

FW3010PF-5000H 参数

2U 千兆

序号	项目	要求
1	基本要求	
1.1	自主研发	产品应为国内自主研发，并拥有软件著作权登记证书
1.2	产品资质要求	<ul style="list-style-type: none"> ● 公安部颁发的《计算机信息系统安全专用产品销售许可证》 ● 中国信息安全产品测评认证中心颁发的《国家信息安全认证产品型号证书》 ● 国家保密局涉密信息系统安全保密测评中心颁发《涉密信息系统产品检测证书》 ● 中国人民解放军信息安全测评认证中心《军用信息安全产品认证证书》
1.3	厂商资质要求	<ul style="list-style-type: none"> ● 安全产品原厂商必须通过ISO9001质量体系认证
2	硬件性能参数	
2.1	网络接口	6 个 100M /1000M 以太网电口 可扩展 4 个 GBIC 光口 2 个异步串行管理接口
2.2	产品外观	采用 2U 机架式设备
2.3	MTBF	平均无故障时间(MTBF)不小于 10 万小时
2.4	并发连接数	支持 180 万的并发连接
2.5	吞吐量	8G
3	功能参数	
3.1	工作模式	支持透明、路由、NAT、透明路由的混合模式的工作模式
3.2	NAT	产品应当支持多种网络地址转换，包括： <ol style="list-style-type: none"> (1) 支持源网络地址转换 (2) 支持目的网络地址转换 (3) 支持双向地址转换 (4) 支持端口映射
3.3	动态路由	支持动态路由协议如：OSPF、RIP 等
3.4	策略路由	支持策略路由
3.5	多接入	同时支持两个公网出口，按管理员制定的策略对出网数据进行分流； 产品应该支持 ADSL 拨号接入
3.6	IP/MAC 绑定	防火墙应具有局域网 MAC 扫描、IP/MAC 地址绑定功能，且必须具备 MAC 的自动学习功能
3.7	VLAN	支持 802.1Q 协议的穿透； 可根据 VLAN 设定访问控制规则
3.8	DHCP	支持 DHCP 服务器、DHCP Relay、DHCP 客户端
3.9	内容过滤	支持对 HTTP、SMTP、FTP 的内容过滤
3.10	深度过滤	支持对最新版本的 MSN、QQ 等即时消息 (IM) 工具进行拦截、封堵； 支持对可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 支持 URL 过滤，支持对脚本如 Cookies、Active 控件、Script 脚本的过滤以及 Web 页面修复等 支持对邮件的收发邮件地址过滤，邮件转发等，支持对邮件主题、正文、收发件人、附

		件名、附件内容等关键字匹配过滤
3.11	国家地区过滤	只需选择国家/地区名称，即可过滤与该国家/地区 IP 的通信。如：选择美国、日本、韩国、台湾地区等，即不能浏览这些地区的网站/论坛，不能收发这些地区的电子邮件等
3.12	代理服务	提供应用代理功能，包括 HTTP、FTP、TELNET、SMTP、POP3、DNS、ICMP、SOCKS 代理以及自定义代理，并可实现透明代理
3.13	多媒体协议支持	支持 H.323，UPNP 等多种多媒体协议，保证视频会议等媒体应用的流畅性
3.14	NAT 下多媒体支持	支持在 NAT 工作方式下的多媒体协议穿透
3.15	时间	支持基于时间的访问控制、应当可以手工配置时间
4	QOS	
4.1	流量控制	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
		安全策略与带宽管理结合，在设置安全策略时，即可一并设置带宽/流量管理策略，方便、灵活
4.2	流量配额	比如只允许使用 5G 的累积流量，则当累积流量大小达到设定的 5G 时，可以使用两种处理方式：拒绝或限速
4.3	计费功能	在防火墙管理系统中已经内置了一个计费公式，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
4.4	保证带宽	产品支持对某一网络对象的保证带宽设定
4.5	最高带宽	产品支持对某一网络对象的最高带宽限定
4.6	优先级设定	产品支持对网络对象或应用的带宽优先级设定
5	VPN	
5.1	连接协议	支持 IPSEC/PPTP/MPLS/L2TP 协议，提供端到端的安全隧道
5.2	安全认证	支持 IPsec 和 IKE，支持集中统一的证书管理（可由安全管理中心统一产生、分发证书）
5.3	加密算法	支持 3DES、DES 等加密算法，支持标准 MD5、SHA-1 认证算法
5.4	网关—网关	支持网关—网关的 VPN 方式
5.5	客户端—网关	支持客户端-网关的 VPN 方式
5.6	NAT 支持	支持隧道的 NAT 穿越，支持对隧道内明文的访问控制
5.7	产品互通性	产品采用标准的 IPsec，本身可以同其他国际主流品牌的 VPN 网关互通
5.8	动态 VPN	ADSL 拨号状态下的 VPN 功能
6	高可用性	
6.1	多机集群	支持多台防火墙主机的集群
6.2	双机热备	支持双机热备，支持主从、主主两种模式，防火墙切换时间小于 1 秒
6.3	负载均衡	支持防火墙间均衡和服务器均衡；服务器支持多种算法：权重、最小连接等
6.4	链路聚合	产品应当实现接口物理链路的线路冗余备份
7	安全性	
7.1	系统安全	专用 OS，系统本身无漏洞
7.2	抗攻击	产品应当可以防止非法报文攻击：land、Smurf、Pingofdeath、winnuke、tcp_sscan、ip_option、teardrop、targa3、ipspooft；统计型报文攻击：Synflood、Icmpflood、Udpflood、Portscan、ipsweep
7.3	抗端口扫描	产品可防 TCP、UDP 等端口扫描

