Panorama 防火墙管理最佳实践

10.0 (EoL)

docs.paloaltonetworks.com

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

December 3, 2020

Table of Contents

Panorama 添加防火墙最佳实践

Panorama™ 管理服务器是集中管理和监控新一代防火墙的 Palo Alto Networks 网络安全管理解决方案。本文档涵盖了引入新防火墙或将现有防火墙迁移到 Panorama 以简化操作的最佳实践。

> 用例 - 将新一代防火墙引导至 Panorama
> 用例 - 将新一代防火墙迁移至 Panorama

用例 - 将新一代防火墙引导至 Panorama

开始使用 Panorama™ 管理服务器的第一个用例是将新部署为托管设备的防火墙添加到 Panorama。

STEP 1 | **Associate Devices**（关联设备）或 **Import**（导入）多个防火墙，以简化引入流程。

- 从一个位置将防火墙添加到 Panorama 时，使用设备组、模板堆栈、收集器组和日志收集器关联防火墙，而不是在已将防火墙成功添加到 Panorama 后再手动关联。
- 如果要添加大量防火墙，请使用 CSV 文件将所有新防火墙导入 Panorama。通过 CSV 文件，您可以将所有防火墙与设备组、模板堆栈、收集器组和日志收集器相关联，而不需要手动关联。该选项在添加大量防火墙时尤其有用，手动关联防火墙可能需要很长时间才能完成。

STEP 2 | 请启用 **Auto Push on 1st Connect**（首次连接时自动推送）并配置 **To SW Version**（到 **SW** 版本），以便在首次成功连接到 Panorama 时，自动将设备组和模板堆栈配置推送到托管防火墙，并将托管防火墙升级到选择的指定 PAN-OS 版本。这包括在 PAN-OS 升级路径中为每个 PAN-OS 版本自动安装所有必需的内容更新。

- 如果您使用 CSV 文件将所有新防火墙导入 Panorama，请启用 **Auto Push on 1st Connect**（首次连接时自动推送），并在 CSV 文件中配置 **To SW Version**（到 **SW** 版本）以简化导入流程。
- 当实施基于角色的访问控制时，利用设备组和模板管理员以将防火墙添加到其访问域中的设备组和模板，而不是为所有 Panorama 管理员启用超级用户权限。

STEP 3 | 将防火墙成功添加到 Panorama 后，请创建并应用标记，以便更轻松地搜索和筛选托管防火墙。随着使用 Panorama 管理的防火墙的数量不断增加，这有助于让托管防火墙保持有序。

STEP 4 | 如果缺少或没有 IT 人员，而您要将防火墙部署到远程站点，请设置零接触配置 (ZTP) 来简化初始防火墙部署，从而无需远程站点的网络或 IT 管理员，您就可以自动引入新的托管防火墙。

用例 - 将新一代防火墙迁移至 Panorama

开始使用 Panorama™ 管理服务器的第二个用例是将现有防火墙过渡到 Panorama。如果可能，请在迁移过程中与 Palo Alto Networks 销售工程师或专业服务工程师合作，确保将防火墙配置正确迁移到 Panorama。

STEP 1 | 计划是关键 — 在开始迁移之前，务必确保理解以下几点：

- 检查 Palo Alto Networks 兼容性表格，了解 Panorama 与防火墙的兼容性（包括日志收集器和内容版本），从而确保在迁移过程中不会遇到兼容性错误。
- 对于一组防火墙中所有防火墙之间共享的设置，按照减少冗余性和简化设置管理的方式计划设备组和模板层次结构。
- 准备后迁移测试计划，以便在成功将防火墙迁移至 Panorama 后验证关键流量和应用程序流量。

STEP 2 | 当您将防火墙迁移至 Panorama 管理时，请启用 **Import devices' shared objects into Panorama's shared context**（将设备共享对象导入 **Panorama** 的共享上下文），从而避免复制相同的配置对象。

STEP 3 | 成功迁移后，请检查 **Policies**（策略）以识别重复的规则。在 **Commit**（提交）到 Panorama 之前删除一条重复的规则，以避免提交时出错。

