Chapter 48
Network Traffic and Security Event Collecting System

Hee-Seung Son, Jin-Heung Lee, Tae-Yong Kim and Sang-Gon Lee

Abstract In the beginning stage of the security functions, defending and monitoring was treated as a single solution. Today's security management system has reached at the state of integration of risk management systems and security management system. However, the existing system can have negatively leak of internal information and be inefficient for prevention and post event tracing of security instance. Therefore if we formalize the event information from a variety of security systems and do correlation analysis, we can establish a more active defense. In this paper we built up a developmental environment for network management system using a customized Linux System and several network devices. Using SNMP and SYSLOG, network information are collected from the network equipment and recorded on Maria DB in Linux Server. We also developed a database system and a monitoring system for the collected data.

Keywords Security management system · SNMP · Syslog · MIB · Linux OS

48.1 Introduction

In today's Internet environments, there are many varieties of security threats. Recently there have been some attacks using DDOS that paralize computer networks. Network of the Republic of Korea and the United States government agencies, portal sites and financial institutions server were paralyzed by the DDOS attack in July 7, 2009 [1]. And in March 3, 2011 a more advanced method has been used to paralyze the computer network [2]. More recently in June 26, 2015, group of hackers in Europe attacked the three Korean bank's computer network including

H.-S. Son · T.-Y. Kim · S.-G. Lee (✉)
Dongseo University, Busan, South Korea
e-mail: nok6@dongseo.ac.kr

J.-H. Lee
Mobilizone, Busan, Korea

F. Pasila et al. (eds.), *Proceedings of Second International Conference on Electrical Systems, Technology and Information 2015 (ICESTI 2015)*,
Lecture Notes in Electrical Engineering 365, DOI 10.1007/978-981-287-988-2_48

Daegu Bank, which increased a lot of threats [3]. In addition to these DDOS attack, there are other attacks such as IP spoofing, MAC address spoofing, ARP spoofing and session hijacking. It is quite sure that a variety of attacks will be found in the future. Although many security control system has been built as responds to these attacks, most of them offer only single solution for a specific attack. Security devices such as IDS and firewall provide only partial protection [4].

While security control systems that are currently used can simply detect intrusions or block the packets [5], we are planning to build an integrated security control system which can actively cope with those attacks. If we use simple network management protocol (SNMP) and syslog, it is possible to collect various information from the network. And if we develop an algorithm to analyze this information, we can effectively respond to variety of threats.

In this paper, as the first phase of the study for the integrated security control system construction, we build an environment for collecting network traffic and security event (here after we call NTSE) based on SNMP and syslog. We also developed database system and monitoring system for the collected data.

48.2 Background Knowledge

48.2.1 SNMP

SNMP is an Internet-standard protocol for managing devices over IP networks. Typical devices that support SNMP include routers, switches, servers, workstations, printers, modem racks and more. SNMP is widely used in network management systems to monitor network-attached devices for conditions that warrant administrative attention. Version 3 is the most updated version with security enhancement.

As shown in Fig. 48.2, manager, the agent and management information base (MIB) is the major entities of SNMP. Manager will request the necessary information to the agent, then the agent responses by sending back the collected information from network device [6]. Finally, MIB is a database that actually stores the information in a structured format. Even though the devices in companies will have their own MIB, there is a standardized MIB. An object is a unit of information managed by the DB management target device. Objects in the SNMP are organized in a hierarchical structure or a tree structure (Fig. 48.1).

Fig. 48.1 SNMP information gathering process

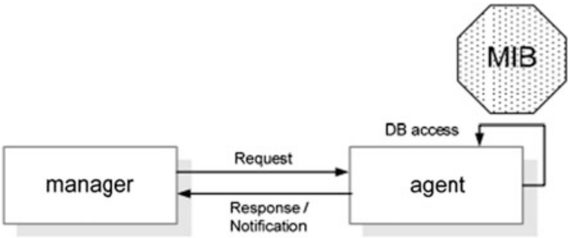


Table 48.1 Syslog type

Log name	Log file name	Related daemon	Described
Kernel log	/dev/console		Lof scattered on the console
System log	/ver/log/messages	syslogd	Linux kernel log and main log
Security log	/var/log/secure	inetd	Log by inetd
Mail log	/var/log/maillog	sendmail popper	Mail log (Log by sendmail)
Cron log	/var/log/cron	crond	Log by crond
Booting log	/var/log/boot.log		Log on at system boot
FTP log	/var/log/xferlog	Ftpd	FTP log
Web log	/usr/local/apache/logs/access_log	httpd	Apache (web server) log
Name server log	/var/log/named.log	named	Name server (DNS) log

