WFW-3000 下一代防火墙手册

深圳维盟科技股份有限公司

版权声明

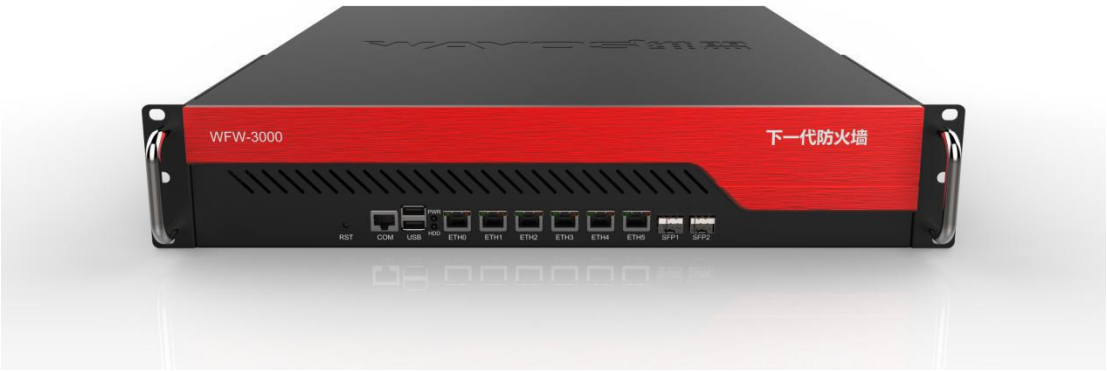
免责声明

本手册内容依据现有信息制作，由于产品版本升级或其他原因，其内容有可能变更。维盟科技保留在没有任何通知或者提示的情况下对手册内容进行修改的权利。

本手册仅作为使用指导，维盟科技在编写本手册时已尽力保证其内容准确可靠，但并不确保手册内容完全没有错误或遗漏，本手册中的所有信息也不构成任何明示或暗示的担保。

一、产品介绍

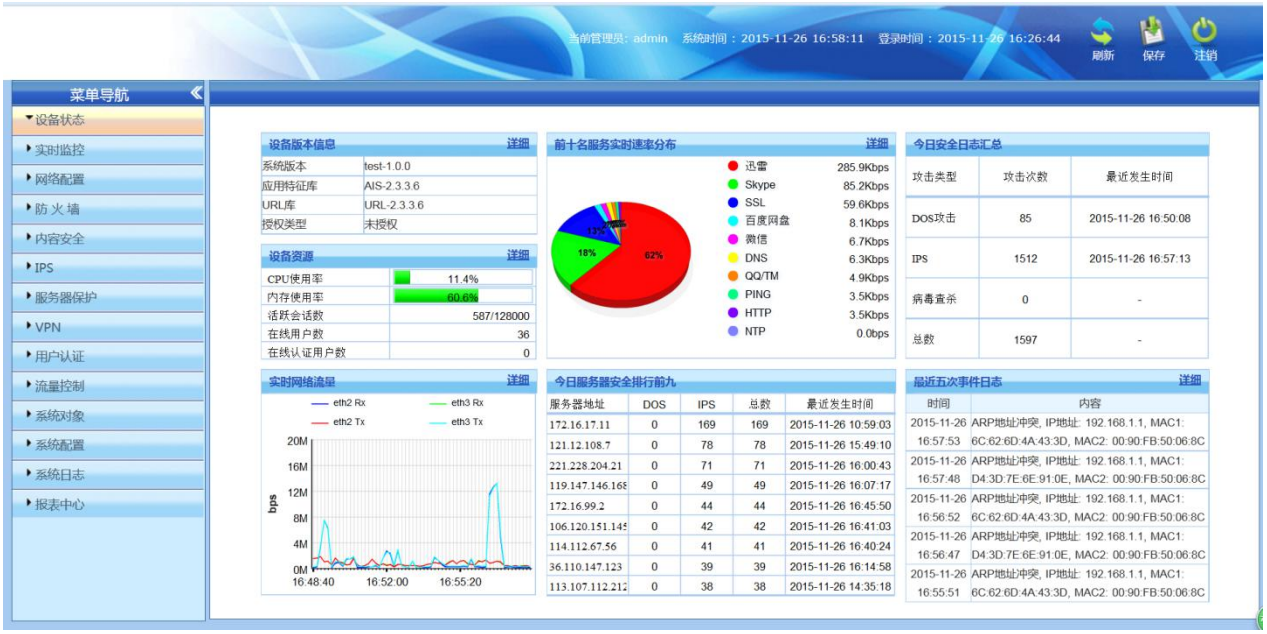
WFW-3000 下一代防火墙支持网桥，路由，旁路，以及网桥和路由混合模式等方式部署网络，支持多种用户认证方式，深度的应用识别，提供基于用户和应用的控制策略，以及 L2-L7 的安全防护，同时支持 PPTP,L2TP,IPsec ，ssl VPN，可视化的用户，流量，安全统计和监控，是一款可以全面应对应用层威胁的高性能防火墙。通过深入洞察网络流量中的用户、应用和内容，能够为用户提供有效的应用层一体化安全防护，帮助用户安全地开展业务并简化用户的网络安全架构。



