

Data Visualization for Network Access Rules of Critical Infrastructure

An-Byeong Chae^{1(✉)}, Jeong-Han Yun², Sin-Kyu Kim²,
Kang-In Seo³, and Sung-Woo Kim¹

¹ Interaction Design, Graduate School of Techno Design,
Kookmin University, Seoul, Korea
monkeyactive@gmail.com, caerang@kookmin.ac.kr

² National Security Research Institute, Daejeon, Korea
{dolgam, skkim}@nsr.re.kr

³ Interdisciplinary Program of Information Security,
Chonnam National University, Gwangju, Korea
knuei2014@gmail.com

Abstract. Control systems widely used in the national infrastructures are mainly aimed at regular performances of the specified tasks. Therefore, whitelisting security solutions or program that define all usable assets and approachable relationships between rules are widely applied to. The working procedure of the whitelisting control system can be described not just by simple accessing abilities, but various rules such as communication period, frequency, sequence of communication objects, concurrency and inclusion relation etc. As a whitelisting has recently developed more complicatedly, it is believed that the research of the information visualizing which helps the users recognize priority information and the research of the UI which let users manage those information more efficiently are necessary. We have set an extended form of whitelisting that is required for control system security, and it is also based on general requirements in that field. Basing on the analysis of relevant tools and interviews with security experts, we propose a visualize method to manage whitelist information more easily and effectively.

Keywords: Data visualization · Network access rules · Traffic log

1 Introduction

Most infrastructures such as power plant, dam, water sewage systems, and traffic control system have received accepted developed IT technologies, which are currently configured with a lot of network servers, PCs, and controllers. Since cyber-attacks are mainly caused by at the level of massive terrorist groups or nations, not by an individual who is looking for fun, lots of researches have been done to strengthen the cyber security for those infrastructures.

The background of the security starts from understanding exact assets and applying specific access control rules for each asset. The main purpose of the control systems is for regular execution of defined jobs. So, recent security studies are more about the defining of the accessible relationship of the rules among available assets.

In order to visualize regular job executions of control systems by using whitelisting of access control rules (ARs), not just the fact that an actual access itself is made or not is checked, but also many rules are applied including communication cycle and frequency per access-allowed relationship, order, concurrency and inclusion relation between communication targets. As whitelisting becomes more complicated to use, it is now necessary that more studies which let the users enable to distinguish what is more important or not among information through the emphasized expression and primary location of the information.

This study aims to allow the users to easily manage expanded whitelist-based access rules, and suggests UX improvement plans that visualize communication status (traffic log) for easier understanding based on it.

2 Background

We have developed a network switch, called F.Switch which makes existing whitelist-based access rules be applied, and F.Manager by which many F.Switches can be managed comprehensively. The baseline in this study is the whitelist managing system in F.Manager we developed. This paper briefly introduces F.Manager.

Figure 1 is an overall conceptual diagram of how F.Manager manages the F.Switches installed in the control system network and manages the control system internal network security control.

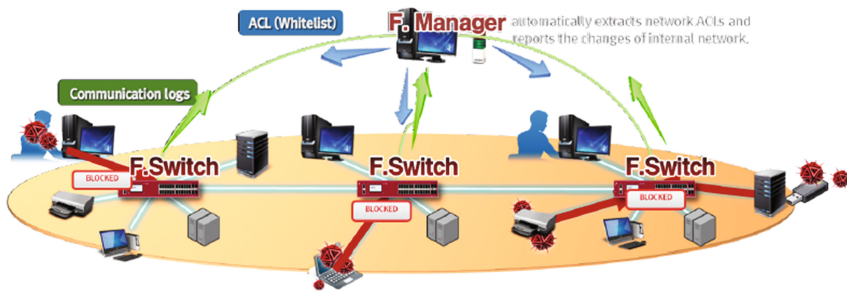


Fig. 1. A complete conceptual diagram of F.Manager and F.Switch

A network switch that can monitor all the traffic of the internal network without installing a SW agent in the control system and can apply a whitelist-based access list (AR List) remotely is called F.Switch, An integrated management system for efficiently managing and utilizing such F.Switches is called F.Manager.

F.Switch can log source (IP, MAC, port) – protocol – Destination (IP, MAC, port) information of all packets generated by the unit time set by the user. Unlike sampling-based monitoring (Ex. Netflow), F.Switch monitors all traffic passing through F.Switch and then solves many problems of control system security by blocking traffic and breaking alarms that violate the AR List. In addition, the security practitioner had

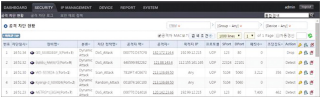
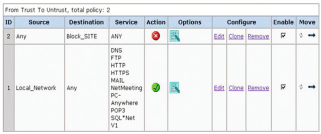


to control and manage all the installed F.Switches of the control system all at once. So we designed F.Manager, an integrated management system that can manage multiple F.Switches installed in the control system network in one place.