7.4	抗地址欺骗	具备抗 arp 欺骗功能，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
7.5	内置入侵检测	系统应当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断开连接，实现入侵主动防护（IPS）
7.6	IDS 联动	支持与 IDS 产品的联动，并提供标准的联动协议
8	日志管理	
8.1	日志记录	产品详细记录防火墙上曾经发生过的事件（配置管理、运行信息、网络攻击、端口扫描等）
8.2	日志审计	产品可以按条件进行日志查询
8.3	日志存储	本地和网络数据库两种存放方式，支持主流的数据库，日志数据可以导出
8.4	管理授权	产品采用分权管理的安全机制，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 管理员可以在任何地点对防火墙进行实时监控和配置
9	管理功能	
9.1	GUI 界面	产品具备全中文的 GUI 界面
9.2	命令行	产品支持命令行的配置方式
9.3	集中管理	产品支持集中管理功能
9.4	配置导入导出	支持产品配置的导入导出功能
9.5	设有灾难恢复机制	当防火墙的部分文件系统由于物理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。能够察看网络内部所有主机的运行状况，网络异常时，能够查找网络内部所有异常主机。支持恢复出厂设置。
9.6	状态监控	产品可以通过图形界面对网络接口、处理器、存储器等关键部件的状态进行实时监控
9.7	远程管理	产品支持远程管理

FW3010PF-2000H 参数

1U 千兆，电口，不支持光纤连接

序号	项目	要求
1	基本要求	
1.1	自主研发	产品应为国内自主研发，并拥有软件著作权登记证书
1.2	产品资质要求	<ul style="list-style-type: none"> ● 公安部颁发的《计算机信息系统安全专用产品销售许可证》 ● 中国信息安全产品测评认证中心颁发的《国家信息安全认证产品型号证书》 ● 国家保密局涉密信息系统安全保密测评中心颁发《涉密信息系统产品检测证书》 ● 中国人民解放军信息安全测评认证中心《军用信息安全产品认证证书》
1.3	厂商资质要求	<ul style="list-style-type: none"> ● 安全产品原厂商必须通过ISO9001质量体系认证
2	硬件性能参数	
2.1	网络接口	6 个 10/100M /1000M 以太网电口 2 个异步串行管理接口 2 个 USB 接口
2.2	产品外观	采用 1U 机架式设备
2.3	MTBF	平均无故障时间(MTBF)不小于 10 万小时
2.4	并发连接数	支持 150 万的并发连接
2.5	吞吐量	5G
3	功能参数	
3.1	工作模式	支持透明、路由、NAT、透明路由的混合模式的工作模式
3.2	NAT	产品应当支持多种网络地址转换，包括： <ol style="list-style-type: none"> (1) 支持源网络地址转换 (2) 支持目的网络地址转换 (3) 支持双向地址转换 (4) 支持端口映射
3.3	动态路由	支持动态路由协议如：OSPF、RIP 等
3.4	策略路由	支持策略路由
3.5	多接入	同时支持两个公网出口，按管理员制定的策略对出网数据进行分流； 产品应该支持 ADSL 拨号接入
3.6	IP/MAC 绑定	防火墙应具有局域网 MAC 扫描、IP/MAC 地址绑定功能，且必须具备 MAC 的自动学习功能
3.7	VLAN	支持 802.1Q 协议的穿透； 可根据 VLAN 设定访问控制规则
3.8	DHCP	支持 DHCP 服务器、DHCP Relay、DHCP 客户端
3.9	内容过滤	支持对 HTTP、SMTP、FTP 的内容过滤
3.10	深度过滤	支持对最新版本的 MSN、QQ 等即时消息 (IM) 工具进行拦截、封堵； 支持对可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 支持 URL 过滤，支持对脚本如 Cookies、Active 控件、Script 脚本的过滤以及 Web 页面修复等 支持对邮件的收发邮件地址过滤，邮件转发等，支持对邮件主题、正文、收发件人、附

