融讯光通
RONG XUN GUANG TONG

网络安全等保建设方案

（能源电力）

北京融讯光通科技有限公司

2023 年 12 月

融讯光通
RONG XUN GUANG TONG

目　录

第 1 章　项目背景

当下，智能化发展、数字化转型已成为油气行业前沿热点，各能源企业竞相发力，发布了自己的数字化转型规划，并陆续大规模实施信息化建设项目。企业通过运用先进的数字化技术，充分整合行业资源，优化组织结构和业务流程，提升企业治理能力和人员素质，可大幅度提高能源勘探开发作业效率和产品服务质量，有效降低综合成本和行业风险。

随着网络技术的不断发展应用，企业在网络安全等保建设方面也存在一些不足或隐患，如：

1. 技术更新滞后：由于企业的信息化建设起步较早，很多系统和设备已经使用了很长时间，技术更新换代的速度相对较慢。这导致了等保系统在应对新型网络攻击和安全威胁时，可能存在一定的技术短板。

2. 人员素质不高：企业的信息安全人才相对匮乏，尤其是具备高级技能和丰富经验的专业人才。这在一定程度上影响了等保系统的建设和维护工作。

3. 安全意识薄弱：部分企业的员工对网络安全和信息安全的重要性认识不足，缺乏足够的安全防范意识。这可能导致等保系统在实际运行中出现漏洞，给企业带来潜在的安全风险。

4. 管理制度不健全：企业在等保系统的管理方面，可能存在制度不健全、执行不到位等问题。这可能导致等保系统的实际运行效果不佳，无法充分发挥其应有的作用。

第 2 章　建设目标

以“主动防御、简易部署、安全合规、动态扩充”为核心，打造专用于能源电力企业解决等保 2.0 建设难点与痛点的快速解决方案，实现统一的安全运营及管理。

通过部署等保一体机，能够帮助企业顺利通过等级保护测评。同时从物理安全、网络安全、主机安全、应用安全、数据安全等多个层面进行体系化等级保护建设,提高安全运维效率。同时,通过等保一体机可以提供的定制化安全增值服务,实现全网动态监测、精确感知、主动防护。

等级保护一体机具备如下特点：

1) 满足合规要求
   - 满足等级保护 2/3 级要求
   - 满足行业规范要求
2) 极简运维模式
   - 多种安全设备统一维护平台
   - 减少现网部署调整工作量
   - 设备部署上线快速/简单
3) 可弹性扩展
   - 按需定义，弹性扩展
   - 业务敏捷，快速上线支持新要求

第 3 章　整体建设

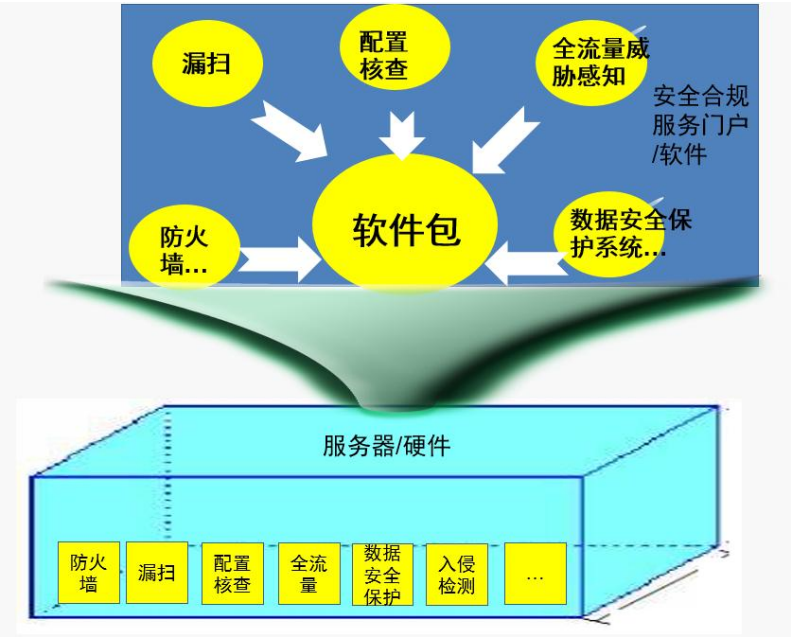
设备提供等保二级、三级套餐防护，综合了审计类、防护类和主机安全类三大块； 业务灵活编排，根据等保需求，可以灵活增加或者减少业务应用软件包，提供个性化安全增值服务； 统一运维平台：多业务应用软件运维平台统一； 支持其它软硬件平台扩展，包括服务器、工控机、云计算资源等。