3 Related Equipment Analysis

3.1 Comparative Analysis of Domestic and International Security Program Related to AR List



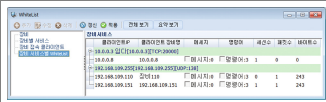
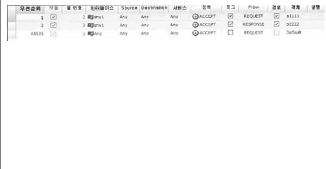
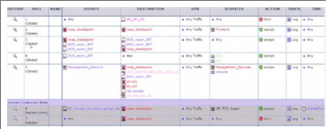
In the existing network access control list, visualization features of security-related programs in Korea and abroad were grasped to obtain information needed for extended access rules. Total 15 programs were analyzed and each programs were compared to identify the common elements of the visualization and their advantages and disadvantages (Table 1).

Table 1. Comparative analysis of domestic and foreign security program equipment.

Category	Name	Equipment features	Screen example
Korea	VIPM PLUS [1]	<ul style="list-style-type: none"> - Network Integrated Security Solution - Customizable information for user's intent - Icon + text form 	
	Juniper Firewall/VPN [2]	<ul style="list-style-type: none"> - Integrated solution for secure network environment - Intuitively express information structure - Category names are difficult to understand. 	
	SECUI-NGX [3]	<ul style="list-style-type: none"> - Providing external and internal network services and protecting services - Iconic representation is effective - Name Expression Intuitive 	
	SubGATEplus [4]	<ul style="list-style-type: none"> - Effective handling of internal and external network threats - Use a variety of visual expressions - Many icons can cause confusion 	


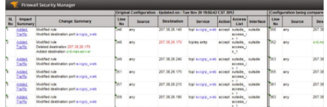

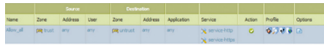

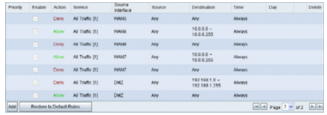
(continued)

Table 1. (continued)

Category	Name	Equipment features	Screen example
	SecuwayGate [5]	<ul style="list-style-type: none"> - Intrusion Prevention System - Use a lot of visual representation (icon) - Consistency of the menu is low 	
	Genian NAC [6]	<ul style="list-style-type: none"> - User and terminal control accessing the network - Information structure Intuitively expressed - Difficult to recognize icon and visual representation 	
	SNIPER AMS [7]	<ul style="list-style-type: none"> - Ensure safety through network management based on whitelist policy - It is difficult for the user to recognize because of the unusual sorting method 	
	SNIPER IPS [8]	<ul style="list-style-type: none"> - High Performance Intrusion Prevention System - Priority for critical information is not appropriate 	
Foreign	Algosec [9]	<ul style="list-style-type: none"> - Security management system focusing on blocking malicious traffic - Intuitively identifiable for Source and Destination elements - Use Easy Names 	

(continued)

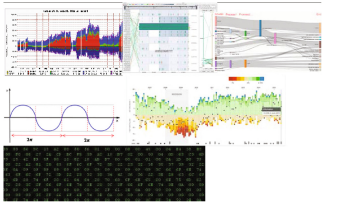
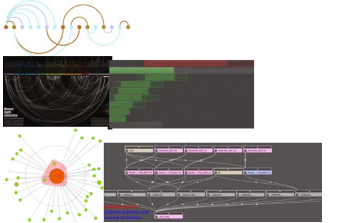
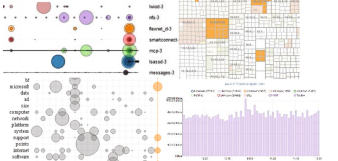
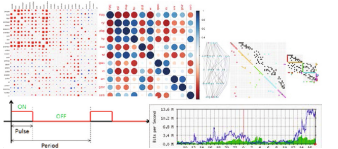
Table 1. (continued)

Category	Name	Equipment features	Screen example
	Firewall Builder5 [10]	<ul style="list-style-type: none"> - A standard firewall system that supports multiplatform and is easy to create and modify policies - Icon Visualization Excellent - Use a lot of visual representation (icon) 	
	Solarwinds (Firewall Security Manager) [11]	<ul style="list-style-type: none"> - Role of firewall security management and network configuration management - This system only used text without icons - Priority for critical information is not appropriate 	
	Tufin [12]	<ul style="list-style-type: none"> - Network Integrated Security Solution - This system only used text without icons - Category names are difficult to understand. 	
	Paloalto [13]	<ul style="list-style-type: none"> - New concept security platform that recognizes and controls applications and users - Excellent grouping of relevant information 	
	ProSecure [14]	<ul style="list-style-type: none"> - Next Generation Firewall System for Modern Business - The system uses a button function to provide a visual representation 	
	Cisco RV Router [15]	<ul style="list-style-type: none"> - Implement a new dimension of basic connectivity to the user experience - This system only used text without icons 	

3.2 Traffic Log Related Data Visualization Program

Traffic logs should be set to monitor entire of the characteristics of traffic at a glance. For this purpose, various data visualization programs were investigated. Total 40 programs were analyzed and the visualization data that can be used in connection with this task were referred to (Table 2).

