中国医学科学院肿瘤医院

集成平台防火墙

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](#_Toc494093065)

[集成平台防火墙 0](#_Toc494093066)

[技术需求 0](#_Toc494093067)

[一、 项目概述 2](#_Toc494093068)

[二、 技术要求 2](#_Toc494093069)

[2.1设备清单 2](#_Toc494093070)

[2.2详细要求 2](#_Toc494093071)

[2.2.1数据交换区防火墙 2](#_Toc494093072)

[2.2.2集成平台区域防火墙 4](#_Toc494093073)

[三、 服务 6](#_Toc494093074)

[四、 资质 6](#_Toc494093075)

# 项目概述

数据上报平台（集成平台）的建设是依据国家相关政策要求，根据医院业务系统的实际需要，基于现代信息系统安全保障理论，采用现代信息安全保护技术，按照一定规则和体系化的信息安全防护策略进行整体设计。目标是建立一套符合国家和国际标准的、能够保障整个平台安全的保障体系，包括技术、管理和运行等内容

为了满足集成平台项目的安全设计要求，需要购置防火墙，为数据交换区与集成平台服务器区提供全面的网络防护功能。

# 技术要求

## 2.1设备清单

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **项目** | **配置描述** | **数量** |
| 1 | 数据交换区防火墙 | 吞吐量5Gbps，最大每秒新建连接数50,000，最大并发连接数2,000,000，标配6个千兆电口；1U标准机架式设备。 | 1台 |
| 2 | 集成平台区域防火墙 | 吞吐量14Gbps，最大每秒新建连接数150,000，最大并发连接数2,000,000，标配6个千兆电口，4个千兆光纤接口，2个万兆光纤接口；2U标准机架式设备，标配冗余电源。 | 2台 |

