专业应用交付　高性能融合安全

iKuai-SGW-12 下一代防火墙

产品概述

iKuai-SGW-12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-12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。
- 支持统一管理，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。

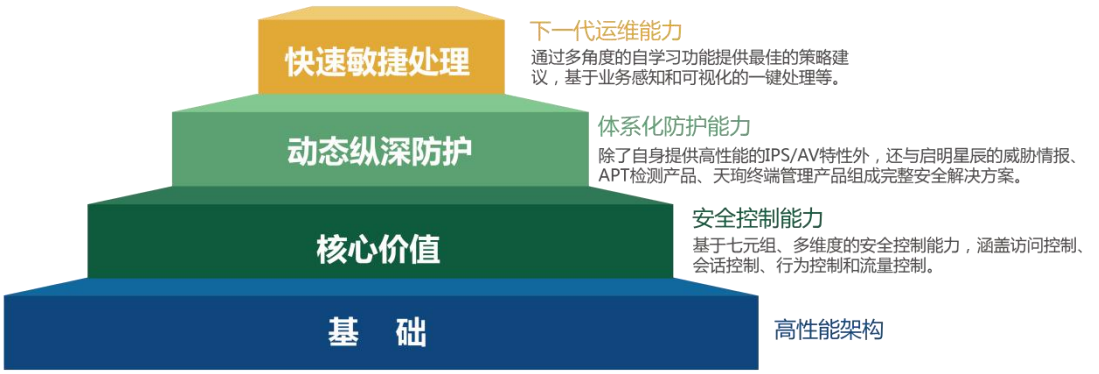
>> 组网方式灵活

- 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。

>> 高可靠性

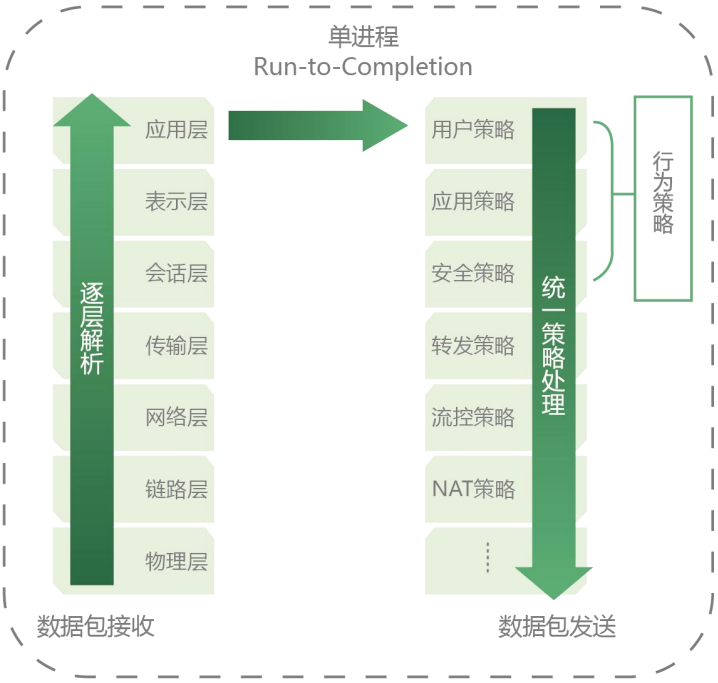
- 支持双机热备、VRRP功能。不会成为网络瓶颈和故障点，确保网络高可靠性。
- 支持多链路负载均衡，可以动态监控链路的实时状态，提供多种专业的静态和动态流量分担方法，从而有效提升多链路接入的效率、可靠性和整体性能。

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-12			
规格	描述	规格	描述
内存	4G	硬盘	8G
接口	10 个千兆电口+2 个千兆 Combo 口	USB 接口	2 个 USB2.0
最大吞吐	2.5Gbps	并发连接	120 万
每秒新建	3 万/秒	IPSec 性能	500Mbs
电源	AC 100-240V	功耗	≤30W
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	5.3kg
尺寸(长宽高)mm	440*330*44	选配(拓展)	无

