ESTABLISHMENT OF VIRTUAL POLICY BASED NETWORK MANAGEMENT SCHEME BY LOAD EXPERIMENTS IN VIRTUAL ENVIRONMENT

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

[1]Sugiyama Jogakuen University, Aichi, [2]Gakushuin Women's College, Tokyo and [3]Aichi Institute of Technology, Aichi, Japan

ABSTRACT

In the current Internet-based systems, there are many problems using anonymity of the network communication such as personal information leak and crimes using the Internet systems. This is because the TCP/IP protocol used in Internet systems 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 solution for solving the above problem, there is the approach of Policy-based Network Management (PBNM). This is the scheme for managing a whole Local Area Network (LAN) through communication control of 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 course 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 been studied theoretically about the Destination Addressing Control System (DACS) Scheme. By applying this DACS Scheme to Internet system management, we intend to realize the policy-based Internet system management finally. In the DACS Scheme, the inspection is not done about compatibility to cloud environment with virtualization technology that spreads explosively. As the result, the coverage of the DACS Scheme is limited only in physical environment now. In this study, we inspect compatibility of the DACS Scheme for the cloud environment with virtualization technology, and enlarge coverage of this scheme. With it, the Virtual DACS Scheme (vDACS Scheme) is established.

KEYWORDS

policy-based network management, DACS Scheme

1. INTRODUCTION

The current Internet system is a distributed autonomous system, and does not perform the unified safety and effective operation. When the Internet system is accessed by the user that does not understand structure of the Internet system very much, there are many problems using anonymity of the network communication, such as personal information leak and crimes using the Internet systems. The news of the information leak in the big company is sometimes reported through the mass media. On the other hand, the study for the purpose of putting the whole Internet system into the integrated management state is not performed now. Therefore, we aim at the realization of the secure and effective operative Internet system by promoting the study of the Internet Policy Based Network Management (Internet PBNM) under the long view. The Internet PBNM is the concept that we have proposed than before, and is the management scheme for managing the whole Internet system by applying the thinking of PBNM to it. In Figure 1, the image of Internet PBNM is described.

DOI: 10.5121/ijcnc.2016.8313

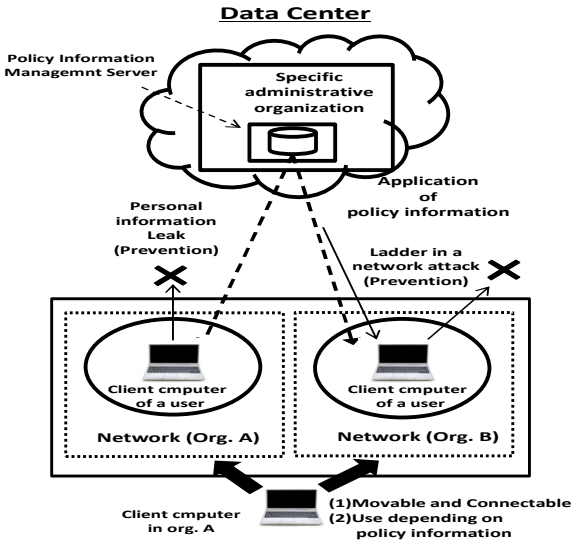

Figure 1 Internet PBNM

The study of the Internet PBNM has four steps as follows.

- (Step1) Study on the PBNM managing the network of the specific organization
- (Step2) Study on the PBNM managing the network group in the plural organizations
- (Step3) Study on the PBNM managing the network group in the local domain that is within a constant range
- (Step4) Study on the PBNM finally establishing Internet PBNM

In this paper, the study of the final stages in (Step1) is described. After the completion of this study, we are going to shift to (Step2). The existing PBNM realizes the network management of the own organization based on network policy and security policy. It manages the whole network of the specific organization through communication control (access control, encryption of the communication, quality of service). The existing PBNM is standardized in plural organizations such as Internet Engineering Task Force (IETF), Distributed Management Task Force (DMTF), Telecoms and Internet converged Services and protocols for Advanced Network (TISPAN) of European Telecommunications Standards Institute (ETSI), International Telecommunication Union Telecommunication Standardization Sector (ITU-T). However, when we aim at the realization of Internet PBNM by extending this existing PBNM, it becomes the required condition that a specific administrative organization manages the network which other organizations hold. The existing PBNM is the scheme that places the Policy Enforcement point (PEP) for communication control on the course of a network. Therefore, the administrative organization must change the other organization's network equipment. Then, the following problems occur.

