**1、货物需求一览表**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **设备名称** | **单位** | **数量** |
| 1 | 网络防火墙 | 台 | 1 |

**2、技术标准和要求**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **名称** | **详细技术指标及功能需求** | **单位** | **数量** |
| **1** | **网络防火墙** | \*1、整机吞吐量≥30Gbps，七层吞吐量≥20Gbps，并发连接数≥10,000,000，每秒新建连接数≥320,000。  \*2、标准2U机架设备,冗余电源，≥16个千兆光口，≥4个万兆光口，≥2个高速USB2.0接口，≥1个RJ45串口。  3、支持路由，网桥，单臂，旁路，虚拟网线以及混合部署方式。支持链路聚合，上下行接口联动，802.1Q VLAN Trunk、access接口，子接口。支持静态路由，动态路由支持RIP，OSPF，支持基于5元组和应用类型的策略路由。  4、支持基于八元组的访问控制规则，八元组包括源／目的IP，源／目的端口，源／目的区域，用户（组），应用类型，服务类型。  #5、应用识别支持的应用总数超过1100种，识别规则总数超过3000条（提供产品界面截图并加盖厂商公章）。  6、支持Land、Smurf、Fraggle、WinNuke、Ping of Death、Tear Drop、IP Spoofing攻击防护、支持SYN Flood、ICMP Flood、UDP Flood、DNS Flood、ARP Flood攻击防护，支持IP地址扫描，端口扫描防护，支持ARP欺骗防护功能、支持IP协议异常报文检测和TCP协议异常报文检测。  7、支持IPv4／IPv6 NAT地址转换，支持源目的地址转换，目的地址转换和双向地址转换，支持针对源IP或者目的IP进行连接数控制。  8、支持基于应用类型的策略路由应用引流。  9、支持URL过滤和文件过滤功能，URL过滤支持GET，POST请求过滤和HTTPS网站过滤，文件过滤支持文件上传和下载过滤。  10、支持入侵防护功能，且入侵防护漏洞特征具备中文相关介绍，包括但不限于漏洞描述，漏洞名称，危险等级，影响系统，对应CVE编号，参考信息和建议的解决方案。可以对SSL加密数据进行入侵行为检测. (提供产品界面截图并加盖厂商公章)  11、入侵防护漏洞规则特征库数量在3900条以上（提供产品界面截图并加盖厂商公章）。  #12、支持对常见应用服务和数据库软件的口令暴力破解防护功能，且支持对常见应用服务和数据库软件的的弱密码扫描（提供产品界面截图并加盖厂商公章）。  #13、支持SQL注入防护、XSS攻击防护、CSRF攻击防护、系统命令注入防护，文件包含攻击，目录遍历攻击，信息泄露，恶意爬虫，网站扫描等，具备独立的Web应用防护规则库，Web应用防护规则总数在3000条以上（提供产品界面截图并加盖厂商公章）。  #14、支持针对Web内容管理系统的安全防护，如dedecms，phpcms，phpwind，Empirecms，discuz，wordpress，joomla等，支持的CMS类型数量不少10种（提供产品界面截图并加盖厂商公章）。  #15、支持Web漏洞扫描功能，可扫描WEB网站SQL注入、XSS、跨站脚本、目录遍历、文件包含、命令执行等脚本漏洞（提供产品界面截图并加盖厂商公章）。  16、支持敏感数据防泄密功能，内置预定义的敏感信息类型，如银行卡号、邮箱、身份证、手机号码、MD5等，支持敏感信息自定义，支持根据文件类型进行敏感文件下载过滤。  #17、支持对客户端／服务器是否被种植了远控木马或者其他病毒，恶意软件从而形成僵尸主机进行检测，僵尸主机识别特征总数在60万条以上（提供产品界面截图并加盖厂商公章）。  #18、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（提供产品界面截图并加盖厂商公章）。  #19、支持对指定IP自定义业务名称，在报表中可快速识别业务系统存在的漏洞威胁和遭受攻击情况；  #20、支持网关型网页防篡改，支持动态网页/静态网页篡改防护，全面保护网站的静态网页和动态网页，支持网页的自动发布、篡改检测、应用保护、警告和自动恢复，保证传输、鉴别、地址访问、表单提交、审计等各个环节的安全，完全实时杜绝篡改后的网页被访问的可能性及任何使用Web方式对后台数据库的篡改（提供产品界面截图并加盖厂商公章）。  #21、支持对经过设备的流量进行分析，发现被保护对象存在的漏洞（非主动扫描），并根据被保护对象发现漏洞数量进行TOP 10排名，列出每个服务器发现的漏洞类型以及数量，支持生成和导出威胁报告，报告内容包含对整体发现的漏洞情况进行分析。（提供威胁报告并加盖厂商公章）  #22、提供安全报表，报表内容体现被保护对象发现漏洞情况以及遭受到攻击的漏洞统计，可以查看到有效攻击行为次数和攻击趋势。（提供安全报表并加盖厂商公章）  #23、支持目的地址转换，包括地址和端口静态转换映射;支持源地址转换，包括静态、动态地址转换和动态端口转换三种机制。支持双向地址转换，支持一条策略完成源和目的地址转换。系统应具备完整的地址转换日志，至少保存60天日志。  #24、系统支持外置数据中心，支持自定义统计指定IP/用户组/用户/应用在指定时间段内的服务器安全风险、终端安全风险等内容，并形成报表；支持每天/每周/每月自动生成报表，并将报表自动发送到指定邮箱，可以自定义报表内容；支持报表以HTML、Excel、PDF等格式导出。 | **台** | **1** |

**3、质保及售后服务要求**

3.1所有投标产品3年免费质保。

3.2所有产品接到采购人保修电话4小时免费上门服务，24小时排除故障。

3.3在质保期内所有产品提供免费配置服务。