功能规格

功能	描述
部署模式	支持透明、路由、混合及单臂部署
IPV6/V4 双栈	支持 IPV6/V4 双栈同时工作，所有安全功能均支持双栈下使用
物理接口	支持手动设置 IP 地址，支持 DHCP 获取 IP 地址，支持多 IP 地址
802.1Q VLAN	支持，最多 4096 个 VLAN，物理接口支持以 TAG 或 UNTAG 方式加入 VLAN
VLAN	支持 VLAN 透明桥模式下的二层转发及安全控制
透明桥接口	支持桥接口配置管理
接口联动	支持多个物理接口（可以多于 2 个）绑定为接口联动组，实现联动组内接口之间链路状态一致
链路聚合	支持链路聚合，最多可将 16 个接口捆绑为一个链路；支持 LACP 链路汇聚控制协议，支持以目的 MAC 哈希方式或源目的 IP 及端口哈希方式进行包分配
静态路由	支持静态路由，支持等价路由，支持静态路由权重，支持多种静态路由健康检查方式，支持 BFD 检查
动态路由	支持 RIPv1、RIPv2、OSPFv2（支持 BFD 检测）、BGP4 等动态路由协议
策略路由	支持基于入接口、源 IP、目的 IP、服务端口、应用的目的策略路由，在一条策略路由匹配项中可设定多个下一跳，
链路负载均衡	支持链路负载均衡，提供轮询、加权轮询、哈希等多种负载均衡算法，支持链路双重健康检查，支持设定链路的优先级和权重
健康检查	支持通过 ICMP、TCP、DNS 和 HTTP 协议实现对链路可用性或路由下一条的健康检查，
会话保持	支持对等价路由、策略路由和链路负载均衡的目的会话保持功能，支持对会话保持的超时时间和目标掩码进行设定

NAT	支持源 NAT、目的 NAT、静态 NAT，支持一对一、一对多和多对多等形式的 NAT；支持 NAT 源端口复用，单个公网 IP 支持的并发会话数量无限制，支持 NAT 命中次数统计、并发连接数统计。
NAT46/NAT64	支持跨协议 NAT 转换，包括将 IPv4 协议转换为 IPv6，或将 IPv6 协议报文转换为 IPv4
ALG	支持各种应用协议的 NAT 穿越：FTP、TFTP、H.323、SQL*NET
NAT 地址池	支持多个连续或不连续地址段作为 NAT 地址池，支持基于哈希的源地址保持策略；支持地址池健康探测
VPN	IPSEC VPN 支持 SM1/SM2/SM3/SM4 国密算法
	支持 IPSec VPN、L2TP、GRE，支持站点到站点模式和中端到站点模式，支持 PC/手机/Pad 的 IPSec VPN 接入。
	支持 SSL VPN，支持隧道模式及 WEB 代理模式，支持证书认证（双因子认证）；支持软件国密算法套件
	SSLVPN 客户端支持 windows、linux、MAC OS 以及麒麟、统信等国产化操作系统
STP	支持标准 STP 生成树协议
DHCP	支持 DHCP Server，支持 DHCP 协议下的 IP-MAC 绑定策略
DNS Server	支持作为标准 DNS 服务器提供 DNS 服务，支持 DNS 授权区域 （DNS ZONE）
DNS 记录	支持多种 DNS 记录 ，包括 A ，AAA，NS，CNMAE，TXT，MX，PTR 记录
DNS 透明代理	支持 DNS 透明代理，支持多个外部 DNS 服务器负载均衡，负载均衡算法包括轮询/加权轮询/优先级等；
防火墙访问控制	基于网络接口、安全域、源 IP、目的 IP、域名地址、服务端口、应用、用户的访问控制；支持时间表设定，支持绝对时间和周期时间；应用采用基于 DPI/DFI 的智能应用识别技术实现动态识别
	支持策略预编译，确保在大量复杂策略的情况下，防火墙性能不衰减，支持策略预编译自动更新，当策略关联的地址对象等信息修改时，自动更新编译结果
	支持设定防火墙策略默认动作：默认阻断全部或默认允许全部。
	支持基于防火墙策略的流量统计和命中统计
	支持基于源地址、目的地址、服务类型和动作的策略搜索
	支持策略去重功能，完全相同的防火墙策略系统自动提示重复。
	支持安全策略预编译功能，在大量防火墙策略情况下，采用策略预编译功能将大幅减少因策略匹配而造成的性能衰减
	支持基于物理接口、VLAN 接口和链路聚合接口的安全域设定，支持安全域内自动允许互访
	支持到防火墙本地报文的安全过滤与阻断，并记录日志
会话控制	支持基于接口/安全域、地址、用户、服务、应用和时间参数的总连接数控制策略
	支持基于接口/安全域、地址、用户、服务、应用和时间参数的每秒总连接速率控制策略
	支持基于接口/安全域、地址、用户、服务、应用和时间参数的每源 IP 连接数控制策略

