Methodology for Improving Performance of Traffic Control System Through Processing Traffic Control Policies Sequentially

Sang Wan Kim , Joon Kyung Lee,
Dong Won Kang
Next Generation Communication Research Dep.
ETRI
Gajongdong Yusonggu Deajon, Republic of KOREA
wanni@etri.re.kr, leejk@etri.re.kr, dwkang@etri.re.kr

Sang Ha Kim
Department of Computer Engineering
Chungnam National University
Gungdong Yusonggu Deajon, Republic of KOREA
shkim@cnu.ac.kr

Abstract— **This paper relates to a traffic control system, and more particularly, to a technique for reducing the load of a traffic control system that has to process a large capacity of traffic on a high-speed line, through policy establishment sequentially by a policy server. Among high-speed data transmission technologies, a traffic control system for internet traffic control on a high-speed line basically requires high performance capable of processing a large capacity of traffic. However, in order to process a large capacity of traffic on a high-speed line, a high performance processor for traffic control is also needed. However, such a high performance processor increases the cost of the traffic control system. For this reason, this paper suggest a method for reducing the load of a traffic control system by allowing the traffic control system to define policies for processing traffic and perform the policies sequentially. The paper's suggesting method include controlling input volume of traffic to the traffic control system based on a filter policy , a system policy, a common service policy, and a subscriber policy in this order, which are established by the traffic control system, according to characteristics of the packet. Therefore, by processing policies sequentially, it is possible to in advance prevent a traffic control system from processing unnecessary traffic. Also, by differentiating policies to be performed for each subscriber and establishing policy layers requiring a relatively long time to process traffic at later stages, it is possible to reduce the load of the traffic control system upon processing traffic and accordingly improve the performance of the traffic control system**

Keywords-Internet; Traffic Control; Traffic Control Policy; Network Control

I. INTRODUCTION

Many researchers have studied the network policy issues. Cataldo Basile proposed the model for policy representation to adopt policy in the enforcement elements independently [1]. Ehab et al. described Firewall policy management and a model to simplify the management of firewall policy [2]. Kanada proposed two rule-based building block architecture s for policy-based network control [5][6]. And there are some papers focused on the issues about management of policy rule [7][8][9][10]. Jan van Lunteren proposed the scheme to reduce the complexity of a classification rule set and storage requirement [3]. But, in this paper, we will focus on a scheme using sequential policy set to reduce traffic volume which is processed for a long time in traffic control system. So, we propose a new methodology to increase the performance of traffic control system with policy unit which process input traffic sequentially.

Recently, the demand for the network appliance on network is increased to solve the problems due to the excessive Internet traffic loads. In the network environments, high-speed data transmission technologies have been developed to transmit a large amount of information quickly and accurately. With help of development of circuit and component technologies, free frequency bands without requiring specific permissions, popularization of portable computers, etc., technologies for transmitting data at high speed under a mobile environment have been developed and used. Among such high-speed data transmission technologies, a traffic control system for the high-speed Internet line requires basically high performance which is capable of processing a large capacity of traffic.

We developed an Internet traffic control system in order to provide common platform which can control the traffic in real-time. Our system, which is named High-speed Internet Traffic Control and Analysis Platform (HITCAP), can collect and analysis not only with the header information of a packet but also payload of a packet which is including site address, email, Voice over IP(VoIP) and even metadata which includes optional keyword: information of the receiver or the sender and attached files. Our system distinguishes and classifies the traffic of the applied service with the advanced technology, DPI (Deep Packet Inspection). It also lets system manager to control and analyze the chosen service with DPP (Deep Packet Processing). However, in order to process a large amount of traffic packets on a high-speed line, a high-performance H/W processor for traffic control is also needed. Such a high performance H/W processor increases the cost of the traffic control system. For this reason, this paper suggest a new method for reducing the load of a traffic control system by allowing the traffic control system to define policies for processing traffic and perform the policies sequentially.

The proposed methodology include controlling a packet of the traffic control system based on a filter policy, a system policy, a common service policy, and a subscriber policy in this order, which are established by the traffic control system according to characteristics of the packet. Therefore, by processing policies sequentially, it is possible to in advance prevent a traffic control system from processing unnecessary traffic. Also, by differentiating policies to be performed for each subscriber and establishing policy layers requiring a relatively long time to process traffic at later stages, it is possible to reduce the load of the traffic control system upon processing traffic and accordingly improve the performance of the traffic control system. Section II describes developed traffic control H/W system, Section III proposes main idea, and then, we perform the evaluation test in Session IV. Finally, Session V concludes this paper.

