属性（如类别、子类别、风险、标记（预定义标记或自定义标记）和特征匹配应用程序过滤器。当新应用程序与筛选条件

匹配时，防火墙会自动将新应用程序添加到筛选器。具有应用程序筛选器的安全策略规则会自动控制与筛选器匹配的新应用程序。

应用程序筛选器是比应用程序组更宽松的控件。您可以准确控制应用程序组中的应用程序。您定义的属性控制哪些应用程序在应用程序筛选器中，这可能导致更广泛的成员资格，并允许比您需要允许的更多的应用程序。这就是为什么它们最适合发现流量，以便您可以控制它。

使用案例包括：

- 在您还不熟悉流量的新部署中，使用应用程序过滤器分析不同类别和子类别的流量，以便您可以发现网络上存在哪些类型的应用程序。

  您还可以创建应用程序过滤器来发现成熟部署中不同类型的流量。

- 筛选新应用程序的规则库。创建匹配新应用程序的筛选器，并将规则放置在规则库的顶部附近。使用 Policy Optimizer 可查看应用程序并对其进行控制。

  内容更新控制新应用程序。当应用程序内容更新发布时，新应用程序将被视为新应用程序，直到下一个应用程序内容更新发布。发布通常发生在每个月的第三个星期二左右。在发布下一组新应用程序之后，前一组新应用程序不再被视为新应用程序，并且应用程序过滤器不再与它们匹配。遵循应用程序和威胁内容更新的最佳实践，并决定如何在下次应用程序内容更新之前处理新应用程序。

- 在迁移方案中，使用应用程序筛选器来阻止或允许广泛的特定应用程序类型，然后使用 Policy Optimizer 将其缩小到仅限于网络上需要的应用程序。应用程序筛选器还使您能够确保某些类型的新应用程序在与筛选器匹配时自动被允许。
- 通过自动处理与筛选器匹配的新应用程序来适应未来的规则。这在迁移和新部署的应用程序发现阶段以及成熟环境中都很有用。

  例如，使用基于 **Palo Alto Networks** 标记的应用程序过滤器创建允许规则。这可确保您允许所有当前的 Palo Alto Networks 应用程序和所有未来的 Palo Alto Networks 应用程序。

  另一个示例是创建一个规则，用于筛选新内容交付的 App-ID，以便安全地处理它们，直到您可以更仔细地检查它们。

8. 应用程序定义不是静态的。应用程序内容更新可以更改应用程序的定义，从而更改规则处理应用程序的方式。请遵循应用程序内容更新的最佳实践，以确保您有时间进行更新所需的任何更改。

网站访问（URL 过滤）

高级 URL 过滤需要许可证。将 Advanced URL Filtering 与 PAN-OS、Prisma Access（通常包含在 Prisma Access 许可证中）和 Cloud NGFW for AWS 配合使用。

基于网站类别的 URL 过滤简化了出站安全策略，并保护您免受恶意网站的攻击。每个 URL 类别定义了一组具有相同类型内容的网站，例如，**health-and-medicine**（健康和医学）、**games**（游戏）或 **hacking**（黑客）网站。还有三个类别定义了特定类别中站点的相对风险级别：**low-risk**（低风险）、**medium-risk**（中风险）和 **high-risk**（高风险）。将类别与风险级别结合使用，可以创建安全策略规则，根据 URL 类别中的风险阻止或允许通信。

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。

STEP 1 | 根据 URL 类别确定要解密的目标流量，因为 URL 类别使您能够轻松识别有风险的流量。

首先解密风险最大的URL类别，然后随着经验的积累解密更多的流量。

STEP 2 | 在控制出站 Internet 流量的安全策略规则中：

- 附加 URL 筛选配置文件以简化安全策略。配置最佳实践 URL 过滤配置文件，以阻止所有类别的恶意网站（针对站点访问和用户凭据提交）和所有其他类别的警报，并将其附加到允许 Web 访问的所有规则。
- 控制由于法律、合规性、业务、隐私、监管或其他原因而无法使用 URL 类别解密的流量。例如，使用适当的用户和应用程序创建安全策略规则，该规则指定适当的类别作为匹配条件，并且不解密与该规则匹配的通信。
- 配置自定义 URL 类别，以便您可以基于 URL 筛选的安全策略规则创建例外。将自定义 URL 类别添加到 URL 筛选配置文件中，并将其附加到相应的安全策略规则，或将自定义类别用作安全策略中的匹配条件。加密使您能够阻止大多数用户访问 URL 类别，但允许特定用户（如 PEN 测试人员和信息安全）访问，阻止整个类别（如社交网络），但允许访问 LinkedIn，或控制解密内容。例如：
  - 将 URL 类别与基于风险的类别组合作为匹配标准，以根据风险阻止或允许 URL 类别的流量。例如，要阻止访问有风险的金融站点，请创建一个安全策略规则，指定 **financial-services**（金融服务） URL 类别和 **high-risk**（高风险）类别作为匹配条件，并将规则 **Action**（操作）设置为 **Deny**（拒绝）。将此规则置于允许访问 **financial-services**（金融服务）URL 类别的规则之上，以便防火墙在允许访问中风险和低风险站点之前阻止高风险站点。
  - 如果防火墙资源的可用性阻止您解密所有可以合法解密的通信以及用于业务目的，请使用自定义 URL 类别创建安全策略规则，并匹配解密价值不大的低风险通信。例如，要绕过低风险流媒体服务的解密，请创建一个安全策略规则，指定 **streaming-media**（流媒体） URL 类别和 **low-risk**（低风险）类别作为匹配条件，并将规则 **Action**（操作）设置为 **Allow**（允许）。如果流量使用TLSv1.2或更低版本，请为流量创建无解密策略和配置文件，以阻止坏会话。如果流量使用 TLSv1.3 或更高版本，请不要为流量创建无解密策略和配置文件。
- 将安全策略规则中的源区域设置为受保护的内部网络（信任区域）。不要指定外部区域或 **any**（任何）区域作为源，因为您只对出站通信应用 URL 筛选。（对入站流量应用 URL 过滤甚至可能导致 DoS 攻击。）

STEP 3 | 要安全地将 URL 筛选配置文件设置转换为最佳实践并创建最佳实践 URL 筛选配置文件，请执行以下操作：

1. 克隆默认的 URL 过滤配置文件（命名为 **default**）并对其进行编辑。
2. 适当地修改配置文件（例如，最佳实践 URL 过滤配置文件）。
3. 将 URL 类别的所有操作设置为同时对站点访问和用户凭据提交发出警报。（默认的允许操作不会生成日志。） 您必须手动将 URL 类别设置为警报，以生成日志并获得流量的可见性。

   将新类别添加到 *URL* 筛选时，默认情况下，该类别设置为允许站点访问和用户凭据提交。手动设置新类别以在网站访问和用户凭据提交时发出警报，以获取其 *URL* 过滤日志。还相应地更新自定义*URL*类别。
4. 将恶意 URL 类别的所有操作设置为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：
   - 命令和控制 - 恶意软件或受损系统用于与攻击者的远程服务器通信的 URL 和域。
   - 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。
   - 恶意软件 - 已知有恶意软件或用于命令和控制 (C2) 流量的站点。
   - 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。
   - 勒索软件 - 已知会分发勒索软件的网站。
   - 扫描活动 - 探测现有漏洞或进行有针对性的攻击.
5. 某些 URL 类别具有很强的恶意潜力，但并非绝对恶意。将这些 URL 类别的所有操作设置为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：
   - 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。
   - 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。
   - 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。
   - 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。
   - 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。

- 已寄放 - 经常用于凭据网络钓鱼或个人信息盗窃的域。
- 代理规避和匿名程序- 常用来绕开内容筛选产品的 URL 和服务。
- 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。

6. 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。
   - 滥用药物 - 宣传非法和合法药物滥用的网站。
   - 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。
   - 侵犯版权 - 包含非法内容且存在责任风险的域名。
   - 极端主义 - 宣扬恐怖主义、种族主义、剥削儿童内容等的网站。
   - 赌博 - 彩票和赌博网站。
   - 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站点。）
   - 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。
   - 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。
7. 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。）
8. 对于 URL 筛选配置文件中的 URL 筛选设置：
   - 禁用 **Log Container Page Only**（仅日志容器页面），默认情况下启用。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）。
9. 启用 **User Credential Detection**（用户凭据检测）（需要配置和启用 User-ID）。

STEP 4 | 将 URL 筛选应用于安全策略规则，并在防间谍软件安全配置文件中配置 DNS Sinkhole（需要高级威胁防护或活动的旧版威胁防护订阅和 DNS Security 订阅才能使用基于云的 DNS Security），以查看哪些计算机受到感染以及它们试图连接 DNS 的位置。

策略操作和其他设置

安全策略操作指定是允许还是阻止通信，以及如何阻止您不允许的通信。服务质量 (QoS) 控制带宽（如果需要），以确保规则允许的流量接收适当的带宽。

STEP 1 | 为每个安全策略规则定义操作。

- 只 **Allow**（允许）认可和容忍的流量。您允许的流量越多，不属于您的业务，风险就越大。防火墙阻止您在安全策略规则中未明确允许的通信。
- 安全策略规则越是遵循最低权限访问原则，所需的阻止规则就越少。如何阻止流量取决于您希望如何响应要阻止的应用程序。
  - 使用 **Deny**（拒绝），它使用应用程序的默认操作，除非您希望防火墙通过重置客户端、服务器或两者，或通过静默丢弃通信，以特定方式响应应用程序。
  - 当您想要静默拒绝服务而不发送重置响应时，请使用 **Drop**（丢弃）。当您阻止明显的恶意流量时，例如当您根据 predefined Palo Alto Networks EDLs（预定义的 Palo Alto Networks EDL）阻止时，**Drop**（丢弃）操作可防止通信的恶意端知道其被阻止的原因。
  - 如果您有只重置客户端或只重置服务器的用例，请确保您了解客户端-服务器方向性（通信的哪一端发起连接），这是基于规则的源和目标设置。

STEP 2 | 如有必要，应用 QoS 来控制某些应用程序的带宽。

QoS 是可选的。了解您要优先考虑带宽的应用程序，以及在将 QoS 应用于策略时要限制其带宽的应用程序。例如，在使用特定流媒体应用程序的热门活动（如世界杯）期间，您可以允许员工使用这些应用程序查看活动，并限制其带宽，以确保为业务活动提供适当的带宽。另一个例子是，当为流行应用程序发布更新时，大量下载可能会影响带宽可用性。要防止这种情况，请应用 QoS 来限制应用程序下载流量的可用带宽。

日志记录和日志转发

记录和存储日志对于调查事件至关重要。与您的以下团队沟通：

- 安全运营中心 (SOC)，确保您在必要时捕获正确的信息以调查事件。
- 审计合规团队，确保您为审计和合规捕获正确的信息。
- 法律团队确保您不会存储违反当地法规、合规性、业务要求、隐私等的明文或其他数据。

STEP 1 | 考虑您现在和将来需要的日志存储容量，并相应地调整日志存储容量。

- 规划存储容量，以便您可以保留足够长的日志来调查威胁。时间长短取决于您的调查程序。
- 确保您的 SOC 可以从存储日志的任何位置获取日志。Cortex Data Lake (CDL) 集中化日志存储和分析，并提供可随日志量扩展的解决方案。
- 不要在多个地方存储相同的日志。使用 CDL 或单独的存储空间，如日志收集器。将日志从一个存储空间移动到另一个存储空间时，不要使用复制。相反，准备并执行硬切换。

> 如果在防火墙或 *Panorama* 上启用重复日志转发，则系统和配置日志不会发送到 *CDL*，因此 *CDL* 日志将不完整。因此，不要为日志备份启用重复日志转发。
>
> 如果必须拆分日志存储，请以一致的方式分离日志转发。例如，将所有 *Prisma Access* 日志发送到 *CDL*，并将所有防火墙日志发送到日志收集器。

STEP 2 | 考虑您想要记录什么、如何记录以及出于合规性或存储空间原因不想记录或不能记录什么。

对于大多数应用程序，记录所有信息，以帮助安全操作中心 (SOC) 调查。但是，有一些应用程序和情况，您不能采取全面的日志：

- 根据合规性、业务要求、审计要求（如 ISO）、隐私注意事项（如 PII、GDPR）和 SOC 要求，评估规则是否需要记录日志。如果应用程序不加密 SSN、凭据、PII 等信息，请小心以明文记录这些信息。
- DNS、NTP、系统日志等基本服务会创建数千个小会话，从而产生许多不必要的日志，这会影响日志存储并使调查事件变得更加困难。对于这些服务，请仅配置威胁日志转发，除非您有存储容量来接收其他日志。

STEP 3 | 在安全策略规则中，在会话结束时而不是开始时记录通信，以避免记录临时应用程序。

Log At Session Start（在会话开始时记录）也会消耗比仅在会话结束时记录更多的资源。在大多数情况下，您只能 **Log At Session End**（在会话结束时记录）。仅在需要对应用程序与安全策略规则不匹配的原因进行故障排除时同时启用 **Log At Session Start**（在会话开始时记录）和 **Log At Session End**（在会话结束时记录），以便查看 GRE 隧道等活跃的长时间隧道会话（除非在会话开始时记录，否则无法在 ACC 中查看这些会话），同时获取对运营技术/工业控制系统 (OT/ICS) 会话的可见性（这也是长时间会话）。

> *Policy Optimizer* 和 *Cloud App-ID Engine (ACE)* 不将在会话开始时登录的规则计入其统计信息中。

STEP 4 | 记录与区域间默认默认规则（默认情况下允许区域内的所有通信）和拒绝规则（默认情况下阻止安全策略规则不明确允许的区域之间的所有通信）匹配的通信。

STEP 5 | 配置日志转发配置文件并将其分配给安全策略规则，以将日志发送到相应的存储（如 CDL或日志收集器），并向相应的管理员发出事件警报，特别是严重、高和中等威胁事件。

Cloud Managed Prisma Access 将所有日志转发到 *CDL*。

- 确保每个安全策略规则都附加了日志转发配置文件。

  为所有新的安全策略规则创建一个基本的默认日志转发配置文件，并将其命名为 **`default`**，并确保它记录威胁。将配置文件设置为 **`default`** 会使防火墙自动将其应用于所有新的安全策略规则，从而确保所有新规则都具有日志转发配置文件。

  与为每个新规则单独附加日志转发配置文件相比，替换或修改需要不同日志处理的少数规则的配置文件（如与合规性、个人信息、本地法规、业务要求等相关的流量日志，或常见服务（如 DNS 或 NTP）的日志）更容易。

