Load Experiment of the vDACS Scheme to Use between Plural Organizations for Applications to the Small and Medium Size Scale Organization

Kazuya Odagiri
Sugiyama Jogakuen University
Aichi, Japan
e-mail: kodagiri@sugiyama-u.ac.jp,
kazuodagiri@yahoo.co.jp

Naohiro Ishii
Aichi Institute of Technology
Aichi, Japan
e-mail: ishii@aitech.ac.jp

Shogo Shimizu
Gakushuin Women's College
Tokyo, Japan
e-mail: shogo.shimizu@gakushuin.ac.jp

Makoto Takizawa
Hosei University
Tokyo, Japan
e-mail: makoto.takizawa@computer.org

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 problem such as the personal information leaks, 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 by a user unit. In the 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 scheme to control on a client, 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 for the last goal, we perform the load experiment of the cloud type virtual PBNM named the vDACS Scheme, which can be used by plural organizations, for applications to the small and medium size scale organization.**

Keywords- policy-based netwok management; DACS Scheme; NAPT

I. 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. However, they are the studies for managing the specific part of the Internet system, and have no purpose of managing the whole Internet system.

As a study for managing the whole Internet system for the purpose of controlling it by a user unit, the PBNM [2] exists. The PBNM is a scheme for managing a whole Local Area Network (LAN) through communication control by a user unit, and cannot be applied to the Internet system. The 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. Since most of the computer network users in a campus are students and they do not check frequently their e-mail, it is difficult 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, 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. The client means a client

computer. It is difficult to apply a scheme for controlling on a network course to Internet system practically, because the communication control mechanism needs to be located on the path between network servers and clients without exception. Because the scheme for controlling on a client locates the communication control mechanisms as the software on each client, it becomes possible to apply the scheme for controlling on a client to Internet system by devising the installing mechanism so that users can install the software to the client easily.

As the scheme to control on a client, 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 scheme to Internet system, we will realize the policy-based Internet system management. Then, the Wide Area DACS system (wDACS system) used 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. In this paper, as the progression phase of the third phase for the last goal, we perform the load experiment 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 load experiment results are described.

II. MOTIVATION AND RELATED RESEARCH

In policy-based network management, there are two types of schemes. The scheme to control on a network course 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.
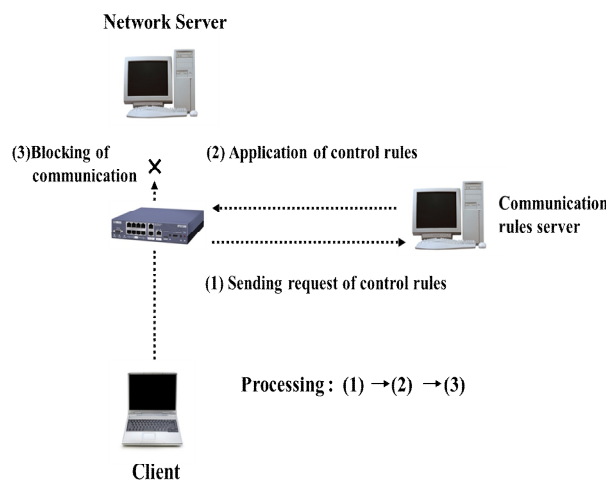

Figure 1. Principle in Scheme to Control on a Network Course

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].
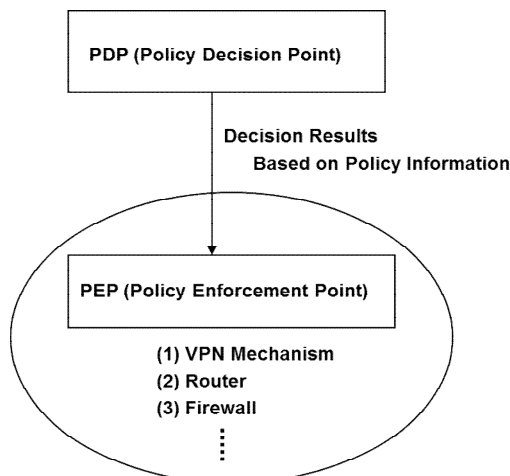
Figure 2. Essential Principle

