A Dynamic IPS Allocation Scheme using OpenFlow for Economical Secure Networking

Pichaya Kietkaroon, Yusuke Watanabe,
Junichi Murayama
School of Information and Telecommunication Engineering
Tokai University
2-3-23 Takanawa, Minato-ku, Tokyo, 108-8619, Japan

Takahiro Hamada,
Yuminobu Igarashi

NTT Secure Platform Laboratories
3-9-11 Midori-cho, Musashino-shi, Tokyo 180-8585, Japan

***Abstract*—OpenFlow is attractive as a base of the data center network. IPS is also attractive as a security appliance. Then combining Openflow with IPS is an important issue. The simple solution is to screening all flow in an OpenFlow network using IPS. However, it may degrade throughput performance or increase equipment cost. In order to solve this problem, we propose a novel IPS allocation scheme. In this scheme, at first, security level is checked on each flow. Then a forwarding path is selected from IPS-involved path or cut-through path. From the result of the experiments, we can increase the number of cut-through flows when the number of secure flows is large. Consequently, we can increase the whole network throughput without any additional equipment cost.**

Keywords—OpenFlow, IPS, security, flow control, cut-through

I. INTRODUCTION

The security awareness of data center and network isolation demand from the enterprise customers have been growing up [1]. Virtual Local Area Network (VLAN) is an attractive technology to respond to this demand. However, the shortage of VLAN-ID has been pointed out [2] for deploying to huge data centers. As the isolation technology, we focus on the OpenFlow [3]-[5] in place of VLAN.

OpenFlow introduces the flow-based forwarding paradigm rather than the Internet's datagram-based one. Here flow represents the multiple packets that are transferred continuously between the same source and destination. Although flow granularity is variable, it is typically expressed as five tuples: the source/destination IP addresses, Protocol Type and the source/destination TCP/UDP port numbers [3].

In enterprise networks, Intrusion Prevention System (IPS) is necessary to filter out unauthorized accesses. OpenFlow networks as data center networks also need IPS [6]-[7]. However, IPS may lose the merit of high throughput/cost ratio of OpenFlow. For example, deploying many IPSs may achieve high throughput but increase the equipment cost. Similarly, sharing an IPS with all flows reduces cost but may degrade throughput.

In order to solve this problem, we propose a dynamic IPS allocation scheme. In this scheme, a single IPS is deployed and shared by multiple flows. At first, all the flows share the IPS. Then, IPS classifies flow into some security levels: black, grey and white. Next, a flow path is selected for each flow. A black (malicious) flows is filtered out. A grey (suspicious) flow is forwarded via IPS. A white (secure) flow is forwarded along the cut-through path. IPS and OpenFlow controller cooperate with each other to change the flow path. According to the simulation result, it can achieve high performance/cost ratio when white flows are dominant.

The rest of this paper is organized as follows: Section II introduces basic IPS allocation schemes. Section III represents the proposed dynamic IPS allocation scheme with path control technology. Section IV shows the evaluation and the results. Finally Section V concludes this paper with brief summary.

II. BASIC IPS ALLOCATION SCHEME

The network model assumed in this paper is shown in Fig.1. A data center deploys an OpenFlow network. The network comprises OpenFlow switches, OpenFlow controllers and transmission links. An OpenFlow switch accommodates multiple physical interface ports and transfer flows between those ports using an OpenFlow switch table. An OpenFlow controller controls an OpenFlow switch table in an OpenFlow switch. This network accommodates multiple enterprise customers. In order to meet the high security requirement, customers are isolated and IPSs are deployed. The following two basic schemes are applicable to this model:

