

PA-500

PA-500 下一代防火墙主要特点:

通过 APP-ID™ 每时每刻在各端口对全部应用程序进行分类。

- 识别应用程序，不考虑端口、采用的加密（SSL 或 SSH）或规避技术。
- 使用应用程序（而不是端口）作为全部安全启用策略决策的基础：允许、拒绝、计划任务、检查、应用流量整形。
- 对未识别的策略控制用应用程序、威胁取证、创建自定义 App-ID 或抓包进行深层分析。

通过 CONTENT-ID™ 和 WILDFIRE™ 防止已知和未知的各种威胁。

- 在各端口阻止 exploit 病毒攻击、恶意软件和间谍软件等已知威胁，无需担心常见的威胁逃避手段。
- 与 NAC、802.1X 无线以及带 XML API 的其他非标准用户存储库进行集成。
- 向运行 Microsoft Windows、Mac OS X、Linux、Android 或 iOS 平台的本地和远程用户部署统一的策略。

通过 CONTENT-ID™ 和 WILDFIRE™ 防止已知和未知的各种威胁。

- 在各端口阻止 exploit 病毒攻击、恶意软件和间谍软件等已知威胁，无需担心常见的威胁逃避手段。
- 限制未经授权的文件和敏感数据传输，控制与工作无关的网络浏览。
- 识别未知恶意软件，分析 100 多项恶意行为，在下一可用更新中自动创建和发送特征库。



PA-500

Palo Alto Networks™ PA-500 是针对企业分支机构和中等规模企业的高速防火墙部署。PA-500 使用连网、安全、威胁防御和管理专用计算资源管理网络流量。

高速背板分为单独数据和控制平面，从而确保在任何流量负载情况下始终可以进行管理访问。PA-500 下一代防火墙的控制元素是一个特定安全操作系统 PAN-OS™，允许各组织使用 App-ID、User-ID、Content-ID、GlobalProtect 和 WildFire 安全地启用应用程序。

性能和能力 ¹	PA-500
防火墙吞吐量（已启用 App-ID）	250 Mbps
威胁防御吞吐量	100 Mbps
IPSec VPN 吞吐量	50 Mbps
每秒新会话	7,500
最大会话	64,000
IPSec VPN 隧道/隧道接口	250
GlobalProtect (SSL VPN) 并发用户	100
SSL 解密会话	1,000
SSL 入站证书	25
虚拟路由器	3
安全区	20
最大策略数量	1,000

¹ 使用 PAN-OS 5.0 在理想测试条件下测得性能和能力。

关于 PA-500 下一代防火墙详细功能描述，请访问：
www.paloaltonetworks.com/literature。

硬件规格

I/O

- (8) 10/100/1000

管理 I/O

- (1) 10/100/1000 带外管理端口 (1) RJ-45 控制台端口

存储容量

- 160GB HDD

电源/ (平均/最大功耗)

- 180W (40W/75W)

最大 BTU/小时

- 256

输入电压 (输入频率)

- 100-240VAC (50-60Hz)

最大电流消耗

- 1A@100VAC

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

- 10.16 年

最大浪涌电流

- 110A@230VAC; 51A@115VAC

可安装机架 (尺寸)

- 1U、19" 标准机架 (1.75" 高 x 10" 深 x 17" 宽)

重量 (独立设备/发货时)

- 8 磅/13 磅

安全性

- UL、CUL、CB

EMI (电磁干扰, ELECTROMAGNETIC INTERFERENCE)

- FCC A 级、CE A 级、VCCI A 级、TUV

认证

- FIPS 140 2级, ICESA、UCAPL

环境

- 工作温度: 32-122°F, 0-50°C
- 非工作温度: -4-158°F, -20-70°C

网络参数

接口模式:

- L2、L3、Tap、虚拟线 (透明模式)

路由

- 模式: OSPF、RIP、BGP、静态
- 转发表大小 (每设备/VR条目): 1,250/1,250
- 基于策略的转发
- 以太网上点对点协议 (PPPoE)
- 多播: PIM-SM, PIM-SSM, IGMP v1、v2 和 v3