48.2.2 Syslog

In the computing system, syslog is a widely used standard for message logging. It permits separation of the software that generates messages which is then stored in the system, and the software that reports and analyzes them. Computer system designers may use syslog for system management and security auditing as well as general information, analysis, and debugging messages. A wide variety of devices, such as printers, routers, and message receivers across many platforms are using the syslog standard. This permits the consolidation of logging data from different types of systems in a central repository [7]. As shown in Table 48.1 the basic log files provided in the current Linux system are classified into 9 types.

In order to continuously operate a syslog server, system log management daemon is required. Demon is a computer program that runs as a background process in a multitasking computer operating system rather than operates as direct control of an interactive use. It starts when the computer system is started and stops when the system is being shutdown.

48.3 Network Traffic and Security Event Collecting System

48.3.1 Log Collecting System Requirement

For the system design, we selected five requirements among several requirements [8].

Correctness As the most important requirement, in order to efficiently manage networks, it is necessary to collect correctly all of the logs that occur in the internal network. However, in the most business networks today, traffic capacity is extremely high because of the rapid increase of the network based business process. Even though the log-collecting-system receives, processes and compresses these massive amounts of data, it should not offer a defective or erroneous information associated with that.

Integrity Because the collected log messages are used to monitor and detect future attacks, these messages are very important. Thus the reliability of the information source has a very close relationship with the system performance. Digital signature to the log data can provide reliability of the data, however it is impractical to apply the digital signature to the log data in the current network environment. If the log data is used as the evidence in criminal investigations, it may require a certain level of system integrity for legislation.

Storage and processing While storing the collected logs, they should not be tampered. The collecting system must be secure from the deletion and modification of log data by the insider or illegal intruder. Because the original log data is ill-formed, it should be processed before being provided to the administrator so that he/she can intuitively identify attacks.

Normalization Normalization is the task of normalizing the type of collected log data for the use of processing and reporting by network analyst or security analyst. That is a step of generating well-known log event formats. For this step, the various elements are mapped into the data to illustrate the log data into a common format. The original log data are converted into more meaningful information by classification and normalization.

Log data mining Data mining technology can be utilized to obtain better information from the raw log data for a better attack prediction and detection. Thus, by introducing this technology in the log collecting system, we can decrease the reliance on network exporter and make the general administrator to verify the log and to monitor the traces of penetration easily.

48.3.2 System Design and Implementation

In this paper we implemented a system that collects and analyzes all network traffic from a number of the network devices in an internal network. This system can provide basic data for detecting of attacks and provide a fast attack event extracting function by analyzing vast network traffic. If our system is utilized for detection and defense technology of attack events, based on the information that has been collected, it allows the detection and response to attacks through secure management and attack event analysis of the large capacity of the log data and network application systems.

Figure 48.2 is a schematic structure of the implemented system. Agent is a program that plays a role of Syslog and SNMP where such functions are not supported in an operating server. It is a TCP application program and sends NTSE from network device to our collecting system. Because most of the network devices provide Syslog and SNMP services, they can send NTSE directly using the Syslog and SNMP trap. However most of general servers do not provide these two

