ATLANTIS PRESS International Journal of Networked and Distributed Computing, Vol. 5, No. 2 (April 2017) 62–70

Functional Evaluation of the Cloud Type Virtual Policy Based Network Management Scheme for the Common Use between Plural Organizations

Kazuya Odagiri [1], Shogo Shimizu [2], Naohiro Ishii [3]

[1] Sugiyama Jogakuen University,
17-3 Hosigaokamotomachi Chikusa-ku
Nagoya, Aichi 464-8662, Japan
E-mail: kodagiri@sugiyama-u.ac.jp, kazuodagiri@yahhoo.co.jp

[2] Gakushuin Women's College,
3-20-1 Toyama Shinzyuku-ku
Tokyo 162-8650, Japan
E-mail: shogo.shimizu@gakushuin.ac.jp

[3] Aichi Institute of Technology,
1247 Yachigusa Yakusa-cho
Toyota Aichi 470-0392, Japan
E-mail: ishii@aitech.ac.jp

Abstract

In the current Internet system, there are many problems using anonymity of the network communication such as personal information leaks and crimes using the Internet system. This is why TCP/IP protocol used in Internet system does not have the user identification information on the communication data, and it is difficult to supervise the user performing the above acts immediately. As a study for solving the above problem, there is the study of Policy Based Network Management (PBNM). This is the scheme for managing a whole Local Area Network (LAN) through communication control for every user. In this PBNM, two types of schemes exist. The first is the scheme for managing the whole LAN by locating the communication control mechanisms on the path between network servers and clients. The second is the scheme of managing the whole LAN by locating the communication control mechanisms on clients. As the second scheme, we have studied theoretically about the Destination Addressing Control System (DACS) Scheme. By applying this DACS Scheme to Internet system management, we will realize the policy-based Internet system management. In this paper, as the progression phase of the third phase for the last goal, we perform the functional evaluation of the cloud type virtual PBNM, which can be used by plural organizations.

1. Introduction

In the current Internet system, there are many problems using anonymity of the network communication such as personal information leaks and crimes using the Internet system. The news of the information leak in the big company is sometimes reported through the mass media. Because TCP/IP protocol used in Internet system does not have the user identification information on the communication data, it is difficult to supervise the user performing the above acts immediately. As studies and technologies for managing Internet system realized on TCP/IP protocol, those such as Domain Name System (DNS), Routing protocol, Fire Wall (F/W) and Network address port translation (NAPT)/network address translation (NAT) are listed. Except these studies, various studies are performed elsewhere. However, they are the studies for managing the specific part of the

Internet system, and have no purpose of solving the above problems.

As a study for solving the problems, Policy Based Network Management (PBNM) [2] exists. The PBNM is a scheme for managing a whole Local Area Network (LAN) through communication control every user, and cannot be applied to the Internet system. This PBNM is often used in a scene of campus network management. In a campus network, network management is quite complicated. Because a computer management section manages only a small portion of the wide needs of the campus network, there are some user support problems. For example, when mail boxes on one server are divided and relocated to some different server machines, it is necessary for some users to update a client machine's setups. Most of computer network users in a campus are students. Because students do not check frequently their e-mail, it is hard work to make them aware of the settings update. This administrative operation is executed by means of web pages and/or posters. For the system administrator, individual technical support is a stiff part of the network management. Because the PBNM manages a whole LAN, it is easy to solve this kind of problem. In addition, for the problem such as personal information leak, the PBNM can manage a whole LAN by making anonymous communication non-anonymous. As the result, it becomes possible to identify the user who steals personal information and commits a crime swiftly and easily. Therefore, by applying the PBNM, we will study about the policy-based Internet system management.

In the existing PBNM, there are two types of schemes. The first is the scheme of managing the whole LAN by locating the communication control mechanisms on the path between network servers and clients. The second is the scheme of managing the whole LAN by locating the communication control mechanisms on clients. It is difficult to apply the first scheme to Internet system management practically, because the communication control mechanism needs to be located on the path between network servers and clients without exception. Because the second scheme locates the communication control mechanisms as the software on each client, it becomes possible to apply the second scheme to Internet system management by devising the installing mechanism so that users can install the software to the client easily.

