深圳市宝实置业有限公司关于

采购网络信息安全设备及配套服务的询价函

各单位：

我司拟开展网络信息安全设备及配套服务采购招标工作，现邀请贵单位根据相关法规及采购要求对本次计划采购的网络信息安全设备及配套服务进行报价。本次询价结果可能作为我司评估该项目采购费用的参考依据，请贵单位在保证能提供采购需求的网络信息安全设备及配套服务前提下报价。

请贵单位于2025年5月16日前将营业执照复印件、报价函等材料（加盖公章）扫描件发至邮箱zhangjinjun@szbsjt.sihc.com.cn ，原件资料提交（或邮寄）至深圳市宝安区三区金融街建安一路9号恒明珠国际金融中心21楼。

特此函达。

附件：1.网络信息安全设备及配套服务采购需求

1. 报价函

深圳市宝实置业有限公司

2025年5月9日

（联系人：张进军，联系电话：13501569190）

附件1

网络信息安全设备及配套服务采购需求

一、采购背景

根据我司新桥东先进产业园区及企业内部网络信息安全保障需求，为保障新桥东园区及企业内部办公的网络信息安全，结合网络信息安全保障的实际要求，拟采购2套防火墙、2套网络行为管理设备、2套统一端点安全管理设备、1套零信任管理设备、1套Web应用防护设备、2年安全托管服务、2人/年驻场服务。

