

**IP-COM**

无线网络解决方案专家

# FW300

## 下一代融合型防火墙

# FW300

## 下一代融合型防火墙

---

### 产品简介

IP-COM下一代防火墙(简称:NGAF)提供L2-L7层安全可视的全面防护,通过双向检测网络流量,有效识别来自网络层和应用层的风险,提供比同时部署传统防火墙、IPS和WAF等多种安全设备更强的安全防护能力,可以抵御来源更广泛、操作更简便、危害更明显的应用层攻击。此外,NGAF还提供基于业务的风险报表,内容丰富直观,用户可实时了解网络和业务系统的安全状况,有效提升管理效率、降低运维成本。



## 产品特征

- intel X86 2.0GHz处理器, 建议最大带机量1000人
- 6\*10\100\1000Mbps网口, 2\*USB接口, 1\*Console接口
- 数千种主流应用识别, 精细的应用层管控及安全防护
- 融合了漏洞防护、Web 安全防护等多种安全技术
- 基于线路、应用、用户、时间的精细化带宽管理
- 数万种流量异常特征库, 全面的IPS漏洞防护
- 百万级病毒库定期更新, 基于流引擎的网络病毒防护
- 支持透明模式、路由模式、旁路模式、混杂模式部署

## 核心优势



### 完备的基本防火墙特性

可同时抵御网络层和应用层攻击, 通过双向检测网络流量, 精确识别应用、用户、内容和威胁, 安全可视化的全面防护

基于应用协议识别的入侵防御功能, 提供针对漏洞、后门进行的木马、蠕虫、缓冲区溢出、扫描等入侵行为的检测和防御;

支持对常用协议流量和压缩文件的病毒进行查杀。



### 全方位应用洞察与控制

针对网络应用实现全面、精准、便捷的管控。拥有精准而全面的识别库, 可识别数千种应用特征和数千万条URL条目, 每2周更新一次;

实现“用户+应用+内容”的多维精细化的访问控制, 增强安全策略的有效性;

基于“用户+应用+时间”保障核心业务的带宽, 保障核心业务的运行, 限制非关键业务最大带宽, 避免网络拥塞, 高效利用带宽资源。



### APT攻击和僵尸网络检测

结合深度内容检测和攻击行为分析技术, 可更有效地检测和定位APT攻击;

