paloalto TECHDOCS

BPA 入门

10.2

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

May 13, 2022

Table of Contents

评估安全策略功能采用

最佳实践评估 (BPA) 工具可帮助您了解当前的安全策略功能采用级别，并帮助您评估安全状况的成熟度和有效性。采用 WildFire、漏洞防护、SSL 解密等功能有助于检测和预防攻击。深入了解在不同环境中如何以及在何处使用各个功能，这对于了解如何最好地保护网络及其宝贵资产至关重要。

最佳实践入门介绍了如何访问和运行 BPA。通过 BPA 报告的“功能采用热图”部分，您可以查看安全策略规则库中这些功能的采用情况。观看热图简介视频以了解热图，并利用 BPA 视频库和 BPA+ 视频库来了解关于该工具的更多信息。

在 *Panorama* 管理的环境中，*Panorama* 可以管理大量的新一代防火墙。您是要在 *Panorama* 上还是要在各个防火墙上运行 *BPA*？您需要权衡速度、便利性和完整性。

在 *Panorama* 上运行 *BPA* 既快速又方便，并且可以评估托管防火墙的大部分功能，但不能检查本地防火墙覆盖。

在每个托管防火墙上运行 *BPA* 会评估完整的配置（包括本地覆盖），但需要更多时间。

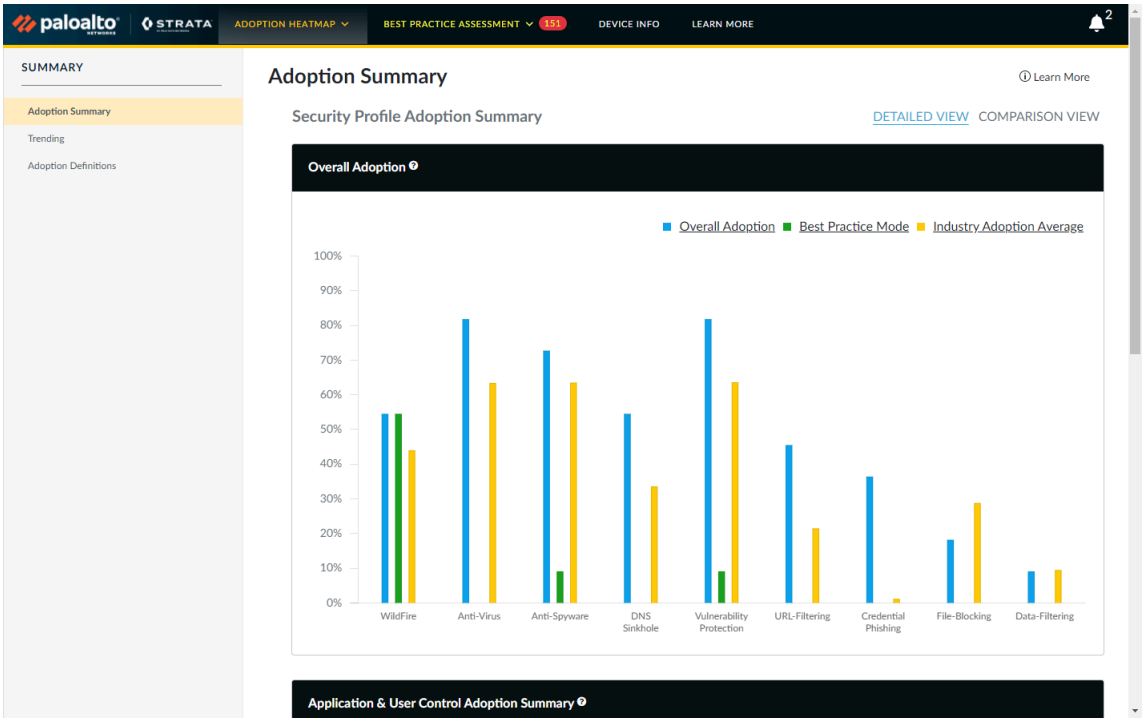
最实用的方法是先在 *Panorama* 上运行 *BPA*。检查结果，决定是否需要关注任何特定托管设备，然后在这些设备上运行 *BPA*。这种方法可以节省时间，同时仍可以专注于相关信息，让您能够改善安全状况。

查看并分析 Heatmap（热图）选项卡上的信息，以确定安全功能采用的差距，并确定要改进的方面：

- 查看采用摘要
- 识别采用中的差距
- 确定要改进的规则

查看采用摘要

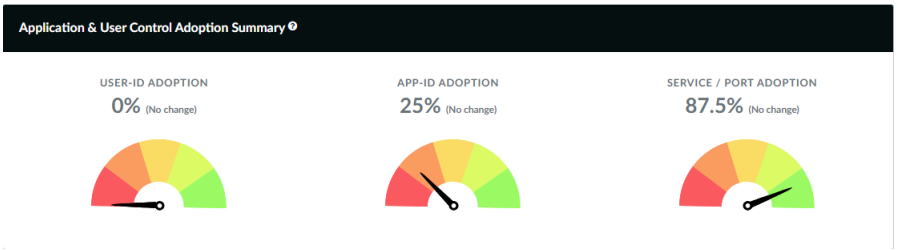
您或您的 Palo Alto Networks 代表运行 BPA 之后，结果 HTML 报告将在“采用热图”页面的“采用摘要”中打开。“采用摘要”视图概述了设备对安全功能的总体采用情况。该报告显示每个指标的当前采用率百分比（除行业平均值外，它提供了行业采用率平均值），并在括号中显示自上次在设备配置文件上运行 BPA 以来的采用率百分比变化（如果该值与您上次运行 BPA 时的值相同，则为 **No change**（无变化））。



整体采用率 — 安全策略允许规则中的安全配置文件采用率。百分比基于启用了一个或多个配置文件的允许规则的数量。BPA 不计算禁用的规则或阻止规则。

行业平均值 — 公司行业在允许规则中采用安全配置文件的平均采用率。

最佳实践模式 — 在允许规则中按建议的最佳实践方式配置安全配置文件的采用率。BPA 仅计算具有通过所有最佳实践检查的配置文件的规则。

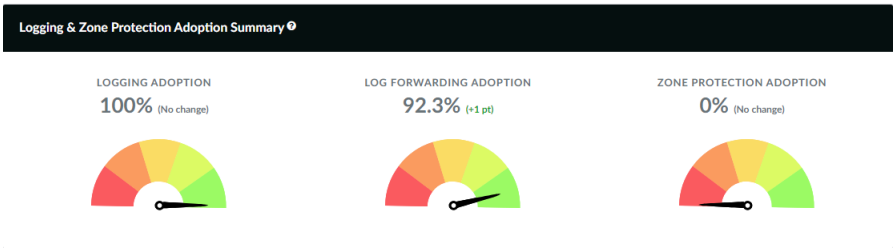


App-ID 采用 — 跨安全策略规则采用 App-ID。该百分比值基于具有一个或多个已定义应用程序的允许规则的总数（应用程序不是 **any**（任何））。BPA 不计算禁用的规则。

User-ID 采用 — 跨安全策略规则采用 User-ID。该百分比值基于具有用户（包括 **known-user**（已知用户）和 **unknown**（未知））或用户组的允许规则的总数。BPA 不计算禁用的规则。

服务/端口采用 — 跨安全策略规则采用服务/端口。该百分比值基于具有已定义服务或端口的允许规则的总数（服务不 **any**（任何））。BPA 不计算禁用的规则。

BPA 不计算阻止规则的 *App-ID*、*User-ID* 或服务/端口采用率，因为阻止的基本原因因企业而异，因此 *BPA* 无法根据阻止规则提出建议。

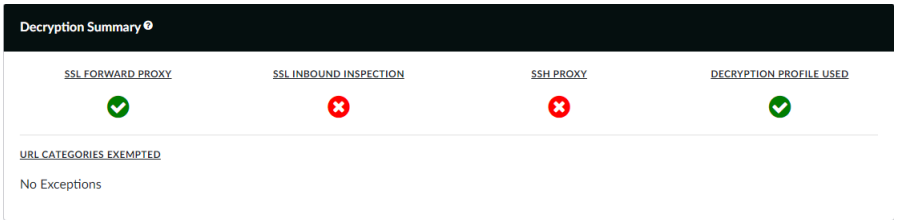


日志记录采用 — 跨安全策略规则的 **Log at Session End**（会话结束时记录）采用率。该百分比值基于已启用 **Log at Session End**（会话结束时记录）的规则总数。BPA 不计算禁用的规则。

