中国共产党开封市纪律检查委员会
开封市纪检监察系统工作网项目技术参数变更

序号	内容	原技术要求	现变更为
1	防火墙	1.产品不低于5个千兆电口，4个千兆光口，2个万兆光口，,网络层吞吐量(双向)：IPv4：11500GMbps，IPv6：11700Mbps 应用层吞吐量(单向)： IPv4：8000Mbps，IPv6：8150Mbps TCP新建连接速率： IPv4：95万/秒,IPv6:95万/秒 TCP并发连接数：IPv4：2000.00万，IPv6：2000.00万； 2.★支持策略略路由，支持根据入接口、源/目的IP地址、协议、用户、应用、选路算法、探测等多种条件设置策略路由；（提供截图） 3.★支持一体化安全策略配置，可以通过一条策略实现五元组、源MAC、源地区、目的地区、域名、应用、服务、时间、长连接、并发会话、WEB认证、IPS、AV、URL过滤、WAF、邮件安全、数据过滤、文件过滤、审计等功能配置,简化用户管理；（提供截图） 4.★支持在一台物理设备上划分出128个相互独立的虚拟系统，可根据连接配额及连接新建速率为每个虚拟系统分配资源，实配不少于24个虚拟防火墙授权；（提供截图） 5.支持IP DDOS防护，可对IP Flood、IP Frag Flood、端口扫描、IP 地址扫描，以及Fraggle、icmp redirect、icmp unreachable、land、ping of death、smurf、route record、source route、tcp flag、tracert、winnuke等异常报文攻击； 6.★内置静态黑名单功能，可设置多个对象条件，如：五元组信息、源MAC、地址范	1.产品不低于5个千兆电口，4个千兆光口，2个万兆光口，网络层吞吐量(双向)：IPv4：11500GMbps，IPv6：11700Mbps 应用层吞吐量(单向)：IPv4：8000Mbps，IPv6：8150Mbps TCP新建连接速率： IPv4：95万/秒，IPv6：95万/秒 TCP并发连接数： IPv4：2000.00万，IPv6：2000.00万； 2.★支持策略路由，支持根据入接口、源/目的IP地址、协议、用户、应用、选路算法、探测等多种条件设置策略路由；（提供截图） 3.支持一体化安全策略配置，可以通过一条策略实现五元组、源MAC、源地区、目的地区、域名、应用、服务、时间、长连接、IPS、AV、URL过滤、WAF、邮件安全、数据过滤、文件过滤、审计等功能配置，简化用户管理； 4.支持IP DDOS防护，可对IP Flood、IP Frag Flood、端口扫描、IP 地址扫描，以及Fraggle、icmp redirect、icmp unreachable、land、ping of death、smurf、route record、source route、tcp flag、tracert、winnuke等

