# 奇安信网神入侵检测系统

|  |  |
| --- | --- |
| **指标项** | **参数要求** |
| 性能指标 | 1U专业机架式硬件设备，至少具备6个10/100/1000自适应电口，2个扩展板卡插槽，设备采用单电源，配置有USB、console接口，至少3Gbps网络吞吐量，至少1Gbps IDS吞吐能力，最大并发数80万，每秒新建连接数3万/秒，含三年IDS特征库升级服务，三年硬件质保服务。 |
| 网络接口 | 产品具备接口配置IPv6地址功能，包括接口名称、IP地址/掩码、地址类型和IPv6路由通告，并可以显示当前本机的IPv6邻居信息。 |
| 部署模式 | 产品具备透明接入、旁路部署等多种部署模式。 |
| 路由 | 产品具备IPV4、IPV6的静态路由配置，包括目的地址、网关。 |
| 产品具备显示主路由表中的路由条目的功能，包括目的地址、网关和路由标志。 |
| IP/MAC绑定 | 产品具备IP/MAC绑定功能，支持手动添加和自动探测IP/MAC对应关系。 |
| DNS | 产品具备DNS自学习安全缓存、DNS静态缓存功能来检测DNS欺骗、缓存污染、DNS劫持等DNS攻击行为。 |
| 高可靠 | 产品具备双机热备功能，保障设备的高可靠性。 |
| 应用识别 | 产品具备丰富的应用识别特征库，提供P2P下载、网络电视、即时通讯、股票软件、流媒体、网络电话、手机应用等多种应用识别类型，且特征库数量不少于3000。（提供产品功能截图加盖厂商公章进行证明） |
| 产品具备自定义应用协议，提供除五元组之外的应用技术、应用属性、风险级别、类型、子类、协议、匹配内容、应用层长度等多项设置。（提供产品功能截图加盖厂商公章进行证明） |
| ACL | 产品具备基础访问控制列表功能，可配置源及目的IP、时间调度、用户、网络服务、流入接口、应用对象、源域、目的域等，并能够对ACL进行冲突检测。 |
| 产品具备高级访问控制列表功能，可对源及目的MAC、报文头部信息（SYN标志、分片标志、TTL、DSCP、Precedence、TOS）、内网域地址、外网域地址、长连接超时时间等细粒度项进行配置。（提供产品功能截图加盖厂商公章进行证明） |
| 产品具备基于地域的访问控制列表功能，支持根据国家、地区等元素进行地域访问检测。 |
| 服务资源 | 产品具备预定义服务类型，内置预定义了HTTP、HTTPS、ICMP、ICMPV6、telnet、smtp、pop3、SNMP、DNS、IGMP、OSPF、IGRP、GRE、syslog、remotedesk等多种服务，并支持自定义服务对象及类型。 |
| 安全策略 | 产品具备一体化安全策略模板功能，通过单条策略既可完成多项策略设置，可以配置源目的地址、国家地区、源目的域、源目的MAC、时间对象、用户、虚拟身份、服务对象、URL分类等对象，同时可在同一策略下，调用入侵检测、一体化防病毒、文件检测、URL检测、数据检测、威胁情报、口令检测、挂马防护、僵尸网络等应用安全策略进行安全检测。（提供产品功能截图加盖厂商公章进行证明） |
| 配置向导 | 产品具备配置向导功能，通过引导用户配置，包括拓扑图、桥接口配置、地址区域流、IDS、可视、概览等多项元素实现快速配置上线。（提供产品功能截图加盖厂商公章进行证明） |
| 双病毒引擎病毒库 | 产品具备双病毒引擎功能，提供本地病毒引擎与云端第三方病毒引擎功能，支持16类500余万种病毒特征库。（提供产品功能截图加盖厂商公章进行证明） |
| 防病毒技术 | 产品具备病毒多种扫描模式，支持快速扫描和16层深度压缩文件的扫描模式，提供基于HTTP、FTP、IMAP、POP3、SMTP协议的病毒扫描功能。（提供产品功能截图加盖厂商公章进行证明） |