高可用性

- 模式: 主动/主动、主动/被动
- 故障检测: 路径监视、接口监视

地址分配

- 设备地址分配: DHCP 客户端/PPPoE/静态
- 用户地址分配: DHCP 服务器/DHCP 中继/静态

IPV6

- L2、L3、Tap、虚拟线 (透明模式)
- 功能: App-ID、User-ID、Content-ID、WildFire 和 SSL 解密

VLAN

- 每个设备/接口最大支持 802.1q VLAN 标签: 4,094/4,094
- 最大接口: 250
- 聚合接口 (802.3ad)

NAT/PAT

- 最大 NAT 规则: 125
- 最大 NAT 规则 (DIPP): 125
- 动态 IP 和端口池: 254
- 动态 IP 池: 16,234
- NAT 模式: 1:1 NAT、n:n NAT、m:n NAT
- DIPP 超量开通 (相同的源端口及IP对应不同目标IP数量): 1
- NAT64

虚拟线

- 最大虚拟线: 125
- 映射到虚拟线的接口类型: 物理和子接口

L2 转发

- ARP 表大小/设备: 500
- MAC 表大小/设备: 500
- IPv6 邻居表大小: 500

安全性

防火墙

- 对应用程序、用户和内容实施基于策略的控制
- 分段数据包保护
- 侦察扫描保护
- 拒绝服务 (DoS) / 分布式拒绝服务 (DDoS) 保护
- 解密: SSL (入站和出站)、SSH

WILDFIRE

- 识别和分析目标和未知文件超过 100 多项恶意行为
- 通过特征库更新对新发现的恶意软件生成并自动提供保护
- 在 1 小时内提供特征库更新, 集成日志/报告; 通过 WildFire API 可以每天提交 100 个样本及 1,000 次基于文件哈希值进行报告检索 (需要订购)

文件和数据过滤

- 文件传输: 对超过 60 多个独特文件类型进行双向控制
- 数据传输: 对未经授权的内容和 SSN 传输进行双向控制
- 隐蔽下载保护

用户整合 (USER-ID)

- Microsoft Active Directory、Novell eDirectory、Sun One 和基于 LDAP 的其他目录
- Microsoft Windows Server 2003/2008/2008r2、Microsoft Exchange Server 2003/2007/2010
- Microsoft Terminal Services、Citrix XenApp
- 使用 XML API 方便的与非标准用户存储库进行集成

IPSEC VPN (站点到站点)

- 密钥交换: 手动密钥、IKE v1
- 加密: 3DES、AES (128 位、192 位、256 位)
- 身份验证: MD5、SHA-1、SHA-256、SHA-384、SHA-512
- 创建动态 VPN 隧道 (GlobalProtect)

威胁防御 (需要订购)

- 应用程序、操作系统漏洞攻击保护
- 病毒串流扫描 (包括 HTML、Javascript、PDF 和压缩文件中嵌入的病毒)、间谍软件、蠕虫

URL 过滤 (需要订购)

- 预定义和自定义 URL 类别
- 最近访问过 URL 的缓存
- 串流扫描作为安全策略部分匹配条件
- 浏览时间信息

服务质量 (QOS)

- 通过应用程序、用户、源、目的地、接口, IPSec VPN 隧道等实现基于策略的流量整形
- 具有 8 个保证、最大和优先带宽参数的流量等级
- 实时带宽监视
- 根据策略区分服务标记
- 支持 QoS 的物理接口: 4

SSL VPN/远程访问 (GLOBALPROTECT)

- GlobalProtect 网关
- GlobalProtect 门户
- 传送: 自适应IPSec、SSL
- 身份验证: LDAP、SecurID 或本地 DB
- 客户端操作系统: Mac OS X 10.6, 10.7 (32/64 位)、10.8 (32/64 位)、Windows XP、Windows Vista (32/64 位)、Windows 7 (32/64 位)
- 支持第三方客户端: Apple iOS、Android 4.0 和更高版本、Linux 用 VPNC IPSec

管理、报告、可视化工具

- 集成的 Web 界面、CLI 或中内管理 (全景)
- 多语言用户界面
- Syslog、Netflow v9 和 SNMP v2/v3
- 基于 XML 的 REST API
- 应用程序的图形化摘要、URL 类别、威胁和数据 (ACC)
- 查看、过滤器和出口流量、威胁、WildFire、URL 和数据过滤日志
- 完全可定制的报告

关于 PA-500 下一代防火墙详细功能描述, 请访问: www.paloaltonetworks.com/literature。