日志转发采用 — 跨安全策略规则的日志转发配置文件采用率。该百分比值基于已配置日志转发配置文件的规则总数。BPA 不计算禁用的规则。

区域保护采用 — 跨安全策略允许规则的区域保护采用率。该百分比值基于源区域已配置区域保护配置文件的允许规则的总数。BPA 不计算禁用的规则。

对于这些指标中的每一个，各百分比旁的括号中的值是自上次在设备配置文件上运行 BPA 以来的采用率百分比变化（如果该值与您上次运行 BPA 时的值相同，则为 **No change**（无变化））。



解密摘要 — 如果配置包括 SSL 转发代理、SSL 入站检查和 SSH 代理的解密策略规则，则会显示。该摘要还显示配置是否包括解密配置文件，并标识免除解密的设备的 URL 类别。

如果您不解密 *URL* 类别（或个别应用程序），则无法检查其流量，因为防火墙无法查看加密流量中的内容。防火墙只能检查解密的流量。

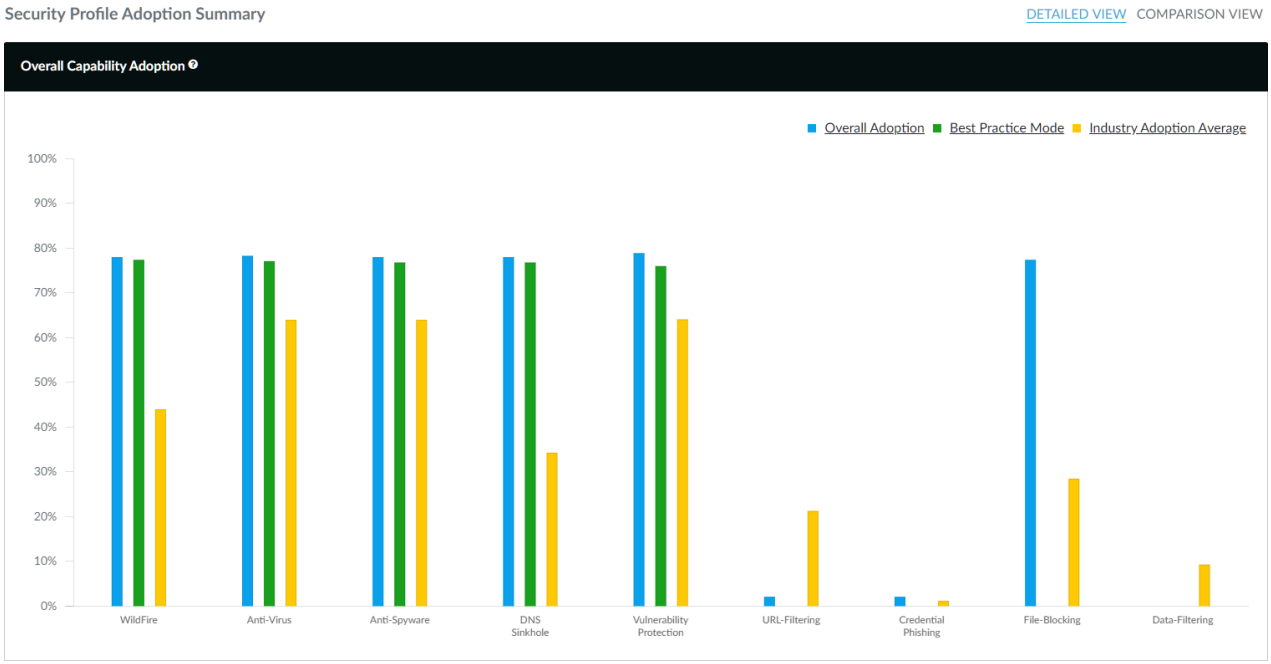
下一步：识别采用中的差距以了解哪些方面可以提高安全性。

识别采用中的差距

采用热图选项显示安全策略的强大之处以及安全策略功能采用方面的差距，从而让您专注于改进弱点。要获得对流量的最大可见性和最大程度的防御攻击，请设立安全功能采用目标，并将以下建议用作最佳实践基准。根据基准评估当前态势，以确定安全策略功能采用中的差距。

采用热图有助于识别可以提高安全策略功能采用率的设备、区域和领域。您可以按设备组、序列号以及 Vsys、区域、基础架构区域、标记、规则详细信息和区域映射查看采用信息。**Local Filters**（本地筛选器）对设备组、基础架构源区域、基础架构目标区域、目标、源区域、目标区域和标记进行筛选，从而缩小范围并识别差距。下面按基础架构区域（**Adoption Heatmap**（采用热图） > **Areas of Architecure**（基础架构区域））显示采用热图：

在 **Adoption Heatmap**（采用热图） > **Summary**（摘要）中，单击 Adoption Summary（采用摘要）以检查以下功能的采用率。使用建议作为差距识别条件 — 如果实际采用率与建议不符，则计划缩小差距：



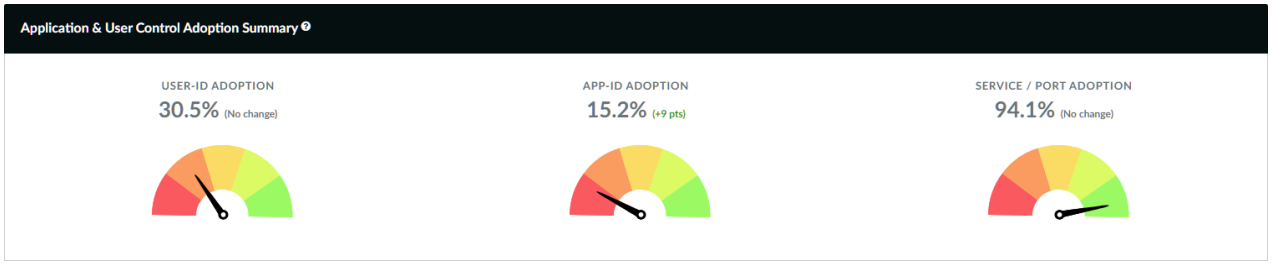
- 将 WildFire、防病毒软件、防间谍软件、漏洞保护和文件阻止安全配置文件应用于允许流量的所有规则，目标是达到 100# 或几乎达到 100# 的采用率。如果您未将配置文件应用于允许规则，请确保有充分的不应用配置文件的业务原因。

  在所有允许规则上配置安全配置文件可让防火墙检查已解密的流量是否存在威胁，无论应用程序或服务/端口如何。更新配置后，运行 BPA 以测量进度并捕获未附加安全配置文件的新规则。

  您可以将 ***WildFire*** 配置文件应用于没有 ***WildFire*** 许可证的规则。覆盖范围仅限于 ***PE*** 文件，但这仍然可以提供对未知恶意文件的有用可见性。

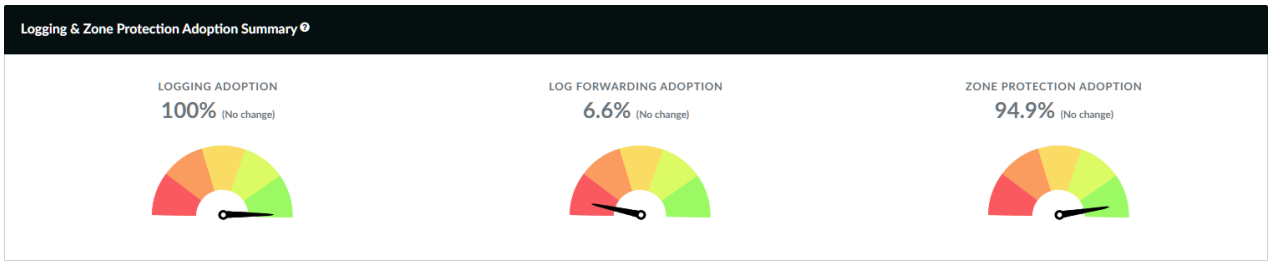
- 在防间谍软件配置文件中，将 DNS Sinkhole 应用于所有规则，以防止遭到入侵的内部主机发送恶意和自定义域的 DNS 查询，从而识别和跟踪可能受到攻击的主机，并避免 DNS 检查中的漏洞。启用 DNS Sinkhole 可在不影响可用性的情况下保护您的网络，因此您可以且应该立即启用它。
- 对所有出站 Internet 流量应用 URL 筛选和凭证防窃（网络钓鱼）保护。

在采用率摘要的应用程序中和用户控制采用摘要中，检查以下功能的采用率。使用建议作为差距识别条件 — 如果实际采用率与建议不符，则计划缩小差距：



- 将 App-ID 应用到尽可能接近 100# 的规则。将 User-ID 应用到具有用户的源区域或地址范围的所有规则（某些区域可能没有用户源；例如，数据中心区域的源应该是服务器，而不是用户）。利用 App-ID 和 User-ID 创建策略，允许适当的用户使用受限制（和容忍）的应用程序。明确阻止恶意和不需要的应用程序。
- 目标为 100# 或接近 100# 的服务/端口采用率 — 不允许非标准端口上的应用程序，除非有充分的业务原因。