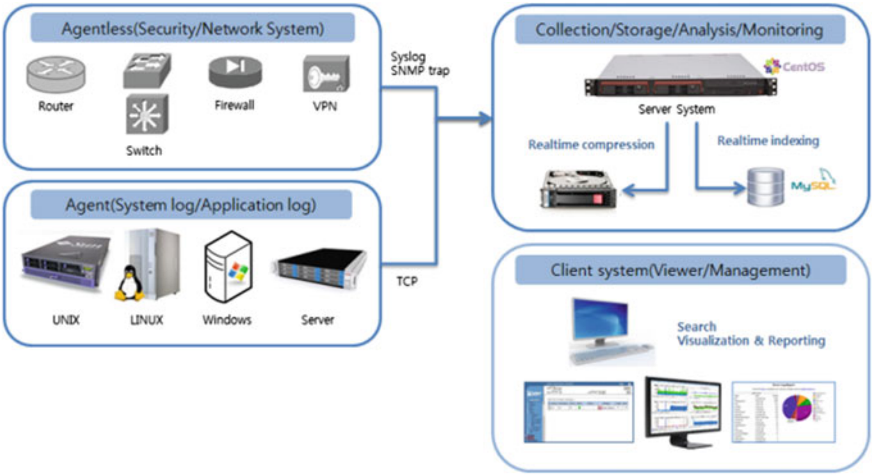

Agentless(Security/Network System)
Router
Switch
Firewall
VPN
Syslog
SNMP trap
Agent(System log/Application log)
UNIX
LINUX
Windows
Server
TCP
Collection/Storage/Analysis/Monitoring
CentOS
Server System
Realtime compression
Realtime indexing
MySQL
Client system(Viewer/Management)
Search
Visualization & Reporting

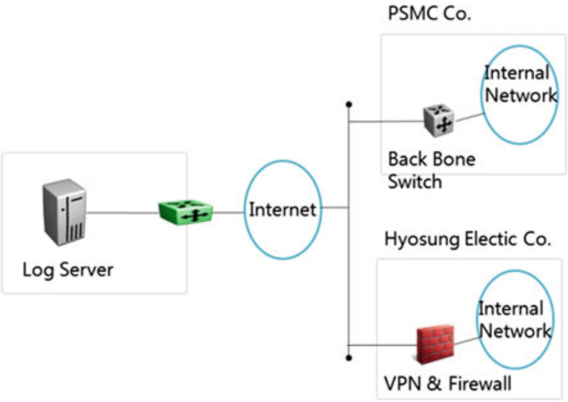
Fig. 48.2 The concept diagram for a network traffic and security event collecting system

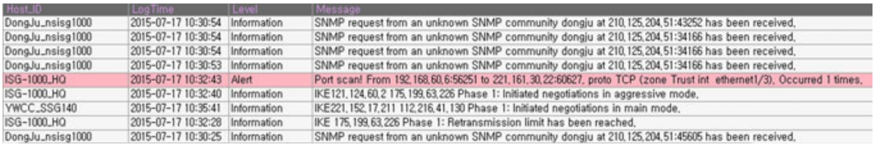
services, therefore the agent creates packets for NTSE and sends them to the NTSE collecting system.

For the development environment, a log server was prepared by installing Centos 6.5 Linux system on a custom hardware platform and mounting the SNMP and syslog on the Linux system as shown in Fig. 48.3. Log server program has been implemented in the environment of C#, .NET 4.5 and a WPF (Windows Presentation Foundation). We used Maria DB for the archive of the collected data. Server program was coded in C++ utilizing the POCO Libraries [9]. We developed four data viewer for SNMP information, syslog event, syslog analysis, and network device status monitoring.

Our log server was deployed in the real time network to check the possibility of real time application. As shown in Fig. 48.3, the log collecting server, backbone

Fig. 48.3 Real implementation network diagram





Host_ID	LogTime	Level	Message
DongJu_nsisg1000	2015-07-17 10:30:54	Information	SNMP request from an unknown SNMP community dongju at 210,125,204,51:43252 has been received,
DongJu_nsisg1000	2015-07-17 10:30:54	Information	SNMP request from an unknown SNMP community dongju at 210,125,204,51:34166 has been received,
DongJu_nsisg1000	2015-07-17 10:30:54	Information	SNMP request from an unknown SNMP community dongju at 210,125,204,51:34166 has been received,
DongJu_nsisg1000	2015-07-17 10:30:53	Information	SNMP request from an unknown SNMP community dongju at 210,125,204,51:34166 has been received,
ISG-1000_HQ	2015-07-17 10:32:43	Alert	Port scan! From 192,168,60,6:56251 to 221,161,30,22:60627, proto TCP (zone Trust int ethernet1/3), Occurred 1 times,
ISG-1000_HQ	2015-07-17 10:32:40	Information	IKE121,124,60,2 175,199,63,226 Phase 1: Initiated negotiations in aggressive mode,
YWCC_SSG140	2015-07-17 10:35:41	Information	IKE221,152,17,211 112,216,41,130 Phase 1: Initiated negotiations in main mode,
ISG-1000_HQ	2015-07-17 10:32:28	Information	IKE 175,199,63,226 Phase 1: Retransmission limit has been reached,
DongJu_nsisg1000	2015-07-17 10:30:25	Information	SNMP request from an unknown SNMP community dongju at 210,125,204,51:45605 has been received,

