**终端准入管理设备项目需求**

**一、基本介绍**

目前医院信息化建设程度很高，但网络与信息安全风险问题也随之而来。非授权人员极易实现网络的非法入侵和访问，而目前医院网络目前尚无安全可靠、有效的防护手段，无法有效规避由此引发的安全事件，网络中的设备、人员、管理、数据等资源都未得到充分的安全保障，使得终端设备系统迅速成为高风险应用领域，一旦出现黑客攻击、数据窃取等事件，将有可能造成治安管理失控、敏感信息泄漏等后果，严重危害社会稳定。

针对以上所述亟待解决的问题，从终端设备的前端接入、安全隔离、管理控制等方面综合考虑，急需医院网络前端接入安全防护的整体解决方案。

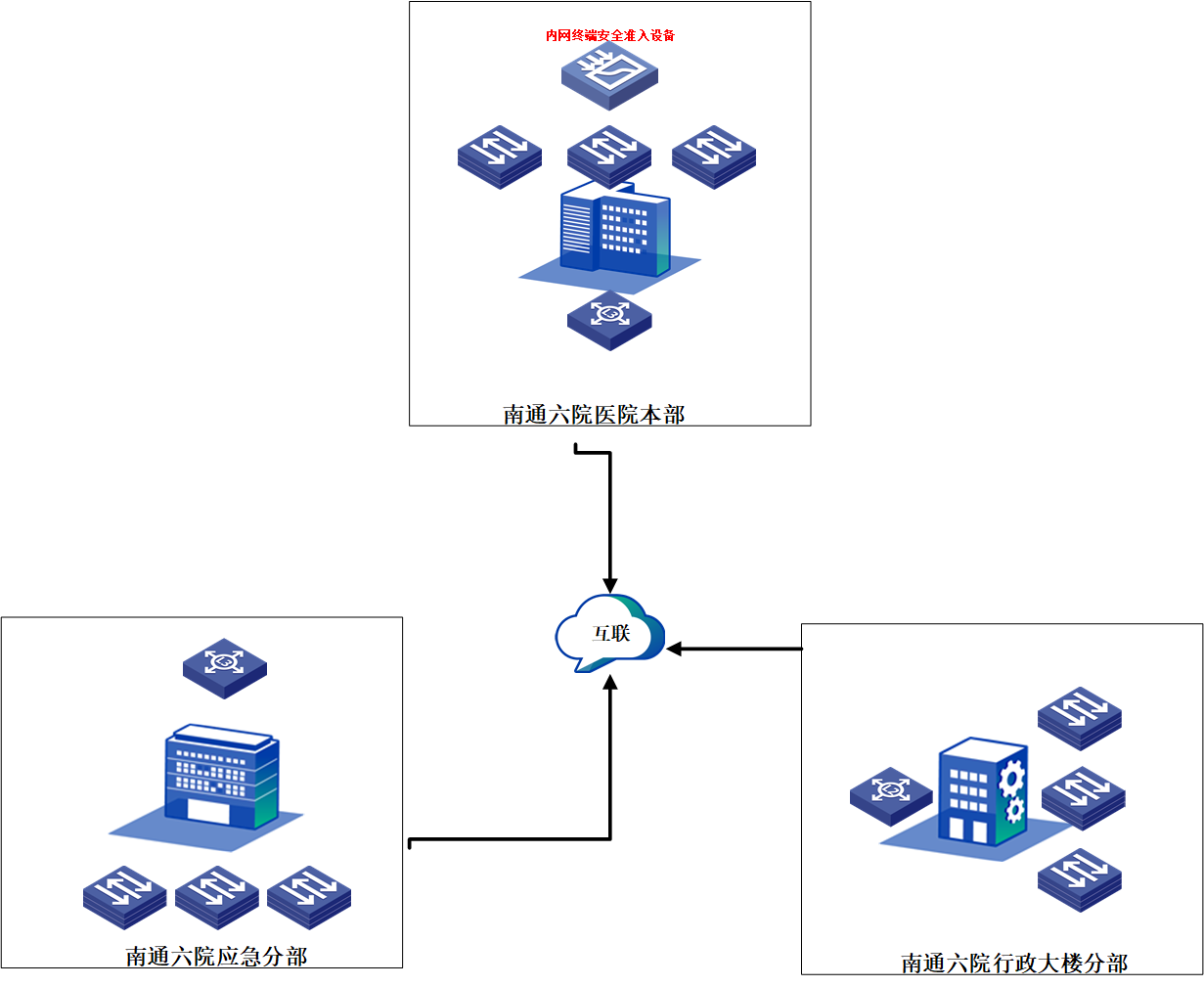
**二、项目需求**

总体实现：目前医院信息化办公网是的关键业务平台，业务种类越来越多，重要性越来越突出。“第三方”工程人员驻点开发、维护时可以直接进入数据中心核心资源区域，带来数据管理安全方面的风险。同时由于工作需要每天也将有数量不小的外来访客需要临时接入网络，这样不仅对医院内网数据安全构成威胁。因此医院内网计算机的系统安全以及日常的运行维护显的尤为重要，如果出现安全漏洞或安全事故，将会严重影响整体业务运行安全。

