**招标文件**

**项目名称：****国贸物业网络安全设备采购项目**

**项目编号：GMWY-2017-29**

**招标人：厦门国贸物业管理有限公司**

**厦门国贸物业管理有限公司**

**2017年 6月**

# 招标项目说明与要求

## 项目背景

厦门国贸物业管理有限公司（以下简称公司）在网络及信息系统使用过程中暴露出一些网络及信息安全问题。为全面解决物业公司网络及信息系统存在的安全问题，拟采购一批网络安全设备。

## 招标项目一览表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 货物名称 | 技术参数 | 数量 | 备注 |
| 1 | SSL VPN设备 | 详见本章 | 1台 |   |
| 2 | 下一代防火墙设备 | 详见本章 | 2台 |   |
| 3 | 边界隔离网关设备 | 详见本章 | 1台 |  |
| 4 | 上网行为审计设备 | 详见本章 | 1台 |  配置2个1000M口AP（2.4G/5G） |
| 5 | 一体化网关设备 | 详见本章 | 20台 |  按需采购 |

## 主要技术参数要求（带★参数为必须满足项）

### 招标货物一览表

#### SSL VPN设备

|  |  |  |
| --- | --- | --- |
| 指标项 | 技术及服务项目 | 参数说明 |
| 设备要求 | 数量 | 1 |
| 保修 | 三年软硬件维保、三年软件升级服务 |
| 基础项要求 | 性能要求 | ★1、标准1U机架尺寸，独立非插卡式VPN硬件设备，配备≥4个千兆电口，支持并发SSL并发SSL用户数≥800，授权并发SSL用户数≥500，SSL加密速度≥200Mbps；每秒新建用户数≥75。配备IPSec VPN功能，不限IPSec VPN数量（移动用户除外），支持与第三方国际标准IPSec VPN对接，支持隧道间路由功能。支持并开启授权并发用户数≥100 的APP应用封装模块。 |
| 部署要求 | 2、支持网关模式、单臂（旁路）模式、多机热备模式、集群模式、分布式模式。 |
| 便利性要求 | 3、支持终端使用包括Win7、Mac、Linux等操作系统、支持IE、Firefox、Safari、Google Chrome、Opera等浏览器来登录SSLVPN系统，并完整支持各类应用。（提供Win7、Mac、Linux下各种浏览器的使用截图） |
| 加密算法 | ★4、产品应支持国际通用标准的商用密码密码算法（简称“商密”），包括：AES、DES、3DES、DH、RSA、RC4、MD5、SHA1等；产品可扩展支持中国国家标准的商用密码算法（简称“国密”），包括：SM1（含SCB2），SM2、SM3、SM4。（提供以上所有项界面截图证明） |
| 统一门户 | ★5、可支持虚拟门户功能，在一台设备上配置不同的访问域名、IP地址，以及不同的使用界面，实现一台设备为多个不同用户群体服务的的使用效果。(提供虚拟门户设备截图证明) |
| 单点登录 | ★6、支持单点登录功能（SSO）,支持移动用户登录VPN后再登录内部B/S、C/S应用系统时不需要二次重复认证。（需提供单点登录截图证明） |
| 核心功能 | 中间人防护 | ★7、产品必须支持防中间人攻击，在用户登录SSLVPN时智能判断存在中间人攻击行为，断开被攻击的连接，并可提示异常现象和记录攻击日志。（提供中间人攻击页面配置截图）； |
| 专线功能 | 8、支持客户端注销后自动清除所有缓存、Cookies、浏览器历史记录、保存的表单信息，实现零痕迹访问；支持VPN专线功能，可配置用户在接入SSL VPN的同时，断开与Internet其他连接。 |
| 权限分配 | ★9、产品应具有用户/用户组细粒度的权限分配功能：可以针对被访问资源的IP地址、端口、提供的服务、URL地址等进行权限控制；针对同一B/S资源，可对不同用户做到细致到URL级别的授权；支持主从认证账号绑定，必须实现SSL VPN账号与应用系统账号的唯一绑定，VPN资源中的系统只能以指定账号登陆，加强身份认证，防止登录SSL VPN后冒名登录应用系统。（需提供主从账号绑定截图证明） |
| 用户认证 | ★10、产品必须支持Local DB 、USB KEY、短信认证、硬件特征码、动态令牌、数字证书认证、LDAP、RADIUS、等认证方式；可针对用户/用户组设置认证方式的与、或组合，可进行用户名/密码、LDAP、USB KEY、硬件特征码、短信认证或动态令牌的五因素捆绑认证 。（提供以上认证选项功能界面截图证明） |
| CA认证 | ★11、设备内部必须支持自建CA中心，便于数字证书认证平台搭建(提供内置CA中心页面截图)；支持与基于PKI体系的第三方CA进行结合认证 ，可根据CA某字段将通过CA认证的用户自动映射到指定用户组，方便进行权限授权配置；支持CRL证书撤销列表；单台VPN设备可扩展同时支持5套以上CA根证书；(提供5套以上CA根证书页面截图证明) |
| 多网接入 | ★12、必须支持至少4条以上的外网多线路配置；并在设备单臂部署模式下，多线路接入前置网关，仅依靠SSLVPN设备同样可实现SSLVPN接入用户的多线路自动优选功能（提供配置界面截图证明）； |
| 自动寻址 | ★13、支持启用多线路时，自动检测故障线路，并自动踢出故障线路；一旦线路恢复，可在一定时间内自动恢复。支持启用多线路时，自定义用户访问选路策略，包括按上/下行带宽，轮询，按优先级等方式；支持利用网页进行动态寻址的方法，客户端不安装插件、不依靠IP地址库、不依赖于第三方动态IP寻址、直接根据速度探测实现用户端接入线路的自动优选,用户通过访问寻址代理页面（Webagent页面）自动寻找VPN设备IP(非DDNS）。（提供Webagent配置截图证明）； |
| 智能优化 | ★14、支持针对不同的web页面进行数据优化，支持动态压缩技术，基于数据流进行压缩，减少不必要的数据传输。（提供web优化截图证明） |
| 远程应用发布 | ★15、产品必须支持远程应用发布功能，无需二次开发，把Windows应用发布到移动智能终端中或将C/S资源Web化；手机客户端必须经过苹果公司官方检测，并发布在苹果官方应用商店appstore，产品客户端必须通过google公司官方检测并发布在google应用商店PlayGoogle；产品客户端必须支持非“越狱”或非“Root”权限的手机/PAD安装。（提供远程应用发布，苹果官方应用商店手机客户端截图证明）； |
| ★16、支持远程应用使用本地输入法；支持本地输入法和远程服务器输入法可切换，在小屏幕或网络带宽差的情况下，支持在本地先批量输入文字再点击发送，避免零散数据在广域网上的频繁交互；远程应用发布应该支持云存储，能够将手机、PAD、PC电脑中的文档、照片等上传到云端，或下载到本地终端，并实现基本的复制、剪切、粘贴、新建、重命名等操作；产品必须支持经过集成的，基于Android IOS平台的第三方软件开发包（SDK），并实现基于Android IOS平台第三方应用软件（APP）代码量不超过20行。（要求提供代码Demo和企业证明）平台提供自动APP代码嵌入功能，在系统中添加APP应用可自动生产嵌入SDK代码的APP安全应用，实现App应用的安全加固 （提供APP自动封装界面截图证明）； |
| 应用权限控制 | 17、远程应用发布必须支持应用权限控制项，不得通过远程应用访问任何未经授权的windows资源，至少应该包括：未经授权的应用程序、注册表、任务管理器、资源管理器、控制面板、cmd命令提示行、Win+R运行命令行、管理选型、映射网络驱动器选型、断开网络驱动器选型、回收站、网上邻居等。并支持隐藏本地原有磁盘，仅提供公共磁盘； |
| 协议优化 | ★18、支持改写WindowsRDP协议，经改写的协议必须独立于OS运行环境，避免跨平台兼容性问题，针对图像数据，服务端必须支持有损压缩算法；服务端必须能够支持过滤动态内容（gif/flash/video）以减少传输流量，且根据客户需要配置。（提供RDP改写页面配置截图证明） |
| 生厂商资质 | 19、生产商资质：软件研发体系国际认证CMMI5、售后服务体系通过ISO9001认证，国家密码管理局发布的《SSL VPN技术规范》起草单位之一。 |
| 产品资质 | ★20、产品资质：提供产品IPV6 Ready认证证书，并在全球IPV6测试中心官网可查，SSL VPN必须在近四年内至少曾有一年在中国国内市场占有率为前三名，提供权威的第三方机构数据证明。 |
| 兼容性要求 | 设备联动 | ★21、为保障设备安全联动，要求与下一代防火墙和上网行为审计为同一品牌。 |

