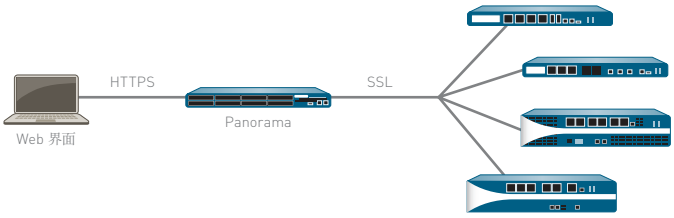
PANORAMA

Panorama 为 Palo Alto Networks 下一代防火墙提供集中策略和设备管理。

- 图形化显示网络应用、用户以及潜在的安全风险摘要。
- 企业集中策略与本地策略相结合，是管理员获得最大灵活性。
- 基于角色的权限管理功能能够为不同的管理员分配设备层或全局管理权限。
- 根据网络流量、安全事件和配置修改进行集中分析、研究和报告。



大型企业通常在他们的整个网络中部署很多防火墙，由于个别设备之间的复杂性和不一致性，对它们的管理和控制过程很麻烦。其结果是增加管理工作和相关费用。

Panorama 为 Palo Alto Networks 下一代防火墙提供集中管理和可视性。管理员可以从一个位置全局洞察穿过防火墙的应用程序、用户和内容，了解网络中到底发生了什么，并结合应用配置策略，提供最大限度的保护和控制同时最大限度地减少管理工作。管理员可以通过集中管理平台的汇总数据或本地防火墙上存储的数据上进行分析、报告和取证。

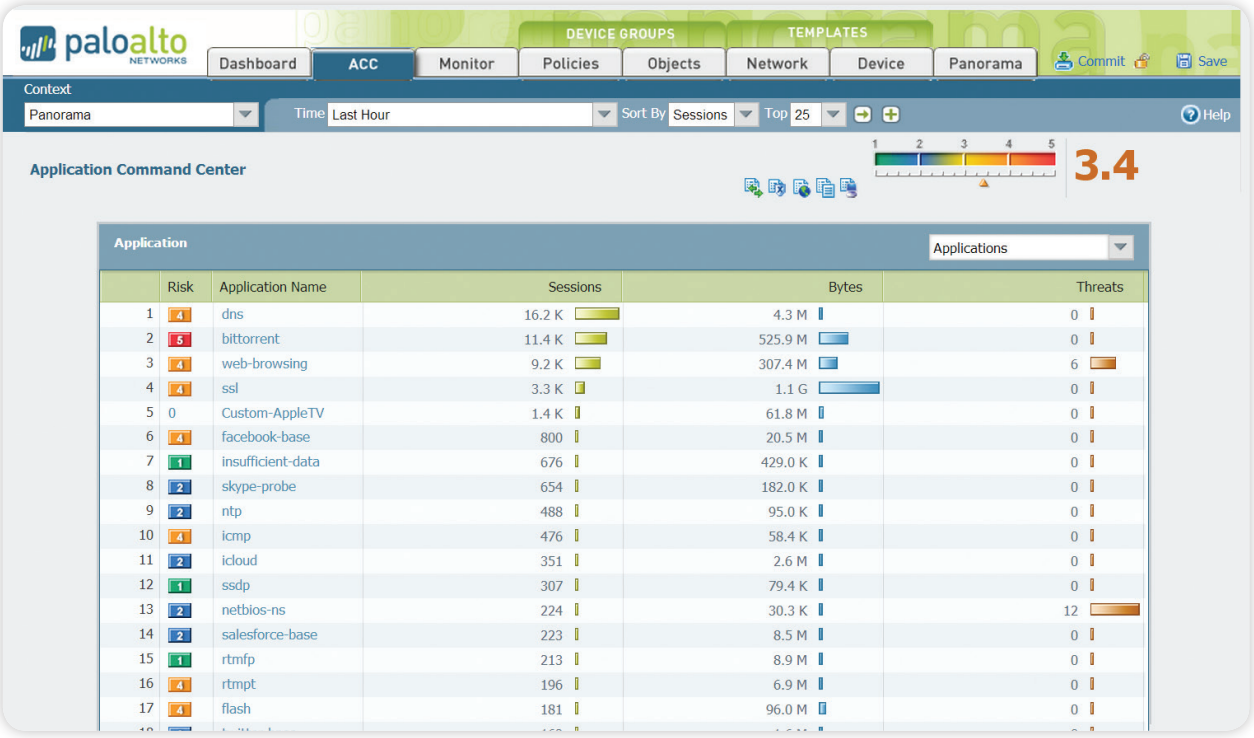
Panorama 提供与其他 Palo Alto 设备一样的 Web 界面和风格，最大限度地减少管理员的上手时间。Palo Alto Networks 强调一致性的管理理念，与其他产品相比较具有显著优势。