二、产品特性

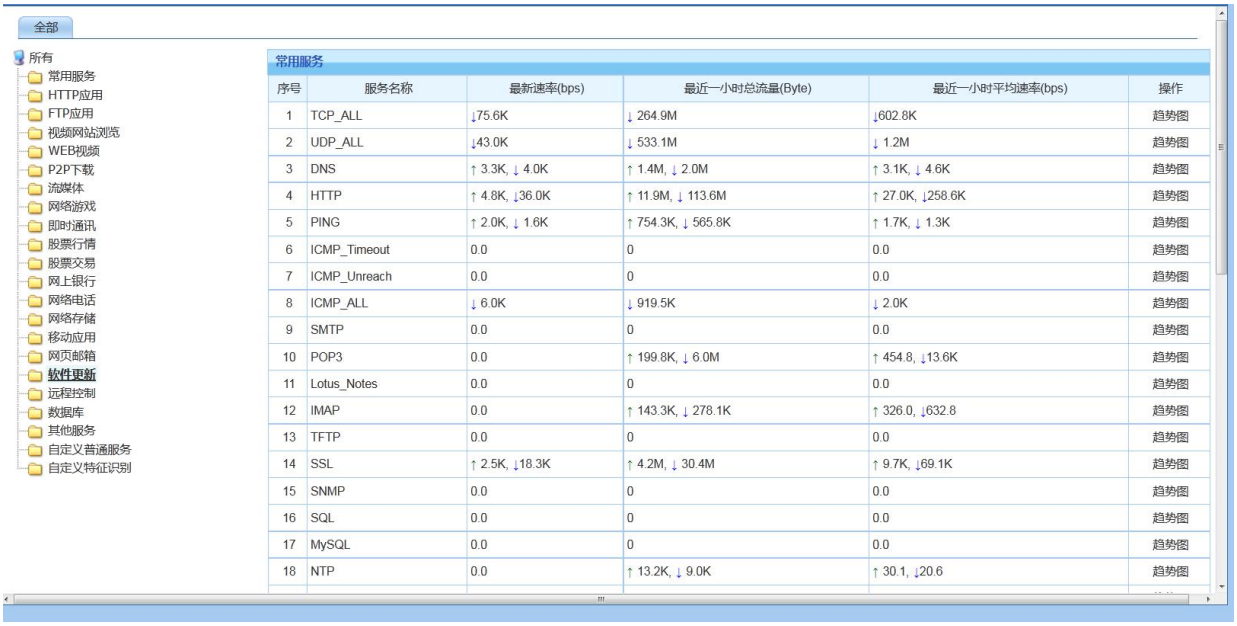
■ 可视化的设备状态

➢ 设备状态页面包含了设备版本信息、设备资源、实时网络流量、前十名服务实时速率分布、今日服务器安全排行前九、今日安全日志汇总、最近五次事件日志等七项内容。



■ 实时监控

➢查看设备实时的工作状态，包括设备资源、物理接口、服务监控、用户监控、在线用户、防共享上网、当前黑名单七大部分。



■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、FTP、POP3 和 SMTP 这四种常用协议进行杀毒，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。

