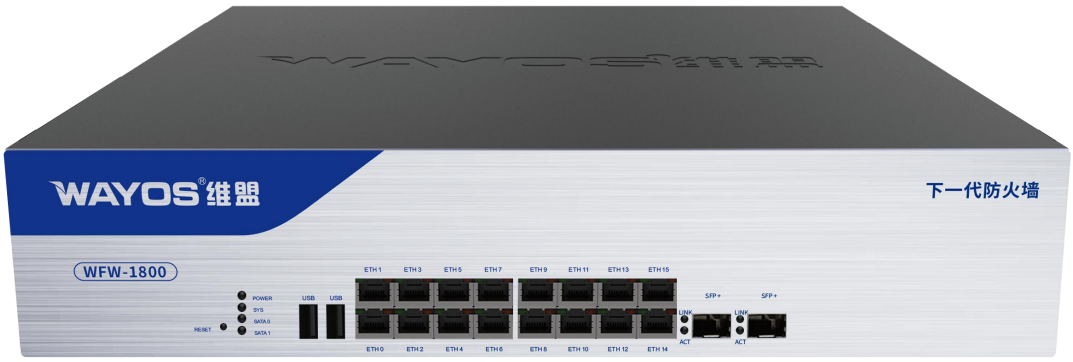
下一代融合型防火墙 WFW-1800

一、 产品简介

WFW 系列产品是深圳维盟科技专为企业和运营商客户设计的网络安全产品，通过将路由器和防火墙无缝融合于同一个硬件平台，实现强大的智能组网功能、组网安全防御功能、专业的 VPN 功能等多种特色功能，不但能为用户提供广泛和深入的安全防护和安全连接功能，同时可以降低与安全相关的总体设备成本以及部署的复杂程度，是网络安全解决方案的理想选择。

WFW-1800 下一代融合型防火墙是深圳维盟能科技面向中大型企业客户开发的新一代企业级防火墙设备。WFW-1800 采用了全新的硬件平台和体系架构，实现路由器和防火墙性能的跨越式突破，可支持 16 个 GE（千兆网口）接口和 2 个 SFP 万兆光口，能满足中大型企业级别应用的需求。

WFW-1800 下一代融合型防火墙可提供强大的路由能力，支持网桥、路由，以及网桥和路由混合模式等方式部署网络，支持多种用户认证方式；支持多线路接入及策略路由功能，SFP 光口理论吞吐量可达 9.6Gbps；支持丰富的 QoS 特性。支持深度应用识别，提供基于用户和应用的控制策略，以及 L2-L7 层的安全防护；支持外部攻击防范、内网安全、流量监控、邮件过滤、网页过滤、应用层过滤等功能，能够有效的保证网络的安全；提供多种智能分析和管理手段，支持邮件告警，支持多种日志，提供网络管理监控，协助网络管理员完成网络的安全管理；支持多种 VPN 业务，如 PPTP VPN 、IPSec VPN、L2TP VPN 等，可以构建多种形式的 VPN；满足公安网监 82、83 号令安全要求，支持对接公安网监审计系统等多种维盟特色功能。



WFW-1800 下一代融合型防火墙

二、 特色功能

全新的平台架构

WFW-1800下一代融合型防火墙采用企业级硬件平台，通过多内核、高主频系统实现企业用户对安全设备线性处理能力的需求。

高端的硬件架构，高速稳定的性能

WFW 系列融合型防火墙采用业界领先的电信级网络处理器，具有 2.0GHz 高主频，同时配备高速的 4GB DDR4 内存，结合 Wayos 独有的硬件加速技术，快速识别应用层协议并执行迅速有效的应用调度，能将吞吐量及带机量提高数倍。宽频电信级电源设计，采用电信级的开关电源，具有防雷设计、防过压设计、防浪涌设计，电压可适应 100～265V 大范围，保证在不良自然天气及电压不稳环境下网络的正常运行。

支持多 WAN 接入和智能选路

多线路负载均衡和线路备份，最大化优化网络，保障线路的畅通，满足电信、网通、联通等多家网络服务商的接入。实现“电信流量走电信线路，联通流量走联通线路”对于同一 ISP 多条线路，可以

实现线路叠加，即将流量均衡分配到各条线路；对于线路带宽不一样的多条 ISP 线路而言，可以通过权重模式将流量分配到合适的线路以充分利用多条线路的带宽。同时系统支持自动更新运营商 IP 地址库信息，以保障各 ISP 之间智能选路的准确性。