中央可视性：应用程序管控中心

使用 Panorama 的应用程序命令和控制（ACC）可为管理员提供穿越所管理的 Palo Alto Networks 设备的应用程序图形视图、URL、威胁和数据（文件和关键字）。ACC 从每个设备动态抓取数据，确保正在使用它们的管理员了解网络中存在的应用以及它们可能造成的潜在威胁。管理员只需一次点击即可查询新的或不熟悉的应用程序，点击时将显示应用程序说明、其主要功能、其行为特征以及当前使用者。

此外，URL 类别和威胁分类为管理员可提供一个完整且全面的网络活动图。ACC 的可视性使管理员能够做出明智的决策并对潜在安全威胁做出快速响应。

paloalto NETWORKS
the network security company™



应用程序管控中心提供应用程序流量的总体和局部视图，具有数据挖掘功能以便了解当前活动详情。

全局策略控制：安全启动应用程序

安全的允许应用指在启用威胁防护、文件拦截、数据过滤或 URL 分类策略时允许使用特定应用程序。Panorama 有助于通过允许管理员从一个中央位置管理规则，在整个防火墙网络中安全的允许应用程序。

基于 Panorama 的共享策略有助于在本地设备规则保持安全性和灵活性的同时、确保符合内部或监管规定。在策略和对象上将集中和本地管理控制相结合有助于在安全策略一致性和局布灵活性之间取得平衡。

管理员可以通过目录服务集成部署根据用户安全的允许应用程序或应用程序功能的策略，同时应用程序特定的威胁防御可保护内容和网络。通过一条策略根据用户（而不是 IP 地址）安全的允许应用程序的能力使各企业能够显著减少所需策略数量。与目录服务集成的一个额外好处是显著减少与雇员增加相关的管理费用、减少可能每天发生的移动和改变－在雇员从一个用户组移动到另外一个用户组时无需额外修改即保持相同的安全策略。

流量监测：分析、报告和取证

Panorama为本地设备管理提供了强大的日志、报表功能。在管理员执行日志查询和生成报告时，Panorama 直接从所管理的防火墙或转发到 Panorama 的日志中动态获取尽可能多的数据。在全部设备上获取最新信息使管理员能够应对安全事件并积极主动地保护企业资产。

- **日志查看器：**无论针对个别设备还是全部设备，Panorama 管理员均能够通过点击一个按钮使用动态日志过滤和/或使用表达式生成器快速查看活动日志，从而定义排序条件。可以保存结果以备将来查询或导出以便做进一步分析。
- **定制报告：**既可以按原样使用预定义报告，也可以其进行定制，或将其组合为一个报告以满足特定要求。
- **用户活动报告：**在 Panorama 中，用户活动报告显示使用的应用程序、访问的 URL 类别、访问的网站以及个别用户在指定时间内访问的全部 URL。无论受到哪个防火墙的保护或者可能正在使用什么IP或设备，Panorama 均使用用户的活动的聚合视图构建报告。