系统可采用硬件部署和云端部署两种方式。

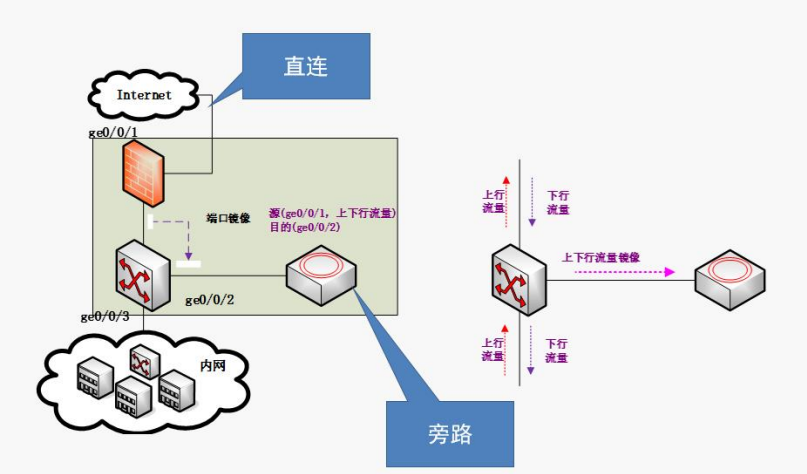
3.1 硬件部署

硬件采用服务器方式部署，适用于小型机房通过等保场景。

等保二级采用一台服务器，等保三级根据冗余需求，采用两台服务器配置。服务器内置多种产品虚拟机。



产品拓扑如下，

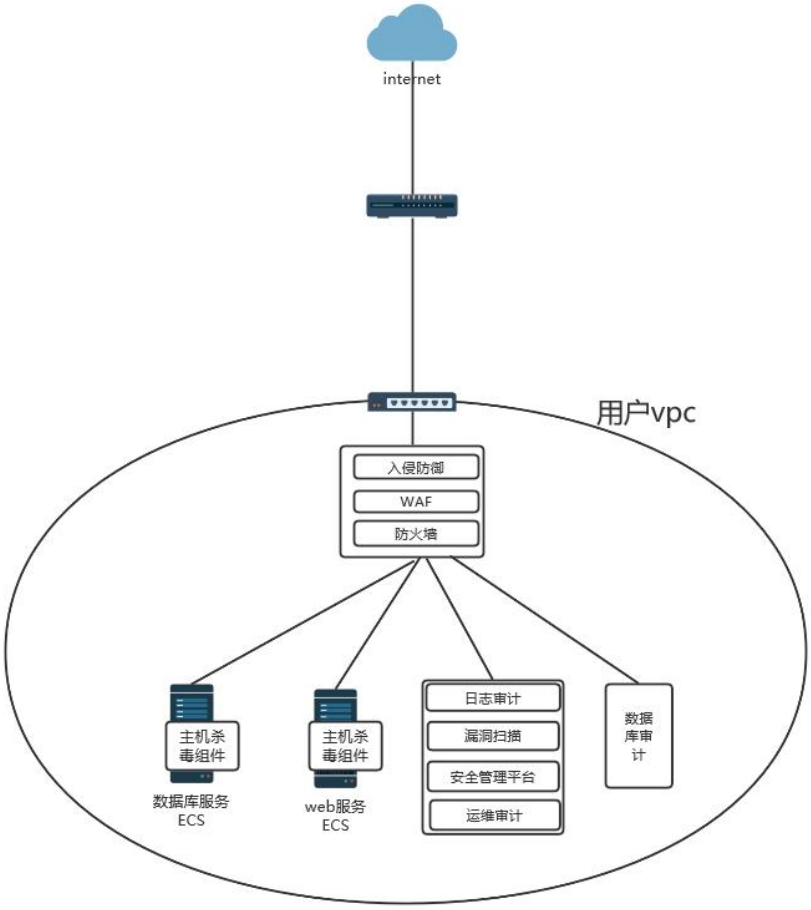


根据拓扑，在用户内外网之间放置等保直通车。在这个组网设计中，用户的业务系统与虚拟防火墙部署在同一虚拟网络内，用户内网服务器与防火墙的网关需要配置指向防火墙。通过虚拟防火墙，内网服务器与互联网网关隔离，访问内网服务器的流量都要进出虚拟防火墙。

3.2 云端部署

云端部署适用于私有云、VPC 和混合云。目前等保直通车分为防火墙、一体机（包含 WAF、运维审计系统、运维监控系统、日志审计系统、安全管理平台）及漏扫；每个系统需要单独开通 1 台虚拟机资源，防火墙采用线上开通虚机后台替换镜像的方式部署，一体机和漏扫采用后台开通虚机，将虚机网络关联到用户 VPC（虚拟私有云）内的方式进行部署；

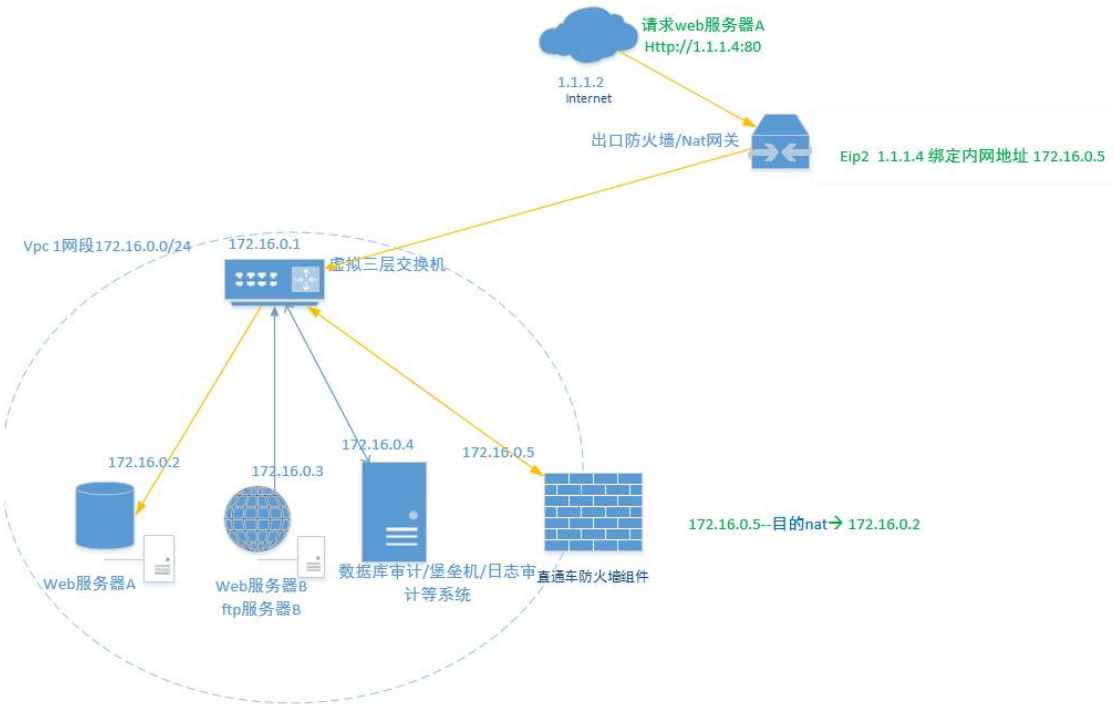
整体 VPC 内部署关系示意图,图中审计部分采用旁路方式接入，非审计部件（防火墙、入侵防御、WAF）采用直连方式。



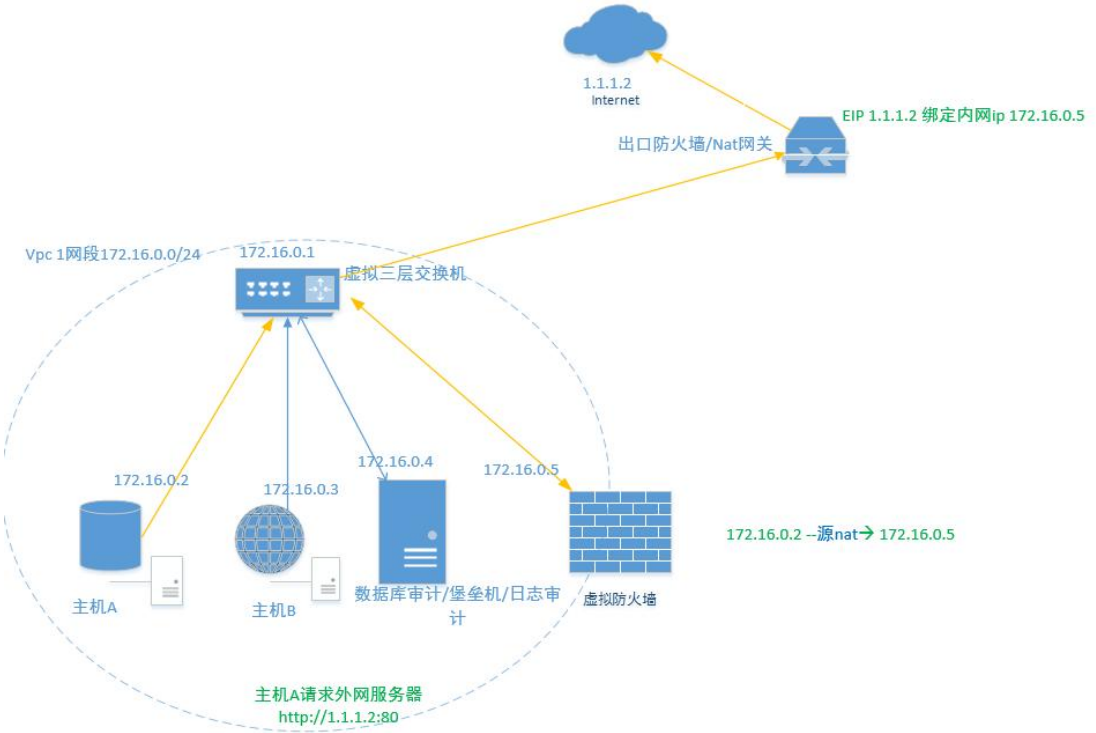
在这个组网设计中，用户的业务系统与虚拟防火墙部署在同一 VPC 内，用户 VPC 内网服务器与防火墙的网关需要配置指向防火墙。通过虚拟防火墙，内网服务器与互联网网关隔离，访问内网服务器的流量都要进出虚拟防火墙。