STEP 4 | 当您将设备配置包导出或推送到托管防火墙时，请启用 **Merge with Candidate Config**（与候选配置合并）、**Include Device and Network Templates**（包括设备和网络模板）以及 **Force Template Values**（强制使用模板值），从而强制提交防火墙上的任何待处理本地更改（包括推送中的所有设备组和模板），并删除不在 Panorama 上的设备组或模板中的任何本地配置。这样可以确保将 Panorama 管理的基线配置推送到已迁移到 Panorama 的所有防火墙。

STEP 5 | 执行迁移后测试，以验证迁移是否成功，并且所有功能正常。随着时间的推移，请根据需要优化配置。通过移除未使用或重复的对象，使用 Expedition 等工具定期评估配置健康状况，并通过策略优化器来优化安全策略规则库。

Panorama 防火墙配置管理最佳实践

防火墙有两种类型的配置 — 安全和网络。Panorama 使用设备组来管理安全配置（如对象、策略规则以及模板和模板堆栈），以便管理网络配置。

> 在 Panorama 上管理设备组配置
> 在 Panorama 上管理模板和模板堆栈配置
> 在 Panorama 上管理模板和模板堆栈变量

在 Panorama 上管理设备组配置

通过应用继承原则和实施防火墙定义的设备组层次结构，设备组提供了一种组织和重用策略的途径。虽然 Panorama 支持跨层次结构中的多个设备组重用相同的设备组配置，但是，您也可以通过自定义任何本地配置来覆盖继承的配置。

- 当您设计设备组层级结构时，请考虑您的功能和区域需求，并了解前规则与后规则之间的区别。

  例如，创建您希望托管防火墙应用的没有任何例外的安全前规则，同时创建安全后规则来清除与安全前规则不匹配的任何流量。
- 避免过度使用共享设备组，确保小型托管防火墙不会超出功能限制。在适当的设备组级别管理配置对象可以更高效地减少不同步防火墙的数量，因为只要修改一个共享配置对象，所有防火墙都会变成不同步。
- 通过使用自定义地址对象指定地址范围或地理位置，配置自定义区域。

  虽然企业使用 RFC 1918 地址空间，但监管整个 10.0.0x 网络的策略并没有帮助。请使用自定义地址对象来定义自定义区域，从而指定地址范围或地理位置。这样，您可以创建细粒度和相关性更强的策略，从而缩小攻击面。
- 为每个设备组配置 **Master Device**（主设备），从而让 Panorama 可以收集用户组映射。在设备组中配置主设备后，当您创建策略规则时即可使用用户组。此外，您可以使用 Panorama 收集的用户组映射筛选 ACC 和 Monitor（监视）选项卡。
- 关联 **Reference Templates**（参考模板）以参考托管防火墙中不包含的模板中包含的网络配置对象，从而完成安全配置。这样，您可以利用不同设备组和模板的共同配置对象，而不会过度使用 **Share**（共享）设备组，或重新创建相同的网络配置对象。

在 Panorama 上管理模板和模板堆栈配置

利用模板和模板堆栈，在托管防火墙中重用网络和防火墙配置对象的共同设置（如日志记录和高可用性 (HA)），同时，您仍可以根据需要为不同模板堆栈中的多个托管防火墙配置模块化模板（可合并）。

- 即使配置不完整，利用设置的逻辑分组创建模板也可以实现模块化。请注意，配置必须完整，并且在模板堆栈级别（而不是在每个模板中）解析所有参考。您可以重用、引用和覆盖来自不同模板的对象，从而完成模板堆栈配置。
- 创建特定于模型的模板（例如，网络接口配置）和特定于用例的模板（例如，管理员，基于角色的访问控制集）。这使您能够在将正确的模板添加到模板堆栈时混合和匹配它们。
- 使用要在模板中覆盖或位于托管防火墙本地的网络配置来配置模板堆栈。

在 Panorama 上管理模板和模板堆栈变量

创建模板和模板堆栈变量来最大限度利用配置共享，并且在托管防火墙中重用网络以及设备配置对象。

- 在适当位置使用模板和模板堆栈变量，从而利用更少的模板管理托管防火墙配置，并简化配置。

  例如，防火墙之间的 IP 地址通常不同。利用模板变量，您可以通过指定变量（而不是 IP 地址）来创建需要的配置。将配置推送到托管防火墙时，Panorama 可以根据按托管防火墙配置的值为每个防火墙填充正确的 IP 地址。
- 利用默认值无创建变量，确保不会误将不正确的配置推送到托管防火墙。

