**大庆市人民医院银行专线边界UTM（安全网关）系统采购项目公告**

大庆市人民医院银行专线边界UTM（安全网关）系统采购。本项目为大庆市人民医院与龙江银行合作项目。面向各类型企业进行采购，欢迎有能力的国内供应商参加。

依据庆财采【2018】9号文相关条款，采用竞争性谈判采购方式采购。

**一、项目编号：****LR-2020-003**

**二、项目名称：****大庆市人民医院银行专线边界UTM（安全网关）系统采购**

**三、采购方式：****竞争性谈判**

**四、技术需求及数量**

本项目预算：96,000.00元，参与谈判供应商谈判最终报价超出预算的谈判无效。详见第二部分“项目需求”。

**五、供应商资格条件**

除符合《中华人民共和国政府采购法》中有关供应商申请取得政府采购资格的相关条件外，还应符合下述资格条件：

1、提供参与本项目竞争供应商有效的营业执照或事业单位法人证书。

2、提供参与本项目竞争供应商有效的电子与智能化工程专业承包资质证书。

3、提供参与本项目竞争供应商有效的安全生产许可证证书。

4、单位负责人为同一人或者存在直接控股、管理关系的不同供应商，不得参加同一合同项下的政府采购活动。

5、参与本项目的供应商需提供所投产品的《检验检测报告》，要求级别为增强级或以上。

6、本项目不接受联合体参与。

**六、获取文件**

本项目使用纸质标书参与谈判(一正三副)。咨询电话：0459-6612123

1、获取文件时间：公告之日起至2020年 6 月 5 日截止。

注：请参与本项目谈判的供应商在2020年 6 月 5 日 16 时 30 分前自助下载招标文件，逾期则无法下载招标文件，由此造成的后果由供应商自行承担。

2、网上自助下载文件的方式、程序及流程

详见：<https://www.dqsrmyy.com/>

**七、退出竞争时限**

如供应商退出竞争，必须在提交竞价文件截止时间前48小时，否则不予退出。

**八、谈判文件售价：免费**

**九、谈判时间及地点(如有 变化，另行通知)**

1、提交谈判响应文件截止时间及谈判时间：2020年 6 月 9 日 13 时 30 分。

2、谈判地点：大庆市人民医院 。

采购单位：大庆市人民医院

采购单位地址：大庆市人民医院

采购单位联系人： 李永光

采购单位联系方式：6612123

邮 编：163311

日期：2020年 6 月 2 日

**项目需求**

UTM系统 1套

1. 标准1U机架式设备，内置专用安全操作系统，配置单电源；提供千兆电口数量≥6个，支持Bypass。
2. 防火墙吞吐量≥10Gbps、最大并发连接数≥380万、每秒新建连接数≥50万；
3. 提供三年硬件维保服务，三年入侵防御特征库升级服务、三年防病毒特征库升级服务、三年应用识别库升级服务
4. 支持基于硬件Hypervisor技术的底层虚拟化，各个虚拟防火墙之间完全隔离，可运行不同的防火墙版本；可配置任意虚拟防火墙的CPU核心数量、网络接口数量、内存大小、存储空间大小，提供功能截图并加盖制造商公章；
5. 每个虚拟防火墙均提供完整的安全功能，包括防火墙、入侵防御、防病毒、上网行为管理和流控、VPN、IPv4/IPv6双栈等；
6. 支持基于接口/安全域、地址、用户、服务、应用和时间的防火墙访问控制策略；
7. 支持基于接口/安全域、地址、用户、服务、应用和时间的会话控制策略，包括总连接数控制、每秒总新建连接数控制、每IP总连接数控制、每IP新建连接数控制；
8. ★具备APT防御功能，可对exe、rtf、pdf、xls（x）、ppt（x）、doc（x）、pps（x）、swf、rar、zip等常见的格式进行动态沙箱分析，可对rtf、pdf、xls（x）、ppt（x）、doc（x）、pps（x）做PE内嵌检测，并且能指出文件偏移位置; 提供功能截图并加盖制造商公章；
9. 支持策略预编译技术，在大量防火墙访问控制策略情况下整机性能不受影响；
10. 支持并开通网络入侵检测及防御功能，入侵防御事件库事件数量不少于4000条；
11. 可基于IP地址、网段、用户、时间、VLAN、协议类型等条件设定入侵防御模块的检测事件及响应方式；
12. 具备协议自动识别功能；支持自定义事件功能；
13. 提供SQL注入攻击、XSS攻击的检测和防御功能，对Web服务系统提供保护，
14. 支持对文件感染型病毒、蠕虫病毒、脚本病毒、宏病毒、木马、恶意软件等过滤，病毒库数量不少于1000万；
15. 支持并开通基于DPI和DFI技术的应用特征识别及行为控制，应用识别的种类不少于1000种；
16. 支持并开通基于URL分类库的WEB访问管理，URL分类库规模不少于2000万条；
17. 支持并开通基于线路和多层通道嵌套的带宽管理和流量控制功能；
18. 支持静态路由、动态路由（RIP、OSPF、BGP4）；
19. 支持基于入接口、源地址、目标地址、服务端口、应用类型的策略路由；
20. 支持并开通链路负载均衡，提供轮询、加权轮询、哈希等多种负载均衡算法；
21. 支持通过ICMP、TCP、DNS和HTTP协议实现对链路可用性的多重健康检查；
22. 支持基于威胁情报云的动态防护功能，防火墙支持将用户对互联网的访问信息发送至威胁情报云进行实时情报查询及防护；
23. ★支持SD-WAN功能，可对SD-WAN隧道的时延、抖动、带宽占用率、丢包率等提供可视化展示，提供功能截图并加盖制造商公章；
24. 支持DNS透明代理功能，可将指定范围内的DNS请求自动重定向至管理员指定的DNS服务器，且支持多台DNS服务器的负载均衡；
25. 支持标准DNS服务器功能，支持多种DNS 记录 ，包括A ，NS，CNMAE，TXT，MX，PTR记录；
26. 支持基于WEB和命令行的设备管理模式，WEB界面和命令行模式下均可实现对设备所有功能的管理配置；
27. 支持整机威胁统计和展示，包括基于地理位置的威胁地图展示、基于威胁级别和威胁类型的统计分析、基于威胁事件源/目的主机的TOP10统计展示、基于具体威胁事件/威胁类型的TOP10统计展示等，统计展示的时间周期包括1小时/1天/7天/30天；
28. 支持基于流量的TOP100用户和TOP100应用的流量曲线图，流量曲线图的统计周期包括小时、天、7天和30天；
29. 支持基于并发会话数量的TOP100用户和TOP100应用的并发数量曲线图，并发数量曲线图的统计周期包括小时、天、7天和30天；

**注：1.要求设备为原厂原装且产品交付前最新生产未被使用过的全新产品，具有设备的合法使用权； 3年质保服务（含防病毒、入侵防御、上网行为模块特征库3年升级服务），原厂商提供免费上门安装、调试。**

**2.参与本项目投标供应商要求提供7X24小时服务，针对报修的一般性故障应在30分钟内处理完成，较大故障应在2小时内处理完成，重大故障应在12小时处理完成，全程维护保障。**