|  |  |  |  |
| --- | --- | --- | --- |
| **项目** | **产品名称** | **型号及功能** | **数量** |
| 1 | 防火墙 | H3C F1000-AK1242硬件：采用非X86多核架构，2U机架式设备，16个千兆电口（含2个管理电口）+4对Combo口+6个千兆光口+2个万兆光口，2个接口扩展槽位，1个硬盘扩展槽位（配备硬盘不小于500G），双电源。性能：三层吞吐量10Gbps，应用层吞吐量4G，防病毒吞吐量1G，IPS吞吐量800M，全威胁吞吐量600M；并发连接数220万，每秒新建连接数（HTTP）6万。功能：支持路由、透明、混合模式部署，支持AI智能防护、AI智能策略、AI智能分析、AI智能诊断等AI能力，支持WEB安全防护、资产扫描、加密流量检测、应用审计、数据安全、网页过滤、带宽管理、IPS、AV等应用层安全功能，支持链路负载、服务器负载，支持SSL VPN \IPSEC VPN等多种VPN功能，支持国密算法，支持IPV6协议及翻译技术，支持多虚一集群以及一虚多虚拟化功能。。配套授权：15个SLL VPN用户授权，链路负载不限制链路数量。硬件质保服务：五年原厂硬件质保及5\*10\*NBD备件服务，五年WAF特征库、IPS、防病毒AV、ACG应用识别特征库升级服务。服务要求：原防火墙及网络线路割接，设备安装调试，安全策略更新，等保测评配合，攻防演练工程师现场支持服务，提供每季度设备及安全巡检（详细配置要求见附件一） | **1** |
| 2 | 路由器 | 华为AR2240C | **1** |
| 3 | 企业级交换机 | 华为S5720-32X-EI-AC，三层千兆8光口24电口 | **1** |
| 4 | 接入层交换机 | 华为S5735S-L24T4S-A，三层千兆4光口24电口网管交换机 | **8** |

附件一：

|  |  |
| --- | --- |
| **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，自带双交流电源，支持配置成双直流电源。（多核架构需提供证明材料）。 |
|
| 扩展性 | 要求具备接口扩展能力 |
| ★接口要求 | 至少16个千兆电口（含2个管理电口）+4对Combo口+6个千兆光口+2个万兆光口，2个接口扩展槽位，1个硬盘扩展槽位.支持不少于4个接口扩展槽位，扩展类型包括4端口千兆电（带PFC功能）、4端口千兆光、4端口万兆光、6端口万兆光 |
| ★性能要求 | 网络层吞吐量≥10G，最大并发连接数≥220万，每秒新建连接数≥8万，每秒新建连接数≥15万。SSL VPN并发用户不低于4000；IPSec VPN隧道数不少于4000；虚拟防火墙数量≥8； |
|
|
|
| 升级服务 | 整机同时具备防火墙、链路负载均衡、入侵防御、防病毒、带宽控制、应用识别和web应用防护等功能。SSL VPN，默认免费提供15个并发（用户）授权 |
| 部署模式 | 实现路由模式、透明（网桥）模式、虚拟网线模式、旁路镜像模式。 |
| 路由实现 | 实现静态路由、策略路由、和多播路由协议，并支持RIP、OSPF、BGP等路由协议。 |
| NAT功能 | 实现一对一、多对一、多对多等多种形式的NAT，实现DNS、FTP、H.323等多种NAT ALG功能。 |
| NAT地址池支持动态探测和可用地址分配，支持各种应用协议的NAT 穿越，实现SQLNET、TFTP、RTSP、PPTP、FTP、H.323、SIP等多种NAT ALG功能。 |
| ★VPN | 实现高性能IPSec、L2TP、GRE VPN、SSL VPN等功能。 |
| 支持IPsec VPN隧道自动建立，无需流量触发； |
| 支持IPsec VPN智能选路，，根据线路质量实现自动链路切换。（需提供产品功能截图证明） |
| SSL VPN支持IPv6接入方式，包括TCP/WEB接入和IP接入 |
| SSLVPN支持页面定制功能特性，包括登录页面、交互信息、提示信息的定制功能； |
| 可基于每个SSL VPN用户的会话连接数、连接时间和流量阀值进行细颗粒度的管控。（提供功能截图） |
| 攻击防护 | 实现安全区域划分，访问控制列表，配置对象及策略，动态包过滤，黑名单，MAC和IP绑定功能，基于MAC的访问控制列表，802.1q VLAN 透传等功能。 |
| 安全策略 | 支持一体化安全策略，可基于时间、用户、应用、IP、域名等内容进行安全策略设置； |
| 支持策略冗余分析， 冲突策略分析以及命中率统计。 |
| 支持策略风险调优，支持安全策略优化分析，支持策略数冗余及命中分析，支持基于应用风险的策略调优，可根据流量、应用、风险类型等细粒度展示，并给出总体安全评分，便于用户更好的管理安全策略。（提供功能截图） |
| ★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。对来自Web应用程序客户端的各类请求进行内容检测和验证，确保其安全性与合法性，对非法的请求予以实时阻断，从而对各类网站进行有效防护。 |
