# 附件2：紫金学院网络中心防火墙技术参数

|  |  |
| --- | --- |
| **技术指标** | **指标要求** |
| **硬件规格** | 硬件平台采用多核网络专用架构，使用64位MIPS多核处理器，非X86多核架构或ASIC架构,；配置冗余双电源。 |
| 设备高度≥2U，标配2个通用扩展槽位，配置2个10/100/1000 MBase-T电口，8个万兆SFP+光口,每个接口可划分到不同安全域实现各接口间的安全隔离，提供独立的带外管理接口和HA接口。 |
| **性能** | 吞吐率(bps)≥80G，最大并发连接数≥3000万，VPN吞吐量(bps) ≥50G，每秒新建连接数≥110万，提供IPSec VPN隧道数≥18000条，并发SSL VPN用户许可≥6个。 |
| **网络适应性** | 支持透明、路由、混合、直连（虚拟线）模式 |
| 支持对3000+ 种应用的识别和控制，包括200+移动应用，提供产品界面截图有效 |
| 要求支持多系统引导，并可在WEB界面上直接配置启动顺序 |
| 支持静态路由、等价路由、策略路由，以及BGP、RIPv1/v2、OSPF、ISIS等动态IPv4路由协议（非透传），提供产品界面截图 |
| 支持将任意接口数据完全镜像到设备自身的其他接口用于抓包分析，支持基于源IP、目的IP、源端口、目的端口、网络协议（TCP、UDP、ICMP）等条件对镜像流量进行过滤，并且支持选择入方向、出方向及双向流量镜像，提供产品界面截图 |
| 支持基于源地址、目的地址、生效时间、应用协议（http、https、mysql、ms-sql、sqlnet、sip等）限制新建连接、并发连接；提供产品界面截图 |
| 支持基于应用协议的路由功能，根据应用类型进行路由选择。提供产品界面截图有效 |
| 支持基于多出口的DNS代理功能，可根据配置实现对不同外网线路的DNS服务器地址管理，当一条链路出现故障时，流量自动切换到其他链路的同时将DNS服务器进行切换，避免出现跨运营商解析而导致访问变慢或中断；支持为不同运营商的DNS设置不同权重，用户根据权重比例选择不同运营商DNS进行解析实现不同线路的负载均衡功能。提供产品界面截图有效 |
| 支持线路过载保护功能，当某条外网线路拥塞时，自动将其流量切换到其他链路；系统对各出口的流量带宽进行实时监测，当自身接口的流量带宽超过配置的阈值时，新建会话的流量将不再从这个接口转发。当此接口的流量带宽回落到正常值以下时，新建会话的流量再恢复从这个接口转发 |
| 支持基于接口时延的动态切换能力：系统从多出接口向外部某一个或多个目的地址探测时延。当自身接口的时延超过配置的阈值时，新建会话的流量就不再从这个接口转发，而是走其它接口。当此接口的时延回落到正常值以下后，新建会话的流量再允许从这个接口转发，提供产品界面截图有效 |
| **NAT功能** | 支持多对一、多对多的NAT地址转换，且公网地址池可选择逐一使用和同时使用两种模式。 |
| 为解决公网IP地址资源问题，要求必须支持NAT的端口扩展技术，支持NAT full cone模式。 |
| 支持NAT公网地址池中IP有效性检测，避免因NAT地址无法使用导致业务中断，提供产品界面截图有效。 |
| **IPV6功能** | 支持IPV6邻居发现协议、IPV6 SNMP管理、IPV6路由配置、IPV6 DNS配置、IPV6策略配置、IPV6 ALG配置、IPV6 6TO4隧道配置、IPV6 4to6隧道配置、NAT-PT配置、NAT64和DNS64配置 |
| 支持对IPV6用户的会话日志监控、流量监控、应用监控功能，并且能够对IPV6用户进行自定义监控统计功能，提供产品界面截图 |
|  **VPN功能** | 支持标准IPSec协议，能够与Cisco等知名厂商的VPN设备互联互通；支持GRE、L2TP、Xauth等VPN连接 |
| **管理功能** | 支持不少于8个配置文件并存，并支持配置文件备注以便配置回退。提供功能截图有效 |
| 提供标准的SNMPV1/V2/V3协议管理方式 |
| 支持基于IP地址的流量统计、支持基于应用的流量统计、支持基于IP地址的会话统计功能，支持基于应用的会话统计包括短时间周期和长时间周期（提供功能截图） |
| **资质要求** | 公安部颁发的《计算机信息系统安全专用产品销售许可证》（第二代防火墙万兆增强级），提供证明文件 |
| 具备中国网络安全审查技术与认证中心颁发的《网络关键设备和网络安全专用产品安全认证和中国国家信息安全产品认证二合一证书》（万兆），提供证明文件 |
| 具备信息产业部颁发的电信设备进网许可证，提供证明文件 |
| 加入微软安全响应中心（Microsoft Security Response Center）发起的MAPP（Microsoft Active Protection Program）计划，作为该计划成员，可在微软发布每月安全公告之前获得微软产品的详细漏洞信息，为用户提供更及时的安全防护。提供微软第三方证明或微软网站截图 |
| **质保授权** | 提供原厂商对本项目的授权和售后服务承诺 |
| 提供五年硬件及软件升级服务 |

