|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **产品名称** | **招标参数** | **总数量** | **单位** |
| 1 | 下一代防火墙 | 1. 产品不少于6个10/100/1000M以太网电口，2个10/100/1000M SFP口，支持单电源，1U机箱。吞吐量3G，IPS吞吐量≥400M，并发连接数≥100万，新建连接数≥3万；提供3年的硬件维保、软件升级，5年特征库升级，含WEB应用防护识别库、IPS特征库、僵尸网络防护库、实时漏洞分析识别库和URL&应用识别库。云端百亿级威胁情报规则库。 2.产品支持路由模式、透明模式、虚拟网线模式、旁路镜像模式等多种部署方式。 ▲3.产品支持对不少于9000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，提供厂家盖章件）。 ▲4.产品应具备独立的勒索病毒防护模块，非普通防病毒功能，支持对特定的业务进行勒索风险自动化评估，并依据评估结果自动生成防护策略，支持在设备界面独立展示勒索风险板块。（需提供产品功能截图证明，提供厂家盖章件）。 ▲5.产品内置不低于15000种漏洞规则，同时支持在控制台界面通过漏洞ID、漏洞名称、危险等级、漏洞CVE标识、漏洞描述等条件查询漏洞特征信息，支持用户自定义IPS规则。（需提供产品功能截图证明，提供厂家盖章件）。 ▲6.产品支持僵尸主机检测功能，产品内置僵尸网络特征库超过128万种，可识别主机的异常外联行为。（需提供产品功能截图证明，提供厂家盖章件）。 ▲7.产品支持策略生命周期管理功能，支持对安全策略修改的时间、原因、变更类型进行统一管理，便于策略的运维与管理。（需提供产品功能截图证明，提供厂家盖章件）。 8.产品支持安全策略有效性分析功能，分析内容至少包括策略冗余分析、策略匹配分析、风险端口风险等内容，提供安全策略优化建议。 9.产品支持对ICMP、UDP、DNS、SYN等协议进行DDOS防护。 10.支持被动监测和主动扫描两种资产识别方式，可梳理离线资产、高危端口开放、冗余端口等安全风险；同时通过可视化的拓扑关系图，直观地展示资产和资产之间的访问关系、访问细节协议端口等信息；   11.支持与本地终端安全响应软件产品联动，防火墙检测发现的病毒主机可以联动终端安全响应软件产品进行微隔离与病毒文件查杀，增强整体终端安全防护能力，提供制造商承诺函。 | 1 | 台 |
| 2 | 下一代防火墙 | 1. 产品不少于8个10/100/1000M以太网电口，2个10/100/1000M SFP口，支持单电源，1U机箱。吞吐量≥4G，IPS吞吐量≥600M，并发连接数≥200万，新建连接数≥6万；提供3年的硬件维保、软件升级，5年特征库升级，含WEB应用防护识别库、IPS特征库、僵尸网络防护库、实时漏洞分析识别库和URL&应用识别库。云端百亿级威胁情报规则库。 2.产品支持路由模式、透明模式、虚拟网线模式、旁路镜像模式等多种部署方式。 ▲3.产品支持对不少于9000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，提供厂家盖章件）。 ▲4.产品应具备独立的勒索病毒防护模块，非普通防病毒功能，支持对特定的业务进行勒索风险自动化评估，并依据评估结果自动生成防护策略，支持在设备界面独立展示勒索风险板块。（需提供产品功能截图证明，提供厂家盖章件）。 ▲5.产品内置不低于15000种漏洞规则，同时支持在控制台界面通过漏洞ID、漏洞名称、危险等级、漏洞CVE标识、漏洞描述等条件查询漏洞特征信息，支持用户自定义IPS规则。（需提供产品功能截图证明，提供厂家盖章件）。 ▲6.产品支持僵尸主机检测功能，产品内置僵尸网络特征库超过128万种，可识别主机的异常外联行为。（需提供产品功能截图证明，提供厂家盖章件）。 ▲7.产品支持策略生命周期管理功能，支持对安全策略修改的时间、原因、变更类型进行统一管理，便于策略的运维与管理。（需提供产品功能截图证明，提供厂家盖章件）。 8.产品支持安全策略有效性分析功能，分析内容至少包括策略冗余分析、策略匹配分析、风险端口风险等内容，提供安全策略优化建议。 9.产品支持对ICMP、UDP、DNS、SYN等协议进行DDOS防护。 10.支持被动监测和主动扫描两种资产识别方式，可梳理离线资产、高危端口开放、冗余端口等安全风险；同时通过可视化的拓扑关系图，直观地展示资产和资产之间的访问关系、访问细节协议端口等信息；   11.支持与本地终端安全响应软件产品联动，防火墙检测发现的病毒主机可以联动终端安全响应软件产品进行微隔离与病毒文件查杀，增强整体终端安全防护能力，提供制造商承诺函。 | 1 | 台 |
| 1. 为保障本次所投防火墙在安全漏洞方面的整体研究水平和及时预防能力，要求本次所投制造商为国家信息安全漏洞共享平台CNVD技术组和用户组成员，要求提供CNVD国家信息安全漏洞共享平台官网界面截图并加盖厂商公章； 2、为体现本次所投防火墙产品制造厂商的软件成熟度，要求本次所投产品制造厂商需获得中国网络安全审查技术与认证中心（CCRC）颁发的软件安全开发服务资质（一级）   3、为应对勒索病毒、挖矿木马、僵尸网络等对业务系统进行攻击，导致数据被加密或被破坏不可用，要求本次所投下一代防火墙制造厂商具备较强的安全应急服务能力，本次所投产品制造厂商需是网络安全应急服务支撑单位（甲级），要求提供有效证书复印件并加盖厂商公章，  4、提供所投产品的制造商项目授权函及售后服务承诺函； | | | | |