II. HITCAP SYSTEM

A. HITCAP H/W PLATFORM

HITCAP system, which we are developing, can process the Internet traffic. HITCAP can classify the high-speed traffic with the Intelligent DPI Device. If input packet is classified by application classification engine as an interested traffic then classification device sends specific service traffic to the DPP (Deep Packet Processing) [12] module.

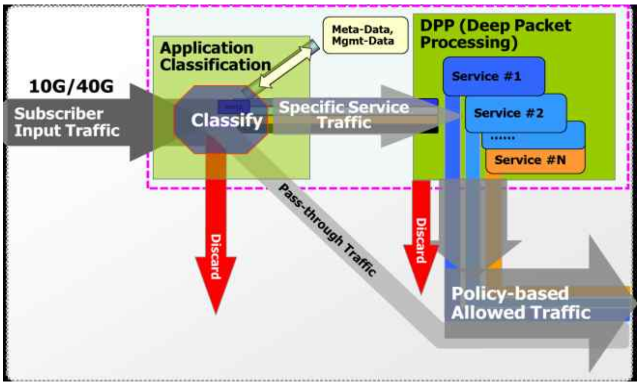


Figure 1. Concept of developed Hardware Platform

Figure 1 presents the concept of HITCAP to process Internet traffic. We implement 2-type of PCI-NIC type HITCAP cards for flexibility, functionality and economic reasons. If we implement on PCI-NIC, it can be installed COTS server without additional cost. If a manager wants to compose the traffic control system using two NICs, the first NIC (HITCAP-X) mainly classifies packets and second NIC (HITCAP-T) processes packets up to Layer 7.

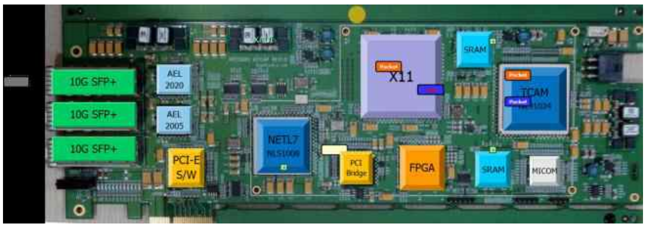


Figure 2. X11 Network Processor based High-speed traffic classification Card

Figure 2 shows a prototype of X11 [10][11]. based high-speed traffic classification card. It uses the systolic type NPU, X11 of Xelerated as network processor [9]. Figure 3 shows OCTEON plus CN5860 based deep packet processing card (HITCAP-T). A user can program c-like syntax and API, but the user must use OCTEON API [12].

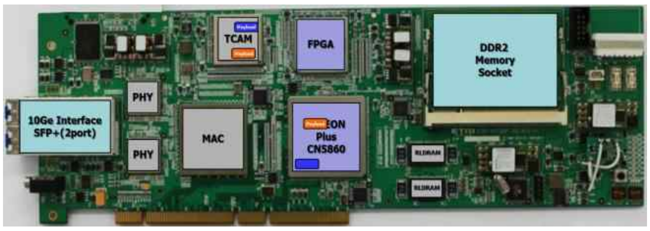


Figure 3. OCTEN CN5860 Network Processor based Deep Packet Processing Card

B. Platform Management System (PMS)

Traffic Control Platform H/W (HITCAP H/W) is managed by the Platform Management System (PMS). All received policy and configuration data are collected by PMS. PMS receives policy from policy server and PMS enforces policy to the adequate HITCAP Hardware [12].

There are some cases of policy enforcement.

- L2~L4 : enforce policy to HITCAP-X only
- L2~L4 with signature :
  -enforce L2~L4 with forward action to HITCAP-X
  -enforce L2~L4 with signature to HITCAP-T

Figure 4 shows Platform Management System (PMS) Configuration and internal modules [12].

