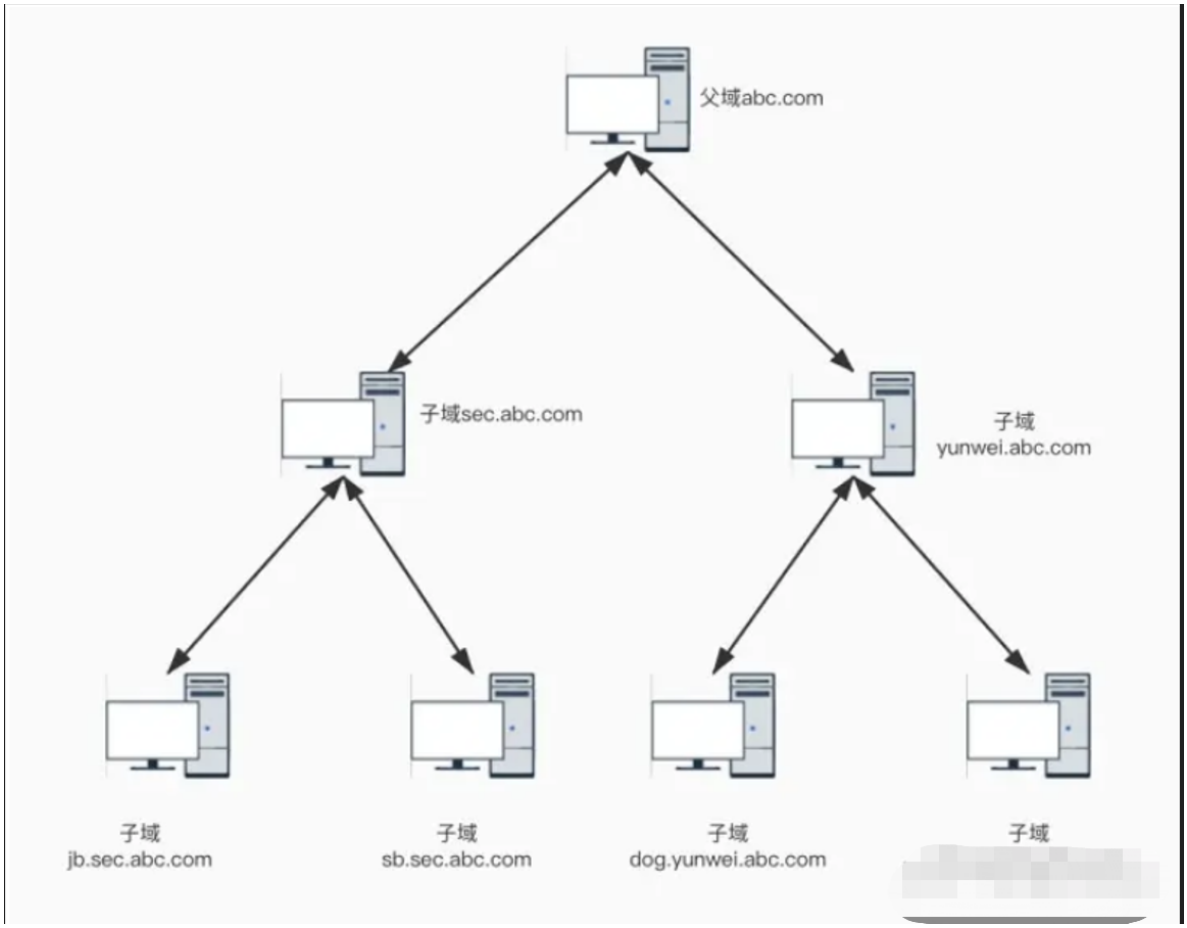
跨域攻击介绍

内网中的域林

很多大型企业都拥有自己的内网，一般通过域林进行共享资源。根据不同职能区分的部门，从逻辑上以主域和子域进行区分，以方便统一管理。在物理层，通常使用防火墙将各个子公司及各个部门划分为不同的区域。