(a) Outbreak of the additional cost by the change of the network equipment
(b) Network topology change by application of the existing PBNM
(c) Limits on security policy and network policy which is caused by the network equipment change by the administrative organization.

For the realization of Internet PBNM by application of the existing PBNM, these problems become a big hindrance. Because the problem of (c) becomes fatal especially, it becomes impossible to apply the existing PBNM to all organizations on Internet system. The authors decided to take the different approach. To be concrete, they aimed at the Internet PBNM by

realization of the PBNM scheme that does not need the network equipment change. As an initial stage, they performed the study of (Step1). First, they established the scheme placing the software PEP only to the physical client that is named Destination Addressing Control Scheme (DACS Scheme). The DACS Scheme controls the specific organization's network by communication control on the client. Because this DACS Scheme is the method to manage the physical clients distributed on the network, the inspection is not done about the compatibility to cloud environment with the virtualization technology that spreads explosively. As the result, the coverage of the DACS Scheme is limited only in physical environment now. In this study, we inspect the compatibility of the DACS Scheme for the cloud environment with virtualization technology, and enlarge the coverage of this scheme. With it, we assume that the Virtual DACS Scheme (vDACS Scheme) is established. After it, we will start the study of (Step2). The rest of this paper is organized as follows. Section 2 shows past works of the network management including the existing PBNM. In Section 3, we describe the mechanisms and effectiveness of the DACS scheme. In Section 4, the vDACS Scheme is established through functional experiment and processing load experiment.

2. MOTIVATION AND RELATED WORKS

In the current Internet system, the problems using anonymity of the network communication such as personal information leak and crimes using the Internet system occur. Because the 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 the studies and technologies for Internet system management other than TCP/IP [1][2], many technologies are studied as follow examples.

(1)Domain name system (DNS) [3]
(2)Routing protocol
(2-a) Interior gateway protocol (IGP) such as Routing information protocol (RIP) [4] and Open shortest path first (OSPF) [5]
(2-b) Exterior gateway protocol (EGP) such as Border Gateway Protocol (BGP) [6]
(3) Fire wall (F/W) [7]
(4) Network address translation (NAT) [8] / Network address port translation (NAPT) [9]
(5) Load balancing [10][11]
(6) Virtual private network (VPN) [12][13]
(7) Public key infrastructure (PKI) [14]
(8) Server virtualization [15]

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 problems, 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 have studied about the policy-based Internet system management. In policy-based network management, there are two types scheme. The first scheme is the scheme described in Figure 2. The standardization of this scheme is performed in various organizations. In IETF, a framework of PBNM [16] 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) [17] was established. After it, PCMIe [18] was established by extending the PCIM. To describe them in the form of Lightweight Directory Access Protocol (LDAP), Policy Core LDAP Schema

(PCLS) [19] 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) [20] was established. Based on the difference in distribution method, COPS usage for RSVP (COPS-RSVP) [21] and COPS usage for Provisioning (COPS-PR) [22] 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.

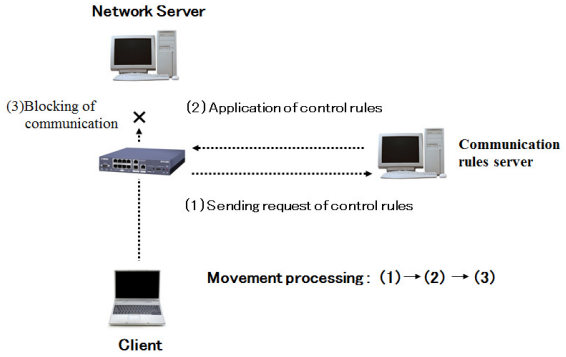

Figure 2 Principle in First Scheme

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 [23], 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） [24] was opened. The CIM was extended to support the DEN, and was incorporated in the framework of DEN. In addition, Resource and Admission Control Subsystem (RACS) [25] 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) [26] was established in International Telecommunication Union Telecommunication Standardization Sector (ITU-T).

