中国医学科学院肿瘤医院

集成平台上报VPN

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](#_Toc494094893)

[集成平台上报VPN 0](#_Toc494094894)

[技术需求 0](#_Toc494094895)

[一、 项目概述 2](#_Toc494094896)

[二、 技术要求 2](#_Toc494094897)

[2.1系统配置 2](#_Toc494094898)

[2.2详细要求 2](#_Toc494094899)

[SSL VPN 2](#_Toc494094900)

[三、 服务 4](#_Toc494094901)

[四、 资质 5](#_Toc494094902)

# 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。

由于数据上报采用的是互联网上报的方式，而非物理专线上报。所以需要VPN设备建立虚拟专用的加密网络，来保证上报数据的安全可靠性。

# 技术要求

## 2.1系统配置

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **项目** | **配置描述** | **数量** |
| 1 | SSL VPN | SSL加密吞吐量≥240Mbps，最大并发用户800，标配6个千兆电口，1U标准机架式设备。 | 1台 |

## 2.2详细要求

###  SSL VPN

|  |  |
| --- | --- |
| 技术指标 | 指标要求 |
| 性能要求 | SSL加密吞吐量≥240Mbps，最大并发用户800，标配6个千兆电口，1U标准机架式设备。 |
| 硬件规格 | 标准1U机架式设备，标配6个千兆电口，内存≥1G； |
| 部署方式 | ★支持网关模式、单臂模式部署两种方式；支持与VPN-2150-YL双机热备 |
| 基本特性 | 专业VPN设备，采用标准SSL、TLS 协议，同时支持IPSec VPN、SSLVPN两种VPN，非插卡或防火墙带VPN模块设备； |
| 支持对基于HTTP、HTTPS、FileShare、DNS、H.323、SMTP、POP3、Telnet、SSH等的所有B/S、C/S应用系统，支持基于TCP、UDP、ICMP等IP层以上的协议的应用，例如即时通讯、视频、语音、Ping等服务；；  |
| 支持PC终端使用包括Windows10、Windows8、Windows7、Windows Vista、Windows xp、Mac OS、Linux等主流操作系统来登录SSLVPN系统，并完整支持该操作系统下的各种IP层以上的B/S和C/S应用；支持Windows、IOS、Android、塞班、黑莓等操作系统的智能手机、PDA、平板电脑（PAD）等移动终端的SSL VPN接入，或通过PPTP、L2TP VPN方式接入； |
| ★支持终端使用包括IE6、7、8、10、11或其他IE内核的浏览器，以及最新版本的非IE内核浏览器，如Windows EDGE，Google Chrome，Firefox，Safari，Opera最新版登录SSLVPN系统，登录后可完整支持各种IP层以上的B/S和C/S应用；  |
| 产品应支持国际通用标准的商用密码密码算法（简称“商密”），包括：AES、DES、3DES、DH、RSA、RC4、MD5、SHA1等； |
| 易用性 | #可支持虚拟门户功能，在一台设备上配置不同的访问域名、IP地址，以及不同的使用界面，实现一台设备为多个不同用户群体服务的的使用效果；  |
| 支持断线重连自动技术，防止用户误操作关闭浏览器导致VPN隧道断开；防止用户在无线网络环境下网络正常切换时VPN隧道断开； |
| 支持智能递推技术，针对多外链的门户网站进行动态嗅探页面内的链接并完成资源自动授权，防止资源漏访；支持Web参数修正，可针对Flash、Java、Applet、或视频播放器对象所引用资源路径进行修正，避免无法播放的问题； |
| 终端安全 | ★产品必须支持防中间人攻击，产品可在用户登录SSLVPN时智能判断存在中间人攻击行为，断开被攻击的连接，并可提示异常现象；（可提供证明材料） |
| 支持客户端注销后自动清除所有缓存、Cookies、浏览器历史记录、保存的表单信息，实现零痕迹访问； |
| 支持VPN专线功能，可配置用户在接入SSL VPN的同时，断开与Internet其他连接；  |
