广东省职业病防治院网络安全设备采购公告

我院网络安全设备项目采用议价方式进行采购，欢迎符合资质的报价人前来参加。有关事项如下：

1. 项目编号：GDZFYSB202506-01
2. 项目名称：广东省职业病防治院网络安全设备采购项目
3. 最高限价（人民币）：17 万元整
4. 采购数量：2 台
5. 技术参数及配置要求

序号	产品名称	技术参数	数量
1	网络接入控制系统	详见附件	1 台
2	Web 应用防火墙	详见附件	1 台

6.设备验收：如属计量设备，验收时需提供计量合格或校准证书，计量或校准所产生费用由报价人承担。

7. 保修期：提供不少于 3 年的免费质保，终身维护；

8. 交货期：签订合同后 20 日内；

9. 合格报价人的基本条件：

（1）具有独立承担民事责任能力的在中华人民共和国境内注册的法人；

（2）报价人为所投产品的制造商或者代理商；

（3）报价人未被列入“信用中国”网站(www.creditchina.gov.cn)“记录失信被执行人或重大税收违法失信主体或政府采购严重违法失信行为”记录名单；不处于中国政府采购网(www.ccgp.gov.cn)“政府采购严重违法失信行为信息记录”中的禁止参加政府采购活动期间。（以提交报价文件截止之日在“信用中国”网站（www.creditchina.gov.cn）及中国政府采购网(www.ccgp.gov.cn)查询结果为准，如相关失信记录已失效，报价人需提供相关证明资料）。

10. 报价文件要求：

（1）对照“第 9 点”的相关证照复印件加盖公章；

（2）对照“第 5 点技术参数及配置要求” 提供用户需求书（响应表）。“★”号条款为议价时的重要参考指标，偏离将导致报价无效；带“▲”条款负偏离可能会严重影响议价结果；

（3）设备报价单（需注明产品的产地、品牌、型号、保修期、议价方式）。

（4）本项目**议价时间**为2025年6月23日下午4点，本项目**接受现场议价和电话议价两种方式，**报价公司请在报价文件封面及报价单内注明选择哪种方式议价。参加现场议价的公司代表请于**议价时间**到达本单位办公楼4楼会议室参加议价；选择电话议价请在2025年6月23日下午4点至5点时间段内保持联系电话畅通。如有特殊情况不能如期议价，将会电话通知已交报价文件公司联系人。

以上资料一式一份装在档案袋并密封好。档案封面上应注明议价项目编号、名称、报价公司名称、联络人及手机电话号码、参加的**议价方式**。

11. 符合资质的报价人请在 2025 年6月18日至 2025 年6月23日中午12点期间把响应文件递交(或邮寄) 到广州市海珠区新港西路海康街 68 号 。联系人：钟工， 联系电话：020-34063091。

