南京市江宁医院防火墙项目需求

一、项目建设内容

南京市江宁医院防火墙项目主要进行网络安全边界加固建设。考虑重要节点、重要设备，规划在互联网出口部署2台一体化安全网关；在湖山路院区与其他院区之间部署1台一体化安全网关。主要用于实现医院内部、外部网络之间的边界隔离、访问控制等安全防护。同时满足等保三级通用技术要求8.1.2安全通信网络-8.1.2.1网络架构d)；8.1.3 安全区域边界-8.1.3.1边界防护a)、8.1.3 安全区域边界-8.1.3.2访问控制a)b)c)d)。

二、产品关键技术及主要功能

防火墙是实现网络安全最重要的基础设施之一，而访问控制则是防火墙最基础也是最核心的安全特性。传统防火墙使用基于IP和端口信息作为其实现访问控制和流量分类的基础参数，然而，在新一代业务环境下，新的攻击者通常对网络流量进行了伪装。此外，用户对带宽资源的管理需求也日益增强。面对海量应用、复杂攻击，传统防火墙基于IP和端口的分类方式难以有效落实管理意图，难以将安全控制能力有效落地。

本次选用的一体化安全网关需要采用多平面系统架构、多核并行处理、一体化报文处理引擎、智能应用识别和用户识别、软件定义广域网SDWAN等关键技术。支持强安全控制、智能流量控制、入侵防御、病毒过滤、WEB防护、SDWAN、基于沙箱和威胁情报的高级持续威胁（APT）检测防御及多维度网络状态可视化呈现等功能。同时提供防火墙日志云端存储与分析服务；支持基于硬件技术的底层虚拟化；支持扩展集中策略分析模块，可集中对所有防火墙安全策略进行冗余、收敛、潜在冲突分析，能够确保各项功能和性能的有效实现。

具体功能需求如下：

一）、性能要求

1. 互联网出口一体化安全网关 2台

**★标准2U设备，双电源；标配6个10/100/1000M自适应千兆电接口和12个combo接口[每个Combo口为一对互斥的千兆口，即1个千兆SFP插槽（不含SFP模块）和1个千兆电口]；同时标配》=60G硬盘；具备下一代防火墙访问控制，支持入侵防御、网络防病毒、上网行为及URL分类管理、流控和IPSec VPN模块；并发连接数320万，吞吐不低于8G**。

1. 院区边界一体化安全网关 1台

**★标准2U设备，双电源；标准配置10个10/100M/1000M自适应千兆电接口、8个千兆SFP接口（不含SFP光模块）及4个万兆接口；另外设备包含至少3个扩展板卡，可以扩展到最多34个接口。标配》=60G硬盘；具备下一代防火墙访问控制、支持入侵防御、网络防病毒、上网行为及URL分类管理、流控和IPSec VPN模块；吞吐不低于30G。**