在采用摘要的日志和区域保护采用摘要中，检查以下功能的采用率。使用建议作为差距识别条件 — 如果实际采用率与建议不符，则计划缩小差距：



- 目标是采用或接近 100# 的日志和日志转发采用率。
- 在所有区域配置区域保护配置文件

在摘要中：

功能	采用率目标
WildFire	尽可能接近 100# 的安全策略规则
反病毒	尽可能接近 100# 的安全策略规则
防间谍软件	尽可能接近 100# 的安全策略规则
漏洞	尽可能接近 100# 的安全策略规则
文件传送阻止	尽可能接近 100# 的安全策略规则
URL 筛选和凭据防窃	所有出站 Internet 流量
App-ID	尽可能接近 100# 的安全策略规则
User-ID	具有用户的源区域或地址范围的所有规则
服务/端口	尽可能接近 100# 的安全策略规则
记录	尽可能接近 100# 的安全策略规则
日志转发	尽可能接近 100# 的安全策略规则
区域保护	所有区域

查看采用热图时，请使用 **Local Filters**（本地筛选器）缩小范围。使用结果信息来确定安全策略功能的差距，根据差距识别标准进行衡量，并改进或建立新的差距识别标准以供进一步调查。例如，要创建一个显示控制 Internet 机构架构区域流量的规则采用率的筛选器：

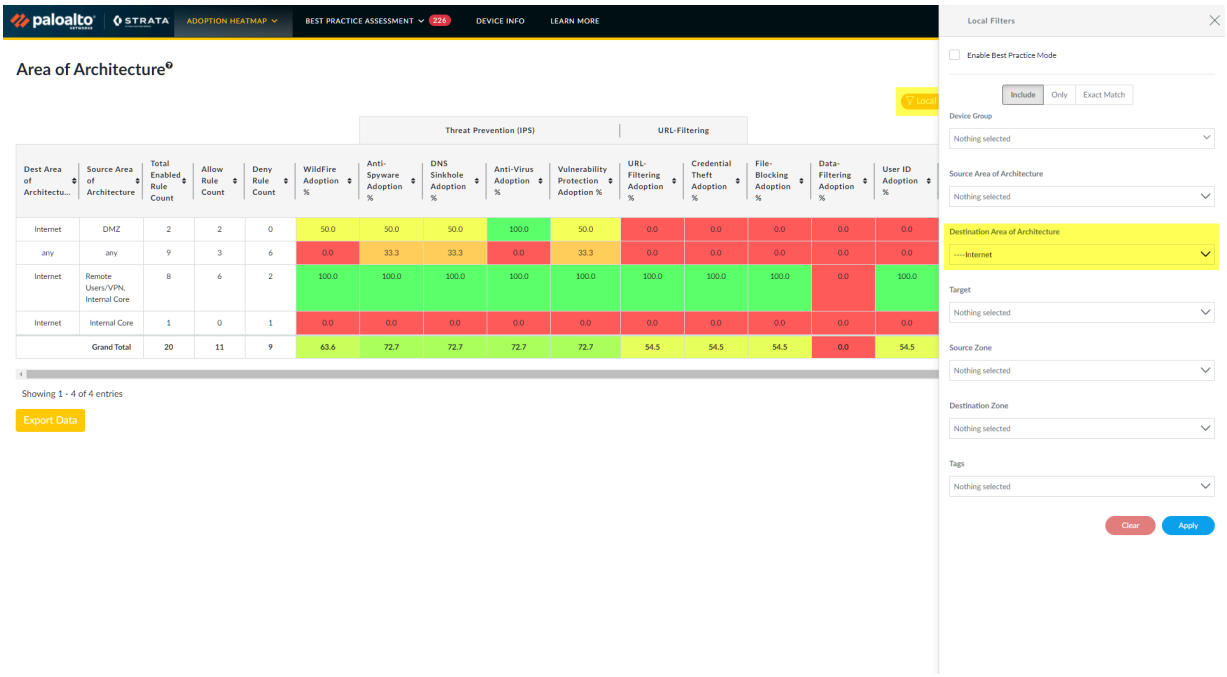
STEP 1 | 选择 **Adoption Heatmap**（采用热图） > **Areas of Architecture**（基础架构区域）。

STEP 2 | 单击 **Local Filters**（本地筛选器），展开筛选器选项。

STEP 3 | 将 **Destination Area of Architecture**（基础架构目标区域）设置为 **Internet**。

STEP 4 | 单击应用。

BPA 筛选结果：



根据安全目标和标准解释结果。例如，如果您的目标是将 WildFire 应用于 100# 的允许规则，而筛选出来的采用热图显示只有 50# 的 DMZ 允许规则具有 WildFire 配置文件，这样您便确定了需要改进的目标差距。

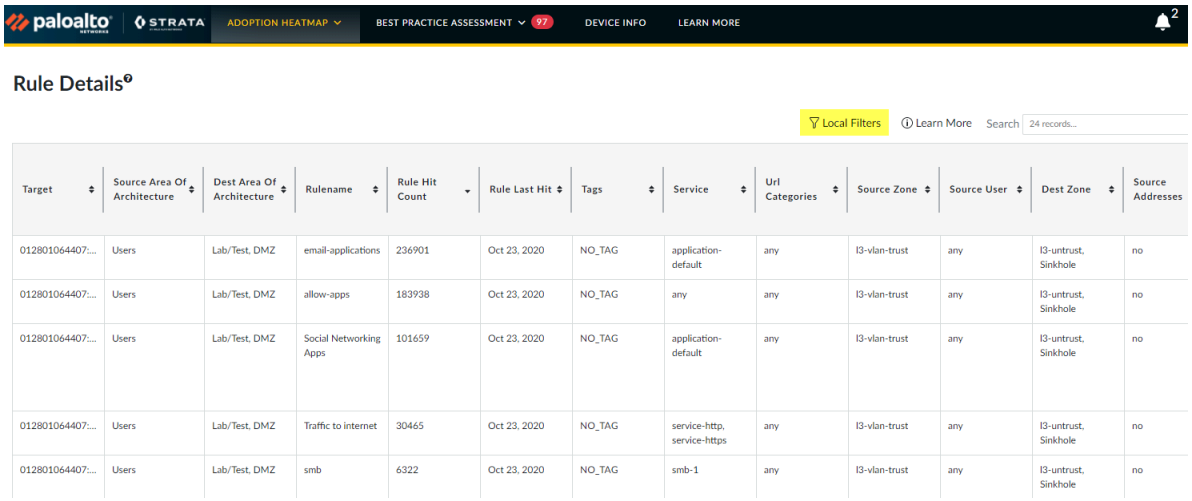
STEP 5 | 下一步：确定要改进的规则。

确定要改进的规则

在确定安全策略功能采用的差距后，请使用 **Adoption Heatmap**（采用热图） > **Rule Detail**（规则详细信息）视图列出需要进一步调查或修复的规则。配置 **Local Filters**（本地筛选器）以匹配在确定采用方面的差距时制定的差距识别条件。这会生成规则列表，您可以将其导出并交给负责防火墙安全策略的运营团队。