#### 下一代防火墙设备

|  |  |  |
| --- | --- | --- |
| 指标项 | 技术及服务项目 | 参数说明 |
| 设备要求 | 数量 | 2【★双机热备】 |
| 保修 | 三年软硬件质保与三年软件及病毒库升级服务 |
| 基础项要求 | 性能要求 | ★1、标准2U机架式设备，配置16个千兆电口，8个千兆光口，4个万兆光口。整机吞吐量80Gbps，应用层吞吐量45G。最大并发会话数≥1800万，硬盘大小≥500G，每秒新建会话数≥65万，支持槽位扩展（无须重新配置参数）。 |
| 基本功能 | ★2、 支持包过滤，网络地址转换，状态检测，应用流量识别，应用层安全防护，用户控制，深度内容检测，支持并开启不限IPSec VPN数量，支持隧道间路由功能，支持SSLVPN功能。支持统一安全运维管理； |
| 部署要求 | 3、支持路由、透明、旁路、虚拟网线，混合模式+ |
| 策略路由 | ★4、为保障网络中应用的高效运行，应具备应用层流量的引流，支持针对应用的策略路由（提供基于应用的策略路由的配置页面截图证明）； |
| 模块要求 | ★5、为保证整体网络安全，所投设备必须支持威胁的分析发现与防护并重，因此必须具备威胁发现功能：威胁情报预警与处置、业务系统实时漏洞分析功能，具备威胁防御功能：敏感信息泄漏防护、服务器保护、恶意链接防护(需提供以上威胁发现、威胁防护所有功能界面截图，并可提供实际测试)； |
| 模块联动 | ★6、为保证能有效防护大规模攻击，所投设备必须具备并开启web应用防护、入侵防御、僵尸网络的联动封锁功能，可智能生成临时规则封锁攻击源IP，临时封锁时间可自定义（需提供入侵防护、web应用防护、僵尸网络设置联动封锁配置功能截图证明、设置IP冻结时间，设置时间自动刷新封锁IP列表的截图证明，并可提供实际测试）；  |
| 脚本检测 | 7、为保证网络安全，必须具备PHP,JSP,ASPX等主流脚本语言编写的webshell后门脚本上传检测功能；  |
| 关键URL认证 | ★8、为保证网络安全，必须支持对重要业务系统提供重要URL或者其他应用服务的短信认证机制（提供至少包括web、rdp、pptp、nntp、rlogin等四种以上服务进行短信认证加强登录防护的配置截图证明，并可提供实际测试）； |
| 核心功能 | 基本功能 | ★9支持并开启IPSec VPN、SSL VPN、APT检测、IPS入侵防护、WEB攻击防护、网页篡改防护、病毒防护。 |
| Web防护能力 | ★10、为保证网络安全，应支持WEB行为进行过滤，提供Web攻击防护、Web远控木马防护等功能，web应用防护能力通过开源web应用安全项目组（OWASP）评测认证，并且在OWASP的25项评测要求中，获得满分（五星）评测项在19项（含）以上（提供OWASP认证证书以及对应的web攻击防护能力测评报告）； |
| Web扫描 | 11、为实现对业务系统的安全分析，支持Web漏洞扫描功能，可分析web网站各类漏洞，包括SQL盲注，LDAP注入，存储型跨站脚本，操作系统命令，文件包含等脚本漏洞（需提供以上五类详细的漏洞扫描截图证明）； |
| 僵尸网络监测 | 12、为保证网络流量安全纯净，必须支持对PC终端、服务器是否变成了僵尸肉鸡进行检测，识别特征总数在50万条以上（需提供木马远控、恶意链接、移动安全、异常流量的僵尸网络检测功能截图证明、僵尸网络识别库超过50万条的界面截图，并可提供实际测试）； |
| 异常连接检测 | 11、支持异常连接检测，对21，22，25，53，69，80/8080，110，143，443等常见端口的协议异常流量检测，并支持RDP和SSH端口反弹链接检测； |
| 恶意连接防护 | 12、当前互联网威胁变化迅速，为保证网络安全能及时防护最新威胁，设备需具备终端请求恶意链接检测拦截功能，提供接入云端安全联动功能； |
| 异常流量监测 | 13、支持对内网主机外发的异常流量进行检测，如ICMP，UDP，SYN，DNS Flood等DDoS攻击行为，支持外网对内网主动发起的异常流量进行检测，如ICMP，UDP，SYN，DNS Flood等DDoS攻击行为； |
| 攻击分析 | ★14、为实现安全可视化，应支持对各类威胁行为进行深度分析，输出网络总存在的威胁问题，并对各类威胁行为输出有效攻击次数和攻击趋势；（提供具备有效攻击、攻击趋势的威胁报告证明，并可提供实际测试）  |
| 安全可视化 | ★15、为加强管理员对网络安全的了解，需要在设备首页多维度的展示发现的安全威胁，如入侵风险，实时漏洞风险，僵尸主机威胁，数据风险，被防护网站黑链风险，对外Dos攻击和攻击者地图等，并支持将所有发现的安全问题进行归类汇总列为待处理问题，针对给出相应的解决方法指引（要求提供首页界面展示入侵风险，实时漏洞风险，僵尸主机威胁，数据风险，被防护网站黑链风险，对外Dos攻击和攻击者地图等7大功能界面截图，并提供针对待处理问题相对应的解决方案指引截图）； |
| 热点事件分析 | ★16、为保证能够抵抗新型安全威胁，设备必须提供最新的威胁情报信息，能够对新爆发的流行高危漏洞进行预警和自动检测，发现问题后支持一键生成防护规则（要求提供设备发布最新威胁情报信息、自动进行预警检测以及一键生成防护规则的功能截图）； |
| 安全评估 | 17、网络安全建设是长期的过程，需要定期的做安全评估，因此设备必须支持针对服务器的漏洞风险评估功能，支持对ftp、mysql、oracle、mssql、ssh、rdp、netbios、vnc等应用的弱密码扫描，扫描完成后生成安全风险评估报告并自动添加安全策略(为了保障与防火墙之间智能联动，要求提供内置风险分析功能模块的界面截图证明、提供支持上述所有应用的弱密码扫描功能截图证明、同时能查看针对扫描出来的风险自动添加策略的界面截图)； |
| 黑链检测 | ★18、设备必须支持对被防护网站是否被挂黑链进行检测，支持显示TOP5黑链主机及黑链（游戏、色情、反动及非法内容等）类型分布、危害或影响，同时支持在设备界面提供参考解决方案（提供提供识别赌博、游戏、色情、广告等黑链的功能界面截图）； |
| 口令防护 | ★19、设备必须支持对常见应用服务（FTP、SSH、TELNET、SMTP、IMAP、POP3、RDP、SMB、VNC）和数据库软件（MySQL、Oracle、MS SQL）的口令暴力破解防护功能（必须提供以上所有对常见应用服务和数据库软件的口令暴力破解防护功能界面截图）； |
| 产品资质 | 20、产品应具备计算机信息系统安全专用产品销售许可证； |
| ★21、产品经过国际知名实验室NSS Labs测试，并获得recommended推荐级别（提供NSS Labs相关测试报告）； |
| ★22、要求厂商具备优秀的技术创新实力，提供防火墙产品入围GARTNER魔力象限的证明（需提供防火墙产品入围GARTNER魔力象限截图证明）； |
| 23、产品具备ICSA labs认证证书（提供证明材料） |
| 厂商资质 | ★24、为保证产品功能稳定性及可靠性，厂商应通过CMMI5级认证（提供证书复印件证明） |
| ★25、所投品牌厂商是第二代防火墙标准（GA／T 1177-2014）起草单位之一（提供相关证明复印件）； |
| 兼容性要求 | 设备联动 | 26、★为保障设备安全联动，要求与SSL VPN和上网行为审计为同一品牌。 |

