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

王丽娜1,2,张浩1,2,余荣威1,2,高汉军1,2,甘宁1,2.基于VPE的可信虚拟域构建机制[J].通信学报,2013,(12):167~177

基于VPE的可信虚拟域构建机制

Building mechanism of trusted virtual domain via the VPE

投稿时间： 2013-01-04

DOI：10.3969/j.issn.1000-436x.2013.12.019

中文关键词：虚拟以太网 边界安全策略 可信虚拟域加入协议 可信虚拟域管理协议 跨域访问协议 分离式设备驱动

英文关键词:virtual private ethernet border security strategy TVD join protocol TVD management protocol inter-TVD access protocol separate device driver

基金项目:国家自然科学基金资助项目(61373169, 61103219, 61303213)；教育部博士点基金优先发展领域基金资助项目(20110141130006)

作者	单位
王丽娜1,2，张浩1,2，余荣威1,2，高汉军1,2，甘宁1,2	1. 武汉大学 空天信息安全与可信计算教育部重点实验室，湖北 武汉 430072；2. 武汉大学 计算机学院，湖北 武汉 430072

中文摘要:

针对现有可信虚拟域构建方式无法满足云计算灵活配置等特性的问题，结合云计算企业内部敏感数据的防泄漏需求，提出了基于VPE的可信虚拟域构建方法TVD-VPE。TVD-VPE利用分离式设备驱动模型构建虚拟以太网VPE，通过后端驱动截获数据分组，并进行边界安全策略检查，最后对满足策略的数据帧进行加密。同时，还设计了可信虚拟域加入/退出协议确保用户虚拟机安全加入/退出，为边界安全策略的部署设计了面向可信虚拟域的管理协议，同时为高特权用户的跨域访问设计了跨域访问协议。最后，实现了原型系统并进行了功能测试及性能测试，测试结果证明本系统可以有效地防止非法访问，同时系统对Xen的网络性能的影响几乎可以忽略。

英文摘要:

Due to lack of flexible networking control, most exiting trusted virtual domain deployment approaches fail to provide elastic and secure interconnection. A trusted virtual domain architecture TVD-VPE was proposed in cloud computing enterprises which greatly enhances sensitive data protection. TVD-VPE constructs a virtual private ethernet based on separate device driver, VPE captures network packets at the backend driver and checks whether the packets comply with border security strategy, and data frames are encrypted among trusted virtual domains to ensure the security of sensitive data. Simultaneously, four protocols were proposed, TVDJOP/TVDEXP protocol for any new VM joining in or exiting TVD securely, TVDMP protocol for deploying border security strategy, and Inter-TVD protocol for authorizing cross-domain access. Finally, the prototype system and tests of its functionality and performance were implemented. The experiment results reveal that the architecture can effectively prevent unauthorized access between these trusted virtual domains, while introduces little overhead to Xen network performance.

查看全文 查看/发表评论 下载PDF阅读器

关闭