例如，要创建规则详细信息筛选器以识别允许所有流量且未配置漏洞保护配置文件的规则：

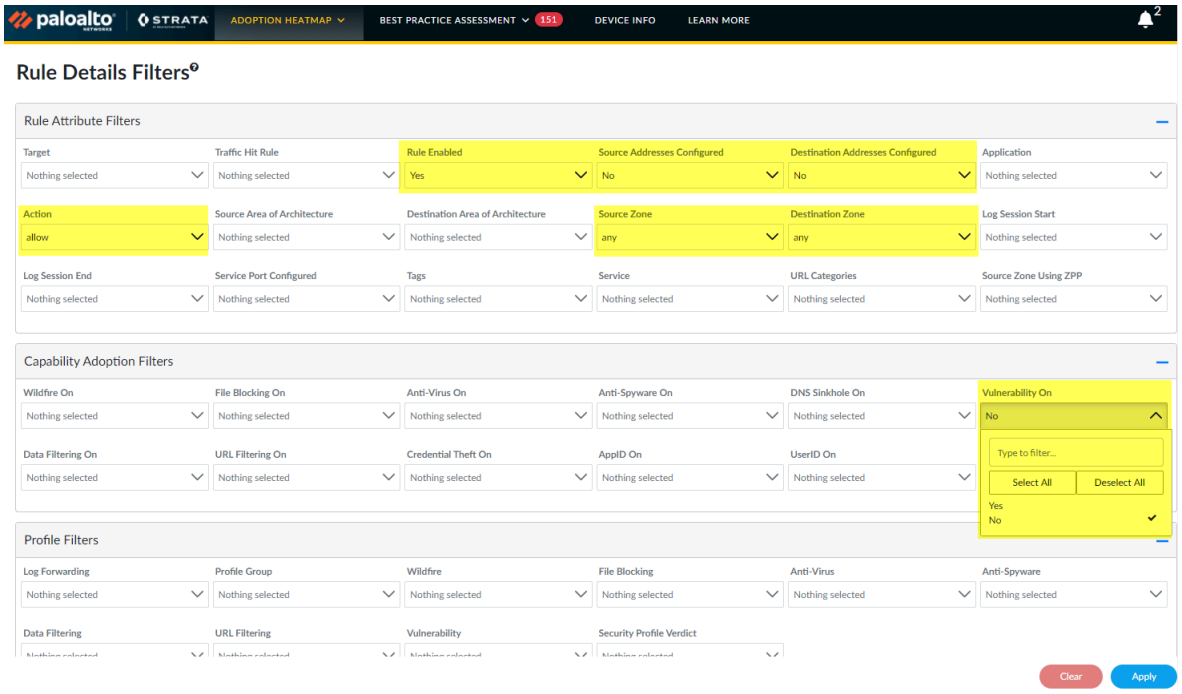
STEP 1 | 从“采用热图”菜单中，选择 **Rule Detail**（规则详细信息）以查看“规则详细信息”页面。



Target	Source Area Of Architecture	Dest Area Of Architecture	Rulename	Rule Hit Count	Rule Last Hit	Tags	Service	Url Categories	Source Zone	Source User	Dest Zone	Source Addresses
012801064407:...	Users	Lab/Test, DMZ	email-applications	236901	Oct 23, 2020	NO_TAG	application-default	any	l3-vlan-trust	any	l3-untrust, Sinkhole	no
012801064407:...	Users	Lab/Test, DMZ	allow-apps	183938	Oct 23, 2020	NO_TAG	any	any	l3-vlan-trust	any	l3-untrust, Sinkhole	no
012801064407:...	Users	Lab/Test, DMZ	Social Networking Apps	101659	Oct 23, 2020	NO_TAG	application-default	any	l3-vlan-trust	any	l3-untrust, Sinkhole	no
012801064407:...	Users	Lab/Test, DMZ	Traffic to internet	30465	Oct 23, 2020	NO_TAG	service-http, service-https	any	l3-vlan-trust	any	l3-untrust, Sinkhole	no
012801064407:...	Users	Lab/Test, DMZ	smb	6322	Oct 23, 2020	NO_TAG	smb-1	any	l3-vlan-trust	any	l3-untrust, Sinkhole	no

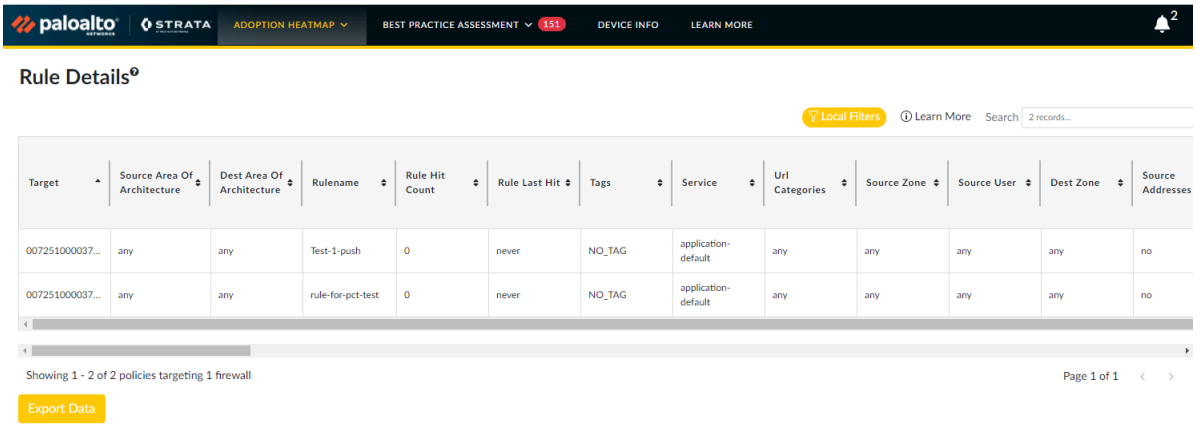
STEP 2 | 单击 **Local Filters**（本地筛选器）以查看筛选器选项，然后选择以下筛选器：

- 源区域 = **any**（任何）
- 目的区域 = **any**（任何）
- 源地址已配置 = **No**（否）
- 目标地址已配置 = **No**（否）
- 操作 = **allow**（允许）
- 规则已启用 = **Yes**（是）
- 漏洞保护开启 = **No**（无）



STEP 3 | 单击 **Apply Filter**（应用筛选器）。

BPA 列出了与筛选器匹配的规则：



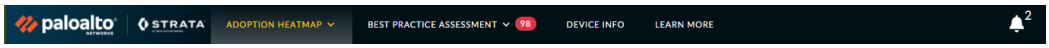
STEP 4 | 要将筛选的规则列表导出到 .csv 文件，请单击 **Export Data**（导出数据）。

STEP 5 | 下一步：评估最佳实践配置。

评估最佳实践配置

最佳实践评估 (BPA) 工具可帮助您了解安全策略中当前的最佳实践配置级别，以便您评估安全状况的成熟度。观看BPA 简介视频以了解 BPA，并利用 BPA 视频库和 BPA+ 视频库来了解关于该工具的更多信息。

BPA 报告首次在采用热图页面上打开。点击 **Best Practice Assessment**（最佳实践评估）以查看报告的 BPA 部分，该部分重点介绍采用下一代防火墙和 Panorama 的配置最佳实践。



除本文档外，您还可以查看 BPA 演示和一个关于如何运行 BPA 的短片，了解有关使用 BPA 的更多信息。

BPA 报告根据 200 多种最佳实践检查评估下一代防火墙或 Panorama 配置文件。BPA按策略、对象、网络和设备/Panorama 信息对评估结果进行分组，与 PAN-OS 用户界面类似。

在 *Panorama* 管理的环境中，*Panorama* 可以管理大量的新一代防火墙。您是要在 *Panorama* 上还是要在各个防火墙上运行 *BPA*？您需要权衡速度、便利性和完整性。

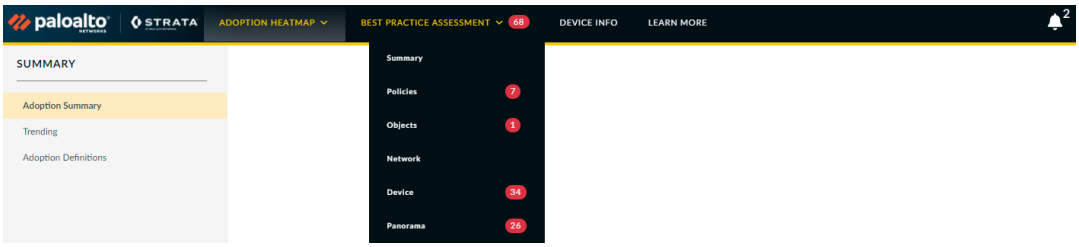
在 *Panorama* 上运行 *BPA* 既快速又方便，并且可以评估托管防火墙的大部分功能，但不能检查本地防火墙覆盖。

在每个托管防火墙上运行 *BPA* 会评估完整的配置（包括本地覆盖），但需要更多时间。

最实用的方法是先在 *Panorama* 上运行 *BPA*。检查结果，决定是否需要关注任何特定托管设备，然后在这些设备上运行 *BPA*。这种方法可以节省时间，同时仍可以专注于相关信息，让您能够改善安全状况。