互联网用户访问防火墙绑定的公网地址时，此时在虚拟防火墙上添加了 DNAT 规则，那么互联网用户就能够访问位于 VPC 内的内网服务器了。并且，在虚拟防火墙上配置了 SNAT 规则，内网服务器也能够访问互联网。

互联网用户访问内网服务器示意图：



内网用户访问互联网示意图：



第 4 章　功能及性能指标

4.1 等保二级功能技术规格

4.1.1　整体部署要求

序号	要求
1	支持有限数量虚机部署整套一体机产品（最多 4 台，可支持等保三级压缩至 2-3 台，等保二级压缩至 1-2 台）；
2	整套产品均为软件形态
3	支持单系统盘部署启动，允许数据盘挂载
4	支持 qcow2 部署包
5	支持单网卡部署
6	审计与流量监测平台支持探针模式部署
7	支持高速硬盘与高速网卡
8	cpu 支持兼容模式

4.1.2　等保安全管理产品技术要求

序号	指标项	规格要求
1	资产管理方式	支持按照安全域归类
		支持按照业务属性归类
		支持按照设备类型归类
		支持按照所属网段归类
2	可管理的资产类型	支持资产属性查看包含：
		资产基本信息
		资产配置信息，比如操作系统、接口数量等
		支持多种资产维护方式，资产人工维护和资产自动发现
		支持主机设备管理支持 windows、linux 等主流系统
		支持物理、虚拟主机
		支持网络设备管理
3	事件收集方	支持多种收集方式：

序号	指标项	规格要求
	式	SYSLOG、SNMP TRAP 、SNMP 轮询、TELNET/SSH、专用代理程序等方式从网络设备、安全设备、主机系统、应用程序按照一定策略收集原始日志数据
4	事件关联分析	支持多种关联分析方式，如交叉关联分析法和基于规则关联分析法
5	脆弱性信息收集	支持第三方结果导入分析，支持部分开源漏洞扫描软件的漏洞结果导入
		支持主动漏洞扫描
		支持扫描计划定制，支持根据绝对时间、周期、扫描内容、扫描对象等条件指定扫描计划
6	扫描策略	支持扫描周期、扫描内容等
		扫描动作
7	风险预警	风险分析需充分考虑资产价值、威胁发生的概率、脆弱性被威胁利用的概率这三个元素，因此根据这三个元素预先设定一个三维风险价值矩阵，然后逐一确定目标信息资产的价值、威胁发生的概率、脆弱性被威胁利用的概率，从而科学地从风险的预先价值矩阵中计算出对应的风险量化值。
8	安全策略配置	安全策略分级，支持公共策略、私有策略
		账号认证设置，支持安全产品的自动认证
		访问策略配置
		响应策略配置
		备份恢复策略
		升级策略
		公共策略集中制定，支持公共安全策略集中分发，备份，恢复，升级等

4.1.3 集中审计产品技术要求

序号	指标项	集中审计产品技术要求
1	功能要求	系统从不同设备或系统中所获得的各类日志、事件中抽取相关片段准确和完整地映射至安全事件的标准字段

序号	指标项	集中审计产品技术要求
		对安全事件重新定级。能根据统一的安全策略，按照安全设备识别名、事件类别、事件级别等所有可能的条件及各种条件的组合对事件严重级别进行重定义
		系统既可以完全收集采集对象上的日志信息，也支持在安全事件收集引擎上设置过滤条件，可过滤出无关安全事件，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，从而减少对网络带宽和数据库存储空间地占用。

4.1.4 运维审计产品技术要求

序号	指标项	指标描述
1	设备类型	Windows 类主机、域控主机、域控内主机、Unix 类主机、Linux 类主机、各种网络设备、安全设备、网元、数据库、Web 应用等
2	身份认证及管理	运维审计系统身份认证方式：本地认证、RADIUS 认证、LDAP 认证、AD 域认证
		支持三权分立，内置管理员角色，支持自定义角色权限
		支持创建临时用户
		支持访问限制，即同一时间只接受一个 IP 访问
		支持用户自动/手动锁定、激活
3	用户及组管理	支持运维用户的全生命周期管理，包括添加、修改、删除、停用/启动、更新时间；
		支持对用户进行分组，分层次管理，分组以树形方式展现
		支持用户列表信息按字段自动排序
		支持 Excel 表用户批量导入/导出
		支持对用户按科室、部门等进行独立管理、独立授权
4	主机及组管理	支持主机管理，包括主机 IP、名称、类型、访问协议、端口、帐号及密码等信息；资产信息字段可自定义扩展
		支持对主机设备进行分组，分层次管理，分组以树形方式展现
		支持主机列表信息按字段自动排序
		支持对主机设备按科室、部门等进行独立管理、独立授权
		支持智能运维脚本：支持运维审计系统定时自动执行包含运维指令的脚本，支持执行结果输出

序号	指标项	指标描述
5	操作审计	支持对字符协议、图形协议、数据库操作进行操作审计
		支持记录 RDP 会话中的键盘输入信息
		支持记录 RDP 会话剪贴板（复制粘贴）内容
		支持 sftp/ftp 文件传输协议审计
		支持记录 WEB 资源完整访问 URL 地址
		支持记录通过客户端直连访问字符协议的操作审计
		支持高级检索功能，查询条件可任意组合
		支持字符协议的指令检索，支持图形协议的键盘输入检索，并可展现本次会话的所有操作
		支持被检索命令的高亮显示

