



## iKuai-SGW-560A 下一代防火墙产品

### 产品概述

iKuai-SGW-560A下一代防火墙，是面向移动互联时代的全面保障L2-L7安全的新一代安全产品。产品采用高性能硬件平台，结合单路径并行处理的用户识别、应用识别和安全检测引擎，实现对用户、应用和内容的深入分析，为用户提供高性能、可视化、精准有效的应用层一体化安全防护体系。iKuai-SGW-560A支持基于管道的4层嵌套的带宽管理，支持包含链路负载均衡技术的全面的智能网络管理，结合双机热备和VRRP高可靠性保障，可灵活的部署在透明、NAT、VPN、多出口、双链路等网络环境中，帮助用户方便安全的开展业务的同时简化网络安全架构，为客户信息安全保驾护航。

## ■ 产品特点

### >> 高性能

- 采用自主操作系统，高性能硬件平台。
- 通过多核并行化处理、特征库树形存储、流扫描处理、零拷贝、高性能硬件平台等技术手段，实现整个处理过程一次拆包。
- 开启多重防护功能，确保高速度、低时延的安全防护。

### >> VPN

- iKuai-SGW 内置VPN功能，支持GRE、IPSec、L2TP、SSLVPN多种VPN业务模式。
- 支持对VPN隧道内的数据流进行管理，规范VPN隧道内上网行为并消除管理盲区。

### >> 配置维护简洁

- iKuai-SGW的安全策略采用集中展示，独立配置，一体化检测的方案，为用户提供清晰可见的策略展现，提升用户管理运维体验。
- 防火墙策略、应用控制策略、审计策略、安全防护策略、入侵检测策略、防病毒策略、VPN策略、流控策略集中展示，独立配置。
- 管理者可以根据不同的管控需求，为不同的用户定制不同的管理策略，灵活方便，维护简单，条理清晰，效果良好。
- 可通过我司的云平台可以进行统一管理，设备、网络运行状态可视化分析，支持远程管理，有效减少运维的成本。

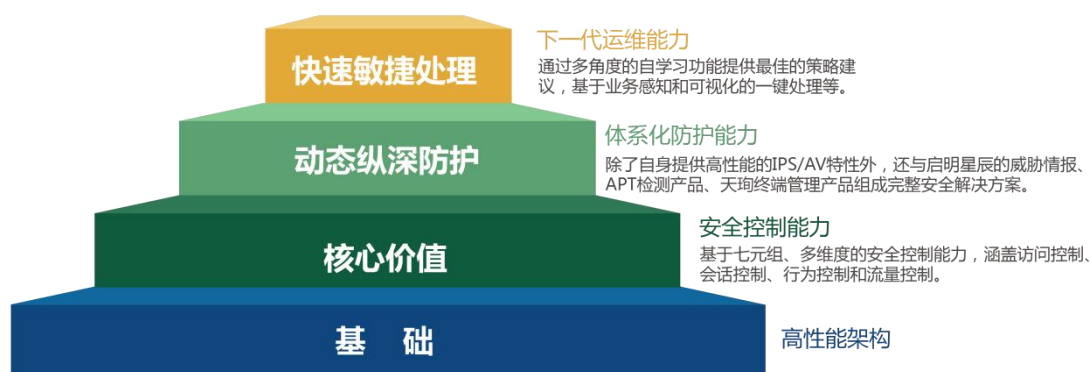
## &gt;&gt; 组网方式灵活

- 支持MCE IPSEC、802.1Q、GRE、VPN track等网络特性
- 支持PPPoE、DHCP、Vlan、Trunk等多种接入方式,可以灵活部署在路由模式、透明模式和混合模式的网络中。
- 系统支持IPv4/IPv6双协议栈,支持NAT64、NAT46、NAT66等地址转换技术,可以方便的部署在v6、v4网络边界,为更新升级过程中的网络提供安全方案。

