怎样解决网络边界安全问题 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/461/2021_2022__E6_80_8E_E6_A0_B7_E8_A7_A3_E5_c101_461760.htm 人们为了解决资源的共享而建立了网络，然而全世界的计算机真的联成了网络，安全却成了问题。因为在网络上，你不清楚对方在哪里，泄密、攻击、病毒等等，越来越多的不安全因素让网络管理者难以安宁，所以把有安全需求的网络与不安全的网络分开，是没有办法的选择。分离形成了网络的“ 孤岛 ”，没有了连接，安全问题自然消失了。 然而因噎废食不是个办法，没有连接，业务也无法互通，网络孤岛的资源在重复建设、浪费严重，并且随着信息化的深入，在各种网络上信息共享需求日益强烈，比如：政府的内网与外网，需要面对公众服务；银行的数据网与互联网，需要支持网上交易；企业的办公与生产网，老总们的办公桌上不能总是两个终端吧；民航、铁路与交通部的信息网与互联网，网上预定与实时信息查询是便利出现的必然…… 一、网络边界上需要什么 把不同安全级别的网络相连接，就产生了网络边界。防止来自网络外界的入侵就要在网络边界上建立可靠的安全防御措施。下面我们来看看网络边界上的安全问题都有哪些： 非安全网络互联带来的安全问题与网络内部的安全问题是截然不同的，主要的原因是攻击者不可控，攻击是不可溯源的，也没有办法去“ 封杀 ”，一般来说网络边界上的安全问题主要有下面几个方面： 1、信息泄密：网络上的资源是可以共享的，但没有授权的人得到了他不该得到的资源，信息就泄露了。一般信息泄密有两种方式： ◆攻击者（非授权人员）进入了网络，获

取了信息，这是从网络内部的泄密◆合法使用者在进行正常业务往来时，信息被外人获得，这是从网络外部的泄密 2、入侵者的攻击：互联网是世界级的大众网络，网络上有各种势力与团体。入侵就是有人通过互联网进入你的网络（或其他渠道），篡改数据，或实施破坏行为，造成你网络业务的瘫痪，这种攻击是主动的、有目的、甚至是有组织的行为。3、网络病毒：与非安全网络的业务互联，难免在通讯中带来病毒，一旦在你的网络中发作，业务将受到巨大冲击，病毒的传播与发作一般有不确定的随机特性。这是“ 无对手 ”、“ 无意识 ”的攻击行为。 4、木马入侵：木马的发展是一种新型的攻击行为，他在传播时象病毒一样自由扩散，没有主动的迹象，但进入你的网络后，便主动与他的“ 主子 ”联络，从而让主子来控制你的机器，既可以盗用你的网络信息，也可以利用你的系统资源为他工作，比较典型的就是“ 僵尸网络 ”。 来自网络外部的安全问题，重点是防护与监控。来自网络内部的安全，人员是可控的，可以通过认证、授权、审计的方式追踪用户的行为轨迹，也就是我们说的行为审计与合轨性审计。 由于有这些安全隐患的存在，在网络边界上，最容易受到的攻击方式有下面几种： 1、黑客入侵：入侵的过程是隐秘的，造成的后果是窃取数据与系统破坏。木马的入侵也属于黑客的一种，只是入侵的方式采用的病毒传播，达到的效果与黑客一样。 2、病毒入侵：病毒就是网络的蛀虫与垃圾，大量的自我繁殖，侵占系统与网络资源，导致系统性能下降。病毒对网关没有影响，就象“ 走私 ”团伙，一旦进入网络内部，便成为可怕的“ 瘟疫 ”，病毒的入侵方式就象“ 水 ”的渗透一样，看似漫无目的，实则无孔不入。

3、网络攻击：网络攻击是针对网络边界设备或系统服务器的，主要的目的是中断网络与外界的连接，比如DOS攻击，虽然不破坏网络内部的数据，但阻塞了应用的带宽，可以说是一种公开的攻击，攻击的目的一般是造成你服务的中断。 二、边界防护的安全理念 我们把网络可以看作一个独立的对象，通过自身的属性，维持内部业务的运转。他的安全威胁来自内部与边界两个方面：内部是指网络的合法用户在使用网络资源的时候，发生的不合规的行为、误操作、恶意破坏等行为，也包括系统自身的健康，如软、硬件的稳定性带来的系统中断。边界是指网络与外界互通引起的安全问题，有入侵、病毒与攻击。 如何防护边界呢？对于公开的攻击，只有防护一条路，比如对付DDOS的攻击；但对于入侵的行为，其关键是对入侵的识别，识别出来后阻断它是容易的，但怎样区分正常的业务申请与入侵者的行为呢，是边界防护的重点与难点。 我们把网络与社会的安全管理做一个对比：要守住一座城，保护人民财产的安全，首先建立城墙，把城内与外界分割开来，阻断其与外界的所有联系，然后再修建几座城门，作为进出的检查关卡，监控进出的所有人员与车辆，是安全的第一种方法；为了防止入侵者的偷袭，再在外部挖出一条护城河，让敌人的行动暴露在宽阔的、可看见的空间里，为了通行，在河上架起吊桥，把路的使用主动权把握在自己的手中，控制通路的关闭时间是安全的第二种方法。对于已经悄悄混进城的“危险分子”，要在城内建立有效的安全监控体系，比如人人都有身份证、大街小巷的摄像监控网络、街道的安全联防组织，每个公民都是一名安全巡视员，顺便说一下：户籍制度、罪罚、联作等方式从老祖宗商鞅就

开始在秦国使用了。只要入侵者稍有异样行为，就会被立即揪住，这是安全的第三种方法。 作为网络边界的安全建设，也采用同样的思路：控制入侵者的必然通道，设置不同层面的安全关卡，建立容易控制的“ 贸易 ”缓冲区，在区域内架设安全监控体系，对于进入网络的每个人进行跟踪，审计其行为等等 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com