什么是网络安全中的“ DMZ ”？ PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/251/2021_2022__E4_BB_80_E4_B9_88_E6_98_AF_E7_c101_251048.htm DMZ是英文“ demilitarized zone ”的缩写，中文名称为“ 隔离区 ”，也称“ 非军事化区 ”。它是为了解决安装防火墙后外部网络不能访问内部网络服务器的问题，而设立的一个非安全系统与安全系统之间的缓冲区，这个缓冲区位于企业内部网络和外部网络之间的小网络区域内，在这个小网络区域内可以放置一些必须公开的服务器设施，如企业Web 服务器、FTP服务器和论坛等。另一方面，通过这样一个DMZ区域，更加有效地保护了内部网络，因为这种网络部署，比起一般的防火墙方案，对攻击者来说又多了一道关卡。网络结构如下图所示。网络设备开发商，利用这一技术，开发出了相应的防火墙解决方案。称“ 非军事区结构模式 ”。DMZ通常是一个过滤的子网，DMZ在内部网络和外部网络之间构造了一个安全地带。 DMZ防火墙方案为要保护的内部网络增加了一道安全防线，通常认为是非常安全的。同时它提供了一个区域放置公共服务器，从而又能有效地避免一些互联应用需要公开，而与内部安全策略相矛盾的情况发生。在DMZ区域中通常包括堡垒主机、Modem池，以及所有的公共服务器，但要注意的是电子商务服务器只能用作用户连接，真正的电子商务后台数据需要放在内部网络中。 在这个防火墙方案中，包括两个防火墙，外部防火墙抵挡外部网络的攻击，并管理所有内部网络对DMZ的访问。内部防火墙管理DMZ对于内部网络的访问。内部防火墙是内部网络的第三道安全防线（前面有了外部

防火墙和堡垒主机），当外部防火墙失效的时候，它还可以起到保护内部网络的功能。而局域网内部，对于 Internet的访问由内部防火墙和位于DMZ的堡垒主机控制。在这样的结构里，一个黑客必须通过三个独立的区域（外部防火墙、内部防火墙和堡垒主机）才能够到达局域网。攻击难度大大加强，相应内部网络的安全性也就大大加强，但投资成本也是最高的。