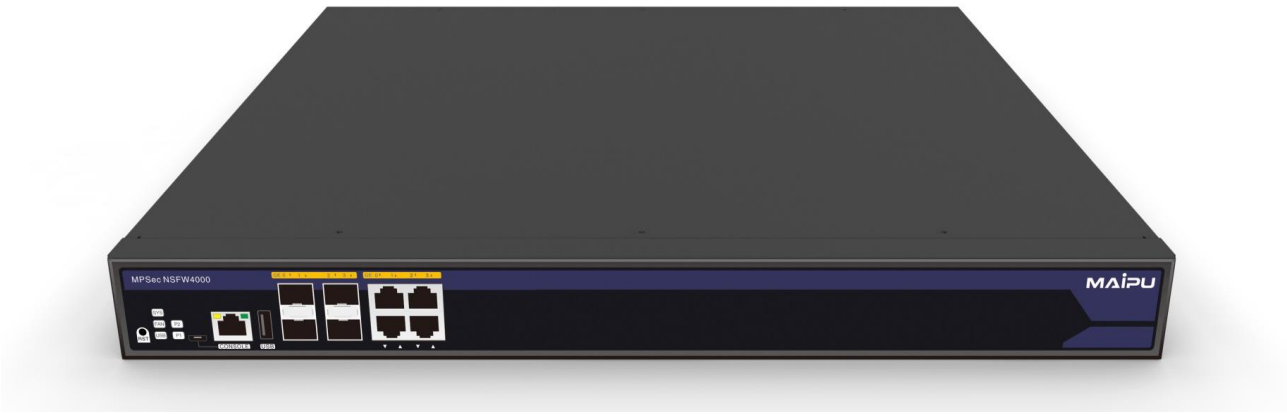
MPSec NSFW4000-F5 下一代自主安全防火墙

产品彩页

目　录

1 产品概述



MPSec NSFW4000-F5 下一代自主安全防火墙

MPSec NSFW4000是采用国产芯片、可以全面应对应用层威胁的高性能下一代自主安全防火墙，通过深入洞察网络流量中的用户、应用和内容，能够为用户提供有效的应用层一体化安全防护，帮助用户安全地开展业务并简化用户的网络安全架构。

MPSec NSFW4000可精确识别几千种网络应用，并提供详尽的应用流量分析和灵活的策略管控。结合用户识别、应用识别、内容识别，可为用户提供可视化及精细化的应用安全管理。同时，MPSec NSFW4000内置了威胁检测引擎，能够抵御包括病毒、木马、SQL注入、XSS跨站脚本、CC攻击在内的各种网络攻击，有效保护用户网络健康及Web服务器安全。

MPSec NSFW4000提供了全面的应用安全防护和灵活的扩展方式，可部署于政府、金融、企业、教育等各个行业，广泛适用于互联网出口、数据中心、网络与服务器安全隔离等多种应用场景。

2 产品特征

◆ 信创名录内自主安全产品

MPSec NSFW4000 通过了公安三所的严格检验，是信创名录内的防火墙产品。整机采用最先进的国产芯片或元器件，包括国产多核 CPU、国产内存条、国产 Flash 等，网络安全设备实现芯片级的自主安全，杜绝国外芯片或元器件存在的“后门”潜在威胁。

◆ 自主稳定的硬件平台

MPSec NSFW4000 硬件由迈普自主设计、制造，共享迈普 20 年的网络设备硬件制造工艺，在产品可靠性与生命周期延续上，可以得到很好的价值保障。

- 硬件平台稳定可靠：共享迈普 20 年的网络设备硬件制造工艺，在市场上长达 20 年，超过 25 万台的长期验证，保障 MPSec NSFW4000 稳定运行可靠。
- 冗余电源设计，固化双交流电源，保障业务安全稳定。

◆ 精细化的应用访问控制

MPSec NSFW4000通过了公安三所的软件测试，完全满足信创场景功能和性能需求。支持深度应用识别技术，可根据协议特征、行为特征及关联分析等，准确识别几千种网络应用，包括数百种移动终端应用。在此基础上，MPSec NSFW4000为用户提供了精细而灵活的应用安全访问控制。