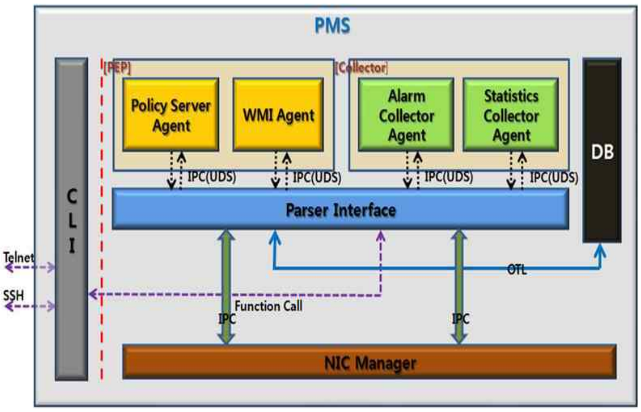
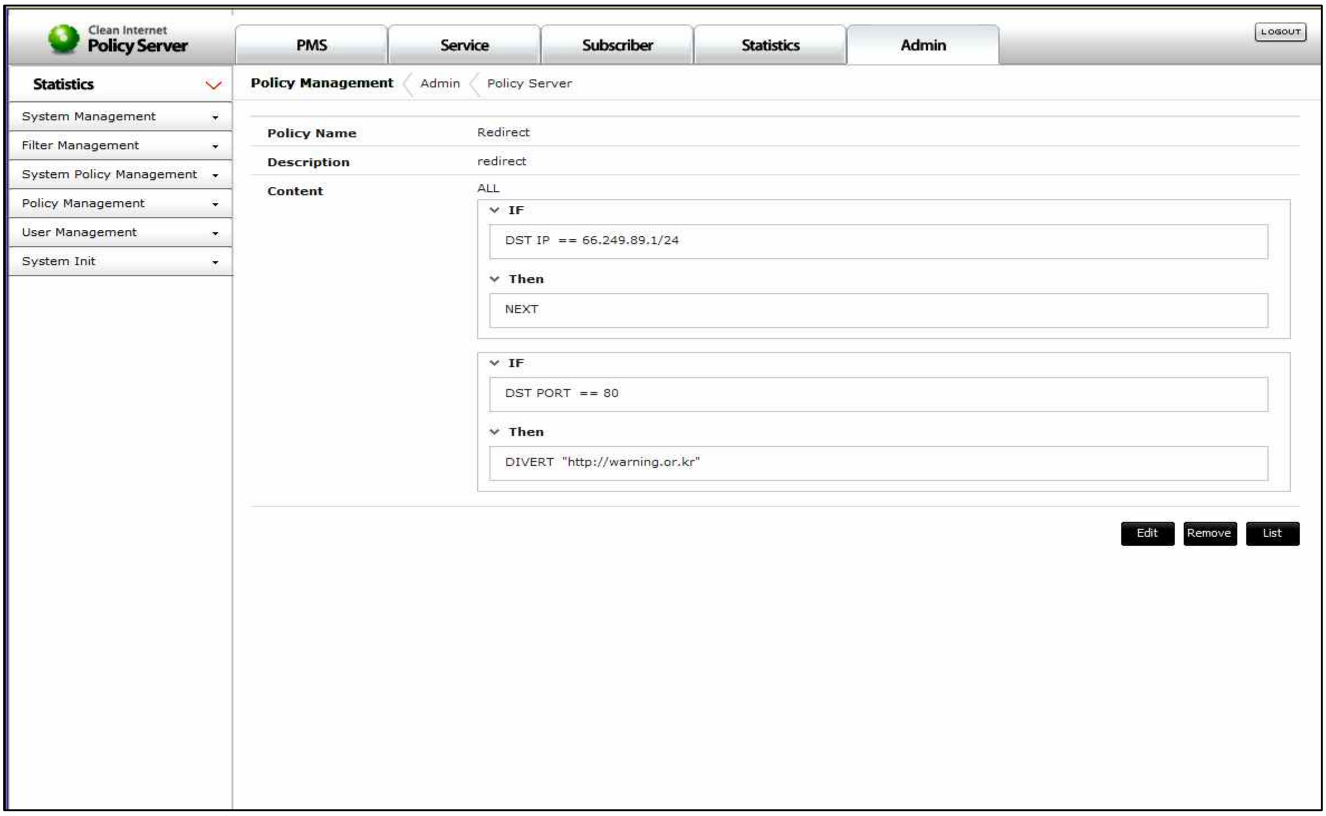


Figure 4. Concept of Policy Management System

C. Policy Server (PS)

The policy server manages policy rules between applications and policy enforcement points like HITCAP-hardware [11]. A manager can easily add and re-configure policies to manage and control traffic, optimization and admission control, etc. A wide variety of interfaces make it easy for manager to integrate the policy server into any type of network service [12]. Figure 5 shows Policy Server (PS) GUI.



