Tips of Allowlist Based Firewall Operation for the Tokyo 2020 Games

OSAWA Yoshika SASAKI Junichi ASOU Takamichi IWASA Isao

Abstract

The data network for the Olympic and Paralympic Games Tokyo 2020 adopted the Allowlist firewall system as a network-level security measure. After two and a half years of operating the access control lists (ACLs) on the firewalls installed in the data network for the Games, including the preparation period, the total number of ACLs at the time of the Games was over 400,000 lines (up to 260,000 lines for a single FW). This article introduces the operations performed to keep this huge number of ACLs consistent with the network policy without misconfiguration.

Keywords : Tokyo 2020 Games, Allowlist, Firewall, ACL, Security policy

1. Introduction

The Allowlist scheme clarifies necessary communication information (IP addresses and port numbers) in advance as communication requirements, and blocks all communication that does not meet these requirements.

While this method provides strong security, it is complicated because the number of access control lists (ACLs) set in the firewall (FW : Firewall) is huge, and the FW settings must be added or deleted each time the communication requirements updated due to changes in the environment, such as installation of servers or construction of venues. And complexity in operation can be prone to configuration errors. So that, this method is extremely rare to be adopted in enterprises.

However, in case of the data network for the Olympic and Paralympic Games Tokyo 2020 (hereinafter referred to as "Tokyo 2020 Games") we dared to take on this challenge as the network infrastructure supporting a mission-critical international event, and overcame a number of problems through well designed workflow, operation, and thorough auditing.

This article describes the efforts made for the operation and management of FWs in the Games Data Network, using the "Allowlist" method, as described in Section "2-2 Architecture of Data Network for the Tokyo 2020 Games".

2. ACL Management of FWs

FW is a device that increase security by controlling network-level connectivity, and the configuration information for controlling them is called ACL.

In the Games Data Network, FWs were deployed in the Data Centre where servers related to the Games operation were deployed, and in all the 57 venues where the Games Data Network was available.

The information to create ACLs for the FWs was managed by the communication requirements tables submitted by each of the 52 Functional Areas (FAs) of

OSAWA Yoshika
Technology Planning Department, Nippon Telegraph and Telephone Corporation
E-mail Yoshika.osawa@ntt.com
SASAKI Junichi
Network Business Headquarters, Nippon Telegraph and Telephone East Corporation
E-mail j.sasaki@east.ntt.co.jp
ASOU Takamichi
New Business Development Headquarters, Nippon Telegraph and Telephone East Corporation
E-mail Takamichi.asou.yv@east.ntt.co.jp
IWASA Isao
Network Business Headquarters, Nippon Telegraph and Telephone East Corporation
E-mail i.iwasa@east.ntt.co.jp

The Journal of The Institute of Electronics, Information and Communication Engineers, Vol.105, No.8, Supplement, pp.32-37, August 2022

the Organising Committees using the Games Data Network. The total number of ACLs at the beginning of the Tokyo 2020 Games exceeded 400,000 lines, of all the FWs, the one that set most ALCs was the FW installed in the Primary Data Centre (PDC) which had more than 260,000 lines (Table 1).

Table 1　Number of ACLs for Major Venues

	Venue	Equipment	Number of ACLs
1	PDC (Primary Data Centre)	PDC-OIN-FW	263,290
2		PDC-SVMGMT-FW	6,311
3		PDC-OTN-FW	65,675
4	SDC (Secondary Data Centre)	SDC-OIN-FW	124,167
5		SDC-SVMGMT-FW	688
6		SDC-OTN-FW	1,803
7	International Broadcasting Centre	IBC-OIN-UTM	4,113
8	Main Press Centre	MPC-OIN-UTM	2,284
9	Olympic Stadium	OLS-OIN-UTM	1,921
10	Technology Operation Centre	TOC-OIN-UTM	2,645