1.3.1.3 上网行为审计

|  |  |  |
| --- | --- | --- |
| 设备要求 | 数量 | 1 |
| 保修 | 三年软硬件质保与三年URL库升级 |

|  |  |  |
| --- | --- | --- |
| 基础项要求 | 网络接口 | ≥6个千兆电口 |
| 存储介质 | ≥128G SSD硬盘 |
| 尺寸 | ≥1U机架式 |
| 吞吐量 | ≥2Gbps |
| 用户规模 | ≥4500 |
| 部署模式 | 必须支持两台及两台以上设备同时做主机的部署模式 |
| 智能选路 | ★1、采用基于网关或网桥的线路自动选路方法的技术,能够为上网用户智能的选择最快的上网线路,并且设备需要支持网关、网桥、旁路等多种部署模式 (必须提供国家权威机构出具的网关，网桥自动选路此技术的证明文件并加盖投标人公章) |
| 用户认证 | 2、支持本地用户名/密码认证、第三方认证（Radius、LDAP、POP3等）以及IP/MAC绑定，并且能够支持USB-KEY双因素的用户身份认证，通不过认证的用户禁止上网，并且能够根据需要进行差异化的策略认证；支持与LDAP服务器结合进行优化，便于客户实现策略管理在AC上进行，用户管理在域上进行，不需同步用户到本地组织结构中即可实现策略管理功能 |
| 网页过滤 | 3、支持根据访问的URL、网页关键字进行网页过滤，支持设置拒绝以IP访问网页行为；支持在放行URL时，自动放行主域名的子链接中被禁止的网站，保证网页显示完整；必须支持未知网页的自动识别与分类（提供界面证明） |
| 规则库 | 4、设备内置应用识别规则库，支持超过4600条应用规则数，支持超过2100种以上的应用，650种以上移动应用，并保持每两个星期更新一次，保证应用识别的准确率（提供产品界面截图） |
| 核心功能 | 短信认证 | 5、支持短信认证方式，用户输入手机号作为用户名，通过短信猫或短信平台发送验证码；短信认证能够根据不同用户推送不同认证页面，该认证页面可自定义，编辑内容包括文字、颜色风格、图片，且图片支持轮询播放（提供界面证明） |
| Web访问质量 | ★6、支持针对内网用户的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；支持以列表形式展示访问质量差的用户名单；支持对单用户进行定向web访问质量检测（以上各条需提供产品界面截图） |
| 微信和二维码认证 | ★7、支持与微信结合的认证方式，用户关注微信公众号后即通过身份认证，后台记录用户ID；支持与第三方微信平台无缝对接，不需要修改第三方微信平台代码；支持二维码认证，管理员扫描访客的二维码后对其网络访问授权 |
| 内容审计 | 8、支持记录加密的和明文的邮件内容、BBS发帖以及聊天内容审计；必须能审计木马、病毒、恶意脚本和插件、端口扫描等危险行为；必须能审计来自外网访问内网网站，在内网服务器下载上传下载文件，发帖的行为；支持指定用户扩展支持通过USB-Key免审计的功能；必须能审计来自外网访问内网网站、在内网服务器下载上传文件、在内网服务器发贴、从内网服务器上收发邮件的行为 |
| 热点管理 | ★9、支持能自动发现网络中通过无线上网的热点和移动终端的IP和终端类型；支持管理员配置热点信任列表；支持发现信任列表外非法接入的热点和终端，并阻止该热点/终端上网；支持将非法热点接入网络的行为通过邮件告警通知管理员，并在数据中心支持行为记录和查询；支持以图表方式显示移动终端接入趋势（提供产品界面截图） |
| AP管理 | 10、支持并开启无线AP管理功能（授权不于10个），能够直接查看到接入点状态、射频状态、无线网络状态、接入用户状态（所有项提供产品界面截图）支持基于SSID维度的上网权限、上网审计、上网安全、终端提醒、和流控等策略 |
| 认证联动 | ★11、为提高兼容性，保证用户认证和权限一致性，要求上网行为管理设备支持与下一代防火墙设备为同一品牌设备，进行用户认证信息共享，包括本地密码认证、外部密码认证、手机短信验证、单点登录和dkey认证信息在上网行为管理和防火墙设备之间的转发及接收（提供认证信息共享的产品界面截图） |
| 安全功能 | 网站安全 | 12、采用基于网关、网桥防范网络钓鱼网站的技术，支持识别并过滤SSL加密的非法网站、钓鱼网站、金融购物网站等，保证浏览网页的安全性；必须支持基于关键字过滤SSL加密的论坛、BBS上的发贴行为，同时支持允许用户浏览帖子但不准发贴功能（提供国家权威机构出具的网关，网桥防范网络钓鱼此技术的证明文件并加盖投标人公章） |
| 脚本安全 | 13、支持识别执行脚本的网页，并过滤脚本中隐藏木马等程序的网页（必须提供国家权威机构出具的网络插件安全检查方法此技术的证明文件并加盖投标人公章） |
| 管理功能 | 流量控制 | ★14、支持基于应用类型、网站类型和文件类型划分与分配带宽；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；空闲值可自定义（提供界面证明）支持通过抑制P2P的下行流量，来减缓P2P的上行流量，从而解决网络出口在做流控后仍然压力较大的问题（提供界面证明） |
| 高性能日志模式 | 15、支持日志高性能模式处理，精简冗余日志（提供产品界面截图） |
| 外置数据中心支持服务器虚拟化 | ★16、提供自有品牌的免费服务器虚拟化产品与外置DC联动，服务器虚拟化能够根据实际用户和流量规模合理分配硬件资源，保障最优资源分配。同时，外置DC能够与服务器虚拟化底层联动，优化磁盘读写，提高查询速度（提供自有品牌服务器虚拟化软件截图证明） |
| 应用标签 | 17、支持根据标签选择应用，标签分类至少包含安全风险、高带宽消耗、发送电子邮件、降低工作效率、外发文件泄密风险、主流论坛和微博发帖6大类；支持弱特征识别等相关技术，以应对P2P软件种类多、版本多、更新快的问题；必须支持无插件封堵浏览器配置公网代理服务器和通过代理软件代理上网行为（提供设备操作界面截图证明） |
| 产品资质与认证 | 18、设备生产厂商售后服务体系通过ISO9001认证（提供证书复印件） |
| ★19、设备生产厂商的研发体系通过国际认证CMMI5（提供证书复印件） |
| 具备下一代互联网网络审计系统/增强级《计算机信息系统安全专用产品销售许可证》、《中国国家信息安全产品认证证书》、IPv6 Ready Phase-2认证、《销售许可证（互联网公共上网服务场所）》。 |
| 兼容性要求 | 设备联动 | ★20、为保障设备安全联动，要求与下一代防火墙和SSL VPN为同一品牌。 |

1.3.1.4 边界隔离网关

|  |  |  |
| --- | --- | --- |
|  指标项 | 技术及服务项目 | 参数说明 |
| 设备要求 | 数量 | 1 |
| 保修 | 三年硬件维保与软件升级 |
| 基础项要求 | 性能要求 | 1. ★标准1U机架式设备，单电源，配置4个千兆电口 ，三层吞吐量≥2Gbps，应用层吞吐量≥400M，最大并发会话数≥25万，硬盘大小≥SSD 32G，每秒新建会话数≥1.5万；
 |
| 基本功能 | ★2、支持包过滤，网络地址转换，状态检测，应用流量识别，应用层安全防护，用户控制，深度内容检测，支持IPSec VPN，支持统一安全运维管理；开通入侵防御检测模块， 支持并开启IPSec VPN、SSL VPN、APT检测、IPS入侵防护、WEB攻击防护、网页篡改防护、病毒防护。 |
| 策略路由 | 3、为保障网络中应用的高效运行，应具备应用层流量的引流，支持针对应用的策略路由（提供基于应用的策略路由的配置页面截图证明）； |
| 模块要求 | ★4、为保证整体网络安全，所投设备必须支持威胁的分析发现与防护并重，因此必须具备威胁发现功能：威胁情报预警与处置、业务系统实时漏洞分析功能，具备威胁防御功能：敏感信息泄漏防护、服务器保护、恶意链接防护(需提供以上威胁发现、威胁防护所有功能界面截图，并可提供实际测试)； |
| 模块联动 | 5、为保证能有效防护大规模攻击，所投设备必须具备web应用防护、入侵防御、僵尸网络的联动封锁功能，可智能生成临时规则封锁攻击源IP，临时封锁时间可自定义（需提供入侵防护、web应用防护、僵尸网络设置联动封锁配置功能截图证明、设置IP冻结时间，设置时间自动刷新封锁IP列表的截图证明，并可提供实际测试）；  |
| 脚本检测 | 6、为保证网络安全，必须具备PHP,JSP,ASPX等主流脚本语言编写的webshell后门脚本上传检测功能；  |
| 异常流量监测 | 13、支持对内网主机外发的异常流量进行检测，如ICMP，UDP，SYN，DNS Flood等DDoS攻击行为，支持外网对内网主动发起的异常流量进行检测，如ICMP，UDP，SYN，DNS Flood等DDoS攻击行为； |
| 攻击分析 | ★14、为实现安全可视化，应支持对各类威胁行为进行深度分析，输出网络总存在的威胁问题，并对各类威胁行为输出有效攻击次数和攻击趋势；（提供具备有效攻击、攻击趋势的威胁报告证明，并可提供实际测试）  |
| 安全可视化 | ★15、为加强管理员对网络安全的了解，需要在设备首页多维度的展示发现的安全威胁，如入侵风险，实时漏洞风险，僵尸主机威胁，数据风险，被防护网站黑链风险，对外Dos攻击和攻击者地图等，并支持将所有发现的安全问题进行归类汇总列为待处理问题，针对给出相应的解决方法指引（要求提供首页界面展示入侵风险，实时漏洞风险，僵尸主机威胁，数据风险，被防护网站黑链风险，对外Dos攻击和攻击者地图等7大功能界面截图，并提供针对待处理问题相对应的解决方案指引截图）； |

1.3.1.5 一体化网关

|  |  |  |
| --- | --- | --- |
| 指标项 | 技术及服务项目 | 参数说明 |
| 设备要求 | 数量 | 20 |
| 保修 | 三年硬件维保与软件升级 |
| 基础项要求 | 性能要求 | ★1、标准1U机架式设备，单电源，配置2个WAN(1000M)、1个LAN（1000M）、10个LAN(100M) 、1个DMZ(1000M) ，三层吞吐量≥200Mbps，IPSec vpn加密速度≥40Mbps，最大并发会话数≥2万，； |
| 基本功能 | ★2、支持包过滤，网络地址转换，状态检测，应用流量识别，应用层安全防护，用户控制，深度内容检测，支持统一安全运维管理 支持并开启IPSec VPN。 |
| 策略路由 | 3、为保障网络中应用的高效运行，应具备应用层流量的引流，支持针对应用的策略路由（提供基于应用的策略路由的配置页面截图证明）； |
| 用户认证、审计 | ★4、WEB认证，IP-MAC绑定，IP/MAC认证，自动创建帐号。实时记录日志包括访问的时间、上网行为操作的拒绝/通过、主机的IP、访问对象的类型、访问对象的名称等 |
| 广告营销 | 5、基于特定用户或者终端实现广告页面的推送。 |
| 应用识别规则 | 6、应用识别规则库、可手工添加基于“深度内容检测”技术的新应用协议识别规则，实现个性化识别和封堵，提供无限扩展能力 |
| 访问控制 | ★7、以半小时为单位，支持任意的时间段设置；支持每天多个时间段设置；支持每周七天每天各不相同的时间 段设置，为客户提供最灵活的时间段控制能力 |
| 流控 | 8、允许指定用户使用P2P行为，但对其占用的带宽资源进行管理和控制、将出口中指定的带宽资源划分，并将指定的带宽资源分配给指定对外提供访问的服务器，实现对外发布 应用的保障 |
| 防火墙 | ★9、支持抵御来自公网的DoS攻击，支持对爆发于内部网络的DoS攻击进行检测和防御 网的DoS。支持对内网ARP欺骗的防御。内置基于状态监测的企业级防火墙，提供网关设备安全、组织内网安全双重保护 |
| 路由交换集中管理 | ★10、支持局域网划分VLAN， 通过VLAN访问控制，可允许或者拒绝VLAN之间的访问。支持DNAT、SNAT等多种NAT地址转换策略。支持DHCP服务功能。支持SC集中管控，实现配置策略下发，软件升级、管理维护等 |
| 安全可视化 | ★11、为加强管理员对网络安全的了解，需要在设备首页多维度的展示发现的安全威胁，如入侵风险，实时漏洞风险，僵尸主机威胁，数据风险，被防护网站黑链风险，对外Dos攻击和攻击者地图等，并支持将所有发现的安全问题进行归类汇总列为待处理问题，针对给出相应的解决方法指引（要求提供首页界面展示入侵风险，实时漏洞风险，僵尸主机威胁，数据风险，被防护网站黑链风险，对外Dos攻击和攻击者地图等7大功能界面截图，并提供针对待处理问题相对应的解决方案指引截图）； |
| 兼容性要求 | 设备联动 | ★12、为保障设备安全联动，要求与下一代防火墙和SSL VPN为同一品牌。 |

