原招标文件P9-11页“4.网络设备要求”中

**4.1安全网关**

|  |  |
| --- | --- |
| 指标项 | 参数要求 |
| 产品形态 | 1、支持固化千兆电口≥8个，固化千兆光口≥4个。 |
| 2、支持双硬盘插槽，硬盘容量≥1T，硬盘支持可插拔更换、支持内存≥4GB。 |
| 3、标准1U机箱，多核非X86架构。 |
| 4、▲支持1+1冗余电源。 |
| 5、NAT转发吞吐率≥2.0Gbps；并发NAT连接数≥400W；新建NAT连接数≥1500。 |
| 6、支持流量识别保障功能：能够精确识别网络应用，保障关键业务的系统带宽，配置应用协议库，协议识别数量≥1500种。 |
| 7、配置URL数据库及应用特征库5年升级，另外URL数据库和应用特征库支持远程HTTP自动升级。 |
| 8、配置≥350个SSLVPN接入授权。 |
| 9、配置350路IpsecVPN接入授权。 |
| 功能参数 | 10、▲支持静态路由、RIP(V1/V2)、RIPng、OSPFv2等多种路由协议 |
| 11、为保证在多条外网线路情况下带宽的合理分配使用，设备必须支持多链路负载均衡，负载均衡可基于带宽、负载等多种方式。 |
| 12、支持正向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。 |
| 13、支持IPV6环境 |
| 14、支持状态检测防火墙功能，实现网络安全防护 |
| 15、▲支持网关、网桥等多种部署模式，灵活安装。 |
| 16、支持SNMPV2和V3版本，支持多TRAP接收主机配置。 |
| 17、支持DHCP功能，对内网提供DHCP服务。 |
| 18、支持VRRP(VirtualRouterRedundancyProtocol，虚拟路由冗余协议)。 |
| 19、DHCP地址池分配状态，可生成IP、MAC对应关系列表。 |
| 20、支持HTTPS和HTTP的WEB方式管理。 |
| 21、▲支持VPN内流量的可视化监控，提供设备截图。 |
| 22、▲支持WEB本地认证方式、Radius认证、微信认证功能。提供设备截图。 |
| 产品资质 | 23、为保障产品代码质量，供货厂商需通过CMMI4认证，提供证书复印件。 |
| 24、▲为了保障工程质量，投标设备生产厂家应具备信息系统集成及服务资质三级（含以上），提供证书复印件，并且厂商盖章确认。（证书名称与设备厂商一致） |
| 25、▲投标设备厂商应是自主研发、技术创新的企业，应有独立的企业技术中心，受国家的认可，并提供网站查询地址及证明文件，并且厂商盖章确认。 |