  对于管理 *IoT Security* 的安全策略规则，请使用 ***IoT Security*** 默认配置文件 - 启用 ***EAL*** 的预定义日志转发配置文件，该配置文件为 *IoT Security* 提供了所需的所有日志类型，包括增强的应用程序日志。

- 使用 Policy Optimizer 中的**Log Forwarding for Security Services**（安全服务的日志转发）来标识未附加日志转发配置文件的安全策略规则（在筛选器中选择 **None**（无））。为每个没有日志转发配置文件的规则添加适当的日志转发配置文件。

STEP 6 | 出于调查目的，请确保您知道流量的真实来源和目的地，而不仅仅是真实来源和防火墙之间的代理设备（如负载平衡器、 NAT 设备或恶意 DNS 服务器）的 IP 地址。如果防火墙和真实源之间存在代理设备，则取决于您的网络架构和应用程序：

- 在负载均衡器前放置防火墙以查看真实的源 IP 地址。
- 通过在数据包捕获设置中配置接收阶段，进行预 NAT 数据包捕获。
- 应用 URL 筛选配置文件，该配置文件允许将 X-Forwarded-For (XFF) 字段记录到安全策略规则（**Objects**（对象） > **Profiles**（配置文件） > **URL Filtering**（**URL** 过滤）中的 **URL Filtering Settings**（**URL** 过滤设置））。XFF 字段显示原始源 IP 地址。XFF 日志位于 URL 过滤日志中。

安全配置文件

安全配置文件扫描允许的通信中是否存在病毒、恶意软件、间谍软件、恶意文件类型以及其他已知和未知威胁，并阻止这些威胁。将安全配置文件附加到安全策略规则，允许通信将威胁防护应用于与规则匹配的通信。

使用第 1 天的模板，提供用例不可知的最佳实践安全配置文件，以允许正确的方式流量。第 1 天配置可在客户支持门户（**Tools**（工具） > **Run Day 1 Configuration**（运行第 **1** 天配置））上获得，需要支持登录。从这里过渡到最佳实践威胁阻止，如此处所述。

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。对于 SSL 转发代理（出站）解密，请先实现 *User-ID* 和 *URL* 过滤，以便您可以有效地定位解密。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。

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。

订阅 Advanced Threat Prevention 云服务，实时防范包括未知命令和控制以及零日漏洞在内的威胁。Advanced Threat Prevention 适用于 PAN-OS 和 Prisma Access 3.2 Innovation 及更高版本的 Innovation 部署。如果您运行较早版本的 Prisma Access，请使用常规威胁预防订阅。

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。

Cloud Managed Prisma Access 的最佳实践安全配置文件建议与 PAN-OS 和 Panorama Managed Prisma Access 的建议略有不同。此外，在 *Cloud Managed Prisma Access* 中，您无法将单个安全配置文件应用于安全策略规则，只能应用配置文件组。配置文件组包括您在组中包含的安全配置文件。

最佳实践建议侧重于如何做才能最安全，这是您的安全配置文件的最终目标。但是，要确保业务关键型应用程序的可用性，首先要阻止已知的恶意流量，并对大多数其他流量发出警报。遵循最佳实践安全配置文件转换建议，从警报安全地转换为最佳实践阻止流量的安全配置文件，并在从警报转换为阻止时保持谨慎，以避免影响业务关键型应用程序。

将安全性配置文件设置从警报转换为阻止的时间是当您确信配置文件已适当调整，您已进行了任何必要的例外处理，并且您不会无意中触发阻止业务关键型应用程序的签名时。

这个简化的部分向您展示了最佳实践设置。创建最佳实践安全配置文件提供了有关设置原因的更深入信息。

- 防病毒配置文件（包括 WildFire 签名和内联机器学习操作）
- 反间谍配置文件（包括 DNS 策略/Sinkholing 和内联云分析）

  要提供全面的覆盖范围，请订阅高级 *URL* 过滤订阅和 *DNS* 安全订阅，以了解并防范恶意 *URL*、域和 *DNS* 协议滥用。
- 漏洞保护配置文件（包括内联云分析）
- 文件阻塞配置文件
- WildFire 分析配置文件

STEP 1 | 克隆预定义的默认防病毒配置文件，将其重命名，并在将防病毒配置文件安全地转换为最佳实践设置时对其进行编辑。

要将防病毒配置文件安全地转换为最佳实践配置文件，请执行以下操作：

1. 误报不多。立即为对您的业务不重要的应用程序部署最佳实践防病毒配置文件。

2. 对于业务关键型应用程序，首先要发出警报，以确保不会影响关键应用程序的可用性。当您确信防病毒配置文件不会阻止这些应用程序时，过渡到阻止。
3. 如果您有现有的部署或正在迁移，并且您有一个现有的阻止，请复制它，因为您已经了解流量以及为什么要阻止它。
4. 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。

监视威胁日志，查看是否有任何业务关键型应用程序导致警报或阻止。如果您拥有高级 WildFire 或旧版 WildFire 订阅，请监视 WildFire 提交日志，并使用 WildFire 操作设置。

最佳实践防病毒配置文件可阻止已知的恶意软件、病毒和勒索软件僵尸程序：

- 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。
- 设置防火墙在某些协议中检测到病毒时要采取的操作。最安全的操作是重置客户端和服务器，以确保会话终止：
  - 对于 smtp、pop3 和 imap 协议（它们的默认操作是“警报”），将 **Signature Action**（签名操作）更改为 **reset-both**（重置两者）。将其他协议的 **Signature Action**（签名操作）保留为 **reset-both**（重置两者）。
  - 对于 smtp、pop3 和 imap 协议（它们的默认操作是“警报”），将 **WildFire Signature Action**（**WildFire** 签名操作）更改为 **reset-both**（重置两者）。将其他协议的 **WildFire Signature Action**（**WildFire Signature** 操作）保留为 **reset-both**（重置两者）。
  - 对于 smtp、pop3 和 imap 协议（它们的默认操作是“警报”），将 **WildFire Inline ML Action**（**WildFire Inline ML** 操作）更改为 **reset-both**（重置两者）。将其他协议的 **WildFire Inline ML Action**（**WildFire Inline ML** 操作）保留为 **reset-both**（重置两者）。

将最佳实践配置文件附加到所有允许规则。

配置 *WildFire* 签名操作和 *WildFire Inline ML* 操作需要 *WildFire* 订阅。

在 *Cloud Managed Prisma Access* 中，*Antivirus* 和 *WildFire* 合并在一个配置文件中，而不是单独的配置文件。

STEP 2 | 克隆预定义的默认防间谍配置文件，将其重命名，并在将防间谍配置文件安全地转换为最佳实践设置时对其进行编辑。除了反间谍签名策略，配置文件还控制 DNS Sinkhole 策略。

要将防间谍配置文件安全地转换为最佳实践配置文件，请在 **Signature Policies**（特征码策略）中：

1. 误报相对较少。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。
2. 中等严重性签名可能会产生误报，所以需要初始监控。针对内部流量的中等严重性特征码发出警报，并阻止面向外部的流量的中等严重性特征码。监视威胁日志（**Monitor**（监视）> **Logs**（日志）> **Threat**（威胁））以查看是否可以阻止收到警报的应用程序，或者是否需要允许这些应用程序。
3. 对于业务关键型应用程序，将 **Action**（操作）设置为 **Alert**（警报）以确保应用程序可用性。但是，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来应用程序，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。
4. 在转换期间为所有严重性签名启用单个数据包捕获，以便在有资源的情况下，根据需要更详细地调查事件。当您转到最佳实践配置文件时，如果低严重性和信息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，则转换为禁用这些严重性级别的数据包捕获。

数据包捕获占用管理平面资源。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。

5. 在实施完整的最佳实践反间谍配置文件之前，根据需要创建例外，以修复任何确认的误报。

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。

一旦您确信自己了解了要阻止的流量，就将配置文件的 **DNS Policies**（**DNS** 策略）转换为最佳实践：

- 将 DNS 签名的 **Policy Action**（策略操作）设置为 **Sinkhole**，以便识别可能受到攻击的主机，这些主机会尝试通过跟踪主机并阻止其访问这些域来访问可疑域。将 **Packet Capture**（数据包捕获）设置为 **extended-capture**（扩展捕获）。

  在 *PAN-OS* 系统上，将 *DNS Sinkhole* 地址设置为 *IP* 地址，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*，使用 *Sinkhole IP* 地址。

- 将所有 **DNS Security** 域类型设置为 Sinkhole，并将命令和控制域的 **Packet Capture**（数据包捕获）设置为 **extended-capture**（扩展捕获），将除“寄放域”（PAN-OS 10.0 及更高版本）以外的所有其他域类型的数据包捕获设置为 **single-packet**（单个数据包）。
- 阻止加密 DNS 查询使用的所有 DNS 记录类型，以防止客户端在 DNS 解析过程中加密客户端 Hello。

将配置文件的 **Inline Cloud Analysis**（需要 Advanced Threat Prevention 订阅和 PAN-OS 10.2 及更高版本）设置为对所有出站流量 **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）。

在过渡反间谍软件配置文件中，如果您现有的反间谍软件控件可以阻止流量并满足您的业务需求，请立即实施这些控件，因为您已经了解流量以及阻止流量的原因。

最佳实践反间谍软件配置文件检测命令和控制 (C2) 流量，防止受感染的系统建立出站连接，并启用 DNS Sinkholing 来识别受感染的主机。使用 GlobalProtect 在 PAN-OS 中自动隔离被入侵的

设备，而使用 Panorama Managed Prisma Access，您还可以 隔离 Cloud Managed Prisma Access 中被入侵的设备。

对于 **Signature Policies**（签名策略）：

1. 将关键、高和中等严重性的 **Action**（操作）设置为 **reset-both**（重置领着），并将 **packet-capture**（数据包捕获）设置为 **single-packet**（单个数据包）。
2. 对于低和信息严重性，将 **Action**（操作）设置为 **default**（默认）并禁用 **packet-capture**（数据包捕获）。

对于 **DNS Policies**（**DNS** 策略），请使用建议用于过渡期的相同设置。对于所有签名源，将 **Policy Action**（策略操作）设置为 Sinkhole，对于 **Palo Alto Networks Content**（**Palo Alto Networks** 内容）以及命令和控制域，将 **Packet Capture**（数据包捕获）设置为 **extended-capture**（扩展捕获），对于除了寄放域之外的所有其他 DNS Security 域，将 **Packet Capture**（数据包捕获）设置为 **single-packet**（单个数据包）。

Inline Cloud Analysis（内联云分析）的最佳实践设置与过渡设置相同。对所有出站流量启用该功能，并将操作设置为 **reset-both**（重置两者）。

使用 DNS Security 服务保护您免受基于 DNS 的高级威胁（需要 DNS Security 许可证和 Advanced Threat Prevention 或有效的旧版 Threat Prevention 订阅）。

将最佳实践配置文件附加到所有允许规则。

STEP 3 | 克隆预定义的严格漏洞保护配置文件，将其重命名，并在将漏洞保护配置文件安全地转换为最佳实践设置时对其进行编辑。

漏洞保护配置文件可防御缓冲区溢出、非法代码执行以及利用客户端和服务器端漏洞的其他尝试。要将漏洞保护配置文件安全地转换为最佳实践配置文件，请执行以下操作：

1. 误报率很低。为对您的业务不重要的应用程序设置规则，以便立即阻止（**reset-both**（重置两者））。
2. 对于业务关键型应用程序，首先要发出警报，以确保不会影响关键应用程序的可用性。当您认为漏洞保护配置文件不会阻止这些应用程序时，过渡到阻止。
3. 如果您有现有的部署或正在迁移，并且您有一个现有的阻止，请复制它，因为您已经了解流量以及为什么要阻止它。
4. 对于严重、高和中等严重性的 **brute-force**（暴力攻击）类别，将特征码设置为“提醒”，并精确调整它们，直到您可以轻松地过渡到阻止。将 **Packet Capture**（数据包捕获）设置为 **extended-capture**（扩展捕获）。
5. 将关键和高严重性规则的签名设置为 **reset-both**（重置两者），并将 **Packet Capture**（数据包捕获）设置为 **single-packet**（单个数据包）。
6. 将中等严重性规则的签名设置为 **alert**（警报），并将 **Packet Capture**（数据包捕获）设置为 **extended-capture**（扩展捕获）。
7. 将低严重性和信息严重性规则的签名设置为 **default**（默认值），并将 **Packet Capture**（数据包捕获）设置为 **single-packet**（单个数据包）。
8. 对于 **Inline Cloud Analysis**，请使用与初始漏洞防护规则相同的标准来警报和阻止业务应用程序。如果您有现有的控制，复制它们来阻止流量。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。

数据包捕获占用管理平面资源。检查系统资源（例如，***Dashboard***（仪表板） > ***System Resources***（系统资源））以了解在实施数据包捕获之前和之后的使用情况，从而确保系统具有足够的资源。

监视威胁日志，查看是否有任何业务关键型应用程序导致警报或阻止。如果您有 WildFire 订阅，请监视 WildFire 提交日志并使用 WildFire 操作。

最佳实践漏洞保护配置文件控制如何处理严重、高、中、低和信息事件严重性的客户端和服务器端漏洞。在配置文件中，配置六个规则：

1. 在转换配置文件中创建防止暴力攻击的三条规则，并将 **Action**（操作）设置为 **reset-both**（重置两者），将 **Packet Capture**（数据包捕获）设置为 **single-packet**（单个数据包）。
2. 在一个规则中组合 simple-client-critical、simple-client-high、simple-client-medium、simple-server-critical、simple-server-high 和 simple-server-low 严重性。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）。

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）。仅将此配置文件应用于内部流量。

3. 对于 simple-client-low 和 simple-server-low 严重性，将 **Action**（操作）设置为 **default**（默认），并将 **Packet Capture**（数据包捕获）设置为 **single-packet**（单个数据包）。
4. 对于 simple-client-informational 和 simple-server-informational 严重性，将 **Action**（操作）设置为 **default**（默认），并 **disable**（禁用）数据包捕获。（信息活动可能会生成相对大量的数据包捕获流量，与潜在威胁数据包捕获相比，这些流量并不是特别有用。）
5. 将 **Inline Cloud Analysis**（内联云分析）操作设置为 **reset-both**（重置两者）。

要更精细地控制漏洞保护配置文件并针对特定用例微调漏洞保护，请在配置文件中为客户端和服务器端检测的每个严重性创建单独的规则。当操作和数据包捕获设置相同时，将它们组合在一个规则中以简化配置是有意义的。

