**奉化区电子政务外网违规外联监测项目技术参数**

随着政府信息化发展的不断深入，电子政务外网面临的安全挑战十分严峻。据近些年安全事件统计情况发现，电子政务外网上各类违规接入、私搭乱建等行为愈演愈烈，埋下了众多安全隐患，尤其是私建互联网出口等行为，严重的甚至可能导致电子政务外网被互联网黑客、境外情报机构等直接入侵破坏。

根据省大数据局下发的检测数据发现奉化区电子政务外网存在部分未知的互联网IP出口地址，对奉化区电子政务外网带来了未知的安全风险。通过建设网络资产与边界感知系统，在奉化区电子政务外网范围内实现通过网络流量分析、主动扫描探测等技术，对奉化区电子政务外网互联网违规出口进行全方位实时监测，及时发现、定位这些违规出口，可根据外联服务器获取的电子政务外网地址、互联网出口地址、首次发现时间和最后更新时间等信息对这些违规出口事件进行查处整改，消除这些未知的安全风险，守住奉化区电子政务外网合规出口。

| **指标大类** | **指标项** | **产品性能参数和要求** |
| --- | --- | --- |
| 总体要求 | ★产品资质 | 1.产品须获得中华人民共和国公安部的**《计算机信息系统安全专用产品销售许可证》**；2.产品须具有**《计算机软件著作权登记证书》**及**《软件评测报告》；** |
| 运行环境 | 1.系统采用B/S架构，管理员只需浏览器即可访问系统进行操作。2.产品要求集成数据库，无须再独立安装数据库系统，亦无须对数据库进行专门的维护。 |
| 使用界面 | 系统必须采用基于浏览器的用户界面，至少支持IE、Chrome浏览器。 |
| ★硬件参数 | 硬件规格 | 采用标准机架式的1U硬件设备，全内置封闭式结构，专用安全加固Linux操作系统。 |
| 硬件参数 | **QPS（TPS）：≥**2000个（IP）**并发处理数：≥**100万（数据包）**数量内存**：16GB（最大支持16GB\*2）**硬盘**：128GB硬盘**网络接口**：6个千兆电口，2个万兆光口**其他接口**：1个VGA接口，2个USB接口 |
| 性能指标 | **最大镜像流量**：20Gbps**最大扫描扫描速率：**50Mb/s**扫描耗时：**8个B类网段平均扫描耗时约40秒 |
| **主要功能** | 内外网互联行为发现 | ★1.在无需安装客户端的情况下，支持通过镜像流量分析自动发现管理域内同时连接内网和互联网的设备，可在外联服务器上取证，取证信息包含外联设备内网IP、外联出口IP、首次发现时间和最后更新时间等信息。**（需提供公安部信息安全产品检测中心等权威测评机构对该项功能的检测结果作为证明）。** |
| 2.不依赖于客户端和镜像流量分析，支持通过主动扫描自动发现管理域内同时连接内网和互联网的设备，可在外联服务器上取证，取证信息包含外联设备内网IP、MAC、外联出口IP、首次发现时间和最后更新时间等信息。 |
| 非授权外联（内外网交叉混用） | ★在无需安装客户端的情况下，支持自动发现管理域内曾经脱离内网并且连接过互联网的设备，可在外联服务器上取证，取证信息包含外联设备内网IP、外联出口IP、首次发现时间和最后更新时间等信息。**（需提供公安部信息安全产品检测中心等权威测评机构对该项功能的检测结果作为证明）。** |
| 线路外联 | 支持依赖客户端或不依赖客户端两种模式，自动发现内网某个网络设备（如：交换机、路由器等）同时连接内部网路和互联网等其他网络，造成内网设备潜在外联的重大隐患。上报内网外联网络设备管理口IP、MAC及外网出口IP地址等信息。 |
| 信息外泄 | 自动发现管理域内将内网应用系统或网站页面保存后拷贝至互联网计算机打开的疑似信息外泄行为，可在外联服务器上取证，上报发生外泄信息的设备内网IP、外泄时外网IP、首次发现时间、最后更新时间和外泄网址等信息。 |
| 资产管理 | 资产发现 | 采用多种技术手段，发现网络内存活的资产，并上报资产的IP、在线状态等信息。支持各类网络资产识别，包括：计算机设备、网络设备、安全设备、安防设备、办公设备、专用设备等。 |
| 配置管理 | 资产发现识别 | 1.支持信息采集的开关配置，支持手动触发重新扫描；2.支持资产扫描范围的配置；3.支持服务器区IP范围配置，增加识别服务器设备的准确性；4.支持交换机权限配置，配置信息包含：管理口IP、MAC地址、设备名称、设备别名、设备类型、厂商、所属部门、设备型号、负责人、所在位置、SNMP只读团体名； |
| 网关状态 | 支持展现管理端系统所管辖的单个或多个网关系统状态信息，展示内容包含：在线离线状态、设备序列号、所在地、时钟快照、镜像流量、镜像延迟、策略、网关版本信息。 |

注意：投标时需提供技术参数中标“★”要求提供的资料，并在合同签订时对技术参数中的功能逐一测试。