		围、应用、用户，实现对特定报文进行快速过滤；（提供截图） 7. 支持 CPU 利用率、内存利用率、磁盘利用率、会话数告警及 CPU 利用率、内存利用率、磁盘利用率等硬件资源实时利用率及其历史使用情况追踪； 8. 安全操作系统采用冗余设计（提供截图），出于安全性考虑，多系统需在设备启动过程中进行选择不得在 WEB 维护界面中设置系统切换选项。（提供操作系统兼容性证明） 9. 提供完善的审计数据查询功能，方便管理员对用户的上网行为进行审查和分析。支持对用户上网行为进行完整的审计数据查询，包括访问网站、邮件收发、FTP 等；（提供截图）同时支持对用户上网流量时长进行完整的审计数据查询，包括服务端 IP、用户名、协议、上行流量、下行流量、总流量、时间等； 10. 支持 ICMPv6、ND、DHCPv6、RADVD、IPv6 静态路由、RIPng、OSPFv3 等；	异常报文攻击； 5. 内置静态黑名单功能； 6. 支持 CPU 利用率、内存利用率、磁盘利用率、会话数告警及 CPU 利用率等硬件资源实时利用率及其历史使用情况追踪； 7. 提供完善的审计数据查询功能，方便管理员对用户的上网行为进行审查和分析。同时支持对用户上网流量时长进行完整的审计数据查询，包括服务端 IP、用户名、协议、上行流量、下行流量、总流量、时间等； 8. 支持 ICMPv6、ND、DHCPv6、RADVD、IPv6 静态路由、RIPng、OSPFv3 等；
2	入侵防御系统	1. 产品由专用的国产化硬件平台、国产化安全操作系统及功能软件构成。支持 B/S 管理模式，无需安装独立的控制台软件。 2. 产品不小于 4 个千兆电口（至少提供 2 组 Bypass 接口），3 个千兆光口，满检速率≥6500Mbps，TCP 并发连接数≥80 万。 3. 支持在线抓包，可配置抓包数量、协议类型、源 IP、源端口、目的 IP、目的端口、源或目的 IP、源或目的端口、文件名、接口、VLAN ID 等。支持在线多任务并行抓包。（提供截图证明） 4. ★支持规则库升级无缝加载技术，整个升级过程检测引擎工作不间断。 5. 支持攻击检测规则库、应用识别库、URL 分类库（扩展支持）、僵尸主机规则库、威胁情报库（扩展支持）、地理信息库，各规则库相互独立。（提供截图证明）	1. 产品由专用的国产化硬件平台、国产化安全操作系统及功能软件构成。支持 B/S 管理模式，无需安装独立的控制台软件。 2. 产品不小于 4 个千兆电口（至少提供 2 组 Bypass 接口），3 个千兆光口，满检速率≥6500Mbps，TCP 并发连接数≥80 万。 3. 支持在线抓包，可配置抓包数量、协议类型、源 IP、源端口、目的 IP、目的端口、源或目的 IP、源或目的端口等。（提供截图证明） 4. 支持规则库升级无缝加载技术，整个升级过程检测引擎

		6. 支持设置的监控内容有：CPU 占用率、内存占用率、磁盘占用率、并发连接数、新建连接数、接口速率百分比、冗余电源、规则库过期。（提供截图证明） 7. 支持对源地址、目的地址、事件风险等级、事件类型、TopN 等条件设置报表模板。（提供截图证明）报表可支持手动导出和自动导出两种方式。 8. ★支持独立的攻击检测引擎，涵盖 13000 种以上的攻击检测规则库。规则库支持按照攻击类型、操作系统、风险等级、应用类型、流行程度等方式进行分类。（提供截图证明） 9. ★智慧引擎检测功能能够实现对目标文件实时检测实时还原的效果，不依赖规则库即可实现对未知恶意程序检测。（提供截图证明） 10. ★支持对传统协议生成流量审计日志，包括 TCP/UDP、ICMP、HTTP、SMTP、POP3、IMAP、FTP、SMB、NFS、文件、MYSQL、MSSQL、ORACLE、POSTGRESQL、DB2、REDIS、MONGODB、达梦、南大通用、人大金仓、SSL、RDP、DNS、SNMP、TFTP、IKEV2、LDAP、SIP、SSDP、SOCKS4、SOCKS5、AFP、VNC、SSH、DHCP、RADIUS、NTP、认证、SPICE、FEIQ、WAP 等。（提供截图证明）	工作不间断。 5. 支持攻击检测规则库、应用识别库等。 6. 支持设置的监控内容有：CPU 占用率、内存占用率、磁盘占用率、并发连接数、新建连接数、接口速率百分比、冗余电源、规则库过期。（提供截图证明） 7. 支持对源地址、目的地址、事件风险等级、事件类型、TopN 等条件设置报表模板。（提供截图证明）报表可支持手动导出和自动导出两种方式。 8. ★支持独立的攻击检测引擎，涵盖 13000 种以上的攻击检测规则库。规则库支持按照攻击类型、操作系统、风险等级、应用类型、流行程度等方式进行分类。
3	入侵检测系统	1. 产品由专用的国产化硬件平台、国产化安全操作系统及功能软件构成。支持 B/S 管理模式，无需安装独立的控制台软件。 2. 产品不小于 4 个千兆电口，3 个千兆光口，2 个万兆光口。满检速率≥23500Mbps。TCP 并发连接数≥450.000 万。 3. ★支持独立的攻击检测引擎，涵盖 15000 种以上的攻击检测规则库。规则库支持按照攻击类型、操作系统、风险等级、应用类型、流行程度等方式进行分类。（提供截图证明） 4. ★支持工控漏洞攻击、车联网漏洞攻击、	1. 产品由专用的国产化硬件平台、国产化安全操作系统及功能软件构成。支持 B/S 管理模式，无需安装独立的控制台软件。 2. 产品不小于 4 个千兆电口，3 个千兆光口，2 个万兆光口。满检速率≥23500Mbps。TCP 并发连接数≥450.000 万。 3. ★支持独立的攻击检测引擎。 4. 支持 ARP 攻击检测，支持基