为加强网络安全管理及加强内网终端的安全管理，准备在医院内网建立内网准入管理机制，医院内网准入管理系统将重点解决以下问题：

* 用户入网身份证书认证化
* 入网终端登记注册认证化
* 网络边界设备管理（如HUB/NAT设备）
* 防止终端IP/MAC仿冒入网
* 禁用双网卡行为
* 移动存储设备授权使用
* 保障业务客户端的正常安装
* 入网终端必合规
* 提供终端远程维护功能，提升终端运维效率
* 动态网络拓扑，快速定位终端。
* 安全检查一目了然、智能傻瓜式修复
* 用户权限的细粒度分派及管理

……



安全感知平台以及探针均通过旁路部署，不对现有网络拓扑造成影响。

**三、功能模块**

**3.1实名强认证**

一一对应用户和终端,通过IP/MAC/硬盘ID等多种标识唯一绑定入网终端，防止有人通过仿冒合法终端IP/MAC信息而非法入网。

**3.2安全客户端安装率监测**

可通过与交换机即时联动工作，从网络层强制每一个入网终端必须符合医院内网要求的管理规范，没有安装指定客户端（比如：外联检测客户端、杀毒软件、系统补丁等）的终端计算机将拒绝其接入网络，从技术层面彻底杜绝私自卸载客户端或不装客户端情况的发生。并且客户端的安装也可以完全采用入网推送方式，而不需要每台终端手动下载安装。

**3.3终端漏洞智能修复**

提供“一键式”智能修复功能，通过傻瓜式的漏洞修复模式为员工提供简单、形象的安全自我修复功能，完全不需要管理员的介入即可完成终端安全风险项修补，最终将管理人员从日常重复、繁琐、低效的运维管理工作中解脱出来。

**3.4角色网络权限控制**

通过灵活的终端分级、分组、分域管理，同时根据不同组别的资产（或用户角色），采取不同的安全检查规范，同时向安全联动设备下发预设的接入控制策略，按照用户角色权限规范限定用户的网络使用行为和范围，形成全面、严密的区域访问布控。

**3.5 设备指纹（防IP/MAC仿冒）**

可对网内所有IP设备进行扫描和指纹特征的采集锚定，再进行IP设备与指纹唯一关联绑定。

**3.6网络设备私接滥用管理（HUB/NAT）**

具有NAT识别和检测机制，能够自动发现通过路由器进行多重NAT转换后所隐藏的真实计算机设备和IP地址，还能够对HUB的共享接入行为做实时检测、阻断管理。当多台计算机通过HUB接入网络时，可即时产生报警并通过切换Vlan、关闭端口等方式禁止HUB接入网络。

**3.7网络透视与管理**

能够对全网终端进行终端对应交换机端口的直观拓扑展示。在拓扑图上可以全面展示网络中的网络设备、安全设备、服务器系统、网络连接等信息。能够从整体上首先把握网络的运行和安全状况。在拓扑展示图上可以进一步向下细化定位，直至每台终端设备。也可以通过终端设备向上检索，找到其连接的交换机，及该交换机在网络中的位置、运行情况和安全状态等信息。