附件：技术参数

1.网络接入控制系统

指标项	指标要求
★基本规格	标准 2U 机架式设备，配置标准国产化硬件平台，国产化操作系统标准 1U 设备，配置冗余双电源；配置≥6 个千兆电接口，≥4 个千兆光接口，≥2 个网络扩展插槽(可额外扩展千兆电口/光口、万兆光口)；≥8G 内存，配置≥128GB SSD 固态硬盘存储；具备终端设备的准入控制、用户身份认证、终端安全检查功能； 提供三年软件升级服务和三年原厂标准硬件维保服务。
	在同时开启网络安全准入、终端用户认证、终端安全检查的安全策略下，整机吞吐量≥4Gbps；支持管理≥500 个终端设备（提供≥300 个终端设备的准入控制授权，≥300 个用户身份认证授权，≥300 个终端安全检查授权）；
部署特性	支持纯串行、纯旁路、设备旁路部署、业务逻辑串行部署方式；通过集中管控平台，可实现全局安全策略给下级，执行结果和日志可以上报给集控管控平台。
	支持 HA 双机热备模式，可自动进行主/备模式切换；系统基于 Linux 内核自主开发的 OS 安全操作系统，并且支持双操作系统冷备，当常用系统出现故障，可以切换使用备用系统恢复业务。
准入控制特性	▲支持多种准入控制技术（802.1X、EVG、DHCP、ARP、SNMP、端口镜像、策略路由、透明网桥），并且支持至少四种以上准入技术的复用，如 802.1x、DHCP、端口镜像、策略路由混合部署。（提供产品功能截图）
	支持入网终端能够在安检结束后重定向到指定 Portal 页面，重定向页面支持 HTTP 协议、HTTPS 协议，并且可自定义端口的 WEB 服务。
	▲支持准入 IP/MAC 黑白名单管理功能，处于黑名单表中的 IP 和 MAC 会被准入设备判定为非法设备，处于白名单表中的 IP 和 MAC 会被准入设备信任。（提供产品功能截图）
	支持 Portal 登录门户自定义提示信息（中英文）、是否显示欢迎页、来宾入口、员工入口等。
	支持网络资产自动采集功能，并能够自动分类网络中的接入设备，如交换路由设备、PC 设备、服务器、IP 电话、网络打印机等，同时能够及时发现网络中出现的新设备，对外来终端的接入行为进行告警。
	▲支持在设备视图针对单个终端进行相关操作，包括设为可信、禁用来宾、强制下线、隔离、IP/MAC 绑定、重注册、探测等动作。（提供产品功能截图）
	支持发现内网私接 hub、非网管交换机等，能够及时产生告警并阻断接入设备入网；支持 Hub 下多个终端需分别认证才能入网。
	▲支持一机多网管控，根据终端所访问的目标地址，自动判断所属安全域，无需安装客户端，即可实现对目标网络的访问控制规则，在同一时间，只能访问一个网络，实现多网互斥访问。（提供产品功能截图）

身份认证特性	支持系统内置账号认证、Radius 认证、AD 域账号认证、LDAP 账号认证、证书认证、短信认证、OAuth 认证、动态令牌认证等多种身份认证方式，并且支持多种认证方式组合使用。
	▲支持证书本地管理和发放，实现数字证书的签发、审核、验证、吊销等全生命周期管理和维护。（提供产品功能截图）
	支持指定的时间段可以接入认证，其它时间不允许认证。
	支持来宾角色选择，能够设定来宾设备的访问权限和入网时长、员工可以为来宾申请来宾码，来宾使用来宾码可以接入网络、访客支持二维码扫描方式授权入网。
终端安全检查特性	▲支持终端入网的安全基线检查功能，包含 SP 补丁检查、系统补丁检查、系统时间检查、计算机名规范检查、防病毒软件检查（支持软件版本检查）、IP/MAC 绑定检查、Windows 防火墙检查、操作系统版本检查等。支持 linux 安全检查。（提供产品功能截图）
	支持终端入网的账号密码检查功能，包含账户安全检查、密码安全检查。
	▲支持终端入网的软件安全检查功能，包含进程红名单、进程黑名单、软件红名单、软件黑名单、软件白名单、系统服务检查。（提供产品功能截图）
	支持终端 USB 设备授权管控，可对终端外设（键盘、鼠标）、移动存储、其他 USB 设备设置允许或禁止使用；并且可自定义配置 USB 黑白名单功能，并支持免认证终端功能。
	▲支持终端入网环境安全检查功能，包含屏保检查、远程桌面检查、AD 域检查、WSUS 更新设置检查、共享资源检查。（提供产品功能截图）
	支持非法外联监控，通过 ping 或者 telnet 探测方式检测非法外联行为，执行向服务端发送报告或断开网络或提示客户端操作，支持 Linux 系统违规外联检查。
产品资质	★产品需符合 GB 42250-2022《信息安全技术 网络安全专用产品安全技术要求》等相关国家标准的强制性要求，提供有效证明材料。
	★产品具备市面上良好的信创操作系统、CPU 等扩展兼容能力，提供不少于 2 家国产化兼容互认证书及加盖原厂公章；
	▲产品具备先进的攻击防护能力，支持对网络攻击行为，如 Smurf 入侵、LAND 攻击、WINNUK 攻击等，能够对攻击行为的发现和告警，提供第三方权威检测机构出具的报告证明，报告中必须有此能力体现;
厂商资质	产品原厂商具备《CMMI 5 证书》，提供证书复印件。
	▲产品原厂商具备中国信息安全测评中心颁发的《国家信息安全测评信息安全服务资质证书》，认证等级为安全工程类三级或以上，提供证书复印件；