## 技术响应要求

1、投标人须提供投标设备的品牌、型号、详细配置及主要技术参数、性能说明及功能介绍，同时还应提供各主要部件的生产厂家、品牌及型号。

2、投标人必须提供所投标设备的全套配置清单（含数量及型号）。

3、投标人提供的货物必须为品牌机，产品应符合国家有关标准。

4、★为接入统一管理平台，保障产品间的有效对接和联动，整合完整高效的解决方案，防止重复建设，所投安全产品（SSLVPN、下一代防火墙、上网行为审计 ）应为同一品牌。

5、投标人应明确投标产品和招标要求存在正负偏离情况。

## 商务要求

### 供应商资质要求与投标资格证明文件

1、★投标人应具有独立的法人资格，注册资本应在人民币1000万元及以上或等值外币，并提供经年检的法人营业执照（副本）有效复印件；

2、投标人代表若不是法定代表人的，应提供法定代表人授权书原件；

3、★本项目最高控制价为人民币50万元整。

4、★投标人若不是投标全部货物制造商的，必须提供其获得货物的制造商或制造商在中国的合法分支机构出具的针对本次投标项目的《原厂商售后服务承诺函》。

5、本项目不允许采用联合投标，不允许转包、分包。

6、应符合《政府采购法》第二十二条的要求。

7、品目中带★参数为必须满足项。

8、★投标保证金：人民币1万元整。

9、投标保证金为投标文件的组成部分之一。

9.1、投标保证金以转帐、电汇等形式提交，必须在投标截止时间前到达指定账户。为方便保证的收取工作，在提交投标的同时，应单独提交保证金到账的相关票据给投标文件接收人员，以便及时开具保证金收据。

9.2、投标保证金用于保护本次招标活动免受投标人的行为而引起的风险。未按规定缴交投标保证金的投标，将被视为无效投标。

9.3、中标通知书发出后，招标人将在未中标的投标人提交了正式收款收据等有关资料之日起的15个工作日内，予以原额无息退还未中标的投标人的投标保证金。

9.4、中标人在收到中标通知书后签定服务承包合同，原投标保证金直接作为合同履约保证金。履约保证金在双方合同终止、交接清楚和债权债务等关系理顺后30日历天内无息返还。

9.5、发生以下情况之一的，投标保证金将不予退还：⑴ 投标人在投标截止期后，投标有效期内撤回投标；⑵以他人名义投标或者以其他方式弄虚作假，骗取中标；（3） 本招标文件中规定的其他没收投标保证金的情形。上述不予退还投标保证金的情况，如签定服务承包合同自动终止，如给招标采购单位造成损失的，投标人还应承担赔偿责任。

9.6、开户名：厦门国贸物业管理有限公司； 开户行：建行厦门市湖滨支行；账号：3510 1551 0010 5000 9378 。

10、招标文件的解释权归厦门国贸物业管理有限公司。

**以上资格证明文件均应加盖投标人公章**

### 实施及售后服务要求

1、投标人应按照本采购项目特点提供长期良好的售后服务，并在投标文件中提供详细具体的售后服务承诺条款及保证。

2、本批招标要求对设备类产品提供自验收合格之日起提供3年免费现场保修维护服务，中标供应商最终维修服务响应时间为2小时，在4小时内到达现场进行免费维修服务，并于48小时内排除故障，使用户系统正常工作。特殊情况无法处理的，因按原厂质保要求进行保修维护。信息安全年度运维提供1年免费现场保修维护服务，中标供应商最终维修服务响应时间为2小时，在4小时内到达现场进行免费维护服务。

3、中标人在设备安装前应派员进行实地勘察，设计安装调试方案，确保有关线路设计合理、运行可靠、维护方便。

4、中标人负责组织专业技术人员进行设备安装调试，用户应提供必须的基本条件和专人配合，保证各项安装工作顺利进行。

5、安装调试到位后的设备由中标人及用户共同进行质量验收签字。

6、设备验收前，中标人须提供完整的技术资料（包括产品说明书、用户手册、出厂明细表或装箱单、制造厂质量合格证书及其他相关文件资料）以及针对该设备实际使用环境的操作手册。

7、中标人向用户提供安装和维修所需特殊专用的工具、备件及清单和中文说明书，其费用包括在投标价格内。

8、中标人应在安装调试后配合招标方免费进行一次应急演练（如设备断电等）

# 投标人须知

## 投标书的充分性

 1、应当认为在正式提交投标书前，投标人已经认真研究招标人提供的招标文件条款和合同文件，对任何可能存在的疑问都已经得到招标人的澄清和解答。

 2、应当认为投标人在提交投标书之前，已对供货现场和其周围环境进行了视察和检查，并对现有道路或其他与现场有关和进出交货现场的交通方式、交通状况全部了解，而且一般应认为投标人已经得到了有关影响其投标和送货实施的全部必要资料。

3、应当认为，投标人已经确认其提交的投标书已经全面充分地体现和覆盖了：

（1）投标人根据合同应承担的全部义务；

（2）为该设备的及时送达因投标人原因造成的缺陷所必须发生的一切开支。

## 投标文件要求：

投标人应当按照招标文件的要求编制投标文件，并保证所提供的全部资料的真实性及准确性，并对投标文件负完全责任。投标文件应对招标文件提出的实质性要求和条件作出完全响应。

1、投标文件全部用A4纸填写并装订整齐。投标文件一式两份，**正本壹份**和**副本壹份，**分别封装。在每一份投标文件及封袋上要明确注明“正本”或“副本”字样，若正本和副本有差异，以正本为准。

2、投标文件必须密封递交，投标文件封口处须加盖投标人印章或由投标人代表签名，并标明招标编号、投标项目名称。

3、投标文件正本和副本须打印并由经正式授权的投标人代表签字。

4、除投标人对错处做必要的修改外，投标文件中不允许有加行涂抹或改写。若有修改须经法定代表人或投标人代表签字或加盖公章。

5、以电报、电话、传真或电子邮件等方式的投标概不接受。

6、投标文件及投标人和招标就投标交换的文件和来往信件，应以中文形式书写；计量单位应使用中华人民共和国法定计量单位、投标报价以人民币为货币单位（招标文件另有要求的除外）。

7、投标文件应包括投标函、投标一览表、技术性能参数的详细描述（项目主要设备及材料一览表）、售后服务承诺书、投标资格证明文件、投标项目设备和材料符合招标文件规定的证明文件、技术响应文件和投标人认为需加以说明的其它内容。投标人应将文件装订成册，并填写投标文件目录或资料清单。

8、投标文件格式

1）投标人应按招标文件中提供的投标文件格式填写投标书、开标一览表及应标响应表等。

2）投标人应按招标文件要求填写投标货物的单价和投标总价。如果单价与总价有出入，以单价为准。投标人对每个分项只能有一个报价，招标人不接受有选择的报价。

3）填写投标价格表时应注意下列要求：

A、技术规格中特别要求、培训及其他附带服务的费用。

B、投标人提供在中华人民共和国制造的货物的投标，其货物的交货价应包括制造该货物所使用的进口零部件及原材料已付的全部关税、销售税和其他税。

4）招标文件没有提供格式的要求响应的文件，投标人可自拟文件格式。

## 投标文件的递交

1、所有投标文件必须在投标截止时间之前，将投标文件密封后送达投标地点。必须在密封外层注上“投标文件”字样。

2、投标人可在投标截止时间前，对所递交的投标文件可以补充、修改或者撤回，并书面通知招标人，该通知须经正式授权的投标代表签字。投标人对投标文件的修改或撤销应密封递交，并在封面注明“补充、修改投标文件”或“撤销投标”字样。补充、修改的内容为投标文件的组成部分。

3、招标人有权根据具体情况修改投标截止时间，并告知所有潜在投标人。

## 违约责任

1、招标人未能在规定的时间内交付货款，每逾期一日，应支付应付货款金额10‰的违约金。

2、中标人如不能按时全部交货，每逾期交货一日，应承担合同总价10‰的违约金；并赔偿因供货不及时造成招标人的经济损失。

3、招标人如在合同的履行过程中发现中标人有以下行为的，可单方面中止合同并要求中标人支付合同总价50%的违约金，违约金不足以赔偿招标人经济损失的部分，招标人有权继续追偿。