**3.8违规外联**

能够支持拨号、双网卡、代理等违规联网行为的即时检查，并能够对违规联网的终端实时断网并通知管理员。

**3.9 移动存储介质管理**

管理员可以通过对存储介质统一注册、授权的方式来加强管理存储介质的使用范围和权限，并支持存储介质分区加密，未经标识的存储介质将不能在医院内正常使用。

针对不同注册状态的存储介质制定不同的控制策略，能够对存储介质进行只读、禁用、放行、脱机生效以及时间范围等做精细控制。

**3.10 远程管理**

管理员可通过平台直接对网络中任一安装了准入客户端终端进行远程操作，包括远程操作远端终端的进程/服务/文件以及可直接对远端终端PC桌面进行控制。

**四、技术参数**

|  |  |
| --- | --- |
| 名称 | 技术参数 |
| 入网规范管理系统 | 功能要求：  1、 设备必须具备HA模式，具有虚拟策略路由地址管理模式；  2、 设备应至少提供安全客户端（Agent）、安全控件、无客户端等多种可供自定义的部署、管理模式；  3、 支持飞腾芯片、银河麒麟64位操作系统的终端安全检查，包括但不限于图形化认证、操作系统版本检查、网络监听端口检查、系统时间检查、P2P软件检查、进程黑白名单、软件黑白名单等；（提供加盖厂商公章的功能配置截图复印件，，并加盖供应商公章）  4、 能够实时监测并发现接入内网的PC、平板电脑、手机、IP设备等终端，能够在第一时间隔离阻断并通知管理员；  5、 对自动发现的终端能够按照类别自动归类，以方便网络终端的统计管理；  6、 准入设备支持基于多厂商Virtual Gateway的VLAN隔离技术，实现无客户端下端口级准入控制。  7、 设备支持基于策略路由技术的准入控制模式；  8、 设备具有完整的补丁管理子系统，无需第三方补丁服务器支持，自身即可以提供完整的流程化补丁管理，包括同步更新、补丁分类、补丁分发、补丁报表等功能；  9、 支持终端入网IE重定向引导，当用户访问网页时能够自动转向到指定的页面或地址，并支持http代理及多重重定向引导；（提供加盖厂商公章的功能配置截图复印件，，并加盖供应商公章）  10、 具有NAT识别和检测机制能够及时发现网内私接的小路由器、无线AP、随身WIFI等NAT设备，帮助清查通过网中网隐藏的真实网络终端。（提供加盖厂商公章的功能配置截图复印件，，并加盖供应商公章）  11、 IP/MAC绑定：能够支持终端IP、MAC地址以及交换机端口的绑定认证，提供入网设备自动学习功能，以及违规终端VLAN隔离机制；  12、 能够对网络打印机、网络摄像头等非智能IP设备做到精准的设备识别，通过伪造合法IP或MAC地址的非法设备和行为，能够被即时发现并阻断；（提供加盖厂商公章的功能配置截图复印件，并加盖供应商公章）  13、 支持多台计算机通过Hub接入网络时，设备后台能够产生Hub接入的报警记录。  14、 在终端无需安装客户端情况下，设备采用切换VLAN，逻辑关闭端口的方式禁止Hub下终端接入，Hub下存在多台终端时，合规的可以入网，不合规的禁止入网，不得采用全禁全放到模式；（提供加盖厂商公章的功能配置截图复印件，，并加盖供应商公章）  15、 支持当前主流智能终端设备的安全准入控制，能够自动识别主流手机、智能终端等设备，并自动进行分类；  16、 设备须提供系统安全配置、用户行为规范等类别检查项，至少提供30种以上标准的安全检查库（自定义除外）；  17、 能够在IE页面检查出终端的杀毒软件情况，内置主流的20种以上的杀毒软件检查库，支持杀毒软件版本、病毒库和运行情况的检查，能够在IE页面显示出检查结果；  18、 能够在IE页面进行入网终端的补丁检查，补丁均划分为严重、重要、中等的类别，能够在IE页面显示出检查结果；  19、 能够在IE页面检查出主流的桌面管理系统客户端是否安装并正常运行，能够在IE页面显示出检查结果；  20、 系统应支持重点业务准入监控功能，当业务准入出现异常时，通过syslog进行告警，并可以汇总到安全日志审计中心，形成统一的安全日志存储池。 |

**五、功能清单**

|  |  |  |
| --- | --- | --- |
| **序号** | **模块** | **功能简述** |
| **1** | 实名强认证 | 通过IP/MAC/硬盘ID等多种标识唯一绑定入网终端，一一对应用户和终端 |
| **2** | 安全客户端安装率检测 | 从网络层强制每一个入网终端必须符合医院内网要求的管理规范，没有安装指定客户端的终端计算机将拒绝其接入网络 |
| **3** | 终端漏洞智能修复 | 通过傻瓜式的漏洞修复模式为员工提供简单、形象的安全自我修复功能，完全不需要管理员的介入即可完成终端安全风险项修补 |
| **4** | 网络角色权限控制 | 按照用户角色权限规范限定用户的网络使用行为和范围，形成全面、严密的区域访问布控。 |
| **5** | 设备指纹 | 可对网内所有IP设备进行扫描和指纹特征的采集锚定，再进行IP设备与指纹唯一关联绑定。 |
| **6** | 网络设备私接滥用管理 | 能够自动发现通过路由器进行多重NAT转换后所隐藏的真实计算机设备和IP地址，还能够对HUB的共享接入行为做实时检测、阻断管理 |
| **7** | 网络透视与管理 | 能够对全网终端进行终端对应交换机端口的直观拓扑展示 |
| **8** | 违规外联 | 支持拨号、双网卡、代理等违规联网行为的即时检查，并能够对违规联网的终端实时断网并通知管理员。 |
| **9** | 移动存储介质管理 | 通过对存储介质统一注册、授权的方式来加强管理存储介质的使用范围和权限 |
| **10** | 远程管理 | 可通过平台直接对网络中任一安装了准入客户端终端进行远程操作 |

**六、项目预算**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **设备名称** | **单位（套）** | **单价**  **（万元）** | **总价**  **（万元）** |
| 1 | 入网规范管理系统 | 1 | 13 | 13 |
| 合计 | 壹拾叁万圆整 | | | 13 |