- 一体化访问控制：从用户、应用、内容、时间、威胁、位置进行一体化的管控和防御。内容层的防御与应用识别深度结合，一体化处理。例如：识别出Oracle的流量，进而针对性地进行对应的入侵防御，效率更高，误报更少。
- 精准应用识别：提供了精细化的应用识别机制。用户可根据应用名称、应用类别、风险级别、所用技术、应用特征等精确筛选出感兴趣的应用类型，如具备文件传输功能的通讯软件，或存在已知漏洞、基

于浏览器的Web视频应用等等，从而实现精细化的应用管控。

- 灵活应用控制：基于深度应用识别及精细化的应用筛选，支持灵活的安全控制功能，包括策略阻止、会话限制、流量管控、应用引流或时间限制等。

◆ 全面的安全防护能力

MPSec NSFW4000提供了基于深度应用识别、协议检测和攻击原理分析的入侵防御技术，可有效过滤病毒、木马、蠕虫、间谍软件、漏洞攻击、逃逸攻击等安全威胁，为用户提供L2-L7层网络安全防护。

- 优化的攻击识别算法。能够有效抵御如SYN Flood、UDP Flood、HTTP Flood 等DoS/DDoS 攻击，保障网络与应用系统的安全可用性。

- 专业Web攻击防护功能。支持SQL注入、跨站脚本、CC攻击等检测与过滤，避免Web服务器遭受攻击破坏；

- 高性能的病毒过滤功能。领先的基于流扫描技术的检测引擎可实现低延时的高性能过滤。支持对HTTP、FTP、SMTP、POP3、IMAP等流量和压缩文件（zip，gzip，rar 等）中病毒的查杀。

- 支持千万级URL特征库的URL过滤功能，可帮助网络管理员轻松实现网页浏览访问控制，避免恶意URL 带来的威胁渗入。

3 产品规格

3.1 硬件规格

产品规格/产品型号		MPSec NSFW4000-F5-AC
硬件架构	CPU	国产 CPU
	硬盘	500GB
固定接口	以太口	4 个千兆电口，4 个千兆光口
	Console 口	1
	USB 口	1
电气特性	电源	冗余电源
	输入	交流 100-240VAC/50-60HZ
	风扇	静音风扇
环境特性	工作环境温度	0-45℃
	工作环境湿度	10%-90%，无凝结
	存储环境温度	-40~65℃
	存储环境湿度	5%-95%，无凝结
尺寸	宽度	19 英寸（442mm）
	高度	1U（44.2mm）
	深度	380mm