		物联网漏洞攻击。如对施耐德、Siemens、SCADA、SERVER-WEBAPP Linksys E 系列、IGSS SCADA 系统、罗克韦尔、华为 HG532 路由产品、Vivotek 智能摄像头、Xiaomi Mi WiFi R3G 路径遍历漏洞攻击等。（提供截图证明） 5. 支持 ARP 攻击检测，支持基于 ARP 请求的源 IP 不合法、响应的源 IP 不合法、响应的目的 IP 不合法、请求的源 MAC 与以太网源 MAC 不同、响应的源 MAC 与以太网源 MAC 不同、响应的目的 MAC 与以太网目的 MAC 不同进行检测。 6. ★支持对 HTTP、FTP、SMTP、IMAP、POP3、TELNET 等服务的隐蔽通信检测，可设置相应警告、联动阻断动作，并可设置忽略知名应用。（提供截图证明） 7. ★支持通过威胁情报检测已知 APT 事件（扩展功能），通过恶意程序检测未知 APT 事件（扩展功能），通过僵尸主机规则库检测已知的 APT 组织。（提供截图证明） 8. 支持支持攻击取证、僵尸主机取证、恶意程序样本、恶意程序无风险样本、威胁情报样本、威胁情报取证、WEB 防护取证、异常流量取证，取证类型支持报文取证和样本文件取证两种形式。（提供截图证明） 9. 支持针对不同类别告警信息进行配置，包括安全（攻击检测、僵尸主机、恶意程序、威胁情报、WEB 防护、异常流量、DDoS 检测、URL 过滤、黑名单）、管理、系统、硬件、容错、测试等，并可进行告警测试。（提供截图证明）	于 ARP 请求的源 IP 不合法、响应的源 IP 不合法、响应的目的 IP 不合法、请求的源 MAC 与以太网源 MAC 不同、响应的源 MAC 与以太网源 MAC 不同、响应的目的 MAC 与以太网目的 MAC 不同进行检测。 5. ★支持对 HTTP、FTP、SMTP、IMAP、POP3、TELNET 等服务的隐蔽通信检测。 6. 支持通过威胁情报检测已知 APT 事件（扩展功能）。 7. 支持攻击取证、僵尸主机取证、WEB 防护取证等，取证类型支持报文取证。 8. 支持针对不同类别告警信息进行配置，包括安全（攻击检测、僵尸主机、恶意程序、威胁情报、WEB 防护、异常流量、DDoS 检测、URL 过滤、黑名单）。
4	漏洞扫描系统	1. 产品需提供不小于 5 个千兆电口，4 个千兆光口，不小于 3800GSATA 硬盘。并发扫描任务不低于 10 个。 2. 支持配置扫描任务最大并发线程数，可根据网络空闲状态调整漏洞扫描的并发进程数量；扫描目标支持 ip、域名、网段、子网的组合配置。	1. 产品需提供不小于 5 个千兆电口，4 个千兆光口，不小于 3800GSATA 硬盘。并发扫描任务不低于 10 个。 2. 支持配置扫描任务最大并发线程数，可根据网络空闲状态调整漏洞扫描的并发进程