| 产品具备MD5黑白名单策略，通过检测文件MD5值判断文件安全性。（提供产品功能截图加盖厂商公章进行证明） |
| 入侵检测 | 产品具备检测防逃逸技术，提供缓冲区溢出、SQL注入、扫描刺探、间谍软件、拒绝服务、病毒、木马后门、漏洞攻击、潜在风险的入侵检测特征库。 |
| IDS特征库 | 产品提供入侵检测特征库，特征数超过10000条。并提供基于正则表达式匹配方式的自定义特征检测策略。（提供产品功能截图加盖厂商公章进行证明） |
| 情报威胁 | 产品具备云端威胁情报功能，提供僵尸网络、钓鱼网站、恶意网站等10大类的威胁情报的检测，并对检测到的威胁事件执行记录日志、邮件、声音等动作。（提供产品功能截图加盖厂商公章进行证明） |
| 口令检测 | 产品具备暴力破解检测功能，提供基于SMTP/IMAP/POP3/TELNET/FTP/RLOGIN/NNTP/TDS-MS-SQL等协议类型的频率检测机制。 |
| 产品具备弱口令检测功能，提供基于POP3/FTP/TELNET协议的口令长度及口令复杂度等7种元素的检测。 |
| 流量自学习 | 产品具备流量自学习功能，通过设置流量学习时间，通过报文、IP排名、域名统计类型建立网络流量基线。 |
| 洪水检测 | 产品具备DDoS洪水检测功能，提供基于ICMP洪水、IGMP洪水、SYN ACK洪水、数据流洪水、ACK洪水、DHCP洪水、最大连接数洪水、每秒新建连接数洪水、UDP洪水、SYN洪水、HTTP报文洪水、CC、端口扫描、ICMP SWEEP攻击、分片洪水、teardrop等类型的检测。 |
| 扫描和欺骗防护 | 产品具备扫描与欺骗检测功能，提供基于LAND攻击、TCP无标记攻击、不带ACK的FIN标记攻击、Ping-of-death攻击、Winnuke攻击、SYN/FIN标记攻击、圣诞树攻击、Smurf攻击、Fraggle攻击、Trinoo扫描、TFN扫描、stacheldraht扫描、tfn2k扫描、IP报文洪水、超长报文、ARP欺骗、地址欺骗、源路由欺骗的检测。 |
| DNS检测 | 产品具备DNS洪水高级防护模式，支持对自定义检测域名及自动域名防护、域名黑名单的检测机制。 |
| URL检测 | 设备具备URL检测功能，用于对用户访问的网址进行检查，支持关键字和正则两种检测方式。 |
| 网络检测 | 产品具备关键字检测功能，支持基于论坛发帖、邮件协议、TELNET、DNS、RSH、FTP、HTTP协议的关键字检测功能。 |
| 文件检测 | 产品具备文件检测功能，对HTTP、FTP、IMAP、POP3、SMTP协议的avi、rmvb、mp3、mp4等文件类型进行监控。 |
| 日志 | 产品具备日志统计功能，支持入侵检测、DDoS、威胁情报、应用安全等10余种类型的详细日志记录功能。 |
| 产品具备日志聚合功能，通过设置时间、聚合条件来实现安全策略日志、入侵检测等日志聚合功能。 |
| 产品具备syslog日志外发功能，通过设置服务器IP地址、端口把本地日志记录外发到日志服务器。 |
| 事件监控 | 产品具备事件监控功能，支持入侵检测、威胁事件、接口事件等10多种类型的事件监控功能，提供基于饼状、柱状类型的数据统计功能。 |
| 告警 | 产品具备邮件告警功能，支持自动或手工告警设置功能。 |
| 流量趋势 | 产品具备流量趋势监控功能，支持实时与历史监控流量趋势的监控统计功能，提供基于应用、用户、接口、协议等多维度的流量数据趋势统计或分析。 |
| 策略统计 | 产品具备策略统计功能，支持对ACL、安全策略的会话数、上下行流量、上下行报文数进行统计分析。 |
| 大屏 | 产品具备安全态势大屏实时展示，可通过产品自带的实时态势监测模块进行攻击态势地图展示，包含对威胁趋势图、风险主机TOP10、威胁等级 、最新入侵事件 、设备运行状态 、资源监控、告警总数等信息统计展示。（提供产品功能截图加盖厂商公章进行证明） |