（1）、在投标文件中弄虚作假、存在欺诈行为的；

（2）、中标人投标文件中表述的生产能力或售后服务或产品性能指标优于招标文件要求并直接影响评委评分、但合同实际履行过程中没能兑现其投标文件表述内容的；

（3）、中标人未能在规定的时间内完全全部交货，经与招标人再次商定延缓交货日期后仍不能按时交货的。

## 投标报价要求

1、投标总报价为货物送达采购人指定地点，交货、安装完毕并经招标人验收合格所可能发生的费用和售后服务费用，包括货物制造、运输、装卸、安装、产品检验检测、税收、售后服务以及相关规定须交纳的其它费用等。

2、投标人响应投标时只能有一个报价，本次招标不接受有选择的投标报价。

## 付款方式

1、货物达甲方指定地点10个工作日内一次付付合同总金额的30 %。

2、设备验收合格正常使用 30 个工作日内付合同金额的65%。

3、余款作为服务保证金，使用正常壹年后7个工作日内付清。

## 合同签订

1. 中标人应在接到中标通知后的5个工作日内完成合同的签订。招标文件、中标人的投标文件均作为合同订立的基础。

招标文件和投标文件就某方面的表述存在差异时，招标人拥有最终选择权。

1. 招标人直接与投标人签订购销合同。

## 到货时间：

1. 中标人应保证收到中标通知书之日起10个工作日内全部到货。

## 投标有效期

投标文件从开标之日起，投标有效期为90个日历日。

# 开标和评标

本次招标、评标过程由厦门国贸物业招投标小组监督。

## 开标

1、招标人在招标公告规定的时间进行开标。

2、开标时，先查验投标原件密封情况，确定无误后拆封唱标。主要公开投标文件正本“开标一览表”内容以及招标部门认为必要的其他内容。

3、开标时，开标一览表（报价表）内容与投标文件中明细表内容不相符的，以开标一览表（报价表）为准。

投标文件的大写金额和小写金额不一致的，以大写金额为准；总价金额与单价金额有差异的，以单价金额为准修正总价金额，但单价金额小数点有明显错误的除外；对不同文字文本投标文件的解释发生异议的，以中文文本为准。

4、为了有助于对投标文件进行审查、评估和比较，招标部门有权向投标人质疑，投标人有责任按照招标人通知的时间、地点递送书面答疑。书面的答疑作为投标文件的一部分，但不得对投标内容进行实质性修改。

## 评标

1、招标人将按照法律、法规规定及根据招标采购项目特点组建评标委员会，评标委员会对投标文件进行审查、质疑、评估、比较和评价。

**2**、**废标界定**

出现以下列情形之一的，由评标委员会初审后按废标处理：

* 1. 出现影响采购公正的违法违规行为；
	2. 投标人报价均超过采购预算（控制价）造成采购人无法支付货款的；
	3. 因重大变故，采购任务取消的；
	4. 应标单位少于三家；
1. **标书作废的界定**

出现下列情况之一的，该投标文件作无效投标处理：

1. 投标文件字迹模糊不清的（三分之二以上评委认为）；
2. 投标内容、技术标准没有实质性响应招标文件要求；
3. 投标内容超出投标企业经营范围；
4. 投标文件缺少开标一览表，或开标一览表未加盖投标人公章的；
5. 投标人递交两份或多份内容不同的投标文件，或在一份投标文件中对同一招标货物报有两个或多个报价，且未声明哪一个为最终报价的，按招标文件规定提交备选投标方案的除外；
6. 投标有效期不满足招标文件要求的；
7. 不满足或未实质性响应招标文件任何一条带★号条款规定的；

## 评标办法

1. 由厦门国贸物业管理有限公司组成招投标小组。
2. 评标原则：招投标小组按有关规定，遵循“公平、公正、科学择优”的原则进行评标。
3. 定标原则：在产品质量符合国家标准、投标文件完全符合标书要求的条件下，采用**最低价格中标原则**。
4. 因本项目的特殊性和工期时间紧等情况，特别规定如下：若本项目在开标后因有效投标人不足三家而公开招标失败时，经公司招标领导小组同意，可针对参与本项目的投标人直接转入竞争性谈判，并按招标文件规定的商务技术条款进行评审，对采购文件作出实质响应的投标人只有两家的，谈判小组可以与两家投标人进行谈判，并按以下评审办法进行评审；只有一家的，可以采取单一来源方式采购，谈判小组按照符合采购需求、报价合理的原则推荐成交投标人。
5. 谈判小对通过以上审核的有效谈判响应投标人进行评审和推荐，
6. 在所有有效谈判响应投标人均符合采购需求，质量和服务相等的前提下，以提出最低
7. 报价的谈判响应供应商作为谈判成交投标人。

## 定 标

定标后，中标人与招标人签订合同。招标文件、中标人的投标文件及其澄清文件等均为签订合同的依据。

# 投标文件格式

**格式1 投标书**

致：厦门国贸物业管理有限公司

根据贵方为网络安全设备招标项目的投标邀请，签字代表 （全名、职务）经正式授权并代表投标人 （投标人名称、地址）提交以下文件正本一份和副本一份。

(1)投标一览表

(2)法定代表人授权书

(3)售后服务承诺书

(4)技术性能参数的详细描述

(5)资格证明文件

(6)技术规格和商务偏离表

(7)按投标人须知要求提供的全部文件

据此函，投标人代表宣布同意如下：

1、投标人将按照招标文件规定履行合同责任和义务。

2、投标人已详细审查全部招标文件，包括修改文件（如有的话）以及全部参考资料和相关附件。我们完全理解并同意放弃对这方面有不明及误解的权利。

3、投标自开标之日起有效期为90个日历日。

4、投标人同意提供按照招标人可能要求的与其投标有关的一切数据或资料，完全理解招标人不一定要接受最低价的投标或收到的任何投标。

5、与本投标有关的一切正式往来通讯请送至：

地址：厦门市思明区体育路41号顺承大厦6楼

电话：0592-2990812 联系人： 李女士

投标人代表姓名、职务：

投标人全称（加盖公章）：

日期： 年 月 日

**格式2 法定代表人授权书(原件)**

兹有 （投标人全称）的法定代表人（姓名）授权 （被授权人姓名），为厦门国贸物业管理有限公司网络安全设备采购项目的投标代理人，以本公司名义处理一切与之有关的事宜。

本授权书仅对该项目有效，特此声明。

法定代表人签字：

被授权人签字： 职务：

投标单位详细地址：

邮编：

联系电话/传真：

E-mail:

投标人全称（加盖公章）：

日期： 年 月 日

**格式3 售后服务承诺书**

致：厦门国贸物业管理有限公司

根据贵方为网络安全设备招标项目的公告，我司对该项目做出如下售后服务承诺：

（内容根据招标文件要求自拟）

投标人全称（加盖公章）：

 年 月 日

**格式4 开标一览表**

投标商签章：

日期：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 产品名称及描述 | 数量 | 品牌，产地，型号 | 设备价格 | 后续特别授权价格（未注明默认免费） | 三年保修期后，每三年保修费（含软件及特征库升级费用，每三年不得超过设备价格10%） |
| SSL VPN设备 | 1 |  |  |  |  |
| 下一代防火墙设备 | 2 |  |  |  |  |
| 上网行为审计设备() | 1 |  |  |  |  |
| 边界隔离网关设备 | 1 |  |  |  |  |
| 一体化网关设备 | 20 |  |  |  |  |
| 设备总报价： |