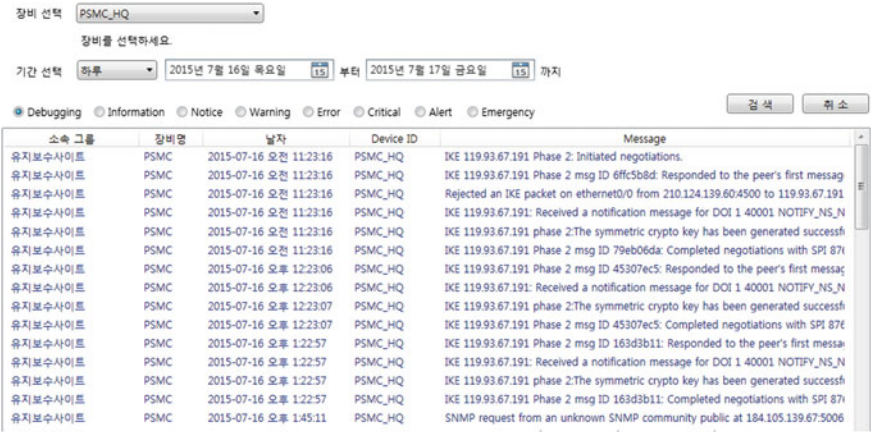
Fig. 48.4 SNMP information collection

switch and VPN firewall are located in separate networks. In the log server, SNMP/Syslog server has been installed so that it receives and processes NTSE from PSMC and Hyosung Electric network.

To collect NTSE for each network devices, Juniper's backbone switches from PSMC network and VPN firewall from Hyosung Electric network were selected. Figure 48.4 shows a screen view of SNMP information collection. Figure 48.5 shows real time syslog event collection from PSMC backbone switch. Figure 48.6 shows syslog analyses view of data from Hyosung Electric VPN device. Figure 48.7 shows network device status monitoring of CPU load, memory usage, and session collected from Hyosung Electric VPN device.

48.3.3 *The Result of System Implementation*

To test our log system in the real network, the proposed system was link with the back bone switch, firewall and VPN equipment in the real network and carried out traffic analysis. As corporate networks become more complex and larger in size, the amount of logs will increase explosively. Furthermore, dealing with the big data and security issues, the need of integrated log management is increasing. If we



장비 선택 PSMC_HQ

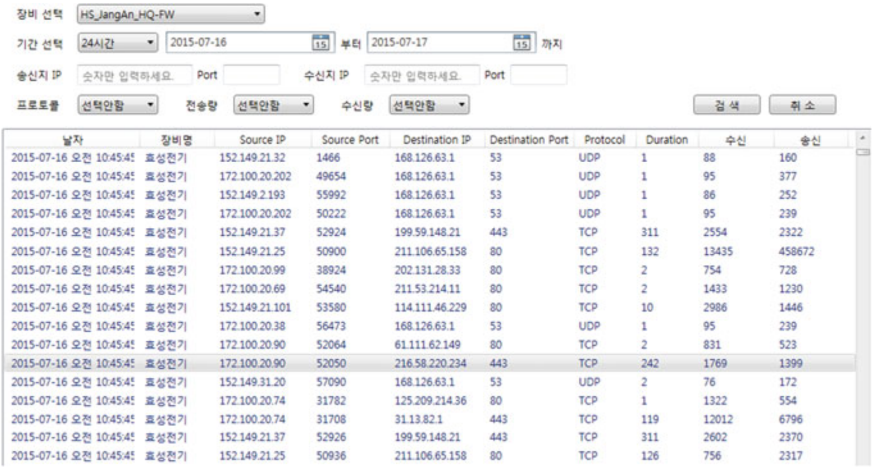
장비를 선택하세요.