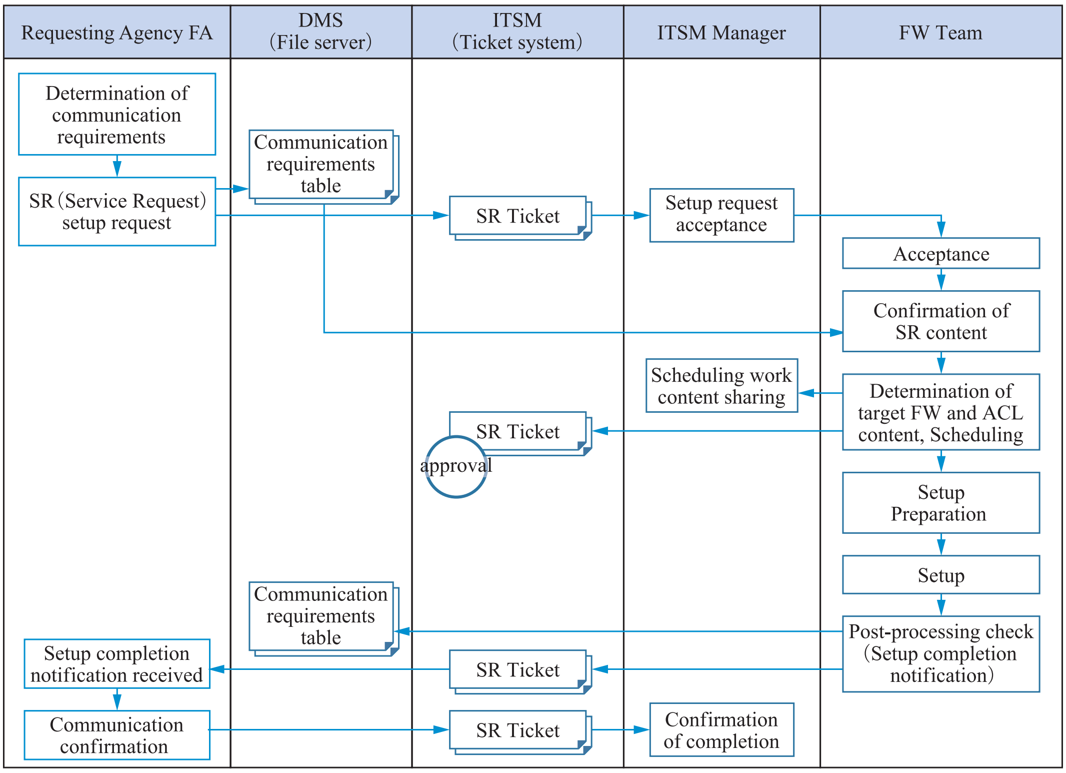
3. Operation and Management of ACL Configuration

3.1　Development of ACL Configuration Workflow

Requests for ACL configuration changes in FWs were managed in work units called Service Requests (SRs).

Each FA filled out the communication requirement tables with the requested information, registered it in the Document Management System (DMS), and submitted the SR through the ticketing system (ITSM). The FW setup team was responsible for the ACL settings. Since SRs were expected to be submitted in large volumes, an ITSM manager was assigned to manage the progress of the tickets.

After receiving a work request from the ITSM manager, the FW configuration team checked the work content, determined the target FW and the ACL content, coordinated schedule for the work date, executed the work, reviewed the results of the work, updated the communication requirements tables, and reported the work completion in the SR ticket. After confirming the completion of the work by ITSM, each FA confirmed the communication and closed the SR ticket (Figure 1).



Requesting Agency FA
DMS (File server)
ITSM (Ticket system)
ITSM Manager
FW Team
Determination of communication requirements
Communication requirements table
SR (Service Request) setup request
SR Ticket
Setup request acceptance
Acceptance
Confirmation of SR content
Scheduling work content sharing
Determination of target FW and ACL content, Scheduling
SR Ticket
approval
Setup Preparation
Setup
Communication requirements table
Post-processing check (Setup completion notification)
Setup completion notification received
SR Ticket
Communication confirmation
SR Ticket
Confirmation of completion

Figure 1　FW Setting Workflow　The workflow from the FA issues the configuration request to confirm the result of the work, and closes the ticket. A responsible person was assigned to each of the requester FA, ticket manager, and FW team to prevent omissions.