独特的进程管理技术

维盟全球首推的进程管理功能，主要应用于电信网通双线或者多条 PPPOE 线路，多用于企业、小区等环境。

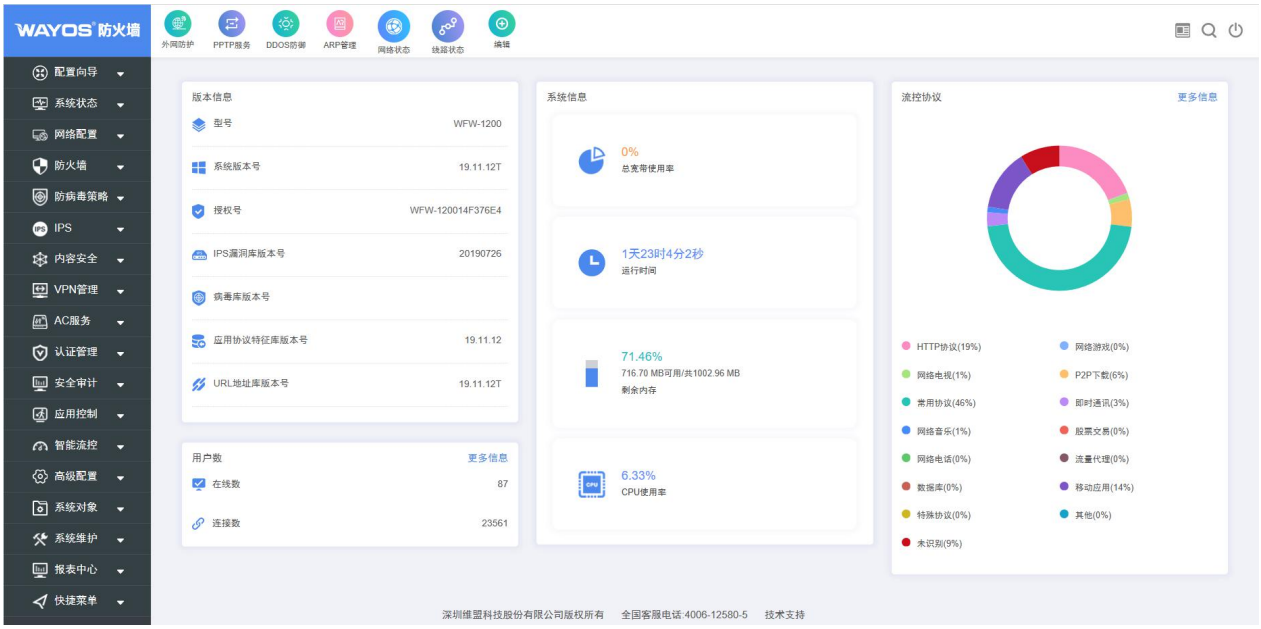
1、可以根据电脑进程或安装程序目录进行分配,将指定的程序（网页、P2P 程序）等所有流量分配到指定的线路。保证指定程序的正常运行。众所周知,即时通信工具其实对带宽需求并不大,其上传下载只有 30-100K 而已。但是通信环境要求稳定。而利用进程策略功能可以将即时通信工具的进程都分配到其中 1 条稳定的线路上,保证通信稳定的同时,节省带宽,节约成本,提高竞争力。