Policy Name Redirect

Description redirect

Content ALL

IF

```
DST IP == 66.249.89.1/24
```

Then

```
NEXT
```

IF

```
DST PORT == 80
```

Then

```
DIVERT "http://warning.or.kr"
```

Figure 5. Policy Server Graphic User Interface

III. Processing Traffic Control Policy Sequentially for Improving Performance of the Control Platform

In the traffic control system, we focused the scheme using sequential policy set to reduce traffic volume which is processed for a long time in traffic control system. So, we proposed methodology to increase the performance of the traffic control system with a policy unit, which processes the input traffic sequentially. We define the policy with the 6 types policy layers. Figure 6 is a diagram illustrating a logical hierarchical structure for establishing policies in a traffic control system. In Figure 1, a policy logical structure, which can be established by the traffic control system, logically has 6 policy layers: a filter policy, a system policy, a common service policy, a subscriber policy, a policy group, and a policy. The filter policy is a filtering policy based on a Virtual LAN (VLAN), an IP version, a protocol type, etc., to determine whether to process the received packet. Traffic filtered according to the filter policy is filtered in/allowed to the next stage or filtered out/dropped from the next stage.

The system policy is a policy to protect the traffic control system. The system policy is composed of a trusted user policy and a system status policy. The received packet is allowed or dropped according to whether a user who has requested or transmitted the packet is ‘trusted’ or ‘untrusted’, which is determined from the policy content established in the trusted user policy.

The system policy is a policy to protect the traffic control system. The system policy is composed of a trusted user policy and a system status policy. The received packet is allowed or dropped according to whether a user who has requested or transmitted the packet is ‘trusted’ or ‘untrusted’, which is determined from the policy content established in the trusted user policy.

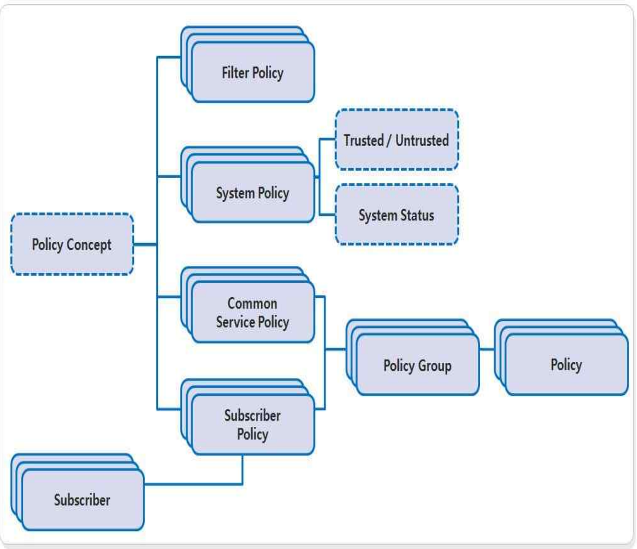


Figure 6. Policy Structure

The system status policy is a system policy for allowing packets if a current amount of traffic is less than the threshold allowable by the system or for controlling the flow of packets based on statistical information about input packets. The system status policy may control the amount of traffic that is input to the traffic control system when a large amount of traffic such as abnormal traffic is generated in a short time.

The policy provides a basic unit policy for controlling packets based on IP addresses, ports and signatures, etc. The policy group, which is a logical group of policies, functions to easily manage the policies, for example, in such a manner as to group predefined policies to create a single policy.

The common service policy, which is a logical group of policy groups, functions to easily manage predefined policy groups. The common service policy may establish a policy that can be applied in common to all input traffic regardless of individual subscribers or systems. For example, in the case of a traffic control system at a college campus, a policy manager can establish a policy for blocking all peer to peer (P2P) traffic, and in this case, the common service policy may define a policy that must be applied to all P2P traffic.