| 事件取证 | 产品具备事件取证分析功能，通过获取接口的报文文件保存在设备中留存为证据，取证文件支持导出功能。（提供产品功能截图加盖厂商公章进行证明） |
| SNMP | 产品具备SNMP功能，支持v1、v2、v3协议的SNMP配置功能项。 |
| 账号安全 | 产品具备账号安全管理功能，具备密码强度、登录处理、解决时间等强制性账号安全策略功能。 |
| 配置文件导入导出 | 产品具备配置文件功能，提供配置文件的导入、导出功能，并可以指定下次启动的配置文件。（提供产品功能截图加盖厂商公章进行证明） |
| 升级维护 | 产品具备系统及特征库升级功能，特征库提供在线和离线升级方式。 |
| 辅助工具 | 产品具备界面诊断工具功能，支持内置提供ping、Tracert、抓包等分析诊断工具。 |
| 移动管控 | 产品具备移动终端管理功能，无需安装APP和第三方插件，通过手机浏览器即可管理设备，并可查看设备CPU、内存、硬盘使用情况。（提供产品功能截图加盖厂商公章进行证明） |
| 资质要求 | 所投产品具备公安部网络安全保卫局颁发的《计算机信息系统安全专用产品销售许可证》。 |
| 所投产品提供国家信息测评中心 EAL 3+级资质。 |
| 所投产品提供[IPv6](https://baike.baidu.com/item/IPv6" \t "_blank) Ready Logo测试认证证书。 |
| 所投产品提供CVE兼容性证书。 |

# 奇安信网神防火墙系统

|  |  |
| --- | --- |
| 指标项 | 参数要求 |
| 性能要求 | 1U机箱，最大吞吐量不少于6Gbps，每秒新建连接数至少8万，并发连接数不少于200万，不少于8个10/100/1000M自适应电口、2个SFP光接口和2个SFP+光接口，至少2个扩展插槽，最大支持不少于1000个IPSec VPN，最大支持不少于300个SSL VPN，包含三年硬件质保服务。 |
| 基础组网 | 产品支持路由、透明、交换以及混合模式接入，满足复杂应用环境的接入需求。支持旁路模式。 |
| 所投产品必须支持VTEP（VxLan Tunnel EndPoint）模式接入VxLAN网络，并可作为VXLAN二层、三层网关实现VxLan网络与传统以太网的相同子网内、跨子网间互联互通；支持通过绑定VLAN、VNI（VXLAN Network Identifier）、远程VTEP，手动管理VxLan网络；支持MAC、VNI、VTEP静态绑定。（提供产品功能截图加盖厂商公章进行证明） |
| 所投产品必须支持MPLS流量透传；支持针对MPLS流量的安全审查，包括漏洞防护、反病毒、间谍软件防护、内容过滤、URL过滤、基于终端状态访问控制等安全防护功能。（提供产品功能截图加盖厂商公章进行证明） |
| 所投产品必须支持支持通过802.3ad协议、轮询、热备等方式将多个物理口绑定为一个逻辑接口，实现接口级的冗余，并可根据：源目的MAC组合、MAC和IP组合或TCP/UDP端口组合等方式实现负载和备份。（提供产品功能截图加盖厂商公章进行证明） |
| 所投产品必须支持MTU≥9000byte的巨型帧Jumbo Frame。（投标文件需提供能够体现上述组合方式的配置选项截图） |
| 所投产品必须支持支持静态路由、策略路由及动态路由。策略路由支持用户自定义其优先级，动态路由应至少支持RIP v1/v2/ng， OSPFv2/v3，BGP4/4+协议；必须支持静态和动态多播路由，动态多播路由必须支持PIM-SM（稀疏模式）。（提供产品功能截图加盖厂商公章进行证明） |
