附件

金凤实验室云服务网络安全采购项目技术参数

**（一）云防火墙（数量：2台）**

**设备用途：**

用于云主机网络边界防护和流量过滤。

**技术参数：**

1.支持提供对多种路由方式的全面支持，包括静态路由、ISP路由、RIP路由、OSPF路由、IS-IS路由、BGP路由、策略路由。增强系统在不同网络环境下的适应性，提供更灵活的网络配置和管理选项。

2.支持基于源目的IP、用户、端口、应用、国家地区、域名、时间表等多对象/多维度的访问控制策略。

3.支持源地址转换SNAT支持静态、动态、动态端口的NAT转换模式，使得在不同网络配置下能够轻松实现各种源地址的转换，满足多样化的网络需求。

4.支持通过一条NAT规则实现源/目地址的转换，使得用户能够通过简单的配置，灵活地管理源和目标地址的转换，满足不同网络环境下的需求。

5.支持对FTP、TELNET、SMTP、POP3、IMAP5种协议进行弱口令检测，减少潜在的风险。

6.支持对FTP、MSRPC、POP3、SMTP、SUNRPC、Telnet、IMAP、SSH、LDAP、SMB、VNC、RDP暴力破解行为的检测，从而提高了各种协议使用的安全性，有效减轻潜在的风险。

7.支持对网站外链防护功能、CC攻击的检测和防御功能、对跨站脚本攻击的检测和防御功能、对SQL注入攻击的检测和防御功能，可以对WEB服务系统提供保护。

8.支持高频交易访问控制功能，可以对URL访问频率进行限制，进而提高系统的安全性和性能，防范异常请求频率对系统造成的潜在威胁。

9.支持针对HTTP、SMTP、IMAP、POP3、VOIP、NETBIOS等20余种协议和应用的攻击检测和防御。

10.支持在出站方向，系统通过实时监控各链路的时延、抖动、丢包率和带宽利用率，实现智能选路、动态调整各链路的流量负载。用户可以配置灵活的LLB模板，并通过配置LLB规则将LLB模板绑定到路由上，以实现对出站链路流量的控制及负载均衡。

11.支持智能链路入站负载均衡SmartDNS功能，当外部用户访问内部服务器时，联通用户解析到的域名IP为联通地址，电信用户解析到的域名IP为电信地址，使外网访问内部服务器的流量可以在多条链路上实现智能分担。

12.支持Windows、Linux、macOS、IOS、Android5种系统的终端检测，检测内容包括OS版本、安全中心、运行进程、安装服务、运行服务等。

13.支持事件日志、网络日志、配置日志、威胁日志、会话日志、NAT日志、URL日志、策略路由日志、云沙箱日志、文件过滤日志、内容过滤日志、上网行为审计日志等日志的记录与展示。

**（二）WEB应用防火墙（数量：2台）**

**设备用途：**

用于云主机访问过滤和攻击拦截。

**技术参数：**

1.支持添加多级精确域名及泛域名。

2.支持接入添加HTTP协议类型。

3.支持开启HTTPS强制跳转，将客户端的HTTP请求强制转换为HTTPS请求。

4.支持选择HTTPS回源方式，包括HTTP或HTTPS。

5.支持通用证书、国密证书双栈证书解密能力，支持按照通信要求自定义设置加密套件，满足安全性要求。

6.支持设置规则白名单，使具有指定特征的访问请求不经过全部、特性防护类型或某个防护规则的检测。

7.支持基于IP、URL、Referer、User-Agent等请求特征进行多维度组合，定义访问匹配条件过滤访问请求。

8.支持设置对身份证、电话号码、姓名等敏感信息进行屏蔽，从而保证业务敏感信息不在请求日志与事件日志中暴露。

9.支持选择负载均衡算法，包括轮询、IPhash。

10.支持拦截、观察、验证码、JS挑战、放行等执行动作。

11.支持根据BOT会话行为特征设置BOT对抗策略，提供公开类型、协议特征、自定义会话特征等多种判定维度的防护策略。

12.支持展示网站域名收到的全部请求次数、全部攻击次数和触发了不同防护模块的防护次数。

13.支持安全事件分析能力，能够查看事件详情，攻击事件上下文，攻击请求及相应原始报文信息，方便完成攻击事件研判，并能够根据事件对攻击IP或检测规则进行一键加白能力。

