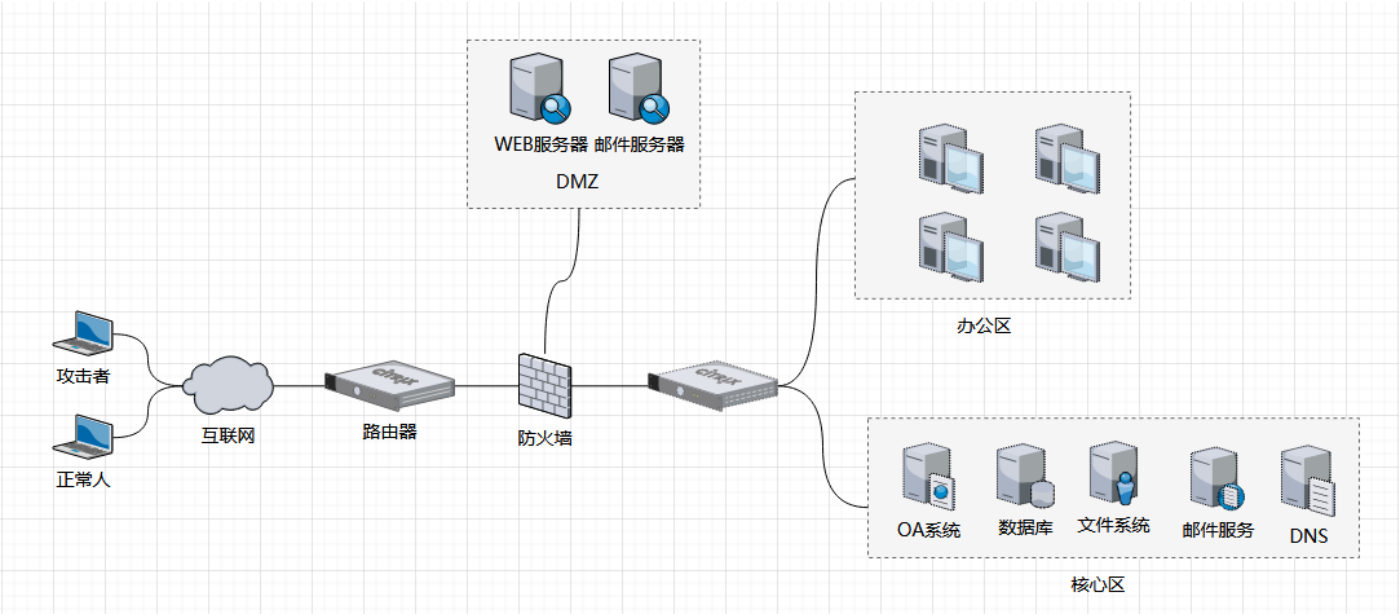
安全域的划分

划分安全域的目的是将一组安全等级相同的计算机划入同一个网段。这个网段内的计算机拥 有相同的网络边界,并在网络边界上通过部署防火墙来实现对其他安全域的网络访问控制策略 ，从而对允许哪些IP地址访问此域、允许此域访问哪些IP地址和网段进行设置。这些 措施,将使得网络风险最小化,当攻击发生时,可以尽可能地将威胁隔离,从而降低对域内计算 机的影响。



在一个用路由器连接的内网中,可以将网络划分为三个区域:

安全级别最高的内网;

安全级别中等的DMZ;

安全级别最低的外网

在配置一个拥有DMZ的网络时,通常需要定义如下访问控制策略,以实现其屏障功能。

内网可以访问外网:内网用户需要自由地访问外网。在这一策略中,防火墙需要执行NAT。
内网可以访问DMZ:此策略使内网用户可以使用或者管理DMZ中的服务器
外网不能访问内网:这是防火墙的基本策略。内网中存储的是公司内部数据,显然,这些数据一般是不允许外网用户访问的
外网可以访问DMZ:因为DMZ中的服务器需要为外界提供服务,所以外网必须可以访问DMZ。同时,需要由防火墙来完成
DMZ不能访问内网:如果不执行此策略,当攻击者攻陷DMZ时,内网将无法受到保护
DMZ不能访问外网:此策略也有例外。例如,在DMZ中放置了邮件服务器,就要允许访问外网,否则邮件服务器无法正常工

办公区:公司员工日常的工作区,一般会安装防病毒软件、主机入侵检测产品等。办公区一般能够访问DMZ。如果运维人员也在办公区,那么部分主机也能访问核心数据区(很多企业还会使用堡垒机来统一管理用户的登录行为)攻击者如果想进入内网,一艘会使用鱼叉攻击、水坑攻击,当然还有社会工程学手段。办公区人员多而杂,变动也很频繁,在安全管理上可能存在诸多漏洞,是攻击者进人内网的重要途径

之

核心区:存储企业最重要的数据、文档等信息资产,通过日志记录、安全审计等安全措施进行严密的保护,往往只有很少的主机能够访问。从外部是绝难直接访问核心区的。一般来说,能够直接访问核心区的只有运维人员或者IT部门的主管,所以,攻击者会重点关注这些用户的信息(攻击者在内网中进行横向移动攻击时,会优先查找这些主机)