3.2 Maintenance of Communication Requirement Tables

The communication requirement tables contained the ID, work contents (setting request flag), source information (name, IP address, protocol, port number), and destination information (name, IP address, port number) for each requirement. Listing the work targets by both name and IP address was to make it easier for the requesting FA and for the approver to identify the targets. The communication requirement tables were updated by overwriting the same files, and the versions were managed by using DMS.

3.3 Preparation for FW Setting

3.3.1 Extraction of Work Contents

After the SR ticket was submitted, the ITSM manager instructed the FW setup team to start the preliminary preparations by downloading the communication requirements tables for the SR from the DMS, confirming that there were no discrepancies between the contents of the SR and the communication requirements tables, and then checking the differences with the versions of the communication requirements tables received in the most recent SR using a tool for requirements comparison.

This process detected omissions in the configuration request flags and prevented discrepancies between the communication requirements tables and the configuration information to be applied to the equipment.

3.3.2 Extraction of Communication Requirements for Each FW

As described in Section 2, the total number of communication requirement tables submitted by FAs amounted to 172. But the communication requirement tables did not contain information of FWs to be worked on, so communication requirements for each FW were added (Figure 2).

If the impact of the settings on the Games Data Network for the competition was significant, the configuration information was applied to the FWs prepared for verification, and the correctness of the settings and the operational status of the FWs were confirmed.

3.4 FW Configuration and Verification

The requirement tables compiled for each FW was batch-registered to the FW management server through the API using an in-house batch installation tool (Figure 3).

