上海市徐汇区教育局教育城域网安全隔离区设备政府采购项目 采购需求文件

特别说明：

如供应商认为本磋商文件存有倾向性、排斥性内容，或有歧视性要求的，请人须知前附表规定的时间方式向采购方提出。

一、项目概况

上海市徐汇区教育局教育城域网是徐汇区教育信息化工作的核心平台，在城域网核心区域部署了200多台服务器，为全区中小学、幼儿园、各教育单位以及互联网提供DNS、WEB、OA、MAIL、视频会议、视频监控、私有云等服务。随着部署业务的类型和数量的增加，业务赖以生存的服务器及服务器运行环境的安全和稳定也日益显得关键和重要。传统的服务器运行环境在发生一些安全事件时，例如网络攻击、传染性网络病毒等，容易导致核心区域乃至全网受到牵连和影响，从而降低了业务的可用性和城域网的可用性。鉴于此，安全隔离区（DMZ区域）的建立是解决目前业务和网络安全隐患的最佳方式。

二、设计原则

1、设计依据

本项目的建设以《中华人民共和国国民经济和社会发展第十四个五年规划和2035远景目标纲要》提出的“加强网络安全保护”为指导，参照《中国教育现代化2035》所要求的“加快信息化时代教育变革”和教育部关于教育行业信息化建设的相关要求作为指引，结合徐汇区教育系统的现状，规划徐汇区教育局教育城域网DMZ区安全建设项目。

参照标准与依据：

- 中共中央、国务院、国家发展和改革委员会印发《中华人民共和国国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要》；
- 中共中央、国务院印发《中国教育现代化2035》；
- 中共中央办公厅、国务院办公厅印发《加快推进教育现代化实施方案（2018—2022年）》；
- 国家发展改革委、教育部、人力资源社会保障部印发《“十四五”时期教育强国推进工程实施方案》；
- 中华人民共和国教育部《教育部2021年工作要点》

- 网络安全等级保护基本要求（GB/T 22239-2019）
- 网络安全等级保护安全设计技术要求（GB/T 25070-2019）
- 网络安全等级保护测评要求（GB/T 28448-2019）
- 网络安全等级保护安全管理中心技术要求（GB/T 36958-2018）

2、建设目标

本项目主要针对 DMZ 区域的进行系统的安全建设，利用下一代防火墙、WAF、负载均衡及主机检测与响应等安全产品，提升 DMZ 区域整体检测与防御能力，能够对异常网络攻击、DDoS 攻击、web 应用攻击、挖矿病毒等进行安全防护。对服务器或云主机的东西向流量行进检测，做到 DMZ 区服务器之间微隔离，解决病毒东西向、横向移动和内网扩散的等问题，为 DMZ 区域的业务系统保驾护航。 同时，对服务器做链路负载和 IPv6 DNS 解析，将 IPv4 地址和 IPv6 地址互相翻译，满足门户网站 IPv6 线路接入访问与安全需求。

为了保障本项目与前几期安全建设的一致性与集中管理，本次建设严格按照徐汇区教育城域网安全顶层设计规划执行，将下一代防火墙、WAF、EDR 等安全设备需接入教育信息中心端安全感知平台进行数据的统一采集和分析展示，DMZ 边界安全状况实时上报监控，及时了解全网安全动态，减少安全运维人员成本，并能通过安全日志的集中管理与分析，多维度信息找到风险来源点和防护薄弱点，进行立体化安全防御。

三、需求说明

根据对 DMZ 区的威胁和风险分析，其建设目标需求主要包括以下方面：

1、防御黑客扫描、渗透入侵、蠕虫、网络病毒等攻击，保障基础网络信息系统的安全性;

2、防御各种流量型、资源耗尽型、应用层 DDoS 攻击，提高网络信息系统的可用性;

3、防御针对 Web、Mail 等业务系统的攻击，保证业务系统的安全稳定运行。

4、各业务需要支持 IPv6 访问，要求 DMZ 区域主要访问链路上的网络与安全设备支持 IPv6。

5、建立纵深的边界安全防御体系、多维度安全监测、预警体系，在整个 DMZ 区域边界、服务器计算环境建立全面的安全防范、建立高可用和高级威胁检测等异常行为预警机制及事后审计追踪机制，完善纵深防护基础设施，提升检测覆盖和自动化检测水平;

四、建设内容

1、DMZ 边界安全加固

首先针对 DMZ 出口区域部署下一代防火墙，针对汇聚数据进行 L2—L7 的深度攻击防御，进行区域划分、隔离防御，主要针对异常网络攻击、反向 DDOS、恶意主机风险、终端漏洞攻击、僵尸网络、分客蠕虫等进行安全防护和分析。例如，内网主机中僵尸木马，针对数据中心进行反向 DDOS 攻击，影响 DMZ 服务器的安全稳定运行。实现加固边界安全同时，能有效隔离城域网内产生的安全威胁，避免通过城域网感染 DMZ 区，甚至被动攻击教育局的数据中心。

2、DMZ 区 web 应用防护

针对 SQL 注入攻击、XSS 跨站脚本攻击、CSRF 攻击命令注入攻击等 web 类攻击行为。通过部署 Web 应用防火墙可以通过高效的 URL 过滤技术，过滤 SQL 注入的关键信息，从而有效的避免网站服务器受到 SQL 注入攻击。跨站攻击产生的原理是攻击者通过向 Web 页面里插入恶意 html 代码，从而达到特殊目的。Web 应用防火墙通过数据包正则表达式匹配原理，可以准确地过滤数据包中含有的跨站攻击的恶意代码，从而保护 DMZ 区域的 WEB 服务器安全。