The subscriber policy, which is another logical group of policy groups, is managed by the predefined policy groups. The subscriber policy is applied only to specific subscribers.

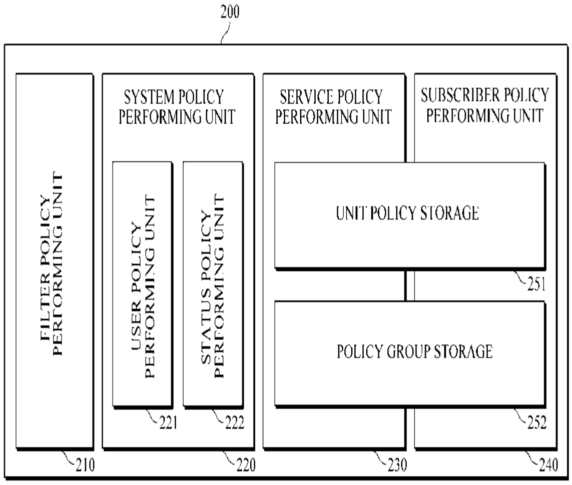

200
FILTER POLICY PERFORMING UNIT
SYSTEM POLICY PERFORMING UNIT
USER POLICY PERFORMING UNIT
STATUS POLICY PERFORMING UNIT
SERVICE POLICY PERFORMING UNIT
SUBSCRIBER POLICY PERFORMING UNIT
UNIT POLICY STORAGE
251
POLICY GROUP STORAGE
252
221
222
210
220
230
240

Figure 7. Policy Processing Module of Control System

Figure 7 is a diagram illustrating an example of a traffic control system 200. In Figure 7, the traffic control system 200 may include a filter policy unit 210, a system policy unit 220, a service policy unit 230, and a subscriber policy unit 240. The filter policy unit 210 filters packets which are input to the traffic control system 200 according to the filter policy based on a Virtual LAN (VLAN), an IP version, a protocol type, etc. The system policy unit 220 may include a user policy unit 221 and a status policy unit 222, and control the filtered packet according to the system policy based on a user's reliability and the amount of traffic. The user policy unit 221 determines whether or not a user who has requested or transmitted the packet is "trusted", and allows the corresponding packets, if the user is "trusted". The status policy unit 222 determines whether a current amount of traffic is less than the threshold allowable by the traffic control system and allows the corresponding packet if the current amount of traffic is less than the threshold. The service policy unit 230 controls all received packets according to the common service policy that is established according to a use purpose of the traffic control system 200. The subscriber policy unit 240 controls the received packet according to the subscriber policy that is established for each subscriber by the traffic control system 200. The service policy unit 230 and the subscriber policy unit 240 may share the unit policy storage 251 and the policy group storage 252. Otherwise the service policy unit 230 and the subscriber policy unit 240 may each include the unit policy storage 251 and the policy group storage 252. The unit policy storage 251 controls the received packet based on the IP address, port, and signature of the packet. The policy group storage 252 which is grouped its unit policies stores in a logical group, creates, and manages all policies that are performed on the traffic control system 200.