将最佳实践配置文件附加到所有允许规则。

STEP 4 | 将您的文件阻止配置文件从警报转换为阻止所有潜在恶意文件类型。

Cloud Managed Prisma Access 不支持安全策略规则的文件阻止配置文件。

文件阻止配置文件阻止网络攻击中使用的潜在恶意文件类型。要将文件阻止配置文件安全地转换为最佳实践配置文件，请执行以下操作：

- 对于业务关键型应用程序，对所有文件类型发出警报，并尽快迁移到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 - Block
    7z、bat、chm、class、cpl、dll、dlp、hta、jar、ocx、pif、scr、torrent、vbe 和 wsf 文件。对所有其他文件发出警报。
  - 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。

预定义的 **strict file blocking**（严格文件阻止）配置文件阻止通常用于网络攻击并且没有上传和下载的实际用例的文件类型。但是，一些用于恶意目的的协议也可能需要用于 Windows 更新等活动。**strict file blocking**（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，仅允许出于业务目的需要访问的用户和使用您要阻止其他通信的协议的业务应用程序。
2. 将允许所需协议的文件阻止配置文件附加到规则。
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。

此方法允许您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。

将最佳实践配置文件附加到所有允许规则。

STEP 5 | 将默认 WildFire Analysis 配置文件附加到所有允许规则，以检测和防止零日恶意软件。

要获得实时更新和其他高级功能，请获取 Advanced WildFire 订阅（PAN-OS 10.0 或更高版本）或 WildFire 订阅。

部署默认 WildFire 配置文件，这是最佳实践配置文件。WildFire 不会影响网络流量，因此不需要过渡期。（但是，防病毒配置文件中的 实践 WildFire 操作设置会影响生成签名的通信，这些签名会导致重置或删除操作，或者导致保留以查找最新的防病毒签名。） 将 WildFire Analysis 配置文件附加到所有允许规则，以将所有文件发送到 WildFire 进行分析。

在 *Cloud Managed Prisma Access* 中，*WildFire* 和 *Antivirus* 合并在一个配置文件中，您可以将其添加到 *Prisma Access* 配置文件组中。

STEP 6 | 安全配置文件组由组合在命名组中的各个安全配置文件组成，这使您能够更轻松且一致地将安全配置文件应用于安全策略规则。

根据规则库的逻辑为不同条件创建安全性配置文件组：

- 每个配置文件组都应该有不同的用途，例如创建特定于通信流的配置文件组。例如，入站流量的配置文件组不需要URL筛选配置文件，但出站流量的配置文件组需要。

  如果您希望区别对待面向内部和面向外部的流量，则特定于流量流的配置文件组可以更容易地设置例外。例如，您可能希望阻止您使用的内部流量并允许外部流量。在这种情况下，您将为内部和外部流量使用不同的配置文件。是否需要单独的配置文件取决于您希望如何处理流量。
- 要使配置文件从警报到阻止的转换更容易，请创建用于初始警报的配置文件组和用于最佳实践阻止的配置文件组。这使得在所有允许规则中对威胁发出警报变得容易。当您可以轻松地从警报状态切换到阻止状态时，配置文件组可以轻松进行更改，因为您只需换出一个对象，而不是每个单独的配置文件。
- 考虑通过将组命名为 **`default`** 来创建默认配置文件组。例如，根据最佳实践安全配置文件转换建议，创建一个配置文件组，该配置文件会发出警报但不会阻止大多数流量。防火墙会自动将默认配置文件组应用于允许通信的所有新安全策略规则。（防火墙不将默认配置文件应用于现有规则。） 这确保了所有新的允许规则都具有一定程度的威胁预防。根据需要编辑或替换默认配置文件。

安全策略规则库最佳实践

安全策略规则库是安全策略规则的有序列表。规则的顺序决定防火墙如何处理流量。

防火墙将流量与安全策略规则进行比较，从安全策略规则库顶部的第一条规则开始。当流量与规则的条件匹配时，防火墙会对流量执行规则的操作，并且不会将该流量与任何其他规则进行比较。如果没有规则与流量匹配，防火墙将丢弃该流量（隐式拒绝）。在规则库中对规则进行排序的方式至关重要，因为防火墙会在第一个规则匹配时对流量采取操作，然后停止将流量与规则库进行比较。

如果您从其他供应商的防火墙迁移安全策略，则以前的防火墙可能会根据其规则库以不同的方式评估流量。例如，规则的顺序可能对旧防火墙没有影响，但它们对 *Palo Alto Networks* 防火墙至关重要。

了解您希望如何处理不同类型的流量以及 #unique_18，帮助您评估如何在规则库中对规则进行排序。按逻辑方式设计和优化您的安全策略规则库，如本节所述。对于现有规则库，如果规则库未得到尽可能优化，请根据本节中的建议计划和测试更改。如果您计划分阶段推出更改，请在适当的时间或时间进行更改。

本节涵盖：

- 对规则库中的安全策略规则进行排序
- 避免规则库膨胀
- 定位以打破规则
- 预防和修复规则遮蔽
- 在 Panorama 上使用设备组层次结构来简化规则库

STEP 1 | 在规则库中对安全策略规则进行逻辑排序。

由于当流量与规则的条件匹配时，防火墙会对流量执行策略规则的操作，因此规则的顺序至关重要，它决定了哪些规则流量匹配，从而决定防火墙对流量采取哪些操作以及防火墙如何检查流量:

1. 将阻止恶意流量的规则放置在规则库的顶部，以防止稍后在规则库中意外允许不良流量。如果您拥有有效的高级威胁防护或有效的旧版威胁防护许可证，请根据预定义的外部动态列表 (EDL) 创建阻止规则并对其进行测试，以确保它们不会阻止您想要允许的流量。在 Panorama 上，将这些规则放在前置规则中，以便它们在任何特定于防火墙的规则之前执行。
2. 允许基本基础设施应用程序和常见服务（例如 DNS 和 NTP）位于规则库顶部附近，以防止意外阻止它们。这些规则通常允许从任何源区域到任何目标区域的流量，并适用于所有对象和所有用户。

   在 Panorama 上，将这些规则放置在预规则中，以便它们在防火墙上任何本地定义的规则之前执行。
3. 所有其他规则的逻辑是将最具体的规则放置在靠近规则库顶部的位置，将最通用的规则放置在靠近规则库底部的位置。如果您将一般规则放在规则库中的特定规则之前，则您想要匹配特定规则的流量可能会匹配一般规则，这可能会对流量应用与您想要的不同的操作和不同的检查。这称为遮蔽 - 另一种规则也会“遮蔽”您希望流量匹配的规则。
4. 如果您尚未转换或无法将所有基于端口和服务的安全策略规则转换为基于 App-ID 的规则，请将基于 App-ID 的规则放在基于端口和服务的规则之前。

STEP 2 | 使规则库尽可能小，以便于管理并避免规则库膨胀。

1. 如果以下 6 个对象中有 5 个在多个规则中相同，则将这些规则合并为一个规则：
   - 源区域
   - 目的地区域
   - 源 IP 地址
   - 目标 IP 地址
   - 服务端口
   - 应用程序

   例如，如果三条规则指定了不同的应用程序，但具有相同的源和目标区域、源和目标 IP 地址以及服务端口，则您可以将这些规则合并为一条规则，该规则指定每条原始规则中的应用程序。
2. 使用组对象可以简化策略创建并减小规则库大小。

   使用应用程序组和地址组有助于整合适用于所有组成员的规则。

   如果您在策略中同时使用单个对象和组对象，请注意，如果对象在规则中单独指定，并且在规则中指定为对象组的一部分，则该对象在组中的成员资格可能会导致规则遮蔽。在这种情况下，防火墙可能不会采取预期的操作，因为流量可能首先匹配错误的规则。如果可能，请合并规则，除非您的更改控制流程需要特定策略来跟踪访问。如果要以不同于组中其他对象的方式对待某个对象，请从组中删除该对象。
3. 当您不再需要规则时，从安全策略规则库中禁用或删除规则。

   当组织更改应用程序或基础架构时，或者当您不再需要临时测试规则时，可能不需要安全策略规则。如果您不禁用或删除这些规则，它们可能会导致流量出现意外操作。最安全的做法是先禁用规则，以便在禁用规则导致问题时再次启用它。禁用规则时，应用带有禁用规则日期的标签。定期使用 Policy Optimizer 的 规则使用情况功能来检查每条规则的未使用时间。经过一段时间后，如果您确信自己确实不需要该规则，请将其删除。

   请注意仅用于定期活动（例如季度会议或年度会议）的应用程序的规则。配置仅在事件时间段内启用规则的 ***Schedule***（计划）可能是合适的。
4. 使用 Policy Optimizer 来优化规则库。Policy Optimizer 可以查找未使用的规则、包含未使用的应用程序的规则、一段时间内未使用的规则以及没有日志转发配置文件的规则，并且使您能够在安全策略中管理新的 SaaS 应用程序（如果您有 SaaS）安全订阅。
5. 在 Panorama 上，使用适用于组织内多个 VSYS 和防火墙的通用全局设备组来实现通用的全局安全策略规则，例如控制通用基本服务以及要应用于广泛设备组的任何其他服务或应用程序的规则。创建设备组层次结构，以便您不必跨组重复规则 - 使用层次结构一次性编写规则并将其应用到所有适当的防火墙组。
6. 作为定期维护的一部分，定期查看安全策略规则库。

STEP 3 | 要对规则进行例外处理，请将更具体的规则放在更一般的规则之前。

例如，您希望阻止员工访问恶意网站，因此您创建了一条通用安全策略规则来阻止所有员工访问所有恶意网站。但是，您的 InfoSec 团队和 PEN 测试人员需要访问权限才能进行测试。在这种情况下，您创建一条规则，仅允许这些用户访问所需的恶意网站（解密流量、对规则应用最严格的威胁配置文件，并仅指定用于测试的应用程序），并将该规则置于规则库中的一般规则之上。

当 InfoSec 和渗透测试人员尝试访问恶意站点进行测试时，他们会被允许，但没有其他用户符合规则的条件，因此一般规则会阻止他们。如果将 InfoSec 和渗透测试团队访问规则放在常规阻止规则之后，则一般规则会遮蔽特定规则，并且 InfoSec/渗透测试人员流量将与一般规则匹配并被阻止。

STEP 4 | 防止一般规则掩盖更具体的规则。

遮蔽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首先匹配一般规则，并且永远不会与特定规则进行比

较。结果是，当防火墙意图执行特定规则中的操作和检查时，防火墙执行一般规则中配置的操作和检查。一般规则会遮蔽具体规则。

遮蔽规则可能会遮蔽规则库中的多个其他规则。

防止遮蔽的最简单方法是从一开始就正确构建规则库。但是，现有规则库和迁移的规则库可能具有遮蔽规则。要防止和修复遮蔽：

1. 了解您想要对流量采取的操作以及您想要如何检查它。

   如果特定规则中的操作和检查是您想要处理流量的方式，请将特定规则移至规则库中的一般规则上方。如果一般规则中的操作和检查是您想要处理流量的方式，那么您不需要特定的规则。

2. 将更具体的安全策略规则放置在规则库中的一般规则之上。如果将一般规则放在前面，它会掩盖特定规则，例如：

   1. 创建阻止所有对 Facebook 的访问的一般规则。
   2. 创建允许营销和 PR 小组访问 Facebook 的特定规则，但将该规则置于规则库中一般 Facebook 规则的下方。
   3. 一般规则会阻止所有 Facebook 访问，无论用户组如何，因此流量永远不会与允许访问您想要允许的特定组的特定规则匹配。

   修复方法是将特定规则移至规则库中一般规则之上。

3. 查看并解决遮蔽规则，以确保防火墙执行您想要的操作并以您想要的方式检查流量。

   当您编写新的安全策略规则时：

   1. 选择一个提交选项，然后在防火墙上执行 **Commit**（提交）或在 Panorama 上执行 **Validate Commit**（验证提交）以检查配置问题。不要提交配置。在继续之前解决验证检查发现的问题。
   2. **Commit**（提交）或 **Commit and Push**（提交并推送）配置。
   3. 提交完成后，从右下角功能区中选择 **Tasks**（任务）以打开“任务管理器”。
   4. 在 **Type**（类型）列中，单击 **Commit All**（全部提交）以显示 **Job Status**（作业状态）。（提交和推送不提供遮蔽信息。）
   5. 单击 **Status**（状态）列消息以打开 **Last Push State Details**（上次推送状态详细信息） 并选择 **Rule Shadow**（规则遮蔽）选项卡。如果没有 **Rule Shadow**（规则遮蔽）选项卡，则防火墙没有遮蔽规则。
   6. **Last Push State Details**（上次推送状态详细信息）的左侧显示遮蔽其他规则的规则。每个遮蔽规则的名称是该规则的链接。对于每个遮蔽规则，单击 **Count**（计数）列中的数字以显示其遮蔽的规则。列出了遮蔽规则名称，但它们不是指向遮蔽规则的链接。
   7. 遮蔽规则列表在提交操作中并不持久，因此捕获每个遮蔽规则的遮蔽规则列表至关重要。例如，使用脚本通过 API 提取状态、将列表复制并粘贴到文本编辑器中、截取屏幕截图、拍照或记下遮蔽规则和被遮蔽规则的名称。

为了验证遮蔽规则，*PAN-OS* 配置 ***Commit***（提交）操作。如果检测到规则遮蔽，它会生成一条警告消息，标识受影响的规则。如果在捕获遮蔽列表之前执行另一次提交操作，遮蔽信息将丢失。请务必立即捕获此信息。

8. 在安全策略规则库中查找每个遮蔽和遮蔽规则并捕获每个规则的配置。
9. 将每个遮蔽规则与其并排遮蔽的规则进行比较，并了解每个规则的用途。这使您能够一起评估相关规则并了解您希望如何处理规则控制的应用程序。
10. 当您了解要如何处理遮蔽规则及其遮蔽规则中的应用程序时，可以组合规则以简化规则库、禁用或删除重复规则，并将特定规则移至一般规则之上以解决遮蔽问题。
11. 迭代以修复任何剩余的阴影。
12. 对每个遮蔽规则重复该过程。

