浅析网络安全中防火墙和IDS的作用 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__E6_B5_85_E6_9E_90_E7_BD_91_E7_c101_251023.htm 随着互联网的兴起，网络服务、媒体的多元化发展，网络与越来越多的商业应用和经济领域的联系越来越多，与此同时，安全问题也渐渐浮出了水面。 那么，怎么才能做到安全？ 业界的同行曾经说过“ 安全，是一种意识，而不是某种的技术就能实现真正的安全。 ”随着工作的时间渐长，对这句话的体会就越深。再防守严密的网络，利用人为的疏忽，管理员的懒惰和社会工程学也可能被轻易攻破。 因此，在这里我介绍的防火墙和IDS技术，只是我们在网络安全环节中进行的一个防御步骤。不要听信某些商家的销售人员所说的：“ 装上我们的xx防火墙，就能绝对保证您的网络安全 ”等等动听的话语，事实上那不过是为了销售其产品而制造出来的“ 善意的欺骗 ”而已。在网络内进行防火墙与IDS的设置，并不能保证我们的网络就绝对安全了，但是设置得当的防火墙和IDS，至少会使我们的网络更为坚固一些，并且能提供更多的攻击信息供我们分析。 接下来，让我们抛开商家的宣传，正确地认识一下防火墙和IDS的作用吧。 防火墙 一、防火墙能够作到些什么？ 1.包过滤 具备包过滤的就是防火墙？对，没错！根据对防火墙的定义，凡是能有效阻止网络非法连接的方式，都算防火墙。早期的防火墙一般就是利用设置的条件，监测通过的包的特征来决定放行或者阻止的，包过滤是很重要的一种特性。虽然防火墙技术发展到现在有了很多新的理念提出，但是包过滤依然是非常重要的一环，如同四层交换机首要的仍是要具

备包的快速转发这样一个交换机的基本功能一样。通过包过滤，防火墙可以实现阻挡攻击，禁止外部/内部访问某些站点，限制每个ip的流量和连接数。 2.包的透明转发 事实上，由于防火墙一般架设在提供某些服务的服务器前。如果用示意图来表示就是 ServerFireWallGuest 。用户对服务器的访问的请求与服务器反馈给用户的信息，都需要经过防火墙的转发,因此，很多防火墙具备网关的能力。 3.阻挡外部攻击 如果用户发送的信息是防火墙设置所不允许的，防火墙会立即将其阻断，避免其进入防火墙之后的服务器中。 4.记录攻击 如果有必要，其实防火墙是完全可以将攻击行为都记录下来的，但是由于出于效率上的考虑，目前一般记录攻击的事情都交给IDS来完成了，我们在后面会提到。 以上是所有防火墙都具备的基本特性，虽然很简单，但防火墙技术就是在此基础上逐步发展起来的。 二、防火墙有哪些缺点和不足？ 1.防火墙可以阻断攻击，但不能消灭攻击源。“ 各扫自家门前雪，不管他人瓦上霜 ”，就是目前网络安全的现状。互联网上病毒、木马、恶意试探等等造成的攻击行为络绎不绝。设置得当的防火墙能够阻挡他们，但是无法清除攻击源。即使防火墙进行了良好的设置，使得攻击无法穿透防火墙，但各种攻击仍然会源源不断地向防火墙发出尝试。例如接主干网10M网络带宽的某站点，其日常流量中平均有512K左右是攻击行为。那么，即使成功设置了防火墙后，这512K的攻击流量依然不会有丝毫减少。 2.防火墙不能抵抗最新的未设置策略的攻击漏洞 就如杀毒软件与病毒一样，总是先出现病毒，杀毒软件经过分析出特征码后加入到病毒库内才能查杀。防火墙的各种策略，也是在该攻击方式经过专家分析后给出其特征

进而设置的。如果世界上新发现某个主机漏洞的cracker的把第一个攻击对象选中了您的网络，那么防火墙也没有办法帮到您的。 3.防火墙的并发连接数限制容易导致拥塞或者溢出由于要判断、处理流经防火墙的每一个包，因此防火墙在某些流量大、并发请求多的情况下，很容易导致拥塞，成为整个网络的瓶颈影响性能。而当防火墙溢出的时候，整个防线就如同虚设，原本被禁止的连接也能从容通过了。 4.防火墙对服务器合法开放的端口的攻击大多无法阻止 某些情况下，攻击者利用服务器提供的服务进行缺陷攻击。例如利用开放了3389端口取得没打过sp补丁的win2k的超级权限、利用asp程序进行脚本攻击等。由于其行为在防火墙一级看来是“ 合理 ”和“ 合法 ”的，因此就被简单地放行了。 5.防火墙对待内部主动发起连接的攻击一般无法阻止“ 外紧内松 ”是一般局域网络的特点。或许一道严密防守的防火墙内部的网络是一片混乱也有可能。通过社会工程学发送带木马的邮件、带木马的URL等方式，然后由中木马的机器主动对攻击者连接，将铁壁一样的防火墙瞬间破坏掉。另外，防火墙内部各主机间的攻击行为，防火墙也只有如旁观者一样冷视而爱莫能助。 6．防火墙本身也会出现问题和受到攻击 防火墙也是一个os，也有着其硬件系统和软件，因此依然有着漏洞和bug。所以其本身也可能受到攻击和出现软/硬件方面的故障。 7.防火墙不处理病毒 不管是funlove病毒也好，还是CIH也好。在内部网络用户下载外网的带毒文件的时候，防火墙是不为所动的（这里的防火墙不是指单机/企业级的杀毒软件中的实时监控功能，虽然它们不少都叫“ 病毒防火墙 ”）。 看到这里，或许您原本心目中的防火墙已经被我拉下了神台。是的

，防火墙是网络安全的重要一环，但不代表设置了防火墙就能一定保证网络的安全。“ 真正的安全是一种意识，而非技术! ”请牢记这句话。 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