IPS　　新增　修改状态　删除全部　计数清零

序号	名称	源区域	源IP	目的区域	目的IP	漏洞列表	匹配计数	状态	操作
1	保护客户端	三层内网	全部	三层外网	全部	保护客户端 Application漏洞攻击...	0	☑	修改 上移 下移 移动 删除
2	保护服务器	三层内网	全部	三层外网	全部	保护服务器 Scan漏洞攻击...	0	☑	修改 上移 下移 移动 删除
3	口令暴力破解防护	三层内网 三层外网	全部	三层内网 三层外网	全部	口令暴力破解防护 FTP...	0	☑	修改 上移 下移 移动 删除
4	防恶意软件攻击	三层内网	全部	三层外网	全部	恶意软件 Backdoor漏洞攻击...	0	☑	修改 上移 下移 移动 删除

■ 服务器保护

➢ WEB 应用防护，专门用于保护内网的 WEB 服务器，可以有效防止跨站请求伪造、SQL 注入、XSS 攻击、会话劫持、目录遍历等各种针对 WEB 应用的攻击行为。

■ VPN

➢ 支持 PPTP,L2TP,SSL VPN

■ 用户认证

➢ “用户认证”包括认证策略、组织结构、认证选项、认证服务器、组织管理、临时账号设置等六部分。

➢ 支持短信认证，认证服务器认证包括RADIUS服务器、AD服务器、LDAP服务器。

■ 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、网络服务、时间计划、URL 库、关键字、文件类型等。

➢ 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。

➢ 网络服务共分为：自定义普通服务、自定义特征识别、内置服务。内置服务包含常用服务、HTTP 服务、FTP 应用、视频网站浏览、WEB 视频、P2P 下载、流媒体、网络游戏、即时通信和其他服务等。

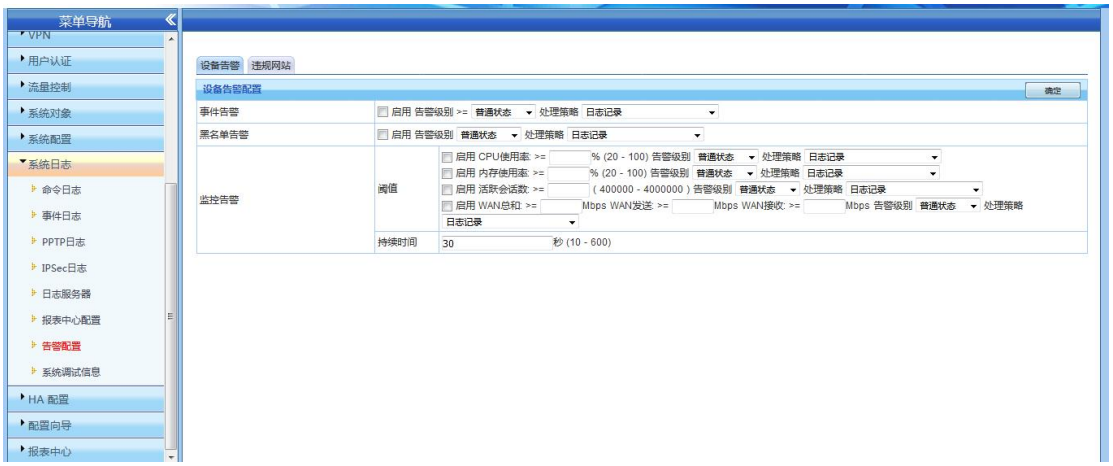
➢ 时间计划用于定义时间段，然后可在【网络配置>策略路由】、【防火墙>安全策略】、【内容安全】、【流量控制】等中引用，以控制这些策略生效或失效的时间，从而可对各种

策略分时间段管理。

- URL 库包括内置和自定义的 URL 库。URL 库可用于【防火墙>安全策略】、【内容安全>应用内容过滤】和【内容安全>应用控制策略】，实现对 URL 的过滤。
- 关键字用于设置关键字，并把关键字分组，这些关键字组可用于【内容安全>应用内容过滤>关键字过滤】中限制某些关键字的搜索和上传。
- 文件类型用于定义文件类型，并把文件类型分组。这些文件类型可用于【内容安全>应用内容过滤>文件输过滤】中限制这些类型的文件的上传和下载。