Table 2. Data visualization resources

Characteristics of data	References
Change over time [18–23]	
Appropriate for expressing mutual relationship [24–28]	
Express size and quantity [23, 29–31]	
Changes in specific elements [32–36]	

4 Requirements for Creating Data Visualizations

With F.Manager, field administrators can easily manage the extended whitelist-based access rules. Therefore, UX should be improved its factors to visualize the communication history (traffic log) efficiently in general condition, especially required for in case an accident happens.

The required factors are gathered through consultations between several field managers and researchers. And relevant information regarding the access control list and the communication status is collected from them. Based on these requirements, we build the data visualizing system.

4.1 Requirements for AR List

Basically, the information provided in the AR List needs to be the key one for smooth management of the field manager, and the information expressed in the AR List should be configured in accordance with the priority.

For this purpose, we analyzed the information that is commonly used through analysis of domestic and foreign security program equipment. We also summarized the specific information that should be included in the AR considering the characteristics of F.Manager with the result of the interview with the field manager, field network analysis (Table 3).

Table 3. The kind of information required for the AR List

AR configuration information	Description of function
Source	IP, Name
Service	Src Port, Protocol, Transmission direction, Dst Port
Action	Allow, Allow time zone, Temporary time allowed, Inactive
Comment	User-written sentence
Flag	None/Red/Yellow/Green/Blue (User settings)
F.Switch List	F.Switches to which the AR applies
Features in AR	<ul style="list-style-type: none"> – Time period (seconds, minutes) – Prohibit concurrent sessions/Allow concurrent sessions (2, 3, many)
Associated ARs	<ul style="list-style-type: none"> – ARs that should generate corresponding traffic sequentially – At the same time, ARs to which the traffic should occur – At the same time, ARs that should not generate such traffic – ARs representing a single 'large service'

4.2 Traffic Log Requirements

There are several elements such as period, frequency and concurrent session, of which they are characteristics of the AR, and they need to be represented in the traffic log. Also, there are sequential, simultaneous, inclusion expression in the relation between ARs as well as an indication of traffic volume. Based on these factors, we investigated graphs which can be used for each characteristic and visualization methods that can efficiently express information and error perceptions. Particularly, the requirements for traffic log visualization are summarized.

Table 4. Characteristics required for traffic logs

Category	Element	Requirements	Visualization material
Features in AR	Period [19, 23, 29 and 35]	<ul style="list-style-type: none"> – Period representation over time – The communication with error is given the highest priority 	
	Frequency [34, 36]	<ul style="list-style-type: none"> – The frequency of the normally occurring communication and the frequency of the communication with the change are distinguished and expressed – The communication with error is given the highest priority 	
	Concurrent sessions	<ul style="list-style-type: none"> – The distinction between concurrently occurring ARs and isolated ARs (Allow concurrent sessions: 2, 3, any) – The communication with error is given the highest priority – A concise expression that does not interfere with the flow of the timeline 	
Associated ARs	Sequential [24, 26 and 27]	<ul style="list-style-type: none"> – A distinction between a related AR and a sole AR 	
	Simultaneous	<ul style="list-style-type: none"> – A concise expression that does not interfere with the flow of the timeline – The ARs that have a relationship are expressed in groups. 	
	Inclusive		

(continued)

Table 4. (continued)

Category	Element	Requirements	Visualization material
Traffic volume [23, 29 and 31]		<ul style="list-style-type: none"> Express the amount of traffic without interrupting the flow of the timeline Need size change for easy recognition of traffic volume change 	

5 Making and Evaluating the 1st Improvement Plan

5.1 Prototype

We focused on data visualization features of their data presentation methods from the existing security programs, including 15 security related programs and 40 data visualization ones. Based on the analysis results, a prototype was created for the list of control system communication status and the traffic log. This prototype will play a big role in producing the final product after the verification of the expert interview and evaluation.

In this document, we propose two prototypes based on extended AR List and communication status (traffic log). Firstly, the AR List was derived the improvement keywords from the issues obtained by comparing and analyzing F.Manager and 15 security related programs. The keywords that we have focused on here are ‘information priority’, ‘grouping’ and ‘intuitive expression’ (Fig. 2).

