Quick Blocking Operation of Firewall System Cooperating with IDS and SDN

Yusei Katsura*, Pranpariya Sakarin**, Nariyoshi Yamai***, Hiroyuki Kimiyama****,
Vasaka Visoottiviseth**

** Graduate School of Science and Technology, Nara Institute of Science and Technology, Nara, Japan*

*** Faculty of Information and Communication Technology, Mahidol University, Nakhon Pathom, Thailand*

**** Institute of Engineering, Tokyo University of Agriculture and Technology, Tokyo, Japan*

***** School of Informatics, Daido University, Nagoya, Japan*

katsura.yusei.ky6@is.naist.jp, pranpariya.sak@gmail.com, nyamai@cc.tuat.ac.jp, kimiyama@daido-it.ac.jp, vasaka.vis@mahidol.edu

***Abstract*— Firewalls, intrusion detection systems (IDSs), and intrusion prevention systems (IPSs) are normally used to filter anomaly traffic and prevent attacks from the Internet. However, preconfiguring firewalls and IDS on multiple devices is an exhausting work for the network administrators. Software Defined Network (SDN) is the concept proposed to make the network management easier by using an SDN controller and SDN switches. In this research, we propose a system that integrates IDS together with SDN in order to block anomaly traffic in a fast manner. Once the IDS detects anomaly traffic, it will send an alert message back to the SDN switch. Then, this alert message will be sent as a PacketIn message to the SDN controller in order to set up rules to block the attack. To evaluate our system, we conduct experiments to compare the performance of our proposed system using syslog and Socket API with the existing method that uses REST API, and another comparison method, in term of processing time. Our experiment results confirm that our proposed method can result in the smaller latency and can quickly block malicious traffic.**

***Keyword*— Firewall, Intrusion Detection System, Software Defined Network, OpenFlow**

Yusei Katsura received B. Info. Env. from Tokyo Denki University, Japan in 2019. He was a research student at Tokyo University of Agriculture and Technology, Japan in 2020. He is currently a Master student at Nara Institute of Science and Technology. His research interest is computer network.

Pranpariya Sakarin received B.Sc. from Faculty of ICT, Maihdol University, Thailand in 2019. She has worked for Refinitiv Software (Thailand) company limited as a Technical Specialist since 2020. Her research interest is computer network.

Nariyoshi Yamai received the B.E. and M.E. degrees in electronic engineering and the Ph.D. degree in information and computer science from Osaka University in 1984, 1986, and 1993, respectively. After working at Nara National College of Technology, Osaka University, and Okayama University, he has been a Professor at the Institute of Engineering, Tokyo University of Agriculture and Technology since April 2014. His research interests include distributed systems, network architecture, and Internet. He is a member of IEEE CS, IEEE ComSoc, IEICE and IPSJ.

Hiroyuki Kimiyama is a Professor in Daido University, Japan. He received B.E. and M.E. from Tohoku University, Japan, in 1988 and 1990, respectively. In 2010, he received Ph.D. from the graduate school information system, the University of Electro-Communications, Japan. He joined NTT corporation in 1990 and became a professor at Tokyo Denki University in 2016. Since 2019, he become a professor at School of Informatics Department of Information Systems, Daido university, Japan. His research interest is high-speed real-time distributed processing. He is a member of ACM, IPSJ and IEICE.

Vasaka Visoottiviseth is an associate professor at Mahidol University, Thailand. She received her Ph.D. degree in computer engineering from Nara Institute of Science and Technology (NAIST), Japan in 2003, M.E. and B.E. degree from Tokyo University of Agriculture and Technology (TUAT), Japan in 1999 and 1997, respectively. Her current research interests are mobile and wireless computing, Internet traffic measurement, and network security. She is a member of IEEE since 1998.