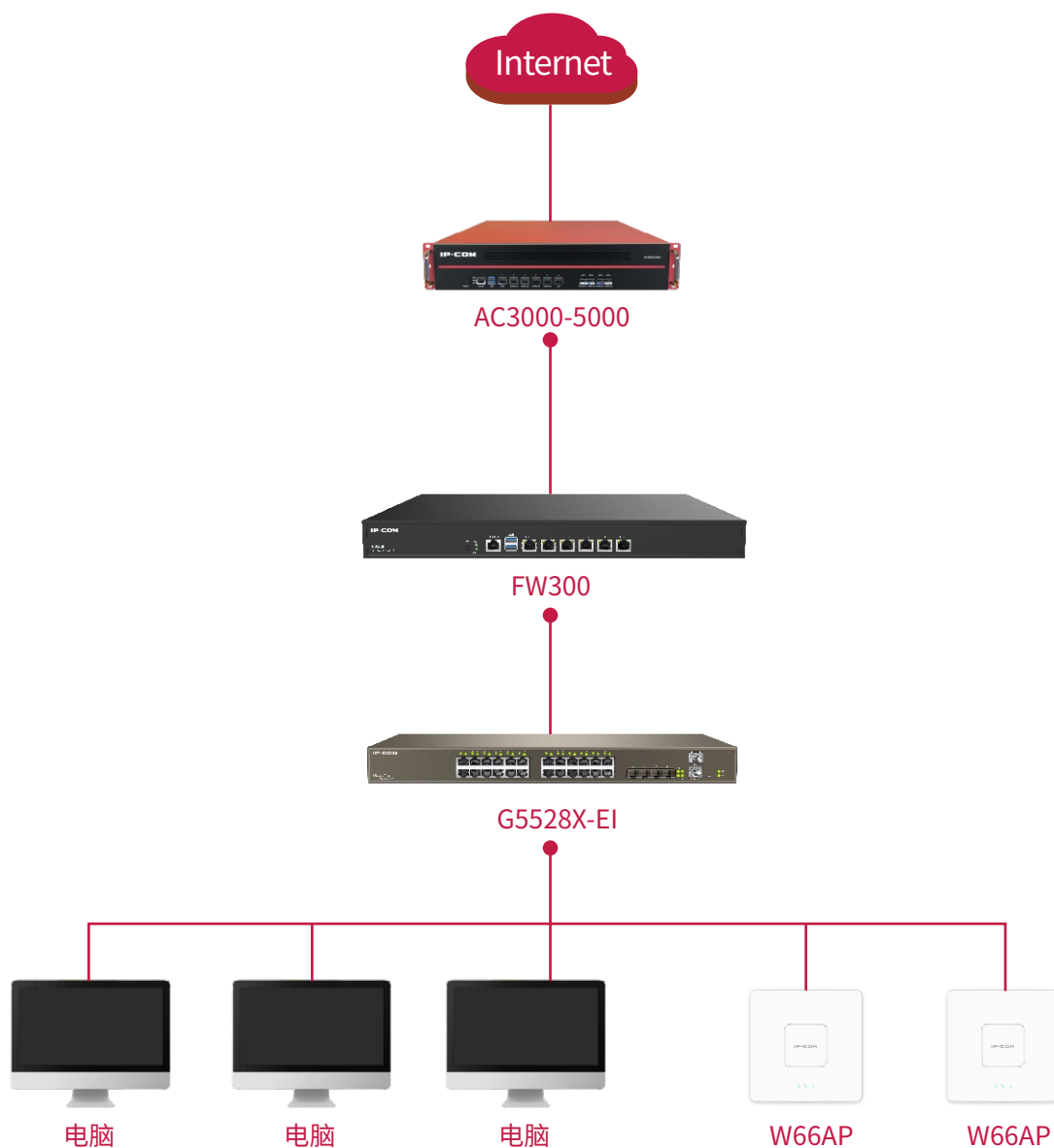
基于终端异常行为分析机制, 能快速发现僵尸网络并阻止攻击外发。



## 直观呈现业务系统安全风险

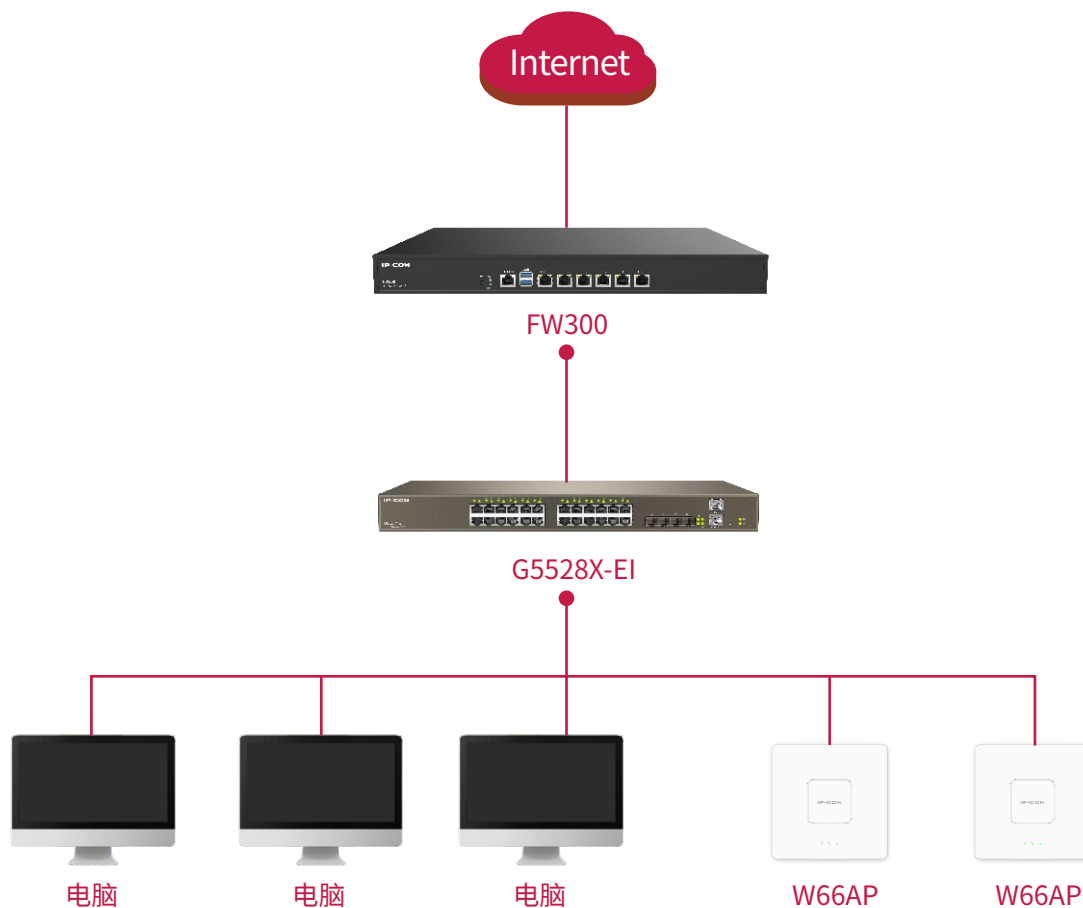
实时发现系统新增漏洞,并能直观呈现业务系统的漏洞及遭受的攻击,快速定位有效攻击,及时采取应急措施,有效提升管理效率,降低运维成本。