| 所投产品必须支持基于策略的路由负载，支持根据应用和服务进行智能选路，支持源地址目的地址哈希、源地址哈希、轮询、时延负载、备份、随机、流量均衡、源地址轮询、目的地址哈希、最优链路带宽负载、最优链路带宽备份、跳数负载等不少于12种路由负载均衡方式，支持基于IPv4或IPv6的TCP、HTTP、DNS、ICMP等方式的链路探测，同时TCP与HTTP可使用自定义目标端口进行测试。（提供产品功能截图加盖厂商公章进行证明） |
| 所投产品必须支持ISP路由负载均衡，最大可支持8条链路负载，支持自定义负载权重，支持基于优先级的ISP路由链路备份；支持基于IPv4或IPv6的TCP、HTTP、DNS、ICMP等方式的链路探测，同时TCP与HTTP可使用自定义目标端口进行测试。（提供产品功能截图加盖厂商公章进行证明） |
| 所投产品必须支持全面的NAT转换配置，包括一对一，一对多，多对一的源、目的地址转换，并至少支持FULL\_CONE模式和SYMMETRIC模式。（投标文件需要提供能够体现上述功能及配置选项的截图以及测试方案） |
| 所投产品必须支持在会话的源、目的地址同为IPv4地址时，可将目的地址转换至指定服务器地址。（提供产品功能截图加盖厂商公章进行证明） |
| 所投产品必须支持在源地址转换过程中，对SNAT（源地址转换）使用的地址池利用率进行监控，并在地址池利用率超过阈值时，通过SNMP Trap、邮件等方式告警。（投标文件需提供能够体现上述功能配置选项截图) |
| 支持IPv4的DNS代理功能，即从指定的入接口或源ISP接收到的DNS解析请求，设备可根据自定义的IP、域名对应关系，代理DNS服务器返回查询结果。（提供产品功能截图加盖厂商公章进行证明） |
| 支持出站的DNS代理功能，支持在不更改内网终端设备DNS服务器地址设置的情况下，将DNS解析请求发送至指定的DNS服务器，并代理原DNS服务器返回解析结果。（提供产品功能截图加盖厂商公章进行证明） |
| 支持DDNS功能，支持Oray向日葵、Pubyun公云、Noip、Changeip提供的DDNS服务，将动态获取的IP地址映射为固定的域名。（投标文件需提供能够体现上述功能配置选项及支持) |
| 支持DNS代理策略功能，支持设置入接口、源地址、目的地址、域名等信息配置代理策略，同时支持手动选择代理或不代理功能，方便灵活根据业务需求调整代理策略。（投标文件需要提供能够体现上述功能及配置选项、DDNS服务商的截图） |
| 所投产品必须设备接口支持配置IPv6地址，并可使用IPv6地址管理设备；支持IPv6手动及自动的IP/MAC探测及绑定。 |
| 所投产品必须支持IPv6下静态路由及策略路由、动态路由，动态路由应包括RIPng、OSPFv3、BGP4+。 |
| 所投产品必须支持NAT64，NAT66、NAT-PT等种IPv4/v6过渡技术，支持针对ICMPv6以及IPv6扩展头防护功能。 |
|
| 所投产品必须支持DNS64功能；支持IPv6入站的DNS代理功能，即从指定的入接口或源ISP接收到的DNS解析请求，设备可根据自定义的IP、域名对应关系，代理DNS服务器返回查询结果。（提供产品功能截图加盖厂商公章进行证明） |
| 所投产品必须支持DS-Lite CPE B4功能，支持成为b4或aftr角色，支持从DHCPv6服务器或手动方式获取AFTR参数。（提供产品功能截图加盖厂商公章进行证明） |
| 所投产品必须支持路由模式、透明模式的HA高可靠性部署，可工作于主备、主主模式，会话、用户、配置可实时同步；HA高可靠性部署支持接口联动，某个端口失效（DOWN），属于同一接口组中其他端口都会进入失效状态（DOWN）；HA高可靠性部署支持配置接口权重；支持链路探测。（提供产品功能截图加盖厂商公章进行证明） |
