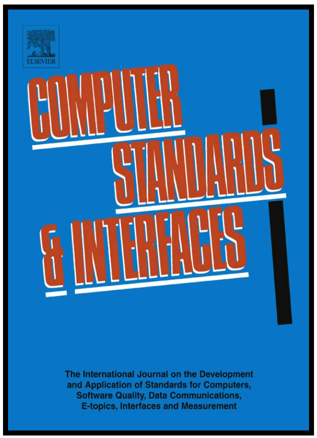
ELSEVIER
COMPUTER
STANDARDS
& INTERFACES
The International Journal on the Development and Application of Standards for Computers, Software Quality, Data Communications, E-topics, Interfaces and Measurement

www.elsevier.com

# Challenges of and Solution to the Control Load of Stateful Firewall in Software Defined Networks

Thuy Vinh Tran, Heejune Ahn

PII: S0920-5489(17)30044-2
DOI: http://dx.doi.org/10.1016/j.csi.2017.01.012
Reference: CSI3197

To appear in: *Computer Standards & Interfaces*

Received date: 16 April 2016
Revised date: 20 January 2017
Accepted date: 26 January 2017

Cite this article as: Thuy Vinh Tran and Heejune Ahn, Challenges of anc Solution to the Control Load of Stateful Firewall in Software Defined Networks *Computer Standards & Interfaces,* http://dx.doi.org/10.1016/j.csi.2017.01.012

# Challenges of and Solution to the Control Load of Stateful Firewall in Software Defined Networks

Thuy Vinh Tran, Heejune Ahn*

Seoul National University of Science and Technology, Electrical & Information Engineering department, 232 Gongneung-ro, Nowon-gu, Seoul, South Korea

tranvinhthuy@seoultech.ac.kr (T. Tran)

heejune@snut.ac.kr (H. Ahn)

*Corresponding author. Tel.: +82 10 6886 6543

## Abstract

Whereas SDN (Software Defined Networks) provides the opportunity for the flexibility of network configuration, the introduction of controller systems raises new issues about developing firewall system design, such as controller attack, rule setup, and communication overhead for control messages. Especially, the delay and overload for dynamic control of stateful firewall are serious bottlenecks. This paper examines the current challenges and their origins, and presents a comprehensive solution to the key operational steps: topology-based selective filtering rules for setup and maintenance stage, three-layer rule structure for in-switch flow tables, and controller attack protection based on adaptive host connection tracking with multiple hashing queues named FlowTracker algorithm. The experiment results using multiple OVS switches and virtual hosts in GENI testbed demonstrate FlowTracker succeeds in monitoring all network connections and completely profiling host normal routine with acceptable latency increment (170ms). Moreover, by utilizing multiple request queues, the proposed DoS attack detection algorithm reduce the response time to DoS 5 to 20 times less than using a single queue.

**Keywords**: Software defined networking; SDN security; stateful firewall; DoS attack

## 1. INTRODUCTION

Software Defined Networking (SDN) [1] introduces the possibilities of faster evolution, hardware independence and centralized-control network. These objectives are realized by decoupling network control functions from packet forwarding. This decoupling feature of SDN impacts firewall system design, and enables the firewall logic and policies of firewalls to be implemented in the controller side whereas the switches execute the switching and filtering operation according to the configured rules. However, the separation of control and data plane causes an increase in the communication bandwidth and controller load to set up the firewall rules.

In the case of a ‘stateless’ firewall, the controller can pre-install the firewall rules in the flow table of each switch, so that the forwarding switch can perform stateless packet filtering without interfering the controller on runtime. On the other hand, a ‘stateful’ firewall requires far more interaction between the control plane and data plane for managing connections. OpenFlow SDN switches utilize the ‘flow’