4.1.5 网站应用防护产品技术要求

序号	指标项	规格要求
1	访问控制	可基于物理接口、源 IP 地址、目的 IP 地址、IP 协议、时间、用户、指定 URL 等定义访问控制策略，需提供界面截图证明
		支持任意数据包碎片进行分片重组，且可自由选择关闭或启动
		支持基于时间计划的黑、白名单，对特定 URL 级别进行访问控制
		能基于多种 HTTP 方法执行访问控制，包括：GET、POST、UNKNOWN、HEAD、PUT、DELETE、MKCOL、COPY、MOVE、OPTIONS、PROPFIND、PROPPATCH、LOCK、UNLOCK TRACE、SEARCH、CONNECT，提供配置界面截图
2	防护机制	支持对 HTTP 和 HTTPS 的协议合法性进行验证和攻击防护
		多引擎检测模式，可监控双向流量，对双向数据实时监测和保护
		智能阻断，基于智能用户行为识别的动态防护机制，识别并彻底阻断黑客的攻击行为
		完善的内置 Web 应用防护事件库，在线和离线升级更新，支持用户自定义防护特征
		支持紧急模式，当并发连接数超过阀值时，WAF 自动进入紧急模式，已经代理的连接正常代理，对新增的请求不进行代理，直接转发，防止 WAF 成为访问瓶颈。当连接数恢复正常时，自动退出紧急模式

序号	指标项	规格要求
3	Web 安全防御	识别非法上传/下载行为，阻断敏感信息泄露、恶意代码攻击、错误配置攻击、隐藏字段攻击、会话劫持攻击、参数篡改攻击、弱口令攻击、Webshell 行为拦截（需要提供截图）
		支持 HTTPS 卸载和加壳，客户端到服务器端可以任意选择 HTTPS 和 HTTP，强化应用层安全
		支持 SQL 注入、XSS 防护，支持使 HTTP 头域中的 Cookie、Referer、User-Agent，Except 字段过防护策略，提供配置界面截图盖章证明
		可以防御盗链攻击、爬虫入侵，网络中的恶意扫描行为
		可以进行 HTTP 报文请求的字段类型进行严格，中等和宽松的限制
		支持 Cookie 安全机制，包括加密和签名的防护方法，支持 Cookie 自学习，提供配置界面截图盖章证明
		支持 CSRF（跨站请求伪造）防护，提供配置界面截图盖章证明
		支持 Web 站点隐藏和伪装的安全策略，包括操作系统类型、web 服务器类型、HTTP 响应报文头和 HTTP 出错页面和过滤，可自定义具体方法(要求提供产品界面截图，加盖厂商公章)
4	抗 DDoS 攻击	抗应用型攻击，包括 TCP Flood、Web cc、http get/post flood、xml 攻击、特定 url 攻击等，并说明其防御原理
		连接耗尽型防护，支持源客户端、指定 URL 目录、web 服务器的连接数防护
		支持 DDoS 机器人自学习功能，学习时间可设置，生成动态的业务场景防护策略
		允许与抗 DDoS 产品联动，从而抗 DDoS 设备和 web 防火墙之间能够同步攻击特征库、同步攻击防护算法
5	WEB 应用漏洞扫描	能够对 SQL 注入、CGI、跨站脚本（XSS）进行应用层漏洞扫描，并生成可视化分析图表
6	Cache 加速	应具备系统内嵌应用加速模块，通过对各类静态页面及部分脚本高速缓存，大大提高访问速度
7	操作安全审计	对与系统自身安全相关的下列事件产生审计记录：管理员登陆后进行的操作行为；对安全策略进行添加、修改、删除等操作行为；对管理角色进行增加、删除和属性修改等操作行为；对其他安全功能配置参数的设置或更新等行为

4.1.6 租户边界防护产品技术要求

序号	指标项	租户边界防护产品技术要求
1	安全防护	支持 4 种安全防护模式，基于网络、用户、应用
		支持内嵌深度包检测引擎，针对数据包进行深度过滤检测
		支持对穿透防火墙的 FTP 服务进行过滤审计
		支持通过预定义过滤文件名实现对 FTP 数据流的区分控制
		支持对 vpn 隧道内的内容检查和防护
2	统一特征库	web 页面下统一对设备支持的特征库进行查看、更新及自定义操作
		支持针对 webmail、应用特征库可以根据客户需求实现定制
3	IPv6 支持	支持基于 IPv6 下的路由，包括：直连路由、静态路由、动态路由（OSPF、BGP 等）等
		支持基于 IPv6 下的 IP 地址/地址组的包过滤、内容过滤、IPS 检测、流量控制以及关联时间控制等
4	VPN	支持 PPTP、GRE、IPSEC 等 VPN
		支持隧道热备份、负载均衡、单臂多线路、星形、网状、树状等多种组网方式
5	安全审计	支持将日志存储在本地，标配 1T 日志存储硬盘，完美满足公安部 82 号令,至少保留用户行为日志 60 天的要求
		支持全部日志按天和统一格式（如：ozlog-20141013.log）存储，可以通过 web 页面查看、删除、导出历史日志列表（提供截图说明）
		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

4.1.7 租户入侵防范产品技术要求

序号	指标项	规格要求
1	IPv6 支持	支持基于 IPv6 下的路由，包括：直连路由、静态路由、动态路由（OSPF、BGP 等）等
		支持基于 IPv6 下的 IP 地址/地址组的包过滤、内容过滤、IPS 检测、流量控制以及关联时间控制等
		支持基于 IPv6 下的 IP/MAC 绑定
		支持基于 IPv6 下的流量牵引
2	入侵防护	采用多检测引擎互为备份的检测机制，需说明实现原理

序号	指标项	规格要求
		支持基于 IP 碎片重组、TCP 流重组、会话状态跟踪、应用层协议解码等数据流处理方式的攻击识别；
		支持模式匹配、异常检测、统计分析，以及抗 IDS/IPS 逃逸等多种检测技术
		可依据端口识别协议类型，可分析 HTTP、SMTP、POP3、FTP、Telnet、VLAN、MPLS、ARP、GRE 等多种协议
		内置攻击特征库，特征数量超过 3,500 条，支持在线、离线升级方式，并可自定义攻击特征，阻挡蠕虫、木马、间谍软件、广告软件、缓冲区溢出、扫描、非法连接、SQL 注入、XSS 跨站脚本等多种攻击
		可对英文、UTF8/GB18030/BIG5 中文编码，GZIP/inflate/trunked 压缩算法的的网页内容进行深度特征码检测的舆情监控和报警
		可对告警事件设置丢弃数据包、阻断会话、页面推送、日志/邮件报警、声音、状态灯报警等
3	抗 DDoS 攻击	抗应用型攻击，包括 Web cc、http get flood、DNS query/reply 泛洪攻击或速率限制、DNS 协议自身安全性、DNS 缓存投毒、域名劫持、容灾恢复等，并说明其防御原理
		抗流量型攻击，包括 syn flood、udp flood、icmp flood、arp flood、frag flood、stream flood 等攻击
		抗蠕虫连接型攻击，可基于 ACL 或者源或目地 IP 地址进行连接数统计和控制，支持连接排行榜，可早期预警
		抗普通常见攻击，包括 ipspoof、sroute、land、fraggle 攻击、sf_scan、null_scan、xmas_scan、smurf 等攻击
		支持基于事件类别，重要等级，发生时间，五元组等进行攻击取证，并说明实现方式
		允许与 WAF/抗 DDoS 产品联动，从而实现 IPS 与抗 DDoS 设备、WAF 防火墙之间能够同步攻击特征库、同步攻击防护算法

