附件三

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 服务名称 | 技术服务参数 | 单位 | 数量 | 备注 |
| 互联网专线服务 | 1.带宽≥200M支持高质量访问互联网，上下行对称带宽，可配置静态固定IPv6或双栈（IPv4和IPv6）地址。 | 条 | 2 |  |
| 防火墙 | 1、设备接口：千兆电口≥10，千兆光口≥2。 ▲2、硬件平台：采用非X86多核架构。(要求提供功能截图或现场演示操作) ▲3、国产化支持：产品自主可控，关键芯片全部国产化。包括但不限于CPU、转发、网卡芯片、电源等。(要求提供功能截图或现场演示操作) 4、性能要求：大包吞吐量≥2Gbps；混合包吞吐量≥2Gbps；小包吞吐量≥1.2Gbps；开启威胁防护设；混合包性能≥600Mbps；并发连接数≥30万；每秒新建连接数≥2万；IPSec VPN并发连接数≥2000；SSL VPN并发连接数≥500。 5、安全特征库：应用识别：应用识别签名数量不少于1500；入侵检测：入侵防御特征库签名数量不少于5000；病毒库：亿级；URL库：URL数量不少于1.2亿。 ▲6、支持恶意域名过滤，实现对C&C进行阻断。(要求提供功能截图或现场演示操作) ▲7、支持HTTP、FTP、SMTP、POP3、IMAP、NFS等协议的病毒防护。(要求提供功能截图或现场演示操作) ▲8、可用于恶意加密流量识别，可检测不解密网络流量下的恶意加密通信流量。(要求提供功能截图或现场演示操作) 9、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。 10、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。 ▲11、流量控制：支持每IP，每用户的最大连接数限制，防护服务器；支持用户流量配额管理。(要求提供功能截图或现场演示操作) ▲12、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；支持DNS过滤，提高WEB网页过滤的性能。(要求提供功能截图或现场演示操作) ▲13、支持外部攻击源自动阻断：对内部网络的主机威胁事件，能够检测并下发黑名单阻断攻击源，支持SQL注入、遍历漏洞、命令注入漏洞等威胁防护能力。(要求提供功能截图或现场演示操作) 14、支持对内部网络的主机失陷事件，能够检测并向用户注册的手机号码和邮箱发送告警通知。 15、支持基于安全防御节点上送的安全日志能够进行日志的聚合、分析、判定动作，去除安全日志的噪音，可以在界面呈现原始事件数量、聚合后的威胁事件数量、攻击源信息。 16、支持黑白名单创建：可通过用户安全运维平台下发全局白名单，对多台本地安全防御节点统一下发白名单。 ▲17、支持威胁信息检索：支持全球恶意IP、恶意域名、恶意文件、漏洞信息等威胁信息的快速检索，数据详情包括但不限于威胁等级、置信度、威胁标签、相关样本、IP反查等信息。(要求提供功能截图或现场演示操作) 18、支持按周、按月为用户提供安全服务报告，安全服务报告将以邮件形式发送至用户订阅邮箱。通过安全服务报告，可以使客户可清晰了解以下信息：1、安全服务概况； 2、威胁防护次数及趋势；3、失陷主机数量及详情；4、外部攻击源数量及趋势；5、恶意文件数量及趋势。 ▲19支持、应能提供云端平台的隐私测评报告，结论为合格或通过。(要求提供功能截图或现场演示操作) ▲20、订阅扩展能力：可以支持SaaS订阅，无需增加额外硬件，支持漏洞扫描、日志审计等功能。(要求提供功能截图或现场演示操作) ▲21.清洗能力≥10Tbps。需提供CNAS或CMA标识的检测报告证明文件并加盖供应商鲜章； ▲22.采用近源式清洗、分布式清洗，具有全国调动防护能力，具有城域网近目的清洗、城域网、骨干网二级协同联动能力，供应商在全球部署有清洗中心，全球清洗中心数量≥50个；需提供清洗中心能力需提供节点测试截图，及CNAS或CMA标识的检测报告证明文件并加盖供应商鲜章。 ▲23.采用基于管道侧的清洗中心，支持基于需防护目的IP地址的可实现国际流量、国内运营商分方向的流量压制功能，无需修改DNS配置和IP地址，仅需提供防护目标对象即可进行防护，及CNAS或CMA标识的检测报告证明文件并加盖供应商鲜章。 ▲24具有中环联合认证中心颁发的《网络型防火墙生态产品认证证书》，提供证书复印件； | 套 | 1 |  |