As the second scheme, we have studied theoretically about the Destination Addressing Control System (DACS) Scheme. As the works on the DACS Scheme, we showed the basic principle of the DACS Scheme, and security function [14]. After that, we implemented a DACS System to realize a concept of the DACS Scheme. By applying this DACS Scheme to Internet system, we will realize the policy-based Internet system management. Then, the Wide Area DACS system (wDACS system) [15] to use it in one organization was showed as the second phase for the last goal. As the first step of the second phase, we showed the concept of the cloud type virtual PBNM, which could be used by plural organizations [16]. In this paper, as the progression phase of the third phase for the last goal, we perform the functional evaluation to confirm the possibility of the cloud type virtual PBNM for the use in plural organizations. In Section II, motivation and related research for this study are described. In Section III, the existing DACS Scheme and wDACS Scheme is described. In section IV , the proposed scheme and evaluation results are described.

2. Motivation and Related Reserach

In the current Internet system, problems using anonymity of the network communication such as personal information leak and crimes using the Internet system occur. Because TCP/IP protocol used in Internet system does not have the user identification information on the communication data, it is difficult to supervise the user performing the above acts immediately.

As studies and technologies for Internet system management to be comprises of TCP/IP [1], many technologies are studied. For examples, Domain name system (DNS), Routing protocol such as Interior gateway protocol (IGP) such as Routing information protocol (RIP) and Open shortest path first (OSPF) , Fire Wall (F/W), Network address translation (NAT) / Network address port translation (NAPT) , Load balancing, Virtual private network (VPN), Public key infrastructure (PKI), Server virtualization. Except these studies, various studies are performed elsewhere. However, they are for managing the specific part of the Internet system, and have no purpose of solving the above problems.

As a study for solving the above problem, the study area about PBNM exists. This is a scheme of managing a

whole LAN through communication control every user. Because this PBNM manages a whole LAN by making anonymous communication non-anonymous, it becomes possible to identify the user who steals personal information and commits a crime swiftly and easily. Therefore, by applying this policy- based thinking, we study about the policy-based Internet system management.

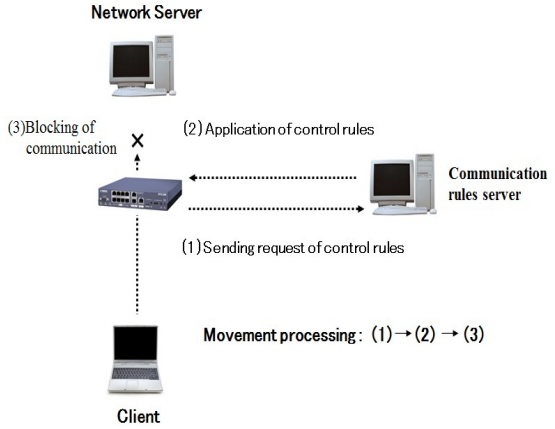


Figure 1. Principle in First Scheme

In policy-based network management, there are two types of schemes. The first scheme is the scheme described in Figure 1. The standardization of this scheme is performed in various organizations. In IETF, a framework of PBNM [2] was established. Standards about each element constituting this framework are as follows. As a model of control information stored in the server called Policy Repository, Policy Core Information model (PCIM) [3] was established. After it, PCMIe [4] was established by extending the PCIM. To describe them in the form of Lightweight Directory Access Protocol (LDAP), Policy Core LDAP Schema (PCLS) [5] was established. As a protocol to distribute the control information stored in Policy Repository or decision result from the PDP to the PEP, Common Open Policy Service (COPS) [6] was established. Based on the difference in distribution method, COPS usage for RSVP (COPS-RSVP) [7] and COPS usage for Provisioning (COPS-PR) [8] were established. RSVP is an abbreviation for Resource Reservation Protocol. The COPS-RSVP is the method as follows. After the PEP having detected the communication from a user or a client application, the PDP makes a judgmental decision for it. The decision is sent and applied to the PEP, and the PEP adds the control to it. The COPS-PR is the method of distributing the control information or decision result to the PEP before accepting the communication.