| 所投产品必须支持将物理防火墙资源，如会话数、安全策略数、源NAT数、目的NAT数，日志存储数量以保留值及最大值的形式自动分配。（提供产品功能截图加盖厂商公章进行证明） |
| 所投产品必须支持虚拟防火墙逻辑接口，可以不占用物理网口的情况下实现虚拟系统之间的相互连接、访问。（提供产品功能截图加盖厂商公章进行证明） |
| 所投产品必须支持对虚系统进行系统配置，包括管理设定、管理主机、证书管理、配置文件导入导出、日志配置；虚系统管理员可分权管理。（提供产品功能截图加盖厂商公章进行证明） |
| 所投产品必须支持在虚系统内独立配置病毒防护、漏洞利用防护、间谍软件防护、URL过滤、文件过滤、内容过滤、邮件过滤、行为管控等安全功能。并可支持对本虚系统内产生的日志进行独立审计。（提供产品功能截图加盖厂商公章进行证明） |
| 访问控制 | 所投产品必须支持基于源安全域、目的安全域、源用户、源地址、源地区、目的地址、目的地区、服务、应用、隧道、时间、VLAN等多种方式进行访问控制，并支持地理区域对象的导入以及重复策略的检查（提供产品功能截图加盖厂商公章进行证明） |
| 所投产品比如支持基于IPv4/v6地址、应用的会话限制，限制动作包每IP新建、每IP并发、所有IP新建、所有IP并发，且可以基于安全域指定限制方向。（提供产品功能截图加盖厂商公章进行证明） |
| 所投产品必须支持基于用户的访问控制，可与LDAP/Radius/证书/Active Directory/TACACS+/POP3等用户认证系统联动。（投标文件需提供能够体现上述功能截图) |
| 支持二层MAC地址IP地址绑定；支持跨三层MAC地址IP地址绑定。（投标文件需提供能够体现上述功能截图) |
| 所投产品必须支持基于关键字的接收、发送或双向Email发件人、收件人过滤，并支持自定义RLB服务器地址配置，并可结合IP黑名单或白名单。 |
| 所投产品必须支持对应用的文件传输行为进行上传、下载、双向的文件类型过滤，应用至少包含即时通讯、常用协议、文件共享、论坛、博客、网页邮件五种分类。（投标文件需提供支持的应用分类和对应的设备配置截图） |
| 所投产品必须支持上传、下载、双向的文件内容过滤；内容过滤支持手工及文件批量导入两种方式进行敏感信息定义；内容过滤至少支持html、doc、docx、xls、xlsx、ppt、pptx、chm、7z等30种常见文件类型；文件类型识别基于文件特征而非扩展名，更改文件扩展名后仍可有效识别。（投标文件需提供支持的文件类型，敏感信息定义方式及对应的设备配置截图） |
| 所投产品必须支持共享上网检测功能，支持共享接入检测和共享接入管控功能，可以通过设置管控地址和例外地址优化管控功能，同时支持阻断或告警动作。（提供产品功能截图加盖厂商公章进行证明） |
| 攻击防护 | 所投产品支持基于不同安全区域防御SYN Flood、UDP Flood、ICMP Flood、IP Flood、DNS Flood、HTTP Flood攻击，并支持警告、丢弃、普通防护（首包丢弃）、增强防护（TC反弹技术）、授权服务器防护（NS重定向）、普通防护（自动重定向）、增强防护（手工确认）等多种防护措施。（提供产品功能截图加盖厂商公章进行证明） |
| 所投产品必须支持可配置阈值的基于安全域或基于二层接口局域网广播防护，防止局域网内广播和多播数据包泛滥。（提供产品功能截图加盖厂商公章进行证明） |
| 所投产品必须支持DHCP协议防护；支持手动定义可信DHCP服务器IPv4和基于阈值限制DHCP请求传输速率。（提供产品功能截图加盖厂商公章进行证明） |
| 所投产品必须能够对HTTP/FTP/POP3/SMTP/IMAP/SMB六种协议进行病毒查杀；本地病毒库规模大于3000万 |