在非生产测试系统上，您可能希望保留遮蔽和遮蔽规则以测试新策略规则和其他测试目的。

STEP 5 | 在 Panorama 上，将安全策略规则放置在设备组层次结构中的适当位置。

放置规则，以便您不必在多个设备组中重复相同的规则。多个设备组通用的规则位于层次结构中这些组的上方，因此一条规则适用于所有组。

- 以深思熟虑的方式构建层次结构，只允许访问您想要访问的防火墙组。在构建设备组时请考虑每个防火墙所需的访问权限，并在创建设备组层次结构时请考虑每个设备组所需的访问权限。构建的关键是通用性--哪些防火墙需要类似的访问权限，哪些防火墙组需要类似的访问权限，以及如何构建一个层次结构，使层次结构中较高的组能够包含适用于其下方级别的规则并消除重复的需要规则。
- 将适用于所有防火墙的规则放置在层次结构中的最高组中，以避免规则重复。
- 将适用于防火墙组集的规则放置在层次结构中足够高的位置，以便您不必重复规则。

《Panorama 管理员指南》提供了有关设备组的深入信息，包括设备组层次结构的示例说明。

Policy Optimizer 最佳实践

Policy Optimizer 可帮助您将基于端口的安全策略规则转换为基于应用程序的规则，并转换为最低特权访问策略规则：

- 发现基于端口的规则（应用程序是 **any**（任何）而不是特定应用程序）并将其转换为遵循最小特权访问原则的基于应用程序的规则（**Policies**（策略） > **Security**（安全） > **Policy Optimizer** > **Rules Without App Controls**（没有应用控制的规则））。
- 从过度配置的规则（**Policies**（策略） > **Security**（安全） > **Policy Optimizer** > **Unused Apps**（未使用的应用））中发现并删除未使用的应用程序。
- 发现并消除不使用的规则，并了解策略规则使用情况（**Policies**（策略） > **Security**（安全） > **Policy Optimizer** > **Rule Usage**（规则使用情况））。

- 发现与安全策略规则中使用的应用程序筛选器和应用程序组匹配的新应用程序。评估新应用程序以及是要允许还是阻止它们（**Policies**（策略） > **Security**（安全） > **Policy Optimizer** > **New App Viewer**（新应用查看器））。

  如果您有 *SaaS Security Inline* 订阅并使用 App-ID Cloud Engine (ACE)，请使用 *Policy Optimizer* 将 ACE App-ID 集成到安全策略规则库中。

- 发现未附加日志转发配置文件的安全策略规则，并将日志转发配置文件添加到这些规则（**Policies**（策略） > **Security**（安全） > **Policy Optimizer** > **Log Forwarding for Security Services**（安全服务的日志转发））。

Policy Optimizer 在 *PAN-OS 9.0* 及更高版本中可用于 *Panorama* 和 *PAN-OS* 防火墙（如果 *Panorama* 运行 *PAN-OS 9.0* 或更高版本，则防火墙可以在 *PAN-OS 8.1* 上）。*Prisma Access* 不支持 *Policy Optimizer*。

Cortex Data Lake (CDL) 兼容性要求 *Panorama* 运行 *PAN-OS 10.0.3* 或更高版本，并且具有云服务插件 *2.0 Innovation* 或更高版本。

Policy Optimizer 最佳实践包括：

- 如何使用 Policy Optimizer - 主要用例，如何将应用程序添加到安全策略规则、排序和筛选规则以及使用应用程序筛选器和应用程序组。
- Policy Optimizer 规则库工作流 - 如何规划向基于应用程序的规则的过渡，将基于端口的规则转换为基于应用程序的规则，消除未使用的规则，以及删除未使用的应用程序以加强规则库。

尽快解密当地法规、合规性、业务要求和隐私注意事项允许的所有流量，以提供更准确的应用程序信息，并了解使用 *Policy Optimizer* 控制的应用程序。如果没有解密，防火墙通常可以识别父应用程序，但通常无法识别功能应用程序。例如，防火墙看到 *“facebook”*，但看不到 *facebook-post*、*facebook-download*、*facebook-file-sharing* 等。您必须解密流量才能获得对功能应用程序的可见性和控制。对于 SSL 转发代理（出站）解密，请先实现 *User-ID* 和 *URL* 过滤，以便您可以有效地定位解密。

如何使用 Policy Optimizer

本节介绍主要的 Policy Optimizer 用例以及如何使用该工具。Policy Optimizer 规则库工作流 介绍工作流程。

Policy Optimizer 用例包括：

- 从基于端口的应用程序规则迁移 - 查看与每个基于端口的规则匹配的第 7 层应用程序，选择要允许的应用程序，并将每个规则转换为一个或多个基于应用程序的规则。
- 新部署 - 发现网络上的应用程序，并随着时间的推移过渡到基于应用程序的策略。
- 成熟的部署- 检查您的规则库，将基于应用程序筛选器的广泛规则转换为基于应用程序组的严格规则（仅允许您批准的应用程序），并消除未使用的规则和应用程序。
- **DevOps** - 了解测试环境中的新应用程序或修改的应用程序。在生产环境中进行更改之前，确定如何在安全策略规则中处理它们。在生产环境中应用新规则和修改后的规则之前，请对其进行测试。

STEP 1 | 与适当的人员合作，了解您希望出于业务目的在网络上允许的批准应用程序，以及您希望允许员工使用的允许的应用程序。

注意哪些应用程序是业务关键型的。请注意哪些应用程序仅定期用于季度、年度或其他事件，并评估相关规则足够长的时间以查看这些应用程序的活动。了解允许应用程序的业务逻辑有助于您了解如何构造安全策略。为了更好地了解应用程序，请在 applipedia 中或防火墙/ Panorama 上的 **Objects**（对象） > **Applications**（应用程序）中查找内容交付的 App-ID。

STEP 2 | 了解如何出于不同目的使用不同的指标对 Policy Optimizer 信息和统计信息进行排序、筛选和检查 Policy Optimizer 信息和统计信息。

不会实时报告 Policy Optimizer 统计信息。更新应用程序列表大约需要一个小时或更长时间，具体取决于应用程序流量和规则库大小。将应用程序添加到规则后，请至少等待一小时，然后再检查流量日志以获取应用程序的信息。如果您没有看到该信息，请稍等片刻，然后再次检查。

Policy Optimizer 会忽略仅 ***Log at Session Start***（在会话启动时记录）的规则的流量，以避免对瞬态应用程序进行计数。（对于在 ***Log at Session End***（在会话结束时记录）的规则，*Policy Optimizer* 将选择规则的统计信息。）

STEP 3 | 了解如何在安全策略中使用应用程序筛选器和应用程序组。

使用安全策略规则中的应用程序筛选器来发现网络上的应用程序。然后将这些规则从应用程序筛选器转换为应用程序组，以便指定要允许的确切应用程序。

- 尽可能使用**application groups**应用程序组来简化和收紧安全策略规则，并减小规则库的大小。

  应用程序组是用户定义的特定应用程序集，您希望在一个具有类似安全处理的规则中进行控制。使用应用程序组将应用程序添加到规则（链接的主题侧重于 ACE 应用程序，但适用于所有应用程序）以使用一个规则控制多个应用程序，而不是为每个应用程序创建单独的规则。在不同规则中重用应用程序组，为不同的用户、源和目标提供对应用程序的不同访问权限。重用组可自动将应用程序添加到多个规则（对应用程序组进行任何更改时，更改将反映在包含该应用程序组的每个规则中）。

- 使用应用程序筛选器：
  - 发现网络上的应用程序。
  - 通过自动处理与筛选器匹配的新应用程序来适应未来的规则。这在迁移和新部署的应用程序发现阶段以及成熟环境中都很有用。

    例如，使用基于 **Palo Alto Networks** 标记的应用程序过滤器创建允许规则。这可确保您允许所有当前的 Palo Alto Networks 应用程序和所有未来的 Palo Alto Networks 应用程序。

    另一个示例是创建一个规则，用于筛选新内容交付的 App-ID，以便安全地处理它们，直到您可以更仔细地检查它们。
  - 在成熟的规则库中使用应用程序过滤器将应用程序添加到规则以阻止不需要的应用程序类型。使用应用程序组有目的地允许流量（链接的主题侧重于 ACE 应用程序，但适用于所有应用程序）。

  应用程序筛选器是应用程序的动态集。应用程序根据您定义的属性（如类别、子类别、风险、标记（预定义标记或自定义标记）和特征匹配应用程序过滤器。当新应用程序与筛选条件匹配时，防火墙会自动将新应用程序添加到筛选器。具有应用程序筛选器的安全策略规则会自动控制与筛选器匹配的新应用程序。

  应用程序筛选器是比应用程序组更宽松的控制。您可以准确控制应用程序组中的应用程序。您定义的属性控制应用程序筛选器中的应用程序，这可能会导致允许的应用程序数超过您需要允许的应用程序数。这就是为什么过滤器最适合发现流量和阻止流量的应用程序子类别。在不同的规则中重用应用程序筛选器，为不同的用户、源和目标提供对应用程序的不同访问权限。

尽可能多地使用应用程序组和应用程序筛选器，而不是将单个应用程序添加到规则中。从 PAN-OS 10.1 开始，您可以直接从 Policy Optimizer 将应用程序添加到应用程序组和筛选器，这是一种最佳实践，因为它使您可以查看规则看到的所有应用程序。

在 PAN-OS 10.1 之前，使用 **Objects**（对象） > **Application Groups**（应用程序组）和**Objects**（对象） > **Application Filters**（应用程序过滤器）将应用程序添加到组和过滤器。

STEP 4 | 根据规则的用途确定要添加到规则中的应用程序。该规则的用途有助于确定谁需要访问应用程序以及如何（源、目标、检查、日志记录）授予访问权限。

STEP 5 | 在策略中重用应用程序筛选器和应用程序组对象，以便为不同的用户组提供对这些应用程序的不同访问级别和/或以不同的方式处理不同的源和目标组合。

User-ID 是创建基于最小特权访问原则的最佳实践安全策略不可或缺的一部分。如果没有 User-ID，则无法指定谁可以使用应用程序。

通过简化规则库重用应用程序组和应用程序筛选器对象可减少规则库膨胀。

Policy Optimizer 规则库工作流

本节介绍如何从基于端口的规则过渡到 Policy Optimizer 工具的基于应用程序的规则和工作流。如何使用 Policy Optimizer 介绍主要用例以及如何使用该工具。

最终目标是锁定规则，以便它们仅允许批准的应用程序和您允许员工使用的应用程序。除此之外，锁定具有合法业务理由访问不同应用程序的用户。使用流量日志和 ACC 可帮助您将规则范围缩小到特定用户，以避免过度配置用户访问权限。与应用程序所有者和其他组合作，了解谁有业务原因访问应用程序。

STEP 1 | 规划从基于端口的规则到基于应用程序的规则的分阶段过渡，并了解关键的转换概念和方法。

迁移和新部署规划和方法：

- 对于从基于端口的规则迁移到基于应用程序的规则，请从基于端口的安全策略规则库开始。对于新的部署和迁移，请基于应用程序筛选器创建规则，以了解不同类型的应用程序，并在规则库底部添加捕获全部规则，这样您就不会意外阻止任务关键型应用程序。将最佳实践威胁防护配置文件（双向）和 URL 筛选配置文件（出站流量）应用于这些规则。当应用程序与 catch-all 规则匹配时，请按照第 2 步中的建议确定要首先开始转换和优化的规则的优先级，以及在将不同类型的应用程序转换为基于应用程序的规则之前遵守规则的时间。

  Policy Optimizer 显示与每个基于端口的规则匹配的特定第 *7* 层应用程序（*App-ID*）。

- 直接在 AIOps 中运行最佳实践评估报告以设置基线，以便您了解当前的最佳实践状态。运行定期报告以衡量进度。进度意味着随着时间的推移，基于端口的规则更少、未使用的规则更少，以及具有未使用应用程序的规则更少。

现有部署规划和方法：

- 如果部署由基于端口的规则或主要基于端口的规则组成，请按照前面的建议迁移到基于应用程序的策略。
- 如果部署主要由基于应用程序的规则组成，请在安全策略规则库的底部放置一个捕获全部规则，以发现并了解与其他规则不匹配的应用程序，并使用严格的安全配置文件来阻止恶意流量。按照第 2 步中的优先级建议收紧规则。

将应用程序从基于端口的规则移动到基于应用程序的规则后，请在Policy Optimizer 和 **Reset Rule Hit Counter**（重置规则匹配计数器）中选择基于端口的规则。这将重置 **Days with no new apps**（没有新应用程序的天数）计数器，以便您可以查看何时有更多新应用程序与原始基于端口的规则匹配，并评估是要允许还是阻止它们。

优化规则后，请等到 **Days with no new apps**（没有新应用的天数）至少达到 7 天后，再重新访问该规则以继续优化规则。当 catch-all 规则和基于端口的规则不再看到要允许的应用程序时，请禁用或删除它们。在禁用或删除规则之前，请注意企业仅用于定期事件的应用程序。

STEP 2 | 确定基于端口的安全策略规则（应用程序设置为 **any**（任何）的规则）并将其转换为第 7 层基于应用程序的规则。

在转换的哪个阶段确定要从基于端口的规则转换为基于应用程序的规则的规则的优先级。这些技术适用于迁移和新部署，以及需要收紧规则库的基于应用程序的现有部署：

1. 在新部署和现有部署中，立即阻止已知恶意和有风险的流量。
2. 基于应用程序筛选器实施 catch-all 规则。
3. 一周后使用已知应用程序转换简单规则。例如，控制端口 21 (FTP)、端口 53 (DNS)、端口 22 (SSH) 的规则非常适合快速转换。基于端口的规则中的应用程序越少、知名度越高，就越有信心将其转换为基于应用程序的规则。
4. 30 天后，转换最稳定的规则。在 30 天内没有新应用程序且控制相对较少应用程序的规则是不错的候选项。
5. 至少 30 天后，开始转换 Internet 访问规则（SSL、Web 浏览）和捕获最多流量的规则。
6. 在经过一段适合的时间，以便通过规则监视到应用程序后，请只发现少量应用的规则。
7. 转换规则时，当 **Days with no new Apps**（当没有新应用的天数）至少达到 7 天（对于复杂规则或具有许多应用程序的规则，时间更长）时查看每个规则，并根据需要处理新应用程序。

克隆规则是从基于端口的规则过渡到基于应用程序的规则的最安全方法。克隆将保留原始的基于端口的规则，并将克隆的规则直接放在原始规则的上方。这使您能够从原始规则中分离出特定的、基于应用程序的规则，而不会危及应用程序可用性，如此克隆用例示例所示，该用例示例将 Web 浏览和 SSL 流量迁移到基于应用程序的规则。与克隆规则不匹配的应用程序将继续与原始的基于端口的规则匹配。当原始规则在适当的时间段内停止在网络上看到所需的应用程序时，您可以安全地禁用或删除原始规则。