Action	Name	F. Switch (Switch)	IP(A)	Direction Protocol / Port	IP(B)	Hit Count	Hit Time	Frequency	Quality Period / Concurrent Session	Relation
	AR-02334	F. Switch A / F. Switch B	121.456.789.0	TCP 80	121.456.789.0	100	2019/02/19 21:26	30 Sec	3	
	AR-02334	F. Switch A / F. Switch B	121.456.789.0	UDP 80	121.456.789.0	100	2019/02/19 21:26	1 Min	any	
	AR-02334	F. Switch A / F. Switch B	121.456.789.0	HTTP 80	121.456.789.0	100	2019/02/19 21:26	30 Sec	any	
	AR-02334	F. Switch A / F. Switch B	121.456.789.0	HTTP 80	121.456.789.0	100	2019/02/19 21:26	30 Sec	1	
	AR-02334	F. Switch A / F. Switch B	121.456.789.0	UDP 80	121.456.789.0	100	2019/02/19 21:26	30 Sec	2	
	AR-02334	F. Switch A / F. Switch B	121.456.789.0	UDP 80	121.456.789.0	100	2019/02/19 21:26	30 Sec	3	
	AR-02334	F. Switch A / F. Switch B	121.456.789.0	UDP 80	121.456.789.0	100	2019/02/19 21:26	30 Sec	3	

Fig. 2. 1st prototype (AR List)

Secondly, the elements which need to be represented in the traffic log and the graphs in line with the characteristic of each element needed to be verified. Through the analysis of 40 data visualization programs, we were able to find out the information representing way of the graphs. We were also able to set a guideline of our prototype after finding the common points among the elements which is required for representing them on the screen. The selected items are as follows.

1. You should be able to view the entire log as time passes.
2. Make a quick error judgment.
3. You should use intuitive expressions that help you recognize information.

Based on this, we could produce two prototypes. Prototype A has the advantage that the overall trends and information of ARs can be grasped by constructing the entire element on one screen. It is basically concentrating on some specific elements, it is easy to find the problematic AR (Figs. 3 and 4).

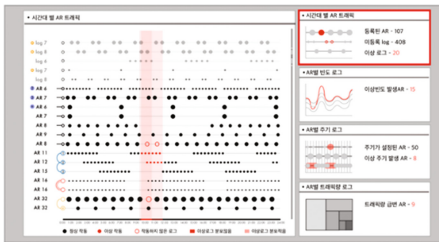


Fig. 3. Traffic Log 1st prototype (A Type)

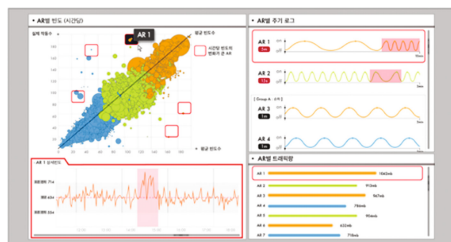


Fig. 4. Traffic Log 1st prototype (B Type)

5.2 Expert Interview and Evaluation

In order to verify the importance and priority of the elements of the information display in the control system communication status list and the traffic log, an in-depth interview with the experts having experience with the security related domain was conducted in addition to the heuristics and the data visualization Likert scale evaluation.

5.2.1 Expert Organization

The interviewees were selected as software developers, network security researchers and UI experts with knowledge of security related domain. Participants in the interviews conducted in-depth interviews and evaluations by watching the prototype screen produced primarily. The questionnaire proceeded as per the order of the processing sequence, and the contents of the question were divided into the control system communication status list and the traffic log screen in the first prototype screen according to each criterion. In addition, several comments from each individual were collected and possible improving points were recorded.

The expert interviews and evaluation took 90 min per expert and were conducted in the form of on-site visits.

5.2.2 Expert in-Depth Interview

The interviews conducted for six experts, and firstly made them recognize the purpose of F.Manager's functions and tasks. The Think-Aloud method was used to investigate the impression of the primary prototype created through its own analysis.

The interview process is divided into AR List and traffic log. In the case of AR List, we verified the suitability of composition of visualization screen based on 'information priority', 'grouping', 'intuitive expression about language and time'. In the case of traffic logs, interviews were conducted on the basis of the selection of the production direction and the characteristics of the preferred screens, and A and B in the two prototypes were examined.

5.2.3 Expert Evaluation

After the in-depth interview, the expert evaluation was conducted to obtain quantified data on the results of the experts' tests. For the AR List, Jacob Nelson's heuristics evaluation was reorganized into 5 different attributes [16], and the traffic log was evaluated by using the Data visualization Likert scale of Hyo-Jeong Kwon [17].

Tables 5 and 6 below are the question list used in the evaluation process.

Table 5. Jacob Nelson, Heuristics Assessment

Property	Question
A. Strive for consistency and standards	Q1. Is the overall screen configuration consistent?
	Q2. Are the details elements (individual elements, icons) of the AR information consistent?
B. Match between system and the real world	Q1. Is it intuitive to understand the information provided?
	Q2. Is it easy to recognize information using visualization that fits the characteristics of the information?
	Q3. Are the comparisons between the provided information (AR) supported directly or indirectly?
C. User Control and freedom	Q1. Is it possible to find the information you want easily and quickly?
	Q2. Is it possible to change the state of the AR information as needed?
D. Design dialog to yield closure	Q1. Does it clearly separate the beginning and end of information access?
	Q2. Does category grouping interfere with viewing information?
E. Visibility of system status & informative feed-forward & back	Q1. Is the visual representation of the current state of the AR? (on/off, Error...)
	Q2. Could the user be aware of the problem himself or herself through a given information screen?