| 所投产品必须支持基于MD5的自定义病毒签名；支持设置例外特征，对特定的病毒特征不进行查杀。（提供产品功能截图加盖厂商公章进行证明） |
|
| 所投产品必须支持漏洞防护功能，同时将漏洞防护特征库分类，至少包括缓冲区溢出、跨站脚本、拒绝服务、恶意扫描、SQL注入、WEB攻击等六种分类；漏洞防护支持日志、阻断、放行、重置等执行动作,可批量设置针对某一分类或全部攻击签名的执行动作；支持基于FTP、HTTP、IMAP、OTHER\_APP、POP3、SMB、SMTP等应用协议的漏洞防护。（投标文件需要提供能够体现漏洞防护特征库分类信息、支持的执行动作以及支持的应用协议的截图） |
| 所投产品必须支持在设备漏洞防护特征库直接查阅攻击的名称、CVEID、CNNVDID、CWEID、严重性、影响的平台、类型、描述、解决方案建议等详细信息。（投标文件需要提供能够在设备上显示以上内容详细信息的截图） |
| 所投产品的漏洞防护特征库及间谍软件库包含高危漏洞攻击特征，至少包括“永恒之蓝”、“震网三代”、“暗云3”、“Struts”、“Struts2”、“Xshell后门代码”以及对应的攻击的名称、CVEID、CNNVDID、CWEID、严重性、影响的平台、类型、描述、解决方案建议等（CVEID、CNNDID、CWEID等信息在漏洞攻击特征中体现）详细信息。（投标文件需要提供设备包含上述所有高危漏洞攻击的特征及对应详细信息的截图） |
| 所投产品必须支持自定义TCP、UDP、HTTP协议的漏洞特征，漏洞特征可通过多个字段以文本或正则表达式的形式进行有序和无序匹配，并可自定义漏洞的源、目的端口范围；同时可标识自定义漏洞的CVE编号或CNNVD编号。（提供产品功能截图加盖厂商公章进行证明） |
| 所投产品必须支持自定义基于TCP、UDP、HTTP协议的间谍软件特征。间谍软件特征可通过多个字段以文本或正则表达式的形式进行有序和无序匹配；并可自定义间谍软件的源、目的端口范围。（提供产品功能截图加盖厂商公章进行证明） |
| 所投产品必须支持IPv4和IPv6流量的HTTPS、POP3S、SMTPS、IMAPS协议进行解密，支持配置基于源安全域、目的安全域、源地址、目的地址、SSL协议服务的解密策略，动作可以设置解密或不解密，并可基于安全域、IPv4和IPv6地址进行例外设置，同时支持将解密后流量镜像到其他设备进行分析统计。（提供产品功能截图加盖厂商公章进行证明） |
| 所投产品必须支持IPv4和IPv6流量的蜜罐引流策略，支持配置基于源安全域、目的安全域、源地址、目的地址、服务、VLAN的引流策略，并支持强制导流，能够通过设置服务器和端口进行引流。（提供产品功能截图加盖厂商公章进行证明） |
| 所投产品必须支持威胁引流功能，威胁引流可以通过开关设置是否开启，通过添加蜜罐地址实现引流，同时支持添加例外域名，做到精细化引流管控。（提供产品功能截图加盖厂商公章进行证明） |
| VPN | 所投产品必须支持L2TP、支持L2TP over IPSec、支持PPTP ，并支持本地认证以及LDAP/Radius/证书/Active Directory/TACACS+/POP3等第三方用户认证系统。支持客户端地址分配。（提供产品功能截图加盖厂商公章进行证明） |
| 所投产品必须支持SSL VPN，支持使用SSL VPN客户端与防火墙建立SSL VPN加密隧道，支持对远程用户进行口令认证或证书认证，或证书认证+口令认证双因素；口令认证支持本地认证以及LDAP/Radius/证书/Active Directory/TACACS+/POP3等第三方用户认证系统；支持USB-key证书；支持本地CA并可为SSL VPN客户端颁发用于身份认证的证书。（提供产品功能截图加盖厂商公章进行证明） |