3、DMZ 运维与审计安全

本地内网依照业务系统和网络系统承载的功能不同和安全需求的不同划分了各类区域，来自互联网的大部分攻击和威胁可以通过互联网出口的下一代防火墙进行十分有效的防护，但是整体网络安全建设不能仅仅考虑外网的安全防护，更应该关注 DMZ 区的运维安全防护，潜伏在内网的安全风险极易通过内网进行横向传播，容易导致 DMZ 网络的安全问题严峻。通过运维审计、日志审计、数据库审计，对 DMZ 网络边界、重要网络节点进行安全审计，审计覆盖到事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等，审计记录的留存时间 6 个月以上且不中断。对远程访问的用户行为、服务器安全事件运维审计日志等进行综合的日志数据分析。

4、DMZ 服务器工作负载保护与异常流量监测

DMZ 区服务器的工作负载保护与传统部署在网络边界上的安全产品有所区别，服务器工作负载保护需基于代理底层技术方案，部署在操作系统层，可以横跨物理服务器、私有云、混合云等多种数据中心环境，并支持云、物理、混合环境部署，能有效帮助用户安全加固服务器、抵御黑客攻击和恶意代码等威胁分析工作。全面且灵活的基线配置检查，协

助用户实现云主机安全配置的集中采集风险分析、处理等工作，并提供详尽的、可实际运行的系统、应用加固方案，指导用户快速处理不安全的配置，从源头解决安全问题。

此外，由于 DMZ 区域访问特征，对外提供大量服务，所以极易被攻击，产生大量威胁、异常流量，需要进行监测处置，计划在 DMZ 区部署潜伏威胁探针，将 DMZ 区流量镜像至探针，对用户到业务资产、业务的访问关系进行识别，基于捕捉到的网络流量对内部进行初步的攻击识别、违规行为检测与内网异常行为识别。发现 DMZ 区域潜伏的安全问题，上报至徐汇区教育局安全态势感知与安全运营中心，及时的进行分析处理。

5、DMZ 服务器负载均衡

运用多台服务器集群的机制，负载均衡设备能将所有真实服务器配置成虚拟服务来实现负载均衡，对外直接发布一个虚拟服务 IP。当用户请求到达负载均衡设备的时候，根据预先设定的基于多重四、七层负载均衡算法的调度策略，能够合理的将每个连接快速的分配到相应的服务器，从而合理利用服务器资源。不仅在减少硬件投资成本情况下解决单台服务器性能瓶颈，同时方便后续扩容，为大并发访问量的系统提供性能保障，提供高可用性。通过多重负载均衡算法将所有流量均衡的分配到各个服务器，不仅充分利用所有的服务器资源，而且各个服务器均衡的承担流量处理任务，从而有效地避免服务器处理任务“不平衡”现象的发生。

五、建设清单

序号	产品名称	服务年限	数量	单位
1	DMZ 区汇聚交换机	3 年	2	台
2	DMZ 区边界防火墙	3 年	2	台
3	DMZ 区 web 应用防火墙	3 年	2	台
4	DMZ 区业务负载均衡	3 年	2	台
5	DMZ 区潜伏威胁探针	3 年	1	台
6	DMZ 区日志审计系统	3 年	1	台
7	DMZ 区数据库审计系统	3 年	1	台
8	DMZ 区堡垒机系统	3 年	1	台

六、产品技术参数要求

1、DMZ 区汇聚交换机

功能及技术指标	参数要求
▲交换机性能	**交换容量≥38.4Tbps，包转发率≥7200Mpps**
▲业务插槽数	**业务插槽数≥3**
电源冗余	电源模块冗余
关键部件热插拔	主控交换卡、电源、接口模块、风扇、网板等关键部件可热插拔
主控引擎	主控引擎模块≥2，满足 1+1 冗余
链路聚合	聚合组数≥1000 组，每组成员≥32 个
	支持 DRNI 跨设备链路聚合
ACL	支持双向 ACL，ACL≥4K
	支持端口 ACL
	支持 VLAN ACL
QOS	每端口支持 8 个优先级队列，3 个丢弃优先级，支持 SP、WRR、SP+WRR 三种队列调度算法
	支持精细化的流量监管，粒度可达 8K
	支持流量整形 Shapping
	支持 WRED 拥塞避免
	支持 802.1p、TOS、DSCP、EXP 优先级映射
可靠性	双引擎快速倒换，主备切换时候板内转发无丢包
	支持 NSF/GR for OSFP/BGP/IS-IS
	支持热补丁功能，可在线进行补丁升级
	支持 BFD，BFD for VRRP/BGP/IS-IS/OSPF/RSVP/LDP/RIP/静态路由。
MAC	MAC 表≥288K
路由表	路由表≥256K
IPv6	支持 RIPng、OSPFv3、BGP4+、IS-ISv6 协议 支持 IPv6 策略路由； 支持 DHCPv6 功能、IPv6 portal 功能、IPv6 管理功能； 支持基于 IPv6 的 VXLAN 二三层互通； 支持基于 IPv6 的 VRRP 功能
ARP	ARP 表≥170K
	ARP 表≥256K
虚拟化	多虚一技术(N:1)，支持 4 框虚拟化技术
	一虚多技术（1:N）
	支持多虚一技术和一虚多技术的配合使用
	通过远程端口扩展，作为控制设备（Controlling Bridge,CB）实现对端口扩展模块（Port Extender,PE）的集中控制，支持二级端口扩展设备级联
	支持基于 IRF3.1 的有线无线统一管理功能
网络安全一体化	支持安全业务插卡 FW、IPS、ACG、LB、SSL VPN
可视化	支持 Telemetry 流量可视化功能

