互联网信息安全设备技术要求

1.行为审计

|  |  |  |
| --- | --- | --- |
| **项目** | **模块** | **功能** |
| 硬件规格 | 产品结构 | 机架式独立硬件设备，系统硬件为全内置封闭式结构，稳定可靠 |
| 多核架构设计，不允许采用X86架构，功能采用模块化结构设计 |
| 最大功率≤300W  |
| 物理接口 | 支持10M/100M/1000M自适应电接口数量≥12，支持千兆SFP光接口数量≥12，万兆接口总数≥4  |
|
|
| 部署适应性 | 部署模式 | 支持路由模式、透明（网桥）模式、混合模式，支持镜像接口，部署模式切换无需重启设备 |
| 接口配置 | 支持以太网接口、VLAN、桥接口、聚合接口、隧道接口、4G无线接口、安全域、IPv6隧道接口、Ipsec隧道接口；支持端口镜像 |
| DNS-DNAT | 支持负载在出接口的DNS请求主动完成DNS服务器替换 |
| DDNS | 支持DDNS功能 |
| 花生壳DDNS | 支持花生壳DDNS客户端以及域名IP绑定功能 |
| 路由支持 | 支持静态路由、策略路由、RIP、OSPF、ISP路由 |
| 链路聚合 | 透明、路由模式下支持将多条链路带宽进行捆绑  |
| IPv6 | 支持接入IPv6网络 |
| 4G支持 | 支持4G扩展网卡 |
| 功能要求 | 安全通信 | 实际配置支持一对一、多对一、多对多等多种形式的NAT，支持H.323等应用协议ALG |
| 实际配置支持基于用户、应用、时间对象的流量管控和策略设置 |
| 应用协议识别 | 支持主流P2P、IM、在线视频、网络游戏、网络炒股等应用识别支持BYOD特征库应用特征库数量不低于5000+  |
| 针对特定无应用指纹的应用：迅雷、P2P下载支持行为模式的智能识别 |
| 支持下一代防火墙IPS、AV、WAF、弱密码扫描、负载均衡等一系列能力 |
| 用户行为审计 | 支持http、邮件、即时通讯、基础协议、娱乐股票、网络应用六个大类维度的用户应用审计 |
| 用户认证功能 | 支持本地web认证，针对本地web认证的认证服务器可以是本地AAA，也支持外部radius、ldap认证服务器 |
| 链路负载均衡 | 支持7元组的链路负载均衡策略 |
| 服务器负载均衡 | 支持一个公网IP映射到内网多台服务器，服务器间支持连接和源地址hash，支持服务器健康检查，提供web配置界面截图 |
| 病毒防护 | 支持800万病毒防护特征库，请提供产品截图 |
| web防护 | 支持1000+规则库，产品分类支持AQL注入攻击、XSS攻击、恶意扫描及爬虫、WebShell攻击、会话劫持、敏感信息泄露、CMS漏洞防护等类型，并提供产品截图 |

2.链路负载均衡

|  |  |
| --- | --- |
| **功能及技术指标** | **详细技术参数** |
| 产品架构 | 采用专用多核硬件架构，不允许采用X86架构，提供CPU型号供货时查验 |
| 硬件配置要求 | 固定接口千兆电口≥16个，千兆光口≥8个，万兆光口≥2个 |
| 扩展槽≥2个 |
| 1U标准机架式设备 |
| 性能要求 | 整机吞吐量≥9G |
| L4新建连接数≥11万 |
| 并发连接数≥1000万 |
| 基本网络功能 | 支持端口聚合 |
| 支持VLAN、STP、MSTP |
| 支持RIP、OSPF、BGP等路由协议 |
| 服务器负载均衡 | 支持包括轮询、加权轮询、最小连接、加权最小连接、随机、加权随机、源地址Hash、源地址端口Hash、目的地址Hash、优先级等负载均衡调度算法 |
| 虚拟化 | 支持多虚一(N:1)后再一虚多(1:N)  |
| API接口 | 支持工业标准的Netconf API接口，实现与第三方管理软件的无缝集成。 |
| SDN网络功能虚拟化 | 设备支持VxLAN技术，实现云数据中心SDN VxLAN网络部署。 |
| 管理方式 | Web（HTTP）、CLI（Telnet/SSH）。支持标准网管 SNMPV3，并且兼容SNMP V2C、SNMP V1。支持中文界面管理，提供截图。支持采用命令行对设备进行功能配置，提供配置虚服务的命令行截图。 |
| 拥有同品牌统一的软件管理平台，能够统一管理虚机、负载均衡设备；控制虚机新建、删除、关机、开机、重启，与此同时联动修改负载均衡配置，从而实现整体系统的动态资源联动。（需提供设备功能界面截图证明） |
| IPv6 | 支持IPv6 基础特性及IPv6的负载均衡，满足今后IPv6网络的升级 |
| 厂商资质 | 厂商必须通过CMMI4认证以保障产品代码质量与稳定性，提供证书复印件 |
| 所投产品具备《计算机软件著作权登记证书》 |

