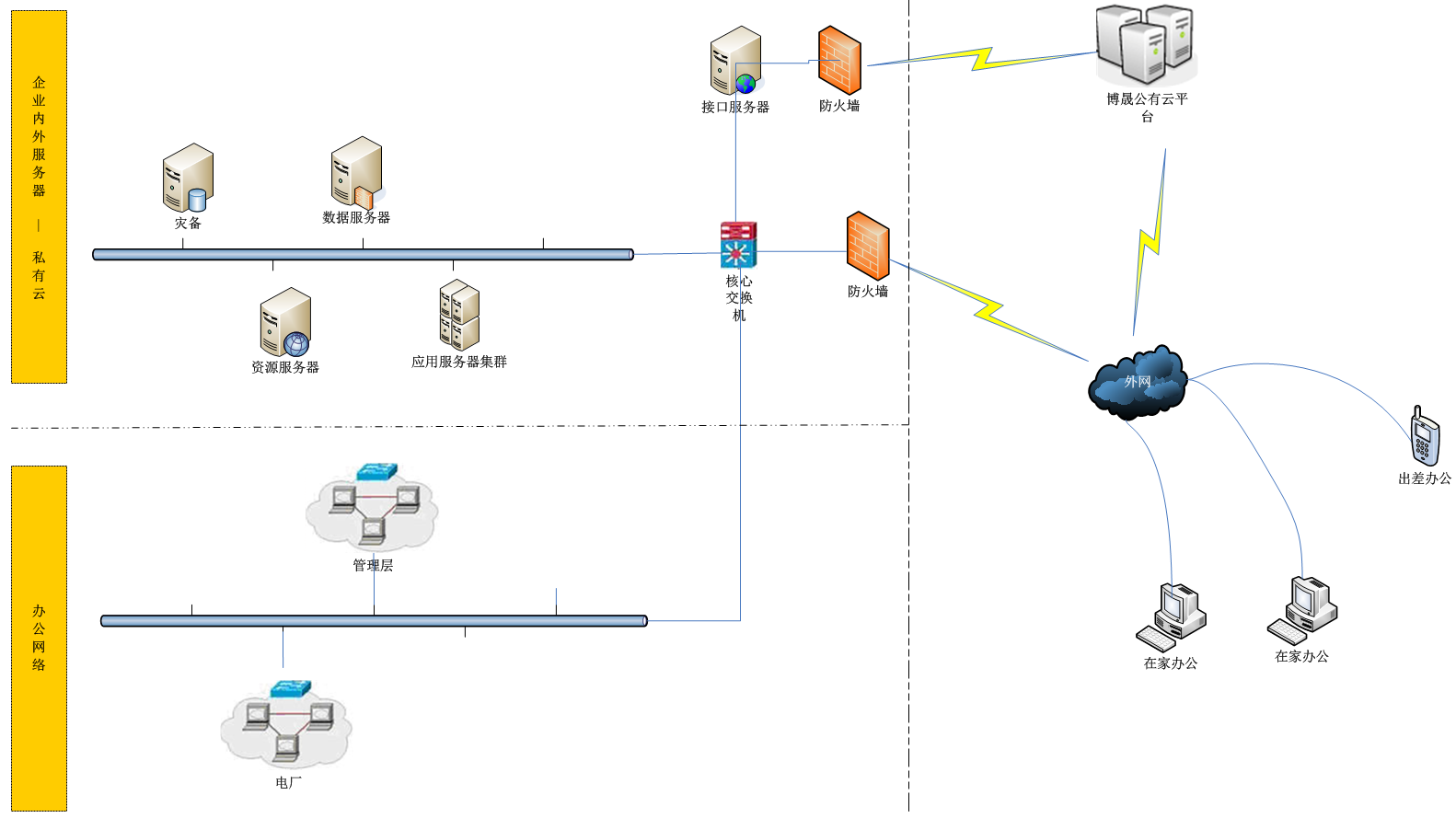
# 数据同步现有方案

## 现实需求

* 企业内网部署云平台，企业员工在企业内网云平台上进行培训学习；
* 企业内网不能访问外网；
* 员工可以在家访问博晟云平台进行培训学习；
* 外网不能获取企业内部业务数据，用户数据等；

