**防火墙招标规格引导**

## 重点说明

其中打★内容为重点引导项，可作为抬高项和定档项指标。

其中打Δ内容为重点引导项，可作为废标项或加分项。

防火墙1U高度，可以作为加分项：

|  |  |  |  |
| --- | --- | --- | --- |
| 占用机架空间 | 4 | 单位（宽\*深\*高）mm | N家投标单位投标的该项指标值为X1、X2、X3、……、XN，第N家投标单位的得分SN=此项满分\*（min（X1、X2、……、XN）/XN）。 |

## 硬件配置及性能

|  |  |
| --- | --- |
| **指标项** | **技术规格要求** |
| 配置要求 | ★实配：千兆电口≥12，万兆光口≥12，40G接口≥2，SSL VPN并发数≥4950，IPSec VPN隧道≥14500，虚拟防火墙数量≥99，配置双电源；  |
| 配置要求 | Δ支持USB3.0（提供设备照片） |
| 硬件架构 | Δ为了提高可靠性，支持风扇可插拔；（提供证明截图）  |
| 硬件架构 | Δ支持前后风道；（提供证明截图） |
| 性能要求 | ★吞吐量≥40Gbps，最大并发连接数≥1200万，每秒新建连接数≥40万，IPSec吞吐量≥29Gbps，SSL\_VPN吞吐量≥3Gbps，IPS吞吐量≥14.5Gbps，SSL代理吞吐量≥6Gbps； |

## 功能参数

**E200E-G8、E1000E-G3/G5/G8/G12/G16功能参数**

|  |  |
| --- | --- |
| 策略管控 | Δ能够基于时间、用户/用户组/安全组、应用层协议、地理位置、IP地址、端口、域名组、URL分类、接入类型、终端类型、设备组、内容安全统一界面进行安全策略配置；（提供功能截图)  |
| 路由功能 | 支持静态路由、策略路由、RIP、OSPF、BGP、ISIS等路由协议 |
| 策略路由支持的匹配条件：源IP/目的IP，服务类型，应用类型，用户(组)，入接口，DSCP优先级； |
| IPV6 | 支持IPv6协议栈、IPV6穿越技术、IPV6路由协议；（提供“IPV6 Ready Phase-2”认证证书复印件） |
| Δ支持IPv6 over IPv4 GRE隧道，6RD隧道； |
| 协议识别 | Δ支持识别国标SIP协议及主流安防厂家的私有协议；（提供功能截图） |
| 流量控制 | 可支持基于应用层协议设置流控策略，包括设置最大带宽、保证带宽、协议流量优先级等； |
| 支持基于用户，IP的带宽保证；  |
| Δ支持每IP， 每用户的最大连接数限制，防护服务器；（提供功能截图） |
| 支持用户流量配额管理；（提供功能截图） |
| 支持流量整形； |
| 支持基于地理位置的流量和威胁分析；（提供功能截图） |
| 策略管理 | 支持策略的模糊查询，策略组，策略规则标签，方便策略的管理及运维； |
| 支持将基于端口的安全策略转换为基于应用的安全策略，分析设备策略风险，及冗余策略，提供安全策略优化建议；（提供功能截图） |
| 数据安全 | 支持数据防泄露，对传输的文件和内容进行识别过滤，对内容与身份证、信用卡、银行卡、社会安全卡号等类型进行匹配；（提供功能截图） |
| 支持DNS过滤，提高WEB网页过滤的性能；（提供功能截图） |
| 支持SafeSearch，过滤掉Google等搜索引擎返回的不健康的内容；（提供功能截图） |
| DDoS防护 | 支持HTTP、HTTPS、DNS、SIP等应用层Flood攻击，支持流量自学习功能，可设置自学习时间，并自动生成DDoS防范策略；（提供功能截图） |
| 支持IP信誉；（提供功能截图） |
| NAT | 支持全面NAT功能，对多种应用层协议支持ALG功能，包括ILS、DNS、PPTP、SIP、FTP、ICQ、RTSP、QQ、MSN、MMS等； |
| 支持源NAT自动探测并排除NAT-IP地址池中无效地址（防封杀）； |
| 支持源NAT地址池使用率超限告警； |
| 支持三元组NAT smart-fullcone； |
| 入侵防御及病毒防护 | 基于特征检测，支持超过2000种特征的攻击检测和防御；（提供功能截图） |
| 支持基于场景进行策略入侵防御的模板定制； |
| 支持对常见应用服务（HTTP、FTP、SSH、SMTP、IMAP）和数据库软件（MySQL、Oracle、MSSQL）的口令暴力破解防护功能；（提供功能截图） |
| ΔIPS检出率获得NSS推荐级。（提供功能截图） |
| 支持恶意域名过滤，实现对C&C进行阻断；（提供功能截图） |
| 可以支持HTTP、FTP、SMTP、POP3、IMAP、NFS等协议的病毒防护； |
| 加密流量安全防护 | Δ支持对HTTPS，POP3S，SMTPS,IMAPS加密流量代理解密后，并进行内容过滤，审计，安全防护；（提供功能截图） |
| 支持基于URL分类的精细化解密，提高解密性能；（提供功能截图） |
| 支持加密流量解密后镜像给第三方设备做审计，安全检测；（提供功能截图） |
| 集中管理及易用性 | Δ支持防火墙向云管理平台自动注册，云管理平台对防火墙进行统一的管理及运维；（提供功能截图） |
| Δ支持U盘升级，减少运维成本；（提供功能截图） |
| Δ开放RESTCONF，NETCONF等北向接口，对接第三方的管理平台；（提供功能截图） |
| 智能威胁防御 | 支持与本地沙箱联动，实现对APT攻击的防御功能；（提供功能截图） |
| 支持防火墙与云沙箱，本地沙箱混合联动，敏感文件在本地沙箱检测，普通文件上传到云沙箱，及保护了客户敏感数据有提高了云检测能力；（提供功能截图） |
| 支持防火墙与网络安全智能分析系统联动，做态势感知，全网威胁展示，并能针对威胁生成阻断策略；（提供功能截图） |
| 支持防火墙与云端WEB信誉系统，文件信誉系统，IP信誉系统联动，实时阻断威胁；（提供功能截图） |
| 支持将网络安全智能分析系统、沙箱的检测结果形成本地信誉，供防火墙查询，从而实现威胁闭环； |
| Δ配置防火墙流探针功能，对网络中的流量进行采集，上送网络安全智能分析系统进行威胁分析；（提供功能截图） |
| 上网用户认证 | 支持AD单点登录，Radius单点登录，NTLM认证，免认证，与认证服务器配合实现微信认证，MAC认证；（提供功能截图） |
| 支持动态安全组，对横向组织机构进行动态授权；（提供功能截图） |
| 支持多认证域，满足多分公司独立管理，认证的述求；（提供功能截图） |
| 支持Portal页面定制及调查问卷，进行营销推广；（提供功能截图） |
| 可靠性 | 支持BFD链路检测，支持BFD与VRRP联动实现双机快速切换，支持BFD与OSPF联动实现双机快速切换；（提供功能截图） |
| 支持HA平滑升级，升级窗口中支持不同版本的软件形成双机热备；  |
| 多出口智能选路 | 可根据目的地址智能优选运营商链路，支持主备接口配置以及按比例分配的负载分担方式； |
| 产品资质 | Δ防火墙产品连续7年进入Gartner企业防火墙四象限，提供证明材料； |
| 具有公安部颁发的防火墙《计算机信息系统安全专用产品销售许可证》，提供证书复印件； |