附件1

局域网安全防护系统采购清单

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 名称 | 质量技术标准 | 单位 | 数量 | 备注 |
| 1 | 入侵检测防御设备 | 质量技术标准参照：附件2《局域网信息系统安全整改技术方案》 | 台 | 1 |  |
| 2 | 主机监控与审计设备 | 质量技术标准参照：附件2《局域网信息系统安全整改技术方案》 | 台 | 1 |  |
| 3 | 漏洞扫描设备 | 质量技术标准参照：附件2《局域网信息系统安全整改技术方案》 | 台 | 1 |  |
| 4 | 补丁分发安全管理系统 | 质量技术标准参照：附件2《局域网信息系统安全整改技术方案》 | 台 | 1 |  |
| 5 | 防火墙设备 | 质量技术标准参照：附件2《局域网信息系统安全整改技术方案》 | 台 | 1 |  |
| 6 | 安全管理终端 | 独立安全管理维护终端，Intel G2030，4GB DDR3 133MHZ，1TB，WIN7 | 台 | 1 |  |
| 7 | 网络交换机 | 三层千兆交换机，背板宽带128Gbps，数据包转发率66Mpps，24个100Base-FX SFP端口，2个100/1000Base-X SFP端口，2个千兆Comb | 台 | 1 |  |
| 8 | 电源滤波插座 | 六位，安防、防雷抗浪涌插座 | 台 | 7 |  |
| 注：1.报价方必须对本项目所有货物进行报价，否则视为无效报价。  2.报价应包含运费、安装费、保管费等所有费用，报价文件中需详细列出明细。 | | | | | |

附件2

局域网信息系统安全整改技术方案

入侵检测和防御设备：

1、硬件规格：▲标准1U机箱,单电源；配置6个千兆电口，内置2路电口Bypass； 1个接口扩展槽位；支持液晶屏，可以显示设备管理IP地址，CPU使用率、温度等信息；性能指标：▲IPS吞吐量≥1000M；最大并发连接数≥100万；系统架构：基于X86架构，采用高性能的Intel多核CPU，采用多核操作系统，提供多核并行安全操作系统软件著作权登记证书复印件；系统管理：提供管理友好的中文Web图形界面配置，支持Telnet、SSH、串口登陆命令行模式配置；支持配置管理IP控制列表、SNMP网管协议以及邮件报警；支持通过web方式调用设备命令行窗口功能，无需登录串口就可对设备进行命令行操作，提供产品界面截图。

2、网络适应性：支持透明、路由、混合多种工作模式；支持静态、策略路由、OSPF、RIPv1/v2、BGP4等动态路由；安全防护：要求提供3年IPS特征库升级服务，内置4000种以上的攻击特征，能够检测包括溢出攻击类、RPC攻击类、WEBCGI攻击类、拒绝服务类、木马类、蠕虫类、扫描类、网络访问类、HTTP攻击类、系统漏洞类等攻击；支持4种安全防护模式，基于网络、用户以及应用，提供功能界面截图。

3、支持以多种方式定义租户，如：VLAN、NVGRE、VXLAN，提供功能界面截图；支持基于租户的安全策略、地址对象/地址组/地址池/权重地址、自定义服务对象/服务组、时间对象/时间组的隔离；支持基于租户的NAT、IP地址配置、IP\_MAC绑定、病毒过滤和防挂马、入侵防护、攻击防护、应用识别、文件控制、ARP防护、内容安全特性（邮件、网页的内容过滤）、策略/静态/多出口路由，提供功能界面截图。

4、统一特征库：支持web页面下对设备支持的特征库进行查看、更新及自定义操作；支持IPS特征库在线、离线升级；智能流量控制：支持基于优化的高速流匹配技术，以多种依据（源IP/目的IP/IP范围/源端口/目的端口/端口范围/接口/用户组/安全策略区域对象/应用协议等）对流量进行控制；支持将攻击流量通过镜像口镜像出去，供第三方设备存储、分析、审计等。

5、负载均衡：支持基于多种方式划分的负载均衡，如按照服务器、链路、全局等不同方面划分；支持8种调度算法（轮询调度、加权轮询调度、源地址散列调度、目标地址散列调度、最小连接调度、加权最小连接调度、基于局部性的最小连接调度和带复制的基于局部性的最小连接调度），提供产品功能截图。

6、集群部署：支持3台以上设备集群部署，可支持200台；支持设备可自动加入集群，和动态退出集群，在中心设备上能对指定的设备或所有成员设备下发配置。高可靠性：支持主备模式(A/S)、主主模式(A/A)等多种热备方式；支持多个心跳口的冗余备份。安全审计：支持全部日志按天和统一格式存储，可以通过web页面查看历史日志列表，且可以针对列表日志进行删除、导出等操作；支持历史日志，保证设备掉电后仍然可以保留上次运行的日志记录。

