防火墙采购技术要求

1、技术要求:

货物名称	技术要求	数量
防火墙	**接口** 8GE **环境温度** 工作：0～45℃ 非工作：-40～70℃ **运行模式** 路由模式、透明模式、混杂模式 **AAA 服务** Portal 认证、RADIUS 认证、HWTACACS 认证、PKI /CA（X.509 格式）认证、域认证、CHAP 验证、PAP 验证 **防火墙：** 安全区域划分 可以防御 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、SYN Flood、UPD Flood、ICMP Flood、DNS Flood 等多种恶意攻击 基础和扩展的访问控制列表 基于时间段的访问控制列表 基于用户、应用的访问控制列表 ASPF 应用层报文过滤 静态和动态黑名单功能 MAC 和 IP 绑定功能 基于 MAC 的访问控制列表 支持 802.1q VLAN 透传 **病毒防护：** 基于病毒特征进行检测 支持病毒库手动和自动升级 报文流处理模式 支持 HTTP、FTP、SMTP、POP3 协议 支持的病毒类型：Backdoor、Email-Worm、IM-Worm、P2P-Worm、Trojan、AdWare、Virus 等 支持病毒日志和报表 **深度入侵防御：** 支持对黑客攻击、蠕虫/病毒、木马、恶意代码、间谍软件/广告软件、DoS/DDoS 等常见的攻击防御 支持缓冲区溢出、SQL 注入、IDS/IPS 逃逸等攻击的防御 支持攻击特征库的分类（根据攻击类型、目标机系统进行分类）、分级（分高、中、低、提示四级） 支持攻击特征库的手动和自动升级（TFTP 和 HTTP） 支持对 BT 等 P2P/IM 识别和控制 **邮件/网页/应用层过滤** 邮件过滤 SMTP 邮件地址过滤 邮件标题过滤 邮件内容过滤 邮件附件过滤	2 台

	网页过滤 HTTP URL 过滤 HTTP 内容过滤 应用层过滤 Java Blocking ActiveX Blocking SQL 注入攻击防范 **NAT：** 支持多个内部地址映射到同一个公网地址 支持多个内部地址映射到多个公网地址 支持内部地址到公网地址一一映射 支持源地址和目的地址同时转换 支持外部网络主机访问内部服务器 支持内部地址直接映射到接口公网 IP 地址 支持 DNS 映射功能 可配置支持地址转换的有效时间 支持多种 NAT ALG，包括 DNS、FTP、H.323、ILS、MSN、NBT、PPTP、SIP 等 **VPN：** L2TP VPN、IPSec VPN、GRE VPN、SSL VPN 高可靠性： 支持双机状态热备（Active/Active 和 Active/Backup 两种工作模式） 支持双机配置同步 支持 IPSec VPN 的 IKE 状态同步 支持 VRRP **易维护性：** 支持基于命令行的配置管理 支持 Web 方式进行远程配置管理 支持 H3C SSM 安全管理中心进行设备管理 支持标准网管 SNMPv3，并且兼容 SNMP v1 和 v2 智能安全策略 **环保与认证：** 支持欧洲严格的 RoHS 环保认证	

2、产品质量及供应商资质要求：

①、所投设备必须满足以上技术参数、配置（功能）要求。

②、质量保证：报价设备是全新的、未使用过的、原包装未拆封的商品，完全符合采购设备规定的质量、规格和性能的要求；

③、供应商需具备所投设备的代理资质或设备厂家授权；售后服务体系通过 ISO9001 认证。

④、售后服务要求：质保期≥三年。

⑤、供应商需满足在中华人民共和国境内注册、具有独立承担民事责任能力的企业法人营业执照经营范围符合采购项目要求。