## &gt;&gt; 高可靠性

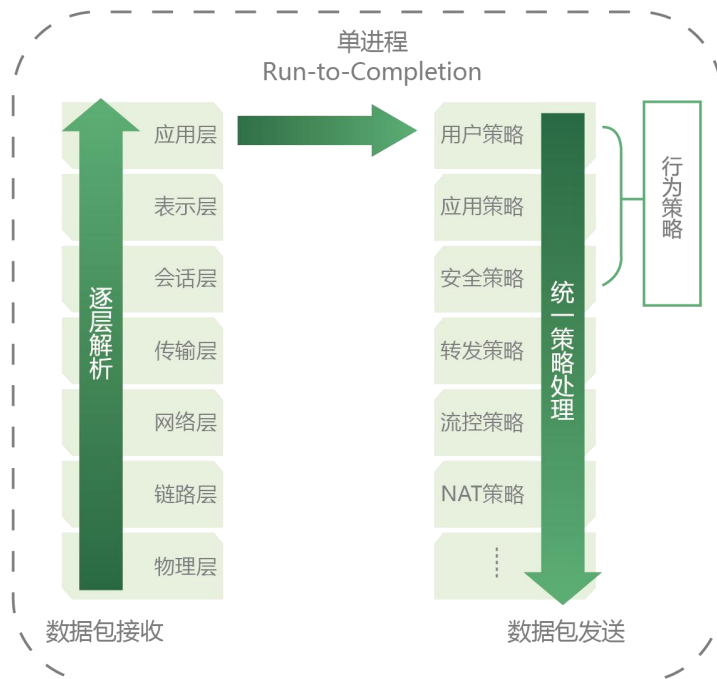
- 支持双机热备、VRRP功能。不会成为网络瓶颈和故障点,确保网络高可靠性。
- 支持多链路负载均衡,可以动态监控链路的实时状态,提供多种专业的静态和动态流量分担方法,从而有效提升多链路接入的效率、可靠性和整体性能。

## 下一代防火墙



将用户和应用作为安全防护的核心,采用先进的用户识别和应用识别技术,实现对用户和应用的精细管控和行为审计。

## 一体化安全引擎



为客户提供基于用户和应用的一体化安全防护引擎，用户身份验证，以及L4-L7层的安全防护并行完成，让安全多维度、无死角。

## 智能流控

全面识别互联网常见应用，包括经常造成带宽滥用、IM即时通讯、在线视频、游戏等。将iKuai防火墙部署于网络出口，可以有效遏制各种应用抢夺带宽和IT资源，从而确保网络资源的合理配置和关键业务的服务质量，显著提高网络的整体性能。

## 产品规格

| iKuai-SGW-560A |                               |                 |            |
|----------------|-------------------------------|-----------------|------------|
| 规格             | 描述                            | 规格              | 描述         |
| 内存             | 16G                           | 硬盘              | 64G        |
| 接口             | 16 个千兆电口, 2 个千兆光口,<br>4 个万兆光口 | USB 接口          | 2 个 USB2.0 |
| 最大吞吐           | 35Gbps                        | 并发连接            | 1000 万     |
| 每秒新建           | 25 万/秒                        | IPSec 性能 (混合包长) | 1Gbps      |
| 电源             | 200~240V, ≤2.5A, 50~60Hz      | 功耗              | ≤150W      |
| 工作温度           | 0-45℃                         | 存储湿度            | 5%-95%     |
| 工作湿度           | 5%-90% (非凝露)                  | 存储温度            | -40-70℃    |
| 机箱颜色           | 黑色                            | 净重              | 15kg       |
| 尺寸 (长 宽 高)mm   | 19 寸/2U<br>(440 × 501 × 88)   | 选配(拓展)          | 网卡         |

## 功能规格

| 功能  | 描述                                         |
|-----|--------------------------------------------|
| 网络  | 支持透明、路由、混合三种工作模式                           |
|     | 支持物理口、BVI 口、VLAN 口、聚合口、隧道口、环回口             |
|     | 支持 GRE 接口                                  |
|     | 支持安全域                                      |
|     | 支持 PPPoE 客户端                               |
|     | 支持 DHCP 服务器和中继                             |
|     | 支持 DHCP 客户端                                |
|     | 支持静态 ARP、IP-MAC 绑定                         |
|     | 支持 DNS 客户端、服务器                             |
|     | 支持静态路由、动态路由 (RIP、OSPF、BGP4)                |
|     | 支持基于应用和用户的策略路由                             |
|     | 支持源 NAT、目的 NAT、静态 NAT                      |
|     | 支持各种应用协议的 NAT 穿越: FTP、TFTP、H.323、SQL * NET |
|     | 支持 FTP、TFTP 协议非标准端口 ALG                    |
| 防火墙 | 支持基于接口/安全域、地址、用户、服务、应用和时间的防火墙策略            |
|     | 支持常见 DOS 攻击防护                              |
|     | 支持基于 TCP、UDP 和 ICMP 的扫描防护                  |