Panorama 管理架构

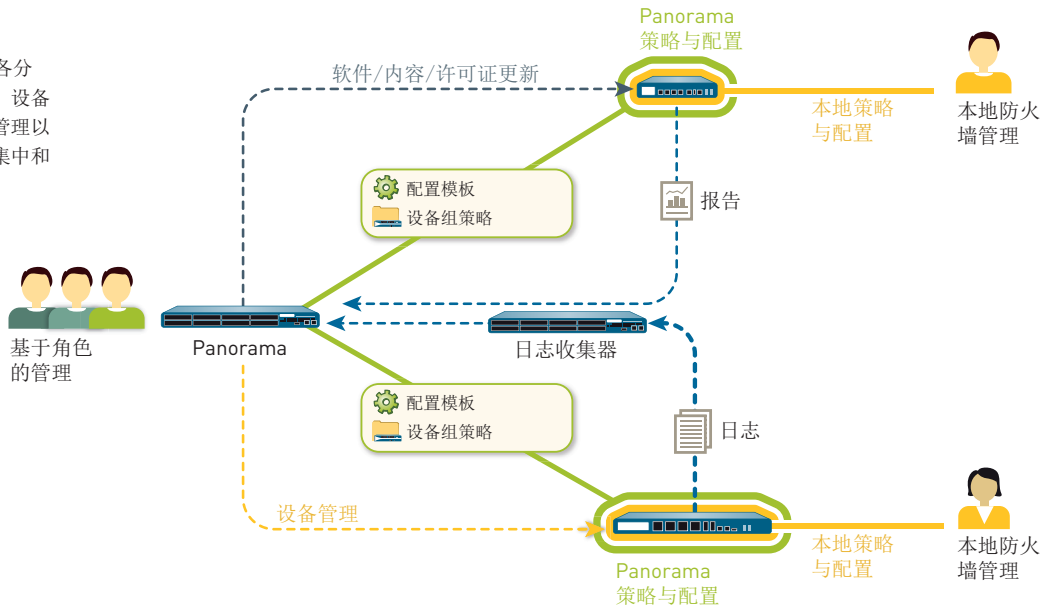
Panorama 使组织能够使用一个提供中央监督和本地控制的模型管理自己的 Palo Alto Networks 防火墙。Panorama 提供一些集中管理工具：

- **模板：**通过模板管理共同的设备和网络配置。模板可用作集中管理配置，然后将变更推送到所管理的各个防火墙。这种方法避免了在许多设备上重复进行相同的个别防火墙变更。这种用途的一个例子就是在数百个防火墙上推送共同的 DNS 和 NTP 服务器设置，而不是依据设备在设备上执行相同的变更。
- **设备组：**Panorama 通过设备组管理共同的策略和对象。设备组用于集中管理很多具有共同要求的设备的规则库。确定设备组中对设备进行分组方式的示例的地理（例如，欧洲和北美）或功能（例如，边界或数据中心）方向。在设备组内，将虚拟系统视为单个设备，与物理防火墙级别相同。从而允许共同的规则库共享某个设备上的不同虚拟系统。

  各企业均可使用共享的中央控制策略的同时由本地防火墙管理员定制本地策略。在设备组级，管理员可以创建要根据匹配条件进行评估的第一套规则（前规则）和最后一套规则（后规则）的共享策略。可在所管理的防火墙上查看前、后规则，但是只能在已定义的管理角色范围内从 Panorama 对它们进行编辑。可通过本地管理员或已经切换到本地防火墙范围的 Panorama 管理员，对本地设备规则（前、后规则之间）进行编辑。此外，企业可以使用由 Panorama 管理员定义的共享对象，即在本地设备规则中可以引用这个对象。
- **基于角色的管理：**各企业均可使用基于角色的管理委派对不同工作人员的功能级管理访问（已启用、只读或已禁用并从视图中隐藏）。 可给予特定管理员访问与其工作有关的任务的适当访问权限，同时使其他访问权限变为隐藏或只读。一个如何使用这种类型访问控制的例子是，给负责整个企业不同任务的人员定义不同的角色，比如安全管理员与网络管理员。对管理员所做全部变更均进行记录，显示发生的时间、管理员、使用的管理界面（Web UI、CLI、Panorama）、采取的命令或行动。
- **软件、内容和许可证更新管理：**随着部署规模的增长，很多组织希望确保以有组织的方式将更新发送到下游盒。例如，安全团队可能更喜欢集中软件更新，然后立即通过 Panorama 发送到各生产防火墙。 使用 Panorama，可对软件更新、内容（应用程序更新、防病毒特征库、威胁特征库，URL 过滤数据库等）和许可证更新过程进行集中管理。

