PA-1410

PA-1420

PA-1400 Series

Palo Alto Networks PA-1400 Series 基于机器学习的下一代防火墙，包括PA-1420和PA-1410，为组织的分支机构以及中型企业提供安全连接而设计。

PA-1400 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。

亮点

- 全球首个基于机器学习的新一代防火墙
- 十次当选 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，可有效阻止 100% 的规避
- 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
- 通过零接触配置 (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

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；新一代防火墙上的云交付和原生集成服务。
- 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)。此外，它还可以自动发现和控制新应用，以跟上 SaaS 安全订阅的爆炸式增长。
- 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-IDTM 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。
- 有关详细信息，请参阅 App-ID 技术摘要。

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。
- 允许您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。
- 无论用户所在位置和用户身份存储在何处，都始终如一地对用户进行身份验证和授权，通过云身份引擎（一种全新的基于云的基础架构，用于基于身份的安全性）快速转向零信任安全状态。有关详细信息，请查看云身份引擎解决方案摘要。

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，以实现隐私和法规上的合规性。
- 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)。
- 允许您使用网络数据包代理将所有流量（解密 TLS、非解密 TLS 和非 TLS）智能地转发到第三方安全工具，并优化您的网络性能和降低运营费用。
- 请参阅此解密白皮书，了解解密的位置、时间和方式，以阻止威胁并保护您的业务。

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。

通过 AIOps 充分利用您的安全投资并防止业务中断

- AIOps for NGFW 提供针对您的独特部署定制的持续最佳实践建议，以加强您的安全态势并充分利用您的安全投资。
- 基于由高级遥测数据提供支持的机器学习，智能地预测防火墙运行状况、性能和容量问题。
- 同时提供可行方案来解决预测到的中断问题。

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。传统的孤岛式安全方案给企业带来了挑战，因为这会引入安全漏洞，增加了安全团队的开销，并以不一致的访问和可视性阻碍业务生产力。

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。

服务包括：

- **Advanced Threat Prevention**：阻止已知漏洞、恶意软件、恶意 URL、间谍软件以及命令和控制 (C2)，对基于 web 的 Cobalt Strike C2 的预防率为 96%，检测到的未知 C2 比业界领先的入侵防御 (IPS) 解决方案多 48%。
- **WildFire 和恶意软件防御**：借助业界最大的威胁情报和恶意软件防御引擎，以 180 倍的速度自动检测和防御未知恶意软件，确保文件安全。
- **高级 URL Filtering**：借助业界首个实时防御已知和未知网站的功能，实现对互联网的安全访问，比其他供应商提前 24 小时阻止 76% 的恶意 URL。
- **DNS Security**：增加 40% 的 DNS 攻击覆盖率，并破坏 80% 使用 DNS 进行命令和控制以及数据窃取的攻击，无需对您的基础架构进行任何更改。
- **企业 DLP**：最大限度地降低数据泄露风险，阻止违反政策的数据传输，并在整个企业内实现一致的合规性，将所有云交付的企业 DLP 的覆盖范围扩大 2 倍。
- **SaaS Security**：借助业界唯一的新一代 CASB 自动查看和保护所有协议中的所有应用，在 SaaS 呈爆炸式增长的环境下先下手为强。
- **IoT Security**：利用业界为智能设备打造的最智能的安全措施，将保护每项“事务”和实施零信任设备安全的速度提升至 20 倍。

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。）

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。

表 1：PA-1400 Series 性能和容量

	PA-1410	PA-1420
防火墙吞吐量 (HTTP/appmix)*	8.9/6.8 Gbps	9.9/9.5 Gbps
威胁预防吞吐量 (HTTP/appmix)†	3.3/3.2 Gbps	5.2/5.0 Gbps
IPsec VPN 吞吐量‡	4.6 Gbps	6.9 Gbps
最大会话数	945,000	1,400,000
每秒新会话数§	100,000	140,000
虚拟系统（基本/最大）‖	1/6	1/6

注意：结果在 PAN-OS 11.0 上测量得出

* 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。

‖ 在基础数量之上增加虚拟系统需要单独购买许可证

PA-1400 Series 基于机器学习的新一代防火墙支持广泛的网络功能，使您能够更容易地将我们的安全功能整合到您的现有网络中。

表 2：PA-1400 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

表 2：PA-1400 Series 网络功能（续）
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
VLANs
每设备/每接口的 802.1Q VLAN 标签数量：4,094/4,094
聚合接口 (802.3ad)、LACP
网络地址转换
NAT模式（IPv4）：静态IP、动态IP、动态IP和端口（端口地址转换）
NAT64, NPTv6
其他 NAT 功能：动态 IP 保留、可调式动态 IP 和端口超额订阅
高可用性
模式：主动/主动，主动/被动
故障检测：路径监测、接口监测
零接触配置（ZTP）
需要使用Panorama 9.1.3或更高版本管理PAN-OS 11.0或更高版本的PA-1400系列硬件

表 3：PA-400 Series 硬件规格
I/O
PA-1410: 10/100/1000 (4), 1/2.5/5 Gb (4)/PoE, 1/2.5/5 Gb (4), gigabit SFP (6), 10 gigabit SFP+ (4)
PA-1420: 10/100/1000 (8), 1/2.5/5 Gb (4)/PoE, gigabit SFP (2), 10 Gigabit SFP+ (8)
管理 I/O
10/100/1000 带外管理端口 (1)
HSCI 10 gigabit 高可用端口 (1)
RJ-45 控制台端口 (1)
USB 端口 (1)
Micro USB 控制台端口 (1)
以太网供电 (PoE)
PA-1410, PA-1420 预计 PoE 总功率: 151W, 单个端口的最大负载: 90W
存储容量
PA-1410 120 GB SSD
PA-1420 240 GB SSD
电源（平均/最大功耗）
AC 450W 电源 (1); 可选购第2个AC 450W电源（1）。
Power Consumption
Maximum: TBD
Average: TBD

表 3：PA-1400 Series 硬件规格（续）
平均无故障工作时间 (MTBF)
24 年
输入电压（输入频率）
100–240 VAC (50–60 Hz)
机架式（尺寸）
PA-1410, PA-1420: 1U, 19" standard rack (1.70" H x 14.15" D x 17.15" W)
重量（独立设备/发运重量）
PA-1410, PA-1420: 15.5 lbs
安全性
cTUVus, CB
EMI
FCC Class A, CE Class A, VCCI Class A
Certifications
See paloaltonetworks.com/company/certifications.html
环境
Operating temperature: 0°C to 40°C at 10,000 feet
Non-operating temperature: -4°F to 158°F; -20°C to 70°C
Airflow
Front to back

To learn more about the features and associated capacities of the PA-1400 Series, please visit paloaltonetworks.com/network-security/next-generation-firewall/pa-1400-series.

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com