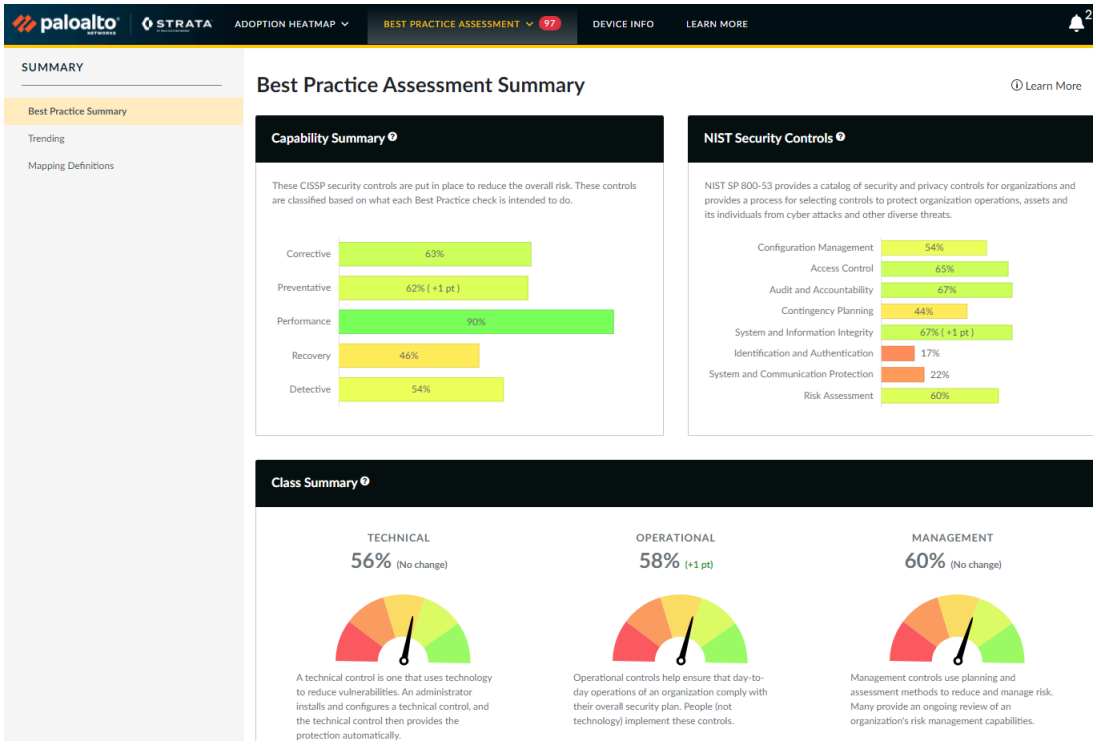
检查并分析信息，找到需要关注和改进的领域：

- 查看最佳实践摘要
- 查看最佳实践策略配置
- 查看最佳实践对象配置
- 查看最佳实践网络配置
- 查看最佳实践设备和 Panorama 管理配置



查看最佳实践摘要

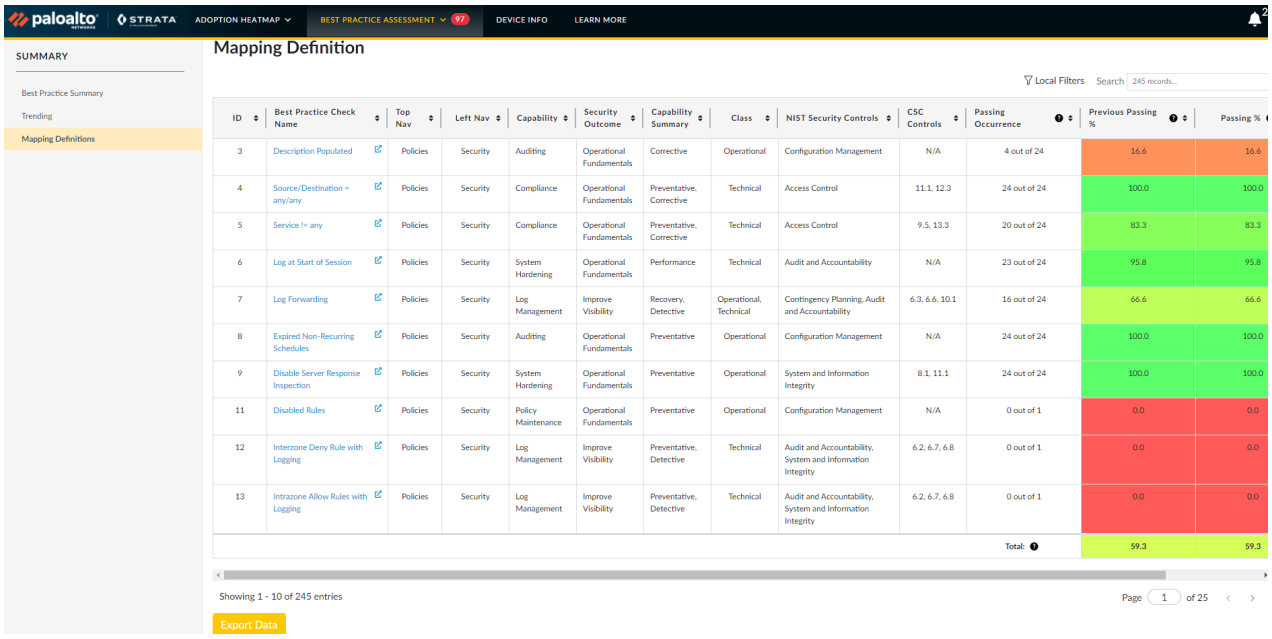
从 **Best Practice Assessment**（最佳实践评估）菜单中选择 **Summary**（摘要）可查看最佳实践摘要。



该摘要介绍了映射到行业标准控制类别的最佳实践配置检查结果，例如 Internet 安全中心 (CIS) 关键安全控制和国家标准与技术研究院 (NIST) 关于安全控制和评估程序的出版物。该信息的目的是提供一种了解 BPA 检查如何与行业标准相关联（而不是作为审计）的好方法。

比如说采用摘要，最佳实践摘要包括自上次在设备配置上生成 BPA 以来的当前采用率和采用进度（在括号中）的衡量标准。

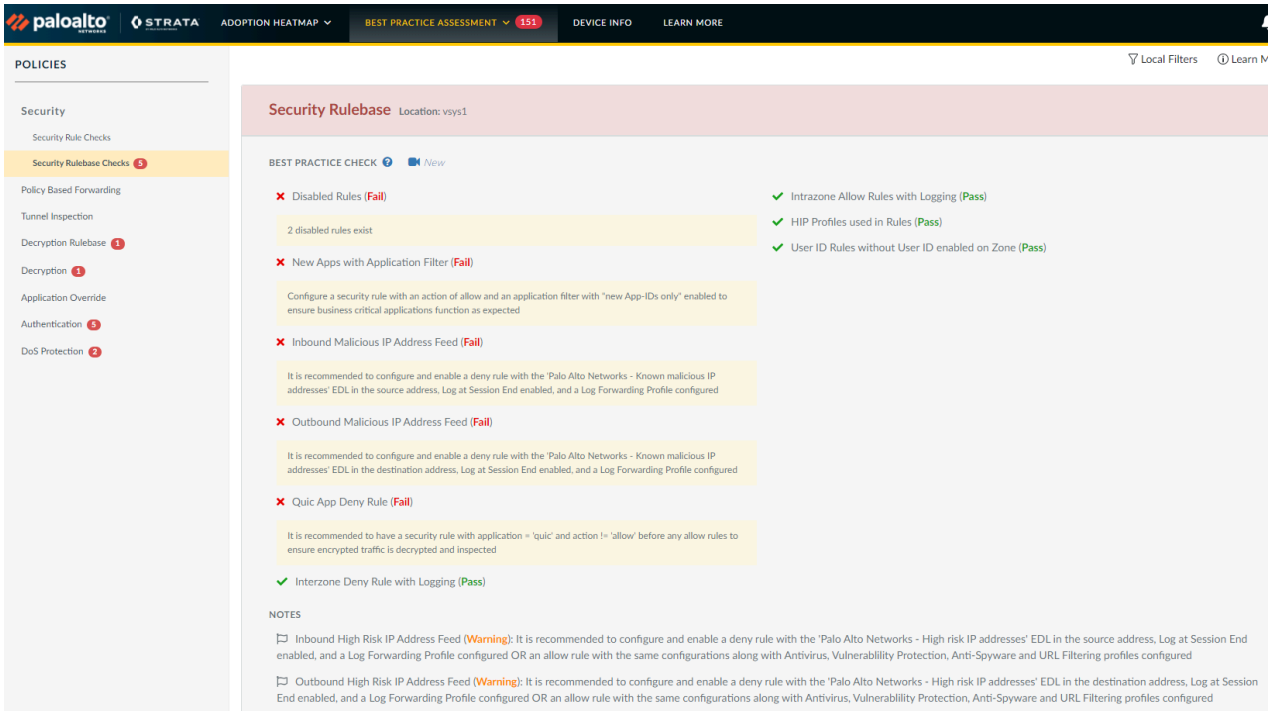
单击 **Mapping Definitions**（映射定义）（左边栏）查看所有映射检查及其各自分数的完整列表。**Show Filters**（显示筛选器）以设置筛选器，**Apply Filters**（应用筛选器）到输出，以及 **Export Mappings**（导出映射）以将映射导出至 .csv 文件。