	支持基于接口/安全域、地址、用户、服务、应用和时间参数的每源 IP 每秒连接速率控制策略
	支持基于接口/安全域、地址、用户、服务、应用和时间参数的每目的 IP 连接数控制策略
	支持基于接口/安全域、地址、用户、服务、应用和时间参数的每目的 IP 每秒连接速率控制策略
入侵防御	采用基于状态的协议分析和协议树匹配算法，同时支持 IPV4 及 IPV6 环境下的入侵防御功能
	系统预定义超过 3600 种攻击特征库，每周更新，并支持用户自定义特征
	支持基于接口/安全域、地址、用户、服务和时间参数的入侵防护策略设置，不同的入侵防御策略可采用不同的事件库和匹配动作
	支持在线、旁路及混合部署
	支持抓包取证，可选择将产生 IPS 事件的会话所有报文进行存储，并与 IPS 日志关联一键导出
防病毒	基于安天防病毒引擎，病毒库数量 220 万条，每周更新
	支持对 HTTP、FTP、POP3、IMAP、SMTP 协议下的文件进行病毒扫描
	支持自定义扫描文件类型
	支持基于接口/安全域、地址、用户、服务和时间参数的防病毒策略设置
	支持在线、旁路及混合部署
弱口令检查	支持对 HTTP、Telnet、SSH、FTP、SMTP、POP3 等各种协议进行弱口令检查，并上报安全事件
	支持高、中、低三种密码检查强度
	支持对源目的 IP 地址进行过滤检查。
	支持对口令频繁暴力破解的检测。检测到暴力破解后可选择告警、阻断访问、阻断源 ip 等动作
抗拒绝服务攻击	支持基于入接口、源地址、目的地址和服务类型的 TCP Flood 防护，包括总报文速率限制、每源主机报文速率限制和每目标主机报文速率限制。在达到管理员设定的阈值时，可选的防护动作包括：智能 syn cookie、阻断超限报文或仅告警。
	支持基于入接口、源地址、目的地址和服务类型的 UDP Flood 防护，包括总报文速率限制、每源主机报文速率限制和每目标主机报文速率限制。在达到管理员设定的阈值时，可选的防护动作包括：阻断超限报文或仅告警。
	支持基于入接口、源地址、目的地址和服务类型的 ICMP Flood 防护，包括总报文速率限制、每源主机报文速率限制和每目标主机报文速率限制。在达到管理员设定的阈值时，可选的防护动作包括：阻断超限报文或仅告警。
	支持对扫描攻击的检测和防护，包括 TCP 扫描、UDP 扫描和 Ping 扫描，管理员可自行设定扫描识别阈值及攻击主机抑制时长。
	支持对 Jolt2、Land-Base、Ping of death、Syn flag、Tear drop、Winnuke、Smurf 等 DoS 攻击的防护
ARP 攻击防护	支持 IP-MAC 绑定，支持对 IP-MAC 绑定的唯一性检查
	支持对特定接口或 IP-MAC 对的主动保护
	支持防 ARP 欺骗功能，可主动关闭 ARP 学习或主动发送合法 ARP
	支持防 ARP Flood 攻击功能，可设定 ARP 报文的攻击识别阈值及攻击主机