Next, in DMTF, a framework of PBNM called Directory-enabled Network (DEN) was established. Like the IETF framework, control information is stored in the server storing control information called Policy Server, which is built by using the directory service such as LDAP [9], and is distributed to network servers and networking equipment such as switch and router. As the result, the whole LAN is managed. The model of control information used in DEN is called Common Information Model (CIM), the schema of the CIM (CIM Schema Version 2.30.0) [11] was opened. The CIM was extended to support the DEN [10], and was incorporated in the framework of DEN.

In addition, Resource and Admission Control Subsystem (RACS) [12] was established in Telecoms and Internet converged Services and protocols for Advanced Network (TISPAN) of European Telecommunications Standards Institute (ETSI), and Resource and Admission Control Functions (RACF) was established in International Telecommunication Union Telecommunication Standardization Sector (ITU-T) [13].

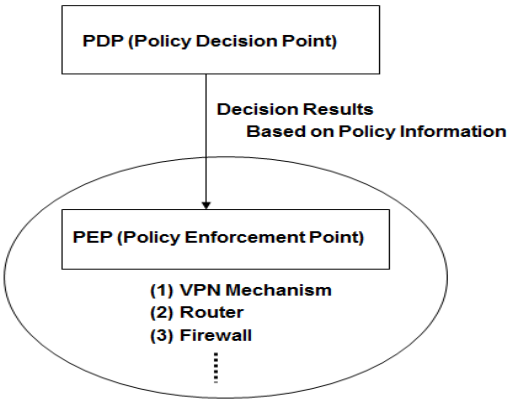


Figure 2. Essential Principle

However, all the frameworks explained above are based on the principle shown in Figure 1. As problems of these frameworks, two points are presented as follows. Essential principle is described in Figure 2. To be concrete, in the point called PDP (Policy Decision Point), judgment such as permission and non-

permission for communication pass is performed based on policy information. The judgment is notified and transmitted to the point called the PEP, which is the mechanism such as VPN mechanism, router and Fire Wall located on the network path among hosts such as servers and clients. Based on that judgment, the control is added for the communication that is going to pass by. The principle of the second scheme is described in Figure 3.By locating the communication control mechanisms on the clients, the whole LAN is managed. Because this scheme controls the network communications on each client, the processing load is low. However, because the communication control mechanisms need to be located on each client, the work load becomes heavy.

When it is thought that Internet system is managed by using these two schemes, it is difficult to apply the first scheme to Internet system management practically. This is why the communication control mechanism needs to be located on the path between network servers and clients without exception. On the other hand, the second scheme locates the communication controls mechanisms on each client. That is, the software for communication control is installed on each client. So, by devising the installing mechanism letting users install software to the client easily, it becomes possible to apply the second scheme to Internet system management. As a first step for the last goal, we showed the Wide Area DACS system (wDACS) system [15]. This system manages a wide area network, which one organization manages. Therefore, it is impossible for plural organizations to use this system.Then, as the first step of the second phase, we showed the concept of the cloud type virtual PBNM, which could be used by plural organizations in this paper.

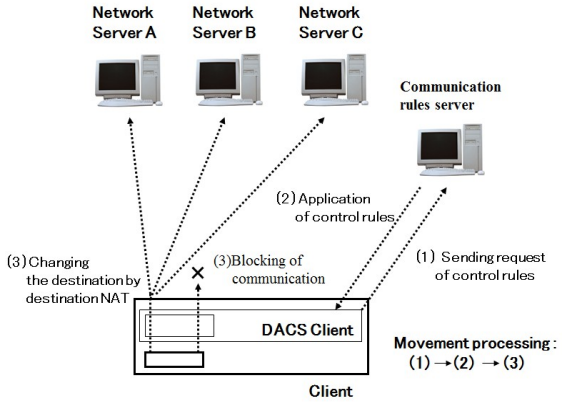


Figure 3. Principle in Second Scheme

3. Existing DACS SCHEME and wDACS System

In this section, the content of the DACS Scheme which is the study of the phase 1 is described.

3.1. Basic Principle of the DACS Scheme

Figure 4 shows the basic principle of the network services by the DACS Scheme. At the timing of the (a) or (b) as shown in the following, the DACS rules (rules defined by the user unit) are distributed from the DACS Server to the DACS Client.