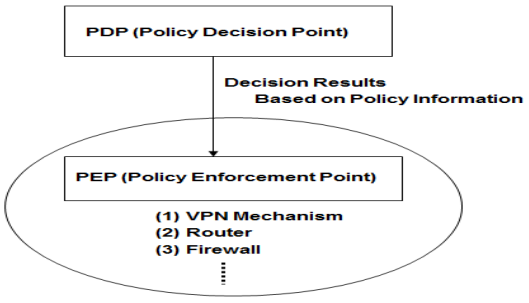

Figure 3 Essential Principle

However, all the frameworks explained above are based on the principle shown in Figure 2. Essential principle is described in Figure 3. 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 firewall 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 4 [27][28][29]. 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 course between network servers and clients without exception.

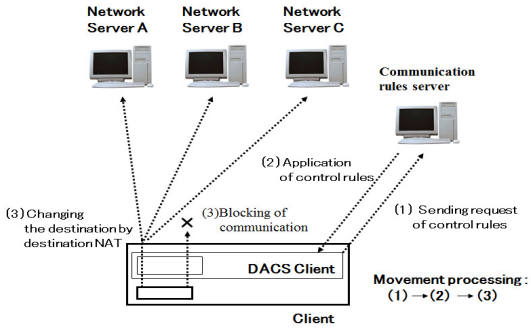

Figure 4 Principle in Second Scheme

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. Furthermore, this point is dissolved naturally when this scheme spread widely generally and the DACS Client becomes installed normally.

The studies of the second scheme are as follows.

(1) Suggestion of the principle in the DACS Scheme [27]
(2) Additional access control function for preventing the access from the physical client that does not have the PEP on it. [28]
(3) Processing load simulation in controlling a large number of physical clients [30]
(4) Software development for realization of the DACS Scheme [29]
(5) Operation and management system in the DACS Scheme [31]
However, the following problems are pointed out in the above study processes.
(d) Operation cost for placing the DACS Client on the physical client
(e) Guarantee of the DACS Client's placement on the physical client
(f) The network topology change that may occur at the time of an application of existing PBNM

In this study, we solve these problems by letting the DACS Scheme to recent trend of the client virtualization in company and university network. In other words, we establish Virtual DACS Scheme. In Section 2 related works and technologies are performed. In Section 3, the existing

DACS Scheme is explained. In section 4, explanation and evaluation of the vDACS Scheme are described. In Section V, conclusion of this study and directionality of the future study are described.

3. EXISTING DACS SCHEME

3.1 BASIC PRINCIPLE OF THE DACS SCHEME

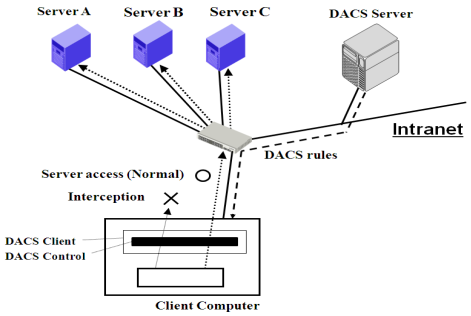

Figure 5 Basic Principle of the DACS Scheme

Figure 5 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 5. In Figure 5, 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 a 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 6. As shown by (1) in Figure 6, 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 6. 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 6.

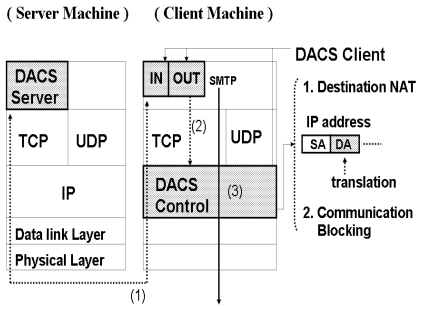

Figure 6 Layer Setting of the DACS Scheme

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 it's subnetwork for example.

