硬件入侵检测系统完全导购(2) 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__E7_A1_AC_E4_BB_B6_E5_85_A5_E4_c101_251041.htm 6、金诺网安KIDS 3000 金诺网络安全技术发展股份有限公司2000年成立于上海，自主开发的拥有知识产权的部分产品有：金诺网安入侵检测系统KIDS、金诺网安外联监控系统KNCS、金诺网安介质取证系统DISKFOREN等。KIDS采用了智能的检测技术，它综合了特征匹配、协议分析和流量异常监测等多种检测技术的优点，能检测多种入侵攻击行为，包括扫描、嗅探、后门、病毒、恶意代码、拒绝服务、分布式拒绝服务、可疑行为、非授权访问、主机异常和欺骗等11大类的安全事件，目前拥有的检测规则超过1800条，安全报警事件1200多条。系统具有完善的攻击事件库，并与国际上标准的漏洞库CVE、BugTraq和Whitehats等保持兼容。KIDS提供了多种分析工具，具有强大的安全事件追踪分析功能。KIDS采用了新一代的包处理技术和协议分析算法，传感器具备强劲的流量处理引擎。 7、东软NetEye IDS 2100 - FE2 东软集团来自东北大学，创立于1991年，总部位于中国沈阳。东软NetEye IDS利用独创的数据包截取技术对网络进行不间断的监控，扩大网络防御的纵深，同时采用先进的基于网络数据流实时智能分析技术判断来自网络内部和外部的入侵企图，进行报警、响应和防范。是防火墙之后的第二道安全闸门。同时具备强大的网络信息审计功能，可对网络的运行，使用情况进行全面的监控、记录、审计和重放，使用户对网络的运行状况一目了然。并且提供网络嗅探器和扫描器用于分析网络的问题，定位网

络的故障。不但保障网络的安全，同时保障网络的健康运行。NetEye入侵检测系统可对自身的数据库进行自动维护，不需要用户的干预。学习和使用及其简易，不对网络的正常运行造成任何干扰，是完整的网络审计、监测、分析和管理系统。NetEye 入侵检测系统可与防火墙联动，自动配置防火墙策略，配合防火墙系统使用，可以全面保障网络的安全，组成完整的网络安全解决方案。 三、实际应用实例 应用环境：在一个企业级的Intranet网络中，在多个关键网段中（DMZ网络服务区、内网区、工作组区）分别部署IDS系统，以实现多处设防；采用IDS管理中心进行集中监控，同时也可与防火墙、网管平台等外围设备进行集成互动。 IDS通常只有两个端口，1个管理口与1个网络监听端口。管理口与控制中心连接，监听端口连接到所要检测区域的中心交换机上。 1、配置交换机的端口镜像 在非共享式的交换机上需要配置端口镜像。交换机端口镜像功能将从指定的交换机端口中复制端口流量到镜像端口中，以便进行流量和协议分析。下面以思科的3500、2900系统的交换机为例讲述如何配置端口镜像： 型号 配置方式 命令步骤 说明 3500,2900 系列 IOS enable,password configure configure terminal interface fastethernet moudle/port 模块 / 端口 port monitor {moudal/port | vlanID} 镜像源端口或 vlan end write show intterface fastethernet moudle/port mornitor 查看镜像 2、设置控制中心 控制中心的任何操作都是通过菜单来完成的，为了增加操作的方便，对常用的一些操作设置了专门的按钮。 3、配置探测引擎 探测引擎分两部分，工具栏和探测引擎/子控制列表。工具栏里罗列了和探测引擎控制相关的常用工具按钮。列表里面是受控制中心直接管理的探测引擎

、和子控制中心。有名称、IP地址、运行策略、通道状态、应用策略的时间等信息。 4、编辑策略 策略分为系统策略以及衍生策略两类，系统策略为系统固有的策略，不可以进行编辑、删除及重命名。衍生策略为系统固有策略的衍生策略，可以由用户更改。 选中一个策略，并按动"衍生策略"按钮，系统则复制一份完全一样的模板，名称是在原有的名字后面加上"衍生策略"。选中一个衍生策略，原"查看策略"按钮就会自动变成"编辑策略"，按动该按钮，系统则以读写方式打开策略编辑器。如图： 5、分析报表 IDS的一个最大的特点就是有详细的入侵检测报表分析，对每一件的网络攻击事件都有详细的记录（如：事件发生的时间、源IP与目的IP、攻击事件等）。根据不同的条件分为几组，方便查找。 6、联动 由于IDS的接入方式都是采用旁路方式来监听网络上的数据流，所以这就限制了IDS本身的阻断功能，IDS只有靠发阻断数据包来阻断当前的行为，阻断的范围很小，只能阻断建立在TCP基础之上的一些行为，如TELNET、FTP、HTTP等，对建立在UDP基础之上或已经完成了TCP三次握手之后的行为就无能为力了。IDS与防火墙联动的目的就是为了更有效的阻断所发生的攻击事件。 在窗口中，选择防火墙的类型；添加防火墙的IP地址即可。当IDS发现有黑客攻击的时候，就会发出阻断数据包传输到防火墙，由防火墙来阻断攻击行为，更好的保护网络。 四、入侵检测系统的一些比较 1、入侵检测系统和等其他安全产品的区别 不同的安全产品会起到不同的作用。单位虽然有了防火墙，但只能对外部来的网络攻击起到防御作用，对于调制解调器的后门却是毫无能力。据国际IDC统计，70%以上的攻击都是来自防火墙管不到的网络内

部。依据目前黑客所掌握的攻击能力，使得现有的安全产品如防火墙、身份认证、防病毒、加密等，在现有的操作系统本身以及各种应用软件的环境下，都不能阻止黑客对系统网络的攻击。