何种入侵防护系统更适合？思科认证考试 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/644/2021_2022__E4_BD_95_E7_A7_8D_E5_85_A5_E4_c101_644652.htm 说到网络攻击，很多运维人员都挠头。这骇客说来就来，很少提前打招呼，还是需要找个反入侵的系统。这反入侵系统种类繁多，功能各有特色。比如IPS，就与大多数IDS系统的被动工作方式不同，入侵防护系统倾向于提供主动防护，其设计宗旨是预先对入侵活动和攻击性网络流量进行拦截，避免其造成损失，而不是简单地在恶意流量传送时或传送后才发出警报。那如何挑选一款适合单位的入侵防护系统呢？什么样的才能解决自己所遇到的问题？ 本文主要探讨挑选入侵防护系统时需要注意的问题和事项。 Q：请问，如何构建适合企业的入侵防护系统呢？ A：这个问题很大的, 通常先了解自己的网络应用, 再分析比较各个产品厂商,最好找到类似的企业案例应用参考. 最后当然实践出真知,上线测试一下,如果可以再模拟攻击一下,看好不好用。 Q：主动防护一般主要是哪几种形式？假如遭到恶意攻击时应采取怎样的应急措施？ A：根据不同的厂家和技术, 可以reject , 0drop , reset 连接等.遭到恶意攻击如果不是性能上的, 可以防火墙或之前的访问控制上直接加黑名单阻断,如果是DOS或DDOS, 在你的日志上有攻击源地址, 你可以找你的接入商要求封掉该地址对你的连接,或者从网络等方式找到该地址的所有维护者,通常是某些IDC里托管的机器,可以联系该IDC管理员,出示证据,解释清楚, 通常管理员会断哪个肉鸡的网再通知哪个所有人,起码我之前这样作过。 Q：学网络安全并不是很好，我想问下，如果把所有的漏洞都补齐，

黑客还能入侵我们的操作系统吗？如何发现自己的系统被入侵了？入侵检测系统，检测的哪种行为算是被入侵？ A：漏洞都补齐(只是理论上,没有哪个厂家宣称自己没有任何弱点) ,也可能被侵入.比如你的系统已经把所有的想象到的补丁都打了, 但你上网访问某些网站,说要下载某个运行软件, 你同意了,或者根本就是混在其他应用里下来的, 是你主动连接下载的,那就没有用.所以通常IPS就是,等你人为的犯错,它也是可以起到一定防护作用的入侵检测系统，检测的哪种行为算是被入侵？要看它的策略定义了。 Q：个人比较头疼被入侵的问题，公司业务已经被入侵过多次，包括webshell、挂马以及DDOS流量攻击，打击很大，但是一直也没找到让人踏实好用的方法解决掉这些问题，趁此机会请教两位安全方向的大师，对于做互联网行业的公司，其公网服务器的保护该做哪些方面的安全措施？哪些设备对这些方面的防护效果会比较好？ A：通常来说.公网上的服务应用,首先建议要用不是那么知名的漏洞很多的那些应用软件,其次系统加固一下,把系统缺省启动的那些不用的应用和端口都关掉,能修正的补丁用上,帐户密码就不用说了, 不要上来Root 权限就可以直接连接,怎么也得用低级帐号登陆再在需要时候切换哪.之后前面最少有防火墙做访问限制,只开放对外的端口和应用,对那些维护类的如telnet / ssh / ftp等在防火墙上最好作好日志记录, 能有先一步的认证机制或VPN连接就更好了,之后如果可以,再放个 IPS , 针对你的应用重点防御. 你觉得防护作的差不多了, 找个知名的攻击类探测扫描器的厂商,针对性攻击尝试一下,如果还有漏洞就再补。 Q：我们公司最近也在做入侵防护系统的选型工作，但是面对市面上那么多品牌和型号的IPS产品，我们该如

何选择呢？需要考虑哪些技术指标呢？ A：这个要多查些网络对比评论的文章了.通常选择的指标, 性能方面有加载检测防护策略条件下的吞吐量, 时间延迟,最大并法容量,新建连接能力等, 硬件上有Fail-open卡,电源风扇磁盘存储的冗余等, 软件功能有检测项目的数目,测试的误报率和漏报率,管理界面的友好度, 统计分析报表等。 Q：一般的中小企业有上这种产品的必要吗? 