广东省人民医院抗DDoS设备采购项目需求

一、项目名称：

广东省人民医院抗DDoS设备采购项目需求

二、项目要求

广东省人民医院为加强对互联网DDoS攻击的防护能力，现采购一套抗DDoS设备。要求抗DDoS产品可以主动将攻击流量牵引至设备内进行清洗，清洗完成后再将正常的访问流量重新注入医院网站服务器。要求设备具备毫秒级的攻击响应能力，具备基于源IP的多维度访问行为分析和AI聚类分析的CC防御技术等先进防护措施，从而保障医院对外服务在遭受网络DDoS攻击时仍能正常运行。

三、采购清单

采购设备及数量如下：

|  |  |  |
| --- | --- | --- |
| 序号 | 名称 | 数量 |
| 1 | 抗DDOS设备 | 1套 |

四、配置参数要求

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 参数项 | 指标项 | 参数 |
| 1　 | 硬件性能 | 硬件 | 标准机架式高性能抗DDoS设备，支持Bypass扩展插槽。 |
| 产品支持国产化CPU芯片（非必备）。 |
| 硬盘：≥20T。 |
| 接口 | 千兆电口≥4个，千兆光口≥4个，万兆光口≥6个,万兆多模光模块≥6，交流电源≥2。 |
| 散热 | 支持风扇冗余和可插拔更换，当风扇模块出现故障时，可以在设备不断电的情况下，对风扇模块进行更换。 |
| 2 | 管理要求 | 管理平台 | 支持集中管理DDOS检测和清洗功能。 |
| 支持通过集中的管理平台实现多台防御设备集中管理、性能监控，支持基于业务划分防护对象，定义防御策略，提供精细化防护；支持业务动态流量基线学习；支持攻击告警、攻击详情、清洗前后流量对比集中展示；支持抓包取证。首页实时监控至少支持攻击告警、设备入出流量对比、设备CPU利用率、IP流量TOPN等。 |
| 3 | DDOS检测功能 | 性能 | 实配检测性能≥10G，支持扩展≥20G。 |
| 网络层泛洪攻击检测及防御 | 支持对SYN Flood、SYN-ACK Flood、ACK Flood、FIN Flood、RST Flood、TCP Malformed、TCP链接耗尽、TCP Fragment Flood、UDP Flood、UDP Fragment Flood、ICMP Flood等常见网络层泛洪攻击识别及防御，支持各类TCP反射、UDP反射攻击的识别和阻断。 |
| 常见应用层攻击检测及防御 | 支持HTTP应用层Flood/HTTP CC识别及防御，支持HTTPS应用层Flood/HTTPS CC识别及防御，支持DNS Query Flood识别及防御。 |
| IPv4/IPv6共栈防御 | 支持IPV4/IPV6共栈防御。 |
| HTTP CC攻击防御能力 | 支持基于行为分析防御针对WEB、APP的HTTP CC/大资源高频请求攻击。 |
| 不解密防御高频HTTPS加密攻击 | 支持基于行为分析不解密防御针对WEB网站、APP的HTTPS应用层攻击。 |
| 报表功能 | 系统支持综合报表查询，报表内容包含攻击趋势、流量对比、攻击类型分布、攻击事件TOP N、流量TOP N等，支持报表导出。 |
| 4 | DDOS清洗功能 | 性能 | 实配清洗性能≥10G，支持扩展≥20G。 |
| 网络层泛洪攻击检测及防御 | 支持对SYN Flood、SYN-ACK Flood、ACK Flood、FIN Flood、RST Flood、TCP Malformed、TCP链接耗尽、TCP Fragment Flood、UDP Flood、UDP Fragment Flood、ICMP Flood等常见网络层泛洪攻击识别及防御，支持各类TCP反射、UDP反射攻击的识别和阻断。 |
| 常见应用层攻击检测及防御 | 支持HTTP应用层Flood/HTTP CC识别及防御，支持HTTPS应用层Flood/HTTPS CC识别及防御，支持DNS Query Flood识别及防御。 |
| IPv4/IPv6共栈防御 | 支持IPV4/IPV6共栈防御。 |
| HTTP CC攻击防御能力 | 支持基于行为分析防御针对WEB、APP的HTTP CC/大资源高频请求攻击。 |
| 不解密防御高频HTTPS加密攻击 | 支持基于行为分析不解密防御针对WEB网站、APP的HTTPS应用层攻击。 |
| 报表功能 | 系统支持综合报表查询，报表内容包含攻击趋势、流量对比、攻击类型分布、攻击事件TOP N、流量TOP N等，支持报表导出。 |
| 5 | 保修 | 保修 | 三年7\*24小时原厂免费上门保修 |

五、部署要求

所采用的产品和技术方案必须兼容采购人现有的网络，如果出现与现有设备不兼容的情况，由报价人负责解决，采购人不支付任何额外的费用。

 报价人负责采购人需求书中列出的所有工作内容，以及其他隐含的配套工作。报价人应充分考虑影响报价的各种因素和风险。采购人不再支付项目金额以外的任何费用。

 报价人必须确保设备硬件套件的完整性和可靠性。对于需求书没有列出，而对该项目的正常运行和维护必不可少的部件、配件和模块等，报价人有责任给予补充。

报价人应当负责本次采购设备的安装调试工作，由于医院业务要求网络7×24小时连续运行，因此，在安装新的设备时，必须尽量保证网络通信不中断。如果一定要暂停网络通信，则必须在预先计划好并得到批准的短暂时间内完成。为此，报价人应制定详细周密的安装配置和系统割接方案，并且这些方案应经过充分的磋商论证和实验证明，方可付诸实施，不允许出现计划外断网的状况。

 设备部署所需的线材由报价人提供，项目不再不支付任何额外的费用

 所有产品要求品牌与实际制造商一致，不要OEM或贴牌产品。报价人的技术指标应答必须与其报价中的设备一致，技术参数和指标必须是真实的；如果发现虚假夸大技术参数或不是所报价设备的技术参数，则按虚假应标处理。