|          |                                                                                                          |
|----------|----------------------------------------------------------------------------------------------------------|
|          | 支持智能 TCP Flood 防御                                                                                        |
|          | 支持 TCPFlood、UDP Flood、ICMP Flood 攻击防护                                                                    |
|          | 支持基于协议的长连接管理                                                                                             |
| 上网行为控制   | 支持应用特征和行为的访问控制策略,可对 IM、流媒体、P2P、游戏、股票等应用行为控制                                                              |
|          | 支持 IM 登陆控制和黑白名单                                                                                          |
|          | 支持网页内容和关键字过滤                                                                                             |
|          | 支持邮件主题、正文关键字、收件人、发件人过滤                                                                                   |
|          | 支持基于 URL 过滤                                                                                              |
| 入侵防御     | 支持基于源、目的、规则集的入侵检测。                                                                                       |
|          | 支持 5 种自定义动作                                                                                              |
|          | 可记录攻击日志和报警。                                                                                              |
|          | 支持系统规则库手动、自动升级。                                                                                          |
|          | 系统定义超过 2000 条规则, 包含 Backdoor, bufferoverflow, dosddos, im, p2p, vulnerability, scan, webcgi, worm, game。 |
|          | 支持 SQL 注入、XSS 攻击防御                                                                                       |
|          | 支持 IDS 联动                                                                                                |
| 防病毒      | 支持 HTTP, FTP, POP3, SMTP, IMAP 协议的病毒查杀                                                                   |
|          | 查杀邮件正文/附件、网页及下载文件中包含的病毒                                                                                  |
|          | 支持 300 万余种病毒的查杀, 病毒库定期与及时更新                                                                              |
|          | 支持启发式扫描查杀未知病毒                                                                                            |
|          | 支持 ZIP/RAR 等压缩文件的病毒查杀                                                                                    |
|          | 支持 TAR 等多种打包文件的病毒查杀                                                                                      |
| 弱口令检查    | 支持对服务器、客户端进行的口令暴力破解的攻击防护                                                                                 |
|          | 支持高、中、低三种密码检查强度                                                                                          |
|          | 支持对常见应用（如 HTTP、Telnet、FTP、SMTP、POP3 等）进行弱口令检查, 并上报安全事件                                                   |
| Web 应用防护 | 支持并开通 WEB 防护功能, 支持对 100 个站点制订 Web 应用防护策略                                                                 |
|          | 支持 HTTP 请求回应的头、体检查                                                                                       |
|          | 支持自定义 WEB 安全防护事件, 可对请求参数、各个头域、内容关键字、文件类型等进行灵活组合生成策略                                                      |
|          | 支持 HTTP 的异常检测, 包括版本、方法、URL、头域字段、传输文件等的合规性检查                                                              |
|          | 支持检测 WEB 攻击事件, 包括: SQL 注入, XSS 跨站脚本攻击, PHP 代码注入, WEBSHELL 攻击、信息泄漏等问题                                     |
|          | 支持独立的 WEB 特征库, 并可以自动、手工升级                                                                                |
| 流量管理     | 支持基于线路和通道嵌套的带宽管理                                                                                         |
|          | 支持基于接口的上下行带宽管理                                                                                           |
|          | 支持高、中、低优先级通道设置                                                                                           |
|          | 支持应用、用户、源地址、服务、时间的通道匹配                                                                                   |