| 产品支持对请求报文头的X-Forward-For字段检测，并对非法源IP进行日志记录和联动封锁。 |
| 支持sql注入、跨站脚本、远程代码执行、字符编码等攻击的防护，支持对网络设备、网页服务器、数据库等设备的专属特征分类，支持CC攻击防护，可基于检测请求报文头的X-forward-for字段，以获取真正的源IP地址（提供功能截图）WAF规则支持用户自定义，同时支持导入和导出功能 |
| 应用识别 | 支持至少5500条以上的应用识别，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） |
| 终端识别 | 当终端流量流经设备时，设备可以分析并提取出终端信息，例如终端的厂商、型号等，并支持在终端信息发生变更时（比如将原厂商的摄像头换为其他厂商的摄像头）向用户发送日志，提示用户。（提供截图） |
| ★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） |
| ★威胁可视化 | 僵尸网络分析，攻击链推导及资产安全风险等级的可视化呈现；基于应用的数据分析 |
| 入侵防御 | 支持基于对包括但不限于操作系统、网络设备、办公软件、网页服务等保护对象的入侵防御策略，支持基于对漏洞、恶意文件、信息收集类攻击等的攻击分类的防护策略，支持基于服务器、客户端的防护策略。且缺省动作支持黑名单（提供截图） |
| 实现对黑客攻击、蠕虫/病毒、木马、恶意代码、间谍软件/广告软件等攻击的防御，实现缓冲区溢出、SQL注入、IDS/IPS逃逸等攻击的防御，实现攻击特征库的分类。IPS发现攻击后抓取报文，并支持通过WEB下载对应抓包文件，供客户进行分析产品支持僵尸主机检测功能，产品预定义特征库超过110万种，可识别主机的异常外联行为。（需提供产品功能截图证明） |
| 支持超过8000种特征的攻击检测和防御。支持在产品漏洞特征库中以漏洞名称、漏洞ID、漏洞CVE标识、危险等级和漏洞描述等条件快速查询特定漏洞特征信息，支持用户自定义IPS规则。 |
| 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，实现病毒日志和报表；支持基于文件协议、邮件协议（SMTP/HTTP/FTP/SMB/POP3/HTTPS/IMAP)、共享协议（NFS/SMB）的病毒功能（提供截图）。可基于病毒特征进行检测、动作响应、提供报表。发现病毒发送的告警信息，支持用户编辑告警内容 |
| 支持云端防病毒，为保证检测时效性，特征缓存数至少保证20万条且缓存保留时间不应少于700分钟（提供截图） |
| 数据安全 | 支持数据防泄露，对传输的文件和内容进行识别过滤，对内容与身份证号、信用卡号、银行卡号、手机号等类型进行匹配。（提供截图） |
| 流量控制 | 可支持基于应用层协议设置流控策略，包括设置最大带宽、保证带宽、协议流量优先级等。 |
| ★共享上网管理 | 支持多用户共享上网行为管理（提供功能界面截图） |
| ★加密流量检测 | 支持HTTPS加密流量的安全检测，支持TCP代理和SSL代理，且代理策略中可同时配置多类过滤条件，具体包括：源安全域、目的安全域、源地址、目的地址、用户和服务。一类过滤条件可以配置多个匹配项（提供截图） |
| IPv6 | 实现IPV6动态路由协议、IPV6对象及策略、IPV6状态防火墙、IPV6攻击防范、IPV6 GRE/IPSEC VPN、IPV6日志审计、IPV6会话热备等功能。 |
| 支持IPV6下的访问控制、IPSec VPN、DDoS防护等安全功能。 |
| ★负载均衡 | 多出口智能选路，支持基于链路权重、带宽、配置优先级、链路质量、用户业务、运营商、域名、时间、DSCP、PPPoE、DNS、地址加权HASH等智能选路方式 |
| LB支持TCP智能监控，支持TCP RST、TCP zero-window或HTTP passive类型的探测模板 |
| 支持智能DNS解析功能，引导访问用户从最优路径的线路接入应用系统。 |
| 支持DNS透明代理功能，可基于负载均衡算法代理内网用户进行DNS请求转发，避免单运营商DNS解析出现单一链路流量过载，平衡多条运营商线路的带宽利用率。（需提供设备功能界面截图证明） |
| 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。 |
| 支持基于Http Accept-Encoding、HTTP Accept-Language、Http Host、Http Request-Method、Http URL-File、Http User-Agent等协议 |
| 支持服务器负载均衡支持基于HTTP RADIUS MYSQL等应用类型的匹配，支持基于IP流量特征、ISP 、用户、入接口、tcp载荷等类型的匹配规则（提供截图） |
| ★DDoS防护 | 能够防范DOS/DDOS攻击：Land、Smurf、Fraggle、Ping of Death、Tear Drop、IP Spoofing、IP分片报文、ARP欺骗、ARP主动反向查询、TCP报文标志位不合法、超大ICMP报文、地址扫描、端口扫描等攻击防范，还包括针对SYN Flood、UPD Flood、ICMP Flood、DNS Flood、http Flood、https Flood、sip Flood等常见DDoS攻击的检测防御。 |