| 权限、服务器安全 | 产品应具有用户/用户组细粒度的权限分配功能：可以针对被访问资源的IP地址、端口、提供的服务、URL地址等进行权限控制；针对同一B/S资源，可对不同用户做到细致到URL级别的授权；  |
| 产品应具有角色授权机制，支持在用户组的基础上，根据角色的不同，组合关联不同的资源权限； |
| ★支持主从认证账号绑定，必须实现SSL VPN账号与应用系统账号的唯一绑定，VPN资源中的系统只能以指定账号登陆，加强身份认证，防止登录SSL VPN后冒名登录应用系统；  |
| 身份认证 | 产品必须支持Local DB 、USB KEY、短信认证、硬件特征码、动态令牌、数字证书认证、LDAP、RADIUS、等认证方式；可针对用户/用户组设置认证方式的与、或组合，可进行用户名/密码、LDAP、USB KEY、硬件特征码、短信认证或动态令牌的五因素捆绑认证；  |
| 支持有驱USB KEY、无驱USB KEY认证，无驱KEY无需在客户端安装驱动，方便用户；  |
| 设备内部必须支持自建CA中心，便于数字证书认证平台搭建；★单台VPN设备可扩展同时支持5套以上CA根证书；  |
| 高速性 | ★必须支持至少4条以上的外网多线路配置；并在设备单臂部署模式下，多线路接入前置网关，仅依靠SSLVPN设备同样可实现SSLVPN接入用户的多线路自动优选功能；  |
| 支持非对称式部署的传输协议优化技术（单边加速），不用在用户终端上安装任何插件和软件，即可提升用户访问应用服务的速度；(提供配置界面截图及第三方评测报告) |
| 支持利用网页进行动态寻址的方法，客户端无需安装插件、不依靠IP地址库、不依赖于第三方动态IP寻址、直接根据速度探测实现用户端接入线路的自动优选,用户通过访问寻址代理页面（简称Webagent页面），通过Webagent页面自动寻找VPN设备IP(非DDNS),该方法不必单独注册域名或占用IP地址，大大降低了系统部署难度；  |
| 支持针对不同的web页面进行数据优化，支持动态压缩技术，基于数据流进行压缩，减少不必要的数据传输；  |
| ★针对B/S资源支持WebCache技术，动态缓存页面元素，提高Web页面响应速度。支持流缓存技术，实现网关与网关、网关与移动客户端之间进行多磁盘、双向、基于分片数据包的字节流缓存加速，削减冗余数据，降低带宽压力的同时提高访问速度；支持共享流缓存功能，实现多分支网关在总部共享流缓存数据，提高流缓存效果；（提供界面配置截图，并提供自主知识产权证明） |
| 稳定性、可扩展性 | 支持253台不同型号设备间进行集群（A/A），支持路由模式、单臂模式下多线路部署的集群；支持集群设备间Session同步，一台设备宕机后其上用户无需重新登录SSLVPN可继续使用；可扩展分布式集群功能，无需专门的全局负载设备即可实现异地SSLVPN设备间的接入用户负载分担、速度优选接入，异地设备间互为备份，分布式集群中用户可通过唯一的一个地址访问到所有加入到分布式集群的SSLVPN设备； |
| #在负载均衡集群部署模式下，支持授权漂移，即当集群中一台设备宕机，该宕机设备中的并发授权自动迁移到其他正常的设备中，而无需额外购买授权； |
| 产品必须支持经过集成的，基于Android IOS平台的第三方软件开发包（SDK），并实现基于Android IOS平台第三方应用软件（APP）代码量不超过20行。（要求提供代码Demo和企业证明）支持针对移动APP的VPN安全代码的自动封装，实现App应用的安全加固；  |
| 远程应用 | 可以无需二次开发，即把Windows应用发布到移动智能终端中，也可以支持无需开发，将C/S资源Web化； |
| 支持改写WindowsRDP协议，经改写的协议必须独立于OS运行环境，避免跨平台兼容性，针对图像数据，服务端必须支持有损压缩算法；服务端必须能够支持过滤动态内容（gif/flash/video）以减少传输流量，且根据客户需要配置；  |
| 产品资质 | 提供中华人民共和国公安部颁发的《计算机信息系统安全专用产品销售许可证》；提供产品IPV6 Ready认证证书，并在全球IPV6测试中心官网可查；提供公安部信息安全产品检测中心颁发的《GA/T 686-2007信息安全技术 虚拟专用网安全技术要求》三级或三级以上检测报告；提供SSL VPN必须在近三年内至少曾有一年在中国国内SSL VPN或VPN硬件市场占有率为前三名，提供权威的第三方机构数据证明。 |

# 服务

SSL VPN 配置100个 SSL 并发授权；

所有设备提供三年软件升级和三年硬件质保服务。

# 资质

1. **★**《计算机信息系统安全专用产品销售许可证》；

2、 售后服务体系通过ISO9001认证。