		件名、附件内容等关键字匹配过滤
3.11	国家地区过滤	只需选择国家/地区名称，即可过滤与该国家/地区 IP 的通信。如：选择美国、日本、韩国、台湾地区等，即不能浏览这些地区的网站/论坛，不能收发这些地区的电子邮件等
3.12	代理服务	提供应用代理功能，包括 HTTP、FTP、TELNET、SMTP、POP3、DNS、ICMP、SOCKS 代理以及自定义代理，并可实现透明代理
3.13	多媒体协议支持	支持 H.323，UPNP 等多种多媒体协议，保证视频会议等媒体应用的流畅性
3.14	NAT 下多媒体支持	支持在 NAT 工作方式下的多媒体协议穿透
3.15	时间	支持基于时间的访问控制、应当可以手工配置时间
4	QOS	
4.1	流量控制	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
		安全策略与带宽管理结合，在设置安全策略时，即可一并设置带宽/流量管理策略，方便、灵活
4.2	流量配额	比如只允许使用 5G 的累积流量，则当累积流量大小达到设定的 5G 时，可以使用两种处理方式：拒绝或限速
4.3	计费功能	在防火墙管理系统中已经内置了一个计费公式，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
4.4	保证带宽	产品支持对某一网络对象的保证带宽设定
4.5	最高带宽	产品支持对某一网络对象的最高带宽限定
4.6	优先级设定	产品支持对网络对象或应用的带宽优先级设定
5	VPN	
5.1	连接协议	支持 IPSEC/PPTP/MPLS/L2TP 协议，提供端到端的安全隧道
5.2	安全认证	支持 IPsec 和 IKE，支持集中统一的证书管理（可由安全管理中心统一产生、分发证书）
5.3	加密算法	支持 3DES、DES 等加密算法，支持标准 MD5、SHA-1 认证算法
5.4	网关—网关	支持网关—网关的 VPN 方式
5.5	客户端—网关	支持客户端-网关的 VPN 方式
5.6	NAT 支持	支持隧道的 NAT 穿越，支持对隧道内明文的访问控制
5.7	产品互通性	产品采用标准的 IPsec，本身可以同其他国际主流品牌的 VPN 网关互通
5.8	动态 VPN	ADSL 拨号状态下的 VPN 功能
6	高可用性	
6.1	多机集群	支持多台防火墙主机的集群
6.2	双机热备	支持双机热备，支持主从、主主两种模式，防火墙切换时间小于 1 秒
6.3	负载均衡	支持防火墙间均衡和服务器均衡；服务器支持多种算法：权重、最小连接等
6.4	链路聚合	产品应当实现接口物理链路的线路冗余备份
7	安全性	
7.1	系统安全	专用 OS，系统本身无漏洞
7.2	抗攻击	产品应当可以防止非法报文攻击：land、Smurf、Pingofdeath、winnuke、tcp_sscan、ip_option、teardrop、targa3、ipspooft；统计型报文攻击：Synflood、Icmpflood、Udpflood、Portscan、ipsweep
7.3	抗端口扫描	产品可防 TCP、UDP 等端口扫描