(a) At the time of a user logging in the client.
(b) At the time of a delivery indication from the system administrator.

According to the distributed DACS rules, the DACS Client performs (1) or (2) operation as shown in the following. Then, communication control of the client is performed for every login user.

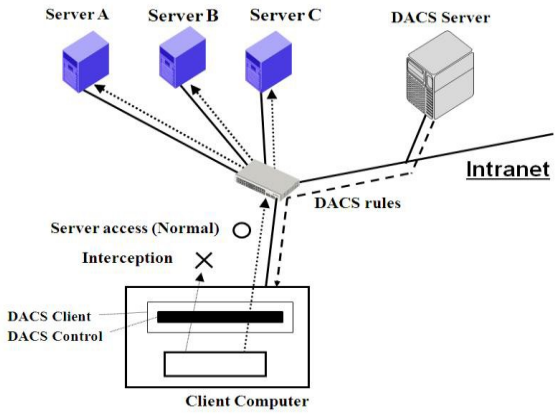


Figure 4. Basic Principle of the DACS Scheme

(1) Destination information on IP Packet, which is sent from application program, is changed.
(2) IP Packet from the client, which is sent from the application program to the outside of the client, is blocked.

An example of the case (1) is shown in Figure 4. In Figure 4, the system administrator can distribute a communication of the login user to the specified server among servers A, B or C. Moreover, the case (2) is described. For example, when the system administrator wants to forbid an user to use MUA (Mail User Agent), it will be performed by blocking IP Packet with the specific destination information.

In order to realize the DACS Scheme, the operation is done by a DACS Protocol as shown in Figure 5. As shown by (1) in Figure 5, the distribution of the DACS rules is performed on communication between the DACS Server and the DACS Client, which is arranged at the application layer. The application of the DACS rules to the DACS Control is shown by (2) in Figure 5.

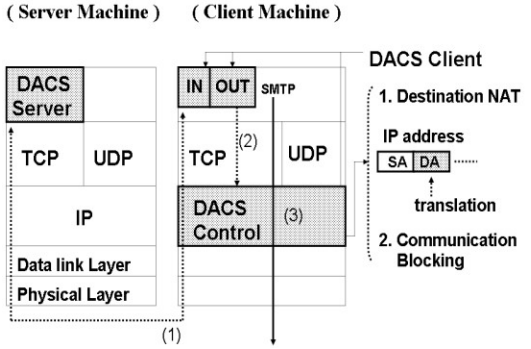


Figure 5. Layer Setting of the DACS Scheme

The steady communication control, such as a modification of the destination information or the communication blocking is performed at the network layer as shown by (3) in Figure 5.

3.2. Communication Control on Client

The communication control on every user was given. However, it may be better to perform communication control on every client instead of every user. For example, it is the case where many and unspecified users use a computer room, which is controlled. In this section, the method of communication control on every client is described, and the coexistence method with the communication control on every user is considered.

When a user logs in to a client, the IP address of the client is transmitted to the DACS Server from the DACS Client. Then, if the DACS rules corresponding to IP address, is registered into the DACS Server side, it is transmitted to the DACS Client. Then, communication control for every client can be realized by applying to the DACS Control. In this case, it is a premise that a client uses a fixed IP address. However, when using DHCP service, it is possible to carry out the same control to all the clients linked to the whole network or its subnetwork for example.

When using communication control on every user and every client, communication control may conflict. In that case, a priority needs to be given. The judgment is performed in the DACS Server side as shown in Figure 6. Although not necessarily stipulated, the network policy or security policy exists in the organization such as a university (1). The priority is decided according to the policy (2). In (a), priority is given for the user's rule to control communication by the user unit. In (b), priority is given for the client's rule to control communication by the client unit. In (c), the user's rule is the same as the client's rule. As the result of comparing the conflict rules, one rule is determined respectively. Those rules and other rules not overlapping are gathered, and the DACS rules are created (3). The DACS rules are transmitted to the DACS Client. In the DACS Client side, the DACS rules are applied to the DACS Control. The difference between the user's rule and the client's rule is not distinguished.

