中国医学科学院肿瘤医院

外网防火墙

技术需求

**信息中心/计算机室**

**2017年5月**

# 项目简介

随着我院整体信息安全建设的不断深入，安全建设已逐步进入细节建设阶段。为满足不同应用间数据安全交互的需要，完善数据交换区管理功能。现在需要增加两台防火墙，实现端口控制、入侵防御、交互管理的功能。

# 参数要求

需求数量：2台，具体参数要求见下表：

|  |  |  |
| --- | --- | --- |
| **项目** | **指标** | **具体要求** |
|
| **性能和容量** | 防火墙吞吐量 | 最大吞吐量≥18Gbps |
| 应用（HTTP）吞吐量 | HTTP应用最大吞吐量≥9Gbps |
| 安全功能全开吞吐量 | 开启全部安全功能的最大吞吐量≥4.5Gbps |
| 新建连接速率 | 每秒新建连接数≥15万 |
| 并发连接数 | 并发连接数≥400万 |
| **硬件规格** | 机箱高度 | 2U机箱 |
| 网络接口 | 6个千兆电口和4个千兆光口 |
| 接口扩展 | 2个接口扩展槽 |
| 电源 | 交流双电源 |
| **基础组网** | 部署模式 | 支持将接口设置为网关模式、透明模式和镜像模式部署 |
| 路由协议 | 支持静态路由、策略路由、RIP、OSPF路由 |
| 地址转换 | 支持多种形式的地址转换功能，可配置源地址转换、目的地址转换及双向地址转换（在一条规则中既实现源地址转换，又实现目的地址转换）策略  |
| DNS透明代理 | 可识别并透明代理到任意DNS服务器的解析请求，支持在不更改终端设备DNS服务器地址设置的情况下，将指定的域名解析为IP地址，或将解析请求发送至指定的DNS服务器，并代理原DNS服务器返回解析结果 |
| IP协议 | 支持IPv4和IPv6双栈，产品具有IPv6 Ready Phase2认证 |
| 高可靠性 | 支持HA高可靠性部署，可工作于主备、主主模式，会话、用户、配置可实时同步 |
|  | 应用协议识别 | 可实现应用控制，应用特征库包含的应用数量（非应用协议的规则总数）大于4000种 |
| **访问控制** | 可深度识别每种应用的安全属性，为每种应用提供预定义的风险系数 |
| 自定义应用 | 可基于协议端口、IP、HTTP-get/post/connect/host/referer/user-agent等参数值自定义B/S应用，并可自定义其应用风险系数 |
| 用户识别 | 支持基于用户的访问控制，可与LDAP/Radius用户认证系统联动，并能够基于POP3和ESMTP协议与邮件系统进行认证联动  |
| 可免认证同步AD/SQL Server/MySQL/ORACLE等系统的用户认证信息 |
| 文件传输控制 | 可对不小于100种应用（要求至少包含20种电子邮件应用、50种论坛发帖应用以及25种网盘、云盘等网络存储应用）的文件传输行为进行文件类型和文件内容过滤 |
| 要求所支持识别的文件类型不少于100种，文件类型识别基于文件特征而非扩展名，更改文件扩展名后仍可有效识别 |
| 要求能够对doc/docx/xls/xlsx/txt等不少于15类文件的内容进行关键字过滤 |
| 外发内容审计 | 可对至少10种电子邮件应用（WebMail）、25种论坛发帖应用（非HTTP-Post）进行外发内容审计 |
| 流量管理 | 支持精细化流量管理功能，可配置主通道、子通道、微通道3层嵌套的流量管理策略 |
| **攻击防护** | 网络攻击防护 | 可防护 ICMP Scan/TCP Scan/UDP Scan等扫描攻击，SYN Flood/ICMP Flood/UDP Flood/DNS Flood等拒绝服务攻击，以及TearDrop/LAND/WinNuke/Smurf/Fraggle/ Ping Of Death等异常数据包攻击。 |
| 会话连接控制 | 支持配置基于源地址、目的地址、协议、端口的并发会话数控制策略，要求上述元组可在一条规则中同时调用 |
| 支持限制每IP发起的每秒新建会话数及每秒数据包数（指数据包的数量，非并发连接数），可配置免受控白名单 |
| 病毒查杀 | 支持病毒云查杀，病毒查杀云支持私有云和公有云，用户可通过配置自行选择 |
| 能够对HTTP/FTP/POP3/SMTP/IMAP五种协议进行病毒查杀 |