As a result of the evaluation, we were able to identify areas that need an improvement, they were generally rated high, though. The results of Jacob Nelson’s heuristics-based AR List showed a high score for consistency of the overall screen configuration and visual representation of the current state and a low score for intuitive cognition received (Fig. 5).

Table 6. Hyo-Jeong Kwon, Data visualization Likert scale evaluation

Property		Question
Functional attribute	Functionality	[Information order/placement] Q1. Can you easily identify the characteristics between ARs? (Sequential, simultaneous, inclusive)
		Q2. Has the characteristics in the AR been adequately reflected? (Period, frequency, concurrent session)
		Q3. Are the information represented by a graph suitable for the characteristics of the AR log?
		Q4. Can the icon on the information screen predict the detail function?
	Familiarity	Q1. Is it possible to intuitively understand the information provided through the expressions commonly used in the nature of information?
		Q2. Is it easy to recognize information using visualization that fits the characteristics of the information?
Cognitive attribute	Understanding	[Explore Information] Q1. Is it possible to easily find the necessary information through the provided visualization information?
		[Interpret information] Q2. Is it easy to grasp the current state of the AR with a graph alone?
	Immersion	Q1. Are there any unnecessary expressions for identifying important elements?
	Sensory attribute	Esthetic
Q2. Is it properly structured in size and color to aid in information awareness?		
Satisfaction		Q1. Is there a willingness to continuously check the information through this screen?
		Q2. Do you think it is user-centric?

The traffic log evaluation results using the data visualization Likert scale of Hyo-Jeong Kwon [17] were evaluated differently in both prototype A and B. Prototype A received high marks in the immersive sense of cognitive attributes because it represented only relevant information without unnecessary elements. Also, they received the same high score in satisfaction of sensory attributes. However, the score of the functional elements of the graph using the AR log is low.

In Prototype B, although it received a high score in the esthetic part of the sensory attribute, unlike the prototype A, the expression of unnecessary information was found and received a low score in the immersion feeling part of the cognitive attribute (Figs. 6 and 7).

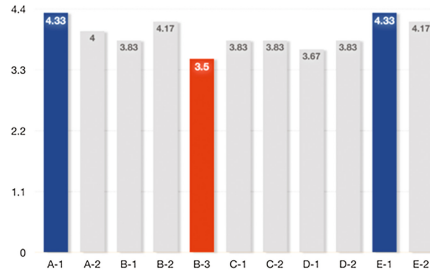


Fig. 5. Jacob Nelson, results of heuristics

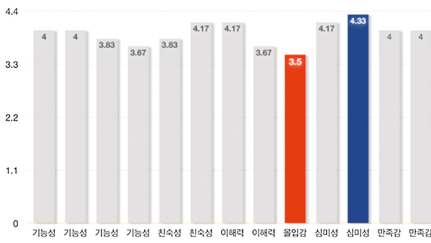


Fig. 6. Hyo-Jeong Kwon, information visualization Likert scale evaluation result (A Type)

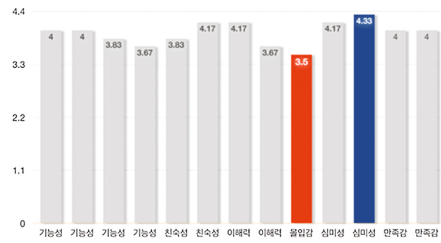


Fig. 7. Hyo-Jeong Kwon, Information visualization Likert scale evaluation result (B Type)

5.2.4 Expert Interview Analysis Result

Through the expert interviews and evaluations, we were able to obtain the necessary insight in the final visualization of data visualization. The results of analysis by AR List and traffic log are as follows.

Firstly, the AR List was able to find total 57 issues. The contents of the issue were information expression, grouping of information, category order and information sorting. We have identified common factors in these issues and derived final improvements.

1. Visual configuration for fast error-detection.
2. How to express to the characteristics of information.
3. Priority-aware category arrays.

Secondly, total 40 issues in prototype A and 37 issues in prototype B were found in the traffic log. The final improvements were derived by combining the features and common issues of different prototypes A and B.

1. Structural Improvement for Integrated Information Verification.
2. Re-selection of a visualization method suitable for information property.
3. Added functions for seamless information search.

6 Data Visualizations Screen Suggestion

In this document, the data visualization screen of AR List and traffic log are shown in the paragraphs below. The screen includes case study, first prototype production, expert interview and evaluation analysis focusing on F.Manager’s whitelist based communication status factor which are from the prior research. Based on the results, we propose a whitelist-based AR communication status list which is the main function of F.Manager, a security network switch management software of the National Security Research Institute and a method of improving the data visualized UX of the traffic log.