## 解决方案



混合云平台主要由两部分构成

第一部分：部署在企业内网中提供生产培训学习服务的私有云。

第二部分：部署在博晟IDC机房中公有云平台，提供在线学习服务，并将外网（在家或外地出差等）学习过程通过公有云平台和接口服务器同步到企业私有云，从而保证企业信息安全，接口服务器同时连接内外网。

数据库同步采我们自行开发的程序，博晟云平台安装服务端，客户内网应用端安装客户端。客户端向服务端提出请求，由服务端从公司数据库提取数据传输给客户端。

数据同步服务是云平台中公共服务，具备通用型，可配置等特点，要求如下：

1、针对主流数据库实现同步：mysql,oracle,mssql等。

2、双向同步。

3、可以通过域名同步。

4、可配置同步间隔时间。

5、网络断网后恢复时，可重新运行同步程序进行重新同步。

## 数据库同步示意图



## 文件同步示意图



## 云计算平台安全防护目标

为确保云平台信息的机密性、完整性、可用性、可控性与可审查性，本项目通过部署安全系统，投入技术力量，加强网络安全管理，达到如下目标：

* 合理管理和分配网络资源，防止滥用网络资源导致网络瘫痪；
* 抵御病毒、恶意代码等对信息系统发起的恶意破坏和攻击，保障网络系统硬件、软件稳定运行；
* 保护重要数据的存储与传输安全，防止和防范数据被篡改，建立数据备份机制和提高容灾能力；
* 加强对重要敏感数据信息的保护，确保数据的机密性；
* 构建统一的安全管理与监控机制，统一配置、调控整个网络 多层面、分布式的安全问题，提高安全预警能力，加强安全应急事件 的处理能力，实现网络与信息安全的可控性；
* 建立认证体系保障网络行为的真实可信以及可审查性，并建 立基于角色的访问控制机制。

## 系统安全防护方案

在云计算平台的建设上，云安全成为了众人关注的焦点，也是企业部署云技术时候最关心的问题。要解决安全问题，应该先正确的认识其安全威胁。

1）传统的安全边界消失

基于边界的安全隔离与访问控制是传统安全防护的重要原则，很大程度上依赖于各区域之间明显清晰的区域边界，强调的是针对不同 的安全区域设置有差异化的安全防护策略；在云计算环境下，基础网络架构统一化，存储和计算资源高度整合，传统的安全设备部署边界正逐步消失，云计算环境下的安全部署需寻找新的模式。

2）虚拟化服务的安全问题

“计算机科学中的任何问题都可以通过增加一层映射而解决”，按照这种思路，当前计算机系统的许多问题可以通过计算机系统的虚拟化而解决。同时，虚拟化作为云计算平台的关键技术，基于存储资源和服务器资源的高度整合，其自身的可扩展性能够极大地拓展基础设施和软件平台层面提供云服务的能力。在这种情况下，如何应对云计算平台基础网络架构、数据存储和应用服务的虚拟化交付，对安全设备的设计构建和安装部署提出了更高的技术要求，也成为云计算环境下信息安全建设所关注的重点。

3）数据集中后的安全问题

一是传统的网络中各种应用服务的标准流量和突发流量有迹可循，流量模型设计相对较为规范、简单，对安全设备的处理能力没有太高的要求。而在云计算环境下，同类型存储或者应用服务器的规模增长迅猛，动辄以万为单位进行扩展，并且不能分而治之，必须依托统一架构的基础网络来承载。与传统网络环境相比，这就对安全设备本身的性能指标提出了更高的要求。二是用户的数据存储、处理、网络传输等都与云计算系统有关。如何避免多用户共存带来的潜在风险；如何保证云服务的身份鉴别、认证管理和访问控制等安全机制符合用户的需求，并能够实施有效的安全审计，这些都成为云计算环境所面临的安全挑战。

4）稳定性和可靠性问题

一是云计算环境下，用户的数据和业务应用流程等均依赖于云计算所提供的虚拟化服务，这必然对云计算服务的稳定性、安全策略部署、容灾恢复能力和事件处理审计等提出了更高更进一步的需求。二是用户、信息资源的高度集中，相对传统的网络平台更加容易成为网络攻击的目标，因各类恶意代码、黑客程序、病毒木马等工具造成的破坏程度将会呈指数级上升。

5）私有云确保企业信息安全

1. 私有云平台采取办公网络与外部网络物理隔离的方式，从而避免外部病毒入侵的可能。同时通过接口服务器进行资源课程同步，从而保证课件信息更新及时，方便安全培训内容及时。