亮点

- 全球首个基于机器学习的新一代防火墙
- 九次当选 Gartner 魔力象限® 网络防火墙领导者
- Forrester Wave™：2020 年第 3 季度企业防火墙领导者
- 在 2019 年 NSS 实验室新一代防火墙测试报告中，安全有效性得分最高，100% 的规避被阻止
- 通过丰富的产品阵容，满足分布式企业的一系列性能需求
- 以桌面形式提供安全性
- 将可视性和安全性扩展到所有设备，包括未托管的物联网设备，且无需部署额外的传感器
- 以主动/主动模式和主动/被动模式支持高可用性
- 通过安全服务提供可预测的性能
- 采用静音、无风扇设计，为分支机构和家庭办公室提供可选的冗余电源
- 通过可选的零接触配置 (ZTP) 简化了大量防火墙的部署
- 通过 Panorama™ 网络安全管理支持集中管理

PA-400 Series

Palo Alto Networks PA-400 Series 包括 PA-460、PA-450、PA-440 和 PA-410，为分布式企业分支机构、零售场所和中型企业提供了基于机器学习的新一代防火墙能力。

利用全球首款基于机器学习的新一代防火墙 (NGFW)，您能够防止未知威胁，查看和保护各个方面，包括物联网 (IoT)，并通过自动策略建议减少错误。

PA-400 Series

PA-400 Series 的控制元素是 PAN-OS®，这正是运行所有 Palo Alto Networks 新一代防火墙的软件。PAN-OS 原生分类所有流量，包括应用、威胁和内容，然后将该流量与用户绑定，而不受位置或设备类型的影响。随后，将应用、内容和用户（即运营业务的要素）用作安全策略的基础，由此改善安全状况，缩短事件响应时间。

主要安全和连接功能

基于机器学习的新一代防火墙

- 将机器学习 (ML) 嵌入防火墙核心，为基于文件的攻击提供内联无签名攻击预防，同时识别并立即阻止以前从未见过的网络钓鱼尝试。
- 利用基于云的机器学习进程将零延迟签名和指令推送回新一代防火墙。
- 使用行为分析检测物联网设备并提出策略建议，这是新一代防火墙上的云交付和原生集成服务的一部分。
- 自动化的策略建议可以节省时间并减少出现人为错误的机会。

通过全面的第 7 层检查在所有时间、所有端口上识别和分类所有应用

- 识别有网络流量的应用，不考虑端口、协议、规避技术或加密 (TLS/SSL)。
- 使用应用而非端口作为所有安全启用策略的决策基础：允许、拒绝、计划、检测以及应用流量整形。
- 提供为专有应用创建自定义 App-ID™ 标签的能力，或为来自 Palo Alto Networks 的新应用请求 App-ID 开发的能力。
- 识别应用中的所有有效负载数据（例如文件和数据模式），以阻止恶意文件并拦截数据泄露尝试。
- 创建标准和定制的应用使用情况报告，包括软件即服务 (SaaS) 报告，这些报告提供了对您网络上所有已认可和未认可的 SaaS 流量的深入洞见。
- 使用内置的策略优化器，支持将旧的第 4 层规则集安全迁移到基于 App-ID 的规则，从而为您提供更安全、更易于管理的规则集。

在任何位置、任何设备上为用户实施安全方案，同时根据用户活动调整策略

- 支持基于用户和组而不仅仅是 IP 地址的可视性、安全策略、报告和取证。
- 轻松地与各种存储库集成以利用用户信息：无线 LAN 控制器、VPN、目录服务器、SIEM、代理等等。
- 允许在防火墙上定义动态用户组 (DUG) 以执行有时间限制的安全操作，而无需等待更改应用于用户目录。
- 应用一致的策略，而不考虑用户的位置（办公室、住宅、旅行途中等）和设备（iOS 和 Android® 移动设备、macOS®、Windows®、Linux 台式机、笔记本电脑；Citrix 和 Microsoft VDI 以及终端服务器）。
- 防止公司凭据泄露到第三方网站，并通过在网络层为任何应用启用多因素身份验证 (MFA) 来防止重新使用被盗的凭据，而不用进行任何应用更改。
- 提供基于用户行为的动态安全操作，以限制可疑或恶意用户。

