通信学报
Journal on Communications
主管单位：中国科学技术协会
主办单位：中国通信学会

陶建喜1,3,4,周立2,周舟1,4,杨威1,4,刘庆云1,4,杨嵘1,4.非对称路由环境下SYN flood攻击防御方法[J].通信学报,2013,(Z1):285~291

非对称路由环境下SYN flood攻击防御方法

SYN flood attack defense strategy for asymmetric routing

投稿时间： 2013-08-06

DOI：10.3969/j.issn.1000-436x.2013.Z1.038

中文关键词：SYN flood 非对称路由 连接管理 SYN分组比例 目的地址熵

英文关键词:SYN flood asymmetric routing connection management SYN packet rate destination IP address entropy

基金项目:国家高技术研究发展计划（“863”计划）基金资助项目（2011AA010703）；国家“242”信息安全计划基金资助项目（2012A99）；中国科学院战略性先导科技专项基金资助项目（XDA06030200）；国家自然科学基金资助项目（61303260）

作者	单位
陶建喜1,3,4，周立2，周舟1,4，杨威1,4，刘庆云1,4，杨嵘1,4	1. 中国科学院 信息工程研究所，北京 100093；2. 国家计算机网络应急技术处理协调中心，北京100029；3. 北京邮电大学 计算机学院，北京 100876；4. 信息内容安全技术国家工程实验室，北京100093

中文摘要:

针对现有网络安全设施无法有效防御非对称路由环境下流量规模较大的SYN flood攻击的问题，对SYN flood攻击检测技术和TCP连接管理策略进行研究，提出了一种轻量级攻击检测和混合连接管理策略相结合的防御方法，利用SYN分组比例和目的地址熵进行攻击检测，并根据检测结果对基于SYN的连接管理策略和基于数据的连接管理策略进行灵活切换。实验证明该防御方法能有效地减轻SYN flood攻击对网络安全设施的影响。

英文摘要:

In order to resolve the problem that existing network security facilities can’t defend against large-scale SYN flood attack under asymmetric routing environment, attack detection technology and connection management strategy were researched, and a defense architecture combining a light-weight detection method with a hierarchical connection management strategy was presented. The detection method uses SYN packet rate and destination IP address entropy, and the hierarchical connection management strategy consists of a method based on SYN packet and a method based on data packet. The experimental results show that this proposed method can mitigate the influence brought by SYN flood attack.

查看全文 查看/发表评论 下载PDF阅读器

关闭