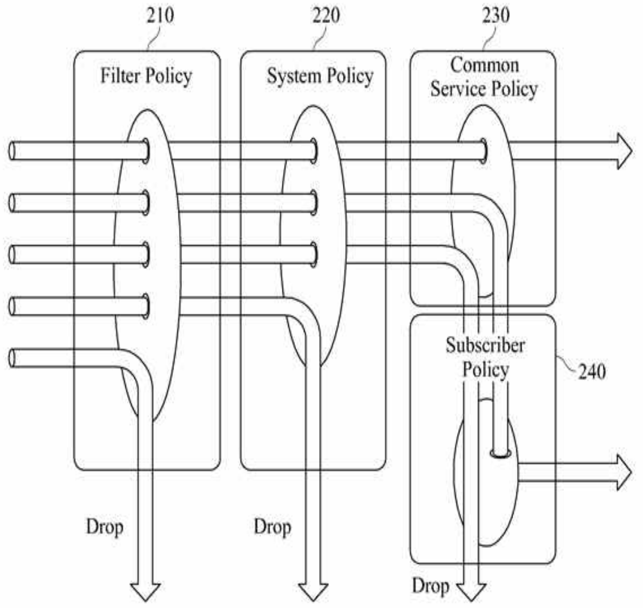


Figure 8. Traffic Processing Flow for controlling traffic with policy

Figure 8 is a view for explaining a method of controlling traffic according to the policies of the traffic control system 200. Figure 8 relates to a procedure for reducing the load of the traffic control system 200 by step-by-step applying logically classified policies. In Figure 7 and 8, when a packet is input to the traffic control system 200, the filter policy block (210) applies the filter policy to filter out the unnecessary packets. The packet, which has passed through the filter policy unit 210, is input to the system policy unit 220. The system policy unit 220 drops untrusted packets (that is, a packet transmitted from an untrusted user) having a disallowable IP address or determines whether a current amount of traffic is more than the threshold and drops the corresponding packet if the current amount of traffic is more than the threshold. That is, the system policy unit 220 drops packets exceeding an allowable amount of traffic, expressed in unit of traffic volume (bps, pps and fps, etc.), thereby could adjust the bandwidth of input traffic.

The packet, that has passed through the system policy per unit 220, is input to the common service policy unit 230. The common service policy unit 230 processes, if the packet satisfies the common service policy. The packet according to the policy established by a policy establisher. The common service policy unit 230 processes packets in advance according to the policy, therefore it reduces traffic load that has to be processed by the subscriber policy unit 240 for performing a policy for each specific subscriber. Finally, the packet, dropped by the common service policy unit 230 is input to the subscriber policy unit 240, and the subscriber policy unit 240 determines whether there is a subscriber policy which the packet satisfies. If there is a subscriber policy which the packet satisfies, the subscriber policy unit 240 controls the packet according to the subscriber policy, and if there is no subscriber policy which the packet satisfies, the subscriber policy unit 240 drops the packet.

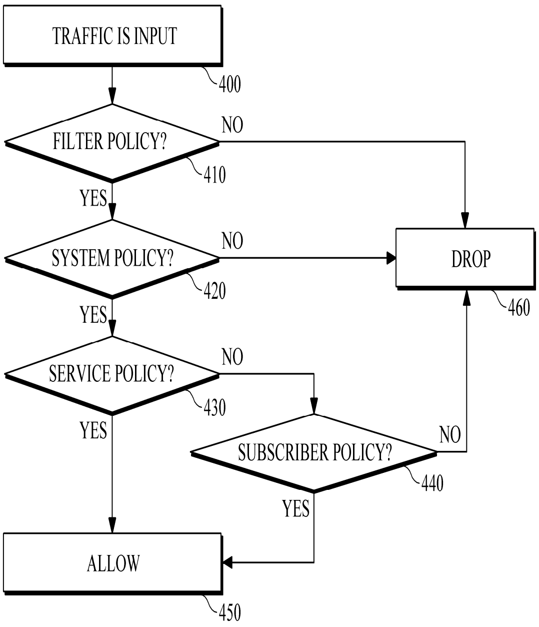


Figure 9. Flowchart of Processing Policy sequentially

Since packets allowed at the earlier stages through policy rules are not subject to policy processing at the later stages, the traffic control load of the traffic control system 200 may be reduced, which leads to improvement of system performance. Figure 9 is a flowchart illustrating another method I of controlling traffic according to a policy of the traffic control system 200 illustrated in Figure 7. In Figure 9, a method of controlling packets sequentially according to the policy processing units (filter policy, the system policy, the common service policy, and the subscriber policy), which are basically set by the traffic control system 200, was described. First, when a packet is input to the traffic control system (400), the packet is filtered according to the filter policy based on a VLAN, an IP version, and a protocol type of the packet (410). If the packet does not satisfy the filter policy, the packet is dropped (460). The packet, which is allowed according to the filter policy, is controlled followed by the system policy based on a user's reliability and the amount of traffic (420). If the packet does not satisfy the system policy, the packet is also dropped (460). All packets, allowed in operation 420 are controlled by the common service policy. Packets which satisfy the common service policy are finally allowed as packets which satisfy all policies of the traffic control system 200 (450). If a packet satisfies the subscriber policy that is established for each subscriber by the traffic control system 200 although the packet does not satisfy the common service policy (440), the corresponding packet is allowed (450), and if the packet does not satisfy the subscriber policy, the packet is finally dropped (460).