有线无线一体化	支持 AC 板卡，POE，POE+
	支持融合 AC 功能， 无需额外配置单独硬件， 并且能在交换机上对所有上线的 AP 进行管理与配置
	支持有线无线一体化的终端准入认证
网管功能一体化	支持内置 SmartMC 智能图形化管理功能，能够实现通过图形化界面设备配置及命令一键下发和版本智能升级
多业务融合化	支持多业务融合板卡，与设备紧耦合无需外部连线，支持部署 Windows Server，实现方案与设备一体化部署
终端管理及网络安全	支持 PC 终端、哑终端、网络设备等连接元素的准入控制和权限划分，确保网络的可信可控 支持设备识别、归类、类型定义，可以对全网资产进行梳理，识别异常终端链接，确保网络的安全性
MPLS	支持 L3 VPN
	支持 VLL
	支持 VLPS
	支持 MCE
FCoE	支持 FCoE 功能
SDN/OPENFLOW	支持 OPENFLOW 支持普通模式和 Openflow 模式切换 支持多控制器（EQUAL 模式、主备模式） 支持多表流水线 支持 Group table 支持 Meter
跨三层互联技术	支持主流的 MAC in IP 技术，如 EVI，实现跨三层网络的二层互联
VxLAN	支持 VXLAN，能够实现 VXLAN 二三层互通
安全特性	支持 IPv4 uRPF
	支持 DHCP Snooping
	支持 ARP 防攻击
	支持 IP Source Guard
	支持 CoPP
	支持广播风暴抑制
	支持 EAD
	支持 MACsec 加密技术
管理特性	支持 Console/AUX/Telnet/SSH2.0
	支持风扇管理
	支持电源管理
	支持在线诊断
	支持 SNMPv1/v2
	支持 SNMPv3
	支持 RMON(RFC2819)
	支持端口镜像
	支持 VLAN 镜像

	支持 RSPAN
	支持流镜像
NAS	支持 802.1x
	支持 mac 认证
	支持 Portal
	支持本地认证
	支持 Radius 认证
	支持 Tacacs+认证
成熟度	提供工信部入网证
▲配置要求	**配置双主控， 实配万兆光口≥24 口，千兆电口≥48，冗余电源模块**

2、DMZ 区边界防火墙

项目	功能项	功能说明
硬件要求	硬件平台	产品采用多核并行处理架构，使用 X86 架构多核处理器，提供中国信息安全测评中心、公安部信息安全产品检测中心、中国软件评测中心、国家版权局之中任意一家机构出具的关于“多核并行安全操作系统”的证书或测试报告。
	硬件规格	机箱规格：1U，内存大小≥8G， minisata SSD 硬盘,硬盘容量≥128G ，电源：冗余电源 接口：千兆电口≥6 个，万兆光口 SFP+≥2 个
性能要求	性能要求	网络层吞吐量≥20Gbps，并发连接数≥220 万，每秒 HTTP 新建连接数≥15 万。
基础网络特性	部署方式	支持路由、透明、虚拟网线、旁路镜像、混合等多种部署方式，适应复杂使用环境的接入要求。
	VPN 功能	产品支持 IPsec VPN 和 SSL VPN 功能。
	路由功能	支持基于 IP 地址、端口、地域、协议、应用等维度配置策略路由策略，支持多种负载均衡算法，包括加权、带宽比例、轮询、线路排序等。
应用控制	应用识别	**▲产品支持对不少于 9500 种应用的识别和控制，应用类型包括游戏、购物、图书百科、工作招聘、P2P 下载、聊天工具、旅游出行、股票软件等类型应用进行检测与控制。（需提供产品功能截图证明）**
	流量控制	产品支持多维度流量控制功能，支持基于 IP 地址、用户、应用、时间设置流量控制策略，保证关键业务带宽日常需求。
	会话控制	**▲产品支持基于地区维度设置流控策略，实现多区域流量批量快速管控功能。所投产品必须提供具备 CMA 认证的第三方权威机构关于“国家/地区的流量管理”功能项的产品检测报告。**
		产品支持基于 IP 对象的会话控制策略，实现并发连接数的合理限制。
访问控制	地域访问控制	支持基于对象、区域和地域维度设置安全访问控制策略，允许或拒绝特定国家或者地区的对象访问内部网络，保障业务重大时期安全可靠性。
安全能力	入侵防御	产品预定义漏洞特征数量超过 7600 种，支持在产品漏洞特征库中以漏洞名称、漏洞 ID、漏洞 CVE 标识、危险等级和漏洞描述等条件快速查询特定漏洞特征信息，支持用户自定义 IPS 规则。

		▲产品支持用户账号全生命周期保护功能，包括用户账号多余入口检测、用户账号弱口令检测、用户账号暴力破解检测、失陷账号检测，防止因账号安全问题导致的非法提权情况发生。（需提供产品功能截图证明）
		产品支持基于 IMAP、FTP、RDP、VNC、SSH、TELNET、ORACLE、MYSQL、MSSQL 等应用协议进行深度检测与防护。
	防病毒	产品支持对多重压缩文件的病毒检测能力，支持不小于 12 层压缩文件病毒检测与处置。
		产品支持病毒例外特征设置，根据文件 MD5 值和文件 URL 设置病毒白名单，不对白名单进行病毒查杀。
		▲产品支持勒索病毒检测与防御功能，为保障勒索病毒的防御效果，所投产品必须提供具备 CMA 认证的第三方权威机构关于“勒索软件通信防护”功能项的产品检测报告。
	勒索专防	具备勒索软件通信防护功能，提供具备 CNAS（中国合格评定国家认可委员会）资质的第三方权威机构关于“勒索软件通信防护”产品功能检测报告。
	DDOS 防护	产品支持对 ICMP、UDP、DNS、SYN 等协议进行 DDOS 防护。
安全运维管理	策略优化	支持对当前应用控制策略异常分析，包括策略风险访问、策略冗余、策略冲突、策略重合、端口放通过大等问题，并提供相关解决方案便于用户快速调优。
	策略生命周期管理	**▲支持应用控制策略生命周期管理，包含安全策略的变更时间、变更类型和策略变更用户，并对变更内容记录日志，方便策略的管理和运维。（需提供产品功能截图证明）**
	与统一管理平台对接	**▲要求终端安全监测系统具备接入徐汇区教育局现有统一管理平台的功能，实现节点设备配置策略下发、升级管理、设备监控告警等功能。（需提供产品功能截图证明）**
资质要求	产品资质	要求所投产品在 IDC 在 2020 年 UTM 品类市场占有率排名前三，提供有效证明材料。
		要求所投产品具备国家信息安全漏洞库兼容性资质证书，提供有效证书复印件。
	厂商资质	要求所投产品的生产厂商为国家信息安全漏洞共享平台(CNVD)技术组支撑单位成员，提供有效证书的复印件。

