艾泰下一代增强级防火墙

FR2000	
FR2000 下一代增强级防火墙支持透明、路由、旁路、混合多种部署方式，支持多种用户认证方式、深度的应用识别、170 万+的 URL 库、内置入侵防御/检测系统、600 万+的病毒库，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 IPSec、SSL VPN，可视化的用户、流量、安全统计和监控；是一款专为高校、互联网企业出口的防火墙产品，建议带机量 500~1000 台。	

关键特性

网络适用性	支持多种部署方式，包括：透明、路由、旁路、混合
	提供固定的 5 个千兆接口，支持物理接口、网桥接口（支持透传）、VLAN 口（Trunk/Access）等
	支持接口 PPPoE 客户端、DHCP 客户端、静态 IP 配置，支持内外口属性设置
	支持端口聚合、支持静态/动态 LACP，支持轮询，基于源/目的 MAC，源/目的 IP 等 7 种聚合算法
	支持 DHCP 服务器和中继，支持排除 IP，支持 DHCP 状态监控
	支持静态路由、策略路由、动态路由 RIPv1/2、OSPFv2/v3、BGP4
	支持源 NAT、目的 NAT、静态 NAT、透明 NAT
防火墙基础	支持源/目的接口/安全域、源/目的 IP 地址、用户、服务、应用和时间的 8 元组防火墙策略
	支持源主机新建和连接数控制
	支持 IPv4/v6 抗应用型 DOS 攻击防护，如 HTTP Flood、DNS query flood 等攻击防护;支持抗流量型攻击防护，如 syn flood、udp flood、icmp flood，tcp flood 等攻击防护；抗常见 DOS 攻击防护，jolt2、land_base、ping_of_death syn flag、 tear_drop 、winnuke 、smurf、 ip spoof 等。
	支持基于 TCP、UDP 和 ICMP 的扫描防护，支持防火墙自身扫描防护
	支持限定主机或接入接口对本地服务的访问，如 DNS、https 等服务；支持协议连接管理
上网行为管理	支持应用识别、应用行为识别，支持桌面、Web 和移动端应用识别，支持应用数 1100+，支持海外应用库和本地应用库；支持特征库手动、自动和定期更新
	支持基于应用、行为、内容应用控制策略，可对 IM、流媒体、P2P、游戏、股票等应用、应用行为和内容进行控制并记录日志
	支持网页内容和关键字过滤，支持 URL 关键字过滤
	支持邮件主题、正文关键字、收件人、发件人的邮件过滤
上网行为审计	支持应用审计，包括账号、用户名、应用名称等审计（审计日志需搭配第三方 Syslog 服务器）
	支持指定用户和主机范围的审计策略
	支持 QQ、微信、whatapp 账号、登录、收发文件等动作审计