### 典型应用1



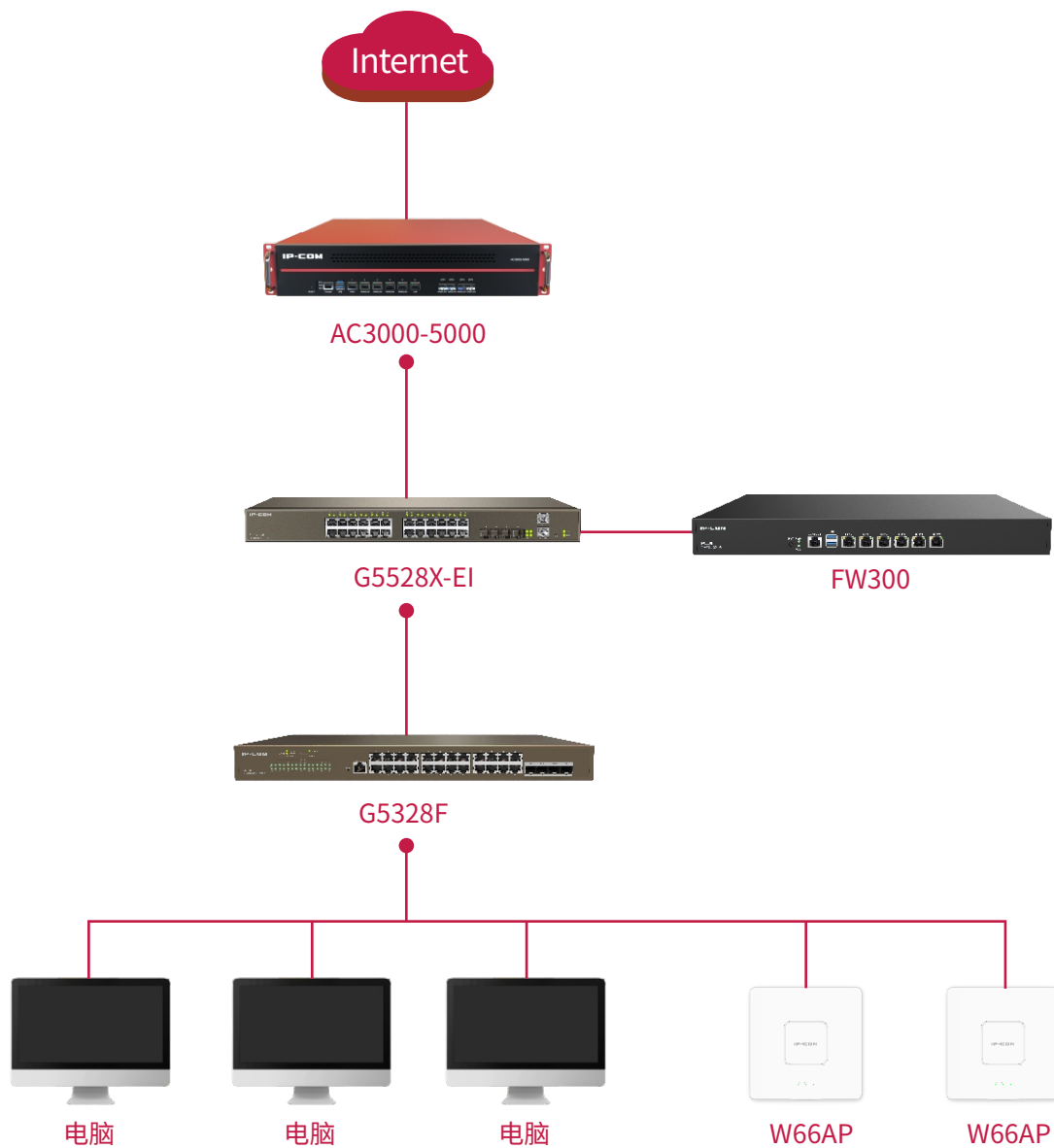
以透明网桥方式接入网络,可以部署到网络的网关位置或各部门的出口位置。无需改动用户网络结构和配置,即插即用,支持单网桥,多网桥的部署方式。