3、DMZ 区 web 应用防火墙

技术指标	指标要求
硬件平台	产品采用多核并行处理架构，提供中国信息安全测评中心、公安部信息安全产品检测中心、中国软件评测中心、国家版权局之中任意一家机构出具的关于“多核并行安全操作系统”的证书或测试报告。
硬件要求	规格：1U 机箱，内存大小≥8G，SSD 硬盘容量≥128GB
	接口：千兆电口≥6 个，万兆光口 SFP+≥2 个。
性能要求	网络层吞吐量≥20Gbps，并发连接数≥220 万，每秒 HTTP 新建连接数≥15 万。

部署方式	支持虚拟网线部署、透明部署、路由部署、旁路镜像等多种部署方式，适应复杂使用环境的接入要求。
IPv6 要求	支持 IPv4/IPv6 双栈工作模式。
	支持 IPv6 环境的安全策略设置，实现 Web 应用防护等安全功能。
协议解析	支持 HTTP、HTTPS 协议流量检测。
	支持 XML、JSON 格式解析。
	支持伪静态解析。
	支持通过 X-Forwarded-For、Cdn-Src-Ip、Clientip 三种方式识别访问的源 IP、并用于日志记录和联动封锁。
HTTP 异常检测	支持识别 HTTP 异常，包含 HTTP 方法过滤、HTTP 头部字段 Referer、User-Agent 等注入检测、Host 检测、URL 溢出检测、POST 实体溢出检测、HTTP 头部溢出检测、range 字段防护、multipart 头部字段异常检测。（需提供产品功能截图证明）
Web 应用防护	**▲支持总防护规则需≥6000 种。其中 Web 应用防护规则至少≥4500 种，Web 应用漏洞攻击防护规则至少≥1000 种。（需提供产品功能截图证明）**
	支持防护 SQL 注入、XSS 攻击、网页木马、网站扫描、Webshell、跨站请求伪造（CSRF）、系统命令注入、文件包含攻击、目录遍历攻击、信息泄露攻击、Web 漏洞攻击等。
	支持 Cookie 攻击防护，支持检测到篡改时将 Cookie 替换为*，支持自定义需要防护的 Cookie 属性范围，包括防护所有 Cookie 属性、防护指定 Cookie 属性、不防护指定 Cookie 属性。
	支持自定义 Web 应用防护规则，通过基于正则表达式自定义规则匹配方向、动作、字符串、危险等级、动作、攻击影响、描述等。
机器人	**▲产品原生支持 BOT 防护功能，可过滤机器人自动化流量，非联动其他组件或产品，并支持用户自定义 URL 保护范围和保护阈值。（需提供产品功能截图证明）**
流量防护	支持自定义 BOT 防护排除功能，支持通过 IP 地址白名单、User-Agent、URL 前缀的方式排除。
语义分析	**▲支持语义引擎用于检测 Web 攻击，能针对不同类型的 Web 攻击如命令注入攻击防护等，单独选择开启或关闭语义引擎检测。（需提供产品功能截图证明）**
	支持自定义语义引擎白名单功能，支持通过规则、URL 参数、IP 地址、Webshell 上传防护、XXE、SQL、PHP 反序列化、PHP 代码注入、命令注入、XSS、后门扫描方式精细化排除。
业务学习	**▲支持业务模型学习监督功能，通过智能分析引擎对业务流量进行分析学习，建立用户业务特征模型，解决因 WEB 应用中因代码不规范和安全检测功能冲突导致的业务误判问题。（需提供产品功能截图证明）**
	支持参数防护，支持主动防护，学习访问 HTTP 的请求参数，总结出参数的路径、变量名、变量类型、长度范围、支持自定义参数防护。
威胁情报	支持设备自动获取云端黑客 IP 进行防护，并能在界面上一键启用和禁用单个云端黑客 IP。
防扫描和	支持 HTTP 应用隐藏，支持过滤如 Server、X-powered-by 类型的 HTTP 响应报文头，支持替换服务器出错页面（5XX）和替换服务器出错页面（4XX）。
数据防泄漏	支持漏洞防扫描，包括 404 页面检测、WAF 规则拦截频率检测、目录访问频率检测、使用不常见的 HTTP 请求方法、匹配强弱规则扫描、敏感文件扫描等扫描行为特征，支持自定义封锁扫描 IP 封锁时间、支持隐藏服务器信息。