注：1、若本页写不开可按此格式另加附页

**格式5 技术规格和商务偏离表**

#### SSL VPN设备

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 指标项 | 技术及服务项目 | 参数说明 | 投标响应（应备注响文件在哪一页） | 正负偏离 | 备注 |
| 设备要求 | 数量 | 1 |  |  |  |
| 保修 | 三年软硬件维保、三年软件升级服务 |  |  |  |
| 基础项要求 | 性能要求 | ★1、标准1U机架尺寸，独立非插卡式VPN硬件设备，配备≥4个千兆电口，支持并发SSL并发SSL用户数≥800，授权并发SSL用户数≥500，SSL加密速度≥200Mbps；每秒新建用户数≥75。配备IPSec VPN功能，不限IPSec VPN数量（移动用户除外），支持与第三方国际标准IPSec VPN对接，支持隧道间路由功能。支持并开启授权并发用户数≥100 的APP应用封装模块。 |  |  |  |
| 部署要求 | 2、支持网关模式、单臂（旁路）模式、多机热备模式、集群模式、分布式模式。 |  |  |  |
| 便利性要求 | 3、支持终端使用包括Win7、Mac、Linux等操作系统、支持IE、Firefox、Safari、Google Chrome、Opera等浏览器来登录SSLVPN系统，并完整支持各类应用。（提供Win7、Mac、Linux下各种浏览器的使用截图） |  |  |  |
| 加密算法 | ★4、产品应支持国际通用标准的商用密码密码算法（简称“商密”），包括：AES、DES、3DES、DH、RSA、RC4、MD5、SHA1等；产品可扩展支持中国国家标准的商用密码算法（简称“国密”），包括：SM1（含SCB2），SM2、SM3、SM4。（提供以上所有项界面截图证明） |  |  |  |
| 统一门户 | ★5、可支持虚拟门户功能，在一台设备上配置不同的访问域名、IP地址，以及不同的使用界面，实现一台设备为多个不同用户群体服务的的使用效果。(提供虚拟门户设备截图证明) |  |  |  |
| 单点登录 | ★6、支持单点登录功能（SSO）,支持移动用户登录VPN后再登录内部B/S、C/S应用系统时不需要二次重复认证。（需提供单点登录截图证明） |  |  |  |
| 核心功能 | 中间人防护 | ★7、产品必须支持防中间人攻击，在用户登录SSLVPN时智能判断存在中间人攻击行为，断开被攻击的连接，并可提示异常现象和记录攻击日志。（提供中间人攻击页面配置截图）； |  |  |  |
| 专线功能 | 8、支持客户端注销后自动清除所有缓存、Cookies、浏览器历史记录、保存的表单信息，实现零痕迹访问；支持VPN专线功能，可配置用户在接入SSL VPN的同时，断开与Internet其他连接。 |  |  |  |
| 权限分配 | ★9、产品应具有用户/用户组细粒度的权限分配功能：可以针对被访问资源的IP地址、端口、提供的服务、URL地址等进行权限控制；针对同一B/S资源，可对不同用户做到细致到URL级别的授权；支持主从认证账号绑定，必须实现SSL VPN账号与应用系统账号的唯一绑定，VPN资源中的系统只能以指定账号登陆，加强身份认证，防止登录SSL VPN后冒名登录应用系统。（需提供主从账号绑定截图证明） |  |  |  |
| 用户认证 | ★10、产品必须支持Local DB 、USB KEY、短信认证、硬件特征码、动态令牌、数字证书认证、LDAP、RADIUS、等认证方式；可针对用户/用户组设置认证方式的与、或组合，可进行用户名/密码、LDAP、USB KEY、硬件特征码、短信认证或动态令牌的五因素捆绑认证 。（提供以上认证选项功能界面截图证明） |  |  |  |
| CA认证 | ★11、设备内部必须支持自建CA中心，便于数字证书认证平台搭建(提供内置CA中心页面截图)；支持与基于PKI体系的第三方CA进行结合认证 ，可根据CA某字段将通过CA认证的用户自动映射到指定用户组，方便进行权限授权配置；支持CRL证书撤销列表；单台VPN设备可扩展同时支持5套以上CA根证书；(提供5套以上CA根证书页面截图证明) |  |  |  |
| 多网接入 | ★12、必须支持至少4条以上的外网多线路配置；并在设备单臂部署模式下，多线路接入前置网关，仅依靠SSLVPN设备同样可实现SSLVPN接入用户的多线路自动优选功能（提供配置界面截图证明）； |  |  |  |
| 自动寻址 | ★13、支持启用多线路时，自动检测故障线路，并自动踢出故障线路；一旦线路恢复，可在一定时间内自动恢复。支持启用多线路时，自定义用户访问选路策略，包括按上/下行带宽，轮询，按优先级等方式；支持利用网页进行动态寻址的方法，客户端不安装插件、不依靠IP地址库、不依赖于第三方动态IP寻址、直接根据速度探测实现用户端接入线路的自动优选,用户通过访问寻址代理页面（Webagent页面）自动寻找VPN设备IP(非DDNS）。（提供Webagent配置截图证明）； |  |  |  |
| 智能优化 | ★14、支持针对不同的web页面进行数据优化，支持动态压缩技术，基于数据流进行压缩，减少不必要的数据传输。（提供web优化截图证明） |  |  |  |
| 远程应用发布 | ★15、产品必须支持远程应用发布功能，无需二次开发，把Windows应用发布到移动智能终端中或将C/S资源Web化；手机客户端必须经过苹果公司官方检测，并发布在苹果官方应用商店appstore，产品客户端必须通过google公司官方检测并发布在google应用商店PlayGoogle；产品客户端必须支持非“越狱”或非“Root”权限的手机/PAD安装。（提供远程应用发布，苹果官方应用商店手机客户端截图证明）； |  |  |  |
| ★16、支持远程应用使用本地输入法；支持本地输入法和远程服务器输入法可切换，在小屏幕或网络带宽差的情况下，支持在本地先批量输入文字再点击发送，避免零散数据在广域网上的频繁交互；远程应用发布应该支持云存储，能够将手机、PAD、PC电脑中的文档、照片等上传到云端，或下载到本地终端，并实现基本的复制、剪切、粘贴、新建、重命名等操作；产品必须支持经过集成的，基于Android IOS平台的第三方软件开发包（SDK），并实现基于Android IOS平台第三方应用软件（APP）代码量不超过20行。（要求提供代码Demo和企业证明）平台提供自动APP代码嵌入功能，在系统中添加APP应用可自动生产嵌入SDK代码的APP安全应用，实现App应用的安全加固 （提供APP自动封装界面截图证明）； |  |  |  |
| 应用权限控制 | 17、远程应用发布必须支持应用权限控制项，不得通过远程应用访问任何未经授权的windows资源，至少应该包括：未经授权的应用程序、注册表、任务管理器、资源管理器、控制面板、cmd命令提示行、Win+R运行命令行、管理选型、映射网络驱动器选型、断开网络驱动器选型、回收站、网上邻居等。并支持隐藏本地原有磁盘，仅提供公共磁盘； |  |  |  |
| 协议优化 | ★18、支持改写WindowsRDP协议，经改写的协议必须独立于OS运行环境，避免跨平台兼容性问题，针对图像数据，服务端必须支持有损压缩算法；服务端必须能够支持过滤动态内容（gif/flash/video）以减少传输流量，且根据客户需要配置。（提供RDP改写页面配置截图证明） |  |  |  |
| 生厂商资质 | 19、生产商资质：软件研发体系国际认证CMMI5、售后服务体系通过ISO9001认证，国家密码管理局发布的《SSL VPN技术规范》起草单位之一。 |  |  |  |
| 产品资质 | ★20、产品资质：提供产品IPV6 Ready认证证书，并在全球IPV6测试中心官网可查，SSL VPN必须在近四年内至少曾有一年在中国国内市场占有率为前三名，提供权威的第三方机构数据证明。 |  |  |  |
| 兼容性要求 | 设备联动 | ★21、为保障设备安全联动，要求与下一代防火墙和上网行为审计为同一品牌。 |  |  |  |