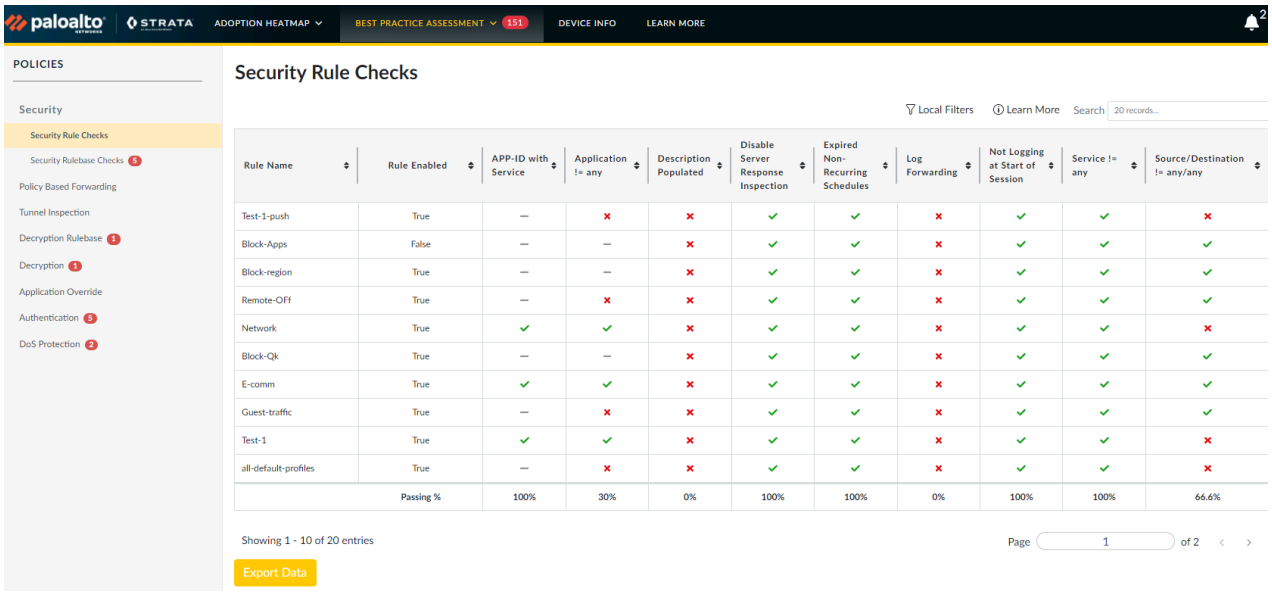
下一步：查看最佳实践策略配置。

查看最佳实践策略配置

Best Practice Assessment（最佳实践评估） > **Policies**（策略）显示与不同类型的防火墙策略相关的所有检查，并且在 **Security Rulebase checks**（安全规则检查）页面上开始。**Security Rulebase checks**（安全规则库检查）按组总结了最佳实践检查结果（包含通过/失败状态），并且提供了如何处理失败检查的建议。单击帮助（ ）以查看每个结果的描述和理由，以及参考技术文档的链接。



从左侧菜单中选择要查看的策略类型以确定潜在的规则改进。例如，**Security Rule Checks**（安全规则检查）显示基于规则的检查结果。单击 **Local Filters**（显示筛选器）以配置筛选器，将结果范围缩小到一个或多个特定失败检查的规则。您可以 **Export Data**（导出数据），从而将列表导出至 .csv 文件，以进行补救分析。



当您查看 **Policy**（策略）信息时，请至少查看以下项目，从而帮助了解策略补救的范围（切换视图）：

- 安全 — 识别 **Source/Destination !=any/any**（源/目标 **!=**任何/任何）检查失败的规则。
- 安全 — 识别 **App-ID with Service**（具有服务的 **App-ID**）检查失败的规则。
- 安全 — 识别 **User-ID Rules without User ID enabled on Zone**（区域上未启用**User-ID** 的 **User-ID** 规则）检查失败的 User-ID 规则。
- 解密规则库 — SSH 代理解密检查。
- 解密 — 每个解密策略规则应具有关联的解密配置文件。

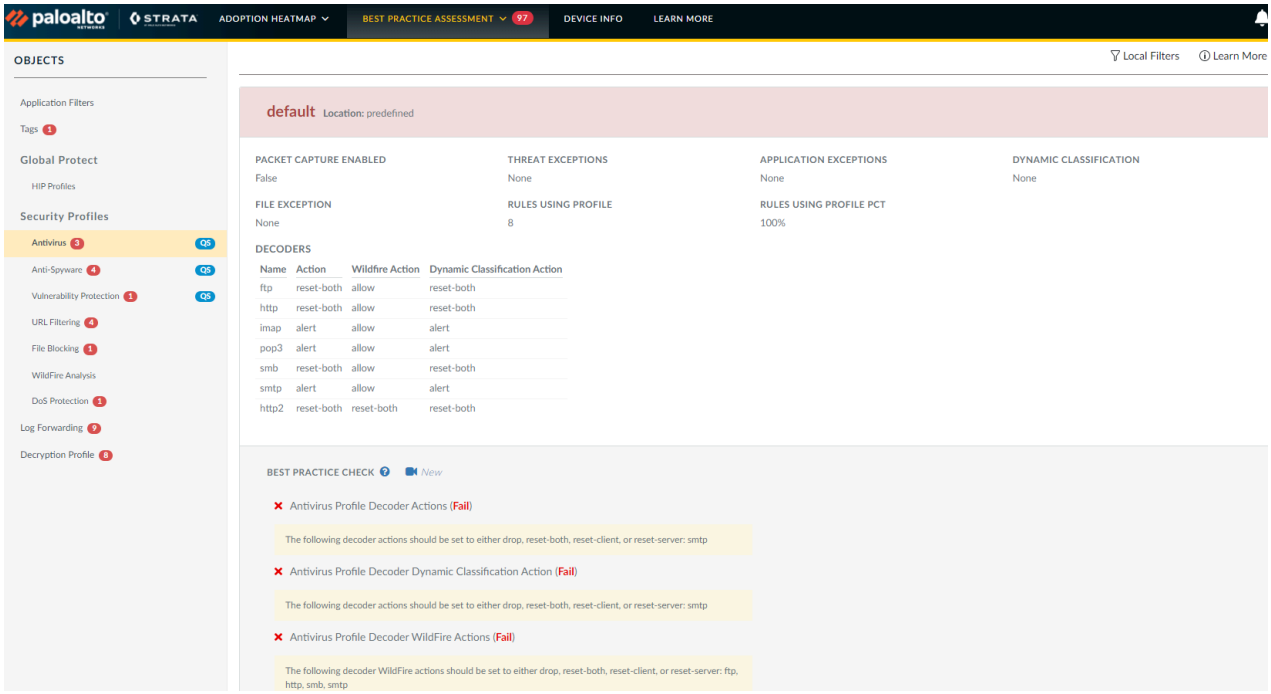
  如果将“不解密策略”应用到流量，则选择不解密的 *TLSv1.3* 流量是一个例外。将“不解密”配置文件附加到策略时，该配置文件将检查证书信息并阻止使用错误证书的解密会话。但是，由于 *TLSv1.3* 会加密证书信息，防火墙无法阻止基于证书信息的未解密流量，因此没有必要将配置文件附加到策略上。

- 应用程序覆盖 — 使用简单自定义应用程序绕过匹配流量的第 7 层检查的应用程序覆盖规则。减少或消除使用简单自定义应用程序的应用程序覆盖规则，以便改善流量可见性并检查这些规则控制的应用程序和内容。

下一步：查看最佳实践对象配置。

查看最佳实践对象配置

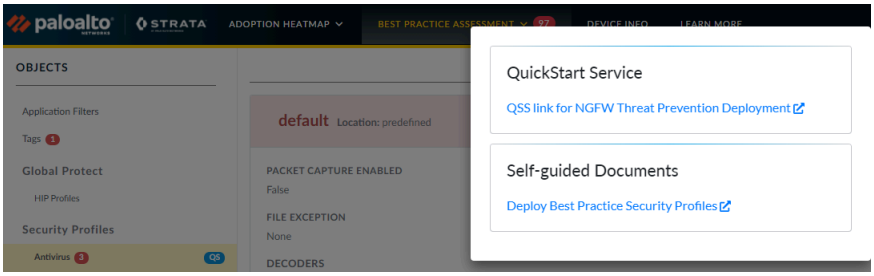
Best Practice Assessment（最佳实践评估） > **Objects**（对象）显示与不同类型的防火墙对象相关的所有检查，并且在 **Application Filters**（应用程序筛选器）页面上开始。选择要查看的对象以了解现有配置，并确定与应用程序筛选器、标签、GlobalProtect、安全配置文件、日志转发和解密配置文件相关的最佳实践配置的潜在差距。以下示例显示选择防病毒安全配置文件对象时的结果。