3.2 软件规格

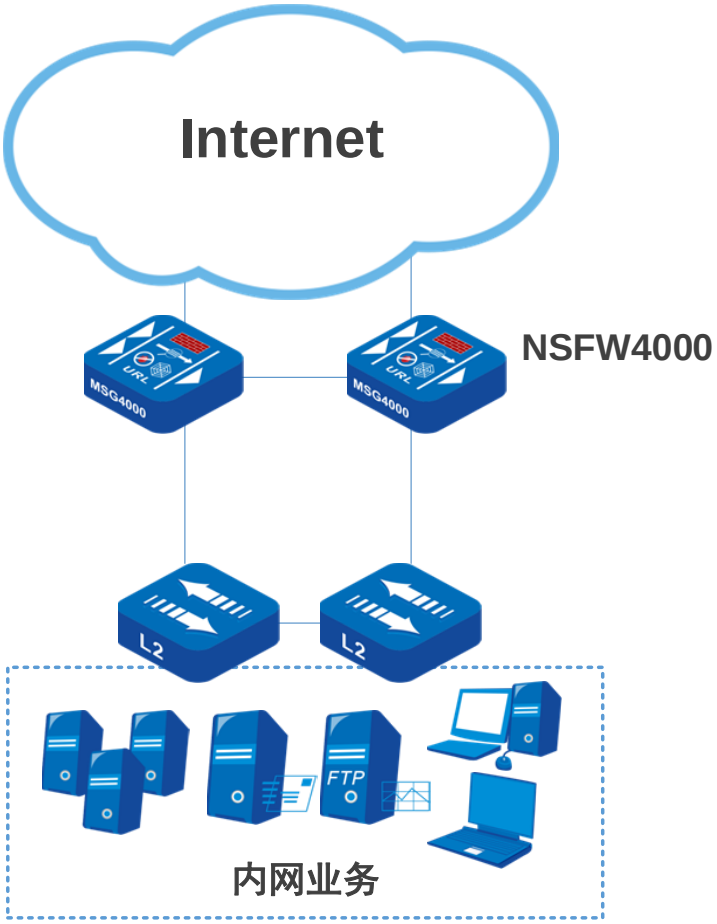
功能规格	功能描述
网络行为识别与管理	● 支持PC、移动终端应用识别 ● 支持虚实身份对应以及时间轴方式显示用户的网络访问轨迹 ● 支持防私接防共享，可自定义限定单IP支持的终端数量以及冻结时间 ● 多达5000多种的应用特征库，包括450多种移动应用 ● 应用特征库支持网络实时更新
用户认证	● 支持本地用户IPv6认证，本地认证页面支持自定义 ● 支持外部服务器用户认证（RADIUS、LDAP、MS AD、TACACS+） ● Web认证、微信认证、短信认证、免认证
防火墙	● 基于深度应用识别的访问控制 ● 基于应用 / 角色的安全策略 ● 强大的 NAT 及 ALG
攻击防护	● 多种畸形报文攻击防护 ● SYN Flood、UDP Flood、HTTP Flood等多种DoS/ DDoS攻击防护 ● 支持 ARP 攻击防护
Web 防护	● 内置Web防护特征库，提供HTTP协议检查、XSS攻击、恶意扫描与爬虫、服务器防护、CMS漏洞防护等不少于11种的防护类型 ● 支持HTTP协议的精确访问控制 ● 支持防盗链、CSRF攻击、CC攻击、应用隐藏、网页防篡改等防护 ● 支持缓存防篡改网页，可手动清理缓存内容

入侵防御	● 基于状态、精准的高性能攻击检测和防御 ● 实时攻击源阻断、IP屏蔽、攻击事件记录 ● 支持针对HTTP、SMTP、IMAP、POP3等多种协议和应用的攻击检测和防御 ● 支持缓冲区溢出、SQL注入和跨站脚本攻击的检测和防护 ● 超过2000种特征的攻击检测和防御，特征库支持网络实时更新
病毒过滤	● 基于流的病毒过滤 ● 支持压缩病毒文件的扫描 ● 支持上百万种病毒的查杀，病毒库定期与及时更新
网页访问控制	● 基于角色、时间、优先级、网页类别等条件的Web网页访问控制 ● 支持自定义URL类别，支持千万级URL特征库，URL库支持网络实时更新
带宽管理	● 根据安全域、接口、地址、用户/用户组、服务/服务组、应用/应用组、时间等信息划分管道 ● 支持四层管道嵌套 ● 对多层级管道进行最大带宽限制、最小带宽保证、每IP或每用户的最大带宽限制和最小带宽保证 ● 基于时间和优先级的差分服务，支持带宽均分策略
VPN	● 支持标准IPSec VPN ● 支持 Android、iOS 等移动设备的安全接入
IPv6	● IPv6访问控制 ● 隧道、ISATAP、6TO4等多种过渡技术 ● IPv6路由（ 静态路由、OSPFv3）
高可用性(HA)	● 主/主模式（A/A）和主/备模式（A/S）

	• 支持配置、会话同步
监控统计	• 支持URL日志、NAT日志、会话日志、威胁日志等 • 支持实时流量统计和分析功能 • 支持安全事件统计功能 • 支持以 ICMP/DNS/TCP 等方式对目标进行连通性和时延探测