**4.2接入层交换机**

|  |  |
| --- | --- |
| 指标项 | 参数要求 |
| 产品形态 | ▲交换容量≥3.36Tbps，转发性能≥166Mpps。 |
| ▲固化10/100/1000M以太网端口≥48，固化1GSFP光接口≥4个；整机最大可用千兆口≥52。 |
| ▲要求所投设备MAC地址≥16K，ARP表项≥1000条,FIB表项≥500。 |
| ▲要求所投产品必须涂装三防漆，充分提升设备绝缘、防潮、防腐蚀、防霉、防盐雾等性能,提供官网截图并厂商盖章确认。 |
| ▲要求所投产品支持防雷等级10KV，提供第三方权威机构测试报告并厂商盖章确认。 |
| 功能参数 | 支持静态路由、RIP/RIPng、OSPFv2/OSPFv3等三层路由协议。 |
| 要求所投设备支持1对1、1对多、多对1和基于流的镜像；且支持RSPAN和ERSPAN |
| 支持专门针对CPU的保护机制，能够针对发往CPU处理的各种报文进行流量控制和优先级处理，保护交换机在各种环境下稳定工作。 |
| ▲支持同时开启IPv4、IPv6ACL、802.1X认证、web认证、防ARP欺骗，CPU保护功能同时开启，不会相互冲突、制约；提供国家级权威机构测试报告复印件作为证明。 |
| ▲支持ARP防欺骗功能，能够禁止非法用户的ARP欺骗报文，保护合法用户免受其害，防止合法用户的数据被窃取，提供国家级权威机构测试报告作为证明并厂商盖章确认。 |
| ▲支持抗攻击，支持CPU限速功能，能限制非法报文对CPU的攻击，保护交换机工作的稳定性，并提供国家级权威机构测试报告作为证明。 |
| ▲所投设备能检测到攻击源，并将攻击源隔离，保护交换机工作的稳定性，提供国家级权威机构测试报告作为证明并厂商盖章确认。 |
| ▲支持专门基础网络保护机制，增强设备防攻击能力，即使在受到攻击的情况下，也能保护系统各种服务的正常运行，保持较低的CPU负载，从而保障整个网络的稳定运行。以第三方权威机构测试报告为准并厂商盖章确认。 |
| 要求所投产品支持sFlow网络监测技术，可提供完整的第二层到第四层信息，可以适应超大网络流量环境下的流量分析，让用户详细、实时地分析网络传输流的性能、趋势和存在的问题。 |
| 支持虚拟化功能，最多可将9台物理设备虚拟化为一台逻辑设备统一管理，并且链路故障的收敛时间≤30ms。 |
| ▲符合国家低碳环保等政策要求，支持IEEE802.3az标准的EEE节能技术，要求提供官网截图并厂商盖章确认。 |
| 产品资质 | ▲提供工信部设备进网许可证复印件和入网测试报告并厂商盖章确认。 |
| ▲为证明所投产品厂家的信息技术服务能力，要求投标产品厂商为ITSS（信息技术服务标准）工作组成员。（提供官网工作组成员截图及查询链接并且厂商盖章确认） |
| ▲投标设备原厂商技术水平在国内同行业中居须处于领先地位，产业规模大，有较强的市场竞争能力和较大的市场覆盖面，须提供国家火炬计划重点高新技术企业认证证书（要求资质证书名称必须与设备制造厂商名称一致并且设备厂商盖章确认） |

**更正为：**

**4.1安全网关**

|  |  |
| --- | --- |
| 指标项 | 参数要求 |
| 产品形态 | ▲1、支持固化千兆电口≥8个，固化千兆光口≥4个。 |
| 2、支持双硬盘插槽，硬盘容量≥1T，硬盘支持可插拔更换、支持内存≥4GB。 |
| 3、标准1U机箱，多核非X86架构。 |
| 4、NAT转发吞吐率≥2.0Gbps；并发NAT连接数≥400W；新建NAT连接数≥1500。 |
| 5、支持流量识别保障功能：能够精确识别网络应用，保障关键业务的系统带宽，配置应用协议库，协议识别数量≥1500种。 |
| 6、配置URL数据库及应用特征库5年升级，另外URL数据库和应用特征库支持远程HTTP自动升级。 |
| 7、配置≥350个SSLVPN接入授权。 |
| 8、配置350路IpsecVPN接入授权。 |
| 功能参数 | 9、支持静态路由、RIP(V1/V2)、RIPng、OSPFv2等多种路由协议 |
| 10、为保证在多条外网线路情况下带宽的合理分配使用，设备必须支持多链路负载均衡，负载均衡可基于带宽、负载等多种方式。 |
| 11、支持正向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。 |
| 12、支持IPV6环境 |
| 13、支持状态检测防火墙功能，实现网络安全防护 |
| 14、▲支持网关、网桥等多种部署模式，灵活安装。 |
| 15、支持SNMPV2和V3版本，支持多TRAP接收主机配置。 |
| 16、支持DHCP功能，对内网提供DHCP服务。 |
| 17、支持VRRP(VirtualRouterRedundancyProtocol，虚拟路由冗余协议)。 |
| 18、DHCP地址池分配状态，可生成IP、MAC对应关系列表。 |
| 19、支持HTTPS和HTTP的WEB方式管理。 |
| 20、支持WEB本地认证方式、Radius认证、微信认证功能。 |
| 产品资质 | 21、为保障产品代码质量，供货厂商需通过CMMI4认证，提供证书复印件。 |
| 22、投标设备厂商具备自主研发、技术创新的能力，有独立的企业技术中心，或具备一定规模的实验室，有丰富的测试环境，获得国内或国际权威机构认可的证明文件，并且厂商盖章确认。 |