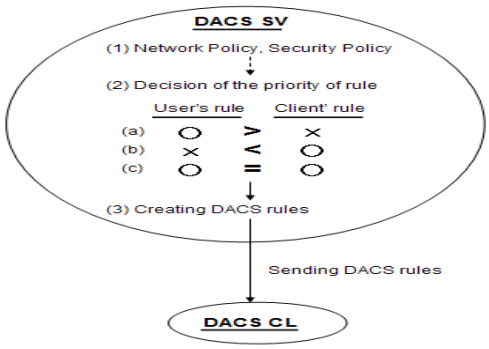

Figure 7 Creating the DACS rules on the DACS Server

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 7. 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.

3.2 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 8.The changed point on network server side is shown as follows in comparison with the existing DACS Scheme.

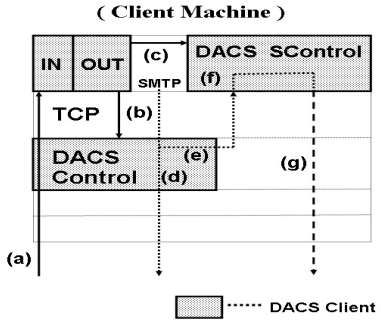

Figure 8 Extend Security Function

SSH Server is located and activated, and communication except SSH is blocked. In Figure 8 the DACS rules are sent from the DACS Server to the DACS Client (a). By the DACS Client that accepts the DACS rules, the DACS rules are applied to the DACS Control in the DACS Client (b). The movement to here is same as the existing DACS Scheme. After functional extension, as shown in (c) of Figure 8 the DACS rules are applied to the DACS SControl. Communication control is performed in the DACS SControl with the function of SSH. By adding the extended function, selecting the tunneled and encrypted or not tunneled and encrypted communication is done for each network service. When communication is not tunneled and encrypted, communication control is performed by the DACS Control as shown in (d) of Figure 8. When communication is tunneled and encrypted, destination of the communication is changed by the DACS Control to localhost as shown in (e) of Figure 8. After that, by the DACS STCL, the communicating server is changed to the network server and tunneled and encrypted communication is sent as shown in (g) of Figure 8, which are realized by the function of port forwarding of SSH. In the DACS rules applied to the DACS Control, localhost is indicated as the destination of communication. In the DACS rules applied to the DACS SControl, the network server is indicated as the destination of communication. As the functional extension explained in the above, the function of tunneling and encrypting communication is realized in the state of being suitable for the DACS Scheme, that is, with the transparent use of a client. Then, by changing the content of the DACS rules applied to the DACS Control and the DACS SControl, it is realized to distinguish the control in the case of tunneling and encrypting or not tunneling and encrypting by a user unit. By tunneling and encrypting the communication for one network service from all users, and blocking the untunneled and decrypted communication for that network service, the function of preventing the communication for one network service from the client, which DACS Client is not installed in is realized. Moreover, even if the communication to the network server from the client, which DACS Client is not installed in is permitted, each user can select whether the communication is tunneled and encrypted or not. The function of preventing information interception is realized.

3.3 SPECIFICATION OF THE DACS SYSTEM

(a) Communications between the DACS Server and the DACS Client

The Communications between the DACS Server and the DACS Client were realized by the communications through a socket in TCP/IP.

(b) Communication control on the client computer

In this study, the DACS Client working on windows XP was implemented. The functions of the destination NAT and packet filtering required as a part of the DACS Control were implemented by using Winsock2 SPI of Microsoft. As it is described in Figure 9 Winsock2 SPI is a new layer which is created between the existing Winsock API and the layer under it. To be concrete, though connect() is performed when the client application accesses the server, the processes of destination NAT for the communication from the client application are built in WSP connect() which is called in connect(). In addition, though accept() is performed on the client when the communication to the client is accepted, the function of packet filtering is implemented in WSPaccept() which is called in accept().