6.1 AR List Final Screen Suggestion

It aims to visualize the whitelist-based AR List information in F.Manager so that it can recognize it a lot quickly and easily. Previously, AR List focused on implementing whitelist information for control system management. After prototyping, the experts suggest the improvement plan through the interview, and finally the proposed screen is the result of efficient operation and management from the viewpoint of the user (Fig. 8).

필터 기준	전체보기	F-Switch로 보기	IP로 보기	총 456개의 AR이 등록됨 (현재 표시된 것은 AR의 4개가 있습니다)										테그 지정	AR 삭제
Action	AR 명	Applied F-Switch	IP (A)	Port (A)	Protocol	Direction	Port (B)	IP (B)	추가	삭제	동시선택	AR간 관계	발생 횟수	확인	
✓	AR_02334	F-Switch A F-Switch B	Client_A_Group	Any	TCP	→	80	Server_B_Group	30 Sec	120	Any	→	150	150번 (# 412-기)	
□	AR_02335	F-Switch A F-Switch B	223.122.243.1	Any	TCP	→	80	223.16.79.2	30 Sec	240	Any	→	150	200번 (# 412-기)	
□	AR_02336	F-Switch B F-Switch D	123.190.110.0	-	ICMP	→	-	123.46.110.0	30 Sec	80	▲	→	150	450번 (# 412-기)	
□	AR_02337	F-Switch C F-Switch D	123.4.233.0	-	ICMP	→	-	143.23.110.0	-	80	▲	3	100번 (# 412-기)		
□	AR_0238	F-Switch A	123.16.89.0	1000	UDP	→	3000	123.76.79.0	30 Sec	120	▲	1	150	300번 (# 412-기)	
□	AR_0239	F-Switch A F-Switch D	213.56.9.0	2300	UDP	→	3000	223.246.79.0	-	240	▼	2	150	100번 (# 412-기)	
□	AR_0240	F-Switch C	12143.89.0	2300	UDP	→	3000	13.44.89.0	60 Sec	80	▲	3	150	600번 (# 412-기)	
□	AR_0241	F-Switch C F-Switch D	53146.69.0	1000	UDP	→	1000	183.196.249.5	60 Sec	80	▲	3	150	150번 (# 412-기)	

Fig. 8. AR List final screen

6.1.1 Visual Configuration for Fast Error Detection

The problematic AR in the AR List is provided at the top of the list, and it is expressed in the background by applying a red color so that it is easy to recognize the abnormality. In addition, a warning icon ‘!’ is displayed in the area where the error occurred in regard to the detailed problem (Fig. 9).



Fig. 9. AR List error occurrence screen (Color figure online)

6.1.2 How to Express to the Characteristics of Information

The name of the information about the provided information should be easily identifiable, and the visual representation of the function that may confuse the user should be limited. In Fig. 10, the indication of the IP forwarder and the receiver are not specified as ‘Server’ or ‘Client’ due to the protocol-related change in the protocol. Instead, it uses a different color in the output area to represent the role.

IP (A)	Service				IP (B)
	Port(A)	Protocol	Direction	Port(B)	
223.6.179.3	2300	TCP	↔	3000	123.56.110.1

Fig. 10. IP and network connection method area in AR List

In Fig. 11, the tag function is used to enable smooth communication among users. Intuitive recognition is also possible by using different colors according to the level of importance. In addition to the color, several icon shapes are also commonly used.

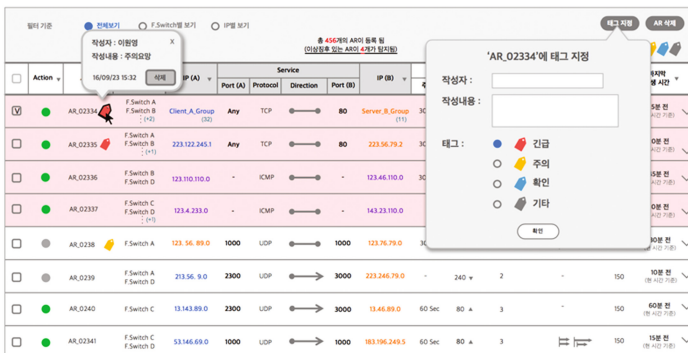


Fig. 11. AR List tag function

6.1.3 Priority-Aware Category Arrays

It is necessary to check if the information to be firstly checked by the user is conspicuous in the AR List, and the placement of such information is highly important. The information in the AR List is divided into AR basic information area, IP and network connection method area, AR characteristic area, AR relation area, AR occurrence frequency and last occurrence time area in order of importance (Fig. 12).