	支持数据泄密防护，支持敏感信息自定义命中次数统计方式，支持自定义文件下载类型过滤；支持检测到敏感数据泄露时短信告警，支持自定义数据泄密规则库。
脆弱性识别	**▲支持通过被动扫描功能，业务系统进行黑链检测、Webshell 检测、漏洞风险检测、配置风险检测、弱口令账户检测。（需提供产品功能截图证明）**
权限控制	支持基于地域维度配置访问控制策略，地址库包含中国大陆及海外地区。
	支持用户登录权限防护，支持 Web 登录和非 Web 登录方式防护，支持短信验证登入。
	支持 URL 防护，可自定义允许访问的地址和拒绝访问的地址。
高可用性	支持主备模式的双机部署，支持心跳线冗余，支持配置同步。
策略模板	支持以安全策略模板方式快速部署安全策略，安全策略模板支持默认模板和自定义模板等多种格式。
系统管理	产品支持系统配置自动备份功能，可通过备份文件快速恢复产品系统配置，降低管理员误操作引入的风险。
	安全规则库支持在线自动升级、手动升级、云端实时升级等多种方式。
	▲产品支持与徐汇教育局现有态势感知平台联动，将本地防火墙产品产生的安全日志等数据上报至态势感知平台，并在态势感知平台进行联动封锁、访问控制。（需提供产品功能截图证明）

4、DMZ 区业务负载均衡

技术指标	指标要求
产品交付	需采用独立的专用硬件 AD 应用交付设备，而非通过添加功能模块方式实现
硬件要求	规格：2U 机箱，内存大小≥16G，SSD 硬盘容量≥240GB 电源：冗余电源，接口：千兆电口≥6 个，万兆光口 SFP+≥6 个。
性能要求	4 层吞吐量≥30G，四层并发连接数≥1600 万，4 层新建连接数 CPS≥50 万，7 层新建连接数 RPS≥50 万
设备部署	支持串接部署方式和旁路部署方式，支持三角传输模式。
负载均衡算法	支持轮询、加权轮询、按主机加权轮询、加权最小连接、按主机加权最小连接、动态反馈、最快响应、加权最小流量、按主机加权最小流量、加权源 IP 哈希、带宽比例、哈希、首个可用、优先级等算法。
服务负载均衡	支持源 IP、Cookie（插入/被动/改写）、HTTP-Header、SSL Session ID 等多种会话保持机制，支持跨虚拟服务的会话保持。
	支持 cookie 加密，提升 cookie 安全性。
	▲支持优先级算法下最少可用节点保障，优先级高的节点故障时会自动进行选举，保证优先级高节点的可用性。（需提供产品功能截图证明）
	支持常见的主动式健康检查功能，提供基于 SNMP、ICMP、TCP/UDP、FTP、HTTP、DNS、RADIUS，ORACLE/MSSQL/MYSQL 数据库等多种类型的探测判断机制，支持对 HTTPS 服务进行内容健康检查
	▲支持被动式健康检查，可根据对业务流量的观测采样，辅助判断应用服务器健康状况；对常规 HTTP 应用可配置基于反映 URL 失效的 HTTP 响应状态码的观测判断机制，对于复杂应用可配置基于 RST 关闭连接和零窗口等异常 TCP 传输行为的观测判断机制。（需提供产品功能截图证明）
	支持配置每台的服务器最大连接限制和新建连接限制，以及单个特定用户或者一个

	用户组中所有用户访问指定应用服务的并发连接总数限制，避免应用系统的服务器过载
	节点支持域名和 IP 两种形式，支持自定义 DNS 查询间隔。
	▲对于超过服务器的连接数上限或者请求数上限的新建连接缓存起来放入队列中，后续分批逐步发送给服务器，而不是直接丢弃数据包。（需提供产品功能截图证明）
IPv6 支持	IPv6 支持双栈模式，支持 NAT46、NAT64、NAT66、FTP ALG、DNS64 等协议转换
	▲提供 IPv6 产品由国家权威检测机构出具的检测报告
业务交付优化	七层虚拟服务支持时间戳、TIME_WAIT 资源快速回收、节点失效关闭连接和重置无效连接功能
	支持 HTTP 缓存功能，利用内存 Cache 缓存用户频繁访问的 web 内容，降低后台服务器的负载压力,提升用户访问的响应速度
	支持 TCP 连接复用功能，利用 HTTP 连接池机制，将来自客户端的多个请求合并成一个连接发送到服务器，减少服务器端的工作负荷，并提升业务效率
	▲支持图片优化技术，通过对图片格式的转换，减少传输流量，提升 web 页面加载速度。无需改动服务器端的图片源文件，可根据浏览器种类自动识别转换类型，将图片转换为对应支持的 WebP 或 JPEG 格式，优化加速效果。（需提供产品功能截图证明）
运维管理	支持全中文管理界面和 HTTPS 方式登录、用户角色管理、多级授权管理;（提供设备操作界面截图证明材料）
	▲产品支持与徐汇教育局现有态势感知平台对接，在态势感知平台联动负载均衡设备进行安全事件的联动封锁、访问控制。（需提供产品功能截图证明）
	内置智能告警系统，支持 E-mail、SNMP Trap 两种告警方式，管理员可基于业务安全所关注方面来选择告警触发事件与对应的告警方式，当业务网络环境中发生问题时（如服务器宕机、网络攻击、链路中断等故障场景），即会自动向管理员发送告警信息；
产品与厂商资质	所投产品具备《IPv6 Ready Phase-2 金色认证证书》(提供复印件)
	设备生产商的负载均衡类产品在近三年内入选 Gartner 应用交付控制器（ADC）魔力象限报告，属于国际市场认可的知名品牌
	设备生产商的负载均衡类产品在近三年内市场占有率曾达到前三名（提供如 IDC、Frost&Sullivan 等第三方机构的市场统计报告）

5、DMZ 区潜伏威胁探针

技术指标	指标要求
硬件参数	规格：2U 机箱，内存大小≥8G，SATA 硬盘容量≥1T 电源：冗余电源
	接口：千兆电口≥6 个，万兆光口 SFP+≥2 个。
性能指标	吞吐性能：≥2Gbps。
部署模式	旁路部署，支持探针接入多个镜像口，每个接口相互独立且不影响
兼容性	**▲需兼容徐汇教育信息中心原有的态势感知平台，进行统一接入管理（需同时提供截图证明与官方兼容证明函，加盖厂商公章）**
资产发现	具备主动发送少量探测报文，发现潜在的服务器（影子资产）以及学习服务器的基础信息，如：操作系统、开放的端口号等。