在转换规则时适当使用应用程序组和应用程序筛选器。

对于迁移方案，请遵循迁移到基于应用程序的策略的最佳实践。

STEP 3 | 检查规则时，请使用应用程序筛选器阻止您知道不希望在网络上使用的应用程序类型。根据子类别、标签和特征阻止流量。使用应用程序筛选器对阻止规则进行例外。不要使用风险作为阻止筛选条件，而是使用风险来确定如何适当地检查、记录和控制流量。

除了用于阻止已知恶意流量的建议的阻止规则外，请定期查看规则并阻止您确定不需要的其他流量：

1. 确定网络上不需要的应用程序类型，并创建与它们匹配的应用程序筛选器。基于这些应用程序筛选器创建阻止规则，并将它们放在任何 catch-all 规则的前面（或从现有规则克隆规则，并将克隆的规则直接放在规则库中原始规则的上方）。
2. 确定在被阻止的应用程序类型中是否存在要允许在网络上使用的特定应用程序。克隆阻止规则，将 **Action**（操作）更改为 **Allow**（允许），然后，除了要允许的应用程序外，删除所有其他应用程序。将允许规则直接放在阻止规则的上方，以创建阻止规则的例外。
3. 监视阻止规则以查看是否要允许任何其他阻止的应用程序。如果为例外创建了允许规则，请将要允许的应用程序添加到该规则中。否则，请为应用程序创建新的允许规则，并将其直接放置在规则库中阻止规则的上方。

例如，文件共享应用程序可能特别危险。解密流量，并在安全策略规则中，仅允许必要的用户用于业务目的的特定文件共享应用程序，并检查和记录流量。在规则库的下一个规则中，使用基于 **file-sharing**（文件共享）子类别的应用程序筛选器来阻止您没有明确、有意允许的所有文件共享应用程序。

STEP 4 | 从过度预配的规则中删除未使用的应用程序。

从规则中删除应用程序之前，请先了解应用程序的用途。

- 比较 **Apps Used**（使用的应用）与**Apps Allowed**（允许的应用）。如果规则允许的应用程序多于规则使用的应用程序，请检查未使用的应用程序并确定是否可以将其删除。
- 请注意，应用程序仅用于季度、年度或其他定期事件。请确保捕获足够长的规则历史记录以查看这些应用程序。还要考虑在测试环境中处于活动状态的应用程序，以及已添加到生产环境中以预期批准应用程序的应用程序。

STEP 5 | 从安全策略规则库中删除未使用的规则。

未使用的规则会使规则库变得混乱和复杂。规则使用情况显示有关不同时间段内未使用规则的信息。评估规则中的应用程序以查看是否需要它们（即使尚未使用）。在删除未使用的规则之前，请考虑：

- 阻止没有匹配的规则 - 请勿禁用或删除这些规则。例如，使用威胁 EDL 的阻止规则不会收到任何匹配。这没有问题，但是，您希望继续阻止以防恶意流量试图访问您的网络。
- 临时规则 - 例如，承包商或审计员的规则。如果有固定的访问时间，请配置计划以控制规则的生效时间，而不是删除这些规则。如果访问是间歇性的，请禁用规则并在需要时启用它们。
- 禁用的策略规则 - 应用包含规则禁用日期的标签。如果在特定时间段（例如，超过一年）内未使用这些规则，则该规则是要删除的候选项。添加 **Description**（说明）以指示禁用规则的原因以及可能需要启用规则的原因或时间，例如，对于审核员或承包商访问。
- 定期使用的应用程序 - 某些应用程序仅用于季度、每年或其他定期事件。捕获控制这些类型应用程序的规则的足够长的历史记录，以确保应用程序不再使用。

STEP 6 | 确保每个规则都附加了适当的日志转发配置文件。

识别没有日志转发配置文件的规则，并向其中添加配置文件（**Policies**（策略） > **Security**（安全） > **Policy Optimizer** > **Log Forwarding for Security Services**（安全服务的日志转发））。

STEP 7 | 将基于应用程序筛选器的宽规则转换为基于应用程序组的窄规则。

使用规则使用情况统计信息来了解如何规则，并使用 Policy Optimizer 将应用程序添加到应用程序组（PAN-OS 10.1 及更高版本；对于 PAN-OS 10.0 及更早版本，请在 **Objects**（对象） > **Application Groups**（应用程序组）中将应用程序添加到应用程序组中），然后创建更严格的规则。

最终目标是仅允许您批准的应用程序，而不是允许与应用程序筛选器匹配的更广泛的应用程序。使用应用程序筛选器发现网络上的应用程序并阻止应用程序的广泛子类别，并使用应用程序组指定要允许的确切应用程序。要使用 Policy Optimizer 将基于应用程序过滤器的规则转换为基于应用程序组的规则，请执行以下操作：

- 根据应用程序筛选器检查与规则匹配的应用程序，并确定要允许的应用程序。
- 对于基于应用程序筛选器的每个规则，选择要允许的应用程序，并将应用程序添加到克隆规则或现有规则中的应用程序组。
- 将应用程序从基于应用程序筛选器的规则移动到基于应用程序组的规则后，请在 Policy Optimizer 和 **Reset Rule Hit Counter**（重置规则匹配计数器）中选择这些规则。这将重置 **Days with no new apps**（没有新应用程序的天数）计数器，以便您可以查看新应用程序何时与这些基于应用程序筛选器的规则匹配。
- 基于应用程序筛选器监视规则，直到 **Days with no new apps**（没有新应用的天数）计数器达到指示规则不再发现新应用程序的阈值。阈值取决于您的环境和应用程序筛选器匹配的应用程序类型。请考虑仅在特定时间段（如季度或年度事件）使用的应用程序，并将筛选器保留足够长的时间以查看这些应用程序，以便将它们添加到相应的应用程序组中。如果应用程

序筛选器规则与网络上所需的应用程序不匹配，请禁用或删除该规则，具体取决于企业的策略。

STEP 8 | 在新应用程序进入您的环境时查看和更新安全策略规则。

定期在新应用查看器中查看新的 App-ID。将应用程序添加到现有和新的应用程序组中，或将应用程序直接添加到现有安全策略规则中。继续将应用程序筛选器转换为应用程序组。

App-ID Cloud Engine 最佳实践

App-ID Cloud Engine (ACE) 可识别防火墙之前标识为 SSL 或 Web 浏览流量的数千个 SaaS 应用程序，而不是特定应用程序。ACE 为这些 SaaS 应用程序提供特定的 App-ID，以便您可以了解、控制并在安全策略中显式使用它们。

ACE 需要 *PAN-OS 10.1* 或更高版本以及 *SaaS Security Inline* 订阅。对于 *Panorama Managed Prisma Access*，*ACE* 在 *Prisma Access* Cloud Services 3.0 Innovation 中可用，并且在 Prisma Access 中也可用。

ACE App-ID 仅在安全策略中受支持。您不能在任何其他类型的策略规则中使用 *ACE App-ID*。

防火墙下载 *ACE App-ID* 的完整目录，但仅下载环境中看到的应用程序的 *ACE App-ID* 签名。

ACE 控制出站流中的 SaaS 应用程序，并充当云访问安全代理 (CASB)。在新部署中，ACE 可识别网络上的 SaaS 应用程序，以简化迁移到第 7 层基于应用程序的策略的过程。

在现有部署中，ACE 提供了工具来安全地了解和管理以前标识为 SSL 或 Web 浏览流量的许多潜在 SaaS 应用程序，并在安全策略中显式控制它们。

尽快解密当地法规、合规性、业务需求和隐私注意事项允许的所有流量，以提供更准确的应用程序信息并获得对 *ACE* 应用程序的可见性。如果没有解密，防火墙通常可以识别父应用程序，但通常无法识别功能应用程序。例如，防火墙看到 *“facebook”*，但看不到 *facebook-post*，*facebook-download*，*facebook-file-sharing* 等。您必须解密流量才能获得对功能应用程序的可见性和控制。对于 SSL 转发代理（出站）解密，请先实现 *User-ID* 和 *URL* 过滤，以便您可以有效地定位解密。

STEP 1 | 在启用 ACE 之前，了解 ACE App-ID 在防火墙上的工作方式。

阅读 ACE 处理和策略使用情况，了解防火墙如何处理 ACE App-ID，包括：

- 防火墙下载 ACE App-ID 的方式和时间。
- ACE App-ID 和内容交付的 App-ID 之间的差异。
- 防火墙如何解决 ACE App-ID、内容交付的 App-ID 和自定义 App-ID 之间的冲突，包括容器应用程序（例如 facebook）及其功能应用程序（例如 facebook-post、facebook-download 等）。

- HA 行为。
- 提交或推送时的 Panorama 行为。

ACE 标识防火墙之前标识为 SSL 或 Web 浏览流量的特定 SaaS 应用程序。启用 ACE 时：

- 如果您的安全策略规则允许 SSL 和 Web 浏览流量，则下载的 ACE App-ID 将与该规则匹配，除非它们与规则中使用的应用程序筛选器匹配。ACE App-ID 根据筛选器的条件（包括标记）匹配应用程序筛选器，就像内容交付的 App-ID 一样。如果 ACE App-ID 与规则中的应用程序筛选器匹配，则会将应用程序隐式添加到规则中。该规则控制 ACE 应用程序而不是 SSL/Web 浏览规则，包括规则的操作（允许或拒绝）、可以访问应用程序的用户、源和目标以及检查和记录应用程序的方式。
- 在将 ACE App-ID 显式添加到规则或 ACE App-ID 与将其隐式添加到规则的应用程序筛选器匹配之前，ACE 应用程序将继续匹配 SSL/Web 浏览允许规则，与启用 ACE 之前相同。
- 如果没有允许 SSL 和 Web 浏览流量的规则，请按照第 3 步中的建议来发现和控制 ACE App-ID。

在策略中显式使用 ACE App-ID 时，防火墙对待应用程序的方式与处理内容传递的应用程序的方式相同。

STEP 2 | 在启用 ACE 之前，请查看安全策略规则库以查找使用应用程序筛选器的规则。

应用程序筛选器允许基于匹配筛选条件（包括标记）的应用程序，因此它们会自动将应用程序添加到规则中，您必须检查这些规则以查看每个筛选器允许哪些特定应用程序以及哪些用户有权访问这些应用程序。当 ACE App-ID 与规则中的应用程序筛选器匹配时，该规则可能不允许与 SSL 和 Web 浏览规则相同的用户。在 SSL 和 Web 浏览规则中有权访问该应用程序的用户可

能会失去对应用程序的访问权限，因为它不再与该规则匹配，并且未在显式规则中指定这些用户。

了解谁需要将哪些应用程序用于业务目的至关重要，尤其是在具有许多规则、应用程序和用户组的环境中。例如，如果在规则的应用程序组中使用 ***Web Apps***（***Web*** 应用）标记，则该标记会将匹配的 *ACE* 应用程序隐式添加到规则中。这些 *ACE* 应用程序与 *SSL* 和 *Web* 浏览规则不匹配，只有 ***Web Apps***（***Web*** 应用）规则中指定的用户才能访问它们。

如果没有规则具有应用程序筛选器，则在启用 ACE 后，ACE 应用程序不会自动匹配现有规则，因为您尚未将任何 ACE 应用程序显式添加到规则。

如果在安全策略规则中使用应用程序筛选器，则在启用 ACE 时：

- 对于拒绝规则，将阻止与规则匹配的 ACE 应用程序，这正是您打算对与拒绝规则匹配的应用程序执行的操作。该规则更有效，因为您现在可以阻止未经批准的 SaaS 应用程序，如果没有 ACE，防火墙将无法识别这些应用程序。
- 对于允许规则，请密切监视规则允许的应用程序。使用筛选器隐式添加应用程序基于条件，而不是管理员有目的地添加特定应用程序。受影响最大的规则是基于广泛标记（如 **Web Apps**（**Web** 应用））的筛选器的规则，该规则适用于大多数 ACE 和内容交付的 App-ID。

在现有部署中，请记住，如果您有一个允许 *SSL* 和 *Web* 浏览流量的规则，则会允许 *ACE* 现在识别的所有应用程序。使用应用程序筛选器阻止您确定不需要的流量类型，并在评估要批准的内容和要阻止的内容时继续允许其余应用程序。

第 3 步、 4 步和 第 5 步演示如何使用应用程序筛选器安全地将 ACE App-ID 添加到规则。

STEP 3 | 显式允许使用应用程序筛选器的 ACE 应用程序，以便可以以受控方式评估应用程序。

创建应用程序筛选器以允许网络上所需的应用程序类型比定期查看所有新的 ACE 应用程序以确定允许哪些特定应用程序更容易。应用程序筛选器使您能够并行检查相同类型的应用程序，并确定要允许将哪些应用程序用于业务目的。

1. 基于 **App-ID Cloud Engine** 标记创建应用程序筛选器，该标记匹配所有 ACE App-ID（在 ACE 之前标识为 SSL 或 Web 浏览的应用程序）。将筛选器附加到具有相应安全配置文件和日志记录的安全策略规则，并将规则放在安全策略规则库的底部。这可确保规则匹配并允许所有新的和现有的 ACE App-ID，除非在早期规则中指定了这些 ACE App-ID。它还确保防火墙阻止规则在防火墙将流量与 ACE 允许规则进行比较之前生效。
2. 随着您对 ACE 应用程序的日益熟悉，请根据子类别、标记、风险和特征创建更具体的应用程序筛选规则，以匹配较小的应用程序组。将这些允许规则直接放在基于**App-ID Cloud Engine** 标记的一般 ACE 允许规则之上。缩小与筛选器匹配的应用程序的范围使您能够并排检查更相似的应用程序，并确定要允许哪些应用程序用于业务目的。

3. 经常查看 Policy Optimizer 中的新应用查看器，以了解哪些下载的 ACE App-ID 与安全策略规则匹配，并更好地了解这些应用程序。评估应用程序并确定是允许还是阻止它们。

不要将用户添加到具有应用程序筛选器以扩大其范围的规则，因为这允许对应用程序进行比所需更多的访问。过度配置用户访问权限会增加风险，并违反零信任网络访问原则。仅允许出于业务目的需要访问的用户。

STEP 4 | 使用应用程序过滤器根据子类别、标记和特征阻止网络上不需要的应用程序类型。不要使用风险作为阻止筛选条件（风险是对类别或子类别内相对风险的评估，不一定是恶意使用的评估）。使用风险来确定如何适当地检查、记录和控制流量。