1. 项目名称

深宝实网络信息安全设备及配套服务采购

三、采购内容

（一）需求内容

|  |  |  |  |
| --- | --- | --- | --- |
| 采购项目 | 规格型号 | 单位 | 数量 |
| 防火墙一 | 1、网络层吞吐量：10G，应用层吞吐量：5G，防病毒吞吐量：1G，IPS吞吐量：1G，全威胁吞吐量：800M，并发连接数≥200万，每秒新建连接数≥6万；  2、产品不少于8个10/100/1000M以太网电口，2个千兆SFP光口，2个USB口和1个RJ45串口，单个电源；  3、产品支持多对一、一对多和一对一等多种地址转换方式；  4、支持路由模式、透明模式、链路聚合模式、旁路镜像模式等多种部署方式；  5、支持服务器漏洞防扫描功能；  6、支持多种SSL VPN用户认证方式，至少包括本地密码认证、LADP认证；  7、支持链路连通性检查功能，支持基于3种以上协议对链路连通性进行探测，探测协议至少包括DNS解析、ARP探测、PING和BFD等方式；  8、支持异常数据包攻击防御，防护类型包括IP数据块分片传输防护、Teardrop攻击防护、Smurf攻击防护、Land攻击防护等攻击类型。 | 套 | 1 |
| 防火墙二 | 1、网络层吞吐量：4G，应用层吞吐量：2G，防病毒吞吐量：600M，IPS吞吐量：1.5G，全威胁吞吐量：1G，并发连接数≥200万，每秒新建连接数≥6万；  2、产品不少于8个10/100/1000M以太网电口，2个千兆SFP光口，2个USB口和1个RJ45串口，单个电源；  3、产品支持多对一、一对多和一对一等多种地址转换方式；  4、支持路由模式、透明模式、链路聚合模式、旁路镜像模式等多种部署方式；  5、支持服务器漏洞防扫描功能；  6、支持多种SSL VPN用户认证方式，至少包括本地密码认证、LADP认证；  7、支持链路连通性检查功能，支持基于3种以上协议对链路连通性进行探测，探测协议至少包括DNS解析、ARP探测、PING和BFD等方式；  8、支持异常数据包攻击防御，防护类型包括IP数据块分片传输防护、Teardrop攻击防护、Smurf攻击防护、Land攻击防护等攻击类型。 | 套 | 1 |
| 网络行为管理设备 | 1、网络层吞吐量≥5.8 Gbps，应用层吞吐量≥750Mbps，带宽性能≥500Mbps，用户数≥1000，准入终端数：500，准入终端数的扩容上限：1000，每秒新建连接数≥1万,最大并发连接数≥50万；  2、不少于6个以太网电口，单个电源，8G内存，128G固态硬盘；  3、支持两台及两台以上设备同时做主机的部署模式；  4、支持客户端SSL解密，客户端会自动推送根证书安装；  5、支持在设置流量策略后，根据整体线路或者某流量通道内的空闲情况，自动启用和停止使用流量控制策略，以提升带宽的高使用率；线路空闲值可自定义；  6、支持MAB免认证，通过MAC地址绑定实现终端设备的免认证接入。  7、支持根据IP、端口、协议等自定义应用规则；支持根据端口设定用户不允许访问的目标IP组提供的服务；支持根据不同的应用类型或具体的某种应用设置允许或拒绝；  8、支持显示设备实时CPU、内存、磁盘占有率（存储）、在线用户数、系统时间、网络接口等信息。 | 套 | 2 |
| 统一端点安全管理设备 | 1、支持管控10000个客户端；  2、支持对系统账号信息进行梳理，了解账号权限分布概况以及风险账号分布情况，支持通过账号名、主机、账号状态、root 权限、账号修改周期进行过滤筛选。  3、为Windows停更的系统提供专项防护，包括漏洞防护、文件防护、暴破入侵防护、系统脆弱点识别和风险端口封堵等多项核心功能；  4、支持自定义拦截终端软件弹窗；  5、为确保统一端点安全管理系统的联动检测能力，产品在远程办公时，可联动本产品在登录前进行检测，未检测通过无法登录；  6、可实时监控文件的状态，在文件读、写、执行或者进入主机时主动进行扫描，支持根据用户性能偏好至少3种防护级别；  7、可通过多维度引擎进行漏斗式检测，保障查杀效果在低误报率的情况下保持高检出率。 | 套 | 2 |