| 入侵防御 | 入侵防御可检测漏洞利用和间谍软件攻击，能防止主流逃逸手段绕过。IPS特征库规模超过17000种，支持识别并拦截不少于7000种漏洞利用攻击和不少于10000种间谍软件活动 |
| 入侵防御系统有效检出率不低于95%  |
| 网址过滤 | 网址分类库规模大于3000万条 |
| 支持URL云服务，设备可与云服务器联动查找本地未识别的URL  |
| SSL 解密 | 可对HTTPS协议进行解密，支持配置基于源地址、目的地址的解密策略 |
| **VPN** | VPN协议 | 支持建立IPSec VPN/SSL VPN/GRE隧道及L2TP VPN。可实现L2TP over IPSec、GRE over IPSec |
| IPSec VPN | 支持星形拓扑组网，并提供中心端的简化配置模板，在中心端仅需配置一个VPN实例即可与多个对端实现同时互联 |
| IPSec VPN支持隧道冗余功能，可将一条VPN隧道指定为另一条隧道的备份隧道，当系统检测到主隧道中断后，自动启用备份隧道转发 |
| SSL VPN | 可提供Windows PC及Android、IOS智能终端适用的SSL VPN接入客户端，智能终端接入APP在应用商店可下载 |
| SSL VPN用户可与LDAP/Radius用户认证系统联动，并能够基于POP3和ESMTP协议与邮件系统进行认证联动 |
| 可基于接入终端的MAC地址、计算机名、硬件特征码等实现终端与SSL VPN登录用户名的绑定，并提供绑定关系批量导入功能 |
| 可基于应用的URL、IP、端口发布接入用户的访问资源池，成功接入的用户可通过资源页面访问应用 |
| 可提供用户自助开户，未开户用户可在线提交用户名、初始口令等相关信息，后台管理员审核批准后账户即可自动开通生效 |
| 支持B/S应用的单点登录配置 |
| 可对已接入的SSL VPN用户执行时长控制，接入超过时长的用户自动下线，时长控制方式需包括客户端空闲时常、在线时长 |
| 可设置SSL VPN用户准入时间控制， 准入时间段以外的时间禁止远程用户接入，准入时间段可基于每日、每周、每月定义 |
| **安全管理** | 网络异常感知 | 可汇总统计全网流量，可进行动态的风险评估并提供全网风险系数值 |
| 能够基于连接数和流量值对风险系数较高的流量进行单独的排名统计 |
| 可分别对单位时间内连接数、流量值激增或骤减幅度最大的应用进行排名统计，并提供连接数、流量的变化百分比，  |
| 安全事件分析 | 所投设备需提供关联分析面板，可将Top应用、Top威胁、Top URL分类、Top源地址、Top目的地址等信息关联，并支持以任意元素为过滤条件进行数据钻取 |
| 可提供关联的威胁事件日志，系统可自动将产生威胁事件的连接经过防病毒、防漏洞、防间谍软件、URL过滤、文件过滤等安全模块检查的日志集中显示 |
| 安全策略管理 | 可在单条策略中启用病毒防护、入侵防御、网址过滤、文件过滤、文件内容过滤等安全功能选项 |
| 可单独评估每条策略的风险系数，提供各策略所允许的高风险应用流量处理建议 ，并支持一键阻断高风险应用 |
| 配置备份恢复 | 支持系统配置的备份和恢复，并可单独导入地址转换（NAT）配置和策略配置 |
| 管理权限设置 | 管理方式支持三权分立管理 ，支持定义具有全部权限的管理员，仅具有策略变更权限的管理员和仅具有日志审计权限的管理员 |
| 设备管理方式 | 支持加密的WebUI和CLI管理，且支持网页命令行管理（WebUI中内嵌CLI管理界面） |
| 集中管理 | 可提供集中管理平台，可基于管理平台对设备批量下发安全策略 |
| 行为审计系统联动 | 可与上网行为管理（或网络行为审计）设备联动，在免认证的情况下同步上网行为管理（网络行为审计）设备中的用户认证信息 |
| **厂商及产品资质** | 产品资质 | 所投产品具备《计算机软件著作权登记证书》  |
| 所投产品具备公安部网络安全保卫局颁发的《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测评中心颁发的《信息技术产品安全测评证书》（EAL3+级） |
| 具备《中国国家信息安全产品认证证书》 |
| 产品生产厂商是具备CVE Compatible兼容性认证 |
| 产品生产厂商是国家信息安全漏洞共享平台（CNVD）用户组成员 |

# 服务

提供原厂五年免费服务，包括软件升级，硬件质保，现场技术支持服务，永久电话支持服务。