微隔离防火墙技术参数

|  |  |
| --- | --- |
| 品牌/型号 | 山石网科、安恒、华三 |
| 技术指标 | 技术参数 |
| 基本要求 | 支持单台物理服务器防护性能指标：最大吞吐量≥5Gbps，最大并发连接数≥170万，最大每秒新建连接数≥3万，IPS吞吐量≥1.5Gbps，AV吞吐量≥1.5Gbps。 |
| 网络微分域方案环境适应性 | 在VMware标准环境，不依赖NSX组件或不依赖第三方SDN产品方案配合，提供云内虚机间网络微分域解决方案。 |
| 采用虚拟机形态提供本地化、分布式网络安全服务，使得业务虚拟机流量不用外出宿主机，即可高效的实现网络安全管控。能为同一宿主机，相同VLAN内的虚拟机之间，提供网络微分域的安全管控服务。 |
| 产品形态 | 产品提供的安全服务能力，无需要求在业务虚机中额外安装第三方插件或Agent软件。 |
| 可靠性 | 为确保业务连续性，要求处理业务流量的安全服务节点具备自动Bypass能力，以应对产品自身故障，或云平台网络通讯异常，误操作等突发状况。 |
| 安全服务能力 | 为满足网络安全可视化监测要求，须在非NSX环境下，支持VSS/VDS网络的旁路侦听部署模式。 |
| 为确保安全服务的有效性，需实时掌握云环境中的资产信息和变更状况，支持对云虚机名称，IP，MAC，网络，宿主机等信息的同步和更新。 |
| 为适应云计算环境下的灵活性和随机性，安全服务的对象需能支持基于虚机名称定义安全防护控制。 |
| 支持会话同步能力，安全防护可随虚机迁移而自动跟随，最大限度的确保安全防护的持续性和业务连续性。 |
| 可视化能力 | 虚拟资产分布可视化，可基于虚拟网络-虚拟机分组方式管理，并呈现各分组之间和分组内部的流量交换关系。 |
| 可通过流量交互关系图跟踪各个虚拟资产的流量、应用、威胁统计状况。流量关系线条可根据威胁等级呈现出不同颜色，可根据风险等级进行筛选展示。 |
| 可基于IP地址，流量，防护状态，虚机和网络名称，应用类型，威胁名称/类型/安全级别等条件不同组合关系控制视图呈现效果，并可基于IP地址，流量，防护状态，虚机名称等条件筛选的结果生成新的展示视图，新的视图可直接点击进行视图展开，无需手动筛选。 |
| 网络攻击防护 | 为避免部分特殊业务被识别为网络攻击而被防护能力阻断，需支持配置白名单，白名单可手动配置IP地址、地址簿、虚机名称、攻击特征等。 |
| DoS/DDoS识别防护能力,包括：DNS Query Flood、SYN Flood、UDP Flood、ICMP Flood、Ping of Death、Smurf、WinNuke，TCP Split Handshake，动作支持记录、阻断两种模式。 |
| 入侵防御 | 支持对HTTP、FTP、SMTP、IMAP、POP3、TELNET、TCP、UDP、DNS、RPC、FINGER+C95、MSSQL、ORACLE、NNTP、DHCP、LDAP、VoIP、NETBIOS、TFTP、SUNRPC和MSRPC等常用协议及应用的攻击检测和防御。 |
| 具备1.2万种以上攻击特征库规则列表，至少支持基于协议类型、操作系统、攻击类型、流行程度、严重程度、特征ID等方式的查询。 |
| 为避免部分特殊业务被识别为入侵动作而被防护能力阻断，需支持配置白名单，白名单可手动配置源地址，目的地址和攻击特征。 |
| 支持缓冲区溢出、SQL注入、XSS防护，支持HTTP头域中的URL、Cookie、Referer、POST检查点配置防护策略。 |
| 运维管理 | 为方便管理员制定安全策略，需支持流量学习到安全策略配置的策略助手功能，提高工作效率。 |
| 为便于网络故障分析定位，需具备流量抓包能力，并可导出pcap格式的抓包文件。 |
| 为应对突发情况时快速恢复配置，需支持全局配置的定期备份和外发能力。 |
| 为改善安全策略的管理有效率，需支持对安全策略冗余检测，以及重叠性检查能力。 |
| 维保服务要求 | 提供至少800个虚拟机的防护授权，五年软件维保服务，五年入侵防御特征库升级服务。 |
| 售后与响应支持服务 | 质保期间，提供7天×24小时×365天的电话支持服务，响应时间为1小时。包括节假日，非工作时间均可通过电话进行各类常见问题疑难解答，问题咨询，产品使用指导等。 |
| 根据采购方要求，在重大故障及重大活动期间，提供现场技术保障支持服务。 |
| 在已知设备软缺陷可能导致潜在问题的情况下，通过配置管理或巡检等方式对产品进行软件版本升级服务。 |
| 当产品出现故障后，采购方与投标品牌原厂工程师共同对故障进行分析并确认是软件缺陷所导致的故障，投标品牌原厂商提供针对该软件缺陷的软件补丁程序，原厂工程师对设备进行软件版本升级服务。 |
| 对软件出现的任何故障提供1小时电话响应服务，提供4小时现场响应服务以及免费上门调试安装、故障排查服务、免费维修服务。 |