|      |                                           |
|------|-------------------------------------------|
|      | 支持带宽限制、带宽保障和弹性带宽                          |
|      | 支持每 IP 限速                                 |
|      | 自动支持流量整形                                  |
|      | 支持基于用户、地址排除策略                             |
| 用户   | 支持用户自动识别                                  |
|      | 支持本地用户认证                                  |
|      | 支持基于源接口 / 安全域，目的接口 / 安全域，源 / 目的地址，时间的用户策略 |
|      | 支持在线用户监控和管理                               |
| IPv6 | 支持 IPv4/IPv6 双协议栈                         |
|      | 支持路由、透明、混合模式部署                            |
|      | 支持 NAT66，支持跨协议转换 NAT64 和 NAT46            |
|      | 支持 DNSv6 服务器                              |
|      | 支持 IPv6 静态路由                              |
|      | 支持 Ipv6 包过滤                               |
|      | 支持 Ipv6 MAC 绑定和扩展头过滤                      |
|      | 支持 Ipv6 策略路由                              |
|      | 支持 Ipv6 隧道；DS - LITE                      |
|      | 支持 DHCPv6 服务器                             |
|      | 支持设备管理和维护协议：PING、HTTP、HTTPS、SSH、TELNET    |
| VPN  | 支持标准协议的 IPSecVPN 协议                       |
|      | 支持基于与共享密钥/证书的协商认证方式                       |
|      | 支持网关到网关和远程接入部署模式                          |
| 对象管理 | 支持地址、服务、时间计划对象化                           |
|      | 支持应用对象化，含应用对象、应用类                         |
|      | 支持关键字对象化，含网页关键字、应用账号关键字、URL 关键字、邮件关键字等    |
|      | 支持用户对象，用户静态绑定                             |
|      | 支持第三方用户认证服务器：LDAP、RADIUS                  |
|      | 支持本地 CA 中心和用户证书签发、维护                      |
|      | 支持 1000 多种应用并定期更新                         |
|      | 支持默认自带 2000+入侵防御事件                        |
|      | 支持网络健康检查模板                                |
| 系统管理 | 支持 WEB（HTTP/HTTPS）、命令行、Console 进行管理配置     |
|      | 支持管理员权限划分，可自定义管理员角色，支持只允许授权管理员访问日志        |
|      | 支持对授权管理员的口令鉴别                             |
|      | 支持管理员用户的第三方用户认证，RADIUS/LDAP               |

|       |                                                      |
|-------|------------------------------------------------------|
|       | 支持 SNMP v1、v2、v3                                     |
|       | 支持 NTP 时钟同步和认证                                       |
|       | 支持本地双配置文件                                            |
|       | 支持系统资源异常使用监控                                         |
|       | 支持 web 图形方式的网络调试、诊断命令和抓包                             |
| 高可用性  | 支持主-主和主-备模式                                          |
|       | 备机可通过配置带外管理 IP 进行管理                                  |
|       | 支持标准的 VRRP 协议                                        |
|       | 支持基于心跳信号丢失、链路断开等多种方式的 HA 切换条件及逻辑                     |
|       | 支持 HA 设备之间的会话自动同步，确保 HA 切换时业务不发生任何中断                 |
|       | 支持设置抢占优先级，高优先级设备可自动抢占主设备状态                           |
| 日志和监控 | 支持本地系统日志、操作日志、攻击实时日志、应用控制日志、网侵防御日志，病毒防护日志            |
|       | 支持 Syslog 系统日志、操作日志、NAT 日志、策略日志、应用控制日志、入侵防护日志、病毒防护日志 |
|       | 支持本地导出为 excel、txt、xml 格式                             |
|       | 支持本地日志存储耗尽机制（可配置删除百分比）                               |
|       | 支持邮件告警                                               |
|       | 支持实时流量统计和分析功能                                        |
|       | 支持在线用户监控、查询、冻结                                       |
|       | 支持系统会话状态监控                                           |
|       | 支持接口状态监控，接口收发包、接口转发速率等                               |
|       | 支持入侵防护统计、病毒防护统计                                      |
|       | 支持 Top10 应用的流量统计和趋势绘图                                |
|       | 支持 Top10 用户的流量统计和趋势绘图                                |

## 全讯汇聚网络科技（北京）有限公司

通讯地址：北京市丰台区南四环西路186号汉威国际广场三区5号楼502

邮政编码：100000

技术支持电话：



访问官方网站

400-877-3227

公司网址: [www.ikuai8.com](http://www.ikuai8.com)