7、安全可视：产品可以图形化显示设备接口面板信息，直观查看接口是否联线，提供功能界面截图；产品界面可以显示设备当前的系统状况，包括CPU使用率、内存使用率、CPU温度等，提供功能界面截图；设备可以图形化展示应用风险指数、网络风险指数便于用户整体了解网络风险等级，提供功能界面截图；提供多种报表，可依据五元组、应用协议、时间点/时间段等元素自定义报表内容并显示。

主机监控与审计设备：

1、设备安全管理：实现对移动存储设备和办公计算机的有效管理，实现对内外网计算机防信息泄漏的有效管理。

2、 终端资产管理：对计算机软硬件资产全方位控制和管理，防止内部人员对计算机硬件资产的恶意盗取，防止内部人员对计算机软件资产的恶意破坏，防止内部人员对计算机软件资产的恶意篡改。

3、 非法接入管理：通过“非法接入管理”功能对恶意接入的计算机进行全方位有效的阻断，保证内网重要敏感数据的安全。

4、 用户身份管理：采用PKI 和数字证书技术，将用户身份跟网络安全系统完全融合在一起，实现了有效的管理和多种身份认证模式，并将用户身份和其所持有的资源实现了无缝的关联，实现人机分离防盗用等身份管理措施。

5、 综合安全审计：对计算机的各种资源如系统安装程序、网络连接状况、系统的服务等都采取有效的审计信息获取手段。针对用户的各种行为进行了详细的审计记录，例如用户的文件操作记录、上网记录、Mail 发送记录、FTP 发送记录等。管理定制各种策略，对用户的违规操作进行了详细的审计。

6、系统辅助功能：提供策略生命周期管理、系统自动安装和远程卸载、多级部署等功能，提高管理效率和满足用户使用的要求。

漏洞扫描设备：

1、扫描任务模块：采用先进的调度算法和执行引擎，在保证正确率的前提下大幅提高检测效率，集成二十二大类实践性检测方法，全方位、多侧面对网络安全隐患尽心扫描分析，覆盖母线网络和操作系统存在的主要弱点和漏洞。模块包括新建任务、编辑任务、执行任务、快速扫描等功能。提供定时扫描、历史任务从新扫描、断点继续扫描、扫描进度查看等功能。扫描时关闭扫描目标的防火墙，可以取得最佳扫描效果，能更彻底发现扫描目标系统自身存在的漏洞。通过专用接口，可跟防火墙、IDS等安全设备进行联动，提高系统的安全相应能力。

2、报表管理模块：采用报表和图形的形式对扫描结果进行分析和评估，直观体现出网络安全状况。可多角度多层次分析扫描结果，提供html打印、html浏览、word、pdf、txt等多种报表格式，提供行政主管、技术人员、安全专家等预定义报表模块，允许自定义报表模块。

3、设备参数模块：提供对系统各参数的设置，包括扫描参数、策略配置、评估参数、上下级引擎、互动配置、网络配置、时间设置、SMTP设置、IP授权。

4、状态监视模块：监视系统资源占用情况，对上下级引擎进行在线检测。实时显示系统硬件资源使用状态和当前登录用户，检测引擎在线情况。

5、维护工具模块：提供系统日常维护工具，包括日志管理、系统升级、导入导出、用户管理、角色管理、修改密码、网络测试、数据备份等。对全面记录系统的访问和重要操作，提供在线升级、本地升级、定时升级方式对漏洞和程序进行升级。导出XML格式的扫描任务文件，可将导出的任务文件和手持式的扫描结果文件导入系统。设定用户权限，登录IP和可扫描IP范围，设定和分配角色权限，检测目标主机是否在线，具有比PING更精确的检测功能。提供备份、恢复、导入、导出数据库功能。

6、辅助功能模块：提供多种模拟攻击的工具，包括端口扫描、弱密码破解、SQL注入检测等。对目标主机进行端口扫描，看对方开放哪些端口，对系统的SMB服务、FTP服务、TELNET服务、POP3服务存在的弱密码进行破解。

补丁分发安全管理系统：

1、安全控制中心：安全控制中心采用B/S架构管理端，具备设备分组管理、策略制定下发、全网健康状况监测、统一杀毒、统一漏洞修复、网络流量管理、终端软件管理、硬件资产管理以及各种报表和查询等功能，支持在虚拟机上安装控制中心，支持控制中心数据恢复与备份。

2、客户端：要求不少于200个客户终端数授权，具备漏洞集中修复、强制修复、自动修复，具备蓝屏修复功能，支持智能屏蔽过期补丁、与操作系统不兼容的补丁，可以查看或搜索系统已安装的全部补丁，支持补丁下载安装顺序设置，可以有效节省漏洞修复时间与减少CPU占用，支持漏洞集中修复过程中的流量控制，补丁分发支持服务端带宽限流与客户端P2P补丁分发加速，有效节省外网带宽资源。