3.入侵检测设备

|  |  |
| --- | --- |
| **功能及技术指标** | **详细技术参数** |
| 硬件架构 | 采用非X86多核架构，双电源，1U的独立盒式设备，具备独立的攻击检测引擎与病毒检测引擎 |
|
| 接口要求 | 至少配置16个千兆电口，8个千兆光口，2个万兆光口，1个console口，2个USB接口。支持接口扩展，接口扩展插槽≥2个，扩展类型包括自带PFC接口，千兆电、千兆光以及万兆光接口 |
| 性能要求 | 吞吐量（全威胁应用层吞吐）≥3.6Gbps，最大并发连接数≥500万，每秒新建连接数≥5万。须提供国家相关部委认可的第三方实验室测试报告证明，提供报告复印件，且设备制造厂商必须盖章。 |
| 硬盘扩展插槽数量≥2；硬盘支持可插拔 |
| 支持1+1AC/DC冗余电源，支持热插拔 |
| 虚拟IPS数量≥4 |
| 部署模式 | 实现路由模式、透明（网桥）模式、混合模式部署。 |
| 路由实现 | 实现静态路由、策略路由、RIP、OSPF、等价路由等路由协议。 |
| 入侵防御 | 攻击特征库数量≥8500、病毒特征库数量≥600W、支持的协议识别数量≥5500、WEB攻击特征库≥3500 |
| IPS检测到攻击报文或攻击流量后，支持Web重定向、黑名单等响应方式，以实现第一时间隔离有安全威胁的主机，（提供配置界面截图） |
| URL过滤 | 设备支持管理者自定义新的URL地址和URL分类 |
| WEB安全 | 支持SQL注入攻击、命令注入、脚本注入等注入类攻击的检测与阻断 |
| 加密流量检测 | 支持HTTPS加密流量的安全检测。（提供功能截图） |
| IPv6 | 实现IPV6动态路由协议、IPV6对象及策略、IPV6攻击防范、IPV6日志审计、IPV6会话热备等功能。 |
| DDoS防护 | 能够防范DOS/DDOS攻击 |
| 虚拟化能力 | 所投设备须支持虚拟入侵防御功能：支持虚拟入侵防御的创建、启动、关闭、删除功能；可独立分配CPU/内存等计算资源；可独立管理，独立保存配置；具备独立会话管理、NAT、路由等功能。上述功能要求须提国家相关部委认可的第三方实验室测试报告证明，提供报告复印件，且必须加盖原厂公章或项目授权章 |
| 支持2台设备堆叠成一台设备使用，实现统一管理，统一配置，所投设备支持高可靠性（包含主备/主主模式）部署，上述功能要求须提国家相关部委认可的第三方实验室测试报告证明，提供报告复印件，且必须加盖原厂公章或项目授权章 |
| 统一管理 | 对多台分布式部署的场景，提供管理软件实现对多台分布式部署的IPS设备进行集中管理 |
| 统计报表 | 支持报表个性化设置功能，至少要支持汇总报表，对比报表，智能报表，综合报表等4中以上报表形式 |
| 日志管理 | 支持安全日志，应用审计日志，设备日志的统一收集与展示 |
| 厂商资质 | 厂商必须通过CMMI5认证以保障产品代码质量与稳定性，提供证书复印件 |
| 产品资质 | 具备《计算机信息系统安全专用产品销售许可证》，要求销售许可证上的产品名称为必须为入侵防御系统或入侵抵御系统（其他UTM类、IDS类、安全网关类的销售许可证无效） |

