

## 知 SecCenter可否与网络、安全设备进行联动?

万欣 2008-09-18 发表

可以。

首先，该方案通过SecCenter安全管理中心与iMC（响应管理控制中心）两大核心组件构成；其中，安全管理中心提供对全网安全事件的采集、分析、关联、汇聚、报表报告展示，响应控制中心实现了安全事件与网管系统、用户管理系统的结合。

其次，联动的策略包括短信通知、Email通知、交换机端口控制、用户阻断、加入黑名单、在线提醒等功能。

比如一个简单的联动流程：终端用户发起对服务器的病毒攻击—> IPS设备检测到该攻击行为后进行阻止并上报SecCenter—> SecCenter经过智能分析后提交iMC—> iMC根据消息类型，下发管理员事先制定的联动策略。

这样，SecCenter安全管理中心与网络、安全的联动整合了安全事件、设备资源、用户资源，通过监控管理、分析管理、响应管理，构成闭环的管理系统，实现了全网统一安全管理。