安全体系结构 Project 2

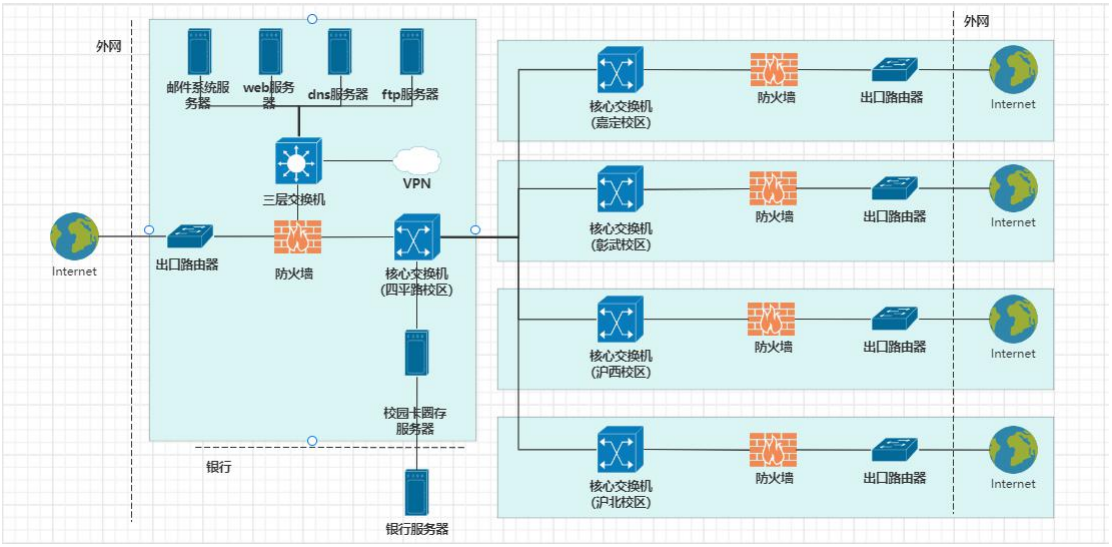
2053182 王润霖

实验内容：

针对同济大学校园网，分别从（a）学校总的视图，（b）嘉定校区管委会视图，画出“三保卫一支撑”四个区域的草图，并列表标出各区域的主要信息资产。

一、同济大学视图

1.绘制网络拓扑结构



2.划分区域边界

（1）物理区域边界

按照校区的物理位置，同济大学校园网可以划分为四平路校区、彰武校区、嘉定校区、沪西校区、沪北校区四个区域。从物理位置角度，各个校区之间的边界为物理区域边界，在边界需要部署核心交换机等信息交换设备。

在区域边界，需要进行安全管控，要求针对所有级别的系统，对于互联网边界侧的安全防护设备，如果无任何安全控制措施或配置错误的策略(例如允许所有流量交互)、无法及时管理访问控制设备并且根据安全需求及时更新策略，可判定为高风险。这是因为互联网充满了安全威胁与不确定性，出口侧缺少防御措施，将导致内部网络直接系统暴露在互联网中，极易成为被攻击的目标。可以采用采用具有访问控制的产品或技术(ACL 控制)，可使用交换机、路由器等产品实现。

此外，还可以进行安全审计等措施。例如：针对所有系统，缺乏对重要用户或重要安全事件的记录与审计，可判定为高风险。在网络边界、重要节点采用网络、日志等审计措施，实现对事件的记录、分析，便于溯源。

（2）划分网络边界

对于同济大学校园网，其边界包括与外网 Internet 的边界，以及对于校园卡充值系统，

其与银行网络的边界。

此外，对于同济大学校园网提供的 VPN 服务，可以实现从外界访问内部网络。

（3）划分业务安全区域

根据边界区域中的不同业务，可以划分为电子邮件系统、网站服务系统、校园银行系统和综合服务系统。

（4）列表标出各区域的主要信息资产

区域	内容	主要信息资产
电子邮件系统	同济大学电子邮件服务	邮件服务器、邮件软硬件支撑环境、邮件数据
网站服务系统	学校网站的访问服务	网站服务器及其软硬件支撑环境、网站的访问数据
校园银行系统	同济大学校园金融服务	金融服务器、金融支撑环境及其数据信息
综合服务系统	校园综合信息服务	学校综合信息数据

3.计算环境

对于同济大学校园网，计算环境提供了校园内可能涉及的业务支持。例如最主要的：综合门户系统、教务系统、财务系统、科研系统，以及学生管理系统、教师管理系统、图书管理系统、实验室管理系统、招生系统、校园卡系统、宿舍管理系统、体育活动系统。各个系统的信息资源，即为主要的信息资产。