#### 5.2下一代防火墙设备

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 指标项 | 技术及服务项目 | 参数说明 | 投标响应（应备注响文件在哪一页） | 正负偏离 | 备注 |
| 设备要求 | 数量 | 2【★双机热备】 |  |  |  |
| 保修 | 三年软硬件质保与三年软件及病毒库升级服务 |  |  |  |
| 基础项要求 | 性能要求 | ★1、标准2U机架式设备，配置16个千兆电口，8个千兆光口，4个万兆光口。整机吞吐量80Gbps，应用层吞吐量45G。最大并发会话数≥1800万，硬盘大小≥500G，每秒新建会话数≥65万，支持槽位扩展（无须重新配置参数）。 |  |  |  |
| 基本功能 | ★2、 支持包过滤，网络地址转换，状态检测，应用流量识别，应用层安全防护，用户控制，深度内容检测，支持并开启不限IPSec VPN数量，支持隧道间路由功能，支持SSLVPN功能。支持统一安全运维管理； |  |  |  |
| 部署要求 | 3、支持路由、透明、旁路、虚拟网线，混合模式+ |  |  |  |
| 策略路由 | ★4、为保障网络中应用的高效运行，应具备应用层流量的引流，支持针对应用的策略路由（提供基于应用的策略路由的配置页面截图证明）； |  |  |  |
| 模块要求 | ★5、为保证整体网络安全，所投设备必须支持威胁的分析发现与防护并重，因此必须具备威胁发现功能：威胁情报预警与处置、业务系统实时漏洞分析功能，具备威胁防御功能：敏感信息泄漏防护、服务器保护、恶意链接防护(需提供以上威胁发现、威胁防护所有功能界面截图，并可提供实际测试)； |  |  |  |
| 模块联动 | ★6、为保证能有效防护大规模攻击，所投设备必须具备并开启web应用防护、入侵防御、僵尸网络的联动封锁功能，可智能生成临时规则封锁攻击源IP，临时封锁时间可自定义（需提供入侵防护、web应用防护、僵尸网络设置联动封锁配置功能截图证明、设置IP冻结时间，设置时间自动刷新封锁IP列表的截图证明，并可提供实际测试）；  |  |  |  |
| 脚本检测 | 7、为保证网络安全，必须具备PHP,JSP,ASPX等主流脚本语言编写的webshell后门脚本上传检测功能；  |  |  |  |
| 关键URL认证 | ★8、为保证网络安全，必须支持对重要业务系统提供重要URL或者其他应用服务的短信认证机制（提供至少包括web、rdp、pptp、nntp、rlogin等四种以上服务进行短信认证加强登录防护的配置截图证明，并可提供实际测试）； |  |  |  |
| 核心功能 | 基本功能 | ★9支持并开启IPSec VPN、SSL VPN、APT检测、IPS入侵防护、WEB攻击防护、网页篡改防护、病毒防护。 |  |  |  |
| Web防护能力 | ★10、为保证网络安全，应支持WEB行为进行过滤，提供Web攻击防护、Web远控木马防护等功能，web应用防护能力通过开源web应用安全项目组（OWASP）评测认证，并且在OWASP的25项评测要求中，获得满分（五星）评测项在19项（含）以上（提供OWASP认证证书以及对应的web攻击防护能力测评报告）； |  |  |  |
| Web扫描 | 11、为实现对业务系统的安全分析，支持Web漏洞扫描功能，可分析web网站各类漏洞，包括SQL盲注，LDAP注入，存储型跨站脚本，操作系统命令，文件包含等脚本漏洞（需提供以上五类详细的漏洞扫描截图证明）； |  |  |  |
| 僵尸网络监测 | 12、为保证网络流量安全纯净，必须支持对PC终端、服务器是否变成了僵尸肉鸡进行检测，识别特征总数在50万条以上（需提供木马远控、恶意链接、移动安全、异常流量的僵尸网络检测功能截图证明、僵尸网络识别库超过50万条的界面截图，并可提供实际测试）； |  |  |  |
| 异常连接检测 | 11、支持异常连接检测，对21，22，25，53，69，80/8080，110，143，443等常见端口的协议异常流量检测，并支持RDP和SSH端口反弹链接检测； |  |  |  |
| 恶意连接防护 | 12、当前互联网威胁变化迅速，为保证网络安全能及时防护最新威胁，设备需具备终端请求恶意链接检测拦截功能，提供接入云端安全联动功能； |  |  |  |
| 异常流量监测 | 13、支持对内网主机外发的异常流量进行检测，如ICMP，UDP，SYN，DNS Flood等DDoS攻击行为，支持外网对内网主动发起的异常流量进行检测，如ICMP，UDP，SYN，DNS Flood等DDoS攻击行为； |  |  |  |
| 攻击分析 | ★14、为实现安全可视化，应支持对各类威胁行为进行深度分析，输出网络总存在的威胁问题，并对各类威胁行为输出有效攻击次数和攻击趋势；（提供具备有效攻击、攻击趋势的威胁报告证明，并可提供实际测试）  |  |  |  |
| 安全可视化 | ★15、为加强管理员对网络安全的了解，需要在设备首页多维度的展示发现的安全威胁，如入侵风险，实时漏洞风险，僵尸主机威胁，数据风险，被防护网站黑链风险，对外Dos攻击和攻击者地图等，并支持将所有发现的安全问题进行归类汇总列为待处理问题，针对给出相应的解决方法指引（要求提供首页界面展示入侵风险，实时漏洞风险，僵尸主机威胁，数据风险，被防护网站黑链风险，对外Dos攻击和攻击者地图等7大功能界面截图，并提供针对待处理问题相对应的解决方案指引截图）； |  |  |  |
| 热点事件分析 | ★16、为保证能够抵抗新型安全威胁，设备必须提供最新的威胁情报信息，能够对新爆发的流行高危漏洞进行预警和自动检测，发现问题后支持一键生成防护规则（要求提供设备发布最新威胁情报信息、自动进行预警检测以及一键生成防护规则的功能截图）； |  |  |  |
| 安全评估 | 17、网络安全建设是长期的过程，需要定期的做安全评估，因此设备必须支持针对服务器的漏洞风险评估功能，支持对ftp、mysql、oracle、mssql、ssh、rdp、netbios、vnc等应用的弱密码扫描，扫描完成后生成安全风险评估报告并自动添加安全策略(为了保障与防火墙之间智能联动，要求提供内置风险分析功能模块的界面截图证明、提供支持上述所有应用的弱密码扫描功能截图证明、同时能查看针对扫描出来的风险自动添加策略的界面截图)； |  |  |  |
| 黑链检测 | ★18、设备必须支持对被防护网站是否被挂黑链进行检测，支持显示TOP5黑链主机及黑链（游戏、色情、反动及非法内容等）类型分布、危害或影响，同时支持在设备界面提供参考解决方案（提供提供识别赌博、游戏、色情、广告等黑链的功能界面截图）； |  |  |  |
| 口令防护 | ★19、设备必须支持对常见应用服务（FTP、SSH、TELNET、SMTP、IMAP、POP3、RDP、SMB、VNC）和数据库软件（MySQL、Oracle、MS SQL）的口令暴力破解防护功能（必须提供以上所有对常见应用服务和数据库软件的口令暴力破解防护功能界面截图）； |  |  |  |
| 产品资质 | 20、产品应具备计算机信息系统安全专用产品销售许可证； |  |  |  |
| ★21、产品经过国际知名实验室NSS Labs测试，并获得recommended推荐级别（提供NSS Labs相关测试报告）； |  |  |  |
| ★22、要求厂商具备优秀的技术创新实力，提供防火墙产品入围GARTNER魔力象限的证明（需提供防火墙产品入围GARTNER魔力象限截图证明）； |  |  |  |
| 23、产品具备ICSA labs认证证书（提供证明材料） |  |  |  |
| 厂商资质 | ★24、为保证产品功能稳定性及可靠性，厂商应通过CMMI5级认证（提供证书复印件证明） |  |  |  |
| ★25、所投品牌厂商是第二代防火墙标准（GA／T 1177-2014）起草单位之一（提供相关证明复印件）； |  |  |  |
| 兼容性要求 | 设备联动 | 26、★为保障设备安全联动，要求与SSL VPN和上网行为审计为同一品牌。 |  |  |  |

**5.3 上网行为审计**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 指标项 | 技术及服务项目 | 参数说明 | 投标响应（应备注响文件在哪一页） | 正负偏离 | 备注 |
| 基础项要求 | 网络接口 | ≥6个千兆电口 |  |  |  |
| 设备要求 | 三年软硬件质保与三年URL库升级 |  |  |  |
| 存储介质 | ≥128G SSD硬盘 |  |  |  |
| 尺寸 | ≥1U机架式 |  |  |  |
| 吞吐量 | ≥2Gbps |  |  |  |
| 用户规模 | ≥4500 |  |  |  |
| 部署模式 | 必须支持两台及两台以上设备同时做主机的部署模式 |  |  |  |
| 智能选路 | ★1、采用基于网关或网桥的线路自动选路方法的技术,能够为上网用户智能的选择最快的上网线路,并且设备需要支持网关、网桥、旁路等多种部署模式 (必须提供国家权威机构出具的网关，网桥自动选路此技术的证明文件并加盖投标人公章) |  |  |  |
| 用户认证 | 2、支持本地用户名/密码认证、第三方认证（Radius、LDAP、POP3等）以及IP/MAC绑定，并且能够支持USB-KEY双因素的用户身份认证，通不过认证的用户禁止上网，并且能够根据需要进行差异化的策略认证；支持与LDAP服务器结合进行优化，便于客户实现策略管理在AC上进行，用户管理在域上进行，不需同步用户到本地组织结构中即可实现策略管理功能 |  |  |  |
| 网页过滤 | 3、支持根据访问的URL、网页关键字进行网页过滤，支持设置拒绝以IP访问网页行为；支持在放行URL时，自动放行主域名的子链接中被禁止的网站，保证网页显示完整；必须支持未知网页的自动识别与分类（提供界面证明） |  |  |  |
| 规则库 | 4、设备内置应用识别规则库，支持超过4600条应用规则数，支持超过2100种以上的应用，650种以上移动应用，并保持每两个星期更新一次，保证应用识别的准确率（提供产品界面截图） |  |  |  |
| 核心功能 | 短信认证 | 5、支持短信认证方式，用户输入手机号作为用户名，通过短信猫或短信平台发送验证码；短信认证能够根据不同用户推送不同认证页面，该认证页面可自定义，编辑内容包括文字、颜色风格、图片，且图片支持轮询播放（提供界面证明） |  |  |  |
| Web访问质量 | ★6、支持针对内网用户的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；支持以列表形式展示访问质量差的用户名单；支持对单用户进行定向web访问质量检测（以上各条需提供产品界面截图） |  |  |  |
| 微信和二维码认证 | ★7、支持与微信结合的认证方式，用户关注微信公众号后即通过身份认证，后台记录用户ID；支持与第三方微信平台无缝对接，不需要修改第三方微信平台代码；支持二维码认证，管理员扫描访客的二维码后对其网络访问授权 |  |  |  |
| 内容审计 | 8、支持记录加密的和明文的邮件内容、BBS发帖以及聊天内容审计；必须能审计木马、病毒、恶意脚本和插件、端口扫描等危险行为；必须能审计来自外网访问内网网站，在内网服务器下载上传下载文件，发帖的行为；支持指定用户扩展支持通过USB-Key免审计的功能；必须能审计来自外网访问内网网站、在内网服务器下载上传文件、在内网服务器发贴、从内网服务器上收发邮件的行为 |  |  |  |
| 热点管理 | ★9、支持能自动发现网络中通过无线上网的热点和移动终端的IP和终端类型；支持管理员配置热点信任列表；支持发现信任列表外非法接入的热点和终端，并阻止该热点/终端上网；支持将非法热点接入网络的行为通过邮件告警通知管理员，并在数据中心支持行为记录和查询；支持以图表方式显示移动终端接入趋势（提供产品界面截图） |  |  |  |
| AP管理 | 10、支持并开启无线AP管理功能（授权不少于10个），能够直接查看到接入点状态、射频状态、无线网络状态、接入用户状态（所有项提供产品界面截图）支持基于SSID维度的上网权限、上网审计、上网安全、终端提醒、和流控等策略（所有项提供产品界面截图） |  |  |  |
| 认证联动 | ★11、为提高兼容性，保证用户认证和权限一致性，要求上网行为管理设备支持与下一代防火墙设备为同一品牌设备，进行用户认证信息共享，包括本地密码认证、外部密码认证、手机短信验证、单点登录和dkey认证信息在上网行为管理和防火墙设备之间的转发及接收（提供认证信息共享的产品界面截图） |  |  |  |
| 安全功能 | 网站安全 | 12、采用基于网关、网桥防范网络钓鱼网站的技术，支持识别并过滤SSL加密的非法网站、钓鱼网站、金融购物网站等，保证浏览网页的安全性；必须支持基于关键字过滤SSL加密的论坛、BBS上的发贴行为，同时支持允许用户浏览帖子但不准发贴功能（提供国家权威机构出具的网关，网桥防范网络钓鱼此技术的证明文件并加盖投标人公章） |  |  |  |
| 脚本安全 | 13、支持识别执行脚本的网页，并过滤脚本中隐藏木马等程序的网页（必须提供国家权威机构出具的网络插件安全检查方法此技术的证明文件并加盖投标人公章） |  |  |  |
| 管理功能 | 流量控制 | ★14、支持基于应用类型、网站类型和文件类型划分与分配带宽；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；空闲值可自定义（提供界面证明）支持通过抑制P2P的下行流量，来减缓P2P的上行流量，从而解决网络出口在做流控后仍然压力较大的问题（提供界面证明） |  |  |  |
| 高性能日志模式 | 15、支持日志高性能模式处理，精简冗余日志（提供产品界面截图） |  |  |  |
| 外置数据中心支持服务器虚拟化 | ★16、提供自有品牌的免费服务器虚拟化产品与外置DC联动，服务器虚拟化能够根据实际用户和流量规模合理分配硬件资源，保障最优资源分配。同时，外置DC能够与服务器虚拟化底层联动，优化磁盘读写，提高查询速度（提供自有品牌服务器虚拟化软件截图证明） |  |  |  |
| 应用标签 | 17、支持根据标签选择应用，标签分类至少包含安全风险、高带宽消耗、发送电子邮件、降低工作效率、外发文件泄密风险、主流论坛和微博发帖6大类；支持弱特征识别等相关技术，以应对P2P软件种类多、版本多、更新快的问题；必须支持无插件封堵浏览器配置公网代理服务器和通过代理软件代理上网行为（提供设备操作界面截图证明） |  |  |  |
| 产品资质与认证 | 18、设备生产厂商售后服务体系通过ISO9001认证（提供证书复印件） |  |  |  |
| ★19、设备生产厂商的研发体系通过国际认证CMMI5（提供证书复印件） |  |  |  |
| 具备下一代互联网网络审计系统/增强级《计算机信息系统安全专用产品销售许可证》、《中国国家信息安全产品认证证书》、IPv6 Ready Phase-2认证、《销售许可证（互联网公共上网服务场所）》。 |  |  |  |
| 兼容性要求 | 设备联动 | ★20、为保障设备安全联动，要求与下一代防火墙和SSL VPN为同一品牌。 |  |  |  |