对于每个防病毒配置文件，报告显示当前配置以及使用配置文件的规则数量。报告显示当前配置下具有通过/失败状态的最佳实践检查结果以及失败的最佳实践检查的建议。单击帮助（ ）可获取每项检查的原因以及最佳实践文档的链接。

当一个或多个检查失败时，配置文件标题会变为红色。报告在底部列出未使用的配置文件，且标题为黄色。

屏幕左侧的某些配置文件页面链接旁的“QS”按钮链接到“快速入门服务”选项。通过帮助您计划和执行防火墙即平台实现方案，**QuickStart Service**（快速入门服务）可以帮助您改善安全功能和投资。**Self-guided Documents**（自引导文档）可以帮助您理解、创建和部署对象。



当您查看 **Objects**（对象）选项卡时，请至少查看以下项目，从而帮助了解补救的潜在范围：

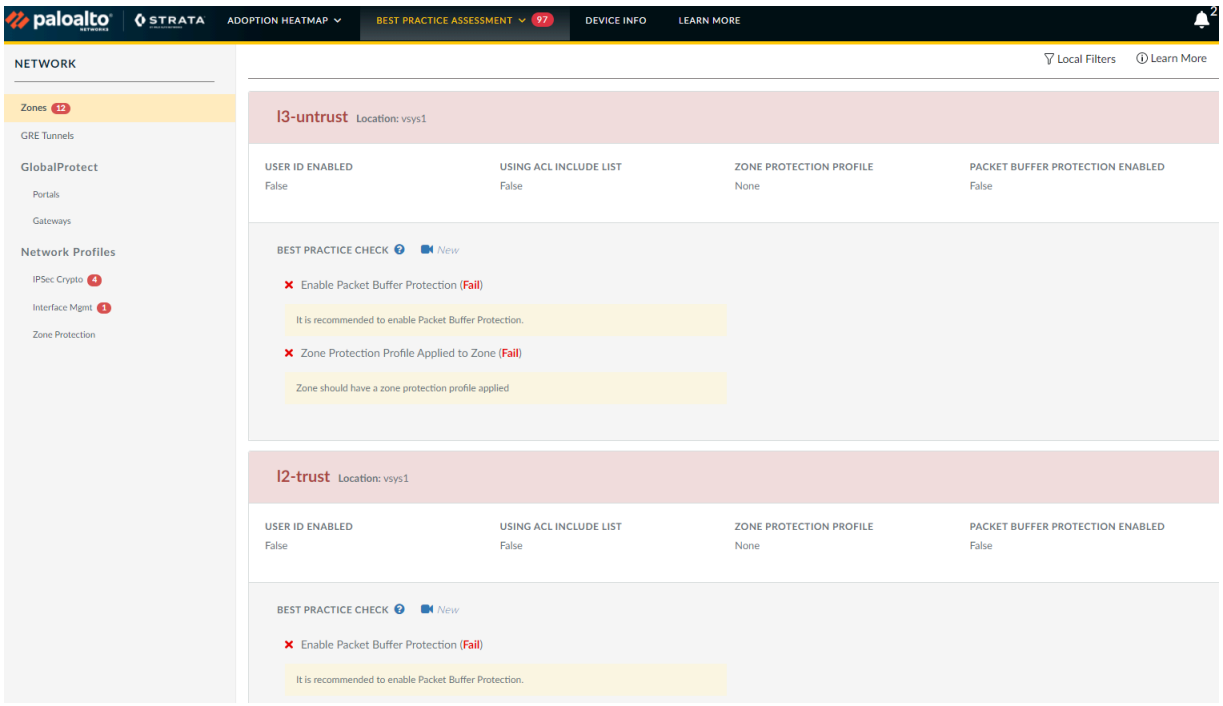
- 防病毒软件 — 防病毒软件和 WildFire 的解码器操作。

- 防间谍软件 — 严格配置文件、DNS Sinkhole。
- 漏洞保护 — 严格配置文件。
- **URL** 筛选 — 是否已阻止已知风险类别。
- **WildFire** 分析 — 配置文件类型（应将所有类型发送到 WildFire 进行分析）。
- 日志转发 — 是否转发所有日志类型（转发所有日志类型）。

下一步：查看最佳实践网络配置。

查看最佳实践网络配置

Best Practice Assessment（最佳实践评估） > **Network**（网络）显示与网络相关的配置的所有检查，并在 **Zones**（区域）页面上开始。在左侧导航栏中，选择要查看的网络检查以了解现有配置，并确定与区域、GRE 隧道、GlobalProtect、IPsec Crypto、接口管理和区域保护配置文件相关的最佳实践配置的潜在差距。以下示例显示了区域的结果。



该报告显示每个项目的当前配置。每个项目的最佳实践检查结果显示在其当前配置的下方。您可以指定一个 **Device Group**（设备组）和/或 **Template**（模板）以限制显示的信息范围。

每项检查都有通过/失败状态以及关于失败的最佳实践检查的建议。单击帮助（ ）可获取每项检查的原因以及最佳实践文档的链接。当一个或多个检查失败时，项目的标题会变为红色。

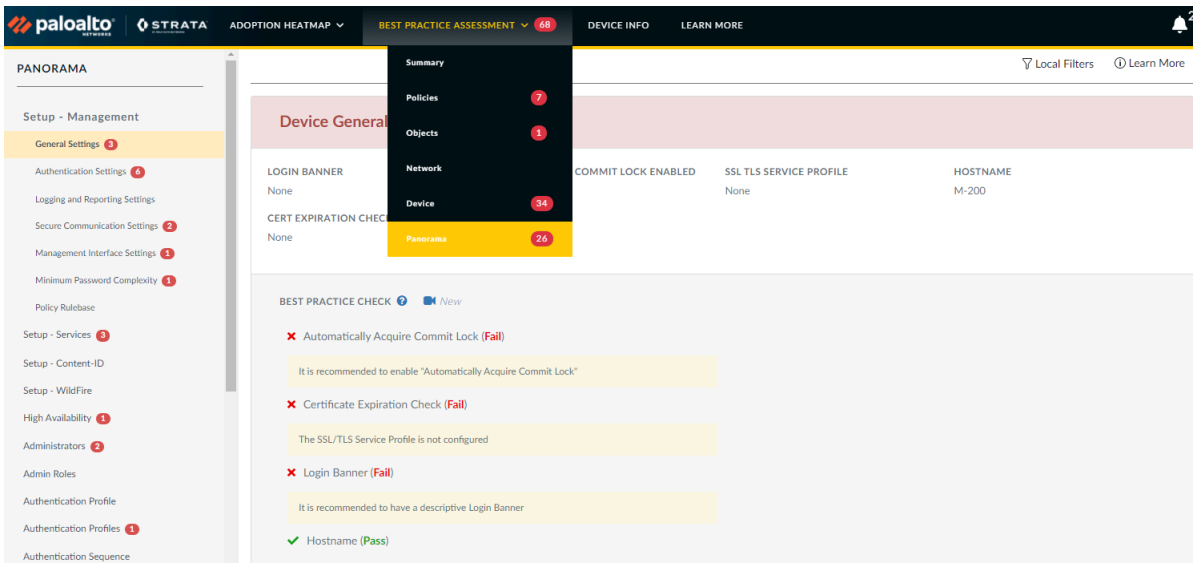
当您查看 **Network**（网络）选项卡时，请至少查看以下项目，从而帮助了解补救的潜在范围：

- 区域 — 是否每个区域都已启用数据包缓冲区保护且具有区域保护配置文件。
- 区域保护 — 是否已启用洪泛保护和基于数据包的攻击防护。

下一步：查看最佳实践设备和 Panorama 管理配置。

查看最佳实践设备和 Panorama 管理配置

显示与设备管理设置和配置相关的所有检查的 **Best Practice Assessment**（最佳实践评估） > **Device**（设备）和 **Best Practice Assessment**（最佳实践评估） > **Panorama** 页面。在标准防火墙上，**Best Practice Assessment**（最佳实践评估） > **Device**（设备）在防火墙设备的“管理设置”页面上的“常规设置”上开始。在 Panorama 上，**Best Practice Assessment**（最佳实践评估） > **Device**（设备）在显示每个模板堆栈的常规设置的页面上开始。**Best Practice Assessment**（最佳实践评估） > **Panorama** 在设备的“管理设置”页面的“常规设置”上开始。选择要查看的检查以了解现有配置，并确定与防火墙和 Panorama 设备管理相关的最佳实践配置的潜在差距。下面的示例显示 Panorama 设备上的“常规设置”结果。