3、病毒、恶意代码、木马防护能力：支持浏览器防护，对篡改浏览器设置的恶意行为进行有效防御，并可以锁定默认浏览器设置。支持文件解压缩病毒查杀，支持对zip、rar等多种格式的压缩文件查杀能力，对敲诈者病毒提供防护机制，同时提供解密工具，解密工具应为自主研发。

4、要求产品具备本地多引擎查杀能力，且引擎可配置。支持linux、国产操作系统杀毒、云桌面（至少两家）产品；要求产品在断网状态下具备不依赖病毒库特征的情况下对未知病毒查杀的能力；要求产品具备主动防御技术；要求产品具备应用级沙箱技术。

5、样本库数量：要求产品具备公有云检测能力，并且公有云特征储备超过100亿（提供证明文件并加盖厂商公章）。

防火墙设备：

1、规格性能：标准配置6个10/100/1000M自适应电口，支持1个扩展槽，1个Console口，1U机架结构，整机吞吐率≥4G，每秒新建连接数≥6万，并发连接数≥180万，64GB SSD固态硬盘存储，部署模式：产品支持路由、透明、交换以及混合模式接入，满足复杂应用环境的接入需求。支持旁路模式，网络协议：支持3G接入，可实现3G连接与有线链路之间的互为备份（要求提供截图，并加盖公章），支持MPLS的透传和针对MPLS的控制。支持802.3ad协议，并可根据：源目的MAC组合、MAC和IP组合或TCP/UDP端口组合等方式实现负载和备份。路由协议：支持静态路由、策略路由及动态路由。策略路由支持用户自定义其优先级，动态路由应至少支持RIP v1/v2/ng， OSPFv2/v3，BGP4/4+协议，支持静态和动态多播路由，动态多播路由必须支持PIM-SM（稀疏模式）。

2、DNS代理：支持入站的DNS代理功能，即从指定的入接口或源ISP接收到的DNS解析请求，设备可根据自定义的IP、域名对应关系，代理DNS服务器返回查询结果。支持出站的DNS代理功能，支持在不更改内网终端设备DNS服务器地址设置的情况下，将DNS解析请求发送至指定的DNS服务器，并代理原DNS服务器返回解析结果负载均衡：支持基于策略的路由负载，支持根据应用和服务进行智能选路，可基于权重做路由负载均衡，支持12种均衡方式：源地址目的地址哈希、源地址哈希、轮询、时延负载、备份、随机、流量均衡、源地址轮询、目的地址哈希、最优链路带宽负载、最优链路带宽备份、跳数负载，支持ISP路由负载均衡，最大可支持8条链路负载，支持自定义负载权重，持基于优先级的ISP路由链路备份。

3、虚拟防火墙功能：支持配置虚拟系统接口，在不占用物理网口的情况下实现虚拟系统之间的相互连接、访问。支持对虚系统进行系统配置，包括管理设定、管理主机、资产管理、证书管理、配置文件导入导出、日志配置。支持在虚系统内进行病毒防护、漏洞利用防护、间谍软件防护、URL过滤、文件过滤、内容过滤、邮件过滤、行为管控等安全功能，并可支持对本虚系统内产生的日志进行独立审计（要求提供截图，并加盖公章）。

4、访问控制：支持基于源安全域、目的安全域、源用户、源地址/地区、目的地址/地区、服务、应用、隧道、时间、VLAN等多种方式进行访问控制。要求设备可基于地理区域配置安全策略，并支持地理区域对象的导入。可实现应用控制，应用特征库包含的应用数量（非应用协议的规则总数）大于2400种。用户识别与认证：支持基于用户的访问控制，可与LDAP/Radius/证书、POP3等用户认证系统联动。URL过滤：支持URL云服务，设备可与云服务器联动查找本地未识别的URL，（需提供可体现URL云端协查的设备截图）。文件传输控制：支持识别HTTP、FTP、POP3、SMTP、IMAP、SMB等应用协议的文件传输行为，并能够对传输的文件进行双向的文件类型过滤。要求所支持识别的文件类型包含常用的文档格式、压缩文件格式和归档文件格式，总数量不少于30种。文件类型识别基于文件特征而非扩展名，更改文件扩展名后仍可有效识别。外发内容审计：支持对HTTP、FTP、POP3、SMTP、IMAP、SMB等应用协议的内容传输进行双向过滤，支持预定义敏感信息库及自定义敏感信息库两种方式进行敏感信息定义，支持阻断及日志两种处理动作；流量管理：支持可多层级、多调度类相互嵌套的带宽管理设置。支持设置每IP最大或最小带宽，支持对每IP进行带宽配合管理，可通过优先级实现多应用的差分服务，并支持对剩余带宽进行基于优先级的动态分配。网络攻击防护：支持防御DNS Flood攻击，并支持警告、阻断、普通防护、增强防护及授权服务器防护等多种防护措施，支持防御HTTP Flood攻击，并支持警告、丢弃、普通防护、增强防护等多种防护措施（要求提供截图）支持局域网广播防护，支持全局配置的局域网广播防护及基于二层接口的局域网广播防护，可以防止局域网内广播和多播数据包泛滥，保障网络正常通信（要求提供截图），支持DHCP防护，可进行DHCP服务器检查、DHCP请求检查和DHCP请求限速等功能（要求提供截图），支持防御IP地址欺骗，可将IP与安全域关联，即指定IP或网段从特定安全域流量流入。