4.防火墙

|  |  |
| --- | --- |
| **功能及技术指标** | **详细技术参数** |
| 硬件架构 | 采用非X86多核架构，具备可插拔冗余电源模块，可插拔冗余风扇模块 |
|
| 接口要求 | 千兆电口≥16个，千兆光口≥8个，扩展插槽≥2个 |
| 性能要求 | 应用层吞吐量≥2G，并发连接数≥500万，新建连接数≥8万，带机量≥8K |
|
|
|
| 升级服务 | 配置三年IPS/AV升级授权 |
| 部署模式 | 实现路由模式、透明（网桥）模式、混合模式。 |
| NAT功能 | NAT地址池支持动态探测和可用地址分配 |
| VPN | 实现高性能IPSec、L2TP、GRE VPN、SSL VPN等功能。 |
| WEB安全防护 | 可针对HTTP/HTTPS的安全策略来专门为Web应用提供保护。 |
| URL过滤 | 设备提供海量预分类的URL地址库，支持根据URL类别实现URL过滤； |
| 设备支持管理者自定义新的URL地址和URL分类； |
| 支持联动云端URL地址库进行全面实施核查。（提供功能截图） |
| 入侵防御 | 支持超过7000种特征的攻击检测和防御 |
| 防病毒 | 可基于病毒特征进行检测，实现病毒库手动和自动升级，报文流处理模式，实现病毒日志和报表；发现病毒发送的告警信息，支持用户编辑告警内容 |
| IPv6 | 实现IPV6动态路由协议、IPV6对象及策略 |
| 负载均衡 | 支持全局负载功能，支持就近性探测末班的配置（提供截图） |
| 虚拟化能力 | 所支持2台设备堆叠成一台设备使用，实现统一管理，统一配置，所投设备支持高可靠性（包含主备/主主模式）部署，上述功能要求须提国家相关部委认可的第三方实验室测试报告证明，提供报告复印件，且必须加盖原厂公章或项目授权章。 |
|
| 厂商资质 | 设备制造厂商符合信息技术服务管理体系符合ISO/IEC 20000-1：2011标准，符合信息安全管理体系符合ISO/IEC 27001：2013标准； |
| 上述资质，须提供相关证书证明，提供证书复印件，且设备制造厂商必须盖章。 |
| 产品资质 | 所投产品须具备公安部监制的计算机信息系统安全专用产品销售许可证； |
| 具备信息产业信息安全测评中心出具的防火墙EAL4+级型式试验报告； |

5.路由器

|  |  |
| --- | --- |
| **功能** | **详细技术参数** |
| 体系架构 | 冗余主控,要求主控切换时不影响业务转发 |
| 包转发率（IPv4）提供第三方测试报告 | ≥360Mpps，  |
| IPv6转发速率 | ≥160Gbps |
| 接口数量 | 实配≥10GE（combo） |
| 电源系统 | 电源数量≥2 |
| 机电设计 | 主机接口与扩展插槽接口均为同一朝向 |
| 广域网优化 | 支持对HTTP/FTP等TCP业务流量进行优化传输技术，提高广域网带宽利用率，权威第三方机构的测试报告 |
| Segment Routing | Segment Routing，控制流量按照预先设置的网络节点逐跳转发，权威第三方机构的测试报告 |
| NTPv6 | 支持IPv6-IPv6报文前缀转换 |
| IPv6 NetStream | 支持IPv6 NetStream |
| ND攻击防御 | 支持ND攻击防御，防止IPv6终端仿冒攻击 |
| 语音特性 | 支持语音特性，包括VoIP、语音接口、SIP等 |