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. Concretely, in the point called Policy Decision Point (PDP) 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, which is located on the network path among hosts (servers and clients). Based on that judgment, the control is added for the communication that is going to pass by.
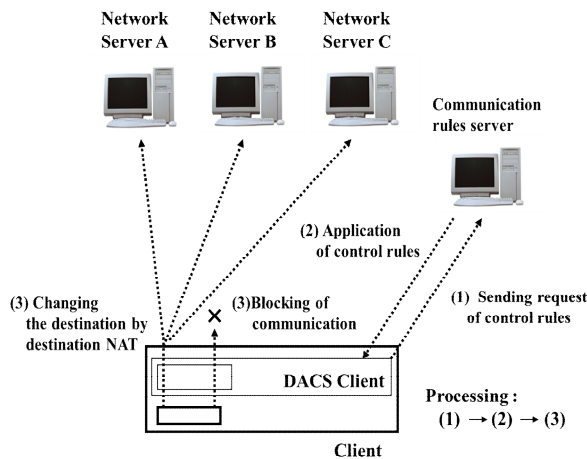

Figure 3. Principle in Scheme to Control on a Client

The principle of the scheme for controlling on a client 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 put a control unit on the network course practically. The communication control

mechanism needs to be located on the path between network servers and clients without exception. This is why, we devised the scheme for controlling the network on a client. The 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 scheme for controlling the network on a client to Internet system. 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.

III.   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.

A   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.

(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.
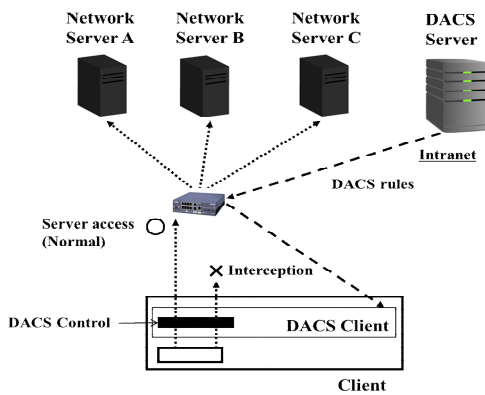
Figure 4. Basic Principle of the DACS Scheme

In order to realize the DACS Scheme, the operation is done by a DACS Protocol as shown in Figure 5. As shown by (1) of the double way arrow between DACS Server and IN block 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.
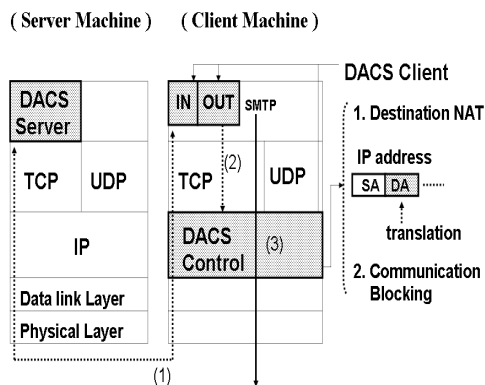

Figure 5. Layer Setting of the DACS Scheme

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.

B   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.
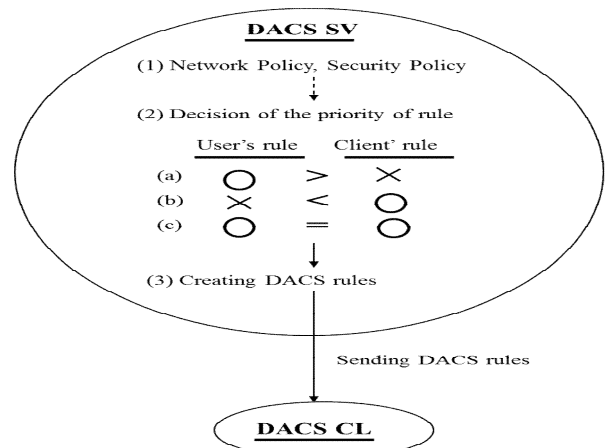

Figure 6. Creating the DACS rules on the DACS Server

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.

C   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 DACS Client, which is installed in the client. 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.
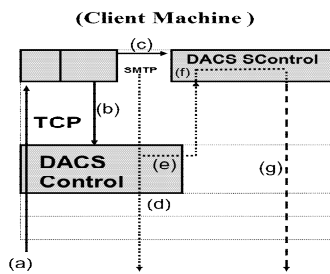
Figure 7. Extend Security Function