7.4	抗地址欺骗	具备抗 arp 欺骗功能，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
7.5	内置入侵检测	系统应当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断开连接，实现入侵主动防护（IPS）
7.6	IDS 联动	支持与 IDS 产品的联动，并提供标准的联动协议
8	日志管理	
8.1	日志记录	产品详细记录防火墙上曾经发生过的事件（配置管理、运行信息、网络攻击、端口扫描等）
8.2	日志审计	产品可以按条件进行日志查询
8.3	日志存储	本地和网络数据库两种存放方式，支持主流的数据库，日志数据可以导出
8.4	管理授权	产品采用分权管理的安全机制，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 管理员可以在任何地点对防火墙进行实时监控和配置
9	管理功能	
9.1	GUI 界面	产品具备全中文的 GUI 界面
9.2	命令行	产品支持命令行的配置方式
9.3	集中管理	产品支持集中管理功能
9.4	配置导入导出	支持产品配置的导入导出功能
9.5	设有灾难恢复机制	当防火墙的部分文件系统由于物理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。能够察看网络内部所有主机的运行状况，网络异常时，能够查找网络内部所有异常主机。支持恢复出厂设置。
9.6	状态监控	产品可以通过图形界面对网络接口、处理器、存储器等关键部件的状态进行实时监控
9.7	远程管理	产品支持远程管理

FW3010PF-1000N 参数

基本百兆

序号	项目	要求
1	基本要求	
1.1	自主研发	产品应为国内自主研发，并拥有软件著作权登记证书
1.2	产品资质要求	<ul style="list-style-type: none"> ● 公安部颁发的《计算机信息系统安全专用产品销售许可证》 ● 中国信息安全产品测评认证中心颁发的《国家信息安全认证产品型号证书》 ● 国家保密局涉密信息系统安全保密测评中心颁发《涉密信息系统产品检测证书》 ● 中国人民解放军信息安全测评认证中心《军用信息安全产品认证证书》
1.3	厂商资质要求	<ul style="list-style-type: none"> ● 安全产品原厂商必须通过ISO9001质量体系认证
2	硬件性能参数	
2.1	网络接口	4 个 10/100M 以太网电口
2.2	产品外观	采用 1U 机架式设备
2.3	MTBF	平均无故障时间(MTBF)不小于 10 万小时
2.4	并发连接数	支持 80 万的并发连接
2.5	吞吐量	300M
3	功能参数	
3.1	工作模式	支持透明、路由、NAT、透明路由的混合模式的工作模式
3.2	NAT	产品应当支持多种网络地址转换，包括： <ol style="list-style-type: none"> (1) 支持源网络地址转换 (2) 支持目的网络地址转换 (3) 支持双向地址转换 (4) 支持端口映射
3.3	动态路由	支持动态路由协议如：OSPF、RIP 等
3.4	策略路由	支持策略路由
3.5	多接入	同时支持两个公网出口，按管理员制定的策略对出网数据进行分流；产品应该支持 ADSL 拨号接入
3.6	IP/MAC 绑定	防火墙应具有局域网 MAC 扫描、IP/MAC 地址绑定功能，且必须具备 MAC 的自动学习功能
3.7	VLAN	支持 802.1Q 协议的穿透；可根据 VLAN 设定访问控制规则
3.8	DHCP	支持 DHCP 服务器、DHCP Relay、DHCP 客户端
3.9	内容过滤	支持对 HTTP、SMTP、FTP 的内容过滤
3.10	深度过滤	支持对最新版本的 MSN、QQ 等即时消息 (IM) 工具进行拦截、封堵； 支持对可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 支持 URL 过滤，支持对脚本如 Cookies、Active 控件、Script 脚本的过滤以及 Web 页面修复等 支持对邮件的收发邮件地址过滤，邮件转发等，支持对邮件主题、正文、收发件人、