	支持在线社区、BBS、社交网站的搜索及发帖（BBS、博客、微博）账号、内容审计
	支持邮件账号、收发地址、主题审计
	支持电子商务在线购物内容搜索审计
	支持 FTP/HTTP 文件传输，网盘文件上传和下载审计
智能流控	支持基于线路和通道的 4 级嵌套应用流控管理策略
	支持基于接口、安全域的总带宽上下行管理
	支持高、中、低等 12 种类优先级通道设置
	支持应用、用户、源地址、服务、时间的五元组通道匹配策略
	支持带宽限制、带宽保障和弹性带宽；支持自动流量整形
	支持每 IP 限速、每应用限速；支持基于用户、地址排除策略
用户认证	支持用户自动识别，支持本地认证，单点认证和第三方认证联动
	支持本地静态绑定、web 用户认证，支持 Portal 用户认证、联动
	支持第三方用户认证服务器认证：RADIUS 服务器、 LDAP 服务器
	支持基于源接口 / 安全域，目的接口 / 安全域，源 / 目的地址，时间的用户策略
	支持在线用户监控和管理
入侵防御/检测	支持基于 IP 碎片重组、TCP 流重组、会话状态跟踪、应用层协议解码等数据流处理方式的攻击识别；支持模式匹配、异常检测、统计分析，以及抗 IDS/IPS 逃逸等多种检测技术，支持在线和旁路部署。
	支持入侵防护事件集 2300+，兼容 CVE/CNCVE,支持事件集自定义，支持手动、自动或定期升级
	可依据端口识别协议类型，可分析 HTTP、SMTP、FTP、Telnet、MPLS、ARP、GRE 等多种协议
	支持事件按照时间合并分析；支持基于语义的 SQL 注入检测；支持主要木马后门攻击防护
	支持如 FTP-HRLO-缓冲区溢出、HTTP-IIS-UNICODE-漏洞、MSSQL2000-远程溢出、GTP-AIX-溢出漏洞等缓冲区缓冲溢出类型攻击防护
	支持主流安全漏洞攻击防护；支持弱口令探测等可疑行为防护
	支持如 BP、NETBUS、DOLLY 等拒绝服务攻击防护
	支持如 TCP 端口扫描、UDP 端口扫描、ICMP 分布式主动机扫描等安全扫描攻击防护
	支持如红色代码、冲击波、震荡波等等蠕虫病毒防护
	网络数据库攻击；CGI 访问；CGI 攻击；支持检测黑名单自动加入或者手动添加
病毒防护	支持 HTTP，FTP，POP3，SMTP，IMAP 协议的病毒查杀、病毒库自动更新、虚拟脱壳、自定义查杀文件大小、查杀可疑病毒、可疑脚本、图片病毒、查杀邮件正文、附件、网页及下载文件中包含的病毒
	支持 600 万余种病毒的查杀，病毒库定期与及时更新
	支持启发式扫描查杀未知病毒、ZIP、RAR、TAR 等压缩及打包文件的病毒查杀，支持超过 20 种的预定义文件格式
	支持恶意网址实时监控与过滤、钓鱼网站监控过滤
	支持主机沙箱联动，支持可疑文件和可疑主机行为分析（可选）
	支持准确定位，查询访问源
	支持 HTTP，FTP，POP3，SMTP，IMAP 协议的病毒查杀、病毒库自动更新、虚拟脱壳、自定义查杀文件大小、查杀可疑病毒、可疑脚本、图片病毒、查杀邮件正文、附件、网页及下载文件中包含的病毒
VPN	支持 IPSec VPN 协议，支持网关到网关和远程接入部署模式 （64 条）
	支持预共享密钥、支持证书认证；支持主模式，野蛮模式，野蛮模式等
	支持 SSL VPN 协议, （64 条）
	支持专有 SSL VPN 客户端，客户端支持 Windows 32 位/64 系统，支持开源的 SSL VPN 客户端系统包括 IOS 安卓 linux

系统管理与监控	支持对象管理，包括：支持用户自定义、支持用户第三方用户同步，支持地址对象，ISP 地址库，应用对象，时间对象，自定义 URL 库，文件类型，服务对象，关键字对象，认证服务器等		
	支持管理员权限划分，支持预定义配置、审计、安全管理员，三权分立，支持管理员设置和分组		
	支持 SNMP v1、v2、v3		
	支持云集中管理，版本自动升级，配置下发，状态实时监控 （可选）		
	支持 HA、备机管理、接口联动、VRRP 等高可用性		
	支持详细的日志和统计报表，包括：系统日志、行为日志、审计日志、安全日志、流量日志、流量统计、流量统计、用户统计、会话统计、入侵防护统计、病毒防护统计、沙箱统计（可选）、设备健康统计等		
	支持日志导出、日志外发设置、本地存储设置等		
详细规格	**接口**	**接口数量**	5 个 RJ-45 端口（10/100/1000M 自适应、正反线自适应）
		管理接口	1 个 MGT（10/100/1000M 自适应、正反线自适应） 1 个 Console
		USB 接口	1 个 USB2.0 1 个 USB3.0
	CPU		J1800
	FLASH		1G
	内存		4G
	按钮		电源开关 Reset 复位按钮
	LED		电源指示灯：PWR 系统状态灯：SYS 系统负载指示灯：CPU 接口指示灯（Link/Act）
	电源及功耗		输入：100-240V AC 输出：12V 3A 功耗小于 36W
	尺寸（长×宽×高）		19 英寸 1U（440*400*44mm）
	工作环境	**温度**	-10~50℃
		高度	0-4000m
		相对湿度	5-95%，不结露
	支持的协议和标准		IPv4/v6，TCP，UDP，ARP， ICMP，NAT，DHCP，DNS，VRRP, SNTP，TELNET，HTTP，HTTPS，SNMP，PPP，PPPoE，PAP，CHAP， RIP，OSPF，BGP，LACP 等
	路由协议		静态路由、RIPv1/2、OSPFv2/v3、BGP4
	管理和配置		WEB（HTTP/HTTPS）、SSH/TELNET、Console