基础检测功能	具备报文检测引擎,可实现 IP 碎片重组、TCP 流重组、应用层协议识别与解析等；具备多种的入侵攻击模式或恶意 UR 监测模式，可完成模式匹配并生成事件，可提取 URL 记录和域名记录。
网站攻击检测	支持 SQL 注入、XSS 攻击、网页木马、网站扫描、WEBSHELL、跨站请求伪造、系统命令注入、文件包含攻击、目录遍历攻击、信息泄露攻击、Web 整站系统漏洞等网站攻击检。
敏感信息检测	支持敏感数据泄密功能检测能力，可自定义敏感信息，支持根据文件类型和敏感关键字进行信息过滤。
漏洞利用攻击检测	**▲支持 Database 漏洞攻击、DNS 漏洞攻击、FTP 漏洞攻击、Mail 漏洞攻击、Network Device、Scan 漏洞攻击、System 漏洞攻击、Telnet 漏洞攻击、Tftp 漏洞攻击、Web 漏洞攻击等服务漏洞攻击检测。（需提供产品功能截图证明）**
	支持 Application 漏洞攻击、File 漏洞攻击、Scan 漏洞攻击、Shellcode 漏洞攻击、System 漏洞利用攻击、Web Activex 等客户端漏洞攻击检测
	支持 FTP、IMAP、MS Sql、Mysql、Oracle、POP3、RDP、SMTP、SSH、Telnet、等协议暴力破解检测
异常流量检测	支持标准端口运行非标准协议，非标准端口运行标准协议的异常流量检测，端口类型包括 3389、53、80/8080、21、69、443、25、110、143、22 等
	支持 ICMP、UDP、SYN、DNS 等协议外发异常流量检测，支持自定义阀值。
僵尸网络行为检测	支持 HTTP 未知站点下载可执行文件、浏览最近 30 天注册域名、浏览恶意动态域名、访问随机算法生成域名、暴力破解攻击、反弹连接、IRC 通信等僵尸网络行为检测。
高级检测	支持 5 种类型日志传输模式,包含标准模式、精简模式、高级模式、局域网模式、自定义模式，适应不同应用场景需求。
	支持传输安全检测日志，包括网络攻击检测日志、漏洞利用攻击检测日志、僵尸网络检测日志、业务弱点发现日志。
	支持传输协议审计日志，包括 https 协议日志、http 协议审计日志、DNS 协议审计日志、邮件协议审计日志、SMB 协议审计日志、AD 域协议审计日志、WEB 登录审计日志、FTP 协议审计日志、Telnet 协议审计日志、ICMP 协议审计日志、LLMNR 协议审计日志
违规访问检测	**▲支持 IP，IP 组，服务，端口，访问时间等定义访问策略，主动建立针对性的业务和应用访问逻辑规则，包括白名单和黑名单方式。（需提供产品功能截图证明）**
沙盒对接	支持将流量还原的文件发送至沙盒分析；可支持第三方沙盒对接。
特征库	**▲内置 URL 库、IPS 漏洞特征识别库、应用识别库、WEB 应用防护识别库、僵尸网络识别库、实时漏洞分析识别库、恶意链接库、白名单库。（需提供产品功能截图证明）**
抓包分析	支持流量抓包分析，可定义抓包数量、接口、IP 地址、端口或自定义过滤表达式。
管理功能	支持设备内置简单命令行管理窗口，便于基础运维调试；
	可实时监控设备的 CPU、内存、存储空间使用情况；
	能够监控监听接口的实时流量情况。
产品资质	要求具备公安颁发的网络入侵检测系统销售许可证
厂商资质	厂商具备软件开发成熟度 CMMI 5 级认证，提供证书复印件；
	厂商应是国家互联网应急响应中心网络安全应急服务国家级支撑单位；
	厂商为国家信息安全漏洞共享平台 CNVD 用户组成员，（提供 CNVD 官网截图证明）；

6、DMZ 区日志审计系统

技术指标	指标要求
硬件参数	规格：2U 机箱，内存大小≥32G，硬盘≥4T，接口：千兆电口≥6 个，万兆光口 SFP+≥2 个。
性能指标	默认包含主机审计许可证书数量≥200，最大可扩展审计主机许可数≥450，可用存储量≥2TB（RAID1 模式），平均每秒处理日志数（eps）最大性能≥2000。
日志采集	支持主动、被动相结合的数据采集方式，支持通过 Agent 采集日志数据，支持通过 syslog、SNMP Trap、JDBC、WMI、webservice、FTP、文件\文件夹读取、Kafka(截图证明)等多种方式完成日志收集
	支持相同 IP 不同设备类型的日志识别
	▲支持通过正则、分隔符、json、xml 的可视方式进行自定义规则解析，支持对解析结果字段的新增、合并、映射。（需提供产品功能截图证明）
	支持对每个日志源设置过滤条件规则，自动过滤无用日志，满足根据实际业务需求减少采集对象发送到核心服务器的安全事件数，减少对网络带宽和数据库存储空间的占用。
日志检索	支持通配符、范围搜索、字段等多种输入方式、搜索框模糊搜索、指定语段进行语法搜索；可根据时间、严重等级等进行组合查询；可根据具体设备、来源/目的所属（可具体到外网、内网资产等）、IP 地址、特征 ID、URL 进行具体条件搜索；支持可设置定时刷新频率，根据刷新时间显示实时接入日志事件；
	支持自定义过滤条件检索，支持对模糊 ip、多个 ip、ip 地址段、应用、协议、MAC 地址等其他字段精准检索，至少支持 AND、OR、NOT 三种运算符；
	▲支持点击事件任意属性字段，可以该字段为条件对事件进行统计分析，排序支持正序和倒序，并可对统计内容进行点击下钻。（需提供产品功能截图证明）
	支持单条事件进行展开，显示事件详细信息和事件原始信息，支持事件详情中任意字段作为查询条件无限制进行二次检索分析。
日志分析	支持网站攻击、漏洞利用、C&C 通信、暴力破解、拒绝服务、主机脆弱性、主机异常、恶意软件、账号异常、权限异常、侦查探测等内置关联分析规则，内置关联分析规则数量达到 350 条以上，支持自定义关联分析规则（需提供截图证明）
	支持预置审计策略模板，包括：Windows 主机类审计策略模板、Linux/Unix 主机类审计策略模板、数据库系统类审计策略模板等，内置审计规则数量不少于 40 条。
	支持内置规则作为模板新建规则，支持调整规则等级，支持通过事件的任意字段制定规则创建策略，支持审计策略命中后可以定义告警并通过相应方式转发，如：邮件、短信等
日志告警	支持告警事件归并、告警确认和告警归档，支持基于频率、频次、时间的设定条件。
	▲日志进行归一化操作后，对日志等级进行映射，根据不同日志源统计不同等级下的日志数量。（需提供产品功能截图证明）
系统管理	提供管理员账号创建、修改、删除，并可针对创建的管理员进行权限设置；支持 IP 免登录，指定 IP 免认证直接进入平台；支持只允许某些 IP 登录平台；支持页

