

## 海信 FW3010-5000A 防火墙技术说明

海信 FW3010-5000A 千兆防火墙采用独立的 FPGA 防火墙加速引擎，是真正千兆线速高端防火墙系统。具有独特的流处理和控制在能力。采用软硬一体化的设计系统安全可靠使用灵活，各项性能指标都达到了国际领先水平。抗攻击能力突出，特别增加了流量管理控制功能，可以出色的平衡安全/效率之间的矛盾，真正做到 2-7 层的全方位立体防护，同时采用大流量拥塞处理技术，保障突发数据量对网络的冲击，缓和“网络脉冲”。最大支持带宽达到 6.2G（1518 字节大包），最小处理能力 4.2G（64 字节），可以广泛适用于大型 ISP、IDC 和各种骨干网络中心。

体系结构	芯片级线速防火墙
并发连接数	最大并发连接数可达200万
千兆光纤/以太网可选	6个host10/100/1000M Base-T接口（普通接口） 支持4个SFP光接口+4个10/100/1000M Base-T接口（线速接口）
<b>新建连接数</b>	<b>系统采用FPGA加速处理每秒新建连接数可以达到30000条</b>
<b>包过滤</b>	<b>支持多达5万条过滤规则，各种大小数据包均达到千兆线速</b>
<b>延迟</b>	<b>各种大小数据包延迟约15us</b>
<b>可升级性</b>	<b>防火墙管理软件和防火墙核心系统都可通过网络升级，确保防火墙系统的最佳工作状态和最安全合理的系统性能。</b>
支持协议	防火墙支持流行的各种网络协议，如OSPF、MPLS、DHCP、VLAN、IPX、RIP、802.1Q、NETBEUI、PPTP、AppleTalk、H.323、BOOTP等，适用广泛的网络及应用环境。支持大多数网络通信协议和应用协议
知识产权	海信数码自主开发，拥有全部源代码
多级登录权限	四级管理权限，并且管理人员可以灵活组合，共有7种配置
灾难恢复机制	独有的灾难恢复机制，设有三层防护机制。当防火墙的部分文件系统由于武力或逻辑的原因遭到破坏的时候，系统会自动自我修复。确保防火墙仍然可以可靠的运行。（绝大部分产品在保存配置时突然断电会导致系统崩溃）
真正的千兆硬件平台	专门设计的带有通讯加速处理模块的硬件防火墙平台，系统与硬件紧密结合，发挥硬件最高效能，提高系统自身安全性
DMZ支持	使对外服务器拥有一个独立的、完全隔离的网段
认证方式（双因子）	口令、NetKey（USB接口）
数字证书支持	支持
路由管理	就是用防火墙来实现路由器的功能，配置相应的路由规则，将不同的网络连到一起的工作模式。可以建立多路由表，控制不同的数据源走不同的路由表。
高级路由管理	海信防火墙提供业界最灵活的高级路由管理能力，将网络管理变成网管