D Application to cloud environment

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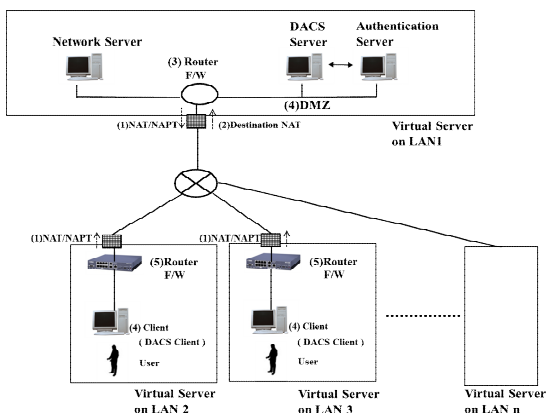

Figure 8. Basic System Configuration of wDACS System

IV. 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.

A. 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.
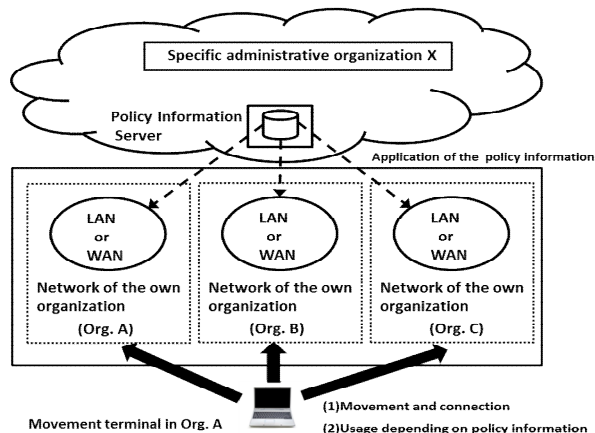

Figure 9. Concept of the Proposed Scheme

B. Implementation of the basic function in the

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 .

C. 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.
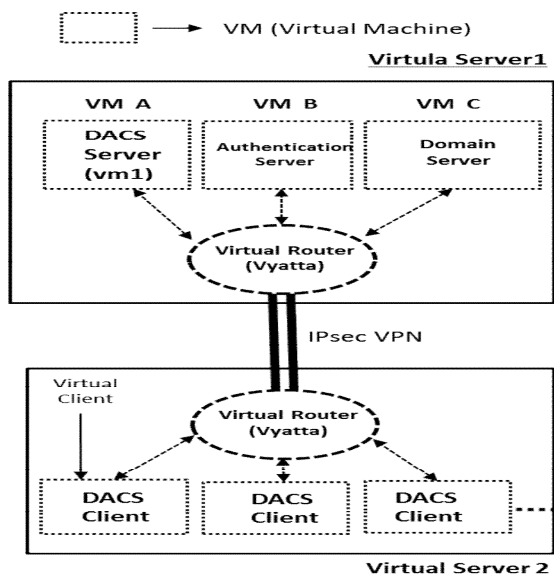
Figure.10 Prototype System

(Processes in the DACS Client)
(p1) The information acquisition from Cent OS
(p2) Transmission from the DACS Client to the DACS
(p3) The information transmission from the DACS Client to
(p4) The reception of the DACS rules from the DACS Server
(p5) Application of the DACS rules of the DACS Control

(Processes in the DACS Server)
(p1) The information reception from the DACS Client
(p2) Connection to the database
(p3) Inquiry of the Database
(p4) Transmission of the DACS rules to the DACS Client