与定期查看所有新的 ACE 应用程序以确定您希望在网络上做什么和不希望做什么相比，基于应用程序筛选器的阻止更容易。使用应用程序筛选器意味着防火墙会立即阻止您知道不需要的新应用程序。

1. 确定网络上不需要的 ACE 应用程序类型。基于这些应用程序类型创建阻止规则，并将它们置于 catch-all 规则之上。
2. 确定这些类型中是否存在要允许在网络上使用的特定应用程序。如果要允许某些应用程序：
    1. 克隆阻止规则。
    2. 将 **Action**（操作）更改为 **Allow**（允许）。
    3. 从规则中删除除要允许的应用程序之外的所有应用程序。
    4. 指定需要访问允许的应用程序的用户，添加相应的安全配置文件，并配置日志记录。
    5. 将新的允许规则直接放在阻止规则的上方，以创建阻止规则的例外。
3. 监视阻止规则以查看是否有任何其他要允许的特定应用程序，并将其添加到现有允许规则或创建新的允许规则以设置这些例外。

例如，文件共享应用程序可能特别危险。仅允许用于业务目的的文件共享应用程序，仅允许必要的用户使用，并检查和记录流量。在安全策略规则库的下一个规则中，使用基于 **file-sharing**（文件共享）子类别的应用程序筛选器来阻止未明确、有意允许的所有文件共享应用程序。监视阻止规则以确保它不会阻止要允许的文件共享应用程序。

STEP 5 | 将基于应用程序筛选器的宽规则转换为基于应用程序组的窄规则。

规则使用情况统计信息显示您的环境中规则的使用情况。使用 Policy Optimizer 将应用程序添加到应用程序组（PAN-OS 10.1 及更高版本）或手动将应用程序添加到应用程序组以创建更严格的规则。

最终目标是仅允许您批准的应用程序，而不是允许与应用程序筛选器匹配的更广泛的应用程序。使用应用程序筛选器发现网络上的应用程序，并使用应用程序组指定要允许的确切应用程

序。要使用 Policy Optimizer 将基于应用程序筛选器的规则转换为基于应用程序组的规则，请执行以下操作：

- 根据应用程序筛选器检查与规则匹配的应用程序，并确定要允许的应用程序。
- 对于基于应用程序筛选器的每个规则，选择要允许的应用程序，并将应用程序添加到克隆规则或现有规则中的应用程序组。
- 将应用程序移到基于应用程序组的规则后，请在 Policy Optimizer 和重置规则匹配计数器中选择基于原始应用程序筛选器的规则。这将重置 **Days with no new apps**（没有新应用程序的天数）计数器，以便您可以查看新应用程序何时与基于应用程序筛选器的规则匹配。
- 基于应用程序筛选器监视规则，以查看 **Days with no new apps**（没有新应用的天数）计数器何时达到指示规则不再看到新应用程序的阈值。阈值取决于您的环境和应用程序筛选器匹配的应用程序类型。考虑仅在特定时间段（如季度或年度事件）使用的应用程序，并将筛选器保留足够长的时间以查看这些应用程序。如果应用程序筛选器规则与网络上所需的应用程序不匹配，请禁用或删除该规则，具体取决于企业的策略。

将基于规则库底部的 ***App-ID Cloud Engine*** 标记的规则保留为捕获全部规则，以允许新的 *ACE* 应用程序。从基于应用程序筛选器的规则移动到基于应用程序组的规则后，所有新的 *ACE App-ID* 都与捕获全部规则匹配。定期检查规则以确定要添加到现有规则和应用程序组的应用程序、哪些应用程序需要新规则以及要阻止哪些应用程序。

STEP 6 | 经常检查 **New App Viewer**（新应用程序查看器），以了解和显式控制以前标识为 SSL 或 Web 浏览应用程序的新 ACE App-ID。在策略中显式使用新的 ACE App-ID，而不是作为 SSL 或 Web 浏览应用程序。

在 Policy Optimizer 的新应用查看器中查看防火墙定期下载的新 ACE App-ID。使用 Policy Optimizer 将应用程序添加到现有和新的应用程序组，或者将应用程序直接添加到现有安全策略规则。继续使用 Policy Optimizer 将应用程序筛选器转换为应用程序组。

策略建议最佳实践

SaaS 策略建议和 IoT 策略建议使 SaaS Security 和 IoT Security 管理员能够创建安全策略建议并将其提交至：

- PAN-OS 防火墙和 Panorama（SaaS 和 IoT 策略建议）。
- Panorama Managed Prisma Access（SaaS 和物联网策略建议）。
- Cloud Managed Prisma Access 权限（仅限 SaaS 策略建议）。

基于云的服务（例如 *IoT* 和 *SaaS* 策略建议）不能用于空隙环境，因为它们需要云连接。

在空隙环境中，对于 *IoT Security*，可以考虑使用 *Panorama* 作为管理引擎，用于与云服务交互并接收策略建议。然后将建议推送到没有云连接的托管防火墙。此解决方案仅适用于策略建议本身。诸如设备到 *IP* 映射之类的功能仍需要托管设备的云连接。

SaaS 策略建议控制 PAN-OS 和 Prisma Access 中未经批准的 SaaS 应用程序。物联网策略建议控制 PAN-OS 和 Panorama Managed Prisma Access 中的非托管网络设备。它们的工作流程有很多相似之处。

要求：

- SaaS 策略建议：
  - SaaS Security Inline 许可证

    SaaS Security Inline 许可证包括 App-ID Cloud Engine (ACE)，它为策略建议提供了数千个 SaaS App-ID。SaaS 策略建议需要 ACE 部署。
  - PAN-OS 10.1 或更高版本适用于 Panorama 操作系统和 Panorama Managed Prisma Access。
  - 企业数据丢失防护 (DLP)，用于实施最佳实践数据丢失防护并获得数据可见性。
  - 为 User-ID 设置 Azure AD，以便在策略规则建议中指定用户（没有 User-ID 就无法创建基于用户的策略规则）。
- 物联网策略建议：
  - IoT Security 许可证。
  - IoT Security 先决条件。
  - 确保适当的 PAN-OS 支持和/或Panorama Managed Prisma Access 支持。
  - 在要控制物联网设备的每个区域中启用 Device-ID。（Device-ID 对 IoT Security 来说就像 User-ID 对 SaaS Security 一样 - Device-ID 是 IoT Security 的“用户”。）

Panorama 只能将 *SaaS* 和 *IoT* 策略建议推送到具有相应许可证的防火墙，因此必须将其安装在使用 *IoT* 和 *SaaS* 策略建议的防火墙上。如果受管设备没有相应的许可证，则推送失败。

除了许可证外，为了以最佳实践方式正常运行，IoT 和 SaaS 策略建议还要求：

- 使用 SaaS 或 IoT 策略推荐的每台设备上都有有效的设备证书。
- 连接到 Cortex Data Lake (CDL)，便于查看交通。
- 在每个安全策略规则建议中配置的转发到 CDL 的日志。对于 SaaS Security，请至少转发流量日志、URL 过滤日志和威胁日志。

SaaS 策略建议可帮助您控制未经批准的应用程序。

要保护未认可的 SaaS 应用程序，请使用 SaaS Security API。*SaaS Security API* 为受支持支持的常见认可的 SaaS 应用程序提供安全保护，并使您能够管理这些 SaaS 应用程序的策略。

- 策略建议概念 - 在推荐策略之前需要了解的重要想法。
- 策略建议工作流程 - SaaS 和 IoT 工作流程以及工作流程最佳实践。

策略建议概念

SaaS 和 IoT 策略建议在工作流程和目标上有许多相似之处。PAN-OS 和 Prisma Access 中策略建议的工作流程和思考过程也有许多相似之处。查看安全策略规则最佳实践以更好地了解规则组成部分的最佳实践。

Cloud Managed Prisma Access 不支持 *IoT* 策略建议。

SaaS Security 和 IoT Security 管理员向 PAN-OS 和 Prisma Access 提交策略建议。PAN-OS 管理员将 SaaS policy recommendations（SaaS 策略建议）和 IoT policy recommendations（IoT 策略建议）导入 PAN-OS 和 Panorama Managed Prisma Access。Cloud Managed Prisma Access 管理员在云平台中导入 SaaS 策略建议。不同的管理员通常必须合作才能推荐和实施策略规则，因此管理员之间的良好沟通至关重要。

物联网策略建议的一般最佳实践包括：

- 了解发现的设备是否属于您的网络。
- 确保您检测到的设备上发现的应用程序适用于这些设备。
- 了解检测到的设备漏洞。
- 留出足够的时间让 IoT Security 收集足够的设备相关数据，从而高信度地识别它们。

SaaS 策略建议的一般最佳实践包括：

- 了解网络上应该和不应该在网络上安装的应用程序和应用程序类型。创建一份正式列表，列出经批准的、允许的和未经批准的应用程序和应用程序类型，并在获得应用程序的可见性时对其进行适当的标记。查看未认可的应用程序的使用情况数据，并使用筛选器来查看谁在使用应用程序以及如何使用应用程序。使用 **Visibility**（可见性）工具查看已发现的应用程序，然后标记已发现的应用程序。
- 了解您要在文件中查找的数据，以便为策略规则建议创建相应的 DLP 配置文件。
- 大多数 SaaS 策略规则建议都是为了屏蔽流量。将最低权限访问权限原则应用于 SaaS 应用程序要比仅将其应用于内容交付的应用程序更为复杂，因为有成千上万的 SaaS 应用程序需要控制。如果 SaaS 策略建议过于严格，则可能会影响业务应用程序。在屏蔽之前，请务必了解要屏蔽的应用程序和应用程序类型。

  使用筛选器将重点放在高风险类别（例如文件传输和 CMS 应用程序）上，并检查哪些应用程序的使用率最高。首先关注这些类别和子类别。
- 使用尽可能多的基于上下文的组件来创建最低权限访问策略建议。使用 Cloud Identity Engine (CIE)实施 User-ID（需要 Azure AD），为用户和组设置必要的访问例外情况。使用企业 DLP 来防止敏感数据丢失。

- 对于 Cloud Managed Prisma Access，如果组织的管理策略允许，请将 SaaS Security 应用程序添加到云管理控制台。使用云管理控制台管理 SaaS 策略建议（以及 SaaS Security 和其他云应用程序），而不是使用独立应用程序来获得以下好处：
  - 通过单一界面管理所有云安全元素，而不是从不同的应用程序界面进行管理。
  - 一个管理员可以执行所有 SaaS 策略建议操作，包括将规则添加到 Prisma Access 规则库。如果您使用独立应用程序进行管理，则可以创建策略建议，但必须切换到其他应用程序或移交给其他管理员才能将规则添加到 Prisma Access。

> 要在云管理控制台中使用 *SaaS Security* 和企业 *DLP*，必须在控制台中启用 Web Security。（这是一项免费功能，不是订阅。）

您可以使用预定义的策略建议和创建用户创建的策略建议来创建 SaaS 策略建议。

策略建议工作流程

此工作流程适用于 IoT Security 以及 SaaS Security 应用程序（PAN-OS、Panorama Managed Prisma Access）和云管理控制台 (Cloud Managed Prisma Access)。每个步骤都表明涉及哪些管理员。对于每位管理员来说，了解参与策略建议的其他管理员的职责会很有帮助。

STEP 1 | （所有管理员）在管理策略建议不同部分的管理员之间建立开放的沟通渠道。

策略建议通常需要不同的管理员共同推荐、导入新的 SaaS Security 和 IoT Security 策略规则，并将其集成到 PAN-OS 或 Prisma Access 规则库中。设计一个流程，确保 IoT Security 或 SaaS Security 管理员向 Panorama、防火墙或 Prisma Access 管理员提交策略建议时保持良好的沟通。移交发生在 IoT Security 或 SaaS Security 管理员创建新规则、修改现有规则或删除规则并启用（在 SaaS Security 中提交）或激活 (IoT Security) 规则。

管理工作流程是：

1. **SaaS Security** 管理员创建新的规则建议，添加应用程序、用户/用户组和 DLP 配置文件，并设置操作。他们审查规则建议，然后将其提交给 PAN-OS、Panorama Managed Prisma Access 或 Cloud Managed Prisma Access。查看 SaaS 安全管理员协作和创作指南。

   IoT Security 管理员评估自动生成的规则建议，根据需要对其进行修改，创建策略集（基于来自同一设备配置文件中物联网设备的流量的一组规则建议），然后将其提交给 PAN-OS 和 Panorama Managed Prisma Access。

2. **PAN-OS** 和 **Prisma Access** 管理员会导入 SaaS 和 IoT 策略建议。他们评估规则建议，将其导入，并将安全配置文件组和其他对象添加到规则中。他们还会在安全策略规则库中对规则进

行排序。当 Panorama 向防火墙和 Prisma Access 推送策略建议时，防火墙和 Prisma 管理员会导入推荐的规则。

管理员必须进行沟通，将相应的对象添加到推荐的规则中，并了解这些规则的用途。

对于 *Cloud Managed Prisma Access*，同一个管理员可以同时处理 *SaaS* 策略建议和 *Prisma Access* 职责，尤其是在管理员在云管理控制台上同时管理两个应用程序的情况下。

3. **SaaS** 和 **IoT Security** 管理员更新或删除规则建议，然后将更改提交给 PAN-OS 或 Prisma Access。

   PAN-OS 和 **Prisma Access** 管理员可以看到规则更新或删除，然后导入更新的规则或从 PAN-OS 或 Prisma Access 中删除规则。

管理员之间的沟通至关重要，这样各方才能了解推荐规则的用途、规则更新的目的以及删除规则的原因。管理员之间的沟通有助于确保 SaaS 和 IoT 策略建议不会在 PAN-OS 或 Prisma Access 中等待管理员注意到它们的存在并将其导入规则库。

STEP 2 | （*SaaS Security* 和*IoT Security* 管理员）SaaS Security 管理员需要评估未认可的 SaaS 应用程序的风险，IoT Security 管理员需要了解设备配置文件，这些配置文件描述了网络上非托管设备的类型及其行为。

IoT Security 会自动了解网络上的非托管设备，并为每组相似设备创建设备配置文件。配置文件描述了设备的特性。

熟悉网络上的 SaaS 应用程序和 IoT 设备：

- SaaS - 至少等待 7 个工作日的数据，然后再分析应用程序以获得策略建议。收集足够的数据以了解应用程序及其业务用途。

  物联网--监控设备配置文件列表，查看哪些配置文件符合策略推荐条件。当设备配置文件的置信度达到 90% 时，您可以创建策略建议，这表示对设备行为的高度可信度。有些设备产生的流量较少，可能需要一段时间才能获得较高的可信度评级。留出时间让 IoT Security 收集足够的数据，以达到 90% 的可信度评级。