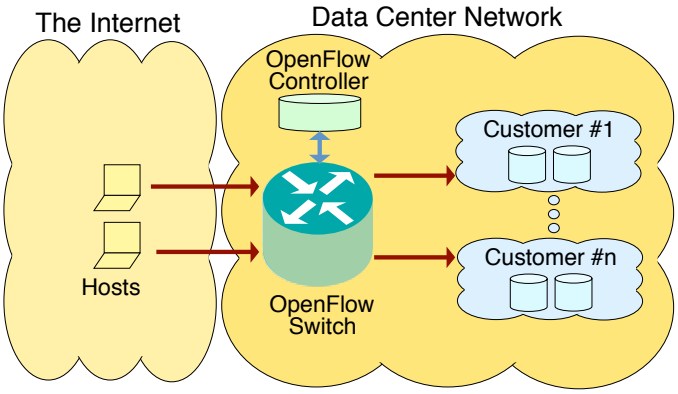

Fig. 1. Network Model

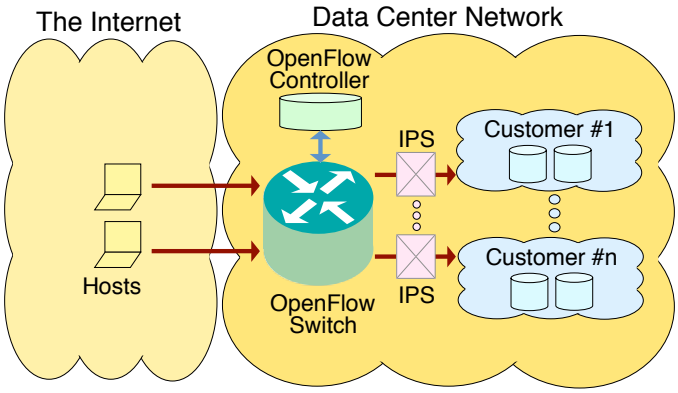

Fig. 2. Exclusive IPS Allocation Scheme

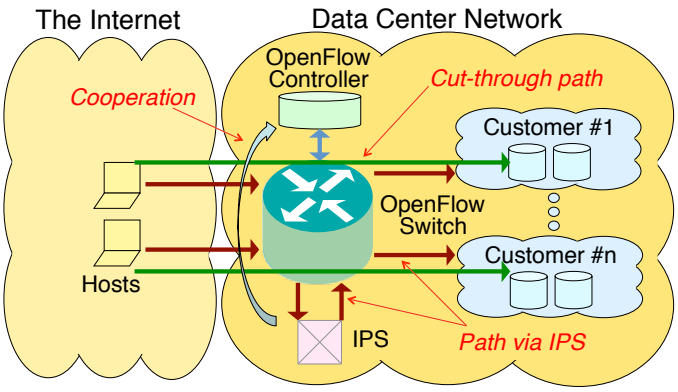

Fig. 4. Proposed Dynamic IPS Allocation Scheme

A. *Exclusive IPS Allocation Scheme*

IPSs are allocated exclusively to each customer as shown in Fig.2. Since each customer can fully use both link bandwidth and IPS capability, they can communicate at high speed. However, their equipment cost becomes too high.

B. *Shared IPS Allocation Scheme*

IPSs are allocated to share with customers as shown in Fig.3. The equipment cost of IPS can be low. However, customer throughput will be degraded if many customers communicate simultaneously.

III. PROPOSED IPS ALLOCATION SCHEME

The proposed IPS allocation scheme is depicted in Fig.4. In this scheme, IPS classifies flows into some security levels: black, grey and white. Then a flow path is replaced according to its flow security level. Black (mallicious) flows are filter out at the IPS. Grey (suspicious) flows are still transferred via IPS. White (secure) flows are transferred along the cut-through path.

At the initial communication stage, each flow is transferred via IPS and examined in detail by IPS. In addition, security level of each flow is determined by the IPS using a flow-analysis log. For example, a long- period flow in which any anomaly events are not detected is classified into a white flow. If a flow cannot be specified as white, it is classified into a grey flow. In addition, if a flow is used obviously for illegal access such as port scan, it is classified into a black flow. After the classification, flow path is replaced according to its security level.