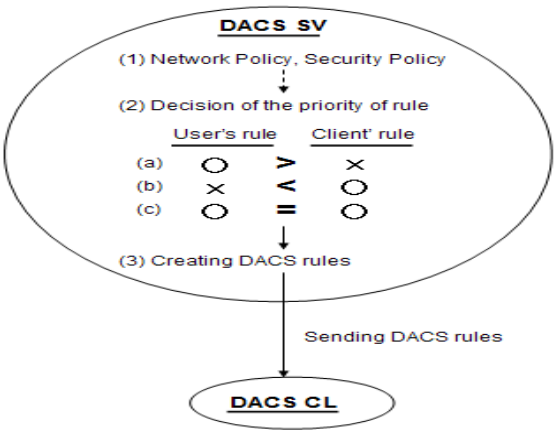


Figure 6. Creating the DACS rules on the DACS Server

3.3. Security Mechanism of the DACS Scheme

In this section, the security function of the DACS Scheme is described. The communication is tunneled and encrypted by use of SSH. By using the function of port forwarding of SSH, it is realized to tunnel and encrypt the communication between the network server and the, which DACS Client is installed in. Normally, to communicate from a client application to a network server by using the function of port forwarding of SSH, local host (127.0.0.1) needs to be indicated on that client application as a communicating server. The transparent use of a client, which is a characteristic of the DACS Scheme, is failed. The transparent use of a client means that a client can be used continuously without changing setups when the network system is updated. The function that doesn't fail the transparent use of a client is needed. The mechanism of that function is shown in Figure 7.

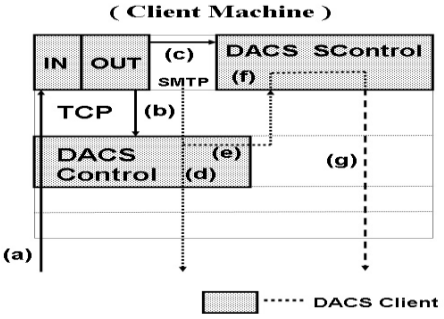


Figure 7. Extend Security Function

3.4. Application to cloud environment

In this section, the contents of wDACS system are explained in Figure 8.

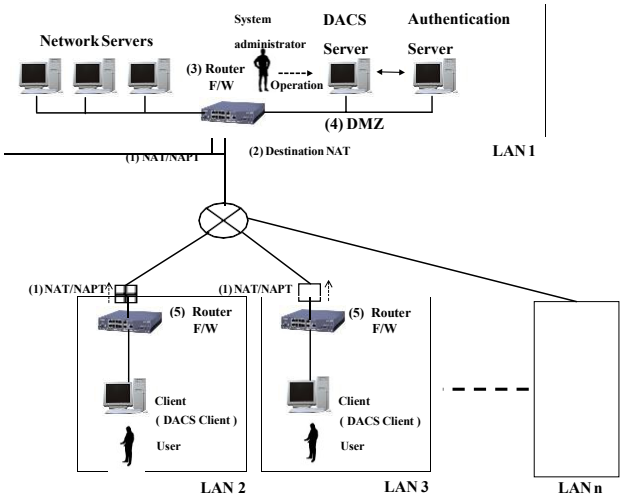


Figure 8. Basic System Configuration of wDACS system

First, as preconditions, because private IP addresses are assigned to all servers and clients existing in from LAN1 to LAN n, mechanisms of NAT/NAPT are necessary for the communication from each LAN to the outside. In this case, NAT/NAPT is located on the entrance of the LAN such as (1), and the private IP address is converted to the global IP address towards the direction of the arrow. Next, because the private IP addresses are set on the servers and clients in the LAN, other communications except those converted by Destination NAT cannot enter into the LAN. But, responses for the communications sent form the inside of the LAN can enter into the inside of the LAN because of the reverse conversion process by the NAT/NAPT. In addition, communications from the outside of the LAN1 to the inside are performed through the conversion of the destination IP address by Destination NAT. To be concrete, the global IP address at the same of the outside interface of the router is changed to the private IP address of each server. From here, system configuration of each LAN is described. First, the DACS Server and the authentication server are located on the DMZ on the LAN1 such as (4). On the entrance of the LAN1, NAT/NAPT and destination NAT exists such as (1) and (2). Because only the DACS Server and network servers are set as the target destination, the authentication server cannot be accessed from the outside of the LAN1. In the LANs form LAN 2 to LAN n, clients managed by the wDACS system exist, and NAT/NAPT is located on the entrance of each LAN such as (1). Then, F/W such as (3) or (5) exists behind or with NAT/NAPT in all LANs.