기간 선택 하루 2015년 7월 16일 목요일 부터 2015년 7월 17일 금요일 까지

● Debugging ○ Information ○ Notice ○ Warning ○ Error ○ Critical ○ Alert ○ Emergency

소속 그룹	장비명	날자	Device ID	Message
유지보수사이트	PSMC	2015-07-16 오전 11:23:16	PSMC_HQ	IKE 119.93.67.191 Phase 2: Initiated negotiations.
유지보수사이트	PSMC	2015-07-16 오전 11:23:16	PSMC_HQ	IKE 119.93.67.191 Phase 2 msg ID 6ffc5b8d: Responded to the peer's first messag
유지보수사이트	PSMC	2015-07-16 오전 11:23:16	PSMC_HQ	Rejected an IKE packet on ethernet0/0 from 210.124.139.60:4500 to 119.93.67.191
유지보수사이트	PSMC	2015-07-16 오전 11:23:16	PSMC_HQ	IKE 119.93.67.191: Received a notification message for DOI 1 40001 NOTIFY_NS_N
유지보수사이트	PSMC	2015-07-16 오전 11:23:16	PSMC_HQ	IKE 119.93.67.191 phase 2:The symmetric crypto key has been generated successfi
유지보수사이트	PSMC	2015-07-16 오전 11:23:16	PSMC_HQ	IKE 119.93.67.191 Phase 2 msg ID 79eb06da: Completed negotiations with SPI 87(
유지보수사이트	PSMC	2015-07-16 오후 12:23:06	PSMC_HQ	IKE 119.93.67.191 Phase 2 msg ID 45307ec5: Responded to the peer's first messac
유지보수사이트	PSMC	2015-07-16 오후 12:23:06	PSMC_HQ	IKE 119.93.67.191: Received a notification message for DOI 1 40001 NOTIFY_NS_N
유지보수사이트	PSMC	2015-07-16 오후 12:23:07	PSMC_HQ	IKE 119.93.67.191 phase 2:The symmetric crypto key has been generated successfi
유지보수사이트	PSMC	2015-07-16 오후 12:23:07	PSMC_HQ	IKE 119.93.67.191 Phase 2 msg ID 45307ec5: Completed negotiations with SPI 876
유지보수사이트	PSMC	2015-07-16 오후 1:22:57	PSMC_HQ	IKE 119.93.67.191 Phase 2 msg ID 163d3b11: Responded to the peer's first messa
유지보수사이트	PSMC	2015-07-16 오후 1:22:57	PSMC_HQ	IKE 119.93.67.191: Received a notification message for DOI 1 40001 NOTIFY_NS_N
유지보수사이트	PSMC	2015-07-16 오후 1:22:57	PSMC_HQ	IKE 119.93.67.191 phase 2:The symmetric crypto key has been generated successfi
유지보수사이트	PSMC	2015-07-16 오후 1:22:57	PSMC_HQ	IKE 119.93.67.191 Phase 2 msg ID 163d3b11: Completed negotiations with SPI 87(
유지보수사이트	PSMC	2015-07-16 오후 1:45:11	PSMC_HQ	SNMP request from an unknown SNMP community public at 184.105.139.67:5006