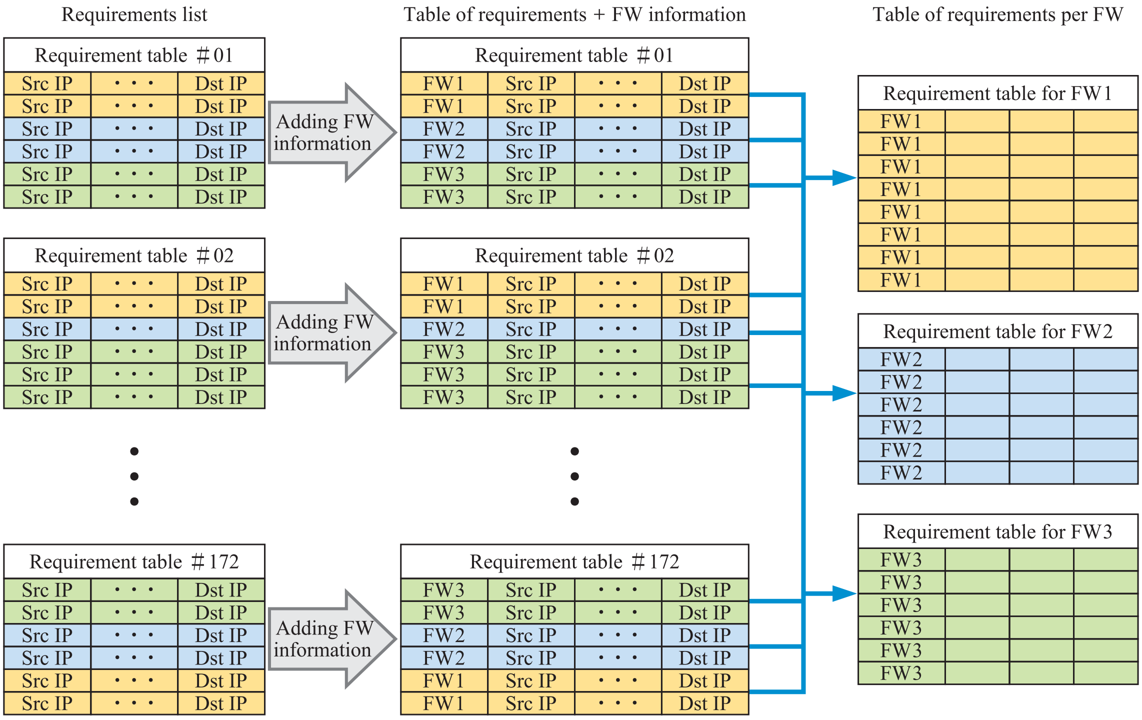

Requirements list
Table of requirements + FW information
Table of requirements per FW
Requirement table ＃01
Requirement table ＃02
Requirement table ＃172
Src IP
・・・
Dst IP
Adding FW information
FW1
FW2
FW3
Requirement table for FW1
Requirement table for FW2
Requirement table for FW3

Figure 2 Image of Extracting Requirements to Be Submitted to Each FW The FWs to be worked on are allocated by each requirement listed in the communication requirement table created by the requester FA, and a requirement table for each FW is created.

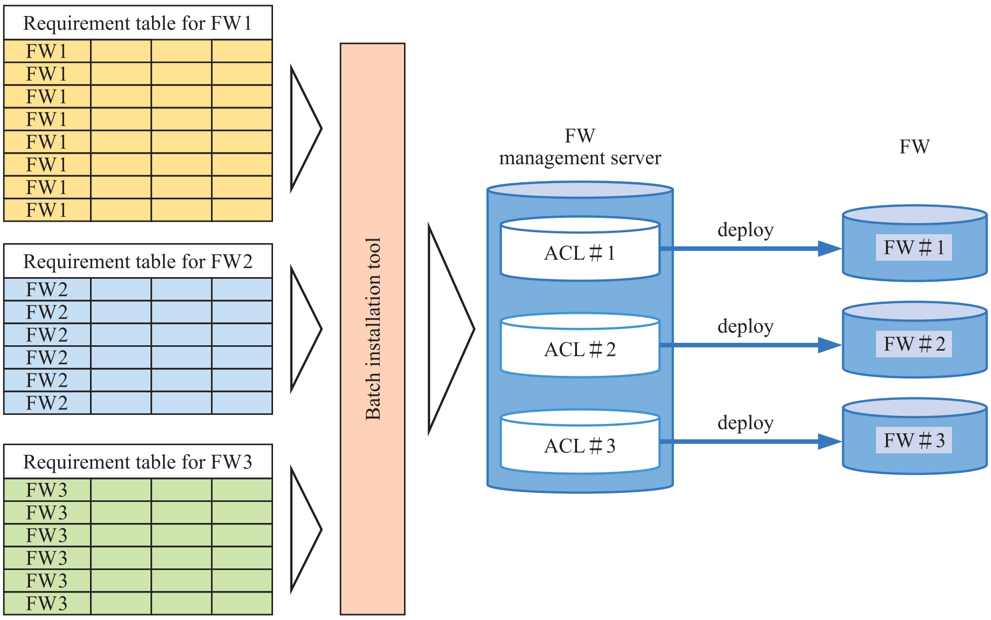


Figure 3　Image of using the Batch Installation Tool　The requirement list for each FW is registered in the FW management server using the batch installation tool, and then the configuration information is reflected in the individual FWs.

