如何配置规则才可以既能够检测出尽可能多的攻击,又保证设备的性能不受影响?

谷会波 2006-09-04 发表

Q: 如何配置规则响应动作才可以既能够检测出尽可能多的攻击,又保证设备的性能不受影响?

A: 总出口的流量要关注一下，如果总出口的流量远小于IPS设备吞吐量的话，打开的过滤器可以更多一些。一般情况下，将Attack类的全部设成Block + Notify，将Network Infrastacture的全设成Block + Notify，将Spyware的过滤器全部搜出（共120多条）设成Block + Notify.然后根据用户需求,打开一些P2P流量的限流或阻断过滤器,以及对IM软件的阻断.