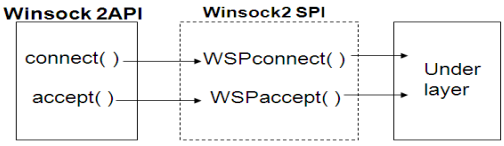

Figure 9 Winsock2 SPI

(c) VPN communication

The client software for the VPN communication, that is, the DACS SControl was realized by using the port forward function of the Putty. When the communication from the client is supported by the VPN communication, first, the destination of this communication is changed to the localhost. After that, the putty accepts the communication, and sends the VPN communication by using the port forward function.

3.4 POINTS OF SOFTWARE SPECIFICATIONS

The characteristic of the DACS System's implementation is the coping processes at the time of conflicting the relation between communication control every user and communication control every client. At this point, by using algorithm shown in Figure 10, the DACS System is implemented. First, as Action 1, the judgment table for client control is searched. If the IP address of the client exists in this table, Action 2 is performed. If not, Action 3 is performed. When Action 2 is performed, the control rules every client are searched and extracted from the IP address rule table which has control rules every client (every IP address). When Action 3 is performed, the judgment table for user control is searched. If the user logging in the client exists in this table, Action 4 is performed. If not, status 1 showing "no applicable rule" is returned. When Action 4 is performed, the Figure 4 Principle in Second Scheme

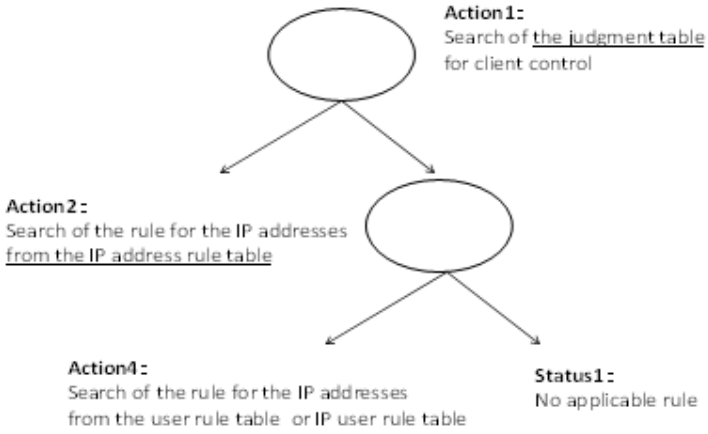

Figure 10 Used Algorism

4. ESTABLISHMENT OF THE VDACS SCHEME

To confirm the possibility of the wDACS Scheme, we performed functional experiments. By the experiments, we confirmed that the software for the existing DACS Scheme could be operated in cloud environment.

4.1 Experiment System

In Figure 11, the experiment system used in this study was described. 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 (CentOS6.5)
Software for DACS Server
Virtual machine B：
Operating System (CentOS6.5)
Authentication server (OpenLDAP2.4)
Virtual machine C：
Operating System (CentOS6.5)
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 (Windows XP Pro)
Software for DACS Client
Virtual router for a gateway (Vyatta6.6：64bit)

Because we assumed that the 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 was connected by IPsec VPN each other.

The DACS Server was located on the virtual machine A (VM A) 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 client. The policy information was sent and received through the VPN connected by two virtual routers on each virtual server.

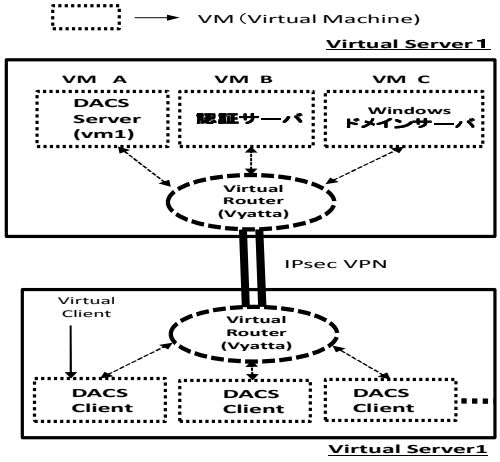

Figure 11 Experiment system

4.2 CONTENT OF THE FUNCTIONAL EXPERIMENT

By using the experiment system in Figure 11, we performed the experiments about two functions as follows.