IV. Performance Evaluation

In Survey of Packet Classification Techniques, we can find lots of solutions to classify packets [4]. HITCAP H/W system adopts TCAM module for classification and adopts NETL7 coprocessor for Layer 7 depth packet inspection. In the processing time cost aspect, TCAM based classification spends low time. But, Layer 7 depth packet inspection needs lot of time to analysis packets. In H/W performance aspect, how much traffic volume is performed with the Layer 7 depth packet inspection module is a critical issue.

The proposed method composes policy processing units (filter policy, system policy, service policy and subscriber policy). Filter policy and system policy units use TCAM chip to classify traffics but, service policy and subscriber policy use NETL7 coprocessor module to inspection packets. If all input packets processed by using Layer 7 depth packet inspection module (NETL7), traffic control system performance is decreased in direct proportion to the input traffic volume. For the performance evaluation, we set the performance test environment in Figure 9.

Figure 10 is a test environment for the performance evaluation using the packet generator and HITCAP system.

Table I shows the generated packets from the packet generator. The generated packets in the Table I are processed in the filter policy unit and service policy unit. Table II shows the generated packets which are processed in the only service policy unit.

TABLE I. GENERATED PACKETS WHITCH IS PROCESEED IN THE FILTER POLICY UNIT AND SERVICE POLICY UNIT

Policy Rule	**Generated Packet**			
	Packet size	***Generated Port***	***Total Volume***	***Protocol***
Filter Policy Using TCAM	1024Byte	Port 1 : 10Gbps Port 3 : 10Gbps	20Gbps	TCP Stream
Service Policy Using NETL7	1024Byte	Port 2 : 10Gbps Port 4 : 10Gbps	20Gbps	UDP Stream

Table III shows experimental results. When we processed input traffic sequentially using filtered policy unit and service policy unit, HITCAP H/W system handled all input traffic, totally 40Gbps traffic (20Gbps TCP stream and 20Gbps UDP Stream). But, when we processed input traffic using only NETL7 deep packet inspection module, HITCAP H/W system handled half of input traffic, only 20Gbps traffic because that all input traffic could not be handled in the NETL7 deep packet inspection module.

TABLE II. GENERATED PACKETS WHITCH IS PROCESEED IN THE ONLY SERVICE POLICY UNIT

Policy Rule	Generated Packet			
	Packet size	*Generated Port*	*Total Volume*	*Protocol*
All Policy using NETL7	1024Byte	Port 1 : 10Gbps Port 3 : 10Gbps	20Gbps	TCP Stream
	1024Byte	Port 2 : 10Gbps Port 4 : 10Gbps	20Gbps	UDP Stream

TABLE III. EXERIMENTAL RESULTS

Policy Rule	Generated Packet		Processing Results
	Packet size	*Input Volume*	*Processing Traffic Volume*
With Proposed Method	1024Byte	40Gbps	**40Gbps**
Without Proposed Method	1024Byte	40Gbps	**20Gbps**

In this experimental results, we show that this methodology could reduce the load of the traffic control system upon processing traffic and accordingly improve the performance of the traffic control system by differentiating policies which are requiring a relatively long time to process traffic.

V. CONCLUSION AND FUTURE WORK

We focused on a scheme using sequential policy set to reduce traffic volume which is processed for a long time in traffic control system. So we proposed another methodology to increase traffic control system performance with policy unit. We suggest a method for reducing the load of a traffic control system by allowing the traffic control system to process policies sequentially. The paper's suggesting methodology includes controlling input volume of traffic based on the policy processing units, which are established by the traffic control system according to characteristics of the packet. Therefore, by processing policies sequentially, it is possible to prevent a traffic control system from processing unnecessary traffic. Also, by differentiating policies to be performed for each subscriber and policies requiring a relatively long time process, it is possible to reduce the load of the traffic control system. Accordingly, it improves the performance of the traffic control system. This proposed method was adopted at our developed traffic control system, HITCAP.

In the future, there is a need to study about the policy enforcement performance issue. Policy server need to enforce lots of policies to the policy execution point timely.

ACKNOWLEDGMENT

This research result has been funded by KCC (Korea Communication Committee).