4.1.8 高危漏洞风险产品技术要求

序号	指标项	指标要求
1	网络适应性	支持 IPv4/v6 双协议栈网络地址解析；支持针对 IPv4/v6 网络中的扫描。

序号	指标项	指标要求
		支持远程管理，自定义可访问设备的网段或 IP；
2	系统漏洞扫描能力要求	产品扫描信息应包括主机信息、用户信息、服务信息、漏洞信息等内容。有效漏洞库至少支持 50000 条以上；
		产品漏洞库应涵盖目前的安全漏洞和攻击特征，漏洞库具备至少 CVE、CNCVE、CNVD、BUGTRAQ、CNNVD 编号；
		支持数据库登录扫描，至少应包括数据库账号，密码，SYSDBA、SYSOPER、NORMAL 认证，SID、数据库名称、实例名称及实例号等登录选项的设置；提供弱口令扫描功能；
3	Web 漏洞扫描要求	漏洞插件库支持按照国际权威安全组织 OWASP TOP 10-2013；
		支持登录认证，至少支持 Cookie 认证、Form 认证、Basic 认证、NTLM 认证、Digest 认证；并支持在线验证是否登录成功，确保授权准确有效
4	报表能力	支持同一任务的两次扫描结果对比，清晰明了的展示出漏洞状态的变更情况；
		在线报表支持手动调整误报、已修复等漏洞类型，导出报表时可选择是否将误报、已修复等漏洞导出
		支持多维度查看分析设备漏洞并导出报告，支持根据节点名称、设备名称、设备 IP、设备管理员、设备操作系统、风险等级、漏洞名称、端口号、检测时间段等查看设备漏洞情况，并保存导出；

4.1.9 网络版杀毒软件

序号	指标项	指标要求
1	网络支持	单向/双向流量，可对单向或双向流量进行监测，
2	疑似文件样本捕获	捕获疑似木马文件，将其完整还原并保存疑似样本。一个疑似样本只保存一次，不重复保存。
3	支持多种文档格式解析	文件格式（包括但不限于 exe、ZIP,RAR,TAR,GZIP,BZIP2,ELF,IPA、mpkg、cab、deb 等格式深度解析），文件可执行性、文件大小（去超大、去超小）、文件日期、白名单等。

序号	指标项	指标要求
4	基于特征的攻击检测	具备通过特征匹配的方式对攻击进行检测的能力,需要有单独的木马文件传播特征库以及僵尸主机特征库。
5	僵尸、木马检测	支持对传统僵尸、木马的检测。
6	攻击样本提取	可以提取出攻击的完整样本文件，并提供对该文件下载的能力

4.2 等保三级功能技术规格

4.2.1 整体部署要求

序号	要求
1	支持有限数量虚机部署整套一体机产品（最多 4 台，可支持等保三级压缩至 2-3 台，等保二级压缩至 1-2 台）；
2	整套产品均为软件形态
3	支持单系统盘部署启动，允许数据盘挂载
4	支持 qcow2 部署包
5	支持单网卡部署
6	审计与流量监测平台支持探针模式部署
7	支持高速硬盘与高速网卡
8	cpu 支持兼容模式

4.2.2 等保安全管理产品技术要求

序号	指标项	规格要求
1	资产管理方式	支持按照安全域归类
		支持按照业务属性归类
		支持按照设备类型归类
		支持按照所属网段归类
2	可管理的资产类型	支持资产属性查看包含：
		资产基本信息
		资产配置信息，比如操作系统、接口数量等
		支持多种资产维护方式，资产人工维护和资产自动发现
		支持主机设备管理支持 windows、linux 等主流系统
		支持物理、虚拟主机
		支持网络设备管理
3	事件收集方式	支持多种收集方式：
		SYSLOG、SNMP TRAP 、SNMP 轮询、TELNET/SSH、专用代理程序等方式从网络设备、安全设备、主机系统、应用程序按照一定策略收集原始日志数据

序号	指标项	规格要求
4	事件关联分析	支持多种关联分析方式，如交叉关联分析法和基于规则关联分析法
5	脆弱性信息收集	支持第三方结果导入分析，支持部分开源漏洞扫描软件的漏洞结果导入
		支持主动漏洞扫描
		支持扫描计划定制，支持根据绝对时间、周期、扫描内容、扫描对象等条件指定扫描计划
6	扫描策略	支持扫描周期、扫描内容等
		扫描动作
7	风险预警	风险分析需充分考虑资产价值、威胁发生的概率、脆弱性被威胁利用的概率这三个元素，因此根据这三个元素预先设定一个三维风险价值矩阵，然后逐一确定目标信息资产的价值、威胁发生的概率、脆弱性被威胁利用的概率，从而科学地从风险的预先价值矩阵中计算出对应的风险量化值。
8	安全策略配置	安全策略分级，支持公共策略、私有策略
		账号认证设置，支持安全产品的自动认证
		访问策略配置
		响应策略配置
		备份恢复策略
		升级策略
		公共策略集中制定，支持公共安全策略集中分发，备份，恢复，升级等

4.2.3 集中审计产品技术要求

序号	集中审计产品技术要求	
1	功能要求	系统从不同设备或系统中所获得的各类日志、事件中抽取相关片段准确和完整地映射至安全事件的标准字段
		对安全事件重新定级。能根据统一的安全策略，按照安全设备识别名、事件类别、事件级别等所有可能的条件及各种条件的组合对事件严重级别进行重定义（提供界面截图证明并加盖厂商公章）

		系统既可以完全收集采集对象上的日志信息，也支持在安全事件收集引擎上设置过滤条件，可过滤出无关安全事件，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，从而减少对网络带宽和数据库存储空间地占用。

4.2.4 安全审计产品技术要求

序号	指标项	指标要求
1	动态审计	支持绑定变量（Bind Variable）的审计
		可根据需要定义审计白名单
2	实时监控与风险控制告警	针对于数据库的操作行为进行实时检测，根据预设置的风险控制策略，结合对数据库活动的实时监控信息，进行特征检测，任何尝试的攻击操作都会被检测到并进行阻断或告警。
3	双向审计	不仅支持对数据请求的报文进行审计，同时应对请求的返回结果进行审计，如操作回应、作用数量、执行时长等内容，并能够根据返回的回应进行审计策略定制。
4	多层业务审计	提供全方位的多层（应用层、中间层、数据库层）的访问审计，通过多层业务审计可实现数据操作原始访问者的精确定位
5	审计层次及规则策略	提供针对用户（数据库）、表、字段、操作的审计规则；
		精细到表、字段、具体报文内容的细粒度审计规则，实现对敏感信息的精细监控；
		基于 IP 地址、MAC 地址和端口号审计；
		提供可定义作用数量动作门限，如 SQL 操作返回的记录数或受影响的行数大于等于此值时触发策略设定；
		提供可设定关联表数目动作门限，如 SQL 操作涉及表的个数大于等于此值时触发策略设定；
		可根据 SQL 执行的时间长短设定规则； 如命令执行时长超过 30 秒进行告警；
		可根据 SQL 执行的结果设定规则；
		可设置登录规则 任何违规的登录行为都会被告警
6	白名单	支持 ip 白名单功能
		可以从风险告警直接获取白名单条件，一键添加白名单；
7	分级管理	支持多级部署环境下数据查询；