- SaaS - 了解用户使用特定 SaaS 应用程序的方式和原因，以及是否有业务原因允许使用这些应用程序。

  IoT - 了解发现的设备是否属于您的网络。如果您的企业是银行业务，那么在您的网络上看到医疗设备可能表示存在问题。

- SaaS - 根据风险承受能力评估 SaaS 应用程序的安全和隐私、身份访问管理和合规性属性。

  IoT - 在医疗环境中，评估医疗物联网设备的合规风险。

- SaaS - 标记已认可、容忍和未认可的应用程序，以对其进行分类。

STEP 3 | （*SaaS Security* 管理员）配置预定义的 SaaS 策略建议。（IoT Security 管理员跳至第 5 步。）

预定义的 SaaS 策略规则建议可阻止应用程序访问、个人帐户访问以及内容共享和访问，并对相应用户强制执行只读访问权限。将应用程序添加到预定义的推荐中是开始锁定 SaaS 应用程序的简便方法。

要在云管理控制台中使用 *SaaS Security* 和企业 *DLP*，必须在控制台中启用 Web Security。（这是一项免费功能。）

在云管理控制台中，同一个管理员能够创建 *SaaS* 策略建议并将其导入 Prisma Access。

1. 选择预定义的规则。（云管理控制台中 **Discovered Apps**（发现的应用）> **Policy Recommendations**（策略建议）或 **Visibility**（可见性）> **Security Rules**（安全规则）。）
2. 选择应用程序并将其添加到规则中。如果该规则不适用于所有用户，请添加用户和用户组。在屏蔽之前，请务必了解要屏蔽的应用程序和应用程序类型，并了解哪些人需要将某些应用程序用于商业目的。

   首先关注有风险的应用程序类型，例如文件共享、内容管理以及协作和生产力应用程序。减少上传到文件共享站点的次数，这样只有出于业务目的需要上传的用户才能仅访问用于业务目的的文件共享应用程序。
3. 如果您拥有企业 DLP 许可证（最佳实践），请添加 DLP 配置文件以检查流量中的敏感信息并防止未经授权的访问，包括支持的 DLP 应用程序的预定义配置文件。
4. 验证规则是否按照您想要的方式执行您需要的操作。
5. **Save**（保存）默认规则。
6. **Enable**（启用）规则以将其提交给 PAN-OS 或 Prisma Access。必须启用 PAN-OS 或 Prisma Access 管理员才能导入规则。

   与负责检查、评估和导入 SaaS 策略建议的管理员就已启用的规则进行沟通。

STEP 4 | （*SaaS Security* 管理员）配置用户定义的 SaaS 策略建议。（IoT Security 管理员跳至第 5 步。）

使用已发现的应用程序视图中的筛选器来查找应用程序及其使用情况指标，并帮助您了解是屏蔽还是允许应用程序。重点关注风险最高的应用程序类别，例如文件传输、内容管理以及协作

和生产力应用程序。同时具有高 **Usage**（使用率）的高 **Risk**（风险）应用程序往往具有最高的风险潜力。选择应用程序以查看谁在使用该应用程序以及他们如何使用它。

当您配置策略建议并提交时，*PAN-OS* 和 *Prisma Access* 会自动创建任何附加的 *HIP* 配置文件、标签和应用程序组。如果您在目标防火墙上有企业 *DLP* 许可证，则还会创建 *DLP* 配置文件（否则，提交失败）。如果 *SaaS Security* 管理员在规则建议中添加了任何其他类型的配置文件，并且这些配置文件在防火墙上尚不存在，则提交失败。如果防火墙上存在附加的配置文件对象，则提交成功。（*PAN-OS* 或 *Prisma Access* 管理员可以将配置文件添加到导入的规则建议中。在 *Cloud Managed Prisma Access* 中，您只能添加个人资料组，不能添加个人资料。）

所有导入 *SaaS* 策略建议的防火墙上都必须有相应的配置文件许可证。

CIE 的用户组在整个组织中保持一致。如果您不使用 *CIE* 或无法从 *CIE* 进行同步，则 *SaaS Security* 中将无法使用 ***Users & Groups***（用户和群组）配置，并且您无法根据用户推出 *SaaS* 策略建议。最佳实践是使用 *CIE*，并根据谁需要出于业务目的访问应用程序来创建应用程序策略。

要实施 *SaaS Security* 和企业 *DLP*，必须在云管理控制台中启用 Web Security。（这是一项免费功能。）

在云管理控制台中，同一个管理员能够创建 *SaaS* 策略建议并将其导入 Prisma Access。

要配置最佳实践 SaaS 策略建议，请执行以下操作：

1. 创建新的 SaaS Security 策略建议：
   - SaaS Security 控制台：**Visibility**（可见性） > **Security Rules**（安全规则） > **Create New Rule**（新建规则）
   - 云管理控制台：**Discovered Apps**（已发现的应用） > **Policy Recommendations**（策略建议） > **Add Policy**（添加策略）
2. 请遵循指定规则名称和描述的最佳实践。
3. 向规则中添加应用程序。

   使用类别、风险和功能筛选器查找 SaaS 应用程序。直接从筛选结果中将应用程序添加到规则中。首先关注风险最大、使用率最高的应用程序。
4. 选择要检测的 **User Activity**（用户活动）。为该规则选择的所有应用程序都必须支持选定的用户活动。如果应用程序不支持某项活动，则界面会返回错误。
5. 配置规则的其余参数：
   - **Users & Groups**（用户和群组）- 您必须使用并从 CIE 进行同步，才能在 SaaS 策略建议中指定用户和群组。

- **Device Posture**（设备状态）- 指定哪些类型的设备可以访问规则的应用程序。在 PAN-OS 或 Prisma Access 中导入规则时，设备状态会自动为移动设备创建主机信息配置文件 (HIP) 对象。
- **Data Profile**（数据配置文件）- 您必须拥有 SaaS Security 和目标防火墙中的企业 DLP 许可证才能使用此功能。通过订阅 Enterprise DLP，您可以为特定 DLP 配置文件创建规则，并且只有在应用程序包含与配置文件匹配的数据时才会将其屏蔽。
- **Response**（响应）- **Allow**（允许）或 **Block**（阻止）匹配规则的流量。大多数建议都是阻止规则，以防止过度配置访问权限。

6. 验证规则是否按照您想要的方式执行您需要的操作。
7. **Save**（保存）规则。
8. **Enable**（启用）规则以将其提交给 PAN-OS 或 Prisma Access。必须启用 PAN-OS 或 Prisma Access 管理员才能导入规则。

   与负责检查、评估和导入 SaaS 策略建议的 PAN-OS 或 Prisma Access 管理员就已启用的规则进行沟通。

   创建 SaaS 策略规则建议提供了有关工作流程的更多详细信息。

STEP 5 | （*IoT Security* 管理员）在 IoT Security 应用程序中配置物联网策略建议（仅限 PAN-OS 和 Panorama Managed Prisma Access）。

当 IoT 的置信度分数（IoT Security 对识别设备的可信程度）达到 90% 或更高时，IoT Security 会根据属于设备配置文件的设备的行为生成 IoT 策略建议。随着 IoT Security 收集有关设备的更

多信息，置信度分数会随着时间的推移而提高。在将自动生成的规则提交给 Panorama、防火墙或 Prisma Access 之前，您可以对其进行编辑。

IoT Security 不为 *PC*、智能手机或平板电脑等 *IT* 设备提供策略建议，但 *IoT Security* 确实可以识别这些设备。

使用自动策略建议，根据多个 IoT Security 租户中同一设备配置文件中物联网设备的行为创建策略规则集。策略规则集包括您为控制设备配置文件中的设备而选择的策略规则建议。

1. 通过以下两种方式之一创建新的 IoT Security 策略建议：
   - 导航到“配置文件” 页面，将光标悬停在配置文件名称上，然后在弹出窗口中单击 **Create Policy Set**（创建策略集）。
   - **Profiles**（配置文件） > **<profile-name>** > **Behaviors**（行为），选择 **Outbound Behaviors**（出站行为），再选择 **Create Policy**（创建策略），然后单击 **Next**（下一步）。
2. **Select Policies**（选择策略）以显示针对所选设备配置文件自动生成的策略建议，包括设备使用的应用程序。
   1. 确保您在列表中看到的应用程序适用于这些设备。例如，当您查看打印机或相机时，您不应该看到 iTunes 应用程序。如果您在列表中看到意外的应用程序，则设备可能遭到入侵。

      了解您的设备和设备配置文件，以便您可以制定适当的建议来管理它们。
   2. 查看 **Alerts Raised**（已发出的警报）。在将警报添加到策略集之前，请先调查具有大量警报的应用程序，尤其是在警报严重性很高或严重的情况下。
   3. 选择要应用于设备的策略。这些策略包含在为设备配置文件设置的策略中。

      如果您没有看到要包含在策略集中的应用程序，请 **Add Rule**（添加规则）以手动选择应用程序和目标类型，然后 **Create**（创建）规则。
   4. 默认情况下，该规则适用于在设备配置文件流量中检测到的所有（**Any**（任何））目的地。如果要限制应用程序的目的地，请单击 **Destination**（目的地） > **Any**（任何），将

Allow any destination（允许任何目的地）关闭，然后取消选中列表中您不想允许的目的地。

5. 如果您对策略集包含的所需规则感到满意，请选择 **Next**（下一步）。

3. 在 **Firewall Configuration**（防火墙配置）> **Policy configurations**（策略配置）中，根据需要修改自动生成的建议。**Policy configurations**（策略配置）显示选定的应用程序。
   - 请按照最佳实践指定策略集名称和描述。请务必使用名称来标识规则的用途，并且描述说明了规则的用途。
   - 将 **Services**（服务）保留为 **application-default**（应用程序默认值），以防止应用程序使用非标准端口，这表明存在规避性、潜在的恶意行为。
   - 在 Panorama 或防火墙上添加安全配置文件和安全配置文件组、日志转发配置文件以及其他对象，而不是在 IoT Security 应用程序中。
4. 查看策略集。如果您确定已根据需要对其进行配置，则 **Create**（创建）策略集，这也会将其保存。
5. **Activate Policy Set**（激活策略集）以使策略规则建议可在 Panorama 和各个防火墙上导入。

   与负责检查、评估和导入 IoT 策略建议的 PAN-OS 或 Prisma Access 管理员就已启用的规则进行沟通。

创建 IoT 策略集提供了有关工作流程的更多详细信息。

STEP 6 | （Panorama 和防火墙管理员）（仅适用于 SaaS Security 的 Cloud Managed Prisma Access 管理员）评估、导入策略规则建议，并在必要时修改策略规则建议。

由于云管理控制台允许在一个地方管理所有云应用程序，因此 *Cloud Managed Prisma Access* 管理员可能是创建 *SaaS Security* 策略建议的同一个管理员。

在导入规则之前：

- 在 Panorama、防火墙和/或云管理控制台上创建安全配置文件组，供您应用于导入的 SaaS Security 和 IoT Security 策略建议。至少创建配置文件组，对大多数流量发出警报并阻止已知的恶意流量以保持可用性随着时间的推移您对策略建议的了解会越来越多，请遵循安全配置

文件最佳实践，在不危及访问关键业务应用程序和设备的能力的情况下使配置文件组尽可能严格。

对于 SaaS 配置文件组，要了解应用程序的类型并了解谁使用应用程序，以确定要使用哪些配置文件以及一开始应该有多严格。

对于 IoT 配置文件组，请了解您的设备和设备配置文件，以便您可以创建适当的安全配置文件组来管理它们。了解规则中应用程序的含义，以便您可以将相应的安全配置文件应用于群组。

创建安全配置文件组时，请咨询 IoT Security 和/或 SaaS Security 管理员，以确保安全配置文件组对 IoT 和 SaaS 策略建议有意义。

- 在 IoT Security 部署中，在要控制物联网设备的每个区域中启用 Device-ID。Device-ID 对物联网设备来说就像 User-ID 对用户来说一样，App-ID 对应用程序来说就是一个唯一的标识符。在未启用 Device-ID 的区域中，您无法在 IoT 设备上强制执行安全策略。
- SaaS 策略建议需要 App-ID Cloud Engine (ACE)，它可以识别成千上万个 SaaS 应用程序，以便您可以创建安全策略来控制它们。ACE 需要将日志转发到 Cortex Data Lake。创建 CDL 配置文件时，请遵循日志转发最佳实践。

> 如果您在任何安全策略规则中使用 *ACE App-ID*，即使该规则仅适用于一个用户或用户组，防火墙也会对所有用户强制执行 *ACE App-ID*。（一旦您在策略中使用 *ACE App-ID*，防火墙就会强制执行 *App-ID*，就像强制执行内容提供的 *App-ID* 一样。）

要导入 SaaS 和 IoT 策略建议，请执行以下操作：

1. 定期检查是否有导入的规则。刷新 IoT 或 SaaS 策略建议页面，确保您看到最新的策略建议：
   - Panorama：**Panorama** > **Policy Recommendation**（策略建议） > **SaaS** 或 **Panorama** > **Policy Recommendation**（策略建议） > **IoT**。
   - 防火墙：**Device**（设备） > **Policy Recommendation**（策略建议） > **SaaS** 或 **Device**（设备） > **Policy Recommendation**（策略建议） > **IoT**。
   - Cloud Managed Prisma Access 权限（仅限 SaaS 策略建议）：选择 **Policy Recommendation**（策略建议） > **Manage**（管理） > **Web Security** > **Web Access**

Policy（**Web** 访问策略），然后选择 **Policy Recommendations**（策略建议）选项卡以查看 **New SaaS Rule Recommendations**（新建规则建议）。

2. 选择并评估新规则。确保导入的规则中的所有对象、地址等都有意义。如果您不确定建议中的某些内容，请咨询 IoT Security 或 SaaS Security 管理员，确保您了解该规则及其组成部分的用途。