2、可对客户机每台电脑的每个进程进行速度限制,有效管理好网络中的每个进程,节省带宽资源的同时保证网络高速流畅。

3、可通过访问控制规则有效控制局域网内每个进程对网络的访问,随时禁止局域网内任何应用程序，企业不再担心 P2P 占用大量带宽,不为员工上班炒股、逛淘宝而烦恼。

可视化的设备状态

设备状态页面包含了设备版本信息、系统信息、实时网络流量百分比、系统运行状态等多项内容。



防火墙

防火墙包括安全策略、NAT 规则、DOS/DDOS 防护、ARP 欺骗防护、应用层网关、加速老化等六部分

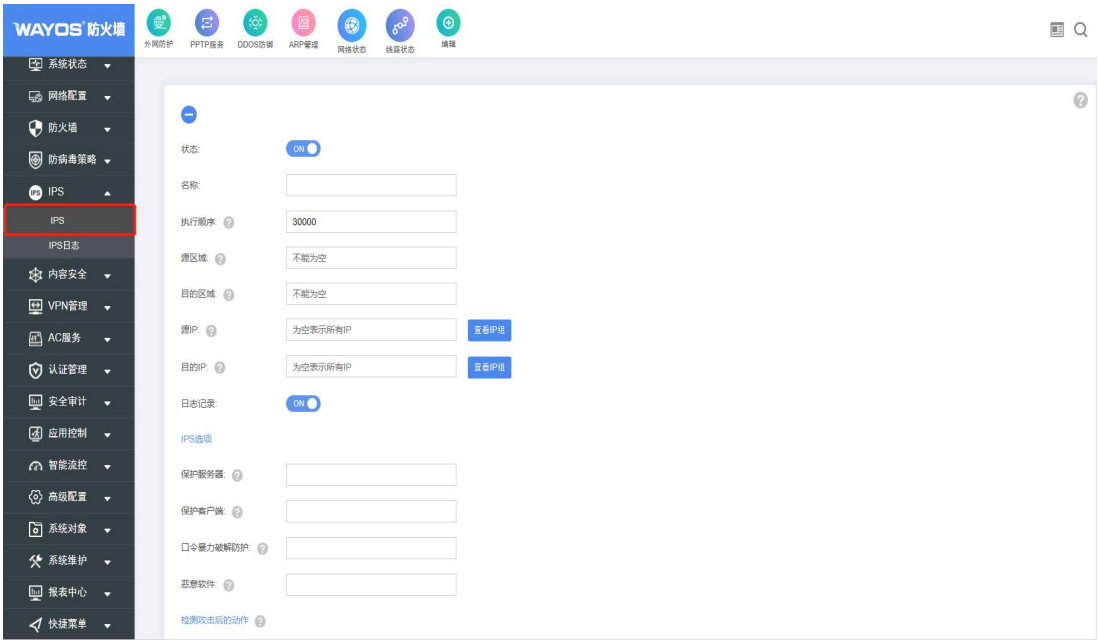
内容安全

内容安全包括应用控制策略、应用内容过滤、防病毒策略三部分。

- 应用控制策略根据报文的源地址、目的地址、服务类型、时间段等参数组合成各种流量，可对这些流量进行阻断或放通，
- 应用内容过滤用于设置内网用户的上网策略，上网策略对象可以同时被多个用户组或用户引用，从而对内网用户进行上网行为的控制。应用内容过滤包括：URL 过滤、关键字过滤、文件传输过滤、邮件过滤、SSL 管理。每个策略对象可以同时设置这 5 部分的内容。
- 防病毒策略针对 HTTP 协议进行杀毒，来保护经过设备数据的安全。一般用于保护内网用户不被病毒入侵。

IPS

入侵防御系统（Intrusion Prevention System）依靠对数据包的检测来发现对内网系统的潜在威胁。IPS 将检查入网的数据包，确定这种数据包的真正用途，然后根据用户配置决定是否允许这种数据包进入目标区域网络。



VPN

支持多种 VPN 业务，如 PPTP VPN 、IPSec VPN、L2TP VPN 等，可以构建多种形式的 VPN

用户认证

支持 Web 认证 portal 方式、Radius 认证等多种用户认证方式，支持所有无线 WiFi 接入终端，采用 Web 认证 portal 方式，引导用户到达商家定制的窗口（商家主页、品牌形象、优惠折扣、商品信息等），并可针对不同智能终端分类推送不同页面认证内容。各用户可以通过手机短信获取验证码等方式认证上网。并结合智慧 WiFi 云

平台，可实现认证信息链接分享、商家账号关注、短信消息推送等多种微营销方式，对商家主页、品牌形象进行宣传、推广。

流量控制

“流量管理”包括线路带宽配置、策略流控、用户流控、黑名单策略、白名单策略。

- 线路带宽配置：用于限制出口(WAN口)线路的总带宽，如限制 WAN1 口为 100M、WAN2口为 300M。
- 策略流控：根据报文的源地址、目的地址、服务类型、时间段等参数组合成各种流量，可对这些流量提供最大带宽限制、保障带宽、预留带宽的功能。
- 基于用户的流控：对单个主机进行带宽限制、会话控制、分类服务限制以及分时段管理。
- 黑名单策略：对超量使用网络资源(流量、带宽、会话)的用户加入黑名单，并进行惩罚。
- 白名单策略：对源地址加入白名单的用户包含的流量全部放行，不受任何策略的控制，也不被审计。