5、病毒防护：能够对HTTP/FTP/POP3/SMTP/IMAP/SMB六种协议进行病毒查杀（要求提供截图，并加盖公章），支持对最多6级的压缩文件进行解压查杀，入侵防御：支持基于FTP、HTTP、IMAP、OTHER\_APP、POP3、SMTP等应用协议的漏洞防护和间谍软件防护。可防护的漏洞类型应至少包括：缓冲区溢出、跨站脚本、拒绝服务、恶意扫描、SQL注入、WEB攻击等。可防护的间谍软件类型应至少包括：木马后门、病毒蠕虫、僵尸网络等（要求提供截图，并加盖公章）支持自定义漏洞签名。可标识自定义漏洞的CVE编号或CNNVD编号。支持自定义基于TCP、UDP、HTTP协议的漏洞，并根据各协议的报文结构，指定一个或多个字段的特征值，这些特征值可以被以文本的形式或正则表达式的形式进行匹配，同时支持是否按顺序对这些特征值进行匹配检测。支持自定义漏洞的源端口范围及目的端口范围（要求提供截图，并加盖公章）。

6、IPSec VPN：支持IPSec VPN功能，并可以提供VPN客户端，可建立“网关-网关”、“客户端-网关”方式的加密隧道，IPSec VPN隧道支持冗余和负载功能，网络异常感知：支持统计网络中确认失陷的主机及有风险但不能完全确认为失陷的主机数量及风险等级状态，并支持查看失陷时间、威胁类别、情报来源、威胁简介、失陷主机IP、用户名、资产等信息，并支持一键跳转处置（要求提供截图，并加盖公章）。安全事件分析：所投设备需提供关联分析面板，可将Top应用、Top威胁、Top URL分类、Top源地址、Top目的地址等信息关联，并支持以任意元素为过滤条件进行数据钻取（要求提供截图）。可提供关联的威胁事件日志，系统可自动将产生威胁事件的连接经过防病毒、防漏洞、防间谍软件、URL过滤、文件过滤等安全模块检查的日志集中显示（要求提供截图，并加盖公章）。支持自定义时间范围内对防火墙上的全部日志进行模糊检索或指定条件的精确检索，快速定位特定目标当前行为是否存在异常，网络中是否存在异常等问题（要求提供截图，并加盖公章）。

附件3

谈判文件领取登记表

我公司已完全知悉本项目谈判公告，现申请到贵单位领取谈判文件。

|  |  |
| --- | --- |
| 项目名称 | 局域网安全防护系统设备竞争性谈判采购 |
| 项目编号 | 2017-HJGZJD-3001 |
| 供应商名称 |  |
| 领取时间 | 年 月 日 时 分 |
| 领取方式 | 派专人现场领取 |
| 领取人（签字） |  |
| 联系电话 |  |

公司名称（公章）：

经办人：

联系电话：

年 月 日

附件4

非外资企业或非外资控股企业的书面声明【参考模板】

（采购机构名称）：

【根据公司股东身份和出资方式、比例等信息如实自行编制，主动声明贵公司为非外资企业或非外资控股企业】

特此声明。

投标人全称：（盖章）

法定代表人（或授权代表）：（签字）

年 月 日

附件5

主要股东或出资人信息【参考模板】

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 序号 | 名称  （姓名） | 统一社会信用代码  （身份证号） | 出资方式 | 出资金额  （万元） | 占全部股  份比例 | 备注 |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

我方承诺，以上信息真实可靠；如填报的股东出资额、出资比例等与实际不符，视为放弃成交资格。

注：1.主要股东或出资人为法人的，填写法人全称及统一社会信用代码（尚未办理三证合一的填写组织机构代码）；为自然人的，填写自然人姓名和身份证号。

2.出资方式填货币、实物、工艺产权和非专利技术、土地使用权等。

3.报价方应按照占全部股份比例从大到小依次逐个股东填写，股东数量多于10个的，填写前10名，不足10个的全部填写。

报价方全称：（盖章）

法定代表人（或授权代表）：（签字）

年 月 日