(a) User authentication function

In this experimental system, the Windows OS (XP Pro) is used as an operating system on each virtual machine in the virtual server 2. In addition, because we intend to release the software developed to realize this scheme, we adopt the user authentication mechanism by free software. To be concrete, user authentication processes are performed between the clients on the virtual server 2 and the DACS Server on the virtual server1. About this point, we could confirm the movement normally.

- (Server1) OpenLDAP server for managing user accounts
- (Server2) Samba server for building a windows domain

(b) Delivery function of policy information

After the process (a), the policy information is sent and received through the VPN connected by two virtual routers on each virtual server. About this process, two cases of movement experiments are performed as follows.

- (Case1) One virtual machine was operated on the virtual server 2.
- (Case2) Some virtual machines (Five virtual machines) were operated on the virtual server 2.

4.3 Result Of Functional Experiment

The communication log was shown in Figure 12.

```
DATETIME:2014/04/10 01:11:18 MESSAGE:ANSWER_DATA recieved --- STATUS=50 (DACS_GET_OK) FUNCTION:main
DATETIME:2014/04/10 01:11:18 MESSAGE:disconnected by win-service!! FUNCTION:main
DATETIME:2014/04/10 01:11:18 MESSAGE:END!! FUNCTION:main
```

Figure.12 Communication log

As the result, we could confirm that the DACS Scheme to manage a physical client conventionally was operated in cloud environment.

4.4 Result Of Processing Load Experiment

Next, by using the experiment system, we measured the processing load to occur on the DACS Server side that is performed by concurrent delivery process of policy information between the DACS Server and the DACS Clients. To be concrete, by using 100 virtual clients, we measured the maximum value of the CPU processing speed on the virtual machine A on the virtual server 1. Because we could not place all virtual clients on virtual server 2 by the limitation of server resources, some virtual machines were located on virtual server 1.

The measure was carried out by using the standard tool of VMWare ESXi. Because we confirmed the consumption of the memory at that time, there was no problem at this point in particular.

The number of measurement is ten times. The maximum value of the CPU processing speed of each time is described in the Figure 13. The average value of ten times was 55.9MHz.

Measurement time	1	2	3	4	5	6	7	8	9	10
Value(MHz)	59	58	51	58	59	59	53	51	53	58

Figure 13 Maximum value of the CPU processing speed

As reference materials, we listed the graph on the result of the measurement from the first to fifth in Figure 14.

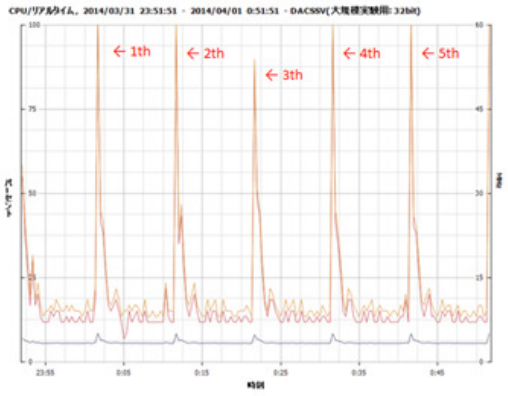

Figure 14 Graph of Maximum value (1th-5th

Then, the graph on the result of the measurement from the sixth to tenth was also listed in Figure 15.

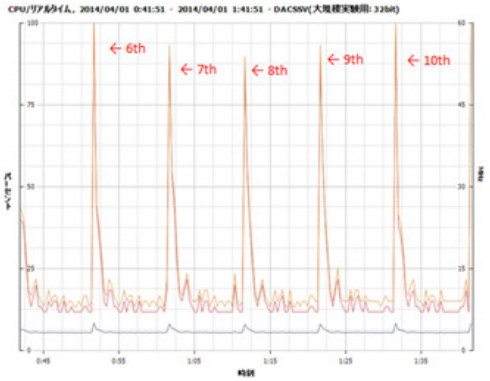

Figure 15 Graph of Maximum value (6th-10th)

Though we explain it for sense, Figure 15 and 16 mentioned above is the figure which was made based on the hard copy of VMWare ESXi tool. The processing load to occur on the DACS Server side was the low value than prior expectation This value is approximately a one-50th of the CPU performance (2.8GHz) of virtual server 1 which placed DACS Server. Though network environment of the experiment system was different from the real network environment, the DACS Sever may tolerate the concurrent processing from the virtual clients of around 5,000(50*100) theoretically. About this point, we intend to do additional experiment after having prepared for additional experiment facilities. If possible, we want to carry out the processing load experiment with number as close as possible to 5,000 mentioned above. Because we could confirm association between the CPU processing performance of the server machine with the DACS Server and the number of client machine with the DACS Client to some extent, we thought that the vDACS Scheme was established.

