前瞻科技與管理　5卷2期，1-22頁（2015年11月）
Journal of Advanced Technology and Management Vol.5, No.2, 1-22 (November, 2015)
DOI: 10.3966/222014242015110502001

運用軟體定義網路提升網路入侵防禦的管理

梁德昭[1,*]　黃翊宸[2]

[1]淡江大學資訊管理學系副教授
[2]淡江大學資訊管理學系碩士生

摘要

在網路的世界中，防杜外部入侵與內部網路攻擊所造成的災害一向是重要的議題，如何有效地防範並減少網路攻擊成功的機會，至關重要。早期通常仰賴入侵偵測或入侵防範系統來預警，如今有了軟體定義網路（Software Defined Network, SDN）的架構提出，使得原本的網路架構得以配合自行開發之SDN應用程式，能夠有效而及時地針對潛在的網路攻擊進行防衛及因應處置。

本文提出將入侵偵測系統（Intrusion Detection System, IDS）或入侵防範系統（Intrusion Prevention System, IPS）配合SDN應用程式自動化的構想，用以優化IDS或IPS告警程序，並縮短網管人員進行防火牆等網路設備修訂網路政策所需時間，進而降低網路攻擊成功之機會，同時封鎖網路攻擊封包來源，使攻擊封包在進網路交換器傳送前即被丟棄，從而大量減少網路攻擊封包所消耗的頻寬。

關鍵詞：Open vSwitch、OpenDaylight、OpenFlow、入侵偵測系統、軟體定義網路

* 通訊作者：梁德昭
電子郵件：tcliang@mail.im.tku.edu.tw

前瞻科技與管理　5卷2期，1-22頁（2015年11月）
Journal of Advanced Technology and Management Vol.5, No.2, 1-22 (November, 2015)

Employing Software Defined Network to Reduce Management Efforts of Instruction Prevention

Te-Chao Liang[1,*], Yi-Chen Huang[2]
[1]Associate Professor, Department of Information Management, Tamkang University
[2]Graduate Student, Department of Information Management, Tamkang University

Abstract

In cyber world, it has been always an important issue that to prevent disasters from external intrusion as well as internal attacks. How to effectively prevent from cyber attacks or reduce the damage of a successful cyber attacks are then critical to be explored. Usually they are rely on intrusion detection or intrusion prevention systems for early warning, however, a software-defined network (SDN) architecture has been proposed such that a self-developed SDN application program can be employed to effectively defense and timely response to the potential network attack.

In this article, a concept that using Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) application with SDN automation is proposed. It can optimize IDS/IPS alert procedures and shorten the time of amending network security policy on network equipment such as firewall and routers. It is supposed to reduce the possibility of a successful cyber attack than the usual way. Furthermore, SDN cooperated with Open Flow can also discard attack packets in advance before they can enter into network switch, this will reduce the bandwidth consumed by network attacks.

Keywords: Open vSwitch, OpenDaylight, OpenFlow, intrusion detection system, software defined network

* Corresponding Author: Te-Chao Liang
E-mail: tcliang@mail.tku.edu.tw