序号	指标项	指标要求
		支持多级管理下审计规则分发；
8	报表管理	提供所有或单个数据库登录用户、源 IP、目的 IP 的审计规则统计、特征告警、对象访问、请求统计等报表功能，并提供用户自定义报表功能；
		能够自动导出 WORD、PowerPoint、PDF 等各种格式文件；
		支持点线图、柱状图、饼图等图文并茂式报表展现；
		支持访问数据的趋势分析；
		可以根据单个库、数据库组生成报表，包括支持严格按照塞班斯（SOX）法案、等级保护标准要求生成多维度综合报告；
		支持按照时间曲线统计流量、在线用户数、并发会话、DDL 操作数、DML 操作数、执行量最多的 SQL 语句等报表；
9	事件回放与追溯	根据事件发生的时间、用户、访问方式、用户 IP、服务器等组合查询，并对过程进行回放和追溯。
10	审计数据库类型	支持 Oracle8/9/10、MS SQL Server2000/2005/2008、Sybase11/12、MYSQL V4/v5 等主流数据库；
11	部署方式	支持端口镜像
		支持分布式部署、集中式管理模式；

4.2.5 运维审计产品技术要求

序号	指标项	指标描述
1	设备类型	Windows 类主机、域控主机、域控内主机、Unix 类主机、Linux 类主机、各种网络设备、安全设备、网元、数据库、Web 应用等
2	身份认证及管理	运维审计系统身份认证方式：本地认证、RADIUS 认证、LDAP 认证、AD 域认证
		支持三权分立，内置管理员角色，支持自定义角色权限
		支持创建临时用户
		支持访问限制，即同一时间只接受一个 IP 访问
		支持用户自动/手动锁定、激活
3	用户及组管理	支持运维用户的全生命周期管理，包括添加、修改、删除、停用/启动、更新时间；
		支持对用户进行分组，分层次管理，分组以树形方式展现

序号	指标项	指标描述
		支持用户列表信息按字段自动排序
		支持 Excel 表用户批量导入/导出
		支持对用户按科室、部门等进行独立管理、独立授权
4	主机及组管理	支持主机管理，包括主机 IP、名称、类型、访问协议、端口、帐号及密码等信息；资产信息字段可自定义扩展
		支持对主机设备进行分组，分层次管理，分组以树形方式展现
		支持主机列表信息按字段自动排序
		支持对主机设备按科室、部门等进行独立管理、独立授权
		支持智能运维脚本：支持运维审计系统定时自动执行包含运维指令的脚本，支持执行结果输出
5	操作审计	支持对字符协议、图形协议、数据库操作进行操作审计
		支持记录 RDP 会话中的键盘输入信息
		支持记录 RDP 会话剪贴板（复制粘贴）内容
		支持 sftp/ftp 文件传输协议审计
		支持记录 WEB 资源完整访问 URL 地址
		支持记录通过客户端直连访问字符协议的操作审计
		支持高级检索功能，查询条件可任意组合
		支持字符协议的指令检索，支持图形协议的键盘输入检索，并可展现本次会话的所有操作
		支持被检索命令的高亮显示

4.2.6 网站应用防护产品技术要求

序号	指标项	规格要求
1	访问控制	可基于物理接口、源 IP 地址、目的 IP 地址、IP 协议、时间、用户、指定 URL 等定义访问控制策略，需提供界面截图证明
		支持任意数据包碎片进行分片重组，且可自由选择关闭或启动
		支持基于时间计划的黑、白名单，对特定 URL 级别进行访问控制
		能基于多种 HTTP 方法执行访问控制，包括：GET、POST、UNKNOWN、HEAD、PUT、DELETE、MKCOL、COPY、MOVE、OPTIONS、PROPFIND、PROPPATCH、LOCK、UNLOCK TRACE、SEARCH、CONNECT，提供配置界面截图

序号	指标项	规格要求
2	防护机制	支持对 HTTP 和 HTTPS 的协议合法性进行验证和攻击防护
		多引擎检测模式，可监控双向流量，对双向数据实时监测和保护
		智能阻断，基于智能用户行为识别的动态防护机制，识别并彻底阻断黑客的攻击行为
		完善的内置 Web 应用防护事件库，在线和离线升级更新，支持用户自定义防护特征
		支持紧急模式，当并发连接数超过阀值时，WAF 自动进入紧急模式，已经代理的连接正常代理，对新增的请求不进行代理，直接转发，防止 WAF 成为访问瓶颈。当连接数恢复正常时，自动退出紧急模式
3	Web 安全防御	识别非法上传/下载行为，阻断敏感信息泄露、恶意代码攻击、错误配置攻击、隐藏字段攻击、会话劫持攻击、参数篡改攻击、弱口令攻击、Webshell 行为拦截（需要提供截图）
		支持 HTTPS 卸载和加壳，客户端到服务器端可以任意选择 HTTPS 和 HTTP，强化应用层安全
		支持 SQL 注入、XSS 防护，支持使 HTTP 头域中的 Cookie、Referer、User-Agent，Except 字段过防护策略，提供配置界面截图盖章证明
		可以防御盗链攻击、爬虫入侵，网络中的恶意扫描行为
		可以进行 HTTP 报文请求的字段类型进行严格，中等和宽松的限制
		支持 Cookie 安全机制，包括加密和签名的防护方法，支持 Cookie 自学习，提供配置界面截图盖章证明
		支持 CSRF（跨站请求伪造）防护，提供配置界面截图盖章证明
		支持 Web 站点隐藏和伪装的安全策略，包括操作系统类型、web 服务器类型、HTTP 响应报文头和 HTTP 出错页面和过滤，可自定义具体方法(要求提供产品界面截图，加盖厂商公章)
4	抗 DDoS 攻击	抗应用型攻击，包括 TCP Flood、Web cc、http get/post flood、xml 攻击、特定 url 攻击等，并说明其防御原理
		连接耗尽型防护，支持源客户端、指定 URL 目录、web 服务器的连接数防护
		支持 DDoS 机器人自学习功能，学习时间可设置，生成动态的业务场景防护策略
		允许与抗 DDoS 产品联动，从而抗 DDoS 设备和 web 防火墙之间能够同步攻击特征库、同步攻击防护算法

序号	指标项	规格要求
5	WEB 应用漏洞扫描	能够对 SQL 注入、CGI、跨站脚本（XSS）进行应用层漏洞扫描，并生成可视化分析图表
6	Cache 加速	应具备系统内嵌应用加速模块，通过对各类静态页面及部分脚本高速缓存，大大提高访问速度
7	操作安全审计	对与系统自身安全相关的下列事件产生审计记录：管理员登陆后进行的操作行为；对安全策略进行添加、修改、删除等操作行为；对管理角色进行增加、删除和属性修改等操作行为；对其他安全功能配置参数的设置或更新等行为