4. the Cloud Type Virtual PBNM for the common use between Plural organizations

In this section, after the concept and implementation of the proposed scheme were described, functional evaluation results are described.

4.1. Concept of the Cloud Type Virtual PBNM for the Common Use between Plural Organizations

In Figure 9 which is described in [16], the proposed concept is shown. Because the existing wDACS Scheme realized the PBNM control with the software called the DACS Server and the DACS client, other mechanism was not needed. By this point, application to the cloud environment was easy.

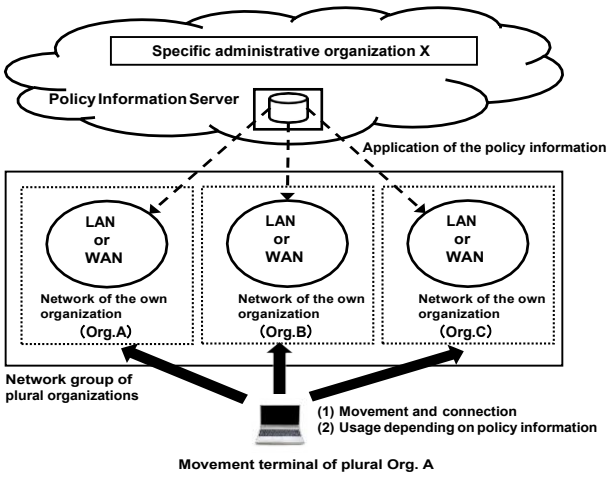


Figure 9. Concept of the proposed scheme

The proposed scheme in this paper realizes the common usage by plural organizations by adding the following elements to realize the common usage by plural organizations: user identification of the plural organizations, management of the policy information of the plural organizations, application of the PKI for code communication in the Internet, Redundant configuration of the DACS Server (policy information server), load balancing configuration of the DACS Server, installation function of DACS Client by way of the Internet

4.2. Implementation of the basic function in the Cloud Type Virtual PBNM for the Common Usage between Plural Organizations

In the past study [14], the DACS Client was operated on the windows operation system (Windows OS). It was because there were many cases that the Windows OS was used for as the OS of the client. However, the Linux operating system (Linux OS) had enough functions to be used as the client recently, too. In addition, it was thought that the case used in the clients in the future came out recently. Therefore, to prove the possibility of the DACS Scheme on the Linux OS, the basic function of the DACS Client was implemented in this study. The basic functions of the DACS Server and DACS Client were implemented by JAVA language. From here, it is described about the order of the process in the DACS Client and DACS Server as follows.

(Processes in the DACS Client)

(p1) The information acquisition from Cent OS

From the Linux OS (Cent OS) which the user logs in, the login user name and Internet domain name, the IP address which is setting on the Cent OS are acquired through the system environment variable.

(p2)Transmission from the DACS Client to the DACS Server

This part was implemented by use of the Socket class. The IP address and port number is set to the Socket, and the DACS Client is connected to the DACS Server on the server machine.

(p3) The information transmission from the DACS Client to the DACS Server

By use of getInputStream() in Socket class, this part was implemented. The information which is acquired from the Cent OS as described in (p1) to the DACS Server.

(p4) The reception of the DACS rules from the DACS Server

This part was implemented by using getInputStream() in the Socket class. This process is performed after the server side process.

(p5) Application of the DACS rules of the DACS Control

This function was implemented by the Runtime class. Because this function uses the function of “firewalld” which is equipped normally, the command of “firewall-cmd” to execute packet filtering and destination nat. After the DACS rules are received from the DACS Server, the DACS rules are applied to the DACS Control in the DACS Client by this process.

(Processes in the DACS Server)

(p1) The information reception from the DACS Client In this process, the DACS Server receives the information which is sent from the DACS Client. This process was implemented by the ServerSocket().