| 零信任管理设备 | 1、产品不少于6个1000M以太网电口，2个1000M SFP口，支持2个USB口和1个RJ45串口，单个电源；  2、最大理论加密流量≥300Mbps，最大理论建议并发用户数≥400，最大理论https并发连接数≥15000，理论https新建连接数≥60个/秒；  3、为充分利用零信任的网络性能，综合网关部署时支持配置聚合网口，并支持将聚合网口作为综合网关的网络部署IP。聚合网口支持通过哈希或802.3ad等标准对闲置网口进行网口绑定，支持通过ARP探测机制对聚合网口进行健康检查。  4、web模式下发布应用资源时，应支持智能改写等模式，以合理适配较规范化的业务系统及复杂老旧的非常规站点。  5、PC和移动端的零信任客户端支持中文或英文。  6、本地集群下各节点的零信任授权数均可共享使用，集群的总接入授权数是各节点授权数的总和。  7、为简化管理员配置工作，提升业务上线效率，对于一些主要在主站点中点击使用的子站点WEB业务系统，且子站点跟主站点业务系统权限一致的场景，零信任系统应支持开启依赖站点功能，并支持采集站点功能对依赖站点进行梳理。 | 套 | 1 |
| Web应用防护设备 | 1、网络层吞吐量≥4G，HTTP应用层吞吐量≥300M，HTTP并发连接数≥150万，HTTP每秒新建连接数≥6万；  2、产品不少于6个10/100/1000M以太网电口，2个千兆SFP光口，支持2个USB口和1个RJ45串口，单个电源；  3、产品支持透明桥接、透明代理、反向代理、旁路分析等多种部署模式；  4、产品支持不同角色赋予不同权限，针对所有导航栏赋予管理员不同的访问导航栏；针对单个应用程序赋予某个用户管理权限；针对单个策略赋予某个用户是否具备查看、编辑、创建权限。  5、产品支持设置HTTP 请求和响应Cookie的最大长度，超出最大长度可配置触发告警及拦截  6、产品内置特征码总数不低于7000，提供可查看具体特征描述；  7、产品支持违反模型的违规行为（包含不正确的请求方法、未授权的URL访问、未授权内容类型、未知参数、参数长度不符、参数类型不符）可作为自定义策略筛选条件，以便于针对某些重要业务接口做基于模型的精细化零信任安全策略数类型不符进行拦截；  8、支持识别业务系统的登录行为及用户信息，对登录失败行为做拦截，对已失陷用户发起的攻击事件，能在告警日志展示WEB登录用户。 | 套 | 1 |
| 安全托管服务 | 1、采用7\*24小时现场应急响应；在48小时内须输出紧急响应服务结果报告，报告内容须包括所遇到的安全问题、安全事故处理过程、处理结果；在72小时内须找出该安全问题发生的原因，并从根本上解决问题，确保相同原因引发的安全问题不再发生；2、7\*24小时威胁鉴定：应当具备云端检测和分析平台，通过采集安全设备和工具的安全告警和安全日志，结合大数据分析、人工智能等技术手段，提供7\*24小时持续不间断的安全威胁分析鉴定，同时在用户界面进行展示；  3、为了保证安全监测的准确率和服务质量，应当支持招标方自定义配置安全规则，以满足日益复杂的安全趋势所带来的安全监测需求；  4、提供一个威胁情报的安全通报工单，工单内容包含威胁情报的基本信息和推送信息以及跟进记录，要求明确说明关联资产信息的排查情况；  5、安全专家每月对安全设备的防护策略进行检查，确保安全设备上的安全策略始终处于最优水平，针对威胁能起到最好的防护效果。云端服务平台应当具备丰富的策略检查工具，支持排查安全设备防护策略配置的合理性；  6、提供7\*24小时的安全守护，不论是白天、黑夜、节假日都应该能做到7\*24H在线服务，并且在节假日期间应当每日提供《节假日值守总结》。 | 年 | 2 |
| 驻场服务 | 1、提供IT运维工程师现场驻点项目进行网络、机房维护服务和安全监测服务；  2、人员具备3年或以上大型机房（300平方米以上）网络\运维经验；  3、拥有至少CCNA或HCNA及以上相关证书。 | 人/年 | 2 |