二）功能需求

|  |  |
| --- | --- |
| 功能项 | 技术要求 |
| 系统架构 | 采用专用多核硬件平台 |
| **★虚拟化** | 支持基于硬件技术的底层虚拟化，各个虚拟防火墙之间完全隔离，可运行不同的防火墙版本，拥有完全独立的CPU、内存、接口等资源。提供虚拟防火墙层资源配置管理界面截图。  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。 |
| 访问控制 | **★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，提供相关界面截图** |
| **★支持基于策略的流量统计和会话统计** |
| 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。提供相关界面截图。 |
| **★支持详细的访问控制策略日志，每条匹配策略的会话均可记录其建立会话和拆除会话的日志；访问控制策略日志可本地记录或发送至Syslog服务器。提供策略配置界面截图及防火墙本地记录的策略建立会话及拆除会话的日志截图**。 |
| 应用控制 | 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 |
| 支持针对应用动作、应用内容的细粒度控制，如设定允许登录的QQ帐号白名单、邮件关键字过滤等 |
| 支持并开通WEB控制功能模块，包括URL访问分类管理、网页关键字过滤、http文件下载类型管理等功能，提供相关页面截图。 |
| URL分类库规模不少于1000万条 |
| 支持IPv6环境下的应用行为管理和控制 |
| 流量控制 | 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，提供至少四层管道嵌套的流控界面截图。 |
| 支持基于接口的上下行带宽管理 |
| 支持高、中、低优先级通道设置 |
| 支持基于应用、用户、源地址、目标地址、服务、时间的通道匹配 |
| 支持带宽限制、带宽保障和弹性带宽 |
| 会话控制 | 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。提供相关界面截图 |
| 入侵防御 | 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 |
| 支持基于接口/安全域、地址、用户、服务、应用和时间的入侵防御策略设定，每个入侵防御策略均可配置检测事件及响应方式。提供相关界面截图。 |
| 具备协议自动识别功能；支持自定义事件功能； |
| 支持IPv6环境下的入侵防御功能，支持在线、旁路及混合部署 |
| WEB防护 | 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，要求相关技术具备自主研发专利，可在国家版权局网站查询，提供查询结果网页截图及专利号； |
| 支持IPv4和IPv6对Web业务实现应用层安全防护 |
| **★APT防御** | 支持扩展APT检测模块，采用沙箱检测技术，对未知木马、病毒、恶意代码具有精确的检测效果，实现对未知威胁、高级持续威胁和0DAY攻击的有效防护。 |
| 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； 提供相关界面截图。 |
| 内置多种沙箱环境与应用环境，使用反反沙箱、时光加速、机器学习等领先技术，确保恶意样本逃逸率大幅降低。 |
| 威胁情报防护 | 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。提供防火墙配置界面及威胁情报云端界面截图。 |
| 支持IPv4和IPv6环境下威胁情报查询和实时防护 |
| 防病毒 | 支持并开通对HTTP、FTP、SMTP、POP3、IMAP协议的病毒检测和过滤功能； |
| 支持基于接口/安全域、地址、用户、服务、应用和时间的防病毒策略设定，提供相关界面截图。 |
| 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。 |
| 防病毒功能开启后，整机处理性能衰减不超过30% |
| 支持IPv4和IPv6环境下病毒检测和过滤功能 |
| **★SDWAN** | 支持广域网双边优化，通过使用TCP动态拥塞控制、TCP窗口处理机制优化、TCP选择性应答、使用快速TCP协议传输以及数据压缩机制，实现对业务访问的有效加速。 |
| 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；提供相关界面截图 |
| 支持多链路智能选路，根据业务对抖动、时延和带宽的要求，在多条不同链路上智能动态选路，通过自动重传技术，实现链路切换时无丢包，业务不掉线；提供相关界面截图 |
| 通过WAN虚拟化技术实现多条链路捆绑，同一个session数据可以在多条链路上同时传输，加速大文件复制业务；提供相关界面截图 |
| 安全联动 | 支持与IDS设备的联动，可接收IDS产品发送的动态访问控制策略；提供相关界面截图； |
| 支持与终端管理系统的联动，可接收终端管理系统的主机状态列表，将不合规终端的访问重定向至终端管理指定页面； |
| 网络特性 | 支持透明、路由、混合、旁路等部署模式； |
| 支持静态路由、动态路由（RIP、OSPF、BGP4），提供相关界面截图。 |