D. Results of the functional evaluation

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

```
<?XML version="1.0" encoding="uft8"?>

<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

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.

By this DACS rules, the next operation was realized. When the user accessed the Web Server with the IP address of 192.168.1.10, the Web Server with the IP address of 192.168.1.12 was accessed actually. As for this communication result, the communication log on each Web server was confirmed by viewing.

V. LOAD EXPERIMENT RESULTS

In this section, after the description of experimental environment, load experiment results are described.

A. Load experiment results to confirm the function of the software for realization of the Cloud Type Virtual PBNM for the Common Use Between Plural Organizations

In this section, the load experiment results are described. In the Figure 12, the experimental environment is described. This environment consists of four virtual servers. In the virtual server 1, servers group such as the DACS Server and user authentication server is stored. In other virtual severs such as the virtual server 2, virtual server 3 and virtual server 4, the virtual client, which is installed the DACS Client is stored. The number of the virtual clients is 100.
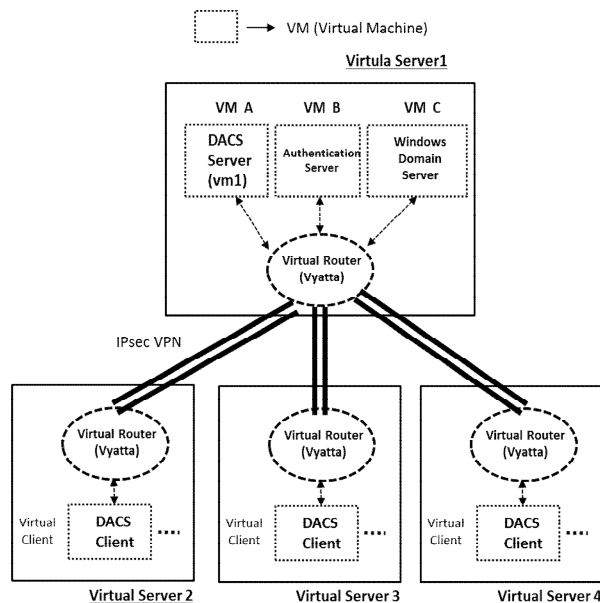

Figure.12 Experimental Environment

By using this experimental environment, the load experiment was executed. Specifically, simultaneous accesses for the DACS SV from the 100 virtual clients were performed at the rate of one time form 15 minutes. The number of the simultaneous connections for the DACS SV was set to 10 on this occasion. The experimental results are described in Table 1.

TABLE I. EXPERIMENTAL RESULTS (1)

	Practice time	CPU Consumption
1	2:02	268
2	2:18	268
3	2:33	276
4	2:48	251
5	3:03	261
6	3:18	252
7	3:33	248
8	3:48	265
9	4:03	265
10	4:18	278

In this table, the practice time of the DACL CL and CPU consumption is described. The average of the results of the

measurement for ten times was 263.2 MHz. This value is around three times of the value shown in Table 2.

TABLE II. EXPERIMENTAL RESULTS (2)

	CPU consumption
1	59
2	58
3	51
4	58
5	59
6	59
7	53
8	51
9	53
10	58

In the experiment of the Table 2, the Windows client is used, and the communications between the DACS SV and the DACS CL is not encrypted. In this experiment, the Linux client is used, and the communications between the DACS SV and the DACS CL is encrypted by SSL. Particularly, because an element of the overhead processes of the SSL is large, it is thought that such a result was derived.

B. Load experiment results for applications to the small and medium size scale organization

In this section, the load experiment results are described. The experimental environment is described. The experimental environment is as previous experiment environment. In this experiment, simultaneous accesses for the DACS SV from the 200 virtual clients were performed at the rate of one time form 15 minutes. The number of the simultaneous connections for the DACS SV was set to 10 on this occasion. The experimental results are described in Table 3.

TABLE III. EXPERIMENTAL RESULTS (3)

	Practice time	CPU Consumption
1	19:48	263
2	20:03	259
3	20:18	261
4	20:33	271
5	20:48	260
6	21:03	266
7	21:18	262
8	21:33	267
9	21:48	274
10	22:03	275

In this table, the average of the results of the measurement for ten times was 265.8 MHz. This value is same as the value shown in Table 1. In other words, when the number of the client is 200, CPU consumption of the DACS SV becomes the constant standard by limiting the number of simultaneous connections to 10.

VI. CONCLUSION

In this paper, we performed the load experiment of the cloud type virtual PBNM, which can be used by plural organizations. In this experiment, the 200 virtual clients with Linux OS are used, and the communications between the DACS SV and the DACS CL are encrypted. The number of the simultaneous connections for the DACS SV was set to 10 on this occasion. As the result, the average of CPU consumption was 265.8 MHz. It became possible to confirm the fact that CPU consumption of the DACS SV becomes about 263~265MHz by limiting the number of simultaneous connections to 10. By this experiment, it was confirmed this proposed scheme was applicable to the network with the 200 clients.

As a future work, we are going to perform more load experiments in the form of changing the number of the virtual clients and the number of the simultaneous connections for the DACS SV to show that it is applicable in a small and medium size scale network with the clients of around 1000.

REFERENCES

[1] V. Cerf and E. Kahin, "A Protocol for Packet Network Interconnection," IEEE Trans. on Commn, vol.COM-22, May 1974, pp.637-648.

[2] R. Yavatkar, D. Pendarakis, and R. Guerin, "A Framework for Policy-based Admission Control, " IETF RFC 2753, 2000.

[3] B. Moore, E. Ellesson, J. Strassner, and A. Westerinen, "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, and 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, and 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, June 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 specification, April 2006.

[14] K. Odagiri, R. Yaegashi,M. Tadauchi, and N. Ishii, "Secure DACS Scheme, "Journal of Network and Computer Applications," Elsevier, Vol.31, Issue 4, 2008, pp.851-861, November.