Action	AR 명	Applied F.Switch	IP (A)	Service			IP (B)	AR내 특성			AR간 관계	발생 횟수	마지막 발생 시간
				Port (A)	Protocol	Direction		Port (B)	주기	빈도			

Fig. 12. AR List information providing area

- AR basic information: AR state(on/off), Name, Applied F.Switch
- IP and network connection method: IP(A) – Service – IP(B)
- AR characteristic: Period, Frequency, Concurrent session
- AR relation: Display information about sequential, concurrent, and inclusive relationships
- AR occurrence frequency and last occurrence time: Cumulative number of occurrences and the last occurrence time in the current time display
- Learn more: Detailed information about AR List

6.2 Traffic Log Final Screen Suggestion

It is aimed to visualize the logs of actual traffic of ARs so that they can be quickly recognized by expressing them in a suitable form for information characteristics. After making the first prototype, UX Direction was derived through an expert interview. The final result reflects the overall log flow and detailed frequency, period, and traffic volume of individual ARs at a glance. In Fig. 13, the number of communication

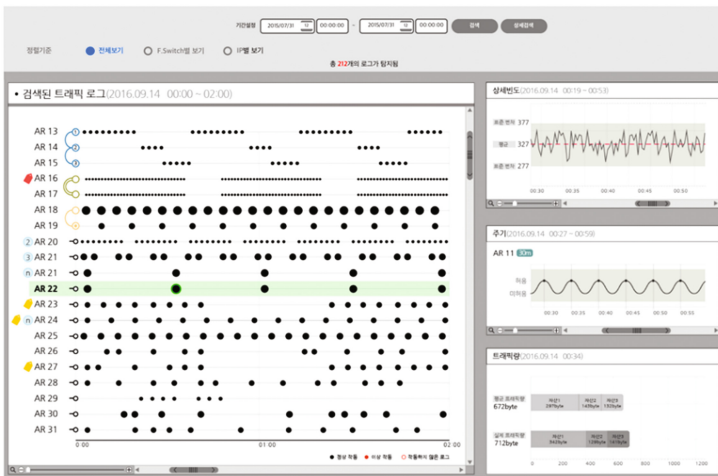


Fig. 13. Traffic log full screen (Color figure online)

operations in the X axis (time) and the Y axis (AR List) is expressed in dot form, the size, interval, and the repetition are displayed according to the characteristics. In addition, the part where the abnormality occurs is marked with red.

6.2.1 Structural Improvement for Integrated Information Verification

In order to comprehensively understand the overall log flow and detailed AR information, the features of A and B in the first prototype were collected. In A type, the overall tendency and information can be grasped. In B type, it is easy to grasp the problematic AR List, and it has an advantage in showing individual characteristics.

6.2.2 Re-selection of a Visualization Method Suitable for Information Property

The visualization method is changed to a commonly used visualization one so that detailed information can be grasped at a glance. In the case of frequency, the numerical value of the average frequency reference deviation was made into a line graph in a certain period. In the case of the period, the repetitive communication status are represented by the characteristics such as sequential, simultaneous, inclusion according to the relationship between the ARs. In the case of traffic volume, the actual traffic volume of the currently selected AR against the average traffic volume is shown in the form of a bar graph. The error expression of each characteristic makes red indication in the region of anomalies, enabling intuitive interpretation (Figs. 14, 15 and 16).



Fig. 14. Frequency graph (Color figure online)

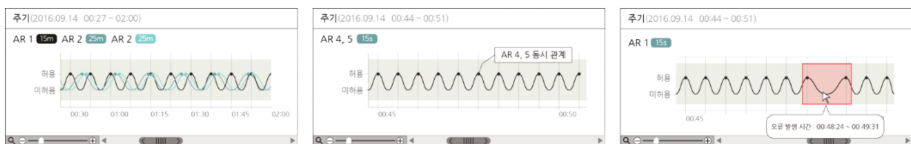


Fig. 15. Period graph (Color figure online)

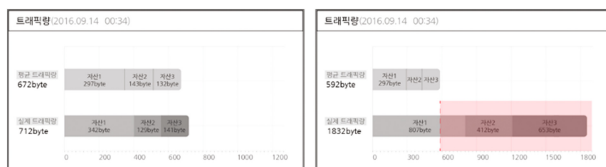


Fig. 16. Traffic volume graph (Color figure online)

6.2.3 Added Functions for Seamless Information Search

Throughout the error detection and zooming function, the user can easily find the AR errors on full screen. In the case of the AR in which the error occurred, a red area is displayed on the scroll, so that the error position can be intuitively detected. In addition, the selected errors are provided for each characteristic in the frequency, period, and traffic volume areas on the right side of the screen (Fig. 17).