	面权限配置和资产范围配置，用于管理账号权限，满足用户三权分立的需求；支持 usb-key 认证
	▲产品支持与徐汇教育局现有态势感知平台对接，收集第三方安全产品日志数据，进行时间分析与汇总，二次转发上报至态势感知平台，并在态势感知平台进行威胁展示。（需提供产品功能截图证明）
	支持网络连通性测试工具，至少支持 ping、tracert route、telnet 三种拨测方法；
	支持个性化定制，支持全系统更换 logo 与系统名称，支持一键恢复默认。
	▲支持 POC 测试工具一键生成数据。（需提供产品功能截图证明）
	支持自定义前台 web 前端和后端 ssh 的端口，支持页面超时时间和开启 ssh 后台登录。
	支持集群配置及集群状态监控
资质要求	厂商具备云安全成熟度成熟度模型 CSA-CMMI 5 认证，（提供证书复印件）；

7、DMZ 区数据库审计系统

技术指标	指标要求
硬件参数	规格：2U 机箱，内存大小≥16G，SATA 存储硬盘容量≥2T
	电源：冗余电源
	接口：千兆电口≥6 个，万兆光口 SFP+≥2 个。
性能指标	吞吐量≥4Gbps SQL 处理性能≥50000 条 SQL/s
部署方式	支持以交换机镜像方式实现对数据库进行审计分析。
	支持以旁路情况下，在数据库服务器上部署探针的方式对数据库进行审计分析。
部署模式	工作模式：数据库审计产品可以旁路镜像模式部署，不影响数据库性能和网络架构；支持多点联合部署；
	支持集中管理，可集中管理多台审计设备审计事件的存储、分析，实现统一配置、统一报表、统一查询；
部署管理	采用 B/S 管理方式，无需在被审计系统上安装任何代理；无需单独的数据中心，一台设备完成所有工作；提供图形用户界面，以简单、直观的方式完成策略配置、警报查询、攻击响应、集中管理等各种任务；
审计功能	支持主流数据库 Oracle（Tdata）、SQL-Server、DB2、MySQL（Tdsql）、Informix、Sybase、Postgresql、Cache、MongDB、K-DB，虚谷
	支持同时审计多种数据库及跨多种数据库平台操作
	支持 HTTP 请求审计，可指定 GET、POST、URL、响应码进行精细审计；
统计功能	支持以图表方式（饼图、柱图、曲线图、清单列表）显示日志数据分布情况；
	支持以源 IP、业务主机、操作类型、SQL 模版、数据库用户为维度的数据库行为排行；
	支持 SQL 响应性能分析；
	支持执行 SQL 语句失败分析，包括登录失败排行，SQL 语句失败排行；
	▲精细化日志秒级查询

	通过 SQL 串模式抽取保障磁盘 IO 的读写性能；分离式存储 SQL 语句保障数据审计速度快。（需提供产品功能截图证明）
	TB 级日志秒级查询、支持指定源 IP、时间日期、客户端程序、业务系统、数据库用户、操作类型等精细日志查询、支持操作类型精细化日志查询、支持风险级别排行统计查询、支持数据库条件的统计查询、支持统计趋势查询分析、支持风险级别查询分析、支持通过多 SQL 语句的统计查询、支持统计分析下钻、支持业务系统元素统计查询
数据安全	**▲内置大量 SQL 安全规则** **包括如下：导出方式窃取、备份方式窃取、导出可执行程序、备份方式写入恶意代码、系统命令执行、读注册表、写注册表、暴露系统信息、高权存储过程、执行本地代码、常见运维工具使用 grant、业务系统使用 grant、客户端 sp_addrolemember 提权、web 端 sp_addrolemember 提权、查询内置敏感表、篡改内置敏感表等。（需提供产品功能截图证明）**
	可以对 SQL 语句进行安全检测，并识别当前的 SQL 操作是否有暴库、撞库等严重性安全问题，如果命中了安全风险规则，那么可根据动作进行阻断、告警、记录等操作，可提示管理员作出相应的防御措施
	支持基于 SQL 命令的 webshell 检测
	支持 SIP 联动实现数据库的风险进行统一分析预警
系统管理	支持审计系统用户（组）管理（添加、修改、删除、停用、启用）；
	提供管理员权限设置和分权管理，提供三权分立功能，系统可以对使用人员的操作进行审计记录，可以由审计员进行查询，具有自身安全审计功能。
	▲产品支持与徐汇教育局现有态势感知平台联动，同步数据库风险日志、管理员操作日志、正常审计日志，便于统一审计。（需提供产品功能截图证明）
日志数据安全	支持 SNMP 方式，提供系统运行状态给第三方网管系统；
	支持 Syslog 方式向外发送审计日志；
	支持对所有审计管理员操作审计系统的动作进行审计；
	支持日志类型、IP 地址权限设置；
产品资质	国家版权局《计算机软件著作权登记证书》
	中国信息安全认证中心《中国国家信息安全产品认证证书》