	抑制时长
黑名单	支持基于 IP 网段、IP 地址范围、ISP 地址库、区域地址库等的多种黑名单阻断方式
	支持分组功能，并支持基于分组的一键启停
	支持对黑名单进行其实生效时间设置
	支持基于 IP 的黑名单功能，可临时或永久阻断特定 IP 的访问，最大支持 3 万条 IP 记录
	支持黑名单的导入导出
	支持在会话管理界面根据当前会话信息直接设置黑名单
域名黑名单	支持基于单条域名的黑名单，可临时或永久阻断对特定域名的访问。域名可设置为精确或模糊匹配。
IP 地址白名单	支持基于单 IP、IP 网段、ISP 地址库、区域地址库的白名单，匹配白名单的用户将跳过防火墙策略、安全防护策略等防火墙过滤直接转发
威胁情报	支持对经过设备访问的域名以及目的 ip 进行威胁情报查询，如果查询威胁访问，支持告警、阻断等动作。支持根据情报的威胁值、信誉值、威胁类型等进行处置判定。
	威胁情报来源支持离线库和云查两种，本地离线库规模为 50W 条，本地查询未命中将通过云查方式继续查询。离线库支持定期自动更新。
	威胁情报支持勒索软件、挖矿软件、网银木马、窃密木马、黑客工具、后门软件、僵尸网络、蠕虫网络、APT 攻击等几十种分类
	支持对命中情报事件进行列表展示，并在整机威胁图表中展示相关内容
恶意文件防护	支持对恶意文件的检测，阻断、日志上报。支持手动添加恶意文件 hash。
	支持恶意文件库的自动升级和离线导入
	支持手工添加、删除恶意文件特征
SSL 流量解密	支持对通过设备的 SSL 流量进行解密。支持代理模式和透明模式两种组网；并支持客户端模式（由内向外）和服务器模式（从外到内）两种模式
	支持对 HTTS、POP3S、SMTPS、IMAPS 等应用协议进行解密过滤
	支持对源地址、URL 分类、域名等进行匹配后进行流量解密
	支持根 CA 推送，支持网站证书自动签发
	支持域名、IP 白名单，支持预定义白名单库
智能应用识别	采用基于深度包检测（DPI）、深度流检测（DFI）和网络行为分析（NBA）技术，实现对主流应用的准确识别。
应用控制	基于智能应用识别，提供领先的应用行为控制功能，可基于应用的深度信息和内容实现精细化控制。
QQ 控制	支持对 PC 端、手机端、WEB QQ、QQ 集成登录插件和 QQ 空间的深度识别，并支持基于 QQ 号的黑/白名单管理
微信控制	支持对微信的登录、收发消息、朋友圈、收发文件及漂流瓶等动作的识别和管理，并支持基于微信号的黑/白名单管理
URL 分类过滤	支持基于预定义或自定义分类，对网站访问进行分类管理和控制，系统内置超过 20 万条网站分类库
社交网络类应用控制	支持对微博、百度贴吧、天涯、Facebook、Twitter 等近百个社交媒体的识别及内容控制
搜索引擎类应用控	支持对百度、谷歌、BING、搜狗、亚马逊等数十种搜索引擎的识别及内容

制	控制
P2P 下载类应用控制	支持对迅雷、电驴、比特精灵等常见 P2P 下载的准确识别和控制
视频类应用控制	支持对优酷、斗鱼、CCTV 等在线视频、视频直播类应用的识别和控制
电子邮件类应用控制	支持对 SMTP、POP3、IMAP 协议的深度识别和控制，支持对 163 邮箱、QQ 邮箱、126 邮箱等 Web Mail 的深度识别和控制，可基于收件人、发件人、邮件标题、邮件内容、附件名称、协议命令等参数实现内容级管理和控制
应用特征库	内置了超过 1000 种应用的应用特征库，包括 Windows 平台、安卓平台及 iOS 平台的绝大多数常见应用
应用分类	基于业务行为模式，一千余种应用被分为 20 大类，并支持基于应用大类或自定义应用组的应用控制
应用特征库升级	支持自动、手动方式的应用特征库升级，特征库更新周期至少每周一次。
技术架构	基于多级令牌桶、智能应用识别和多核并行化技术的专业流控，控制粒度为 1K bps，带宽控制的误差小于 1%
线路设定	支持基于物理接口或 VLAN 接口的线路带宽设定
基于应用的流控管道	支持基于源 IP 地址、目的 IP 地址、应用、服务端口和时间的流控管道定义
多层管道嵌套	支持四层管道嵌套，每层最多 64 个管道，每个流量控制线路最多 2048 个管道嵌套
带宽控制	可设定每个流控管道的最大上行带宽、最大下行带宽、每用户上行带宽、每用户下行带宽
带宽保障	可设定每个流控管道的上行保障带宽和下行保障带宽
优先级	支持管道优先级设定
流量整形	支持自动流量整形
vsys 多实例虚拟化	每台设备支持最多 8 个 vsys 虚拟防火墙，每台虚拟防火墙创建可限制新建、并发、吞吐、防火墙策略数量、NAT 数量、对象数量等关键参数。
	不同 vsys 之间基于标准 vrf 虚拟路由的路由隔离，并支持 bgp、ospf 等路由协议的路由隔离；同时 vrf 虚拟路由器可单独配置。
	vsys 采用单独的用户管理以及完整的三权机制
	vsys 支持路由、桥模式组网，并支持单独的 NAT 策略；并支持 vsys 之间串行流量组网。
	每个 vsys 包含独立的安全业务配置，包括防火墙策略、病毒防护、入侵防护策略
	每个 vsys 包含独立的日志系统，可独立记录相关的系统日志和业务日志
	每个 vsys 包含独立的监控页面，可以单独监控接口流量，cpu 内存占用、新建并发等曲线
双机热备	支持主-主和主-备模式
备机可管理	备机可通过配置带外管理 IP 进行管理
VRRP 协议	支持标准的 VRRP 协议
HA 切换条件及逻辑	支持基于心跳信号丢失、链路断开、远端服务不可达等多种方式的 HA 切换条件及逻辑
连接会话同步	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