   对于 SaaS 策略规则建议，请确保用户对应用程序的访问权限不太广泛。

3. 规则导入过程使您可以修改规则并将其置于安全策略规则库中。选择要导入的一个或多个规则，然后：

   - Panorama 和 PAN-OS 防火墙：**Import Policy Rule**（导入策略规则）。

     一次最多可以导入十个 *IoT* 策略规则。

   - Cloud Managed Prisma Access 权限（仅限 SaaS 策略建议）：**Actions**（操作） > **Import**（导入）。

     在完成以下步骤以添加安全和日志转发配置文件、评估规则并在安全策略规则库中选择其顺序之前，请不要完成规则导入。

   导入规则时，PAN-OS 和 Prisma Access 会自动在策略规则中创建该规则的某些对象：

   - 导入 IoT 策略建议会根据物联网设备配置文件自动创建设备对象，包括设备到 IP 的映射。

     Panorama 导入设备对象并将其推送到托管防火墙后，防火墙会直接从云端下拉设备到 *IP* 的映射。*Panorama* 不参与刷新设备到 *IP* 的映射。

   - 导入 SaaS 策略建议会自动创建任何所需的 HIP 配置文件、标签和应用程序组。对于企业 DLP 配置文件，目标设备必须具有企业 DLP 许可证。任何其他配置文件只有在目标设备上已经存在的情况下才能导入。

4. 向每条规则添加一个安全配置文件组。

   使用配置文件组代替单个配置文件更快、更简单，并且可以防止在规则中意外省略配置文件。它还使您能够从主要发出警报的配置文件组开始，并在获得使用 SaaS 应用程序和 IoT 设备的经验时轻松地将其替换为更严格的配置文件组。

   将配置文件应用于 SaaS 应用程序和 IoT 设备规则有所不同：

   - **SaaS Security** 策略规则建议：
     - PAN-OS 和 Panorama Managed Prisma Access - 将高级威胁防护和高级 URL 过滤最佳实践配置文件应用于 SaaS 应用程序流量。
     - Cloud Managed Prisma Access - 您可以将安全配置文件组应用于策略建议，但不能将单个安全配置文件应用于单个安全配置文件。将安全配置文件添加到配置文件组并将该组应用于规则。

Cloud Managed Prisma Access 的最佳实践安全配置文件建议与 PAN-OS 和 Panorama Managed Prisma Access 的建议略有不同。

- **IoT Security** 策略规则建议 - 为防止恶意行为，请确保安全配置文件适用于设备。与 IoT Security 管理员合作，了解设备配置文件中显示的不同设备的行为和警报。根据行为和警报将配置文件应用于 IoT 策略建议。寻找物联网设备中的常见漏洞，例如制造商凭证薄弱、与有风险的 URL 的连接、过时的防病毒软件、允许访问流氓设备、不安全的协议和 EOL 操作系统，以及未修补或无法修补的设备。
  - 将漏洞保护配置文件和防间谍软件配置文件（以防止命令和控制恶意软件）应用于所有设备。
  - 如果设备有到互联网的出站流量，尤其是到未知目的地的流量，请应用高级 URL 过滤和高级威胁防护。如果设备可以发送文件，请添加高级 WildFire 和文件阻止配置文件。
  - 如果设备有服务器端口并接受传入连接，则除了文件阻止、高级 WildFire 和高级威胁防护配置文件外，还要应用 DoS 防护。

5. 向每条规则添加日志转发配置文件。
   - 要获取 IoT 策略建议，请添加 **IoT Security Default Profile - EAL Enabled**（**IoT Security** 默认配置文件 - 启用 **EAL**）的预定义日志转发配置文件，该配置文件提供了 IoT Security 所需的所有日志类型，包括增强的应用程序日志。
   - SaaS 策略建议要求 ACE 识别 SaaS 应用程序。ACE 要求将日志转发到 CDL，因此基于 SaaS 应用程序的安全策略规则也要求将日志转发到 CDL。

   导入规则后，您可以使用 Policy Optimizer 中的 ***Log Forwarding for Security Services***（安全服务的日志转发），以便一次性将日志转发配置文件应用于多个规则，从而识别未附加日志转发配置文件的安全策略规则（在筛选器中选择 ***None***（无））。

6. 在 Panorama 和 Cloud Managed Prisma Access 中，选择规则是先决规则还是事后规则。（不适用于独立防火墙。）

   评估规则的优先顺序是预先规则，然后是特定于部署的规则，然后是后置规则。Cloud Managed Prisma Access 的预规则和后置规则位于共享配置文件夹中。Panorama 前置规则和后

置规则位于 **Policies**（策略） > **Security**（安全）中。在 Panorama 中，您可以为规则指定设备组。

7. 在安全策略规则库中选择您希望导入的规则遵循的规则。遵循规则库最佳实践。

   请勿选择 ***No Rule Selection***（无规则选择），这会将规则置于安全策略规则库的顶部。规则库的顶部通常是新规则的错误位置。例如，新的允许规则将不受阻止已知恶意流量的关键规则的约束。如果新的屏蔽规则不放在应用程序合法用户的允许规则之后，则可能会阻止合法用户的访问。在规则库中对每条规则进行适当的排序。

8. 检查规则，如果您对此感到满意，请将其导入。

   - **Cloud Managed Prisma Access**—**Import**（导入）。
   - **Panorama** 和独立防火墙 - **OK**（确定）。

     导入规则后，Panorama 管理员必须将规则推送到托管防火墙，防火墙管理员必须先将其导入，然后才能在防火墙上激活规则。刷新 **Device**（设备） > **Policy Recommendation**（策略建议） > **IoT** 或**Device**（设备） > **Policy Recommendation**（策略建议） > **SaaS** 以查看最新建议。

     防火墙管理员可能需要在导入规则后对其进行修改。如果防火墙管理员不确定规则的用途，则应向 Panorama、SaaS Security 或 IoT Security 管理员查询。

     检查安全策略规则库，确保规则顺序正确。

9. （仅限 IoT Security）导入规则后，查看 **Device Object**（设备对象）以检查设备的属性筛选器。

在安全策略中使用物联网设备属性来更好地识别设备。导入 IoT 策略规则会自动导入与设备关联的属性并创建其 Device-ID。Device-ID 对物联网设备来说就像 User-ID 对人们的意义一样。尽管有六个设备属性，但防火墙通常只能从设备接收一个属性。如果设备对象

（**Objects**（对象） > **Devices**（设备））指定了设备不发送到防火墙的属性，则流量与设备不匹配，并且该规则无法控制设备，因此只能指定设备发送到防火墙的属性。

单击规则中的 ***Device-ID*** 可弹出其关联的设备对象。

运行 CLI 命令 **`show iot ip-device-mapping-mp all`** 或 **`show iot ip-device-mapping-mp ip <IP-address>`** 是否收到随规则导入的属性。如果防火墙未收到在设备对象中配置的属性，请从设备对象中移除该属性。

有关详细的配置过程，请参阅相应的管理员指南：

- **IoT Security**：
  - 导入程序
  - 将策略集导入 Panorama
  - 配置设备 ID
- **SaaS Security**：
  - PAN-OS 和 Panorama Managed Prisma Access - 导入 SaaS 策略建议（对于独立防火墙；在 Panorama 上，您还可以指定导入的规则是预规则还是事后规则，然后在 Panorama 中导入规则后将其推送到防火墙。）
  - Cloud Managed Prisma Access - 查看 SaaS 策略建议，导入新的 SaaS 策略建议。

STEP 7 | （所有管理员）根据需要更新和删除策略建议，以使安全策略规则库保持最新。

导入策略建议是一个持续的过程。管理员推荐新规则、修改规则和删除旧规则。随着时间的推移，物联网设备数量不断增长，设备状况也会发生变化。随着时间的推移，SaaS 应用程序的数

量会增加，企业标记为认可、允许和未经批准的应用程序也会发生变化。创建每日、每周和每月项目的清单，以监控和保持对 IoT 设备和 SaaS 应用程序的可见性。

导入更新后的策略建议的程序：

- IoT Security ： 修改和更新 IoT 策略规则建议包括 IoT Security 和 PAN-OS 步骤。
- SaaS Security ：
  - SaaS Security Inline -修改有效的 SaaS 策略规则建议展示了如何修改 SaaS Security 中的现有规则。
  - Cloud Managed Prisma Access - 更新有关Cloud Managed Prisma Access 的导入的 SaaS 策略规则建议。

    如果同一个管理员既是 SaaS 策略推荐又是 Prisma Access 管理员，则可以启用自动更新以自动应用规则建议更改。
  - Panorama Managed Prisma Access 和 PAN-OS - 导入更新的 SaaS 策略建议展示了如何检查和导入更新后的 SaaS Security 策略建议。

删除已删除的策略建议的程序：

- IoT：删除和移除策略规则建议包括 IoT Security 和 PAN-OS 步骤。
- SaaS Security ：
  - SaaS Security Inline - 删除 SaaS 策略规则建议展示了如何删除 SaaS Security 中的现有规则。
  - Cloud Managed Prisma Access - 移除已删除的关于Cloud Managed Prisma Access 的 SaaS 策略规则建议。
  - Panorama Managed Prisma Access 和 PAN-OS - 删除已删除的 SaaS 策略建议。

维护安全策略最佳实践

在规划和部署安全策略最佳实践后，随着网络及其应用程序、用户、设备和基础设施的变化，请保持最佳实践部署。

STEP 1 | 请将所有安全订阅保持最新状态，以避免覆盖范围出现漏洞。

STEP 2 | 保持更新“应用程序和威胁”内容，并遵循应用程序和威胁内容更新的最佳实践。

STEP 3 | 查看发行说明，了解最新功能、默认行为变更、问题等。

STEP 4 | 创建每日、每周、每月（以及您需要的任何其他时期）维护清单。

安全策略部署维护是一项递归任务，因为随着时间的推移，环境中会不断添加和删除新的应用程序、用户和物联网设备。例如，清单可以包括：

- 评估应用程序和威胁内容更新。
- 使用 Policy Optimizer 管理应用程序。
- 查看物联网和 SaaS 策略建议和更新。物联网设备的状态可能会随着时间的推移而发生变化，所使用的 SaaS 应用程序可能会随着时间的推移而发生变化，或者需要区别对待并需要更新。更新应用程序的认可/容忍/未认可标签。
- 设置运行安全态势分析工具的时间。
- 查看发行说明中记录的行为变更和问题。
- 查看安全策略规则，看看是否可以收紧这些规则，或者是否不再需要这些规则。

STEP 5 | 在安全策略中维护 App-ID：

- 查看新的和修改过的内容交付的 App-ID，并根据需要调整规则。
- 在向网络中添加新应用程序时，请将其纳入具体的精细策略规则中。使用标签和应用程序筛选器自动将受制裁的应用程序（包括新的 App-ID Cloud Engine 应用程序）添加到规则中。
- 当公司停止使用某个应用程序时，请将其从允许规则中删除，以防止未经授权的使用。
- 定期查看您的安全策略规则允许的应用程序。

STEP 6 | 在安全策略中维护 User-ID：

- 在向网络中添加新用户时，请将他们添加到相应的用户组以控制他们的访问权限并将他们包括在策略中，或者如果他们不属于任何组，则将其直接添加到规则中。
- 当用户离开公司或合同到期时，请将他们从用户组中移除以阻止访问。如果个人不是作为群组的一员添加的，则将其从规则中删除。
- 从组和策略规则添加和删除用户时，继续遵循用户组映射最佳实践和动态用户组 (DUG) 最佳实践。

STEP 7 | 随着网络和目标的发展，维护和更新安全配置文件和配置文件组。添加新的允许规则时，请确保这些规则附加了相应的安全配置文件。

STEP 8 | 根据需要根据新规则和应用程序更新日志转发：

- 将相应的日志转发配置文件应用于每条新的安全策略规则，或者使用默认的日志转发配置文件将日志转发配置文件自动应用于新规则。如果您使用默认配置文件，请检查规则以确保默认配置文件合适，如果不合适，则将其替换为适当的配置文件。
- 定期查看您正在记录的内容、未记录的内容以及记录方式。确保您记录了要记录的流量，并记录了要记录的所有安全操作中心 (SOC) 操作信息。
- 当管理员加入和离开公司时，更新日志转发配置文件。
- 当新的应用程序进入您的网络时，请更新日志转发以适应它们。

STEP 9 | 使用安全态势分析工具来检查最佳实践部署情况：

- 在 PAN-OS 和 Prisma Access 中，在创建安全策略时使用 Strata Cloud Manager 检查安全策略。
- 定期运行 Strata Cloud Manager 按需最佳实践评估 (BPA)，以衡量部署最佳实践的进展情况。
- 每季度进行一次安全生命周期审查 (SLR)，以便更好地了解您的网络。

STEP 10 | 使用防火墙工具检查活动并根据需要调整安全策略。

- 使用 PAN-OS（也适用于 Panorama Managed Prisma Access）和 Cloud Managed Prisma Access 中的日志信息来调查和监控流量。
- 使用应用程序命令中心查看网络中应用程序、用户、威胁、URL 和内容的图形摘要。
- 使用 App Scope 报告来帮助了解应用程序使用情况和用户活动、带宽使用情况和网络威胁的变化。
- 创建自定义报告以查看要调查的确切数据。

STEP 11 | 定期检查 Policy Optimizer 以检查规则库，查找并修复未使用的规则、过度配置的规则以及包含未使用应用程序的规则。在定期维护中添加检查 Policy Optimizer。

STEP 12 | 使用 SecOps 工具和服务主动监控您的整体安全状况，帮助防范威胁并调查问题：

- Cortex XSIAM 将用于主动监控的 SOC 分析与 SIEM 功能相结合。
- Cortex XSOAR 提供全面的安全编排、自动化和响应，包括响应手册，用于全面的威胁情报管理和实时协作。
- Cortex XDR 提供了一个扩展的检测和响应平台，用于监控和管理云、网络和端点事件和数据。
- SOC 服务，例如 SecOps 预防态势评估、优化和学习研讨会。

STEP 13 | 以下资源提供了有关 Palo Alto Networks 平台、功能和支持的更多信息：

- 安全最佳实践文档门户包含各种手册，例如 IoT Security 最佳实践、管理访问最佳实践和解密最佳实践，以及各种管理员指南中最佳实践主题的链接。
- 管理员指南：
  - PAN-OS 管理员指南
  - Prisma Access 管理员指南（Panorama Managed 和 Cloud Managed Prisma Access 权限）
  - SaaS Security 管理员指南
  - IoT Security 管理员指南
- 文档门户：
  - 云交付安全服务 (CDSS) 文档门户
  - 云身份引擎 (CIE) 文档门户
  - GlobalProtect 文档门户
  - Palo Alto Networks 客户支持门户
- 使用最佳实践监控 IoT Security 部署
- IoT Security 解决方案结构（IoT Security 解决方案工作原理摘要）
- Prisma Access 上的 SaaS Security （Panorama Managed 和 Cloud Managed）
- 对 SaaS Security Inline 问题进行故障排除