8、DMZ 区堡垒机系统

技术指标	指标要求
硬件参数	规格：2U 机箱，内存大小≥8G，存储硬盘 SATA≥2T
	接口：千兆电口≥6 个，万兆光口 SFP+≥2 个。
性能指标	包含运维授权数≥200，最大可扩展资产数≥1000，
	图形运维最大并发数≥200，字符运维最大并发数≥350。
支持协议	字符协议：SSHv1、SSHv2、TELNET
	图形协议：RDP、VNC
	文件传输协议：FTP、SFTP、RDP 磁盘映射、RDP 剪切板

动作流	**▲支持通过动作流配置提供广泛的应用接入支持，无论被接入的资源如何设计登录动作，通过动作流配置都可以实现单点登陆和审计接入。（需提供产品功能截图证明）**
用户管理	支持批量导入、导出用户信息；支持用户手动添加、删除、编辑、设定角色、单独指定登陆认证方式、设定用户有效期
	用户登陆认证方式支持静态口令认证、手机动态口令认证、Usbkey（数字证书）认证、AD 域认证、Radius 认证等认证方式；并支持各种认证方式和静态口令组合认证
运维授权	支持跨部门的交叉授权操作，部门资源管理员可将本部门资源授权给其他部门用户，实现资源临时/长期跨部门访问
	支持按授权名称、用户名称、用户账号、资源名称、资源地址、资源账号查询已授权信息
	▲支持在授权基础上自定义访问审批流程，可设置一级或多级审批人，每级审批可指定通过投票数，需逐级审批通过才可最终发起运维操作。（需提供产品功能截图证明）
访问控制	支持命令黑命单，对字符型设备（如 linux/unix/网络设备）的高危命令执行进行阻断，如 rm、shutdown、reboot 等
	支持命令审批规则，用户执行高危命令时需要管理员审批后才允许执行；命令审批规则可以指定运维人员、访问设备、设备账号及命令审批人（提供截图）
	支持配置资源访问时间规则，即使授权范围内的资源，需在指定时间范围内才可发起访问，确保运维在可信时间范围
审计日志	对字符命令方式的访问可以审计到所有交互内容，可以还原操作过程的命令输入和结果输出，并支持通过搜索操作语句或执行结果中关键字定位审计回放
	图形资源访问时，支持键盘、剪切板、窗口标题、文件传输记录，并且对图形资源的审计回放时，可以从某个键盘、剪切板、窗口标题、文件传输记录的指定位置开始回放
	支持运维审计自查询功能，用户可查看自身的运维审计历史
	支持对 FTP/SFTP 传输的原始文件进行完整记录，并提供下载取证
IPV6	**▲全面支持 IPV6，设备自身可以配置 IPV6 地址供客户端访问，并且支持目标设备配置 IPV6 地址实现单点登陆和审计。（需提供产品功能截图证明）**
虚拟化部署	支持云端快速部署，实现远程运维管理的规范化；可按照运维人员数量，调整云端服务器配置，即可实现性能优化
客户端兼容	全面支持 Windows、linux、国产麒麟系统、Android、IOS、Mac OS 等客户端操作系统下的 H5 页面一站式运维，实现跨终端适应性 BYOD（Bring Your Own Device）
资质	厂商具有中国信息安全测评中心颁发的信息安全服务资质（安全工程类一级）
	厂商具有国家计算机网络应急技术处理协调中心颁发的网络安全应急服务支撑单位证书（国家级）

注：上述“▲”为重要指标，不满足评分时做扣分处理，具体扣分办法详见第六章“评分办法”。

七、售后要求

1、安装和调试

本项目必须在合同签订后**2个月内**全部升级调试完成。供应商负责对施工地点进行现场勘察，保证系统方案既能满足采购技术性能要求，又能确保实施服务顺利进行。安装调试时使用的工具、设备由供应商自行提供。双方应协商制定工程进度表，供应商负责按工程进度表进行施工。设备调试由供应商负责,并提出设备调试的内容、项目、指标和方法,并提供相应的仪器和工具，供应商有责任对买方的技术人员提出的问题进行解答。调试应进行详细记录,系统调试结束后,由供应商技术人员签字后交给买方验收。系统测试的条款应与技术规范一致。基于以上要求，供应商应提供测试条件、方法和过程的草案，最终测试文件由双方共同拟定。

2、设备保修

所有设备需提供至少3年免费原厂质量保修、软件升级服务。

需提供3年免费上门技术支持服务。

3、验收

设备实施完成后，买方将与中标人共同验收。验收时发现问题，买方有权要求中标人立即补发和负责更换。同时中标人应提供必备的技术资料：

设备安装、调试达到技术规范书规定的指标并正常运行5个工作日后，可进行系统验收测试。验收规范(包括项目、指标、方式和测试仪器等)应由中标人提交给买方。买方可根据合同及技术规范书进行修改和补充，经双方确认后形成验收文件作为验收依据。验收测试合格后，双方签署验收协议。

八、其它要求

供应商需提供所投设备原厂商三年售后服务承诺函。

九、付款方式：详见合同条款