		附件名、附件内容等关键字匹配过滤
3.11	国家地区过滤	只需选择国家/地区名称，即可过滤与该国家/地区 IP 的通信。如：选择美国、日本、韩国、台湾地区等，即不能浏览这些地区的网站/论坛，不能收发这些地区的电子邮件等
3.12	代理服务	提供应用代理功能，包括 HTTP、FTP、TELNET、SMTP、POP3、DNS、ICMP、SOCKS 代理以及自定义代理，并可实现透明代理
3.13	多媒体协议支持	支持 H.323, UPNP 等多种多媒体协议，保证视频会议等媒体应用的流畅性
3.14	NAT 下多媒体支持	支持在 NAT 工作方式下的多媒体协议穿透
3.15	时间	支持基于时间的访问控制、应当可以手工配置时间
4	QOS	
4.1	流量控制	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 安全策略与带宽管理结合，在设置安全策略时，即可一并设置带宽/流量管理策略，方便、灵活
4.2	流量配额	比如只允许使用 5G 的累积流量，则当累积流量大小达到设定的 5G 时，可以使用两种处理方式：拒绝或限速
4.3	计费功能	在防火墙管理系统中已经内置了一个计费公式，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
4.4	保证带宽	产品支持对某一网络对象的保证带宽设定
4.5	最高带宽	产品支持对某一网络对象的最高带宽限定
4.6	优先级设定	产品支持对网络对象或应用的带宽优先级设定
5	VPN	
5.1	连接协议	支持 IPSEC/PPTP/MPLS/L2TP 协议，提供端到端的安全隧道
5.2	安全认证	支持 IPsec 和 IKE，支持集中统一的证书管理（可由安全管理中心统一产生、分发证书）
5.3	加密算法	支持 3DES、DES 等加密算法，支持标准 MD5、SHA-1 认证算法
5.4	网关—网关	支持网关—网关的 VPN 方式
5.5	客户端—网关	支持客户端-网关的 VPN 方式
5.6	NAT 支持	支持隧道的 NAT 穿越，支持对隧道内明文的访问控制
5.7	产品互通性	产品采用标准的 IPSec，本身可以同其他国际主流品牌的 VPN 网关互通
5.8	动态 VPN	ADSL 拨号状态下的 VPN 功能
6	高可用性	
6.1	多机集群	支持多台防火墙主机的集群
6.2	双机热备	支持双机热备，支持主从、主主两种模式，防火墙切换时间小于 1 秒
6.3	负载均衡	支持防火墙间均衡和服务器均衡；服务器支持多种算法：权重、最小连接等
6.4	链路聚合	产品应当实现接口物理链路的线路冗余备份
7	安全性	
7.1	系统安全	专用 OS，系统本身无漏洞
7.2	抗攻击	产品应当可以防止非法报文攻击：land、Smurf、Pingofdeath、winnuke、tcp_sscan、ip_option、teardrop、targa3、ipspooft；统计型报文攻击：Synflood、Icmpflood、Udpflood、Portscan、ipsweep
7.3	抗端口扫描	产品可防 TCP、UDP 等端口扫描

7.4	抗地址欺骗	具备抗 arp 欺骗功能，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
7.5	内置入侵检测	系统应当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断开连接，实现入侵主动防护（IPS）
7.6	IDS 联动	支持与 IDS 产品的联动，并提供标准的联动协议
8	日志管理	
8.1	日志记录	产品详细记录防火墙上曾经发生过的事件（配置管理、运行信息、网络攻击、端口扫描等）
8.2	日志审计	产品可以按条件进行日志查询
8.3	日志存储	本地和网络数据库两种存放方式，支持主流的数据库，日志数据可以导出
8.4	管理授权	产品采用分权管理的安全机制，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 管理员可以在任何地点对防火墙进行实时监控和配置
9	管理功能	
9.1	GUI 界面	产品具备全中文的 GUI 界面
9.2	命令行	产品支持命令行的配置方式
9.3	集中管理	产品支持集中管理功能
9.4	配置导入导出	支持产品配置的导入导出功能
9.5	设有灾难恢复机制	当防火墙的部分文件系统由于物理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。能够察看网络内部所有主机的运行状况，网络异常时，能够查找网络内部所有异常主机。支持恢复出厂设置。
9.6	状态监控	产品可以通过图形界面对网络接口、处理器、存储器等关键部件的状态进行实时监控
9.7	远程管理	产品支持远程管理