2.Web 应用防火墙

指标项	指标要求
★基本规格	标准 2U 机架式设备，配置标准国产化硬件平台，国产化操作系统，内存≥32GB，硬盘存储≥8TB，配备冗余双电源，配置≥4 个千兆电口，≥4 个千兆光口，≥2 个网络扩展插槽(可额外扩展千兆电口/光口、万兆光口)；提供三年 Web 应用防护特征库升级及原厂标准硬件维保服务；
	在同时 WEB 应用安全防护策略的情况下，整机吞吐量≥10G，最大并发 HTTP 连接数≥1000 万；HTTPS 吞吐量≥2Gbps;
部署模式	支持透明、旁路部署、单臂部署。
	▲支持智能部署，上线 WAF 设备能够自动感知 Web 网站 IP 和端口（提供产品功能截图）
	▲支持安装向导式部署，按照该部署方式可直接部署完成（提供产品功能截图）
	▲支持 NAT 环境下的用户识别能力（提供产品功能截图）
	支持链路绑定功能。
	支持对 Web 相关应用协议进行自定义，并提供详细协议分析变量。
WEB 防护特性	支持 SQL 注入、XSS 攻击检测与防护功能。
	▲支持 Web 恶意扫描防护的检测与攻击防御能力，需提供产品相关功能截图，提供中国信息安全测评中心、公安部计算机信息系统安全产品质量监督检验中心、国家知识产权局、中国软件测评中心、公安部安全与警用电子产品质量检测中心任意一家机构出具关于“Web 服务器恶意攻击的阻断方法”的检测报告或证书，证明功能有效性及加盖原厂公章；
	▲支持恶意重定向防护功能（提供产品功能截图）
	▲支持人机识别功能（提供产品功能截图）
	▲支持双引擎防护功能（提供产品功能截图）
	支持客户端访问控制功能，预防恶意客户端进行访问频率的多层次恶意访问。
	▲支持获取 Web 安全事件的原始攻击信息（提供产品功能截图）
	支持 Struts2 漏洞的攻击检测与防护。
	支持网页爬虫检测与防护功能。
	支持 WebShell 攻击检测与防护功能。
管理特性	支持手动执行产品升级。
	▲支持自动执行产品升级，不需要用户每次手动升级特征库（提供产品功能截图）
	支持公司网站应提供产品离线升级包下载。
	支持对登陆用户提供防暴力猜解功能，保障用户身份安全。
产品资质	★产品需符合 GB 42250-2022《信息安全技术 网络安全专用产品安全技术要求》等相关国家标准的强制性要求，提供有效证明材料。
	★产品具备市面上良好的信创操作系统、CPU 等扩展兼容能力，提供不少于 2 家国产化兼容互认

	证书及加盖原厂公章； ▲产品具有《WEB 应用防火墙认证证书》，提供证书复印件及加盖原厂公章； 产品具备国际信息安全领域权威的漏洞知识库《CVE》证书，提供证书复印及加盖原厂公章；
厂商资质	产品厂商自 2022 年 1 月 1 日以来获得国家信息安全漏洞共享平台(CNVD)颁发的“原创漏洞发现贡献单位”；提供证书复印件； 产品厂商自 2022 年 1 月 1 日以来获得国家信息安全漏洞库（CNNVD）年度“优秀技术支撑单位”；提供证书复印件；