4 典型应用场景

4.1 互联网出口



安全需求：

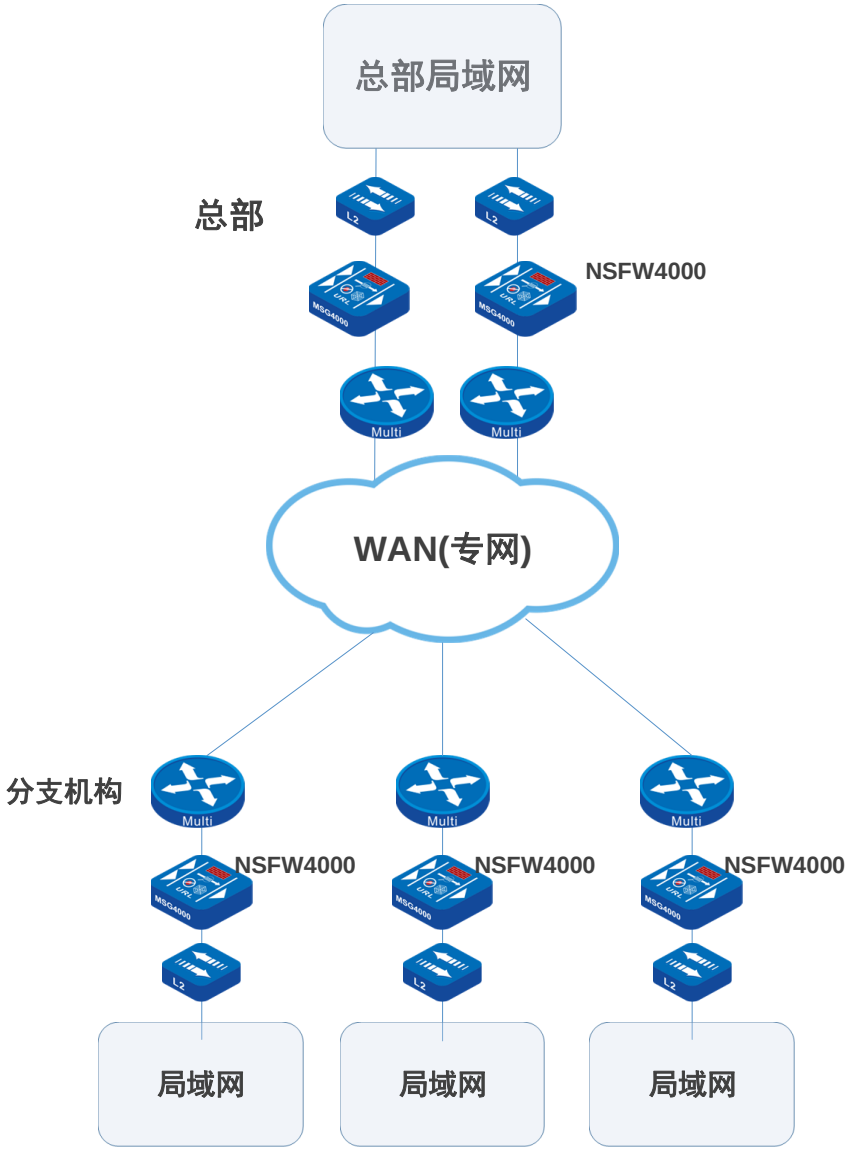
- 多出口链路备份，链路负载均衡；
- 外部病毒，攻击，恶意软件防护；
- 内网用户滥用网络带宽管控；

解决方案：

- 通过 ISP 策略路由，等价路由，链路探测等实现多出口智能选路功能；

- 通过一体化引擎中 IPS，AV，URL 过滤等实现对外部病毒，攻击，恶意站点防御；
- 通过应用层访问控制，带宽管理，URL 过滤，内容过滤等策略实现用户上网管理；