4.2.7 运维监控产品技术要求

序号	指标项	指标要求
1	资源管理要求	支持多种数据采集方式，支持有线/无线网络设备、安全设备、服务器、数据库、中间件、虚拟化设备、存储设备、机房系统、应用系统等多厂商、多种类的资源监控；
		支持提供开放的接口，用户可以自行编制监控脚本，完成相应资源的监控。
2	报表统计要求	支持系统内置多纬度多视角报表模版，包括：资源类报表模版、分析类报表模版、趋势类报表模版、TOPN 报表模版、故障类报表模版等；
3	网络设备管理要求	支持对思科、华为、锐捷、HC、中兴、迈普、迪普等厂家的网络设备进行发现监控，监控内容包括但不限于设备性能、吞吐量，端口流量、端口丢包率、广播包速率，链路通断等。
		支持网络资源详情信息应全部显示出监控接口信息、性能信息、VLAN 表、ARP 表、路由表等；且可直接打开对应设备告警信息、拓扑图定位、面板图、日志信息等。并支持用户拖拽自定义显示页面。
4	主机管理要求	统支持通过 SNMP/SSH/Telnet 等方式可以实现对 Windows、IBM AIX、Linux、FreeBSD、Solaris 等各种操作系统主机的自动监控。采用集中非代理式监测，无需在被监控对象上安装任何代理软件，对原有系统不产生任何影响。
		支持对服务器的 CPU、内存、进程、磁盘、网卡等进行监控。

序号	指标项	指标要求
		支持主机资源应构成主机资源库，其能与网络资源统一管理。
		支持对主机所有监控指标的指标注释，包含指标含义，异常分析，处理建议等。
5	虚拟化管理	支持通过虚拟架构如以 vCenter、数据中心、Cluster、ESXi 主机/宿主机、VM 组、VM 和数据存储组、数据存储的树形关系层级呈现虚拟资源；通过资源类型等多种维度进行虚拟化资源的查看和分析。
6	存储设备管理要求	支持系统通过 SNMP、SMI-S 等多种方式支持对主流存储设备的监控和管理，包括但不限于 EMC、HP、IBM、NetApp、浪潮、华为、宏杉、DELL 等品牌。
		支持监控 HBA 主机、FC、存储设备以及光纤通道状态等。
		支持对存储性能进行统计分析，展示池、数据存储卷、FC 交换机等用户关心的性能指标。
7	应用管理	支持系统监控 Oracle、DB、MySQL、SQL Server、Sybase、demino 等数据库，采用集中非代理式监测，无需在被监控对象上安装任何代理软件，对原有系统不产生任何影响。
		支持对各数据库的分区、进程、表空间、数据文件、日志文件、命中率等指标信息进行采集，用户可对各指标进行告警阈值的设置。
		系统支持应用服务器监控。包含但不限于以下：IIS、Websphere、weblogic、Tomcat 等。

4.2.8 流量分析产品技术要求

序号	指标项	指标要求
1	IM（即时通讯）软件识别	支持 QQ、ICQ、MSN Messenger、Yahoo Messenger 及 AOL Messenger 等协议
2	VoIP 协议识别	支持 Skype、UUCALL、Konge(中桥语音) 、SIP、MGCP 及 H323 等协议
		提供 PC-PC、PC-Phone 模式的呼叫识别、干扰、阻断
3	数据库识别	支持 MS SQL-Server、MySQL 及 Oracle 等
4	企业桌面应用识别	支持 Notes、IMAP、POP、SMTP、FTP、Telnet 及 Syslog 等
5	炒股软件识别	支持 Big Wisdom(大智慧)及 Straight Flush(同花顺)等

序号	指标项	指标要求
6	网络游戏识别	支持 World of Warcraft 及 Globallink 等
7	其他应用业务识别	流媒体、WEB 访问、FTP 下载、网络管理
8	一拖 N 代理软件识别	支持 WinGate、WinProxy、WinRoute、TP-Link 等（包括 NAT 方式及 Proxy 方式）
9	协议分析技术	*采用特征库技术，升级过程无需重启、不中断业务正常运行
		*特征库支持手动升级与自动升级
		提供开放端口，可手工定义协议类型
		支持与第三方配合，共同开发特征库
		可导入用户自行开发的特征库
		*可识别> =900 种应用协议
		可以识别并检测 802.1Q、MPLS、QinQ、GRE 等特殊封装的网络报文。
		国内专业分析团队，提供 24 小时不间断响应，并及时更新特征库
10	应用控制策略	支持阻断功能
		支持限流功能
		支持干扰功能
		支持告警功能
		支持输出报表功能
		支持基于用户、区域、源/目的 IP、IP 组、时间、应用等综合任意组合进行控制
11	URL 过滤功能	支持自定义主机名、IP 地址、关键字等方式设置 URL 库，能够对不同的 URL 策略以及时间表设置不同的响应方式
12	内容过滤	支持对设定关键字方式的过滤
13	行为分析与审计	支持对用户 URL 访问历史记录的查询审计，包括提供访问的用户名/IP、网站信息、网页信息、URL 信息、网页标题、访问时间等
		支持 SMTP/POP3 邮件信息审计，包括记录发件人、收件人、抄送人、暗送人、主题、附件名、时间等
		支持对 FTP 审计，包括记录登陆用户名、用户 IP、服务器 IP、操作类型、传输文件名、访问时间等

序号	指标项	指标要求
		审计系统可接收 NAT 日志，会话开始时间与结束时间，从而实现直接审计到内部用户功能
		审计信息可通过 Excel 倒出、通过邮件直接发送，可按时间、地域、用户名、源/目的 IP、动作、类型等进行查询
		提供对 WEB 网站综合分析、WEB 网站应用分析、WEB 应用行为分析、Email 应用行为分析，包括 Top N（N 为 10~100）的柱状图、排行列表等
14	认证功能	支持 WEB 认证等功能
		支持接入用户数> = 20000 个
		支持与 Radius 服务器联动，分析用户名、IP 等信息
		支持与认证接入服务器实现二次认证

4.2.9 租户边界防护产品技术要求

序号	指标项	规格要求
1	安全防护	支持 4 种安全防护模式，基于网络、用户、应用
		支持内嵌深度包检测引擎，针对数据包进行深度过滤检测
		支持对穿透防火墙的 FTP 服务进行过滤审计
		支持通过预定义过滤文件名实现对 FTP 数据流的区分控制
		支持对 vpn 隧道内的内容检查和防护
2	统一特征库	web 页面下统一对设备支持的特征库进行查看、更新及自定义操作
		支持针对 webmail、应用特征库可以根据客户需求实现定制
3	IPv6 支持	支持基于 IPv6 下的路由，包括：直连路由、静态路由、动态路由（OSPF、BGP 等）等
		支持基于 IPv6 下的 IP 地址/地址组的包过滤、内容过滤、IPS 检测、流量控制以及关联时间控制等
4	VPN	支持 PPTP、GRE、IPSEC 等 VPN
		支持隧道热备份、负载均衡、单臂多线路、星形、网状、树状等多种组网方式
5	安全审计	支持将日志存储在本地，标配 1T 日志存储硬盘，完美满足公安部 82 号令,至少保留用户行为日志 60 天的要求