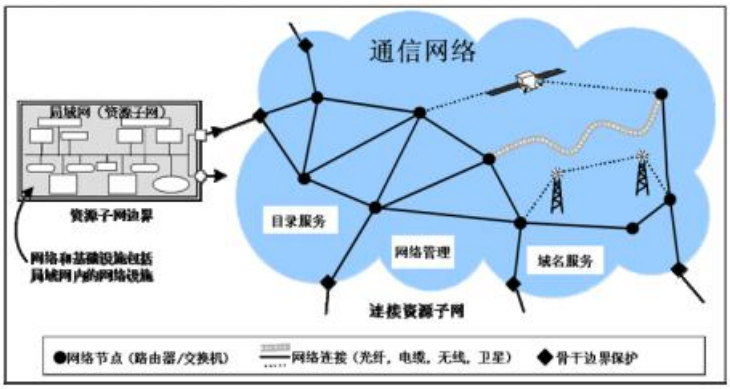
列表标出各区域的主要信息资产：

计算环境	内容	主要信息资产
综合门户系统	校园综合服务计算环境	综合服务信息资源、数据库的数据
教务系统	教学管理计算环境	教务教学资源、数据
财务系统	财务金融相关计算环境	财务金融业务资源、数据
科研系统	学校科学研究工作计算环境	科研资源、数据
学生管理系统	学生管理相关	学生信息数据
教师管理系统	教师管理相关	教师信息数据
图书管理系统	图书管理相关	图书信息数据
实验室管理系统	实验室管理相关	实验室信息数据
招生系统	招生工作计算环境	招生相关资源、数据
校园卡系统	校园卡充值等服务计算环境	校园卡服务资源、数据
宿舍管理系统	宿舍管理相关	宿舍信息数据
体育活动系统	体育活动相关计算环境	体育活动相关资源、数据

4.网络基础设施

从同济大学校园网的角度，网络基础设施包括外部路由器、三层交换机、防火墙、网关、域名、相关的协议。

网络基础设施为各种信息系统和业务系统提供了一个传输用户数据流和用户信息的机制。在网络和基础设施，保护，包括信息服务维修，以防止拒绝服务攻击（DOS），以保护网络中的核心数据传输的保密性及数据流分析的保护。对网络基础设施上所传递信息的保护需要通过在企业外网接入端使用安全路由器，利用 VPN 技术实施保护。



5.支撑基础设施

基本支持服务域包含密钥管理基础设施（KMI）/公共密钥基础设施（PKI）的检测和响应的基础设施，为每一个环节的网络环境提供加密服务预警，对可能的网络攻击检测，并提出了有效的响应识别。

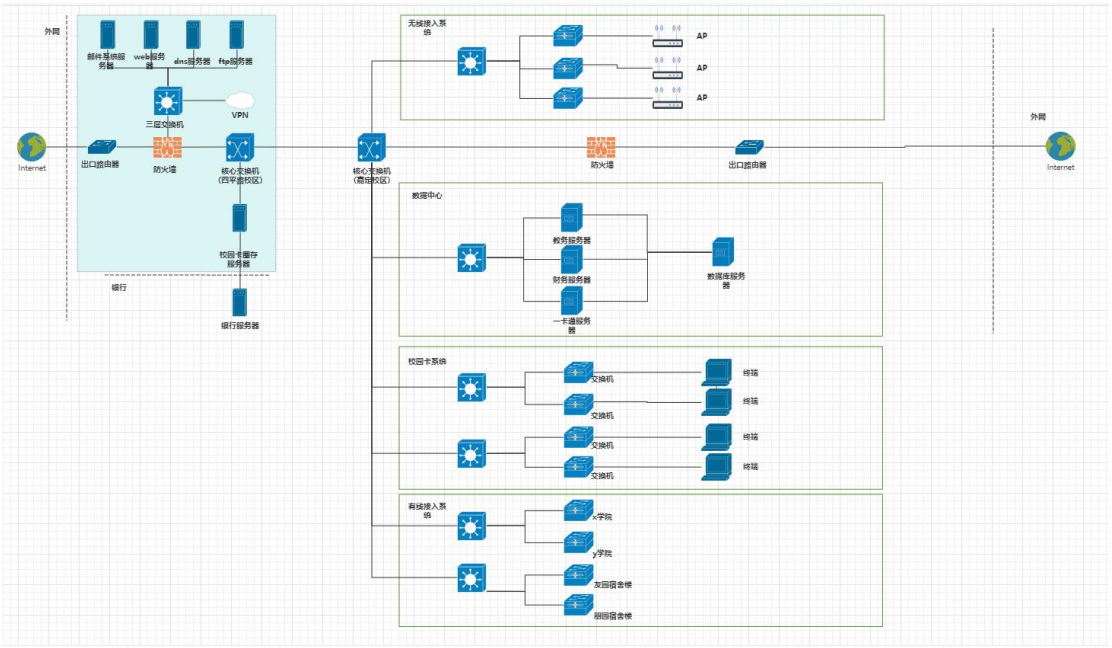
对于同济大学校园网的支撑基础设施，包括统一身份认证、接入认证、公共密钥基础设施（PKI）、系统综合管理（SOC）、安全态势感知。