(p2) Connection to the database

In this process, the connection from the DACS Server to the PostgreSQL database is performed. This process was realized by the function of JDBC driver. To be concrete, it is implemented by the DriverManager class of JAVA.

(p3) Inquiry of the Database

Based on the information which receives from the DACS Client, the inquiry is performed in the form of using SQL language.

(p4) Transmission of the DACS rules to the DACS Client

The DACS Server sends the DACS rules which are created based on the information to the DACS Client. This Process was implemented by the createStatement method defined by the Connection Interface in JAVA. About the basic system which is realized by these processes, the prototype system was implemented.

4.3. Results of the functional evaluation

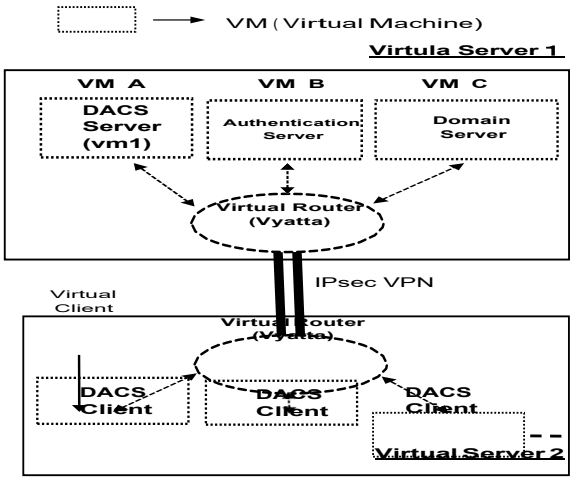
In this section, the results of the functional evaluation for the implementation system are described in Figure 10.

Two virtual servers which placed VMWare ESXi 5.1 were prepared. Each virtual server was constructed as follows.

(1) Virtual Server 1 (CPU：2.8GHz 4Core×1 Memory:16GB)

Virtualization software： VMWareESXi5.1

Virtual machine A：
Operating System (CentOS7)
Software for DACS Server
Virtual machine B：
Operating System (CentOS7)
Authentication server (OpenLDAP2.4)
Virtual machine C：
Operating System (CentOS7)
Windows domain server (Samba3.6)
Virtual router for a gateway (Vyatta6.6：64bit)
(2) Virtual Server 2 (CPU：2.6GHz 4Core×1 Memory:16GB)
Virtualization software： VMWareESXi5.1
Each virtual machine (5 virtual machine)：
Operating System (CentOS7)
Software for DACS Client



Virtual router for a gateway (Vyatta6.6：64bit)

Figure.10 Prototype system

Because we assumed that a service based on this scheme would be offered in the cloud environment, we prepared the experimental environment which each virtual router on each virtual server is connected by IPsec VPN each other.

The DACS Server was located on the virtual machine in the virtual server 1. The DACS Client was located on each virtual client in the virtual server 2, and the DACS Client was located on the CentOS in each virtual machine. The policy information was sent and received through the VPN connected by two virtual routers on each virtual server.

In Figure 11, the setting situation of the DACS rules is described in figure 11. This DACS rules is the rule to change a Web server for the access. The delivery of the DACS rules is between the DACS SV and the DACS CL encrypted by using SSL.

```
<?xml version="1.0" encoding="utf-8"?>
<direct>
  <rule priority="0" table="nat" ipv="ipv4" chain="PREROUTING_direct">
-d 192.168.1.10:80 -j DNAT --to 192.168.1.12:80</rule>


</direct>
```

Figure.11 Setting situation of the DACS rules on the DACS CL

By this DACS rules, the next operation was realized as described Figure 12. When the user accessed the Web Server A having the IP address of “192.168.1.10”, the Web Server B having the IP address of “192.168.1.12” was accessed actually. As for this communication result, the communication logs on the Web server A and Web server A were confirmed by viewing. In the communication log on the Web Server A, it was not possible to discover a trace of the access from the user. On the other hand, in the communication log on the Web Server B, it was not possible to discover the trace of the access from the user. By these log confirmation,

we objectively confirmed that the destination address change by DACS Client was carried out. That is, we confirmed that it is functionally possible to realize the cloud type virtual policy based network management scheme for the common use between plural organizations.