■ 系统日志

- “系统日志”包含：命令日志、事件日志、PPTP 日志、IPSEC 日志、日志服务器、告警配置、系统调试信息。



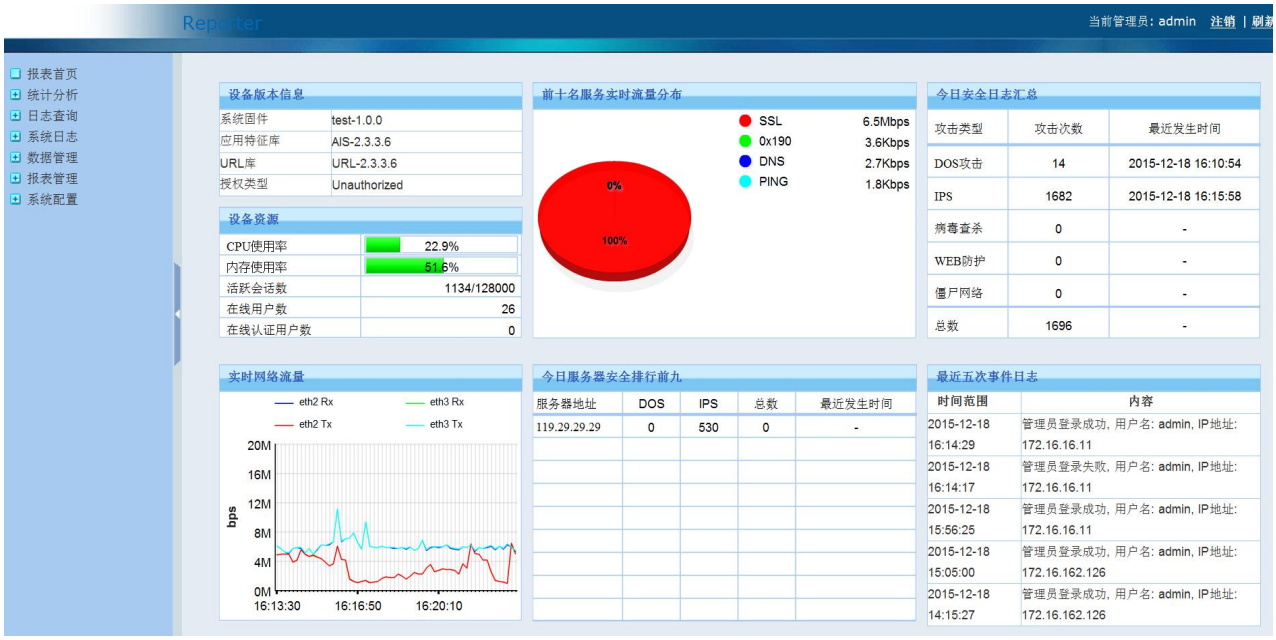
■ HA 配置

HA 配置包括基本信息、双机热备、配置同步三部分。支持主/备、主/主两种模式，主要是在防火墙双机工作，或者两台设备并行工作等场景使用。

- 基本信息用于设置本机的地址与对端地址。本机地址只能选择配置里带有 HA 标识的接口。并且该接口只能与做负载均衡的其他防火墙 设备接口通信，用于收发心跳包信息、交互配置信息等。
- 双机热备用于设置 HA 主/备选举、链路监控、接口监控的相关参数，实现负载均衡和备份的功能。
- 配置同步用于将主设备上除心跳口、业务口、管理口外的配置全部同步到备机上，以免主备切换后，影响其他业务。

■ 报表中心

➢报表中心包括日志审计策略和内置报表中心两部分。其中设备提供的内置报表中心，无需另外安装外置报表中心即可实现对实时监控、统计分析、行为分析的记录与查询功能。在内置报表中心，默认已开启对流量的实时监控、统计分析，应用内容过滤等所有的记录。



三、 产品参数

详细规格	
硬件规格	
DDR	DDR3 8GB (1600)
固态硬盘	8GB
端口规格	
RJ45 电口数	6
USB 接口	2 * 2.0 USB
端口速率(PortRate)	1000Mbps
机壳	2U+铝面板（430 宽*480 深*88 高）
性能指标	
最大并发连接数	4M(400W)
新建会话数率	20000
WAN=>LAN 最大吞吐量	5G
防病毒	820.0M
IPS	950.3M
WAF	160M
防病毒+IPS+WAF	145M
最大用户数	2000
适用网络层吞吐量	1G