4.2 内网安全隔离



安全需求：

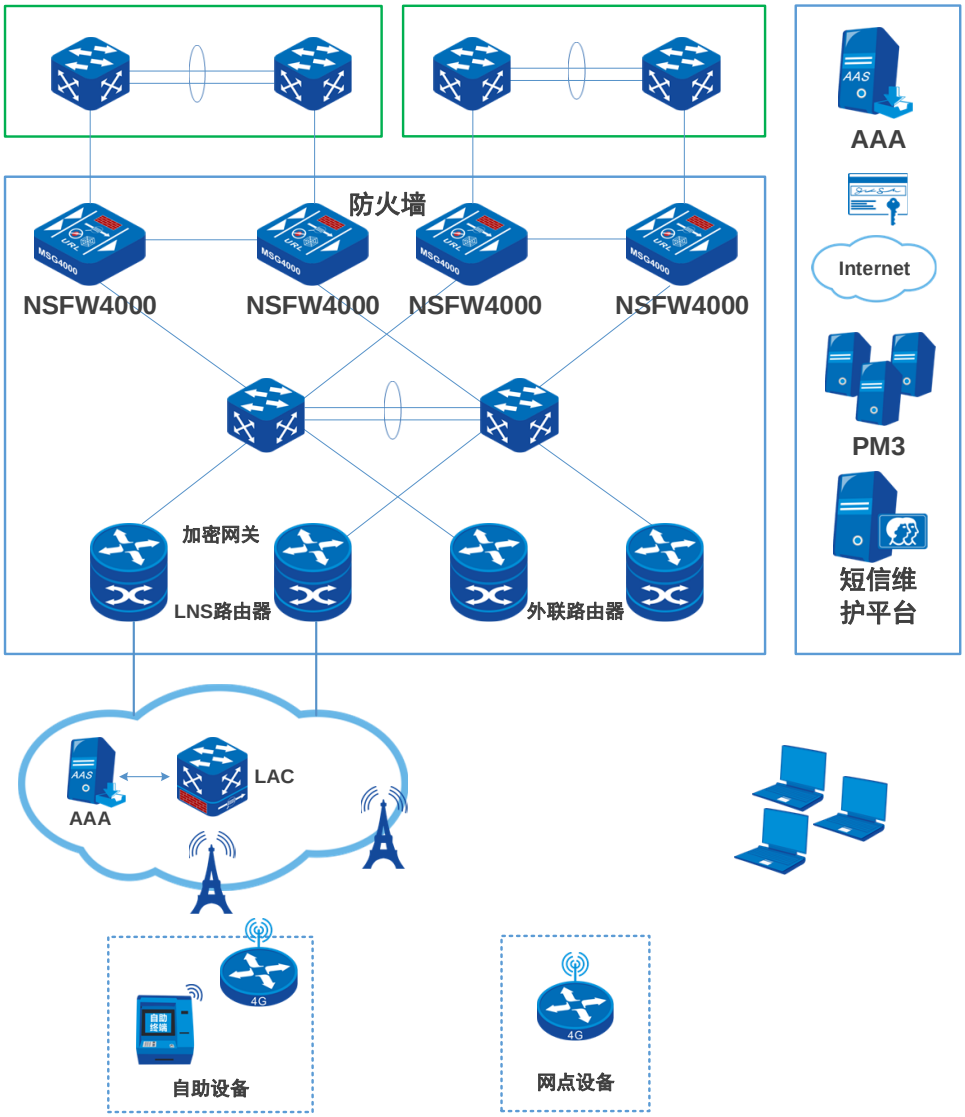
- 内部用户的入侵行为；
- 内部病毒扩散；
- 内部人员的非法访问；

- 资源滥用，挤占业务带宽；

解决方案：

- 基于应用的安全控制，防止非法访问以及业务伪装访问；
- 入侵防御，防病毒，抗攻击，保障总部业务安全可靠；
- 识别上千种应用，基于应用的带宽限制、最小带宽保障，保障业务体验；

4.3 3/4/5G 安全隔离



安全需求：

- 3/4G 拨入人员的非法访问；

- 资源滥用，挤占业务带宽；
- 内部关键业务系统的保护；

解决方案：

- 基于应用的安全控制，防止非法访问以及业务伪装访问；
- 入侵防御，防病毒，抗攻击，保障总部业务安全可靠；