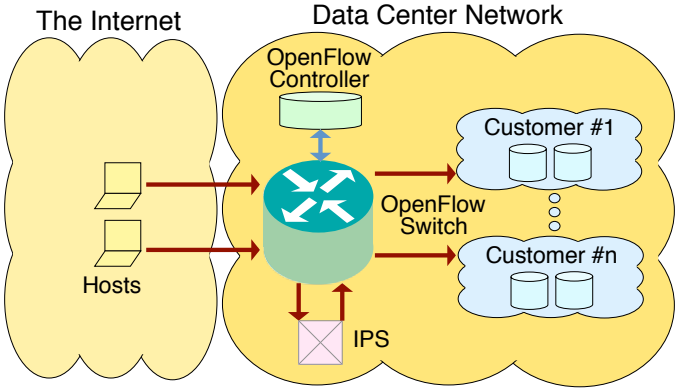

Fig. 3. Shared IPS Allocation Scheme

This path control is achieved by means of the cooperation between an IPS and OpenFlow controller. An IPS that detects white flow sends signals to the OpenFlow controller. Then the controller modifies the flow table in the OpenFlow switch. Finally a flow path via IPS is replaced with a cut-through path according to modification of the OpenFlow switch table.

In the normal condition of network operation, white flows are dominant. In this condition, the number of cut-through flows can be increased. Then the whole network throughput can be also improved without any additional equipment cost.

On the other hand, in the anomaly condition, back and grey flows may be dominant. In this condition, most flow should be reached to IPS. Then the network throughput may be degraded.

IV. EVALUATION

The proposed scheme was evaluated. First, its feasibility was examined by means of the experimental implementation. Then, its throughput was estimated by means of calculation.

A. *Feasibility*

A prototype of the proposed system was implemented using tools listed in Table I. The cooperation behavior between the IPS and OpenFlow controller was confirmed using this prototype.

TABLE I. TOOLS FOR FEASIBILITY TEST

Equipment	Implementation Tool
OpenFlow controller	Trema (ver.0.4.4) [10]
OpenFlow switch	OpenvSwitch (ver.2.1.3) [11]
IPS	Snort (ver.2.9.5.5) [12]
Flow Analysis Function in IPS	td-agent (ver.0.10.55) [13]
Hosts	netperf (ver.2.6.0) [14]

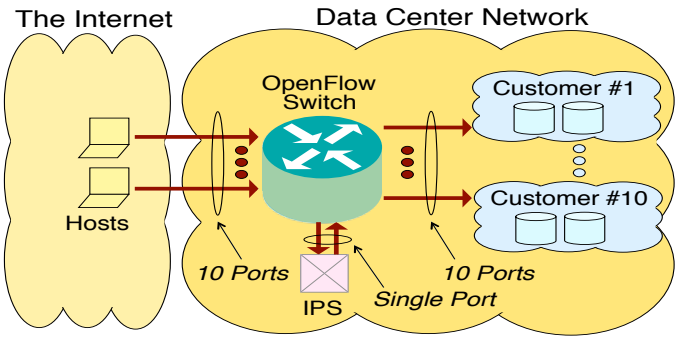

Fig. 5. Network Model for Evaluation

B. *Throughput*

The proposed scheme deploys two kinds of paths. One is a path via IPS and the other is a cut-through path. In this scheme, the link that connects an OpenFlow switch and IPS may become throughput bottleneck because it is shared among all customers. If the number of black and grey flows is small, only a few flows are transferred simultaneously using this link. However, if it is large, many flows are concentrated on this link and some flows may be overflowed.

We estimated the normalized throughput by means of numerical calculation using the network model shown in Fig.5. The calculation conditions are summarized in Table II. The results are shown in Fig.6. When the ratio of black and grey flows to the whole flows is less than 8 percent, 100 percent throughput is maintained. However, when it becomes more than 8 percent, throughput is degraded. This threshold depends on the number of the customer ports that share the IPS.