6.web应用防火墙

|  |  |
| --- | --- |
| 指标项 | 详细描述 |
| 设备要求 | 硬件要求： 2U高机架式硬件架构，标配单电源（可支持双电源冗余），8G内存，1T硬盘，2个以太网千兆管理接口，支持至少6个以太网千兆电口及8个以太网千兆光口，支持至少2个接口扩展槽位性能要求： HTTP吞吐量不低于1Gbps，HTTP并发连接数不低于60万、HTTP每秒新建连接数不低于4万，保护网站站点数量无限制 |
| 系统管理 | 系统采用B/S设计架构，并采用SSL加密通信方式，通过浏览器方便对产品进行远程管理； |
| 支持IPv4、IPv6双栈防护； |
| 支持旁路镜像模式下，对检测到的攻击进行旁路阻断；[（提供截图证明）](#_旁路镜像模式) |
| 支持设置扫描陷阱，防止恶意扫描；[（提供截图证明）](#_防扫描陷阱) |
| 应能识别和防止敏感信息泄露；且可自定义敏感信息特征，如用户名、密码、邮箱、身份证信息、MD5密码等 |
| 审计及告警[[1]](#endnote-0) | 要求具备独立的审计日志、流量日志、攻击日志、DDoS防护日志及威胁情报日志模块，且支持按不同日志分类进行syslog外发，至少支持字符串和json两种数据格式；[（提供截图证明）](#_日志格式) |
| 产品资质 | 1. 具备公安部《计算机信息系统安全专用产品 销售许可证》-增强级
2. CCRC 网络关键设备和网络安全专用产品安全认证证书-增强级（原ISCCC-网专证书）
3. 工业和信息化部颁发的电信设备进网许可证 （用户接入服务管理器进网许可证）
4. 具备国家版权局颁发的《计算机软件著作权登记证书》
 |

1. 7.异常流量检测系统设备

|  |  |
| --- | --- |
| **功能及技术指标** | **参数要求** |
| 设备要求 | 流量清洗系统结构一体化，应采用B/S架构，运行与管理无需外置环境配合，所有功能操作均能够在设备内置的管理接口上完成。 |
| DPI≥2GDFI≥20万flow/s" |
| 采用非X86多核架构，前后通风设计，具备可插拔冗余电源模块 |
| 千兆电口≥16个，千兆光口≥8个，万兆光口≥2个，扩展槽≥2个， |
| 攻击防护能力 | 支持对欺骗与非欺骗的TCP (SYN, SYN-ACK, ACK, FIN, fragments) 、UDP (random port floods, fragments)、ICMP (unreachable, echo, fragments)、(M)Stream Flood及混合类型攻击的防护。 |
| 支持针对SYN、UDP、ICMP、SYN/ACK、FIN/RST、IP Fragment、ACK等网络层Flood类型的攻击防护；支持针对HTTP GET/POST、HTTPS、DNS Query、DNS Reply、SIP等应用层攻击的防护；支持针对CC攻击、慢速攻击、连接耗尽等连接型攻击的防护；（提供功能页面截图） |
| 支持每域名限速DNS合法性检查、DNS过滤、TCP校验、重传校验、Reply状态防护、递归防护； |
| IPV6攻击防护 | 设备必须支持IPv6基本组网功能及IPv6攻击的防御功能，包括支持ISISv6、OSPFv3、BGP4+协议；支持IPv6 Syn Flood、IPv6 DNS Query Flood、IPv6 UDP flood、IPv6 ICMPv6 Flood攻击防御。； |
| FLOOD攻击防御 | 支持识别并防御各类FLOOD攻击，如UDP Flood，UDP Fragment，ACK Flood，SYN Flood，FIN/RST Flood，TCP Misuse，TCP Connection Flood，TCP Fragment，ICMP Flood，ICMP Fragment； |
| HTTP类防护 | 支持HTTP协议的清洗，包括但不限于：HTTP GET FLOOD、HTTP POST FLOOD、HTTP代理攻击。 |
| 指纹防护 | 支持自动挖掘攻击特征功能，能自动发现攻击特征用于攻击防御；（提供功能页面截图） |
| 管理功能 | 管理界面要友好、易用性强，应支持本地管理、远程管理等多种管理方式，并能实时显示攻击事件、流量、系统运行状况等信息。 |
| 支持手动指定参数抓包；手动抓包参数至少支持源目的IP、源目的端口、协议类型、抓包时长、抓包数量等；支持自动抓包，当发生攻击事件时自动抓取报文留作回溯取证；抓包文件支持通过wireshark等分析软件进行解析分析； |
| 牵引方式 | 支持静态和动态牵引方式，并且支持BGP、OSPF路由协议。 |
| 支持二层回注、三层回注、GRE回注、MPLS LSP回注、MPLS VPN回注等多种回注方式。 |
| 产品资质 | 中华人民共和国公安部颁发的《计算机信息系统安全专用产品销售许可证》 |
| 厂商资质 | 要求设备厂商为反网络病毒联盟成员单位，提供证明材料要求设备厂商为CNVD 技术组成员单位，提供证明材料要求设备厂商为CNNVD 一级支撑单位，提供证明材料要求设备厂商为WAPI联盟成员，提供证明材料 |

 [↑](#endnote-ref-0)