达州市中级人民法院互联网安全设备采购项目更正公告

（招标编号：SCZZY2023(Z)003）

一、内容：

四川中卓耀工程项目管理有限公司受达州市中级人民法院的委托，对达州市中级人民法院互联网安全设备采购项目进行询价采购，现对招标项目“第五章 项目技术、商务及其他要求－三、技术服务要求”做如下更正，详附件。

二、监督部门

本招标项目的监督部门为达州市财政局。

三、联系方式

招 标 人：达州市中级人民法院

地　　址：达州市通川区白塔路301号

联 系 人：石老师

电　　话：0818-2121179

电子邮件：/

招标代理机构：四川中卓耀工程项目管理有限公司

地　　址：达达州市通川区东城张家湾路泰合巷34号

联 系 人：李老师

电　　话：17781946097

电子邮件：284254140@qq.com

招标人或其招标代理机构主要负责人（项目负责人）：_____（签名）

招标人或其招标代理机构：_____（盖章）

附件：

项目名称：达州市中级人民法院互联网安全设备采购项目

项目编码：SCZZY2023(Z)003

原招标文件：第五章 项目技术、商务及其他----三、技术服务要求

（一）互联网边界下一代防火墙技术参数要求

4.产品支持IPSec VPN智能选路功能，根据线路质量和应用实现自动链路切换；

7.支持基于网络区域、网络对象、MAC地址、服务、应用等维度进行访问控制策略设置；

10.支持对压缩病毒文件进行检测和拦截，压缩层数支持15层及以上；

△13.支持用户账号安全保护功能，包括用户账号多余入口检测、用户账号弱口令检测、用户账号暴力破解检测、失陷账号检测，防止因账号被暴力破解导致的非法提权情况发生；

△14.产品支持勒索病毒检测与防御功能，针对勒索病毒攻击设置专项安全策略；

15.支持对安全策略管理和审计功能，记录安全策略变更时间、变更账号、变更类型等内容，提升日常安全策略运维效率；

17.产品支持服务器漏洞防扫描功能，并对扫描源IP进行日志记录和联动封锁；

23.具备IT产品信息安全认证EAL4增强级

（二）互联网边界安全行为审计管理技术参数要求

3.支持部署在IPv6环境中，设备接口及部署模式均支持ipv6配置，所有核心功能（上网认证、应用控制、流量控制、内容审计、日志报表等）都支持IPv6；

7.支持PPS异常、丢包异常、ARP异常、内网DOS攻击等异常情况实时监测，显示每日异常事件个数及情况；

9.针对内网用户的web访问质量进行检测，对整体网络提供清晰的整体网络质量评级；

14.支持通过OAuth认证协议对接，支持阿里钉钉，口袋助理，企业微信第三方账号授权认证；

17.能够与同品牌下一代防火墙系统实现认证联动，同时部署产品后，可以实现认证同步机制，实现单点登录；

19.支持代理控制功能，不允许使用外部HTTP代理，不允许使用外部Sock4/5代理，不允许在HTTP，SSL一些的标准端口上使用其他协议；（比如在80端口上传输非HTTP协议数据，在443端口上传输非HTTPS协议数据等）；

（三）互联网终端安全管理技术参数要求

5.支持跳转链接至云端安全威胁响应系统，针对已发生的威胁提供详细的分析结果，包含威胁分析、网络行为、静态分析、分析环境和影响分析；

11.远程办公时，可联动终端安全管理软件在登录前进行检测，未检测通过无法登录； 不符合的检测项可以一键修改和查看修复指引；

12.支持端控安全环境检测、免端流量环境监测，对终端安全管理软件安装情况进行检查、对未装端的用户进行隔离及修复处置；

14.提供勒索病毒整体防护体系入口，直观展示最近七天勒索病毒防护效果，包括已处置的勒索病毒数量、已阻止的勒索病毒行为次数、已阻止的未知进程操作次数、已阻止的暴力破解攻击次数；