  一个值得注意的例外是 DNS IP 地址。在最坏的情况下，托管防火墙也仍应该能够解析 DNS 查询。

配置更改管理最佳实践

通过利用基于角色的访问控制 (RBAC) 以及对托管防火墙的分段访问管理管理员的配置更改。利用动态结构（如外部动态列表 (EDL) 和动态用户组 (DAG)），保持策略规则处于最新状态，同时利用细粒度控制管理管理员可以提交和推送到托管防火墙的配置更改。

- 通过 Panorama 管理管理员角色和访问域
- 简化 Panorama 管理的安全规则
- 大型团队的配置更改管理
- 提交 Panorama 配置更改
- 推送 Panorama 配置更改

通过 Panorama 管理管理员角色和访问域

动态环境中成功进行配置管理的关键是为您的团队成员分配适当的特权。Panorama 提供了广泛的基于角色的访问控制 (RBAC)，从而实现细粒度角色定义。RBAC 可以与访问域相结合，从而方便对托管防火墙进行分段访问。这有助于缩小攻击面，避免意外或恶意滥用管理员权限。

有关正确控制对 Panorama 和托管防火墙配置的访问权限的更多详细信息，请参阅安全管理访问权限最佳实践。

- 定义管理角色，帮助管理员成功管理防火墙，避免过度配置访问权限。
- 如果如果您有多个用于不同目的的防火墙子集，请为 Panorama 管理员创建访问域。例如，如果您的数据中心防火墙、边界防火墙和分支机构防火墙由不同的 Panorama 管理员进行管理，则通过配置和分配访问域，将访问权限限制在管理员管理的防火墙范围内。
- 创建设备组和模板管理员，从而在访问域和管理角色内更好地控制对托管防火墙的管理访问权限。这样可以提供最细粒度的访问权限，允许您的团队在不引起操作问题的情况下完成工作。

简化 Panorama 管理的安全规则

在管理策略规则库时，管理安全策略是最重要的任务之一。

- 利用策略优化器和策略规则使用情况的组合，以转换为基于 App-ID 和 User-ID 的安全策略规则，从而使规则库应用程序可感知。

  在安全策略规则中创建用户组，使其更高效且更便于阅读。此外，您可以利用 Expedition 和最佳实践评估 (BPA) 工具来帮助迭代规则库的版本，从而加强安全状态。
- 评估策略规则库时利用全局查找来识别可能已经存在的对象或规则。这有助于减少配置中不必要的混乱，防止降低 Panorama 上的提交速度。
- 对策略规则进行故障排除，从而测试提议的策略规则配置更改是否已经被只需要修改的现有规则处理。这样，您就可以减少重复的策略规则，防止策略规则库变得过大。
- 使用基于标记的规则组识别规则目的、功能、生命周期或其他特征，从而将相似的规则快速排序和分组到一起。通过基于标记的规则组，您可以直观地区分规则库中的规则集。您可以在一个组中管理这些规则集，也可以单独修改组中的单个规则。
- 为策略规则创建和修改强制实施审核注释，从而为支持安全审核的关键运营功能提供支持。具有一系列文档化的审核注释的规则更容易响应审核请求，而不是依赖于规则描述或外部工具。此外，向 Panorama 提交配置更改时，您可以通过输入描述来补充审核注释。
- 使用外部动态列表、动态地址组和动态用户组之类的动态结构精简配置，并简化安全策略规则的维护。随着环境的变化，您可以根据需要修改这些设置（无需提交）。
- 创建安全策略规则时，以免在 **Target**（目标）选项卡中选择一个或多个托管防火墙，因为这会使托管防火墙配置同步状态不可靠。

  这通常称为策略目标。策略目标在防火墙上（而不是在 Panorama 上）进行评估。其结果是，没有向其推送策略规则的托管防火墙可能错误地显示为不同步。设计设备组层次结构，以最大限度减少或避免目标策略的需求。