| 支持基于入接口、源地址、目标地址、服务端口、应用类型、域名的策略路由。提供相关界面截图。 |
| 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，支持链路负载均衡的目的会话保持功能；提供相关界面截图。 |
| 支持并开通IPSec VPN和L2TP VPN，投标产品实配IPSec VPN隧道数量不少于10000条。 |
| 支持并开通SSL VPN功能，投标产品实配SSL VPN并发用户数不少于3000个。 |
| 支持GRE |
| 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，提供相关界面截图。 |
| 支持源NAT、目的NAT、静态NAT，支持一对一、一对多和多对多等形式的NAT |
| 支持各种应用协议的NAT穿越：FTP、TFTP、H.323、SQL＊NET |
| 支持标准DHCP服务功能，支持DHCP条件下的IP/MAC绑定及IP地址排除等功能。 |
| 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。提供相关界面截图。 |
| 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。提供相关界面截图。 |
| 高可用性 | 支持主-主和主-备模式，主备模式下支持基于设备优先级的主设备抢占功能。 |
| 支持基于心跳信号丢失、链路断开等多种方式的HA切换条件及逻辑 |
| 支持HA设备之间的会话自动同步，包括主主模式和主备模式，确保HA切换时业务不发生任何中断 |
| 支持双路HA物理心跳线，确保HA运行稳定可靠 |
| 支持HA设备之间的配置自动同步，确保用户只需在一台设备进行业务配置 |
| 系统管理 | 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 |
| 支持SYSLOG和SNMP v3，SYSLOG日志支持同时发给多个日志服务器 |
| 支持威胁可视化技术和流量可视化技术，可提供详细的分析展示图表。 |
| 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。提供相关界面截图。 |
| 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。提供相关界面截图 |
| 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、1天、7天和30天。提供相关界面截图 |
| 云日志 | 提供防火墙日志云端存储与分析服务，提供无限量云端日志存储空间 |
| 支持微信告警推送，微信报表推送，任意时间地点的日志查询服务 |
| 集中管理 | 支持防火墙集中管理，包括统一状态监控、配置下发、配置自动备份及回滚、版本统一升级、特征库统一升级等功能。 |
| 支持扩展集中策略分析模块，通过集中策略分析模块，实现：  集中对所有防火墙安全策略进行冗余分析，可分析出哪些安全策略是不必要的冗余配置  集中对所有防火墙安全策略进行收敛分析，也称宽松策略分析。能够支持查看任何一条宽松策略的流量详细信息  集中对所有防火墙安全策略进行命中频率分析，辅助用户快速完成策略次序的调整，从而达到优化防火墙处理性能的目的。  集中对所有防火墙安全策略进行潜在冲突分析，辅助用户快速完成策略的调整，从而达到防火墙访问控制的目的。  提供上述功能截图。 |
| **★原厂服务** | 必须包含三年维保服务，提供原厂实施与支撑服务； |
| 资质要求 | 厂商资质：  **★产品原厂商具备安全服务二级资质和应急响应一级资质及以上资质**  产品原厂商有充分的网络安全研究能力，具备自主发掘漏洞能力  **★产品原厂商为国家级网络安全应急支撑团队**  **★产品原厂商具备国家信息安全服务资质 安全工程类 三级资质**  **★销售许可证：产品具备中华人民共和国公安部颁发的《计算机信息系统安全专用产品销售许可证》，且认证等级为增强级；**  **★型号证书：产品具备中国国家信息安全认证中心颁发的《中国国家信息安全产品认证证书》，且认证等级为增强级；**  产品具备中国国家信息安全测评认证中心颁发的《信息技术产品安全测评证书》证书  **★自主原创证书：产品具备中国信息安全测评中心颁发的信息安全产品自主原创证明**  **★IPv6认证：产品具备全球IPv6测试中心颁发的《IPv6 Ready》金牌认证证书**  **★版权证书：产品具备国家版权局颁发的《计算机软件著作权登记证书》及多核安全操作系统软件著作权**  **★中标单位需在中标后一个礼拜提供测试机进行功能逐条测试，与投标偏离表进行响应。若发现偏离表中有虚假应标项的将取消中标资格，由满足功能要求且排名靠前的公司中标。** |

三、投标人资质要求：

1、符合《中华人民共和国政府采购法》第二十二条规定应当具备的条件；

2、投标人为在中华人民共和国注册的独立企业法人；

3、未被“信用中国”网站（www.creditchina.gov.cn）列入失信被执行人、重大税收违法案件当事人名单、政府采购严重失信行为记录名单；

四、询价地点及时间

1. 地点：南京市江宁医院湖山路院区1号楼一楼（江宁区湖山路169号）
2. 时间：2020年6月8号14：30

五、通讯联络事宜：

联系人：王老师 杜老师

电 话： 52087300 15950530382