		3.★支持扫描系统漏洞数量大于240000种，web漏洞数量大于5000种，数据库大于3000种，CVE漏洞数大于60000（提供截图）。 4.端口扫描支持TCP CONNECT、TCP SYN、TCP FIN、UDP等多种方式，提供标准通用端口、快速扫描端口、全部TCP端口、指定端口四种扫描策略（提供截图）。 5.★请提供设备厂商连续四年为CNVD漏洞信息报送突出贡献单位以及原创漏洞报送（发现）突出贡献单位的证明；（提供证明文件）； 6.支持自定义http请求，包括UserAgent、http cookie、http header、超时时间、重试次数、表单输入（提供截图）； 7.支持漏洞生命周期管理，包括未修复、确定、忽略、修复、已验证五种状态（提供截图）。 8.主机报表支持展示主机风险、漏洞信息，及主机详细的端口信息、端口Banner信息、安装软件信息、操作系统类型。 9.支持对扫描任务进行克隆、搜索、导出、删除、查看等操作，支持断点续扫功能。 10.★支持首页全面展示风险分布及趋势图表，包括主机风险分布、站点风险分布、漏洞风险分布、漏洞top10、资产风险值趋势、资产风险分布趋势（提供截图）。 11.支持无限制IP扫描授权。	数量；扫描目标支持ip、域名、网段、子网的组合配置。 3.端口扫描支持TCP CONNECT、TCP SYN、TCP FIN、UDP等多种方式。 4.支持漏洞生命周期管理，包括未修复、确定、忽略、修复、已验证五种状态（提供截图）。 5.主机报表支持展示主机风险、漏洞信息，及主机详细的端口信息、端口Banner信息、安装软件信息、操作系统类型。 6.支持对扫描任务进行克隆、搜索、导出、删除、查看等操作，支持断点续扫功能。 7.★支持首页全面展示风险分布及趋势图表，包括主机风险分布、站点风险分布、漏洞风险分布、资产风险值趋势、资产风险分布趋势（提供截图）。 8.支持无限制IP扫描授权。
5	堡垒机	1.采用专用硬件架构与安全操作系统，硬件设备可以机架安装。产品采用模块化设计，可以通过扩展卡来增减业务接口，而非软件运维安全审计系统。 2.产品需提供不小于5个千兆电口，4个千兆光口，50个授权许可。 3.★支持混合云资源的管理，即公有云及局域网资源，支持主机、服务器、网络设备、安全设备、数据库等的资产管理；满足公有云、数据中心多种运维场景；	1.采用专用硬件架构与安全操作系统，硬件设备可以机架安装。产品采用模块化设计，可以通过扩展卡来增减业务接口，而非软件运维安全审计系统。 2.产品需提供不小于5个千兆电口，4个千兆光口，50个授权许可。 3.★支持混合云资源的管理，

		4. 通过 IP 网段扫描，快速发现指定 IP 地址范围内的资产，并自动识别 IP 和端口，方便管理员快速添加资产。 5. 支持各种自定义客户端工具，支持通过动作流配置提供广泛的应用接入支持，在不作二次开发的情况下，可灵活扩展且实现帐号口令的代填。 6. 登录规则是对用户登录系统的访问控制；支持登录规则的新建、编辑、启用、禁用和删除；支持用户 IP 地址、MAC 地址和登录时间的访问控制。 7. ★批量运维视图配置，支持标签/九宫格展示方式，便于用户查看运维资产信息。 8. ★支持图形化查看用户的运维记录，查询结果以鱼骨图按照时间倒序自上而下而下展示，每个时间点详细记录运维资产、运维用户、账号、协议、会话时长等详细信息； 9. ★支持快捷菜单，用户可自行设置快捷菜单项，快速定位至此功能，方便用户查找经常使用的功能。	即公有云及局域网资源，支持主机、服务器、网络设备、安全设备、数据库等的资产管理；满足公有云、数据中心多种运维场景； 4. 通过 IP 网段扫描，快速发现指定 IP 地址范围内的资产，并自动识别 IP 和端口，方便管理员快速添加资产。 5. 支持各种自定义客户端工具，支持通过动作流配置提供广泛的应用接入支持，在不作二次开发的情况下，可灵活扩展且实现帐号口令的代填。 6. 登录规则是对用户登录系统的访问控制；支持登录规则的新建、编辑、启用、禁用和删除；支持用户 IP 地址、MAC 地址和登录时间的访问控制。 7. ★批量运维视图配置，便于用户查看运维资产信息。 8. ★支持查看用户的运维记录；

中共开封市纪律检查委员会

2024 年 8 月 5 日