# DMZ区防火墙

|  |  |
| --- | --- |
| **技术指标** | **指标要求** |
| **硬件规格** | 硬件平台采用多核网络专用架构，使用64位MIPS多核处理器，非X86多核架构或ASIC架构,；配置冗余双电源。 |
| 配置≥4个千兆电口，≥4个千兆光口，不能少于1个接口扩展槽位，不少于1个RJ45串口,不少于1个RJ45管理口。含传统防火墙、应用管理、IPSec VPN、资产识别、URL过滤模块、入侵防护模块、防病毒模块。 |
| **性能** | 吞吐率(bps)≥10G，最大并发连接数≥80万，每秒新建不少于4万 |
| **网络适应性** | 支持透明、路由、混合、直连（虚拟线）模式 |
| 支持对3000+ 种应用的识别和控制，包括200+移动应用，提供产品界面截图有效 |
| 要求支持多系统引导，并可在WEB界面上直接配置启动顺序 |
| 支持静态路由、等价路由、策略路由，以及BGP、RIPv1/v2、OSPF、ISIS等动态IPv4路由协议（非透传），提供产品界面截图 |
| 支持将任意接口数据完全镜像到设备自身的其他接口用于抓包分析，支持基于源IP、目的IP、源端口、目的端口、网络协议（TCP、UDP、ICMP）等条件对镜像流量进行过滤，并且支持选择入方向、出方向及双向流量镜像，提供产品界面截图 |
| 支持基于源地址、目的地址、生效时间、应用协议（http、https、mysql、ms-sql、sqlnet、sip等）限制新建连接、并发连接；提供产品界面截图 |
| 支持基于应用协议的路由功能，根据应用类型进行路由选择。提供产品界面截图有效 |
| 支持基于多出口的DNS代理功能，可根据配置实现对不同外网线路的DNS服务器地址管理，当一条链路出现故障时，流量自动切换到其他链路的同时将DNS服务器进行切换，避免出现跨运营商解析而导致访问变慢或中断；支持为不同运营商的DNS设置不同权重，用户根据权重比例选择不同运营商DNS进行解析实现不同线路的负载均衡功能。提供产品界面截图有效 |
| 支持线路过载保护功能，当某条外网线路拥塞时，自动将其流量切换到其他链路；系统对各出口的流量带宽进行实时监测，当自身接口的流量带宽超过配置的阈值时，新建会话的流量将不再从这个接口转发。当此接口的流量带宽回落到正常值以下时，新建会话的流量再恢复从这个接口转发 |
| 支持基于接口时延的动态切换能力：系统从多出接口向外部某一个或多个目的地址探测时延。当自身接口的时延超过配置的阈值时，新建会话的流量就不再从这个接口转发，而是走其它接口。当此接口的时延回落到正常值以下后，新建会话的流量再允许从这个接口转发，提供产品界面截图有效 |
| 支持对HTTP、FTP、SMTP、POP3、IMAP4、SMB等协议的病毒防护 |
| **入侵防御** | 基于特征检测，支持超过4000种特征的攻击检测和防御 |
| 支持CC攻击检测，支持访问限速、代理限速、自定义请求阈值、爬虫友好等方法，检测到CC攻击时支持JS Cookie、重定向、访问确认、验证码四种认证方法，提供产品界面截图有效 |
| **防病毒** | 支持木马病毒、蠕虫病毒、宏病毒、脚本病毒等各种病毒的查杀。 |
| 查杀邮件正文/附件、网页及下载文件中包含的病毒，可支持到10层压缩文件的病毒查杀 |
| **NAT功能** | 支持多对一、多对多的NAT地址转换，且公网地址池可选择逐一使用和同时使用两种模式。 |
| 为解决公网IP地址资源问题，要求必须支持NAT的端口扩展技术，支持NAT full cone模式。 |
| ★支持NAT公网地址池中IP有效性检测，避免因NAT地址无法使用导致业务中断，提供产品界面截图有效。 |
| **IPV6功能** | 支持IPV6邻居发现协议、IPV6 SNMP管理、IPV6路由配置、IPV6 DNS配置、IPV6策略配置、IPV6 ALG配置、IPV6 6TO4隧道配置、IPV6 4to6隧道配置、NAT-PT配置、NAT64和DNS64配置 |
| ★支持对IPV6用户的会话日志监控、流量监控、应用监控功能，并且能够对IPV6用户进行自定义监控统计功能，提供产品界面截图 |
|  **VPN功能** | 支持标准IPSec协议，能够与Cisco等知名厂商的VPN设备互联互通；支持GRE、L2TP、Xauth等VPN连接 |
| 提供SSL VPN功能；必须支持对登录SSL VPN的用户端系统进行端点安全检查，至少包括指定文件、指定进程、系统补丁、浏览器版本、杀毒软件等方面，提供产品界面截图有效 |
| **管理功能** | 支持不少于8个配置文件并存，并支持配置文件备注以便配置回退。提供功能截图有效 |
| 提供标准的SNMPV1/V2/V3协议管理方式 |
| 支持基于IP地址的流量统计、支持基于应用的流量统计、支持基于IP地址的会话统计功能，支持基于应用的会话统计包括短时间周期和长时间周期（提供功能截图） |
| **资质要求** | ★公安部颁发的《计算机信息系统安全专用产品销售许可证》（第二代防火墙万兆增强级），提供证明文件 |
| 具备信息产业部颁发的电信设备进网许可证，提供证明文件 |
| 加入微软安全响应中心（Microsoft Security Response Center）发起的MAPP（Microsoft Active Protection Program）计划，作为该计划成员，可在微软发布每月安全公告之前获得微软产品的详细漏洞信息，为用户提供更及时的安全防护。提供微软第三方证明或微软网站截图 |
| **质保授权** | 提供原厂商对本项目的授权和售后服务承诺 |
| 提供五年硬件及软件升级服务 |