列表标出各区域的主要信息资产：

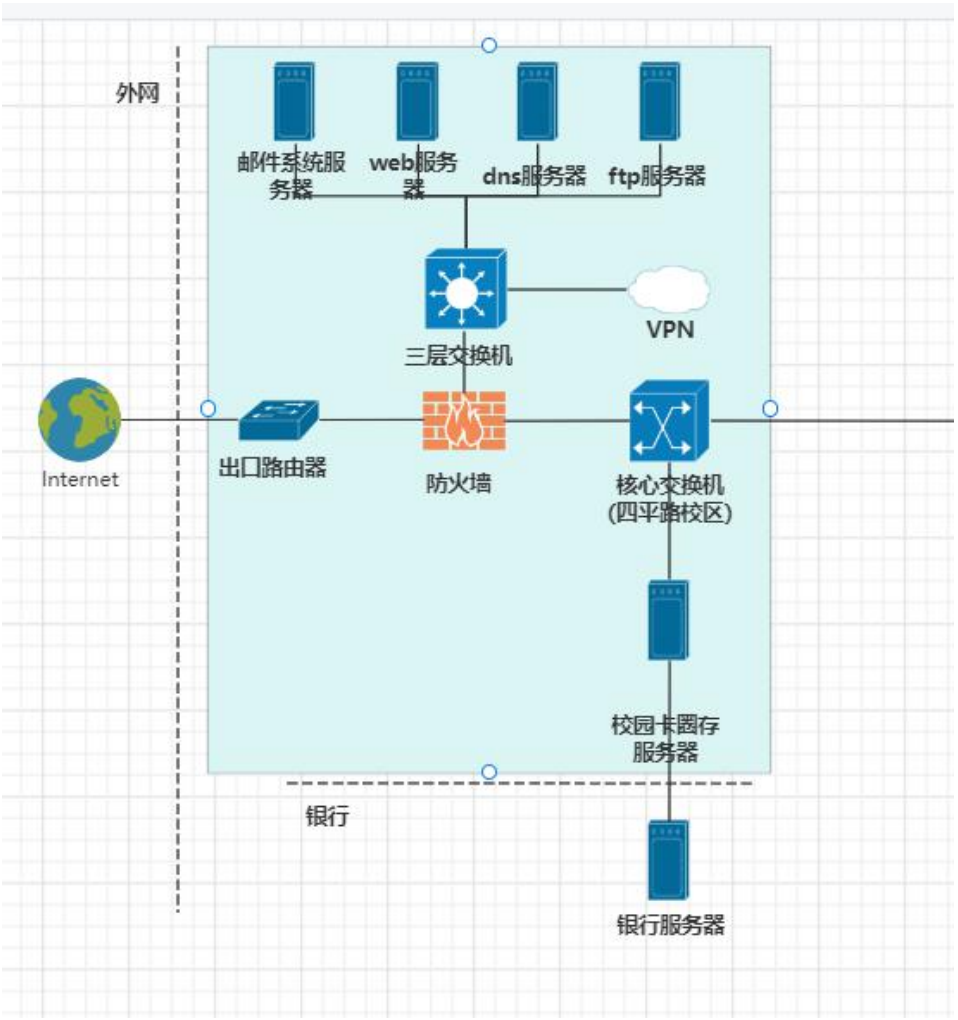
支撑基础设施相关业务	内容	主要信息资产
统一身份认证	在用户访问同济大学校园网时进行统一身份认证	身份认证服务器，数据库及其软硬件环境，身份认证信息
接入认证	在用户从外部网络接入同济大学校园网内网时进行身份认证	身份认证服务器，数据库及其软硬件环境，身份认证信息
公共密钥基础设施	身份验证，加强通信安全	公共密钥、身份认证信息、数字证书、签名等
系统综合管理	管理控制系统内部的资源	综合管理服务器、软硬件环境、数据库、管理信息
安全态势感知	感知同济大学校园网络安全，进行安全预警和响应	安全监控设备、访问控制软硬件环境、入侵检测信息