5.4 边界隔离网关

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 指标项 | 技术及服务项目 | 参数说明 | 投标响应（应备注响文件在哪一页） | 正负偏离 | 备注 |
| 设备要求 | 数量 | 1 |  |  |  |
| 保修 | 三年硬件维保与软件升级 |  |  |  |
| 基础项要求 | 性能要求 | 1. ★标准1U机架式设备，单电源，配置4个千兆电口 ，三层吞吐量≥2Gbps，应用层吞吐量≥400M，最大并发会话数≥25万，硬盘大小≥SSD 32G，每秒新建会话数≥1.5万；
 |  |  |  |
| 基本功能 | ★2、支持包过滤，网络地址转换，状态检测，应用流量识别，应用层安全防护，用户控制，深度内容检测，支持IPSec VPN，支持统一安全运维管理；开通入侵防御检测模块， 支持并开启IPSec VPN、SSL VPN、APT检测、IPS入侵防护、WEB攻击防护、网页篡改防护、病毒防护。 |  |  |  |
| 策略路由 | 3、为保障网络中应用的高效运行，应具备应用层流量的引流，支持针对应用的策略路由（提供基于应用的策略路由的配置页面截图证明）； |  |  |  |
| 模块要求 | ★4、为保证整体网络安全，所投设备必须支持威胁的分析发现与防护并重，因此必须具备威胁发现功能：威胁情报预警与处置、业务系统实时漏洞分析功能，具备威胁防御功能：敏感信息泄漏防护、服务器保护、恶意链接防护(需提供以上威胁发现、威胁防护所有功能界面截图，并可提供实际测试)； |  |  |  |
| 模块联动 | 5、为保证能有效防护大规模攻击，所投设备必须具备web应用防护、入侵防御、僵尸网络的联动封锁功能，可智能生成临时规则封锁攻击源IP，临时封锁时间可自定义（需提供入侵防护、web应用防护、僵尸网络设置联动封锁配置功能截图证明、设置IP冻结时间，设置时间自动刷新封锁IP列表的截图证明，并可提供实际测试）；  |  |  |  |
| 脚本检测 | 6、为保证网络安全，必须具备PHP,JSP,ASPX等主流脚本语言编写的webshell后门脚本上传检测功能；  |  |  |  |
| 异常流量监测 | 13、支持对内网主机外发的异常流量进行检测，如ICMP，UDP，SYN，DNS Flood等DDoS攻击行为，支持外网对内网主动发起的异常流量进行检测，如ICMP，UDP，SYN，DNS Flood等DDoS攻击行为； |  |  |  |
| 攻击分析 | ★14、为实现安全可视化，应支持对各类威胁行为进行深度分析，输出网络总存在的威胁问题，并对各类威胁行为输出有效攻击次数和攻击趋势；（提供具备有效攻击、攻击趋势的威胁报告证明，并可提供实际测试）  |  |  |  |
| 安全可视化 | ★15、为加强管理员对网络安全的了解，需要在设备首页多维度的展示发现的安全威胁，如入侵风险，实时漏洞风险，僵尸主机威胁，数据风险，被防护网站黑链风险，对外Dos攻击和攻击者地图等，并支持将所有发现的安全问题进行归类汇总列为待处理问题，针对给出相应的解决方法指引（要求提供首页界面展示入侵风险，实时漏洞风险，僵尸主机威胁，数据风险，被防护网站黑链风险，对外Dos攻击和攻击者地图等7大功能界面截图，并提供针对待处理问题相对应的解决方案指引截图）； |  |  |  |

5.5 一体网关

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 指标项 | 技术及服务项目 | 参数说明 | 投标响应（应备注响文件在哪一页） | 正负偏离 | 备注 |
| 设备要求 | 数量 | 1 |  |  |  |
| 保修 | 三年硬件维保与软件升级 |  |  |  |
| 基础项要求 | 性能要求 | ★1、标准1U机架式设备，单电源，配置2个WAN(1000M)、1个LAN（1000M）、10个LAN(100M) 、1个DMZ(1000M) ，三层吞吐量≥200Mbps，IPSec vpn加密速度≥40Mbps，最大并发会话数≥2万，； |  |  |  |
| 基本功能 | ★2、支持包过滤，网络地址转换，状态检测，应用流量识别，应用层安全防护，用户控制，深度内容检测，支持统一安全运维管理 支持并开启IPSec VPN。 |  |  |  |
| 策略路由 | 3、为保障网络中应用的高效运行，应具备应用层流量的引流，支持针对应用的策略路由（提供基于应用的策略路由的配置页面截图证明）； |  |  |  |
| 用户认证、审计 | ★4、WEB认证，IP-MAC绑定，IP/MAC认证，自动创建帐号。实时记录日志包括访问的时间、上网行为操作的拒绝/通过、主机的IP、访问对象的类型、访问对象的名称等 |  |  |  |
| 广告营销 | 5、基于特定用户或者终端实现广告页面的推送。 |  |  |  |
| 应用识别规则 | 6、应用识别规则库、可手工添加基于“深度内容检测”技术的新应用协议识别规则，实现个性化识别和封堵，提供无限扩展能力 |  |  |  |
| 访问控制 | ★7、以半小时为单位，支持任意的时间段设置；支持每天多个时间段设置；支持每周七天每天各不相同的时间 段设置，为客户提供最灵活的时间段控制能力 |  |  |  |
| 流控 | 8、允许指定用户使用P2P行为，但对其占用的带宽资源进行管理和控制、将出口中指定的带宽资源划分，并将指定的带宽资源分配给指定对外提供访问的服务器，实现对外发布 应用的保障 |  |  |  |
| 防火墙 | ★9、支持抵御来自公网的DoS攻击，支持对爆发于内部网络的DoS攻击进行检测和防御 网的DoS。支持对内网ARP欺骗的防御。内置基于状态监测的企业级防火墙，提供网关设备安全、组织内网安全双重保护 |  |  |  |
| 路由交换集中管理 | ★10、支持局域网划分VLAN， 通过VLAN访问控制，可允许或者拒绝VLAN之间的访问。支持DNAT、SNAT等多种NAT地址转换策略。支持DHCP服务功能。支持SC集中管控，实现配置策略下发，软件升级、管理维护等 |  |  |  |
| 安全可视化 | ★11、为加强管理员对网络安全的了解，需要在设备首页多维度的展示发现的安全威胁，如入侵风险，实时漏洞风险，僵尸主机威胁，数据风险，被防护网站黑链风险，对外Dos攻击和攻击者地图等，并支持将所有发现的安全问题进行归类汇总列为待处理问题，针对给出相应的解决方法指引（要求提供首页界面展示入侵风险，实时漏洞风险，僵尸主机威胁，数据风险，被防护网站黑链风险，对外Dos攻击和攻击者地图等7大功能界面截图，并提供针对待处理问题相对应的解决方案指引截图）； |  |  |  |
| 兼容性要求 | 设备联动 | ★12、为保障设备安全联动，要求与下一代防火墙和SSL VPN为同一品牌。 |  |  |  |

注：投标人提交的投标文件中与招标文件的技术、商务部分的要求有不同时，应逐条列在偏离表中，否则将认为投标人接受招标文件的要求。

投标人代表签字：

日期：

**格式6 法人营业执照**

现附上由（签发机关名称）签发的我方法人营业执照副本复印件，该执照业经年检，真实有效。

（注：法人营业执照提供复印件，需复印包括能说明经年检合格的内容，由企业加盖公章并注明复印件与原件一致。）

投标人（全称并加盖公章）：

投标人代表签字：

日期：