购买IPS之前需要问的15个问题思科认证 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__E8_B4_AD_E4_B9_B0IPS_E4_c101_644292.htm 需要问的关键问题： 设备配备了双电源吗?由于IPS是一种联机设备，你需要确保它在发生停电时正常运行。 有什么故障切换选择?部署单台IPS意味着你建立一种你的安全防线中存在单故障点的环境。 设备可以处理多少并发会话?IPS系统必须能够扩展来满足峰值需求。 基于特征的IPS具有多少种特征?显然，特征越多越好。 IPS是双向的吗?你需要IPS分析进入的和离开你的网络的传输流，尤其对于黑客试图接管网络上的主机并利用它作为僵尸机来发送(例如)海量的垃圾邮件的情形。 IPS检查2-7层上的数据包吗?一些IPS设备可以检查最高4层的数据包，另一些则可以分析一直到7层的数据包。 配置方便吗?配置是IPS设备存在的一个大问题。你必须调节设备，使它一方面不要成为假报警的来源，另一方面不要让恶意传输流进入。 IPS是否以线速度处理传输流?IPS厂商宣称线速度吞吐量，但真实的吞吐量通常低很多。一定要在你的网络上测试吞吐量。 延时是多少?尤其在处理VoIP传输流和视频流时，你必须确保延时不成为问题。 IPS发出哪些类型的报警?许多客户根据不信任设备自己采取补救行动，宁愿在收到报警后再对攻击做出反应。客户必须决定他们想让设备如何对不同类型的攻击做出响应。 当发生入侵时，IPS采取哪些具体行动?你可能希望IPS阻止攻击，或者你可能希望IPS阻止攻击并立即通知你。你也可能希望它执行取证并提供关于攻击的报告。 IPS提供什么类型的管理系统?尤其当你拥有多台设备时，你需要一种使你可以高效

率地执行更新、调节设置和获得报告的管理系统。 IPS的仪表板是什么样的?它是否直观，易于使用。来源：www.examda.com 设备可以执行什么类型的取证?你需要一种可以分析攻击和识别你的网络防线中存在的安全漏洞的IPS。 设备提供什么类型的报告?你需要简明、提供有关网络上的重大安全事件的高级情报的报告。 编辑特别推荐: 深入理解GFW:路由扩散技术 全方位看透家用路由器 CISCO ASA5520的基本配置 思科寄存器详细解释 Cisco 5520ACL配置的基本配置 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