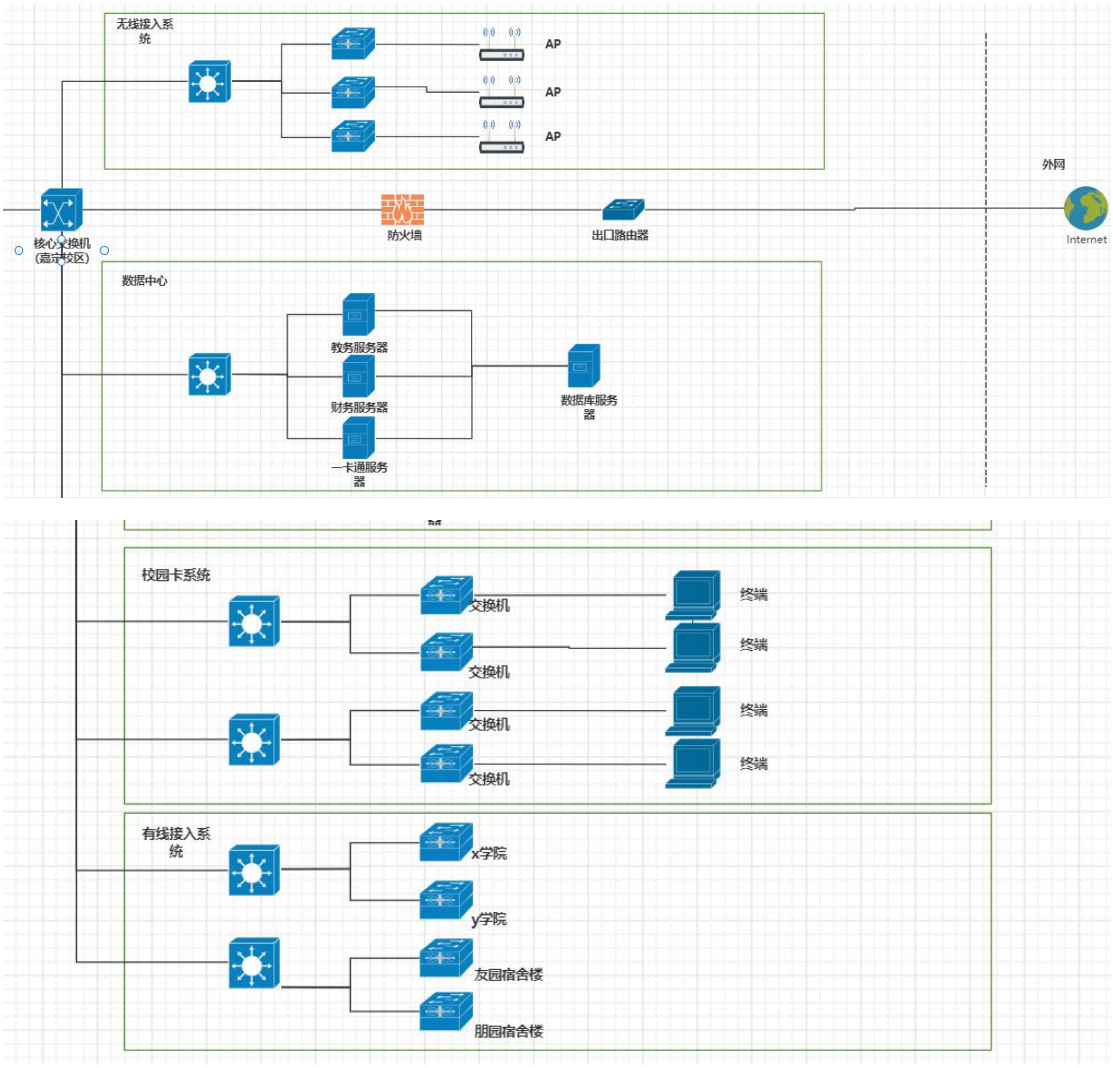
二、嘉定校区管委会视图

1.绘制网络拓扑结构



其中细节展示如下：





2.划分区域边界

（1）物理区域边界

从嘉定校区管委办的角度，划分区域边界，在物理层面，可以划分为不同楼宇的边界、图书馆、学院楼的物理区域边界。

（2）网络区域边界

网络区域边界包括嘉定校区校园网与外网 Internet 的边界、与四平路校区的边界。

（3）划分主要信息资产

区域边界	内容	主要信息资产
嘉定校区与四平路校区	隧道技术、广域网等	软硬件设备、服务器等
嘉定校区与外网 Internet	防火墙、出口路由器	连接网络的软硬件设备、服务器等