| 支持HTTP慢速攻击检测与防护 |
| 支持流量自学习功能，可设置自学习时间，并自动生成DDoS防范策略。（提供功能截图） |
| 诊断中心 | 支持基于接口及IP的报文捕获，并将捕获到的报文生成Wireshark（一种网络封包分析软件）可识别的.cap后缀文件，保存到本地或外部服务器，供用户分析诊断出入设备的流量。（提供截图） |
| 支持网页诊断功能，用于当内网用户访问网页出现故障时，对网络进行基本的诊断，并给出故障原因。（提供截图） |
| 支持报文示踪功能，支持真实流量、导入报文、构造报文等方式，用于分析和追踪设备中各个安全业务模块（如：攻击防范、uRPF、会话管理和连接数限制等）对报文的处理过程，通过查看报文示踪记录的详细信息，有利于管理员对网络故障的快速排查和定位。（提供功能截图） |
| 支持IPsec故障诊断功能，应支持至少三种诊断模式：数据流、接口、IP地址。用于检测IPsec连接的状态，当IPsec连接发生故障时，可以协助用户排查IPsec配置中的问题，并提供可能的原因。（提供功能截图） |
| 国密算法 | 支持国密SM1/2/3/4算法。（提供功能截图） |
| ★虚拟化能力 | 所投设备须支持虚拟防火墙功能：支持虚拟防火墙的创建、启动、关闭、删除功能；可独立分配CPU、接口、吞吐量、内存、磁盘空间等资源。（提供功能截图） |
|
| 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。（提供功能截图） |
| 设备管理 | 支持SNMPv1、SNMPv2、SNMPv3、RMON等网络管理协议，并且支持通过网管软件远程进行设备软件升级、配置等。 |
| 为了保证整个网络的可靠稳定，要求本次采购的安全设备支持A/S，A/A方式部署，支持配置同步和会话同步；（提供截图） |
| 提供开放API接口（RESTful，NetConf），可编程管理防火墙，不再仅依赖网管软件。 |
| ★产品资质 | 所投产品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； |
| 所投产品具备中国信息安全认证中心颁发的国家信息安全产品认证证书； |
| 所投产品具备中国网络安全审查技术与认证中心颁发的EAL4增强级认证证书 |
| 所投产品具备中国信息安全测评中心颁发的EAL4+测评证书。 |
| 要求所投产品具备国家信息安全漏洞库兼容性资质证书。 |
| 所投产品具备ICSA实验室颁发的防火墙证书 |
| 所投产品具备CNNVD颁发的CNNVD兼容性资质证书 |
| 投标厂商为国内知名品牌，防火墙产品需连续四年入围Gartner企业防火墙四象限，提供证明材料。 |
| 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。 |  |
| ★厂商资质 | 制造厂商须符合电信行业质量管理体系标准，以保障产品系统的高可靠性，通过TL9000电信行业质量管理体系认证 |
| 为体现投标产品生产厂商的软件研发和管理实力，厂商软件开发必须通过CMMI5级认证，具备云安全成熟度成熟度模型CS-CMMI 5认证 |
| 投标产品制造厂商应具有完善的售后服务体系，专业的售后服务专业队伍，健全的售后服务制度和质量监测体系，通过服务体系完善程度认证七星级。 |
| 投标产品制造厂商应具有预防潜在的威胁,增强本项目应对灾难的能力，保证产品和服务的连续性，通过ISO 22301业务连续性管理体系认证(认证覆盖的业务范围包括本次投标产品)。 |
| 为保证产品制造厂商所提供的产品是经过严格测试，具备高可靠性保障能力。制造厂商需具备一定规模的可靠性实验室，可独立完成从元器件到整机，从信号质量、安全性、电磁兼容性、环境适应性等丰富的测试环境。实验室获得国家认监委认可。 |
| 为保证投标产品的厂商在安全漏洞方面整体研究水平及安全漏洞及时预防能力。具备网络安全漏洞统一收集验证、预警发布及应急处置体系，进而提高产品的安全性。产品生产厂商须进入国家信息安全漏洞共享平台（CNVD）技术组成员，并为2020年度漏洞信息报送突出贡献单位（CNVD） |
| 为保证投标产品的厂商在安全漏洞方面整体研究水平及安全漏洞及时预防能力。具备网络安全漏洞统一收集验证、预警发布及应急处置体系，进而提高产品的安全性。产品生产厂商须进入国家信息安全漏洞库（CNNVD）一级技术支撑单位 |
| 为衡量投标产品厂商网络安全服务能力，依据《工业和信息化部关于加强电信和互联网行业网络安全工作的指导意见》（工信部保〔2014〕368号）要求，产品生产厂商需获得由中国通信企业协会颁发的网络安全风险评估资质 |
| 为衡量所投产品制造商具备信息系统安全集成服务能力，提供中国网络安全审查技术与认证中心颁发的信息系统安全集成服务一级服务资质证书 |
| 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。 |