设置抢占优先级	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
威胁可视化	指定时间段内（实时/最近 1 小时/1 天/7 天/30 天），防火墙处理的各类威胁事件的详细统计展示，包括基于威胁级别分类展示、基于中国地图/世界地图的攻击源和目标展示、威胁主机 TOP10、威胁事件 TOP10 等
应用流量可视化	指定时间段内（实时/最近 1 小时/1 天/7 天/30 天），防火墙处理的 TOP100 应用及 20 个应用大类的详细流量统计图，包括应用/应用类总体流量展示、应用/应用类总体并发数量展示、每应用/应用类的用户流量分布、每应用/应用类的用户会话分布
用户流量可视化	指定时间段内（实时/最近 1 小时/1 天/7 天/30 天），防火墙处理的 TOP100 用户的详细流量统计图，包括用户总体流量展示、用户总体并发数量展示、每用户的应用流量分布、每用户的应用会话分布
接口流量展示	指定时间段内（实时/最近 1 小时/1 天/7 天/30 天）基于物理接口、VLAN 接口、聚合链路接口的流量展示
系统运行信息	指定时间段内（实时/最近 1 小时/1 天/7 天/30 天），系统总流量、CPU 使用率，内存使用率，设备温度、总连接数，每秒新建连接数的统计图表
本地日志	支持各类日志的本地存储，本地日志支持导出功能
流日志	支持流日志记录，将一条流生命周期内的多个业务模块的操作记录在一条日志中
远程 Syslog 日志	支持，并支持多 Syslog 服务器
审计日志	audit 用户可进行配置日志审计。所有业务配置，都会体现为添加、删除、任意参数修改的形式。
日志级别	分为七级别，用户可以根据级别和日志来源过滤日志的记录或者远程发送
报表	报表内容包括：网络及安全风险概况、网络流量详情、应用统计及风险详情、URL 活动及风险详情、用户统计详情、网络风险威胁详情、威胁说明。
	支持报表模板的裁剪；支持报表自动周期任务：1 天/7 天/30 天
	支持历史报表的汇总展示，导入导出
	支持报表的全局参数配置，包括磁盘占用、自定义封面等
邮件报警	支持，可自行定义在特定日志情况下触发邮件报警
地址对象	支持地址对象，支持将 ISP 地址段设置为地址对象，在地址对象中支持地址/地址段排除。支持域名地址对象主动、被动学习，用户可直接模糊或精确配置域名，系统自动学习提取及对应的 IP 地址
地址对象导入导出	支持地址对象的导入导出，管理员可将地址对象导出为 Excel 文件进行编辑和备份
ISP 地址库	系统内置中国各大运营商 IP 地址库及全球地址库
自定义应用	支持用户自定义应用，实现内网生产业务的可视化呈现
集中管理	支持防火墙集中管理，包括统一状态监控、配置下发、配置自动备份及回滚、版本统一升级、特征库统一升级等功能。
Web 管理界面（HTTP/HTTPS）	支持，支持中文及英文 WEB 界面
命令行管理界面 Console	支持，所有功能均可通过命令行实现，支持 TELNET、SSH 及串口方式进行命令行管理
SNMP	支持 SNMP V1/V2/V3
管理员登录	支持基于本地帐号、Radius、LDAP 的管理员登录认证，支持设定每个管理员帐号的可登录 IP 范围

管理员权限分级	默认提供配置管理员、用户管理员及审计管理员三种用户角色，用户可以通过自行定义管理员角色，生成具有不同权限的管理员
NTP 时间同步	支持从自定义服务器或互联网 NTP 服务器同步系统时间，支持 NTP 认证，支持 NTP 服务器备份
系统配置的备份和恢复	支持，配置文件格式为文本格式
支持本地多配置文件	可按照日、周、月定期备份配置，并从任意配置恢复。
系统资源异常使用监控	支持系统资源异常使用监控，并以文件形式保存在设备本地，并支持导出
网络调试	支持基于 WEB 界面的网络调试功能，支持 PING、TRACEROUTE、TCP 探测方式
自定义抓包	支持基于 WEB 界面的自定义抓包功能

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：
400-877-3227
公司网址：www.ikuai8.com

访问官方网站