3.计算环境

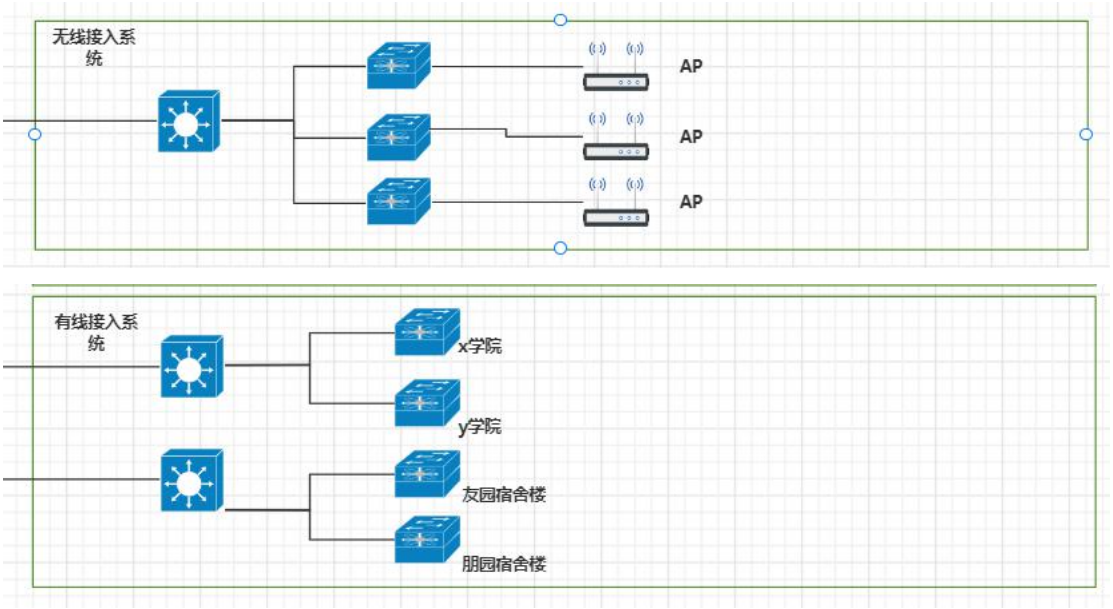
对于嘉定校区管委办的角度，应该有各个学院和实验室的业务计算环境，也就是嘉定校区本地的计算环境。其中，数据中心包含统一身份认证和访问控制、安全存储以及安全审计。

列表标出各区域的主要信息资产：

计算环境	内容	主要信息资产
各学院管理系统	学院相关的计算环境	学院信息资源、数据库的数据、软硬件平台
各实验室管理系统	实验室相关计算环境	实验室信息资源、数据库的数据、软硬件平台

4.网络基础设施

对于嘉定校区管委办视角下的网络基础设施，可能包括无线接入网络、有线接入网络等，来对嘉定校区内部的网络结构进行管理。如图所示。



5.支撑性基础设施

对于嘉定校区管委办的角度，支撑性基础设施应当从嘉定校区内部进行分析，也应当包括统一身份认证、接入认证、公共密钥基础设施（PKI）、系统综合管理（SOC）、安全态势感知。

划分主要信息资产如下表所示：

支撑基础设施相关业务	内容	主要信息资产
统一身份认证	在用户访问嘉定校区各个学院网络或实验室网络时进行统一身份认证	身份认证服务器，数据库及其软硬件环境，身份认证信息
接入认证	在用户从外部网络接入嘉定校区校园网内网时进行身份认证	身份认证服务器，数据库及其软硬件环境，身份认证信息
公共密钥基础设施	身份验证，加强通信安全	公共密钥、身份认证信息、数字证书、签名等

系统综合管理	管理控制系统内部的资源	综合管理服务器、软硬件环境、数据库、管理信息
安全态势感知	感知嘉定校区校园网络安全，进行安全预警和响应	安全监控设备、访问控制软硬件环境、入侵检测信息
域控制	控制区域访问权限	访问控制设备