快速了解关于IDS和IPS的安全区别 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/166/2021_2022__E5_BF_AB_E9_80_9F_E4_BA_86_E8_c101_166596.htm 正如我们大家所知道的那样，互联网的无处不在已经完全改变了我们所知道的网络。过去完全孤立的网络现在连接到了全世界。这种无处不在的连接使企业能够完成过去不可想象的任务。然而，与此同时还存在一个黑暗面。互联网变成了网络犯罪分子的天堂。这些网络犯罪分子利用这种连接向企业发起了数量空前的多的攻击。当互联网最初开始流行的时候，企业开始认识到它们应该使用防火墙防止对它们实施的攻击。防火墙通过封锁没有使用的TCP和UDP端口发挥作用。虽然防火墙在封锁某些端口的攻击是有效的，但是，有些端口对于HTTP、SMTP和POP3通信是有用的。为了保证这些服务工作正常，对这些常用的服务的对应的端口必须要保持开放的状态。问题是，黑客已经学会了如何让恶意通信通过这些通常开放的端口。 为了应付这种威胁，一些公司开始应用入侵检测系统(IDS)。IDS的思路是监视经过你的防火墙的全部通信并且查找可能是恶意的通信。这个思路在理论上是非常好的，但是，在实际上，IDS系统由于某些原因的影响工作得并不好。早期的IDS系统通过查找任何异常的通信发挥作用。当检测到异常的通信时，这种行动将被记录下来并且向管理员发出警报。这个过程很少出现问题。对于初始者来说，查找异常通信方式会产生很多错误的报告。经过一段时间之后，管理员会对收到过多的错误警报感到厌烦，从而完全忽略IDS系统的警告。 IDS系统的另一个主要缺陷是它们仅监视主要的通信

。如果检测到一种攻击，它将提醒管理员采取行动。人们认为IDS系统采取的这种方法是很好的。总之，由于IDS系统会产生很多的错误报告，你真的愿意让IDS系统对合法的网络通信采取行动吗? 在过去的几年里，IDS系统已经有了很大的进步。目前，IDS系统的工作方式更像是一种杀毒软件。IDS系统包含一个名为攻击签名的数据库。这个系统不断地把入网的通信与数据库中的信息进行比较。如果检测到攻击行动，IDS系统就发出这个攻击的报告。 比较新的IDS系统比以前的系统更准确一些。但是，这个数据库需要不断地更新以保持有效性。而且，如果发生了攻击并且在数据库中没有相匹配的签名，这个攻击可能就会被忽略。即使这个攻击被检测到了并且被证实是一种攻击，IDS系统除了向管理员发出警报和记录这个攻击之外没有力量做出任何事情。 这就是入侵防御系统(IPS)的任务了。IPS与IDS类似，但是，IPS在设计上解决了IDS的一些缺陷。 对于初始者来说，IPS位于你的防火墙和网络的设备之间。这样，如果检测到攻击，IPS会在这种攻击扩散到网络的其它地方之前阻止这个恶意的通信。相比之下，IDS只是存在于你的网络之外起到报警的作用，而不是在你的网络前面起到防御的作用。 IPS检测攻击的方法也与IDS不同。目前有很多种IPS系统，它们使用的技术都不相同。但是，一般来说，IPS系统都依靠对数据包的检测。IPS将检查入网的数据包，确定这种数据包的真正用途，然后决定是否允许这种数据包进入你的网络。 正如你所看到的，IDS和IPS系统有一些重要的区别。如果你要购买有效的安全设备，如果你使用IPS而不是使用IDS，你的网络通常会更安全。