## 2.2详细要求

### 2.2.1数据交换区防火墙

|  |  |
| --- | --- |
| 技术指标 | 指标要求 |
| 性能要求 | 三层大包吞吐量≥5G，三层小包吞吐量≥1G，应用层吞吐量≥700M，并发连接数≥200万，新建连接数≥5万； |
| 硬件规格 | 标准1U机架式设备，标配6个千兆电口，内存≥4G，标配64G固态SSD盘； |
| 部署方式 | 支持路由，网桥，单臂，旁路，虚拟网线以及混合部署方式； |
| 路由支持 | 支持静态路由，ECMP等价路由；支持RIPv1/v2，OSPFv2/v3，BGP等动态路由协议；支持多播路由协议；支持路由异常告警功能；#支持多链路出站负载，支持基于源/目的IP、源/目的端口、协议、应用类型以及国家地域来进行选路的策略路由选路功能；  |
| 基础功能 | 访问控制规则支持基于源／目的IP，源端口，源／目的区域，用户（组），应用/服务类型，时间组的细化控制方式；访问控制规则支持失效规则识别，如规则内容存在冲突、规则生效时间过期、规则超长时间未有匹配等情况；#访问控制规则支持数据模拟匹配，输入源目的IP、端口、协议五元组信息，模拟策略匹配方式，给出最可能的匹配结果，方便排查故障，或环境部署前的调试；访问控制规则支持分组管理；支持根据国家/地区来进行地域访问控制；能够识别管控的应用类型超过1200种，应用识别规则总数超过3000条；支持IPv4／v6 NAT地址转换，支持源目的地址转换，目的地址转换和双向地址转换，支持针对源IP、目的IP和双向IP连接数控制；支持基于应用类型，网站类型，文件类型进行带宽分配和流量控制；支持IPSec VPN，SSL VPN，GRE，GRE over OSPF，GRE over IPSec等VPN接入方式； |
| 内容安全 | 内置病毒样本数量超过200万；支持针对SMTP、POP3、IMAP邮件协议的内容检测，如邮件附件病毒检测、邮件内容恶意链接检测，邮件账号撞库攻击检测等，支持根据邮件附件类型进行文件过滤；（需提供相关功能截图证明）  |
| DoS/DDoS攻击防护 | 支持Land、Smurf、Fraggle、WinNuke、Ping of Death、Tear Drop、IP Spoofing攻击防护，支持SYN Flood、IPv4和IPv6 ICMP Flood、UDP Flood、DNS Flood、ARP Flood攻击防护，支持IP地址扫描，端口扫描防护，支持ARP欺骗防护功能、支持IP协议异常报文检测和TCP协议异常报文检测； |
| 僵尸主机检测 | 设备具备独立的僵尸网络识别库，特征总数在40万条以上； ★支持对终端已被种植了远控木马或者病毒等恶意软件进行检测，并且能够对检测到的恶意软件行为进行深入的分析，展示和外部命令控制服务器的交互行为和其他可疑行为； #对于未知威胁具备同云端安全分析引擎进行联动的能力，上报可疑行为并在云端进行沙盒检测，并下发威胁行为分析报告；#支持通过云端的大数据分析平台，发现和展示整个僵尸网络的构成和分布，定位僵尸网络控制服务器的地址；  |
| 安全可视化 | 支持资产的自动发现以及资产脆弱性和服务器开放端口的自动识别； #支持对检测到的攻击行为按照IP地址的地理位置信息进行威胁信息动态展示，实时监测和展示最新的攻击威胁信息；#支持自动生成安全风险报表，报表内容体现被保护对象的整体安全等级，发现漏洞情况以及遭受到攻击的漏洞统计，具备有效攻击行为次数统计和攻击举证；  |
| 安全集中管理 | 支持安全设备的集中管理，包括配置统一下发，规则库统一更新，安全日志，流量日志实时上报等功能；支持接入统一的安全监测平台，通过安全监测平台可以实时看到每台安全设备的详细安全状态信息，包括安全评分级别、最近有效事件、有效事件趋势、用户安全统计、服务器安全统计和攻击来源统计； |
| 高可用性 | 双机支持A/S，A/A方式部署；支持配置同步，会话同步和用户状态同步；支持双机心跳线冗余；★支持与原设备SG-NGAF-1300实现双机热备 |
| 系统配置管理 | 支持以安全策略模板方式快速部署安全策略，安全策略模板支持默认模板和自定义模板等多种格式；支持管理员权限分级，支持安全管理员、审计员、系统管理员三种权限；支持内置规则库的手动/自动更新；支持邮件、短信和微信告警； |
| 产品资质 | 产品应具备计算机信息系统安全专用产品销售许可证；所投防火墙产品经过国际知名实验室NSS Labs测试，并获得recommended推荐级别；所投防火墙产品入围2016年Gartner企业级防火墙魔力象限； |