Fig. 48.5 Syslog event collection



장비 선택: HS_JangAn_HQ-FW

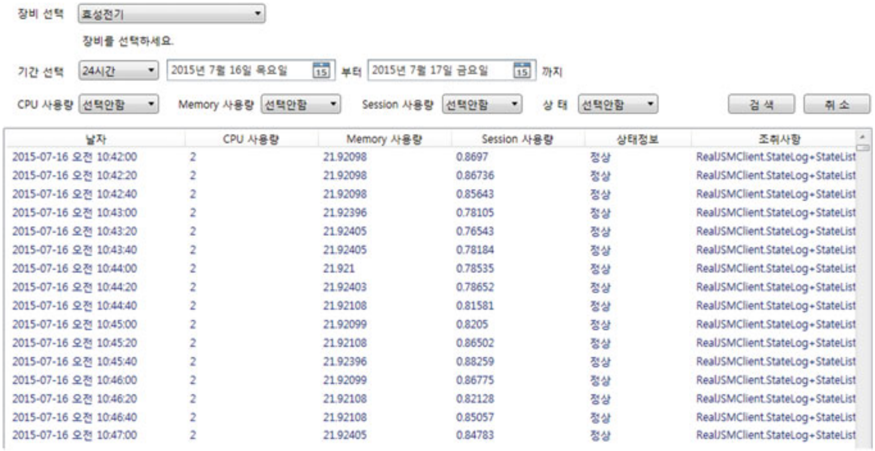
기간 선택: 24시간 | 2015-07-16 부터 2015-07-17 까지

송신지 IP: 숫자만 입력하세요. Port: | 수신지 IP: 숫자만 입력하세요. Port:

프로토콜: 선택안함 | 전송량: 선택안함 | 수신량: 선택안함

날자	장비명	Source IP	Source Port	Destination IP	Destination Port	Protocol	Duration	수신	송신
2015-07-16 오전 10:45:4	효성전기	152.149.21.32	1466	168.126.63.1	53	UDP	1	88	160
2015-07-16 오전 10:45:4	효성전기	172.100.20.202	49654	168.126.63.1	53	UDP	1	95	377
2015-07-16 오전 10:45:4	효성전기	152.149.2.193	55992	168.126.63.1	53	UDP	1	86	252
2015-07-16 오전 10:45:4	효성전기	172.100.20.202	50222	168.126.63.1	53	UDP	1	95	239
2015-07-16 오전 10:45:4	효성전기	152.149.21.37	52924	199.59.148.21	443	TCP	311	2554	2322
2015-07-16 오전 10:45:4	효성전기	152.149.21.25	50900	211.106.65.158	80	TCP	132	13435	458672
2015-07-16 오전 10:45:4	효성전기	172.100.20.99	38924	202.131.28.33	80	TCP	2	754	728
2015-07-16 오전 10:45:4	효성전기	172.100.20.69	54540	211.53.214.11	80	TCP	2	1433	1230
2015-07-16 오전 10:45:4	효성전기	152.149.21.101	53580	114.111.46.229	80	TCP	10	2986	1446
2015-07-16 오전 10:45:4	효성전기	172.100.20.38	56473	168.126.63.1	53	UDP	1	95	239
2015-07-16 오전 10:45:4	효성전기	172.100.20.90	52064	61.111.62.149	80	TCP	2	831	523
2015-07-16 오전 10:45:4	효성전기	172.100.20.90	52050	216.58.220.234	443	TCP	242	1769	1399
2015-07-16 오전 10:45:4	효성전기	152.149.31.20	57090	168.126.63.1	53	UDP	2	76	172
2015-07-16 오전 10:45:4	효성전기	172.100.20.74	31782	125.209.214.36	80	TCP	1	1322	554
2015-07-16 오전 10:45:4	효성전기	172.100.20.74	31708	31.13.82.1	443	TCP	119	12012	6796
2015-07-16 오전 10:45:4	효성전기	152.149.21.37	52926	199.59.148.21	443	TCP	311	2602	2370
2015-07-16 오전 10:45:4	효성전기	152.149.21.25	50936	211.106.65.158	80	TCP	126	756	2317

Fig. 48.6 Syslog analysis view



장비 선택: 효성전기

장비를 선택하세요.