该报告显示每个项目的当前配置。每个项目的最佳实践检查结果显示在其当前配置的下方。查看 **Device**（设备）的信息时，您可以指定一个 **Template**（模板）以限制显示的信息范围。

每项检查都有通过/失败状态以及关于失败的最佳实践检查的建议。单击帮助（ ）可获取每项检查的原因以及最佳实践文档的链接。当一个或多个检查失败时，项目的标题会变为红色。

当您查看 **Device**（设备）或 **Panorama** 选项卡时，请至少查看以下项目，从而帮助了解补救的潜在范围：

- **Dynamic Updates**（动态更新）— 防病毒、应用程序、威胁和 WildFire 更新。
- **Management Interface Settings**（管理接口设置）— 网络连接服务、允许的 IP 地址。
- **Administrators**（管理员）— 本地管理员、管理员密码配置文件。检查 **Device**（设备） > **Administrators**（管理员）或**Panorama** > **Administrators**（管理员），以确保管理员的密码配置符合最低复杂性要求。
- **Minimum Password Complexity**（最小密码复杂性）—密码最低复杂性要求检查。

下一步：最佳实践变更优先级。

最佳实践变更优先级

BPA 报告中的信息量可能非常大。本章提供了一些建议，可帮助您确定改善配置的优先级，以便缩小安全差距，首先实施最高价值的增强，并在实现最佳实践安全状态方面取得进展。

在 *Panorama* 管理的环境中，*Panorama* 可以管理大量的新一代防火墙。您是要在 *Panorama* 上还是要在各个防火墙上运行 *BPA*？您需要权衡速度、便利性和完整性。

在 *Panorama* 上运行 *BPA* 既快速又方便，并且可以评估托管防火墙的大部分功能，但不能检查本地防火墙覆盖。

在每个托管防火墙上运行 *BPA* 会评估完整的配置（包括本地覆盖），但需要更多时间。

最实用的方法是先在 *Panorama* 上运行 *BPA*。检查结果，决定是否需要关注任何特定托管设备，然后在这些设备上运行 *BPA*。这种方法可以节省时间，同时仍可以专注于相关信息，让您能够改善安全状况。

以下主题重点介绍如何根据通常实施新部署的顺序来改进安全状况，首先关注管理，然后关注可见性、控制和执行。现有部署在每个领域均达到了一定的完备度。

- 增强设备管理状况
- 改善流量可见性
- 实施初始最佳实践控制
- 微调和增强最佳实践控制

增强设备管理状况

通过防止可能危及防火墙的未授权的访问，减少意外事件的运营影响并提供对防火墙运营的更大可见性，从而增强设备管理状态以保护防火墙。

- 按照管理访问的最佳实践，防止未经授权和不安全地访问设备的管理界面。
- 将所有系统和配置日志转发到 Panorama 和第三方监控解决方案，从而跟踪与系统相关的事件和配置更改。
- 创建配置备份计划，以便更快地修复与配置相关的问题和系统中断。

配置发生更改后，运行 BPA 以验证更改，衡量进度并确定下一次更改的优先级。

下一步：改善流量可见性。

改善流量可见性

对于无法看到的威胁，您无法保护自己，因此，您必须始终确保全面了解所有用户和应用程序的流量。全面监控网络上的应用程序、内容和用户是实现明智的策略控制的第一步：

- 最大化安全配置文件采用率。在查看采用摘要和识别采用中的差距后，按照安全过渡步骤修复差距，从而迁移到最佳实践安全配置文件实现。
- 在安全策略规则库中最大化日志采用率（包括日志转发），从而检查所有流量。
- 配置动态内容更新的最佳实践，以确保防火墙具有最新的应用程序和威胁签名，从而保护您的网络，并根据网络安全性和可用性需求部署更新。
- 根据最佳实践规划 SSL 解密部署。
- 在用户区域（用户发起流量的内部可信区域）启用 User-ID，将应用程序流量和相关威胁映射到用户和设备。

  不要在外部不受信任区域启用 *User-ID*。如果在外部不可信区域启用 *User-ID*（或 *WMI* 之类的客户端探测），则可以在受保护的网络之外发送探测，并导致 *User-ID* 信息泄露，如 *User-ID* 代理服务帐户名称、域名和加密密码哈希，这可能让攻击者侵入您的网络。

- 减少或消除应用程序覆盖规则，以便检查这些规则控制的应用程序和内容（应用程序覆盖规则是不允许防火墙检查流量的第 4 层规则）。消除或缩小基本应用程序覆盖规则的范围：
  - 验证是否仍存在使用该规则的情况。通常，创建应用程序覆盖规则是为了克服与性能、协议解码器或未知应用程序相关的特定问题。随着时间的推移，PAN-OS 更新、内容更新或硬件升级可能会消除对某些应用程序覆盖规则的需求。如果在防火墙上运行 PAN-OS 9.0（或更高版本），或者在运行 PAN-OS 8.1 的 Panorama 管理的防火墙上运行 PAN-OS 9.0（或更高版本），则可以使用策略优化器将规则转换为第 7 层规则。
  - 减少“应用程序覆盖”规则的范围，使其仅影响尽可能少的流量。定义过于宽泛的规则可能会覆盖超出必要或预期的更多流量。在每个“应用程序覆盖”规则中定义源和目标区域、地址和/或端口，从而尽可能地限制规则的范围。
  - 为内部应用创建第 7 层自定义应用程序。
  - 创建具有自定义超时值的服务对象。
- 计划部署 DoS 和区域保护并进行基准 CPS 测量，以便设置合理的防洪泛阈值。

实施这些原生 App-ID、Content-ID、User-ID 和 SSL 解密功能时，防火墙可以查看和检查您的所有流量（应用程序、威胁和内容），并将事件与用户联系起来，而不管位置、设备类型、端口、加密或攻击者的规避技术如何。

提高 *SSL* 解密、日志记录、泛滥攻击保护、安全配置文件等功能的采用率可能会导致消耗额外的防火墙资源。了解防火墙的容量并确保它们的大小适合处理任何额外的负载。*Palo Alto Networks SE* 或 *CE* 可以帮助您调整部署规模。您还可能需要额外的日志存储空间。

配置发生更改后，运行 BPA 以验证更改，衡量进度并确定下一次更改的优先级。

下一步：实施初始最佳实践控制。

实施初始最佳实践控制

获得网络上流量（应用程序、内容、威胁和用户）的可见性和上下文后，实施严格控制以缩小攻击范围并防止已知和未知威胁，完成向最佳实践配置的过渡。

- 在查看采用摘要并识别采用中的差距后，按照安全过渡步骤迁移到最佳实践安全配置文件，以阻止威胁并缩小攻击面，包括在数据中心实施严格控制来保护企业最宝贵的资产。
- 为数据中心和外围防火墙创建基于应用程序的安全策略规则；对不在数据中心的其他防火墙使用外围防火墙最佳实践建议。如果在防火墙上运行 PAN-OS 9.0（或更高版本），或者在 Panorama 管理的防火墙上运行 PAN-OS 8.1（或更高版本），则可以使用策略优化器将基于端口的规则转换为基于应用程序的规则。
- 创建基于用户的访问策略。
- 部署最佳实践区域保护配置文件到所有区域。
- 部署 SSL 解密，以便防火墙可以获得加密流量的可见性（解密）并进行检查。

实施控制功能后，防火墙可以扫描所有允许的流量，并检测和阻止网络和应用层漏洞利用、缓冲区溢出、DoS 攻击、端口扫描以及已知和未知的恶意软件变体。防火墙控制应用程序和用户访问权限，并且阻止恶意和不需要的应用程序。

配置发生更改后，运行 BPA 以验证更改，衡量进度并确定下一次更改的优先级。

下一步：微调和增强最佳实践控制。

微调和增强最佳实践控制

对网络流量（应用程序、内容、威胁和用户）实施控制后，开始微调控制机制并实施其他功能，以改善安全状况。

- 如果您尚未将内部应用程序转换为自定义应用程序以获得流量的可见性和控制权，请将内部应用程序转换为自定义应用程序。
- 在使用安全过渡步骤以开始转移到最佳实践配置文件后，将安全配置文件调整为符合最佳实践。
- 根据 Palo Alto Networks 和信誉良好的第三方馈送的威胁情报阻止已知的恶意 IP 地址。
- 部署 GlobalProtect 或 Prisma Access，将新一代安全平台扩展到用户和设备（无论他们位于何处）。
- 启用凭据防窃。
- 配置基于网络的多重身份验证。

下一页：运行 BPA 以验证更改，衡量进度并确定下一次更改的优先级，了解关于最佳实践的更多信息，并了解关于 Panorama 和 PAN-OS 下一代防火墙的许多安全功能的更多信息。