序号	指标项	规格要求
		支持全部日志按天和统一格式（如：ozlog-20141013.log）存储，可以通过 web 页面查看、删除、导出历史日志列表（提供截图说明）
		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

4.2.10 租户入侵防范产品技术要求

序号	指标项	规格要求
1	IPv6 支持	支持基于 IPv6 下的路由，包括：直连路由、静态路由、动态路由（OSPF、BGP 等）等
		支持基于 IPv6 下的 IP 地址/地址组的包过滤、内容过滤、IPS 检测、流量控制以及关联时间控制等
		支持基于 IPv6 下的 IP/MAC 绑定
		支持基于 IPv6 下的流量牵引
2	入侵防护	采用多检测引擎互为备份的检测机制，需说明实现原理
		支持基于 IP 碎片重组、TCP 流重组、会话状态跟踪、应用层协议解码等数据流处理方式的攻击识别；
		支持模式匹配、异常检测、统计分析，以及抗 IDS/IPS 逃逸等多种检测技术
		可依据端口识别协议类型，可分析 HTTP、SMTP、POP3、FTP、Telnet、VLAN、MPLS、ARP、GRE 等多种协议
		内置攻击特征库，特征数量超过 3,500 条，支持在线、离线升级方式，并可自定义攻击特征，阻挡蠕虫、木马、间谍软件、广告软件、缓冲区溢出、扫描、非法连接、SQL 注入、XSS 跨站脚本等多种攻击
		可对英文、UTF8/GB18030/BIG5 中文编码，GZIP/inflate/trunked 压缩算法的的网页内容进行深度特征码检测的舆情监控和报警
		可对告警事件设置丢弃数据包、阻断会话、页面推送、日志/邮件报警、声音、状态灯报警等
3	抗 DDoS 攻击	抗应用型攻击，包括 Web cc、http get flood、DNS query/reply 泛洪攻击或速率限制、DNS 协议自身安全性、DNS 缓存投毒、域名劫持、容

序号	指标项	规格要求
		灾恢复等，并说明其防御原理
		抗流量型攻击，包括 syn flood、udp flood、icmp flood、arp flood、frag flood、stream flood 等攻击
		抗蠕虫连接型攻击，可基于 ACL 或者源或目地 IP 地址进行连接数统计和控制，支持连接排行榜，可早期预警
		抗普通常见攻击，包括 ipspoof、sroute、land、fraggle 攻击、sf_scan、null_scan、xmas_scan、smurf 等攻击
		支持基于事件类别，重要等级，发生时间，五元组等进行攻击取证，并说明实现方式
		允许与 WAF/抗 DDoS 产品联动，从而实现 IPS 与抗 DDoS 设备、WAF 防火墙之间能够同步攻击特征库、同步攻击防护算法

4.2.11 租户防毒墙产品技术要求

序号	指标项	规格要求
1	病毒扫描	支持代理模式
		支持流模式
2	病毒库	支持在线自动升级模式
		支持离线手动升级
3	支持多协议查毒	支持 ftp、http、smtp、pop3、imap 等多种协议病毒扫描；
		支持自定义非标准端口下应用协议的病毒防护
4	支持各种阻断类型	支持过滤邮件病毒、文件病毒、恶意网页代码、木马后门、蠕虫等多种类型的病毒；
		支持所有常见文件格式的病毒查杀，可自定义文件阈值大小、类型；
		支持新一代虚拟脱壳和行为判断技术，准确查杀各种变种病毒、未知病毒。

4.2.12 高危漏洞风险产品技术要求

序号	指标项	指标要求

1	网络适应性	支持 IPv4/v6 双协议栈网络地址解析；支持针对 IPv4/v6 网络中的扫描。
		支持远程管理，自定义可访问设备的网段或 IP；
2	系统漏洞扫描能力要求	产品扫描信息应包括主机信息、用户信息、服务信息、漏洞信息等内容。有效漏洞库至少支持 50000 条以上；
		产品漏洞库应涵盖目前的安全漏洞和攻击特征，漏洞库具备至少 CVE、CNCVE、CNVD、BUGTRAQ、CNNVD 编号；
		支持数据库登录扫描，至少应包括数据库账号，密码，SYSDBA、SYSOPER、NORMAL 认证，SID、数据库名称、实例名称及实例号等登录选项的设置；提供弱口令扫描功能；
3	Web 漏洞扫描要求	漏洞插件库支持按照国际权威安全组织 OWASP TOP 10-2013；
		支持登录认证，至少支持 Cookie 认证、Form 认证、Basic 认证、NTLM 认证、Digest 认证；并支持在线验证是否登录成功，确保授权准确有效
4	报表能力	支持同一任务的两次扫描结果对比，清晰明了的展示出漏洞状态的变更情况；
		在线报表支持手动调整误报、已修复等漏洞类型，导出报表时可选择是否将误报、已修复等漏洞导出
		支持多维度查看分析设备漏洞并导出报告，支持根据节点名称、设备名称、设备 IP、设备管理员、设备操作系统、风险等级、漏洞名称、端口号、检测时间段等查看设备漏洞情况，并保存导出；

4.2.13 网络版杀毒软件

序号	指标项	指标要求
1	网络支持	单向/双向流量，可对单向或双向流量进行监测，
2	疑似文件样本捕获	捕获疑似木马文件，将其完整还原并保存疑似样本。一个疑似样本只保存一次，不重复保存。
3	支持多种文档格式解析	文件格式（包括但不限于 exe、ZIP,RAR,TAR,GZIP,BZIP2,ELF，IPA、mpkg、cab、deb 等格式深度解析），文件可执行性、文件大小（去超大、去超小）、

序号	指标项	指标要求
		文件日期、白名单等。
4	基于特征的攻击检测	具备通过特征匹配的方式对攻击进行检测的能力，需要有单独的木马文件传播特征库以及僵尸主机特征库。
5	僵尸、木马检测	支持对传统僵尸、木马的检测。
6	攻击样本提取	可以提取出攻击的完整样本文件，并提供对该文件下载的能力

第 5 章　系统配置装备清单

序号	装备名称	功能配置	数量	单位	单价（万元）	总价（万元）
1.	等保二级一体机	防火墙 WAF IPS 日志审计 主机安全（含零信任杀毒） 漏洞扫描 终端准入控制系统	1	套	15	15
2.	等保三级一体机	安全管理中心 下一代防火墙 IPS 防毒墙 日志审计 数据库审计 主机安全（零信任 EDR、杀毒） 堡垒机 漏洞扫描 终端准入控制系统	1	套	25	25