**（三）服务器安全卫士（数量：20资产数）**

**设备用途：**

用于云主机防病毒。

**技术参数：**

1.支持Agent与服务端通信采用加密传输，保证数据安全。

2.支持Agent基于系统的负载情况主动降级运行，动态调整CPU、内存占用，确保系统正常运行。

3.支持全方位动态展示全网主机安全态势，通过分析风险趋势、防护状态等数据可帮助用户更好地掌握风险情况，提升安全管理能力。

4.支持通过可视化图形方式展示服务器和资产指纹统计情况，支持基于端口、账号、进程、软件多个维度进行Top排名。

5.支持查看主机操作系统、所属地域、Agent状态等资产信息，支持查看是否存在安全风险，支持模糊检索、快捷筛选，方便用户快速管理服务器。

6.支持查看主机操作系统、所属地域、Agent状态等资产信息，支持查看是否存在安全风险，支持模糊检索、快捷筛选，方便用户快速管理服务器。

7.支持展示用户名、是否设置密码、用户组、到期时间、上次登录时间、上次登录IP。

8.支持检测系统中的弱口令，包括常见弱口令、空口令、系统默认口令、口令中包含用户名等场景。

9.支持暴力破解防护能力，实时监控暴力登录系统的账号和IP，支持对入侵事件进行记录并自动拦截。

10.支持实时监控发现各主机创建的进程是否包含后门文件，支持定期扫描关键路径发现Rootkit、Bootkit和其他后门应用。

11.支持对挖矿木马、蠕虫、勒索病毒等进行有效的检测，提供一键检测和定时检测灵活的检测方式，支持对病毒文件进行隔离、删除和信任。

12.支持实时监控分析进程执行命令参数、匹配反弹 Shell 特征，发现反弹 Shell 行为实时告警。

13.支持检测服务器WEB目录下的文件内容，发现WEB网站中存在的后门文件实时告警。

**（四）日志审计（数量：10资产数）**

**设备用途：**

用于存储云主机日志和审计功能。

**技术参数：**

1.支持B/S架构，管理员只需浏览器即可连接到系统进行各种操作。

2.支持集成数据库，无须再独立安装数据库系统，亦无须对数据库进行专门的维护。

3.支持对网络设备、安全设备和系统、主机操作系统、数据库以及各种应用系统的日志、事件、告警等安全信息进行全面的审计。

4.支持审计中心即可通过 SNMP Trap、Syslog、ODBC\JDBC、Kafka、FTP、SFTP、等多种方式完成日志收集功能。

5.支持用户安装独立的日志采集器通过上述方式采集日志并转发给审计中心。

6.支持用户在被采集节点上安装日志代理采集日志并转发给日志采集器或者审计中心。

7.支持资产管理的功能，能够将被审计资产进行分组、分域的统一维护。

8.支持可视化的总体概览，展示资产事件、风险告警等维度数据统计。

9.支持范式化字段至少应包括事件接收时间、事件产生时间、事件持续时间、用户名称、源地址、源MAC地址、源端口、操作、目的地址、目的MAC地址、目的端口、事件名称、事件摘要、等级、原始等级、原始类型、网络协议、网络应用协议、设备地址、设备名称、设备类型等。

10.支持过滤条件可以按照所有范式化后的字段属性来定义。

11.支持查询时选择特定对象下的某个或多个资源内容，帮助用户管理常用的过滤条件。

12.支持显示一段时间的动态日志移动图，能够在图上显示每个时间切片的日志数量、等级，并能够在图上显示每秒事件数。用户点击每个时间切片，可以查看该切片内的日志。

13.支持以图形化的方式展示日志属性之间的聚合关系，显示多维事件分析图。

14.支持对选中的日志进行事件拓扑分析，并可视化地展示一幅描述日志之间的行为相关关系的事件拓扑图。

15.支持告警内容可以自定义，可以根据日志的实际情况将参数（即预定义变量）传递给命令行脚本。

**（五）云堡垒机（数量：20资产数）**

**设备用途：**

用于云主机登录验证和连接。

**技术参数：**

1.支持从登录时间、登录有效期、多因子认证、登录IP限制、登录MAC限制等维度管控用户认证安全。

2.支持纳管资源类型丰富，包括Windows、Linux等主机资源，Mysql、PostgreSQL、Oracle、db2等数据库资源。

3.支持字符协议（SSH、TELNET）、图形协议（RDP、VNC）、文件传输协议（FTP、SFTP）、数据库协议（DB2、MySQL、Oracle、SQL Server），支持基于以上协议的主流三方客户端。

