|  |  |  |
| --- | --- | --- |
| 货物名称 | 技术标准及要求 | 数量 |
| 异常流量清洗 | 1、★标准19英寸机架式设备，提供≥4个全高宽业务插槽，满配交流电源。  2、★配置多核抗DDOS业务模块，可安插在全高宽业务槽中。吞吐容量≥25Gbps；最大并发连接≥2500万；提供≥4个万兆SFP+光口，≥24个千兆光接口。  3、支持扩展独立专业的8种类型以上安全板卡（如：防火墙业务板、IPS入侵防御、WAF业务板等），便于以后安全扩容需求，提供功能证明文件，不限于测试报告、官网和功能截图。  6、支持RIP、BGP、OSPF、MPLS组网，提供功能证明文件，不限于测试报告、官网和功能截图。  7、★支持畸形包攻击防范，支持针对协议漏洞的畸形包攻击防范，比如Land、Smurf、Fraggle、Tear Drop、Winnuke，提供功能证明文件，不限于测试报告、官网和功能截图。  8、支持流量型flood攻击 ： SYN Flood 、SYN-ACK Flood、ICMP Flood、UDP Flood、IP Fragment Flood。  9、应用型flood攻击 ：DNS Query Flood、DNS Reply Flood、HTTP Get Flood、CC。  10、DOS攻击 ：Ping of death、Land、Teardrop、Smurf；  11、支持安全策略基线配置功能，并支持自学习功能实现安全策略基线的更新。  12、支持DNS域名防护 、DNS反射攻击、DNS限速等防护手段，提供功能证明文件，不限于测试报告、官网和功能截图。  13、支持基于IP，协议，端口号三元组的精细化防范配置，可在防护对象下配置三元组业务，防范以三元组为最小粒度，提供功能证明文件，不限于测试报告、官网和功能截图。  14、★支持RIP/OSPF/ISIS/BGP路由协议发布的牵引方式，提供功能证明文件，不限于测试报告、官网和功能截图。  15、具备将检测发现的除DDOS攻击外的异常流量数据包实时导出的扩展能力，为未来进行深度分析、确定攻击特征、制定封堵策略等工作提供基础数据。  16、★支持通过策略路由、MPLS VPN、MPLS LSP、GRE VPN、二层透传等多种方式，将清洗后的干净流量回注给用户，用户正常的业务流量不受影响，提供功能证明文件，不限于测试报告、官网和功能截图。  17、管理中心支持相关业务管理功能（包括提供策略模板、建立清洗任务、引流、告警、自动配置等）、被保护对象管理功能、实施流量数据分析监控功能以及设备管理、报表功能、告警等；  18、支持对检测发现的针对任意指定地址或者地址段的各类攻击流量进行过滤，并能生成可采用人工方式部署到其他网络设备上的策略。  19、可以根据L2-7层协议特征定义业务流，并按需指定流量经过的物理/逻辑业务模块，提供功能证明文件，不限于测试报告、官网和功能截图。  20、具备将检测发现的除DDOS攻击外的异常流量数据包实时导出的扩展能力，为未来进行深度分析、确定攻击特征、制定封堵策略等工作提供基础数据。  21、系统支持以中文图表形式输出流量报表、安全报表、综合报表；支持doc、excel、pdf等格式的报表生成，并支持通过邮件等多种方式输出。报表支持日报、周报、月报和年报，并且支持对设备、IP群组、单台主机形式输出以上报表。  22、支持网管软件统一网管，支持SNMPv1、SNMPv2C、SNMPv3。  23、提供公安部销售许可证、《信息安全风险评估服务一级》资质；CMMI5证书。  24、★提供原厂商项目授权或合法来源渠道的证明文件（包括但不限于销售协议、代理协议等） | 1 |
| 异常流量检测 | 1、★支持与本次采购的异常流量清洗设备进行联动，实时配合下发清洗任务。  2、★设备吞吐容量≥8Gbps；最大并发连接≥250万；固定端口8个电口，24个千兆光接口；具备2个扩展槽，支持扩展万兆。  3、异常流量检测必须是现网销售产品，在官网能找到具体详细型号，并提供官网截图。  4、支持DPI检测功能。  5、支持DFI（Netflow，Sflow，Cflow，Netstream等flow协议）检测功能。  6、支持流量型flood攻击检测 ： SYN Flood 、SYN-ACK Flood、ICMP Flood、UDP Flood、IP Fragment Flood。  7、支持应用型flood攻击检测 ：DNS Query Flood、DNS Reply Flood、HTTP Get Flood、CC。  8、支持安全策略基线配置功能，并支持自学习功能实现安全策略基线的更新。  9、具备将检测发现的除DDOS攻击外的异常流量数据包实时导出的扩展能力，为未来进行深度分析、确定攻击特征、制定封堵策略等工作提供基础数据。  10、系统支持以中文图表形式输出流量报表、安全报表、综合报表；支持doc、excel、pdf等格式的报表生成，并支持通过邮件等多种方式输出。报表支持日报、周报、月报和年报，并且支持对设备、IP群组、单台主机形式输出以上报表。  11、支持网管软件统一网管，支持SNMPv1、SNMPv2C、SNMPv3。  12、★提供原厂商项目授权或合法来源渠道的证明文件（包括但不限于销售协议、代理协议等） | 1 |
| 流量清洗管理平台 | 1、★流量清洗管理平台与异常流量清洗、异常流量检测设备配套使用，可远程下发清洗任务，具备统一管理功能。  2、流量清洗管理平台支持相关业务管理功能（包括提供策略模板、建立清洗任务、引流、告警、自动配置等）、被保护对象管理功能、实施流量数据分析监控功能以及设备管理、报表功能、告警等；  3、流量清洗管理平台支持流量统计功能，包括互联网全局流量统计，基于各类用户和业务、各类流控策略、指定IP地址的流量统计；支持实时流量、历史流量的分析；  4、系统支持集中管理，可以支持http，https登陆，使用web操作，可多用户同时登陆管理中心。  5、支持账号分权分域管理，由管理员统一分配不同账号的管理权限和管理域。  6、系统具备统一管理平台，支持对多台设备的集中管理，日志收集，运行状态监控，策略下发。  7、支持告警和日志管理功能：支持攻击事件触发告警、支持告警通知（短信，邮件、声音）、支持告警过滤、支持自定义日志存储时间、支持告警日志和操作日志支持转储功能。  8、支持对设备运行状态、接口状态、CPU温度、风扇等重要关键部件实时监控。  9、支持操作员的创建，删除和修改，设置访问控制策略。设置登录参数，解除锁定用户。  10、对访问控制策略进行配置管理（创建，删除，修改），根据用户配置使用的访问控制策略进行访问控制。  11、支持TR-069管理协议，支持SNMP管理协议，提供功能证明文件，不限于测试报告、官网和功能截图。  12、★提供清洗管理中心平台配套机架式服务器，满足现网实际管理需求。  13、★提供原厂商项目授权或合法来源渠道的证明文件（包括但不限于销售协议、代理协议等） | 1 |