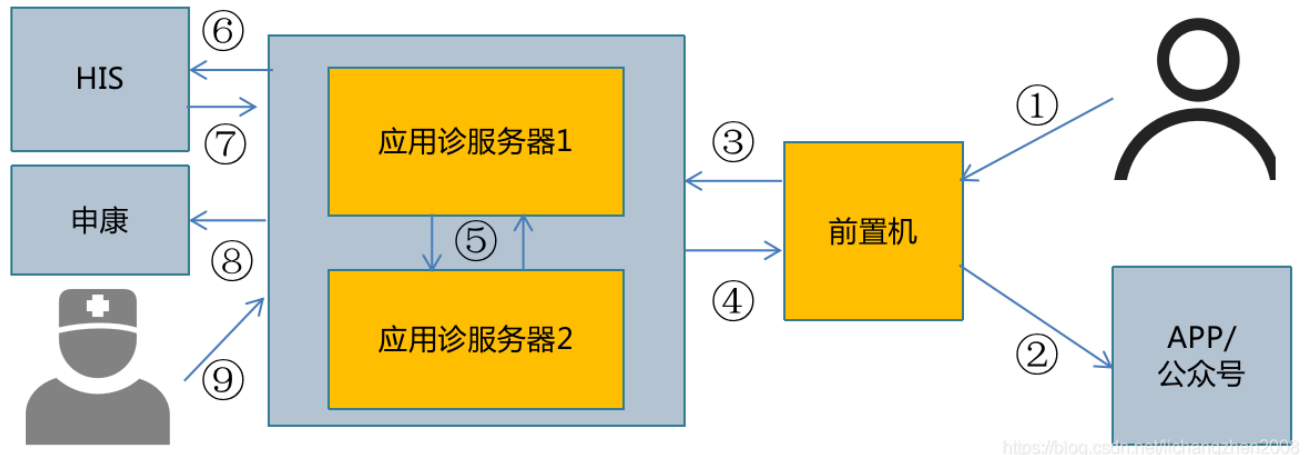




网络开通策略小案例

场景

这是我项目实施中一个经典的网络开通策略场景，作为一个系统（下面称为系统A），需要调用的服务比较多，需要的服务也比较多，涉及的网络区域也比较多



具体要求说明

提供的服务：

- 面向互联网的患者提供患者端服务
- 面向内部医生提供医生端服务

调用的服务：

- 调用第三方的用户信息服务，如公众号身份认证
- 调用HIS和申康的接口

涉及的网络区域比较多：

- 面向互联网
- 面向医院内网区
- DMZ区(Demilitarized Zone隔离区/非军事化区)

开通策略

因此一个完整的网络开通策略如下：

- 1) 互联网到前置机
 - 源地址：192.168.20.11（前置机）
 - 目标端口：443
 - 前置机需要提供**公网IP、域名、证书**
- 2) 开通前置机访问互联网的接口
- 3) 开通前置机到应用服务器78的接口
 - 源地址：192.168.20.11前置机)
 - 目标地址:198.168.9.1 (应用1)、192.168.9.2(应用2)
 - 目标端口：8038、8039
- 4) 开通应用服务器访问前置机的接口
 - 源地址：198.168.9.1 (应用1)、192.168.9.2(应用2)
 - 目标地址:192.168.20.1（前置机）
 - 目标端口：8080
- 5) 开通应用两台服务器间的接口
 - 互相访问，开通8038、8039、3306、27017
- 6) 开通应用服务器访问HIS厂商的接口
 - 源地址：198.168.9.1 (应用1)、198.168.9.2(应用2)
 - 目标地址：（HIS厂商提供）
 - 目标端口：（HIS厂商提供）
- 7) 开通HIS厂商到应用服务器的接口
 - 源地址：（HIS厂商提供）
 - 目标地址：198.168.9.1 (应用1)、192.168.9.2(应用2)
 - 目标端口：8038、8039
- 8) 开通应用服务器访问LIS的接口
 - 源地址：198.168.9.1 (应用1)、198.168.9.2(应用2)
 - 目标地址：（LIS厂商提供）
 - 目标端口：（LIS厂商提供）
- 9) 开通医生访问应用管理端的接口
 - 源地址：医生工作站
 - 目标地址：198.168.9.1 (应用1)、198.168.9.2(应用2)
 - 目标端口：8038、8039

经验心得：

- 由于网络开通策略要走很多流程，一定要规划好，争取一次申请通过，可以节约你大量时间；上面的开通策略，看起来挺复杂，只要作为整体规划好，一条条列，最后也挺清楚的不是嘛
- 流程走完，网管开通好后，一定要及时、一条条地检查确认是否真正开通成功，毕竟是人操作的，总有疏漏。等发现问题再协调人，还得等啊等！
- 上面的目标端口只列了一个，在实际操作中，可以适当多预留几个端口，多开通几个，便于后面业务扩展时备用，毕竟再走流程还要花时间。
- 另外，一定要考虑好可测试性，端口是否连通可以自己验证，页面是否正常访问可以自己验证，别人也很忙的，若自己不能验证指望别人操作告诉你，就是瞎忙！
- 总之，设计规划的时候多花些时间，搞清楚原理，可以大大减少走流程的时间，减少出了问题再协调人的时间，效率大大滴高！