## 典型应用2



以路由模式将设备串接网络中,可以放于内网的任意子网边界,或与核心交换机相连。可以代替防火墙或路由器,需要为设备配置内网和外网接口的 IP 地址。

## 典型应用3



以透旁路方式接入网络,可对网络的流量进行全面的监控和记录,无需改动用户网络结构和配置。

## 产品规格

产品型号	FW300
硬件特性	
CPU	2.0GHz
接口参数	6*10\100\1000Mbps网口, 2*USB接口, 1*Console接口
Bypass	一对(ETH4&ETH5)
存储	32G
产品形态	1U
尺寸	宽 x 深 x 高:430 x 300 x 44.5mm
整机最大功耗	75W
电源输入	交流 90V-264V @47-63Hz
产品净重	4KG
工作温度	0°C ~ +50°C
工作湿度	10%~90%RH 不凝结
存储温度	-40°C ~ +70°C
存储湿度	5~95% RH, 不凝结
功能特性	
基础网络功能	支持基于IPV4/IPV6的联网和局域网设置功能。
策略路由	用于设备有多个外网口接多条外网线路时, 根据源/目的IP、源/目的端口、协议等条件进行出接口和线路选择, 以实现不同的数据走不同的外网线路的自动选路功能。
智能DNS	对于多IP的DNS解析, 根据用户的来路而做出一些智能化的处理, 然后把智能化判断后的IP返回给用户, 而不需要用户进行选择。
NAT规则	支持基于IPV4/IPV6的源地址转换、目的地址转换、双向地址转换。为简化配置, 端口映射功能已经包含双向地址转换功能, 配置和目的地址转换一样。

路由特性	全面支持IPV4/IPV6下的多种路由协议,如静态路由、RIP、OSPF等。
基础防火墙功能	支持防火墙、安全策略、NAT 转换功能。
VPN 功能	支持 IPSec VPN、PPTP/L2TP VPN、SSL VPN。
IPS 入侵防御功能	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。通过对进入设备的数据包进行检测,来保护内网的安全。
DOS/DDOS 防护	DoS/DDoS防护分成外网防护和内网防护两个部分,既可以防止外网对内网的 DoS 攻击,也可以阻止内网的机器中毒或使用攻击工具发起的 DoS 攻击。
服务器防护	类似IP地址簿,用于定义需要防护的内部服务器流量。通过隐藏、过滤信息等手段来保护服务器安全。
病毒防护功能	百万级病毒库,基于流引擎查毒技术,支持对 HTTP、FTP、SMTP和 POP3等协议流量查杀。
应用内容过滤功能	支持海量 URL 库、URL 过滤、非标准端口 URL 管理、关键字过滤、HTTP 文件传输过滤、FTP 文件传输过滤、非标准端口 FTP 过滤、邮件过滤功能。
应用控制策略	支持基于视频流媒体、P2P 下载类、网络游戏、Webmail 邮箱类、软件更新、远程控制、数据库等网络应用的策略控制。 同时支持自定义特征库识别,可根据五元组,数据长度,数据报文特征字符串组合自定义特征。
流量控制	基于报文的源地址、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。
白名单功能	支持基于内网用户的白名单、基于外网 IP 地址白名单、基于时间段的控制白名单控制功能。
部署方式	支持路由模式、透明模式、旁路模式、混合模式。
自身安全防护	支持高可靠性(HA)、防 ARP 欺骗、会话加速老化功能。
故障与告警	支持设备事件日志告警、黑名单告警、CPU、内存、活跃会话数、入侵事件、攻击事件等告警; 支持自动邮件告警、自动短信告警; 支持设备故障、调试信息下载;



报表与统计	内置报表中心, 支持图形化日志统计工具、分层管理、报表生成。
日志功能	支持记录 DoS 攻击日志、IPS 日志、Web 应用防护日志、病毒查杀、网页 URL 日志、阻挡记录、会话记录、告警记录, 以及对日志信息的高级检索。
数据管理	支持对于数据存储策略管理、数据列表查询; 支持数据删除和数据备份。
网管方式	支持Web UI 方式、CLI 方式管理。

**IP-COM**

无线网络解决方案专家

全国服务热线  
**400 665 0066**

深圳市和为顺网络技术有限公司  
IP-COM NETWORKS CO.,LTD.

深圳市南山区中山园路1001号国际E城E3栋  
E3 Bldg.Int'l E-City,#1001 Zhongshan yuan Rd.  
Nanshan District,Shenzhen China.