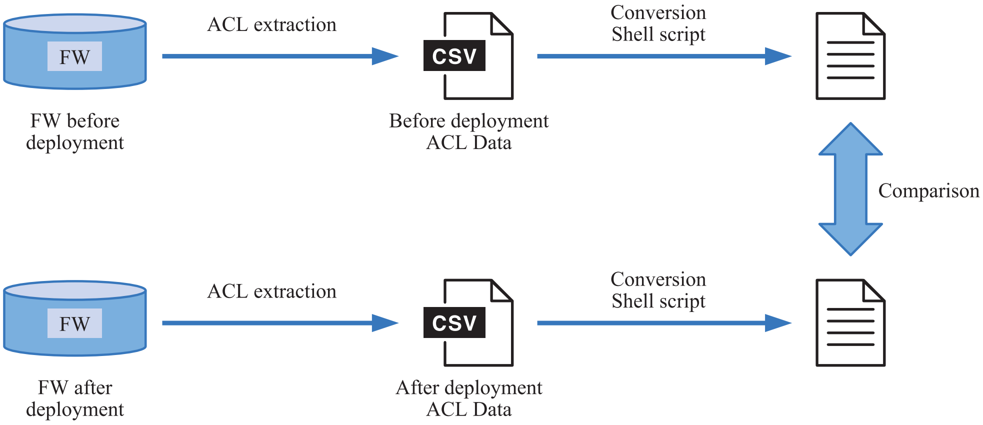


Figure 4　Comparison of Differences Before and After Deployment　The configuration information before and after reflecting ACL configuration information in FWs is compared, and it is confirmed that the result of the work is consistent with the desired result.

The key to this process was to obtain the ACL settings of the FW before deployment and to compare them with the ACL settings after deployment in the post-processing step.

3.5　Post-configuration Processing

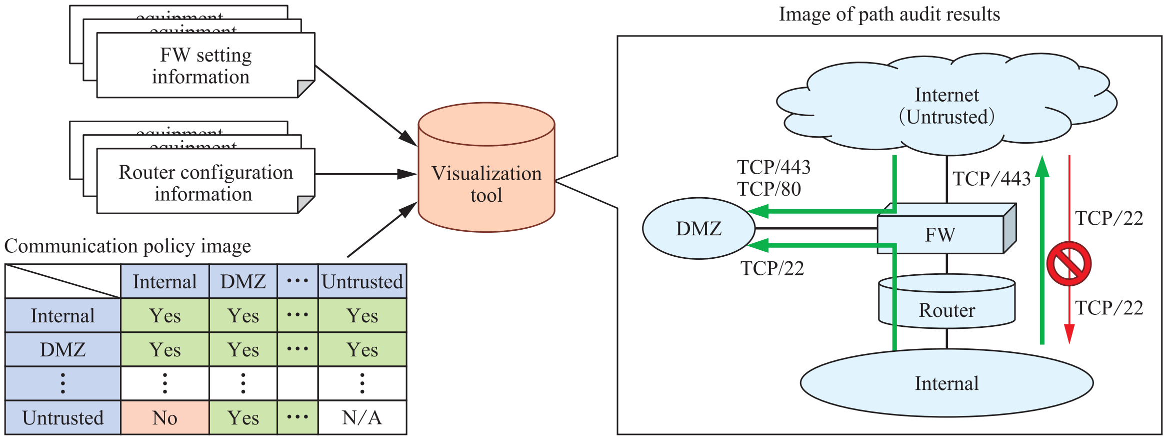
As a post-processing check, we created a tool to check the differences in ACLs before and after deployment, and used it to confirm that the work performed had the desired results (Figure 4).

After the post-processing check was completed by comparing with the ACL settings before and after deployment, the work was flagged as completed in the communication requirement table and registered in the DMS. A SR was issued to the ITSM indicating that the work was completed.

After receiving the SR from ITSM, the requester FA confirmed the communication and closed the ticket.

4.　ACL Audit

The check processes described so far in the FW setup work are all procedures to correctly reflect the communication requirements requested by the FA in



	Internal	DMZ	⋯	Untrusted
Internal	Yes	Yes	⋯	Yes
DMZ	Yes	Yes	⋯	Yes
⋮	⋮	⋮		⋮
Untrusted	No	Yes	⋯	N/A

Figure 5 Image of Path Audit The communication policy states that communication between Internal and Untrusted is No. If all of setting conform to policy, all paths will be drawn in green. However, in this example, communication path is opened for TCP/22 between Internal and Untrusted, then the path in red indicates the existence of an offending path.

the target device. In order to be more flawlessly, the audit was conducted to check the ACL settings from the following two perspectives :

- Comparison of the communication requirement table and the ACLs of the FW.
- Comparison of ACLs and routing information with communication policy (path auditing).