（二）交货时间

以招标方实际需求为准。

四、成果交付及验收标准

供应商按采购方要求的时间完成网络信息安全设备及配套服务交付，经采购方验收且验收合格后签《验收单》。

附件2

网络信息安全设备及配套服务采购报价函

致：深圳市宝实置业有限公司

根据贵公司关于采购网络信息安全设备及配套服务询价函的相关要求，经研究和核算相关文件后，我方在保证能提供采购需求的网络信息安全设备及配套服务前提下，愿以人民币

（单位：万元）报价。

网络信息安全设备及配套服务采购需求报价表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **产品名 称** | **规格型号/技术参数** | **单价（元）** | **数量** | **单位** | **小计（元）** |
| 防火墙一 | 1、网络层吞吐量：10G，应用层吞吐量：5G，防病毒吞吐量：1G，IPS吞吐量：1G，全威胁吞吐量：800M，并发连接数≥200万，每秒新建连接数≥6万；  2、产品不少于8个10/100/1000M以太网电口，2个千兆SFP光口，2个USB口和1个RJ45串口，单个电源；  3、产品支持多对一、一对多和一对一等多种地址转换方式；  4、支持路由模式、透明模式、链路聚合模式、旁路镜像模式等多种部署方式；  5、支持服务器漏洞防扫描功能；  6、支持多种SSL VPN用户认证方式，至少包括本地密码认证、LADP认证；  7、支持链路连通性检查功能，支持基于3种以上协议对链路连通性进行探测，探测协议至少包括DNS解析、ARP探测、PING和BFD等方式；  8、支持异常数据包攻击防御，防护类型包括IP数据块分片传输防护、Teardrop攻击防护、Smurf攻击防护、Land攻击防护等攻击类型。 |  | 1 | 套 |  |
| 防火墙二 | 1、网络层吞吐量：4G，应用层吞吐量：2G，防病毒吞吐量：600M，IPS吞吐量：1.5G，全威胁吞吐量：1G，并发连接数≥200万，每秒新建连接数≥6万；  2、产品不少于8个10/100/1000M以太网电口，2个千兆SFP光口，2个USB口和1个RJ45串口，单个电源；  3、产品支持多对一、一对多和一对一等多种地址转换方式；  4、支持路由模式、透明模式、链路聚合模式、旁路镜像模式等多种部署方式；  5、支持服务器漏洞防扫描功能；  6、支持多种SSL VPN用户认证方式，至少包括本地密码认证、LADP认证；  7、支持链路连通性检查功能，支持基于3种以上协议对链路连通性进行探测，探测协议至少包括DNS解析、ARP探测、PING和BFD等方式；  8、支持异常数据包攻击防御，防护类型包括IP数据块分片传输防护、Teardrop攻击防护、Smurf攻击防护、Land攻击防护等攻击类型。 |  | 1 | 套 |  |
| 网络行为管理设备 | 1、网络层吞吐量≥5.8 Gbps，应用层吞吐量≥750Mbps，带宽性能≥500Mbps，用户数≥1000，准入终端数：500，准入终端数的扩容上限：1000，每秒新建连接数≥1万,最大并发连接数≥50万；  2、不少于6个以太网电口，单个电源，8G内存，128G固态硬盘；  3、支持两台及两台以上设备同时做主机的部署模式；  4、支持客户端SSL解密，客户端会自动推送根证书安装；  5、支持在设置流量策略后，根据整体线路或者某流量通道内的空闲情况，自动启用和停止使用流量控制策略，以提升带宽的高使用率；线路空闲值可自定义；  6、支持MAB免认证，通过MAC地址绑定实现终端设备的免认证接入。  7、支持根据IP、端口、协议等自定义应用规则；支持根据端口设定用户不允许访问的目标IP组提供的服务；支持根据不同的应用类型或具体的某种应用设置允许或拒绝；  8、支持显示设备实时CPU、内存、磁盘占有率（存储）、在线用户数、系统时间、网络接口等信息。 |  | 2 | 套 |  |
| 统一端点安全管理设备 | 1、支持管控10000个客户端；  2、支持对系统账号信息进行梳理，了解账号权限分布概况以及风险账号分布情况，支持通过账号名、主机、账号状态、root 权限、账号修改周期进行过滤筛选。  3、为Windows停更的系统提供专项防护，包括漏洞防护、文件防护、暴破入侵防护、系统脆弱点识别和风险端口封堵等多项核心功能；  4、支持自定义拦截终端软件弹窗；  5、为确保统一端点安全管理系统的联动检测能力，产品在远程办公时，可联动本产品在登录前进行检测，未检测通过无法登录；  6、可实时监控文件的状态，在文件读、写、执行或者进入主机时主动进行扫描，支持根据用户性能偏好至少3种防护级别；  7、可通过多维度引擎进行漏斗式检测，保障查杀效果在低误报率的情况下保持高检出率。 |  | 2 | 套 |  |