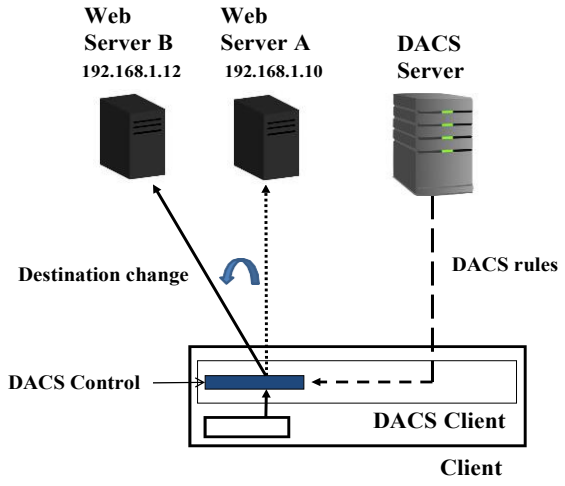


Figure.12 Destination Change on the DACS Client

5. Conclusion

In this paper, we perform the functional evaluation of the cloud type virtual PBNM, which can be used by plural organizations. This study is the third step of the third phase for the final goal of Internet management by the PBNM. In this study, the functional evaluation of the implemented prototype system was performed. As the result, with the communication between the DACS SV and the DACS CL, the normal movement was confirmed. By this evaluation, the technical possibility was confirmed. As a future work, we are going to perform a function experiment and the performance experiment of this system..

Acknowledgements

This work was supported by JSPS KAKENHI Grant Number 26730037. We express our gratitude.

References

1. V. CERF and E. KAHN, A Protocol for Packet Network Interconnection, IEEE Trans. on Commn **22**(5) (1974)637-648.
2. R. Yavatkar, D. Pendarakis and R. Guerin, A Framework for Policy-based Admission Control, IETF RFC 2753 (2000).
3. B. Moore at el., Policy Core Information Model -- Version 1 Specification, IETF RFC 3060 (2001).
4. B. Moore.,Policy Core Information Model (PCIM) Extensions, IETF 3460 (2003).
5. J. Strassner, B. Moore, R. Moats, E. Ellesson, Policy Core Lightweight Directory Access Protocol (LDAP) Schema, IETF RFC 3703 (2004).
6. D. Durham at el.,The COPS (Common Open Policy Service) Protocol, IETF RFC 2748 (2000).
7. S. Herzog at el.,COPS usage for RSVP, IETF RFC 2749 (2000).
8. K. Chan et al.,COPS Usage for Policy Provisioning (COPS-PR), IETF RFC 3084 (2001).
9. CIM Core Model V2.5 LDAP Mapping Specification (2002).
10. M. Wahl, T. Howes, S.Kille, Lightweight Directory Access Protocol (v3), IETF RFC 2251 (1997).
11. CIM Schema: Version 2.30.0 (2011).
12. ETSI ES 282 003: Telecoms and Internet converged Services and protocols for Advanced Network (TISPAN); Resource and Admission Control Subsystem (RACS); Functional Architecture, (2006).
13. ETSI ETSI ES 283 026: Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control; Protocol for QoS reservation information exchange between the Service Policy Decision Function (SPDF) and the Access-Resource and Admission Control Function (A-RACF) in the Resource and Protocol specifica-tion", (2006).
14. K. Odagiri , R. Yaegashi , M. Tadauchi, and N. Ishii, Secure DACS Scheme, Journal of Network and Computer Applications, Elsevier **31**(4) (2008) 851-861.
15. K. Odagiri, S. Shimizu,M. Takizawa and N. Ishii, Theoretical Suggestion of Policy-Based Wide Area Network Management System (wDACS system part-I), International Journal of Networked and Distributed Computing (IJNDC) **1**(4) (2013) 260-269.
16. K. Odagiri,S. Shimizu, N. Ishii, M. Takizawa, Suggestion of the Cloud Type Virtual Policy Based Network Management Scheme for the Common Use between Plural Organizations, in Proc of Int. Conf. on International Conference on Network-Based Information Systems (NBiS-2015)(Taipei, Taiwan, 2015),pp.180-186.