防止隐藏在加密流量中的恶意活动

- 检查 TLS/SSL 加密流量（入站和出站）并向其应用策略，包括使用 TLS 1.3 和 HTTP/2 的流量。
- 提供对 TLS 流量的丰富可视性，例如加密流量大小、TLS/SSL 版本、密码组等，无需解密。
- 支持对传统 TLS 协议、不安全密码和错误配置的证书的使用进行控制，从而减轻风险。
- 有利于解密的轻松部署，并允许您使用内置日志来解决问题，例如证书被锁定的应用。
- 允许基于 URL 类别以及源和目标区域、地址、用户、用户组、设备和端口灵活地启用或禁用解密，用于隐私及合规性用途。
- 允许您从防火墙创建已解密流量的副本（即解密镜像），并将其发送到流量收集工具，以用于取证、历史记录或数据丢失预防 (DLP)。

提供集中管理和可视性

- 在一个统一的用户界面通过 Panorama™ 网络安全管理实现多个分布式 Palo Alto Networks 新一代防火墙（不考虑位置或规模）的集中管理、配置和可视性优势。
- 通过 Panorama 用模板和设备组简化配置共享，并随着日志记录需求的增加扩展日志收集。
- 使用户能够通过应用命令中心 (ACC) 深入且全面地了解网络流量和威胁。

使用云交付的安全服务检测和防止高级威胁

如今，复杂的网络攻击可以在 30 分钟内生成 45,000 个变种，使用多种威胁载体和先进技法布置恶意有效负载。传统的孤立安全方案会引入安全缺口，增加安全团队的管理开销，并由于不一致的访问和可视性阻碍业务生产力，从而给企业造成难题。

我们的云安全服务与业界领先的新一代防火墙无缝集成，利用 80,000 个客户的网络效应，即时协调情报，防范来自所有载体的所有威胁。消除您的所有位置之间的覆盖缺口，并利用平台上始终提供的一流安全性，免受最先进和最具规避性的威胁。

- **威胁预防**—超越传统的入侵防御系统 (IPS)，单次扫描即可阻止所有流量中的全部已知威胁。
- **高级 URL 过滤**—通过业界首个实时 Web 防护引擎和业界领先的网络钓鱼防护，提供一流的 Web 防护，同时最大限度地提升运营效率。
- **WildFire®**—通过对未知恶意软件的自动检测和预防，确保文件安全，该解决方案由业界领先的基于云的分析和来自 42000 多个客户的众包式情报提供支持。
- **DNS 安全**—利用机器学习的强大功能实时检测和防止 DNS 上的威胁，并以情报和情境为安全人员提供支持，以制定策略和快速有效地应对威胁。
- **IoT 安全**—行业最全面的物联网安全解决方案，可在单一平台上提供基于机器学习的可视性、防御和实施功能。
- **企业 DLP**—行业首个云交付的企业 DLP，可始终如一地保护所有网络、云和用户之间的敏感数据。
- **SaaS 安全**—提供集成的 SaaS 安全，使您能够以最低的总体拥有成本 (TCO) 查看和保护新的 SaaS 应用、保护数据并防止零日威胁。

启用 SD-WAN 功能

- 可轻松采用 SD-WAN，只需在现有防火墙上启用该功能即可。
- 可以安全实施 SD-WAN，其已与我们行业领先的安全技术进行了原生集成。
- 通过最大限度地减少延迟、抖动和丢包，提供出色的最终用户体验。

利用单通道架构提供独特的数据包处理方法

- 在单通道中对所有威胁和内容执行联网、策略查找、应用和解码以及签名匹配。这样，可以明显减少在一台安全设备中执行多种功能所产生的处理开销。
- 通过使用基于流的统一签名匹配，在单通道中扫描流量中的所有签名，避免了引入延迟。
- 启用安全订阅时，可实现一致且可预测的性能。（表 1 中，“威胁预防吞吐量”是在启用多个订阅的情况下测量的。）