现更正为：第五章　项目技术、商务及其他----三、技术服务要求

（一）互联网边界下一代防火墙技术参数要求

4.产品支持IPSec VPN智能选路功能，根据线路质量和应用实现自动链路切换；（提供产品功能截图，并加盖投标人公章）

7.支持基于网络区域、网络对象、MAC地址、服务、应用等维度进行访问控制策略设置；（提供产品功能截图，并加盖投标人公章）

10.支持对压缩病毒文件进行检测和拦截，压缩层数支持15层及以上；（提供产品功能截图，并加盖投标人公章）

△13.支持用户账号安全保护功能，包括用户账号多余入口检测、用户账号弱口令检测、用户账号暴力破解检测、失陷账号检测，防止因账号被暴力破解导致的非法提权情况发生；

（提供产品相关功能截图，并提供公安部计算机信息系统安全产品质量监督检验中心、中国信息安全测评中心、中华人民共和国国家版权局之中任意一家检测机构出具关于“账号保护”的相关证书证明功能有效性）

△14.产品支持勒索病毒检测与防御功能，针对勒索病毒攻击设置专项安全策略；（提供产品相关功能截图，并提供公安部计算机信息系统安全产品质量监督检验中心、中国信息安全测评中心、中华人民共和国国家版权局之中任意一家检测机构出具关于“勒索病毒”的相关证书证明功能有效性）

15.支持对安全策略管理和审计功能，记录安全策略变更时间、变更账号、变更类型等内容，提升日常安全策略运维效率；（提供产品功能截图，并加盖投标人公章）

17.产品支持服务器漏洞防扫描功能，并对扫描源IP进行日志记录和联动封锁；（提供产品功能截图，并加盖投标人公章）

23.具备IT产品信息安全认证EAL4增强级（提供相关证明材料）

（二）互联网边界安全行为审计管理技术参数要求

3.支持部署在IPv6环境中，设备接口及部署模式均支持ipv6配置，所有核心功能（上网认证、应用控制、流量控制、内容审计、日志报表等）都支持IPv6；（提供产品功能截图，并加盖投标人公章）；

7.支持PPS异常、丢包异常、ARP异常、内网DOS攻击等异常情况实时监测，显示每日异常事件个数及情况；（提供产品功能截图，并加盖投标人公章）

9.针对内网用户的web访问质量进行检测，对整体网络提供清晰的整体网络质量评级；（提供产品功能截图，并加盖投标人公章）

14.支持通过OAuth认证协议对接，支持阿里钉钉，口袋助理，企业微信第三方账号授权认证；（提供产品功能截图，并加盖投标人公章）

17.能够与同品牌下一代防火墙系统实现认证联动，同时部署产品后，可以实现认证同步机制，实现单点登录；（提供产品功能截图，并加盖投标人公章）

19.支持代理控制功能，不允许使用外部HTTP代理，不允许使用外部Sock4/5代理，不允许在HTTP，SSL一些的标准端口上使用其他协议；（比如在80端口上传输非HTTP协议数据，在443端口上传输非HTTPS协议数据等）；（提供产品功能截图，并加盖投标人公章）；

现增加20.提供产品三年质保、软件升级服务。

（三）互联网终端安全管理技术参数要求

5.支持跳转链接至云端安全威胁响应系统，针对已发生的威胁提供详细的分析结果，包含威胁分析、网络行为、静态分析、分析环境和影响分析；（提供产品功能截图，并加盖投标人公章 ）

11.远程办公时，可联动终端安全管理软件在登录前进行检测，未检测通过无法登录；

不符合的检测项可以一键修改和查看修复指引；（提供产品功能截图，并加盖投标人公章）

12.支持端控安全环境检测、免端流量环境监测，对终端安全管理软件安装情况

进行检查、对未装端的用户进行隔离及修复处置；（提供产品功能截图，并加盖投标人公章）

14.提供勒索病毒整体防护体系入口，直观展示最近七天勒索病毒防护效果，包括已处置的勒索病毒数量、已阻止的勒索病毒行为次数、已阻止的未知进程操作次数、已阻止的暴力破解攻击次数；（提供产品功能截图，并加盖投标人公章 ）