| 安全管理 | 所投产品必须支持基于主机或威胁情报视图，统计网络中确认被入侵、攻破的主机数量，至少可查看被入侵、攻破的时间、威胁类别、情报来源、威胁简介、被入侵、攻破的主机IP、用户名、资产等信息；并对威胁情报发现的恶意主机执行自动阻断。（投标文件需提供能够体现被入侵、攻破的主机状态的截图） |
| 所投产品必须支持基于主机或威胁情报视图，统计网络中存在安全风险的主机数量以及对应的风险等级，至少可查看遭遇风险的时间、威胁类别、情报来源、威胁简介、失陷主机IP、用户名、资产等信息。（投标文件需提供能够体现存在安全风险的主机数量以及对应风险等级的截图） |
| 所投产品必须支持统计网络内威胁事件的数量及对应的风险等级；支持一键跳转查看详情并自动显示关联日志；可基于网络连接、应用名称、威胁事件处置威胁事件。（投标文件需提供能够体现以上功能的截图） |
| 所投产品必须支持用户自定义重点URL分类和应用，并可基于定义的重点关注对象进行用户维度关联，并结合分析中心进行基于关联的用户/地址、URL分类、应用进行二次递进式深度分析，挖掘异常用户及异常网络行为。（投标文件需提供能够体现以上功能的设备截图） |
| 所投设备必须提供关联分析面板，可将Top应用、Top威胁、Top URL分类、Top源地址、Top目的地址等信息关联，并支持以任意元素于为过滤条件且不少于35个维度进行数据钻取。(投标文件需提供包含上述信息的关联分析面板截图) |
| 所投设备必须支持基于网络活动，威胁活动、阻止活动等多维关联统计及分析，发现异常行为。(投标文件需提供包含上述信息的多维关联分析面板截图) |
| 所投设备必须提供关联的威胁事件日志，系统可自动将产生威胁事件的连接经过防病毒、防漏洞、防间谍软件、URL过滤、文件过滤等安全模块检查的日志集中显示。(投标文件需提供关联的威胁事件日志的截图) |
| 所投设备必须支持自定义一个或多个过滤条件，防火墙上的全部日志进行模糊检索或指定条件的精确检索，快速定位特定目标当前行为是否存在异常，网络中是否存在异常等问题，并可记录一个或者多个自定义过滤条件历史。(投标文件需要提供能够体现上述功能及配置选项的截图) |
| 所投设备可在单条策略中启用病毒防护、入侵防御、网址过滤、文件过滤、文件内容过滤、终端过滤等安全功能选项。(投标文件需提供在单条策略中启用安全功能选项的截图) |
| 所投设备必须支持安全策略的快速检索及基于名称、地址、端口、协议多维度的高级策略检索，支持策略的复制、调序、查询。 |
| 所投产品必须支持基于受害主机的一键式阻断链接、记录日志等处置动作，处置周期至少包括1天、7天、30天、90天、永久等。(投标文件需提供能够体现上述功能及配置选项的截图) |
| 所投产品必须支持接收针对突发重大安全事件的“应急响应消息”，并至少在界面显示安全事件名称、类型、当前防护状态、处置状态以及相应的操作等信息；并可根据设备安全配置的变化动态显示应急响应的处理结果。（提供产品功能截图加盖厂商公章进行证明） |
| 所投产品必须支持针对“应急响应消息”的手动或自动处置，处置方法至少包括基于漏洞的处置和基于威胁情报的处置。（提供产品功能截图加盖厂商公章进行证明） |
| 所投产品必须支持加密的WebUI和CLI管理，且支持网页命令行管理（WebUI中内嵌CLI管理界面），投标文件需提供WebUI内嵌CLI管理界面的设备截图。 |
| 所投产品必须支持将告警信息以SNMP Trap、邮件、声音、短信等形式通知管理员，告警信息的范围至少包括配置变更、病毒事件、攻击事件、异常事件、失陷主机告警、并发数告警、CPU利用率、内存利用率、硬盘利用率、接口带宽利用率、NAT端口池利用率等。（提供产品功能截图加盖厂商公章进行证明） |