表 1：PA-400 Series 性能和容量

	PA-460	PA-450	PA-440	PA-410*
防火墙吞吐量 (HTTP/appmix)†	5.2/4.7 Gbps	3.8/3.2 Gbps	3.0/2.4 Gbps	敬请期待
威胁预防吞吐量 (HTTP/appmix)‡	2.4/2.6 Gbps	1.6/1.7 Gbps	0.9/1.0 Gbps	敬请期待
IPsec VPN 吞吐量§	3.1 Gbps	2.2 Gbps	1.6 Gbps	敬请期待
最大会话数	400,000	300,000	200,000	敬请期待
每秒新会话数‖	74,000	52,000	39,000	敬请期待

注：结果在 PAN-OS 10.1 上测量得出

* 在未来将增加 PA-410 性能数据。

† 在启用 App-ID 和日志记录的情况下，利用 64 KB HTTP/appmix 事务测量防火墙吞吐量。

‡ 在启用 App-ID、IPS、防病毒、反间谍软件、WildFire、DNS Security、文件阻截和日志记录的情况下，利用 64 KB HTTP/appmix 事务测量威胁预防吞吐量。

§ 在启用日志记录的情况下，利用 64 KB HTTP 事务测量 IPsec VPN 吞吐量。

‖ 使用 1 字节 HTTP 事务通过应用覆盖测量每秒新会话数。

表 2：PA-400 Series 网络功能
接口模式
L2、L3、旁接、虚拟线路（透明模式）
路由
支持平稳重新启动的 OSPFv2/v3 和 BGP；RIP；静态路由
基于策略的转发
以太网上的点到点协议 (PPPoE)
多播：PIM-SM，PIM-SSM，IGMP v1、v2 和 v3
SD-WAN
路径质量测量（抖动、丢包、延迟）
初始路径选择 (PBF)
动态路径更改
IPv6
L2、L3、旁接、虚拟线路（透明模式）
功能：App-ID、User-ID、Content-ID、WildFire 和 SSL 解密
SLAAC
IPsec VPN
密钥交换：手动密钥、IKEv1 和 IKEv2（预共享密钥、基于证书的身份验证）
加密：3DES、AES（128 位、192 位、256 位）
身份验证：MD5、SHA-1、SHA-256、SHA-384、SHA-512
VLAN
每设备/每接口的 802.1Q VLAN 标签数量：4,094/4,094

表 3：PA-400 Series 硬件规格
I/O
PA-460、PA-450、PA-440：10/100/1000 (8) RJ45 PA-410：10/100/1000 (7) RJ45
管理 I/O
10/100/1000 带外管理端口 (1)、RJ-45 控制台端口 (1)、USB 端口(1)、Micro USB 控制台端口 (1)
存储容量
PA-460、PA-450、PA-440：128 GB eMMC PA-410：64 GB eMMC

表 3：PA-400 Series 硬件规格（续）
电源（平均/最大功耗）
PA-460、PA-450：33/41 W PA-440：29/34 W PA-410：17/18 W
最大 BTU/小时
PA-460、PA-450：141 PA-440：117 PA-410：78
输入电压（输入频率）
100–240 VAC (50–60Hz)
最大电流消耗
PA-460、PA-450：3.4 A @ 12 VDC PA-440：2.9 A @ 12 VDC PA-410：1.5 A @ 12 VDC
最大浪涌电流
PA-460、PA-450：4.2A PA-440：3.3A PA-410：2.1A
尺寸
PA-460、PA-450、PA-440：1.74 英寸（高）x 8.83 英寸（长）x 8.07 英寸（宽） PA-410：1.63 英寸（高）x 6.42 英寸（长）x 9.53 英寸（宽）
重量（独立设备/发运重量）
PA-460、PA-450、PA-440：5.0 磅/7.8 磅 PA-410：3.1 磅/5.9 磅
安全性
cTUVus、CB
EMI
FCC Class B、CE Class B、VCCI Class B
证书
请访问 paloaltonetworks.com/company/certifications.html
环境
工作温度：32 °F 到 104 °F（0 °C 到 40 °C） 非工作温度：-4 °F 到 158 °F（-20 °C 到 70 °C） 被动冷却