기간 선택: 24시간 | 2015년 7월 16일 목요일 부터 2015년 7월 17일 금요일 까지

CPU 사용량: 선택안함 | Memory 사용량: 선택안함 | Session 사용량: 선택안함 | 상 태: 선택안함

날자	CPU 사용량	Memory 사용량	Session 사용량	상태정보	조취사항
2015-07-16 오전 10:42:00	2	21.92098	0.8697	정상	RealJSMClient.StateLog+StateList
2015-07-16 오전 10:42:20	2	21.92098	0.86736	정상	RealJSMClient.StateLog+StateList
2015-07-16 오전 10:42:40	2	21.92098	0.85643	정상	RealJSMClient.StateLog+StateList
2015-07-16 오전 10:43:00	2	21.92396	0.78105	정상	RealJSMClient.StateLog+StateList
2015-07-16 오전 10:43:20	2	21.92405	0.76543	정상	RealJSMClient.StateLog+StateList
2015-07-16 오전 10:43:40	2	21.92405	0.78184	정상	RealJSMClient.StateLog+StateList
2015-07-16 오전 10:44:00	2	21.921	0.78535	정상	RealJSMClient.StateLog+StateList
2015-07-16 오전 10:44:20	2	21.92403	0.78652	정상	RealJSMClient.StateLog+StateList
2015-07-16 오전 10:44:40	2	21.92108	0.81581	정상	RealJSMClient.StateLog+StateList
2015-07-16 오전 10:45:00	2	21.92099	0.8205	정상	RealJSMClient.StateLog+StateList
2015-07-16 오전 10:45:20	2	21.92108	0.86502	정상	RealJSMClient.StateLog+StateList
2015-07-16 오전 10:45:40	2	21.92396	0.88259	정상	RealJSMClient.StateLog+StateList
2015-07-16 오전 10:46:00	2	21.92099	0.86775	정상	RealJSMClient.StateLog+StateList
2015-07-16 오전 10:46:20	2	21.92108	0.82128	정상	RealJSMClient.StateLog+StateList
2015-07-16 오전 10:46:40	2	21.92108	0.85057	정상	RealJSMClient.StateLog+StateList
2015-07-16 오전 10:47:00	2	21.92405	0.84783	정상	RealJSMClient.StateLog+StateList

Fig. 48.7 Network device status monitoring

apply our system to the complex company networks for collecting logs of all networks and analyzing them in real time, it is possible to provide appropriate information as a response. Most network devices do not collect and save logs, but because we can collect and analyze the logs using our system,, the proposed system is very useful to solve this problem. Thus our system can be easily installed and managed in the existing network so that it is not necessary to build a new system to collect the logs.

48.4 Conclusion

In this paper, we designed and implemented a system for collecting and analyzing network traffics to analyze and monitor the security problem of the internal network of an organization in real-time. The proposed system saves all of the traffics generated from storage-less network devices and analyzes the security problem in real time. It enables the organization to monitor the state of the internal network. Also, when security incidents occur, our system can acquire the log data for the traffic information and rapidly analyzes it. The expected benefit of deploying our system is that the network security features can be enhanced by managing the network-based security issues while using the existing network systems.

Acknowledgments This paper was supported by the Ministry of Trade, Industry and Energy (MOTIE) through the fostering project of the Innovation for Engineering Education and by Ministry of Education (MOE) through the project of the Leaders in the Industry-university cooperation.

References

1. Wikipedia Website on 7.7 DDoS Attack. https://ko.wikipedia.org/wiki/7%C2%B77_DDoS_%EA%B3%B5%EA%B2%A9
2. Wikipedia Website on 3.3 DDoS Attack. https://ko.wikipedia.org/wiki/3%C2%B73_DDoS_%EA%B3%B5%EA%B2%A9
3. Financial news website. http://www.fnnews.com/news/201506261801326408
4. Yu, Y.J.: DDoS Attack Detection Method Using Average Rate of Change of Traffic. MS thesis, Graduate school of Chungbuk National University (2011)
5. Tabona, A.: The Top 20 Free Network Monitoring and Analysis Tools for Sys Admins, GFI Blog, 15th, 4, 2015. http://www.gfi.com/blog/the-top-20-free-network-monitoring-and-analysis-tools-for-sys-admins/
6. Kim, Y.S.: Understanding of SNMP concept, Novo networks (2010)
7. Wikipedia Website on Syslog. https://en.wikipedia.org/wiki/Syslog
8. Chuvakin, A.A., Schmid, K.J., Phillips, C.: Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management, 1st edn. Syngress, California (2012)
9. POCO C++ Libraries. http://pocoproject.org/