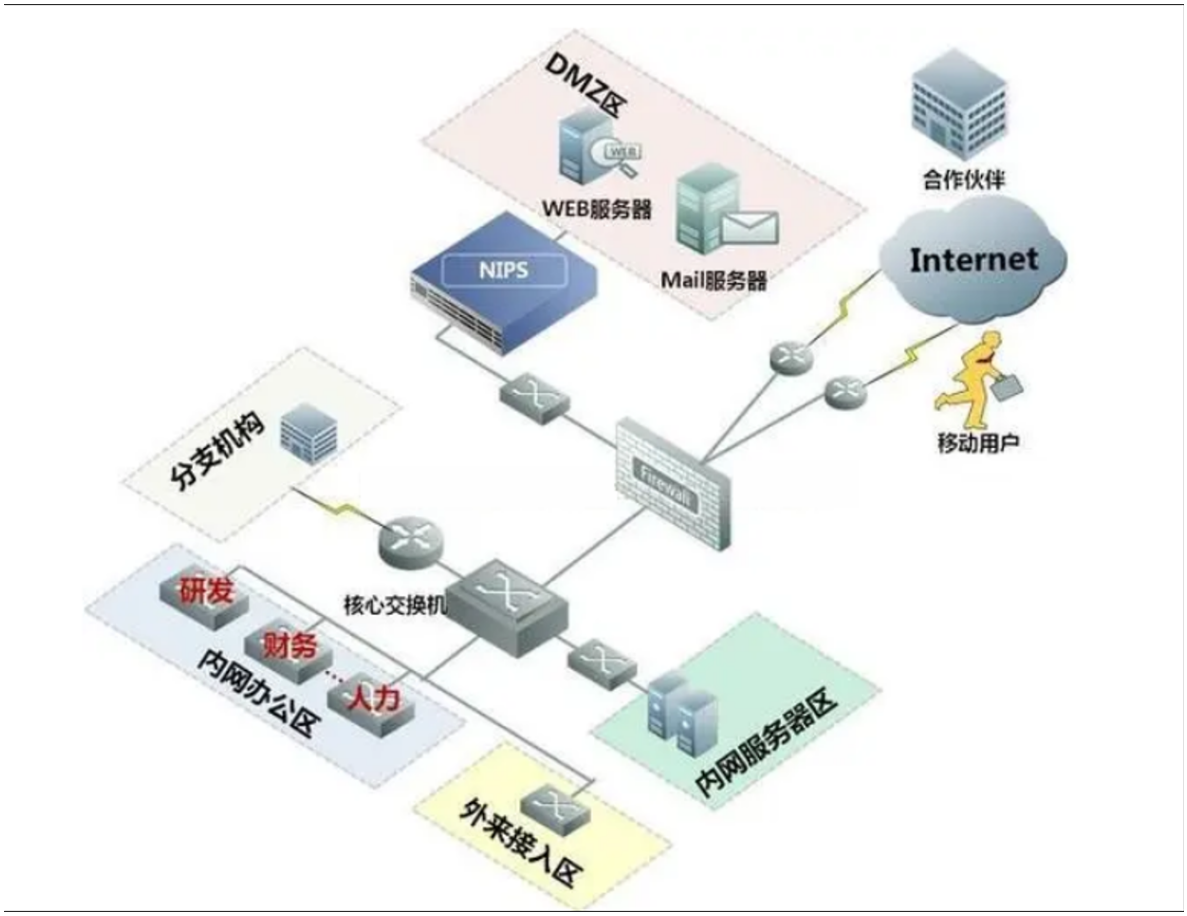


跨域攻击方法

1、常规渗透方法（利用web漏洞）

2、哈希传递票据攻击

3、利用域信任关系



域信任关系

建立域之间的信任关系，是为了一个域的用户能方便地访问其他域的资源，同时也方便了对域网络的管理和维护，域信任作为域中的一种机制，允许另一个域的用户在通过身份验证后访问本域中的资源。同时，域信任利用DNS服务器定位两个不同子域的域控制器，如果两个域中的域控制器都无法找到另一个域，也就不存在通过域信任关系进行跨域资源共享了

域信任关系分类

域信任关系分为单向信任和双向信任

单向信任：是指在两个域之间创建单向的信任路径，即在一个方向上是信任流，在另一个方向上是访问流，受信任域内的用户（或者计算机）可以访问信任域内的资源，但信任域内的用户无法访问受信任域内的资源。也就是说，A域信任B域，那么B域内受信任的主体可以访问A域内信任B域的资源。

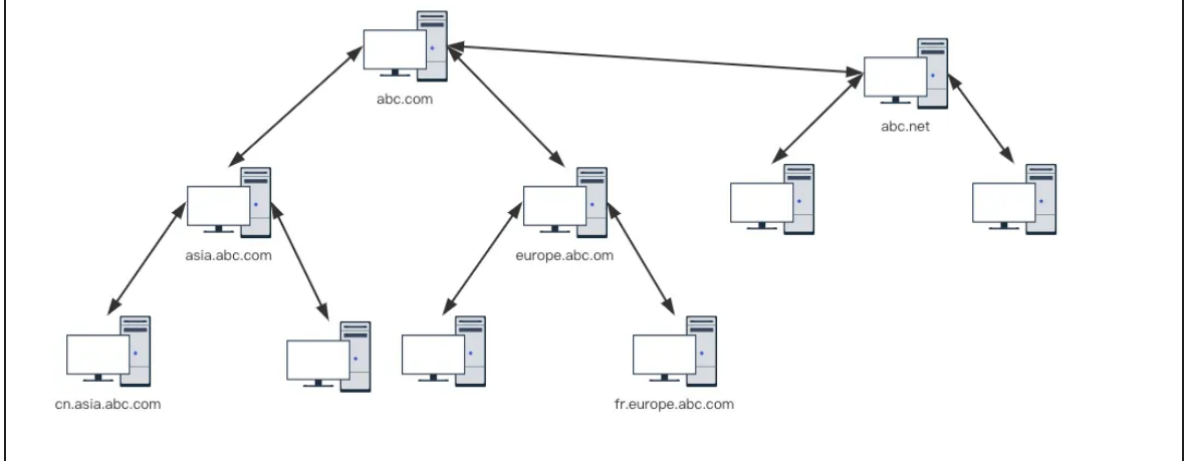
双向信任：是指两个单向信任的组合，信任域和受信任域彼此信任，在两个方向上都有信任流和访问流。这意味着，可以从两个方向在两个域之间传递身份验证请求。活动目录中的所有信任关系都是双向可传递的。在创建子域时，会在新的父域和子域之间自动创建双向可传递信任关系，从下级域发出的身份验证请求可以通关其父域向上流向信任域

域信任关系也可以分为内部信任和外部信任

内部信任：在默认情况下,用活动目录安装向导将新域添加到域树或林根域中，会自动创建双向可传递信任。在现有林中创建域树时，将建立新的树根信任，当前域树中的两个或多个域之间的信任关系被称为内部信任。这种信任关系是可传递的。例如，有三个子域BA,CA,DA,BA域信任CA域，CA域信任DA域，则BA域也信任DA域。

外部信任是指两个不同林中的域的信任关系。外部信任是不可传递的，而且是单向的。

只有domain admins组中的用户可以管理域信任关系


abc.com
abc.net
asia.abc.com
europe.abc.om
cn.asia.abc.com
fr.europe.abc.com