4.1 Comparison of Communication Requirement Table and ACLs

In the FW configuration work, we constructed a flow to ensure that the differences in the communication requirement tables are set, but we cannot eliminate the possibility that human error may be occurred during long-term operation. Therefore, we made an in-house tool to compare the communication requirement table and ACL configuration information, and conducted periodic audits to ensure that all the contents of the communication requirement tables were surely configured in the FW.

4.2 Path Auditing

Path auditing is used to verify the reachability of application level between segments of the network based on the ACLs of FWs and routing information of network devices, and to confirm whether there are communication paths that violate the communication policy specified at the time of design (Figure 5).

The audit targeted routers and FWs of the BON and CPN that were critical to the operation of the Tokyo 2020 Games (PDC : 21 units, Venue : 258 units). Although no fatal policy violations were detected during the Tokyo 2020 Games period, we were able to point out that the management documents had not been updated for the exceptionally permitted paths.

5. Conclusion

This article has described the process management and auditing methods that enabled the operation of an Allowlist-type FW with more than 400,000 lines of ACLs, which achieved consistent network segmentation without omissions, even though configuration change requests were made almost every week for about two and a half years starting in March 2019.

This article focuses on the completed workflow at the time when the operation was established to start the Tokyo 2020 Games, but the road to operational maturity was not an easy one. For example, in the beginning, the understanding of the communication requirements among the parties concerned, including FAs varied, then changes to the format were sometimes unavoidable. Even when format changes were decided upon, careful explanation and adequate time were needed to ensure that the need for such changes was understood. The number and timing of servers and other equipment installed by each FA varied, and when the requests were concentrated, the workload was more than we could have expected.

During the Tokyo 2020 Games, we observed approximately 450 million security events and were able to properly handle and block all of them. However, the Allowlist based micro-segmentation we have created ensures that even if attackers who wanted to launch cyberattacks on the Tokyo 2020 Games were to penetrate deep into the network bypassing the many layers of security measures, it would not be easy for them to conduct their activities.

(Received February 28, 2022 ; Revised March 23, 2022)

OSAWA Yoshika

Completed his master's degree at the University of Tokyo Graduate School of Engineering in 2015. He joined Nippon Telegraph and Telephone East Corporation in the same year, and has been engaged in the design, construction, and operation of the FW deployed in the data network for the Tokyo 2020 Games since 2018. Currently, he works at the Technology Planning Division of Nippon Telegraph and Telephone Corporation.

SASAKI Junichi

Completed his master's degree in information engineering at Muroran Institute of Technology in 2000. He joined Nippon Telegraph and Telephone East Corporation in the same year. Since then, he has been engaged in telecommunication services, development of security infrastructure, and promotion of security business. Currently, he is a chief of the Office of Network Security at Nippon Telegraph and Telephone East Corporation.

ASOU Takamichi

Completed his master's degree at Gunma University in 2007. He completed his master's course at the University of Information Security in 2013. He has been engaged in cyber security policy review and operation. Currently, he is the Manager in charge of Security Services, Business Development Division 3, at Nippon Telegraph and Telephone East Corporation.

IWASA Isao

Completed his master's degree at Saitama University in 1989. He joined Nippon Telegraph and Telephone Corporation in the same year, and has been with Nippon Telegraph and Telephone East Corporation since 2008. Since then, he has been engaged in service development and security-related work for telecommunications services. Currently, he is the General Manager of the Office of Network Security at Nippon Telegraph and Telephone East Corporation.