使用模板、设备组、基于角色的管理和更新管理，各组织均可委派对全部管理功能、可视化工具、策略创建、总体和局布报告和记录的适当访问权限。

Panorama 允许各分支机构通过模板、设备组、基于角色的管理以及更新管理平衡集中和本地管。



部署灵活性

Panorama 可以为硬件设备或虚拟设备进行部署。

硬件设备

需要具备高性能硬件 Panorama、或想要针对大规模日志数据将 Panorama 管理和日志功能分离的组织可以使用 M-100 硬件设备满足其需求。可以采用下列方式部署 M-100：

- **集中式：**在这种情况下，将全部 Panorama 管理和日志功能合并到单个设备中（支持 HA）。
- **分布式：**有的企业可能更希望将管理和日志功能分离。在这种配置下，在管理器和日志收集器之间分割这些功能。
  - **Panorama 管理器：**Panorama 管理器负责处理在所管理的全部设备中与策略和设备配置相关的任务。管理器不在本地存储日志数据，而是使用单独日志收集器处理日志数据。管理器对日志收集器中存储的数据进行分析，用于集中报告。
  - **Panorama 日志收集器：**具有高记录量和保留要求的组织可以部署将从所管理的多个防火墙中聚合日志信息的专用 Panorama 日志收集设备。

管理和日志收集的分离使各组织能够优化他们的部署，以满足可扩展性、组织或地区要求。

虚拟设备

Panorama 可作为虚拟设备部署在 VMware ESX(i) 上，使企业能够支持他们的虚拟化举措和合并数据中心中有时候有限或昂贵的机架空间。 可以采用下列两种方式部署虚拟设备：

- **集中式：**将全部 Panorama 管理和记录合并到单个虚拟设备中（支持HA）。
- **分布式：**Panorama 分布式日志收集支持混合的硬件和虚拟设备。
  - **Panorama 管理器：**虚拟设备可作为 Panorama 管理器使用，负责处理在所管理的全部设备中与策略和设备配置相关的任务。
  - **Panorama 日志收集器：**Panorama 日志收集器负责卸载密集的日志收集和处理任务，可使用 M-100 进行部署。虚拟设备不能用作 Panorama 日志收集器。

具有硬件或虚拟化平台以及组合或分离 Panorama 功能可供选择，为各组织提供了在分布式网络环境中管理多个 Palo Alto Networks 防火墙的最大灵活性。

PANORAMA 规格

支持设备数量	多达 1,000
高可用性	主动/被动
管理员身份验证	本地数据库
	RADIUS

M-100 管理设备规格

I/O

- (1) 10/100/1000、(3) 10/100/1000（供将来使用）、(1) DB9 控制台串行端口

存储（2 种选择）

- M-100 1TB RAID：2 x 1TB RAID 认证的 HDD，用于 1TB 的 RAID 存储
- M-100 4TB RAID：8 x 1TB RAID 认证的 HDD，用于 4TB 的 RAID 存储

电源/最大功耗

- 500W/500W

最大 BTU/小时

- 1,705 BTU/小时

输入电压（输入频率）

- 100-240VAC (50-60Hz)

最大电流消耗

- 10A@100VAC

MTBF（平均故障间隔时间，MEAN TIME BETWEEN FAILURES）

- 14.5 年

可安装机架（尺寸）

- 1U、19" 标准机架（1.75" 高 x 23" 深 x 17.2" 宽）

重量（独立设备/发货）

- 26.7 磅/35 磅

安全性

- UL、CUL、CB

EMI（电磁干扰，ELECTROMAGNETIC INTERFERENCE）

- FCC A 级、CE A 级、VCCI A 级

环境

- 工作温度：40-104°F，5-40°C
- 非工作温度：-40-149°F，-40-65°C

虚拟设备规格

服务器最低要求

- 40 GB 硬盘驱动器
- 4 GB RAM
- Quad-Core CPU (2GHz+)

支持 VMWARE

- VMware ESX 4.1 或更高版本

支持浏览器

- IE v7 或更高版本
- Firefox v3.6 或更高版本
- Safari v5.0 或更高版本
- Chrome v11.0 或更高版本

日志存储

- VMware 虚拟硬盘：2TB 最大
- NFS

paloalto NETWORKS
the network security company™

3300 Olcott Street
Santa Clara, CA 95054

Main: +1.408.573.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com