中国医学科学院肿瘤医院

入侵检测

技术需求

**信息中心/计算机室**

**2017年9月**

目录

[中国医学科学院肿瘤医院 0](#_Toc494183736)

[入侵检测 0](#_Toc494183737)

[技术需求 0](#_Toc494183738)

[一、 项目概述 2](#_Toc494183739)

[二、 技术要求 2](#_Toc494183740)

[2.1清单 2](#_Toc494183741)

[2.2技术参数表格 2](#_Toc494183742)

[三、 服务 3](#_Toc494183743)

[四、 资质 3](#_Toc494183744)

# 项目概述

目前我院网络规模较大，接入终端数量众多。以往只能被动的接收入侵、病毒感染等问题，然后采取应对措施。对问题的处理也不能做到“对症下药”。

通过在内、外网核心旁路接入方式部署入侵检测系统，进行实时入侵检测和分析，能够有效地检测出病毒、木马行为，以及非法入侵系统的恶意行为。并提供准确的修补漏洞、查杀病毒方法。逐步净化网络环境，封堵相关漏洞。

# 技术要求

### 2.1清单

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **项目** | **配置描述** | **数量** |
| 1 | 入侵检测系统 | 吞吐量≥10000Mbps，并发TCP会话数≥1000万，实配病毒检测、木马检测、DDOS检测、恶意上网行为检测、各种攻击行为检测。 | 1套 |

### 2.2技术参数表格

|  |  |  |
| --- | --- | --- |
| **指标项** | **指标子项** | **技术要求** |
| 系统架构 | 系统架构 | 产品应采用2U专用机架式硬件设备，1+1冗余电源，系统硬件为全内置封闭式结构 |
| 硬件架构 | 基本网络接口 | 千兆电口\*6,2对千兆电口Bypass ,万兆光口\*2 |
| ★性能要求 | ★吞吐能力 | 吞吐量≥10000Mbps |
| ★并发TCP会话数 | ≥1000万 |
| **部署能力** | **部署模式** | **★**透明部署（基于透明网桥），需即插即用，无需做任何配置即可防护。支持旁路部署。 |
| **★**策略路由（支持流量牵引） |
| **检测引擎** | 高性能攻击特征检测引擎 |
| **防护规则** | 系统提供完善的内置规则 |
| 提供高度灵活的自定义规则向导，适用于高级用户 |
| **安全特性** | **★规则数量** | **≥24000条** |
| **基本攻击拦截能力** | 支持拦截对操作系统、数据库、邮件服务、FTP的攻击 |
| **★病毒过滤** | 支持过滤病毒、木马、恶意软件通讯行为,**病毒库≥8000条。** |
| **★DDOS检测** | TCP/UDP Flood防护，基于最大上限阀值设置，而非DDOS特征库 |
| **上网行为** | 识别应用库不少于500种，并能够对其进行访问控制 |
| 支持恶意域名防护策略,能够对色情/赌博/钓鱼/黑客/欺诈/违规类别进行域名区分，并提供访问控制 |
| **基本访问控制** | 基于规则、来源/目的IP的、来源/目的端口、时间ACL |
| **NAT** | 支持源NAT、目的NAT、静态地址NAT |
| **规则冲突检测** | 支持对已有的访问控制规则进行冲突检测，发现重复的访问控制策略，帮助用户优化访问控制策略，去除冗余条目。 |
| **网络自适应能力** | **★802.1Q支持** | 支持VLAN解码，在Trunk线路上部署并提供防护 |
| **端口汇聚（Trunk）** | 支持端口汇聚（Trunk），显著提高设备间的吞吐能力 |
| **路由配置** | 支持静态路由的配置 |
| **报表功能** | **报表类型** | 安全报表（入侵统计、按入侵类别统计、被攻击主机、攻击来源IP和地理位置、网络接口流量趋势） |
| **报表查询** | 按事件类型、统计目标或周期类型条件进行统计 |
| **输出格式** | 支持将生成的报表以HTML、Word等通用格式输出 |
| **日志系统** | **日志类型** | 系统日志、审计日志和安全防护日志（入侵记录、攻击源IP所处地理位置、网络流量） |
| **日志查询** | 可基于时间、IP、端口、协议、动作、规则、规则类别、危害等级、等条件进行日志查询。 |
| **日志管理** | 日志导出、清空、自动磁盘日志清理 |
| **系统监控** | **监控类型** | 安全事件监控、访问情况监控、设备负载监控 |
| **系统信息** | 显示网络接口状态，引擎状态、系统CPU、内存及磁盘使用率 |
| **系统诊断和调试功能** | **维护工具** | 抓包工具，可抓取的网络原始报文，用于分析网络状况 |
| **配置备份与导入** | 支持系统配置的备份与导入功能 |
| **高可用性** | **HA双机** | 支持主从部署模式 |
| 支持链路是否正常的监控 |
| 支持双机配置自动同步 |
| **硬件BYPASS** | 内置bypass模块，设备故障直接切换到bypass模式 |

# 服务

三年原厂保修和所有功能模块免费升级服务，7\*24小时电话支持服务。

# 资质

* **★**《计算机信息系统安全专用产品销售许可证》。
* 设备生产厂商应具有漏洞发现能力，具备《中国国家信息安全漏洞库（CNNVD）技术支撑单位资质》
* 设备生产厂商应为CNVD技术组成员单位。