| 所投产品必须支持将不同设备模块产生的不同重要性的日志发送至不同的日志服务器，设备模块至少包括配置、时间、流量、URL过滤、内容过滤、邮件过滤、行为、威胁等，重要性等级至少包括紧急、警报、严重、错误、告警、通知、信息、调试八种。（提供产品功能截图加盖厂商公章进行证明） |
| 所投产品必须支持IPS特征库、威胁情报库、应用识别库等数据库的实时更新或手动更新。（提供产品功能截图加盖厂商公章进行证明） |
| 所投产品必须提供可明文或加密方式调用的Restful API，并可指定Restful API使用的本地端口；为确保设备管理的安全性，所投产品必须支持限制特定主机调用Restful API（提供产品功能截图加盖厂商公章进行证明）支持定义第三方设备、平台通过调用Restful API 至少可配置所投设备的访问控制策略、源NAT策略、目的NAT策略、静态路由、高可用以及区域、地址、服务、时间、用户对象等。（投标文件必须提供所投产品的Restful API使用说明并加盖公司公章） |
| 所投产品必须web页面必须内置抓包工具，并可通过表达式方便灵活的指定抓包过滤条件。（提供产品功能截图加盖厂商公章进行证明） |
| 所投产品必须提供中英文双语管理界面，并在登录页面可选择Web页面使用的语言。（提供产品功能截图加盖厂商公章进行证明） |
| 所投产品必须支持业务接口下Netflow功能，能够通过Netflow实现对网络进行监控，对接口流量进行抓包，并在可将Netflow抓包文件数据外发。（提供产品功能截图加盖厂商公章进行证明） |
| 所投产品必须支持资产管理，能够通过设置资产监控、VPN、源安全域来控制资产识别范围，支持scanner或onvif类型的扫描方式和网段，实现自动或手动资产扫描；支持通过设置IP地址、MAC地址、资产类型、生效市场、厂商、位置等信息来制定黑/白名单，方便日常资产管理，支持通过设置IP地址、MAC地址、资产类型、操作系统、应用、开放的端口和访问的端口等信息来制定资产指纹库。（提供产品功能截图加盖厂商公章进行证明） |
| 协同防御 | 所投产品必须支持与云端联动，至少实现病毒云查杀、URL云识别、应用云识别、云沙箱、威胁情报云检测等功能。（提供产品功能截图加盖厂商公章进行证明） |
| 所投产品必须支持作为轻量级“探针”与本方案中配置的网络威胁感知系统联动，上报网络活动产生的数据至网络威胁感知系统；并支持接收来自网络威胁感知系统推送的处置策略，及时拦截绕过防御措施产生的高级威胁。（提供产品功能截图加盖厂商公章进行证明） |
| 所投产品必须支持作为轻量级“探针”与本方案中配置的NGSOC平台联动，上报网络活动产生的数据至NGSOC平台；并支持接收来自NGSOC平台推送的处置策略，及时拦截绕过防御措施产生的高级威胁。（提供产品功能截图加盖厂商公章进行证明） |
| 所投产品必须支持与本方案中配置的桌面杀毒或终端管理软件联动，实现基于终端健康状态的访问控制；并支持阻断“高风险”终端网络活动的同时，提示被阻断原因及重定向自定义网址。（提供产品功能截图加盖厂商公章进行证明） |
| 所投产品集中管理平台支持安全策略下发、设备统一监控、日志管理、告警管理、报表管理等功能，提供产品截图并提供权威测试机构检测报告。（投标文件需要提供能够体现上述功能的截图以及对应的检测报告） |
| 所投产品必须支持与本地以及云端沙箱联动，检测文件中携带的未知威胁，并接受沙箱下发的处置策略。（提供产品功能截图加盖厂商公章进行证明） |
| 资质要求 | 所投产品具备公安部网络安全保卫局颁发的《计算机信息系统安全专用产品销售许可证》。 |
| 所投产品具备国家信息安全测评中心颁发的《信息技术产品安全测评证书》。 |
| 所投产品具备《计算机软件著作权登记证书》。 |
| 具备《中国国家信息安全产品认证证书》。 |
| 具备中国信息安全测评中心颁发的《国家信息安全漏洞库兼容性资质证书》。 |