### 2.2.2集成平台区域防火墙

|  |  |
| --- | --- |
| 技术指标 | 指标要求 |
| 性能要求 | 三层大包吞吐量≥14G，三层小包吞吐量≥1.5G，应用层吞吐量≥2G，并发连接数≥200万，新建连接数≥15万； |
| 硬件规格 | 标准2U机架式设备，标配6个千兆电口，4个千兆光纤接口，2个万兆光纤接口，内存≥4G，标配1T硬盘，冗余电源； |
| 部署方式 | 支持路由，网桥，单臂，旁路，虚拟网线以及混合部署方式； |
| 路由支持 | 支持静态路由，ECMP等价路由；支持RIPv1/v2，OSPFv2/v3，BGP等动态路由协议；支持多播路由协议；支持路由异常告警功能；#支持多链路出站负载，支持基于源/目的IP、源/目的端口、协议、应用类型以及国家地域来进行选路的策略路由选路功能；（需提供相关功能截图证明） |
| 基础功能 | 访问控制规则支持基于源／目的IP，源端口，源／目的区域，用户（组），应用/服务类型，时间组的细化控制方式；访问控制规则支持失效规则识别，如规则内容存在冲突、规则生效时间过期、规则超长时间未有匹配等情况；#访问控制规则支持数据模拟匹配，输入源目的IP、端口、协议五元组信息，模拟策略匹配方式，给出最可能的匹配结果，方便排查故障，或环境部署前的调试；访问控制规则支持分组管理；★支持根据国家/地区来进行地域访问控制；能够识别管控的应用类型超过1200种，应用识别规则总数超过3000条；支持IPv4／v6 NAT地址转换，支持源目的地址转换，目的地址转换和双向地址转换，支持针对源IP、目的IP和双向IP连接数控制；支持基于应用类型，网站类型，文件类型进行带宽分配和流量控制；支持IPSec VPN，SSL VPN，GRE，GRE over OSPF，GRE over IPSec等VPN接入方式； |
| 内容安全 | 内置病毒样本数量超过200万；★支持针对SMTP、POP3、IMAP邮件协议的内容检测，如邮件附件病毒检测、邮件内容恶意链接检测，邮件账号撞库攻击检测等，支持根据邮件附件类型进行文件过滤；  |
| DoS/DDoS攻击防护 | 支持Land、Smurf、Fraggle、WinNuke、Ping of Death、Tear Drop、IP Spoofing攻击防护，支持SYN Flood、IPv4和IPv6 ICMP Flood、UDP Flood、DNS Flood、ARP Flood攻击防护，支持IP地址扫描，端口扫描防护，支持ARP欺骗防护功能、支持IP协议异常报文检测和TCP协议异常报文检测； |
| 僵尸主机检测 | 设备具备独立的僵尸网络识别库，特征总数在40万条以上； 支持对终端已被种植了远控木马或者病毒等恶意软件进行检测，并且能够对检测到的恶意软件行为进行深入的分析，展示和外部命令控制服务器的交互行为和其他可疑行为； #对于未知威胁具备同云端安全分析引擎进行联动的能力，上报可疑行为并在云端进行沙盒检测，并下发威胁行为分析报告； #支持通过云端的大数据分析平台，发现和展示整个僵尸网络的构成和分布，定位僵尸网络控制服务器的地址；  |
| Web应用安全防护 | 设备具备独立的WEB应用防护识别库，特征总数在3000条以上； 支持HTTP 1.0/1.1，HTTPS协议的安全威胁检测；#支持针对网站的漏洞扫描进行防护，能够拦截漏洞扫描设备或软件对网站漏洞的扫描探测；★支持Web漏洞扫描功能，可扫描检测网站是否存在SQL注入、XSS、跨站脚本、目录遍历、文件包含、命令执行等脚本漏洞； 支持对网站黑链进行检测；  |
| 安全可视化 | #支持资产的自动发现以及资产脆弱性和服务器开放端口的自动识别； #支持对检测到的攻击行为按照IP地址的地理位置信息进行威胁信息动态展示，实时监测和展示最新的攻击威胁信息； #支持自动生成安全风险报表，报表内容体现被保护对象的整体安全等级，发现漏洞情况以及遭受到攻击的漏洞统计，具备有效攻击行为次数统计和攻击举证；  |
| 安全集中管理 | 支持安全设备的集中管理，包括配置统一下发，规则库统一更新，安全日志，流量日志实时上报等功能；支持接入统一的安全监测平台，通过安全监测平台可以实时看到每台安全设备的详细安全状态信息，包括安全评分级别、最近有效事件、有效事件趋势、用户安全统计、服务器安全统计和攻击来源统计； |
| 高可用性 | 双机支持A/S，A/A方式部署；支持配置同步，会话同步和用户状态同步；支持双机心跳线冗余； |
| 产品资质 | 产品应具备计算机信息系统安全专用产品销售许可证；所投防火墙产品经过国际知名实验室NSS Labs测试，并获得recommended推荐级别；所投防火墙产品入围2016年Gartner企业级防火墙魔力象限； |

# 服务

防火墙开启3年Web 应用防护模块，3年防病毒模块，3年入侵防御模块。

所有设备提供三年软件升级和三年硬件质保服务。

# 资质

1. ★产品应具备计算机信息系统安全专用产品销售许可证

2、 网络安全应急服务支撑单位证书（国家级）；

3、 售后服务体系通过ISO9001认证；

4、 国家信息安全漏洞共享平台(CNVD)技术组成员。