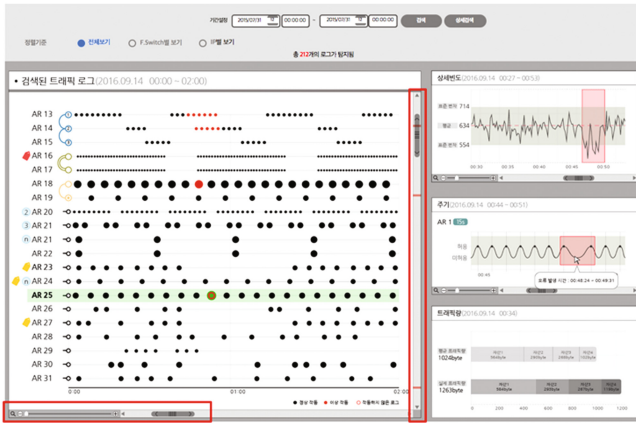


Fig. 17. Scroll (error search) and zooming functions (Color figure online)

6.3 Excellence of Data Visualization Screen Proposal

UX improvement plans that we established and based on assessment for existing products, requirements from the site, and expert interview are excellent for the following reasons.

1. Methods of data expression and prioritization were complemented. Therefore, it is possible to check whitelist data consistently by control system operators, not security experts.
2. It is easy to clearly recognize ARs that are identified as errors (ARs that are not followed at the site).
3. Utilize appropriate graphs for data visualization which based on important factors in communication status monitoring from the security perspective.

The improvement plans make it possible to rapidly search ARs that have necessary data for security work and to understand the entire communication status as well as individual AR's characteristics at a glance.

7 Conclusion

Our study allows to effectively manage the control networks by establishing guidelines for the visualization of traffic log data and whitelist-based AR communication status list. Suggested plans may serve as references that will contribute to more effective work management by users of security programs such as network firewall and network access control solutions. Site tests for various systems are planned in order to move towards easier and more efficient solutions.

References

1. Handreamnet: VIPM Plus Administrator's Guide v1.0 (2014)
2. Zungwon Engineering & Systems: Juniper Firewall/VPN (2008)
3. Secui: SECUI NGX (2011)
4. Handreamnet: SubGATE Plus 100&200 (2005)
5. Future Systems: SecuwayGate GateAdin Pro (2015)
6. Geni Networks: Genian NAC Suite (2013)
7. National Security Research Institute. AMS (2012)
8. Wins: SNIPER IPS v8.0 (2012)
9. Algosec: Algosec (2012–2015)
10. NetCitadel: Firewall Builder5 (2011)
11. Solarwinds: Firewall Security Manager (2012)
12. Tufin: Tufin (2016)
13. Palo Alto Networks: Paloalto PAN-OS (2014)
14. ProSecure Unified Threat Management (UTM) Appliance. <http://www.downloads.netgear.com/files/GDC/UTM9S/UTM9S%20Firewall%20Quick%20Start%20Guide.pdf>
15. CISCO: Cisco Small Business RV0xx Series Routers (2012)
16. Nelson, J., Robert, L.M.: Usability Inspection Methods. Wiley, New York (1994)
17. Kwon, H.-J.: Elements for Evaluating the Usability of the Web-Based Infographic Design (2013)
18. So-In, C.: A Survey of Network Traffic Monitoring and Analysis Tools. https://www.cse.wustl.edu/~jain/cse567-06/ftp/net_traffic_monitors3/
19. TNV. <http://tnv.sourceforge.net/>
20. Sankey Diagrams. <http://jasonheppler.org/projects/csu-workshop/network-literacy.html>
21. Ondas armonicas. <http://acer.forestaes.upm.es/basicas/udfisica/asignaturas/fisica/ondas/armonicas.html>
22. Visualizing the Ebb and Flow of Jobs. <https://www.datainnovation.org/2015/02/visualizing-the-ebb-and-flow-of-jobs/>
23. Network Monitoring tools. http://www.gregconti.com/publications/insecure_conti.pdf
24. Email thread visualization. http://infosthetics.com/archives/2006/06/email_thread_visualization.html
25. Data visualization. <https://mjalexandre.wordpress.com/2015/10/06/critical-design-process-the-design-industries/>
26. Adobe After Effects tools. <https://www.smashingmagazine.com/2015/06/fitting-after-effects-into-a-ux-workflow/>
27. Adobe After Effects. <https://forums.creativecow.net/thread/2/1037619>

28. NetGrok's Network Graph Visualization. https://www.researchgate.net/figure/216017179_fig2_Fig-2-NetGrok%27s-Network-Graph-Visualization
29. The Multi Router Traffic Grapher. <http://oss.oetiker.ch/mrtg/>
30. Visualization Techniques for Assessing Textual Topic Models. <http://vis.stanford.edu/papers/termite>
31. Netmon. <http://www.netmon.com/category/how-to-tutorial-network-monitor/>
32. HINTON DIAGRAM. <https://cs.brown.edu/people/daeil/research.html>
33. Correlation Matrix. <http://www.sthda.com/english/wiki/visualize-correlation-matrix-using-correlogram>
34. Node Quilts. <https://eagereyes.org/techniques/graphs-hairball>
35. PWM graph. <http://www.nlvocables.com/blog/?p=188>
36. Timeline visualization. <http://itblog.emc.com/2014/12/12/smart-data-visualization-helping-decision-makers-get-the-picture/>