**4.2接入层交换机**

|  |  |
| --- | --- |
| 指标项 | 参数要求 |
| 产品形态 | ▲交换容量≥3.00Tbps，转发性能≥160Mpps。 |
| ▲固化10/100/1000M以太网端口≥48，固化1GSFP光接口≥4个；整机最大可用千兆口≥52。 |
| 要求所投设备MAC地址≥16K，ARP表项≥1000条,FIB表项≥500。 |
| 要求所投产品支持防雷等级10KV，提供第三方权威机构测试报告，或厂商的盖章确认说明。 |
| 功能参数 | 支持静态路由、RIP/RIPng、OSPFv2/OSPFv3等三层路由协议。 |
| 要求所投设备支持1对1、1对多、多对1和基于流的镜像；且支持RSPAN和ERSPAN |
| 支持专门针对CPU的保护机制，能够针对发往CPU处理的各种报文进行流量控制和优先级处理，保护交换机在各种环境下稳定工作。 |
| 支持同时开启IPv4、IPv6ACL、802.1X认证、web认证、防ARP欺骗，CPU保护功能同时开启，不会相互冲突、制约；提供国家级权威机构测试报告复印件，或厂商的盖章确认说明作为证明。 |
| 支持ARP防欺骗功能，能够禁止非法用户的ARP欺骗报文，保护合法用户免受其害，防止合法用户的数据被窃取，提供国家级权威机构测试报告或厂商的盖章确认说明作为证明。 |
| 支持抗攻击，支持CPU限速功能，能限制非法报文对CPU的攻击，保护交换机工作的稳定性，并提供国家级权威机构测试报告或厂商的盖章确认说明作为证明。 |
| 所投设备能检测到攻击源，并将攻击源隔离，保护交换机工作的稳定性，提供国家级权威机构测试报告或厂商的盖章确认说明作为证明。 |
| 支持专门基础网络保护机制，增强设备防攻击能力，即使在受到攻击的情况下，也能保护系统各种服务的正常运行，保持较低的CPU负载，从而保障整个网络的稳定运行。以第三方权威机构测试报告，或厂商的盖章确认说明作为证明。 |
| 要求所投产品支持sFlow网络监测技术，可提供完整的第二层到第四层信息，可以适应超大网络流量环境下的流量分析，让用户详细、实时地分析网络传输流的性能、趋势和存在的问题。 |
| 支持虚拟化功能，最多可将9台物理设备虚拟化为一台逻辑设备统一管理，并且链路故障的收敛时间≤30ms。 |
| 符合国家低碳环保等政策要求，支持IEEE802.3az标准的EEE节能技术，要求提供官网截图并厂商盖章确认。 |
| 产品资质 | ▲提供工信部设备进网许可证复印件和入网测试报告并厂商盖章确认。 |
| ▲为证明所投产品厂家的信息技术服务能力，要求投标产品厂商为ITSS（信息技术服务标准）工作组成员。（提供官网工作组成员截图及查询链接并且厂商盖章确认） |
| 投标设备原厂商技术水平在国内同行业中居须处于领先地位，产业规模大，有较强的市场竞争能力和较大的市场覆盖面，须提供高新技术企业认证证书，或产品发明专利梳理、国内外权威市场覆盖报告等设备厂商盖章确认证明。 |