REFERENCES

[1] C. Basile, A. Cappadonia, and A. Lioy, “Network-Level Access Control Policy Analysis and Transformation”, IEEE/ACM Transactions on Networking, vol. 19, Issue: 6, pp. 1597-1609, December, 2011

[2] E. Al-Shaer and H. Hamed, “Modeling and management of firewall policies,” IEEE Transactions on NETWROK AND SERVICE MANAGEMENT, vol. 9, Issue: 2, no. 1, pp. 2–10, Apr. 2004

[3] J. van Lunteren and T. Engbersen, “Fast and scalable packet classification,” IEEE J. Sel. Areas Commun., vol. 21, no. 4, pp. 560–571, May 2003

[4] D. Taylor, “Survey and taxonomy of packet classification techniques, ”Comput. Surveys, vol. 37, no. 3, pp. 238–275, 2005.

[5] Y. Kanada, “Two Rule-based Building-block Architectures for Policy-based Network Control”, 2nd International Working Conference on Active Networks (IWAN 2000), Lecture Notes in Computer Science, No. 1942, pp. 195–210, Springer, October 2000.

[6] Y. Kanada, “A Representation of Network Node QoS Control Policies Using Rule-based Building Blocks”, International Workshop on Quality of Service 2000 (IWQoS 2000), pp. 161–163, June 2000.

[7] D. Haixin, W. Jianping and L. Xing, “Policy-based Access Control Framework for Large Networks”, The Proceedings of the IEEE International Conference on Networks ICON 2000 IEEE

[8] J.D. Guttman, Filtering Postures: Local Enforcement for global policies , Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy , May 4-7 1997, pp. 120-129

[9] Cássio Ditzel Kropiwiec, Edgard Jamhour, Mauro Sérgio Pereira Fonseca and Guy Pujolle, “Policy Framework for Capability-Based Firewall Configuration”, Policy 2007

[10] J. P. Albuquerque, H. Krumm and P.L. Geus, “Policy Modeling and Refinement for Network Security Systems”. IEEE 6th International Workshop on Policies for Distributed Systems and Networks, 2005, pp. 24-33.

[11] A. Westerinen, “Terminology for policy-based management,” RFC-3198, Nov. 2001 [Retrieved: March, 2012]

[12] P. Sang-Kil, Y. Sang-Sik and L. Joon-Kyung, “Multi-stage Traffic Control Platform,” ICCS2011, Nov. 2011

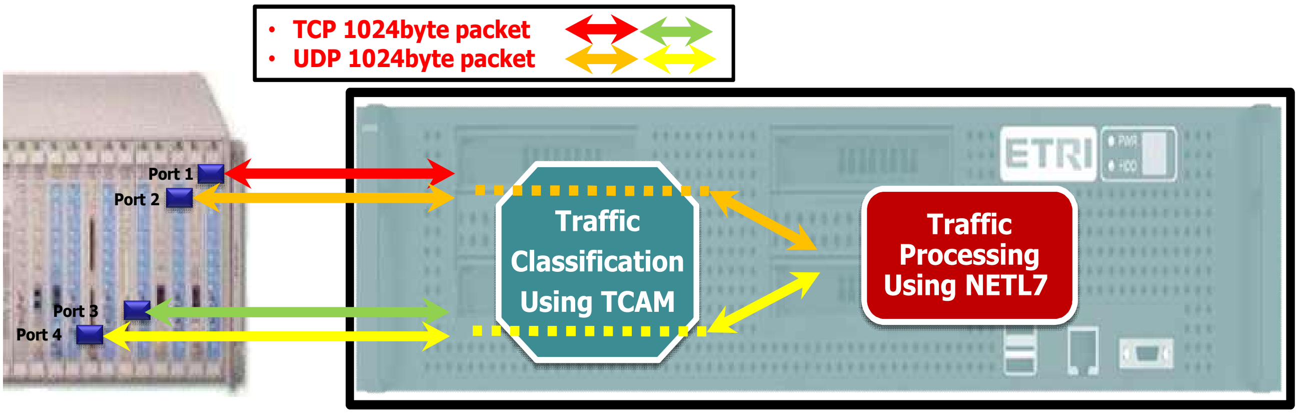


Figure 10. Test Environment for performance evaluation