| 零信任管理设备 | 1、产品不少于6个1000M以太网电口，2个1000M SFP口，支持2个USB口和1个RJ45串口，单个电源；  2、最大理论加密流量≥300Mbps，最大理论建议并发用户数≥400，最大理论https并发连接数≥15000，理论https新建连接数≥60个/秒；  3、为充分利用零信任的网络性能，综合网关部署时支持配置聚合网口，并支持将聚合网口作为综合网关的网络部署IP。聚合网口支持通过哈希或802.3ad等标准对闲置网口进行网口绑定，支持通过ARP探测机制对聚合网口进行健康检查。  4、web模式下发布应用资源时，应支持智能改写等模式，以合理适配较规范化的业务系统及复杂老旧的非常规站点。  5、PC和移动端的零信任客户端支持中文或英文。  6、本地集群下各节点的零信任授权数均可共享使用，集群的总接入授权数是各节点授权数的总和。  7、为简化管理员配置工作，提升业务上线效率，对于一些主要在主站点中点击使用的子站点WEB业务系统，且子站点跟主站点业务系统权限一致的场景，零信任系统应支持开启依赖站点功能，并支持采集站点功能对依赖站点进行梳理。 |  | 1 | 套 |  |
| Web应用防护设备 | 1、网络层吞吐量≥4G，HTTP应用层吞吐量≥300M，HTTP并发连接数≥150万，HTTP每秒新建连接数≥6万；  2、产品不少于6个10/100/1000M以太网电口，2个千兆SFP光口，支持2个USB口和1个RJ45串口，单个电源；  3、产品支持透明桥接、透明代理、反向代理、旁路分析等多种部署模式；  4、产品支持不同角色赋予不同权限，针对所有导航栏赋予管理员不同的访问导航栏；针对单个应用程序赋予某个用户管理权限；针对单个策略赋予某个用户是否具备查看、编辑、创建权限。  5、产品支持设置HTTP 请求和响应Cookie的最大长度，超出最大长度可配置触发告警及拦截  6、产品内置特征码总数不低于7000，提供可查看具体特征描述；  7、产品支持违反模型的违规行为（包含不正确的请求方法、未授权的URL访问、未授权内容类型、未知参数、参数长度不符、参数类型不符）可作为自定义策略筛选条件，以便于针对某些重要业务接口做基于模型的精细化零信任安全策略数类型不符进行拦截；  8、支持识别业务系统的登录行为及用户信息，对登录失败行为做拦截，对已失陷用户发起的攻击事件，能在告警日志展示WEB登录用户。 |  | 1 | 套 |  |
| 安全托管服务 | 1、采用7\*24小时现场应急响应；在48小时内须输出紧急响应服务结果报告，报告内容须包括所遇到的安全问题、安全事故处理过程、处理结果；在72小时内须找出该安全问题发生的原因，并从根本上解决问题，确保相同原因引发的安全问题不再发生；2、7\*24小时威胁鉴定：应当具备云端检测和分析平台，通过采集安全设备和工具的安全告警和安全日志，结合大数据分析、人工智能等技术手段，提供7\*24小时持续不间断的安全威胁分析鉴定，同时在用户界面进行展示；  3、为了保证安全监测的准确率和服务质量，应当支持招标方自定义配置安全规则，以满足日益复杂的安全趋势所带来的安全监测需求；  4、提供一个威胁情报的安全通报工单，工单内容包含威胁情报的基本信息和推送信息以及跟进记录，要求明确说明关联资产信息的排查情况；  5、安全专家每月对安全设备的防护策略进行检查，确保安全设备上的安全策略始终处于最优水平，针对威胁能起到最好的防护效果。云端服务平台应当具备丰富的策略检查工具，支持排查安全设备防护策略配置的合理性；  6、提供7\*24小时的安全守护，不论是白天、黑夜、节假日都应该能做到7\*24H在线服务，并且在节假日期间应当每日提供《节假日值守总结》。 |  | 2 | 套 |  |
| 驻场服务 | 1、提供IT运维工程师现场驻点项目进行网络、机房维护服务和安全监测服务；  2、人员具备3年或以上大型机房（300平方米以上）网络\运维经验；  3、拥有至少CCNA或HCNA及以上相关证书。 |  | 2 | 人/年 |  |
| 总价（元） | | | | | |

我们承诺如下，并承担相应的法律责任：

一、我方所提供的文件资料均真实无误及有效，因我方提供资料不实而造成的责任和后果由我方承担。

二、报价为含税价。报价已包含本次网络信息安全设备及配套服务采购的税费（增值税专用发票，税率13%）人工成本费、运输费、服务费、材料费、租赁费、劳务费、差旅费、办公费、打印费等全部费用。

三、此次报价仅作为项目前期公开询价，与最终投标价格无关。

报价单位：

单位地址：

联系人：

联系方式：

日期： 年 月 日