跟你分析筛选IPS之八大定律 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__E8_B7_9F_E4_BD_A0_E5_88_86_E6_c101_166586.htm 在保护企业网服务器不受攻击方面，安全经理面临着众多的挑战。尽管入侵检测系统（IDS）曾一度广受欢迎，但如今互联网上攻击方式不断翻新，同时，签名技术的IDS检测不到新攻击和变形攻击，也检测不出加密流量中的攻击，因此，传统的IDS在主动性上逐渐显示出其局限性。 那么，企业还有什么选择呢？入侵防护系统（IPS）是企业下一代安全系统的大趋势。它不仅可进行检测，还能在攻击造成损坏前阻断它们，从而将IDS提升到一个新水平。IDS和IPS的明显区别在于：IPS阻断了病毒，而IDS则在病毒爆发后进行病毒清除工作。 目前市场上有许多种产品都被冠以“ 防护 ”的字眼。但是，真正的入侵防护解决方案可使企业不必进行分析即可采取措施保护系统；同时，它可防止攻击对操作系统、应用程序和数据造成损坏。McAfee公司认为，一个理想的入侵防护解决方案应该包括以下八大特点： 主动、实时预防攻击 应该在任何未授权活动开始前找出攻击，并防止它进入重要的服务器资源。 补丁等待保护 补丁管理是一个复杂的过程。在补丁被开发和安装之间，聪明的黑客会对服务器和重要数据造成破坏，McAfee IntruShield入侵防护解决方案可为系统管理员提供补丁等待期内的保护和充足时间，以测试并安装补丁。 保护每个重要的服务器 服务器中有最敏感的企业数据，是大多数黑客攻击的主要目标。通过对IntruShield进行配置，可以设定对服务器的专门保护方案，从而为企业的重要的资源提供深层防护。 签

名和行为规则 检测入侵最有效的方法是采取混合方式，即整合针对具体攻击的签名和行为规则的力量。这一混合方式可提供已知和未知攻击保护，而同时将误报率保持在最低，从而无须做出任何损失性让步。McAfee IntruShield通过进行签名设置，以“ in-line ”模式配置的入侵防护解决方案，可以设定一种响应行为，用以抓取攻击的数据包，从而在黑客对漏洞发动攻击之前，就阻止它们。 深层防护 强大的安全都是基于深度防御的概念，IntruShield独特的体系结构和集成的多项专利技术可以保护那些具有最严格要求的网络。 可管理性 理想的入侵防护解决方案可使安全设置和策略被各种应用程序、用户组和代理程序利用，从而降低安装并维护大型安全产品的成本。 McAfee IntruShield高度自动、易于管理且有很大的灵活性，可分阶段实施安装，从而避免当今原有IDS不可避免的误报。 可扩展性 大型分散式企业需要可升级的可扩展性，以便实现众多受保护的服务器、大流量和分散型安全管理。具有良好可扩展性的IntruShield方案提供了综合的防护体系，可以跨越企业核心网络，企业边界网络，以及分支机构的网络。 经验证的防护技术 企业所要选择的解决方案是否采用了业界先进的新技术，是否经过充分测试、使用，并在受到持续不断地维护，这一点很重要。 因此，无论是混合威胁，还是恶意攻击，都需要有一套合适的安全解决方案。而入侵防护不仅可以检测进出网络的恶意代码和攻击，而且还可以在这些攻击发生之前，将他们进行阻止。 企业在选购的时候，可以参照以上八大定律进行对比和测试，以便选择到合适的产品和方案。 