V. CONCLUSION

Deploying IPS to OpenFlow networks is an important issue to improve security. The conventional basic IPS allocation schemes such as exclusive allocation and shared allocation are not necessarily effective from the viewpoint of throughput performance and equipment cost. In order to solve this problem, we propose a dynamic IPS allocation scheme. In this scheme, flows are classified into some security levels. Then a secure flow path via IPS is replaced to a cut-through path. When secure flows are dominant, IPS load reduces and thus high throughput is maintained. As the consequence, the ratio of performance to cost can be kept high. For future work, we are planning to evaluate throughput performance and functional feasibility in various conditions.

TABLE II. CALCULATION CONDITIONS

Parameters	Value
Number of Interface Ports for Customers	10 ports
Number of Interface Ports for IPS	1 port
Bandwidth of each Interface Port	1 Gb/s
Aging Time of Flow Table	1000 sec
Flow Analysis Time	10 sec
Input Load of Interface Port for Customer	100%
Ratio of Black and Grey Flows to the whole Flows	0% - 20%

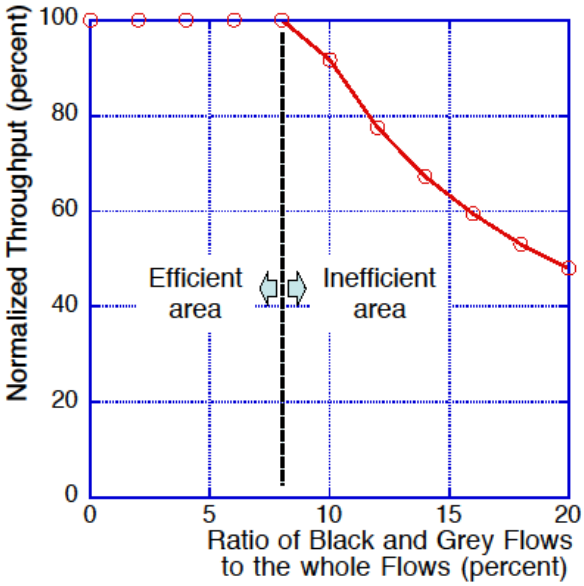

Fig. 6. Result of Numerical Calculation

REFERENCES

[1] T. Tanaka, S. Kawamoto and K. Uehara, “Proposal on Integrated Operations Management Technology for Cloud Infrastructure,” IEICE technical report, CPSY2011-41, October 2011. (in Japanese)

[2] H. Tanabe, K. Akashi, S. Uda, Y, Shinoda and S. Miwa, "Technical trend and interoperability issue of data center network," IEICE technical report, IA2011-62, January 2012. (In Japanese)

[3] K. Okada, Y. Sekiya and Y. Kadobayashi, "A Design Consideration for SDN-based Internet eXchange," Proc. of the Internet Conference, pp.43-49, 2013. (In Japanese)

[4] F. miura and H. Inai, "A Network Scan Detection Algorithm : Using Dynamic Threshold," IEICE technical report, IA-2011-52, December 2011. (In Japanese)

[5] R. Kanamori, N. Motoki, Y. Kawahashi and K. Tsukada, "Gateway management system based on traffic pattern with source address routing," IN2008-90, December 2008. (In Japanese)

[6] M. Hanaoka, K. Kono T. Hirotsu, ”Brownie: Collaboration of Network Intrusion Detection Systems,” IPSJ SIG Notes 2009-OS-111(4), 1-8, April 2009. (In Japanese)

[7] "Trema Full-Stack OpenFlow Framework in Ruby and C," <https://github.com/trema/trema>, January 2015 (Access).

[8] "Open vSwitch: Production Quality, Multilayer Open Virtual Switch," <http://openvswitch.org/>, January 2015 (Access).

[9] "Snort," < https://www.snort.org/>, January 2015 (Access).

[10] "Fluentd: Fluentd is an open source data collector for unified logging layer," < http://www.fluentd.org/>, January 2015 (Access).

[11] "Nteperf: Welcome to the Netperf Homepage," <http://www.netperf.org/netperf/>, January 2015 (Access).