计算机工程 2010 36 (8): 144-146 ISSN: 1000-3428 CN: 31-1289/TP 

安全技术

# 基于Snort的IPv6入侵检测技术

王相林，李蓓蕾

(杭州电子科技大学计算机学院，杭州 310018)

收稿日期 修回日期 网络版发布日期 接受日期

摘要 针对开源入侵检测系统Snort没有提供对IPv6协议的AH和ESP扩展首部支持的问题，提出利用Snort检测ESP加密报文的解决方案。构造ESP检测规则，在Snort协议分析模块加入DecodeESP()函数并添加密钥管理模块，实现Snort对IPv6报文中ESP扩展报头的解析，管理其产生的密钥。给出一种面向ESP的入侵检测系统模型，以验证IPv6加密通信入侵检测的可行性，并给出实验验证过程。

关键词 入侵检测系统；IPv6协议；封装安全有效负载

分类号 TP309

**DOI:**

通讯作者:

作者个人主页: 王相林;李蓓蕾