	人员的一种享受。海信防火墙的路由管理可以分为路由表和路由策略表两个共同作用的快速表，使得路由控制更加灵活（可根据源/目的IP或子网定义策略）。内部设定200个路由优先级，特别是适于大型网络的改造。
透明模式	即网桥模式，一般使用在网络结构比较复杂，网络改造比较困难的环境下
远程/集群管理	通过128位加密的SSL链路层和专门针对防火墙的定制管理程序可以对分布在海信防护墙进行统一的集群式管理，此外还支持远程得ssh管理
P2P协议过滤	可以根据策略控制类似电驴、BT之类的P2P通讯，保障网络资源的有效利用。 可以过滤的P2P应用有：eDonkey、eMule、Kademlia、BitTorrent、extended BT、WinMX、SoulSeek、Ares、AresLite、AppleJuice、Direct Connect、Gnutella、KaZaA、FastTrack!! 是目前最完善和最全的
抗IP欺骗	防火墙将接口控制策略加在相应的接口上，以防止其他接口区域的IP被此接口区域内的主机冒用
内容过滤	过滤Activex、Java、Javascript等恶意代码和管理员策略中指定内容代码
警告通知	声音、指示灯、E_mail
流量控制	两种流量控制方式：一、快速便捷的控制方式，可以精确控制单条规则数据包的吞吐量。 二、详细的流量控制规则。多达八个优先级的流量控制功能，可以根据不同的协议、源/目的端口和源/目的地址（段）、时间六元组的任意组合进行控制。
双机热备	两台防火墙通过串口连接，当工作机出现异常，不能支持网络系统运行时，备份机主动接管工作机的工作，继续支持系统的运行，从而保证网络能够不间断的提供服务
入侵监测	系统对受到的攻击设有完备的记录功能，检测到危险信息时，系统可以根据管理员的设置发出警告
日志管理与审计	记录详细、空间大。可远程记录，也可本地记录，还可以对日志占有系统资源的比例进行设定，超容即发出告警通知。而且提供日志备份
IP与MAC绑定	防止IP地址的伪造，防止内部地址被盗用和内部网络用户进行破坏网络的行为，使防火墙更为安全
ARP主动防御	可以主动防御ARP欺骗，任何针对防火墙的arp欺骗都可以在两秒钟之内自动恢复，使得内部恶意欺骗无法截获用户通过防火墙的通讯
黑名单控制	可以针对不同的网络接口配置不同的黑名单。
负载均衡	支持防火墙间的负载均衡和对内部服务器的负载均衡
计费功能	管理员可以根据用户使用防火墙的具体情况制定相应的计费规则，在防火墙管理系统中我们已经内置了一个计费公式
安全管理	管理员权限分为四级：超级管理员、系统管理员、安全策略员、日志审计员。权限既可分，又可集中。
管理主机锁定	为了防止未经许可的管理员对防火墙进行非法操作，当企图登录防火墙的用户输入用户名和密码时，如果出现一定次数错误，防火墙的锁定管理主机功能会自动将该用户帐号锁定，次数可以设定。对锁定的帐号可

	以通过超级管理员解除锁定，也可以等待系统自动解除锁定，锁定时间可以设置。
用户组策略控制	可以以组的形式管理整个网络用户，简化工作。还可以对一个组或一个组中的某个成员进行增删；有户组可以根据IP地址划分和可以根据MAC地址划分
系统备份、恢复	备份的范围是防火墙上所有的配置文件，包括网络接口的地址、安全策略的配置、计费规则的配置等
系统状态	提供“连接状态”、“ping”等功能，以便管理员及时，准确掌握防火墙的运行状态和测试网络连接之用
DoS攻击拦截	Ping of death,Tcp syn floods,Tear drop,Bomb fragment,Ip spoof,Udp floods等10类DoS攻击拦截。够防御源路由攻击、IP碎片包攻击、DNS/RIP/ICMP攻击、SYN等多种攻击。防火墙系统也能检测到对网络或内部主机的多种拒绝服务攻击。
端口扫描监控	当黑客扫描防火墙上任意接口的端口范围时，检测并阻止该行为
真正的全状态过滤	可以通过策略控制每一次连接的所有工作状态
时间策略控制	匹配规则的时间范围。如：设置不同用户的上网时间段等
IDS联动功能	可以和多种其他厂家 IDS 产品联动,建立以防火墙为核心的网络安全体系
特有模式	支持透明模式（双网桥）和 NAT 同时使用
字符串智能过滤	基于数据端口的字符串过滤；能够区别类似“性”与“性别”要求过滤的不同内容，并支持国旅 CC 攻击（网游行业常见）
灵活的内容过滤	对不同对象（用户名、IP 地址、目标 URL 等）的过滤可采用不同的策略
强大的邮件过滤功能	对不同的对象（邮件来源、接收邮件地址、邮件标题、邮件内容、附件、病毒）进行灵活的过滤，并且具有防止垃圾邮件的功能

智能URL拦截	可以过滤掉包含在合法网页（比如 google 搜索出来的网页）或邮件中的 URL 非法连接地址
VPN	支持 IPSEC/PPTP/MPLS/L2TP/SSL VPN 协议，提供端到端的安全隧道。