## 网络设计

### 纯开放式设计

所有服务器都有公网及私网IP，可从任意位置访问到生产服务器。

### 半开放式

生产服务器只有私网IP，从外网访问不到。但是生产服务器可直接访问外网。

有漏洞，被入侵，反连程序是能够连接出去的。也可以从网络上下载到黑客的挖矿病毒等东西。

### 封闭式

生产服务器只有私网IP，从外网访问不到，也无法访问外网。

被入侵，无法从外网下载任何东西，反连连接不出去。

### 软隔离

软隔离是指，在交换机、防火墙等上配置规则进行隔离

### 硬隔离

硬隔离是指，在网络直接没有物理通路。

## 网络准入

开源系统：packetfence

<https://blog.csdn.net/qq_18204953/article/details/80708303>

<https://blog.csdn.net/qq_18204953/article/details/80758947>

<https://www.cnblogs.com/xixizhouping/articles/6424261.html>

商业：一堆零信任终端

## K8S

Docker Bench Security：一个用于检查Docker主机和容器配置的Shell脚本，可帮助识别可能存在的安全风险和违规配置。

Clair：一个针对Docker镜像进行漏洞扫描的开源工具，可以自动扫描容器中使用的操作系统和软件组件，以便及早发现和修复漏洞。

Sysdig Falco：一个用于实时监控Docker容器的安全事件的开源工具，可以检测到潜在的威胁并自动响应，例如不安全的进程启动、文件修改、网络连接等活动。

Docker Security Playground：一个用于模拟Docker环境中安全问题的开源项目，可以帮助用户了解常见的攻击手法，并研究如何保护Docker环境免受攻击。