系统对象

系统对象包括 IP 组、IPS 漏洞库、病毒库和 URL 库。

- IP 组用于定义一个包含某些 IP 地址的 IP 地址组，这个 IP 组可以是任意的一个 IP、一段 IP 或者 IP 范围的任意组合。
- IPS 漏洞库包括内置和自定义的 IPS 漏洞库。IPS 漏洞库用于 IPS（入侵防御系统）策略的安全监测。
- 病毒库包括内置和自定义的病毒库。病毒库用于防火墙监测病毒的攻击行为特征，用于防病毒策略的安全监测。

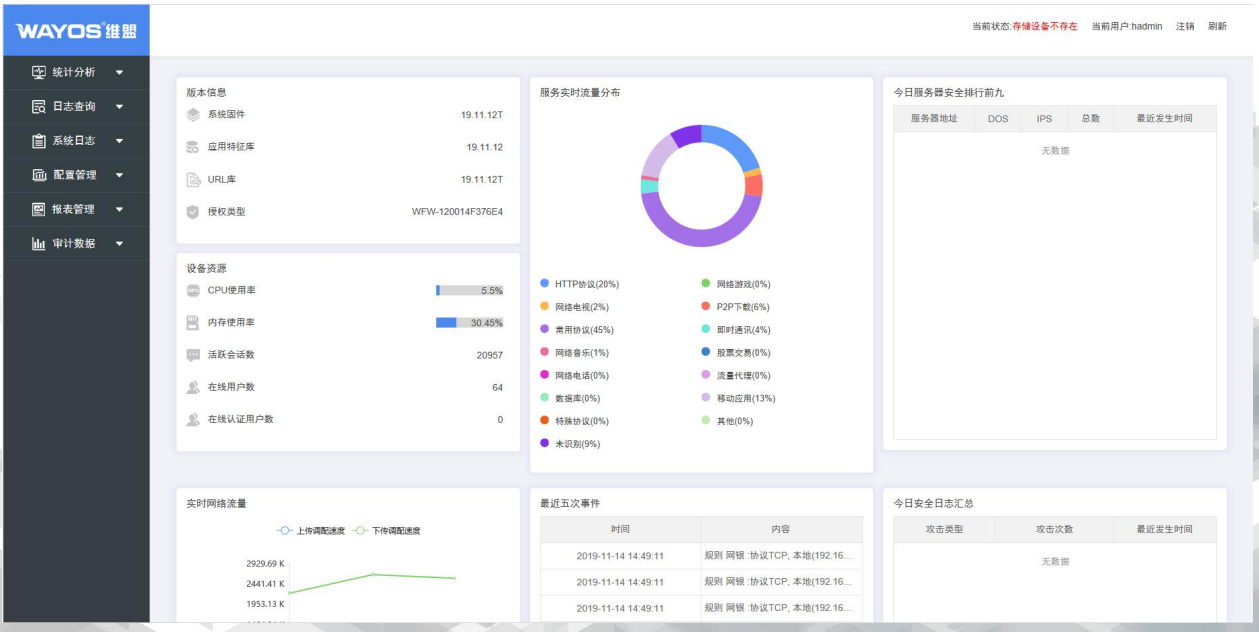
- URL 库包括内置和自定义的 URL 库。URL 库可用于安全策略、应用内容过滤、应用控制策略等，实现对 URL 的过滤。

公安网监设计对接

根据中华人民共和国公安部令第 82 号第 5、6、7、8、9、10、11、12 条之相关规定，公共上网服务场所的网络设备必须具有符合公共安全行业技术标准的互联网接口，并且有上网用户的注册、认证、浏览内容等信息的识别和记录留存功能。WFW-1800 下一代融合型防火墙满足公安网监 82 号令中的安全级别，支持对接公安网监审计系统，全面保障上网安全。同时拥有超强的行为管理功能、智能流量控制、网络防护稳定、多 WAN 接入、支持内网防护、支持智慧 WIFI 营销功能和满足公安网监 82 号令安全级别要求，支持对接公安网监审计系统。

报表中心

报表中心包含了设备版本信息、设备资源、实时网络流量、服务实时流量分布、最近五次事件、今日服务器安全排行前九、今日安全日志汇总等七项内容，并可手动指定某一日志输出至 USB 存储设备。