大型团队的配置更改管理

当大型团队利用 Panorama 来集中管理配置时，发生配置错误。Panorama 支持细粒度操作，包括还原、导入、导出、加载、合并和替换配置操作。您可以在设备组或模板级别执行这些操作。

- 当您尝试将 Panorama 配置快速还原为先前的已知状态时，请考虑仅还原受影响的设备组或模板，而不是整个 Panorama 配置。

  这可以帮助您保留来自其他管理员的更改，因为他们没有对受影响的设备组或模板进行任何配置更改。此外，您可以导出配置，以便离线修改，完成后再将其导入 Panorama。
- 导出正在进行的设备组和模板配置更改，以便将紧急配置更改推送到托管防火墙。导出后，请还原 Panorama 配置，以便进行紧急更改。将更改成功推送到托管防火墙后，您可以导入包括正在进行的配置更改的 Panorama 配置。
- 如果要合并多个 Panorama 配置，请明智地合并设备组和模板配置，以便合并单个 Panorama 上的配置。

提交 Panorama 配置更改

Panorama 提供了多种方法来控制提交过程。了解这些方法并在日常运营中适当采用对您非常有用。

- 当您提交 Panorama 配置更改时，请选择**Commit Changes Made by**（提交以下用户执行的更改），从而只提交您自己的更改，而不提交其他管理员执行的更改。这样可以确保不会误将正在进行或未批准的其他配置更改提交到 Panorama。
- 提交配置更改时，要求管理员 **Preview Changes**（预览更改）并检查更改摘要。对配置更改进行可视化检查通常有助于找出错误，并在以后的操作维护中节省时间。

推送 Panorama 配置更改

Panorama 提供了多种方式来控制将配置更改推送到托管防火墙。了解这些方法并在日常运营中适当采用对您非常有用。

- 在管理员将配置更改推送到托管防火墙之前，要求他们检查推送范围选择（**Commit**（提交）> **Push to Devices**（推送到设备）> **Edit Selections**（编辑选择）），从而验证目标防火墙列表是否正确。

  即使正确设计了设备组层次结构，并且对配置更改进行了完善的计划，但是，在某些情况下，由于维护窗口不同，可能不需要在给定时间内将配置更改推送到所有防火墙。最佳实践是检查目标防火墙列表，确保只将配置更改推送到预期的托管防火墙。
- 保守使用 **Force Template Values**（强制模板值）（**Commit**（提交）> **Push to Devices**（推送到设备）> **Edit Selections**（编辑选择））设置。启用此设置的推送将覆盖整个托管防火墙配置，包括任何本地防火墙配置。

Panorama 上的监视与可见性最佳实践

根据组织需求设计日志基础架构，以获得最佳日志提取和存储性能。然后，利用应用程序命令中心 (ACC)、PDF 摘要报告和自定义报告来识别需要调查和解决的网络活动以及威胁。

- 设计日志记录基础架构
- 在 Panorama 上监视应用程序命令中心 (ACC) 和日志
- 在 Panorama 上生成标准和自定义报告

设计日志记录基础架构

这是在部署新的托管防火墙之前，计划和设计日志记录接触架构的最佳实践。Panorama 管理服务器为设备管理和日志收集提供多个节点。Panorama 模式支持管理防火墙配置以及提取和存储日志。如果您希望 Panorama 只有一个功能，日志收集器模式专为日志提取和存储而设计，而“仅管理”模式则专为防火墙的配置管理而设计。

- 请使用 Panorama 大小调整和设计指南计算日志记录速率，并确定日志存储要求。在决定日志收集器的日志存储容量时很重要，而且它可以基于许多因素（比如法规要求）进行确定。

  当您调整日志存储基础架构时，请咨询销售工程师 (SE)。他们会提供必要的技术专业知识，解释和定制您的部署，满足您的需求。
- 如果由于与此模式相关的许多日志记录限制和局限性，您要部署 Panorama 虚拟设备，请勿使用传统模式。虽然适合于实验室或演示环境，但是，请避免在生产环境的传统模式下使用 Panorama。
- 请在托管防火墙上为日志收集使用单独的接口。这样可以帮助您在与 Panorama 通信的管理接口上保持性能。作为一种可靠的安全最佳实践，为所有接口配置一个允许的 IP 列表。