4.支持设置改密策略，可定时定期修改ssh、telnet协议主机账户密码，确保资源的账户安全。

5.支持通过设置访问控制权限，从访问有效期、登录时间、IP限制、上传/下载、文件传输、剪切板等维度，赋予用户访问资源的权限。

6.支持通过设置命令控制策略或数据库控制策略，对服务器或数据库中敏感、高危操作，强制阻断，加强对关键操作的管控。

7.支持通过配置系统告警，以邮件方式和系统消息方式推送告警通知，以便及时发现系统异常和用户异常操作。

8.支持实时查看正在进行的运维会话，支持监控和中断实时会话。

9.支持对字符、图形运维全程录像记录，回放录像视频。支持生成视频文件，一键下载会话视频。

10.支持ssh、telnet协议的线上多步骤复杂操作自动化执行，告别枯燥的重复工作，提高工作效率。

11.支持通过配置日志备份，可将历史会话日志远程备份至Syslog服务器，实现系统日志容灾备份。

12.支持C/S架构运维接入，包括SSH、RDP、VNC、TELNET、FTP、SFTP、DB2、MySQL、Oracle、postgresql、SCP协议类型主机资源。

13.支持可按用户、用户组、资产、资产组、资产账号维度实现资产对用户进行授权。实现一对一、一对多、多对一、多对多的灵活授权模式。可对资产的服务协议进行精细授权。

14.支持运维操作全程记录，详细记录历史运维会话信息，支持一键导出历史会话日志。

15.支持工单的审批规则可以由系统管理员进行自定义，并且可以设置审批对象和审核人，满足企业流程需求。

16.支持查看已用的存储空间和设置自动删除的内容，包括系统日志、会话日志和录屏文件。

**（六）数据库审计（数量：6资产数）**

**设备用途：**

用于云主机数据库安全审计。

**技术参数：**

1.支持TBase、TDSQL-C（MySQL版及PostgreSQL版）、MAX COMPUTE等协议的审计。

2.支持审计信息能够记录执行时长、影响行数、执行结果描述、返回结果集，提供功能截图，提供功能截图。

3.支持设置日志检索条件时，检索条件可根据历史信息自动弹出，即输入检索条件时支持智能联想。

4.支持历史会话中的审计记录支持直接导出，支持通过“查询分析”按钮跳转至审计日志页面进行进一步的分析筛选。

5.支持告警分析功能，告警分析支持按照“客户端IP+数据库账号”的组合对SQL模板维度进行排行，支持在页面一键添加到白名单、一键添加到信任规则。

6.支持在审计页面直接升级或回退已安装在数据库服务器上的Agent，显示相应的升级/回退进度和结果，且升级或回退不需要输入数据库服务器的账号、密码。

7.支持通过桑基图展示访问数据库的路径，路径包括数据库IP端口、数据库账号、操作类型、数据库/SID、表名等。

8.支持系统资源使用率超阈值（CPU、内存、磁盘）、流量代理异常时触发系统告警，告警支持通过页面展示，支持通过邮件、短信等方式外送。

**（七）漏洞扫描（数量：20资产数）**

**设备用途：**

用于发现云主机漏洞。

**技术参数：**

1.支持最大并发扫描≥60个IP地址，允许最大并发任务≥10个任务，支持无限IP授权扫描。

2.支持多路扫描功能，可以同时对多个隔离业务子网进行扫描。

3.支持对系统漏洞扫描、WEB漏洞、配置合规进行检查和综合分析，可输出同时包含漏洞扫描和配置核查结果的报表。

4.支持断点续扫，可对已完成的扫描任务中没有被覆盖到的目标重新下发扫描任务。

5.支持实时显示扫描结果，包括扫描进度、主机存活数、预计扫描时间、漏洞风险信息等。

6.支持多种报表的默认模板，离线报告支持HTML、WORD、EXCEL、PDF、XML等格式，报告可以直接下载或自动通过邮件直接发送给相应管理人员。

7.支持扫描主流云主机管理系统、云计算组件的安全漏洞，如：VMWareESX/ESXi、KVM、Xen，要求能够扫描大于8000条相关漏洞。