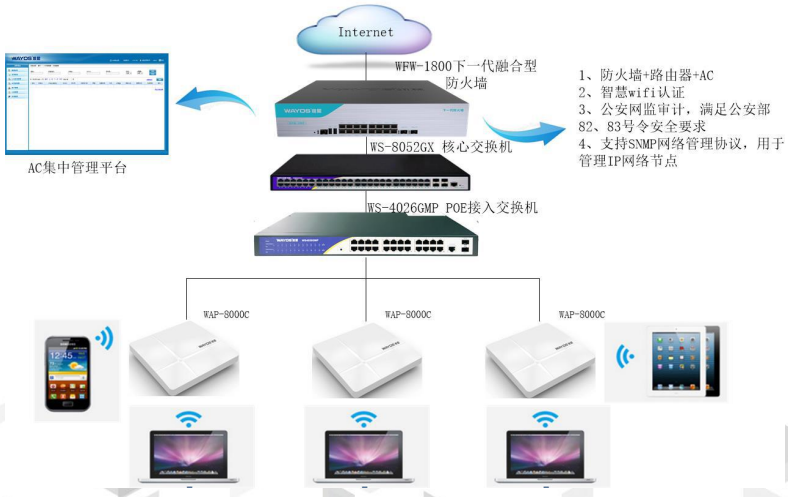
三、 产品参数

硬件规格	
DDR	DDR4 4GB
固态硬盘	内置 32GB，可单独选配 2.5 英寸机械硬盘
端口规格	
RJ45 电口数	16 个 10/100/1000Mbps 自适应电口
SPF 光口数	2 个 2.5G/10Gbps（万兆）光口
USB 接口	1* 3.0 USB，1* 2.0 USB
端口速率(PortRate)	RJ45 电口：10/100/1000Mbps 自适应 SFP 光口：2.5G/10Gbps 自适应
机器规格	
机壳	2U+铝面板
外形尺寸	19 寸
运行环境	
工作温度	0° C～40° C
存储温度	-40° C～70° C
工作湿度	10%到 95% RH 无凝结
存储湿度	5%到 95% RH 无凝结
软件规格	
带机量	400-500 用户
多 WAN、多运营商同时接入	支持
智能 QOS、流控模块、应用协议精准识别	支持
进程管理	支持
上网行为管理	支持
DHCP 服务器（支持分配多个网段 IP）	支持
多子网段	支持
负载均衡	支持
智慧 WiFi	支持
PPPoE 服务器	支持
WEB 认证	支持
Radius 认证	支持
PPTP 服务	支持
IPSec	支持
L2TP IPSec	支持
RADIUS 认证	支持
Portal 认证	支持

PPPOE 认证	支持
MAC 地址过滤	支持
基于协议的访问控制列表	支持
基于接口的访问控制列表	支持
基于时间的访问控制列表	支持
基于对象的访问控制列表	支持
抗攻击特性	支持 Land、Smurf、Fraggle、WinNuke、Ping of Death、Tear Drop、IP Spoofing、CC、 SYN Flood、ICMP Flood、UDP Flood、DNS Query Flood
ARP 欺骗攻击防御	支持
DoS/DDoS 攻击防御	支持
静态和动态黑名单功能	支持
ARP 绑定功能	支持
802.1q VLAN	支持
防病毒攻击策略	支持
IPS 入侵防御监测	支持
邮件过滤	支持
HTTP URL 过滤	支持
HTTP 关键字过滤	支持
URL 重定向管理	支持
应用层过滤	支持
用户行为管理日志	支持
流量攻击实时日志	支持
ARP 日志	支持
DDOS 日志	支持
PPPOE 认证日志	支持
访问控制日志	支持
策略路由日志	支持
URL 重定向日志	支持
应用控制日志	支持
流量统计和分析功能	支持
全局/基于安全域连接数率监控	支持
全局/基于安全域协议报文比例监控	支持
安全事件统计功能	支持

多个内部地址映射到同一个公网地址	支持
多个内部地址映射到多个公网地址	支持
内部地址到公网地址一一映射	支持
源地址和目的地址同时转换	支持
ESP 支持 DES、3DES、AES 多种加密算法	支持
支持 MD5 及 SHA-1 验证算法	支持
支持 IKE 主模式及野蛮模式	支持
账号分级保护，确保未授权用户无法侵入设备	支持
设备登录及操作日志记录	支持
提供网络测试工具，如 Tracert、Ping 命令等，迅速诊断网络是否正常	支持
支持标准网管 SNMPv3，并且兼容 SNMP v2c、SNMP v1	支持
支持 NTP 时间同步	支持
支持 Web 方式进行远程配置管理	支持

四、 经典组网方案



联系方式

地址：深圳市龙华区观湖街道观城社区环观南路 101 号凯美广场 5 层 A505

邮编：518109

电话：4006-12580-5

周一至周日：09:00-22:00