在 Panorama 上监视应用程序命令中心 (ACC) 和日志

应用程序命令中心 (ACC) 是一款交互式可视化工具，用于帮助您快速理解网络中发生的事件。ACC 可以为托管防火墙的日志提供上下文，让您获得关于威胁的流量模式和可操作信息的见解，以便在调查中加以利用。

- 了解如何使用 ACC 中提供的所有数据交互。
  - 使用 ACC 筛选器深入探索具体信息，如地址或用户。
  - 应用全局筛选器以透视 ACC，从而显示您最关注的详细信息，同时排除无关的信息。
  - 如果利用 GlobalProtect，请查看 **GlobalProtect** 活动小部件，根据 HIP 匹配日志查看 HIP 报告，从而理解访问网络的终端设备的安全状态。
  - 缩小感兴趣的信息的范围后，以 CSV 格式导出 ACC 数据，或者以 PDF 格式导出小部件，以便与有兴趣执行进一步调查或修复的团队共享。
- 自定义 ACC 以确保根据您希望监视的具体网络活动进行定制。

  这可以帮助您在调查特定用户或主机时提高效率。从而让无需切换选项卡或滚动太久就可以获得完整的上下文信息。
  - 添加新的小部件到 ACC 并选择内容活动。
  - 添加新的小部件到 ACC 并选择 **URL** 筛选。
  - 默认情况下会显示 **Threat Activity**（威胁活动）小部件。如果未显示，请添加新的小部件并选择 **Threat Activity**（威胁活动）。
- 选择 **Objects**（对象）> **Regions**（区域），并使用 IP 地址范围创建自定义区域，从而使用安全策略规则。使用自定义区域使 ACC 中的相关网络事件的相关性更强。

  例如，您为分支机构配置了自定义区域，并且注意到某些 IP 地址产生了大量流量，行为可疑。通过利用自定义区域，您可以将可疑网络活动关联到具体的分支机构，并按照相应的步骤来调查和执行修复措施。

在 Panorama 上生成标准和自定义报告

Panorama™ 管理服务器提供了一种集中和聚合关于防火墙部署的所有信息的途径，从而让您生成 PDF 报告并创建自定义报告。

- 识别并将组织使用的所有 SaaS 应用程序分类为 **Sanctioned**（已批准）或 **Unsanctioned**（未批准）。

  Panorama 和托管防火墙会将任何没有“已批准”标记的应用程序视为“未批准”在网络上使用。未批准的 SaaS 应用程序可能会暴露在威胁之下，导致私有和敏感数据丢失。为了更便于调查网络活动，务必对 SaaS 应用程序分类。

  1. 选择 **Objects**（对象）> **Applications**（应用程序）。
  2. 根据需要创建自定义 SaaS 应用程序。
  3. 选择一个或多个 SaaS 应用程序并 **Edit Tags**（编辑标记）。
  4. 从“添加标记”下拉菜单中，选择 **Sanctioned**（已批准）或 **Unsanctioned**（未批准）。
  5. 重复执行步骤 1-4，直到根据需要完成标记 SaaS 应用程序。
  6. 选择 **Commit**（提交）> **Commit and Push**（提交和推送），并 **Commit and Push**（提交和推送）配置更改。
- 根据用户组配置用户活动报告和 SaaS 应用程序使用报告，从而在报告中获得更高级别的细粒度。

  例如，您的财务部门将大量数据存储在 GitHub 中。在用户活动和 SaaS 应用程序使用报告中利用用户组可以更轻松地识别这种可疑行为。否则，如果对整个组织运行报告，可能不会注意到这种可疑行为。
- 配置目标驱动和特定的自定义报告，同时将列的数量限制在必要范围内。

  简明的报告参数更便于识别需要调查的网络活动。

创建自定义报告，如果可行，请使用查询生成器快速缩小结果范围。

例如，一个分支机构位置的目标报告要比所有分支机构位置的报告更有效，可操作性也更强。如果您需要包含多个分支机构的报告，最好是运行几个不同的报告，对每个分支机构进行特定的查询。