5. CONCLUSIONS

In this study, we established the vDACS Scheme. Because the existing DACS Scheme was the scheme to manage physical clients, we inspected compatibility of the DACS Scheme for the virtual environment and enlarged coverage of the scheme. To be concrete, after we confirmed that the software for the existing DACS Scheme could be operated with no problem functionally, processing load experiment was performed by using experiment system. As the result, we confirmed that the software moved on the virtual environment normally and the DACS Sever accepted accesses of 100 virtual clients in the range of CPU processing speed of the 55.9MH degree. As future works, we will perform additional processing load experiment by using more clients if possible with the client of around 5,000.

ACKNOWLEDGEMENTS

This work was supported by JSPS KAKENHI Grant Number 26730037. We express the will of thanks here.

REFERENCES

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

[2] B. M. Leiner, R. Core, J. Postel, and D. Milis, "The DARPA Internet Protocol Suite," IEEE Commun.Magazine, vol. 23 pp. 29-34 March 1985.

[3] P. Mockapetris and K. J. Dunlap. "Development of the domain name system," SIGCOMM'88, 1988.
[4] http://tools.ietf.org/html/rfc2453 [retrieved: 2, 2014]
[5] http://www.ietf.org/rfc/rfc2328.txt [retrieved: 2, 2014]
[6] http://tools.ietf.org/html/rfc4271 [retrieved: 2, 2014]
[7] A. X. Liu and M. G. Gouda, "Diverse Firewall Design," IEEE Trans. on Parallel and Distributed Systems, vol. 19, Issue. 9, pp. 1237-1251, Sept. 2008.
[8] http://tools.ietf.org/html/rfc1631 [retrieved: 2, 2014]
[9] M. S. Ferdous, F. Chowdhury, and J. C. Acharjee, "An Extended Algorithm to Enhance the Performance of the Current NAPT," Int. Conf. on Information and Communication Technology (ICICT '07), pp. 315-318, March 2007.
[10] S. K. Das, D. J. Harvey, and R. Biswas, "Parallel processing of adaptive meshes with load balancing," IEEE Tran.on Parallel and Distributed Systems, vol. 12, no. 12, pp. 1269-1280, Dec 2002.
[11] J. Aweya, M. Ouellette, D. Y. Montuno, B. Doray, and K. Felske, "An adaptive load balancing scheme for web servers," Int.,J.of Network Management., vol. 12, no. 1, pp. 3-39, Jan/Feb 2002.
[12] C. Metz, "The latest in virtual private networks: part I," IEEE Internet Computing, vol. 7, no. 1, pp. 87-91, 2003.
[13] C. Metz, "The latest in VPNs: part II," IEEE Internet Computing, vol. 8, no. 3, pp. 60-65, 2004.
[14] R. Perlman, "An overview of PKI trust models," IEEE Network, vol. 13, issue 6, pp. 38-43, Nov/Dec 1999.
[15] A. Singh, M. Korupolu, and D. Mohapatra, "Server-storage virtualization: Integration and load balancing in data centers," Int. Conf. for High Performance Computing, Networking, Storage and Analysis, pp. 1-12, Nov. 2008.
[16] R. Yavatkar et al., "A Framework for Policy-based Admission Control," IETF RFC 2753, 2000.
[17] B. Moore et al., "Policy Core Information Model -- Version 1 Specification," IETF RFC 3060, 2001.
[18] B. Moore, "Policy Core Information Model (PCIM) Extensions," IETF 3460, 2003.
[19] J. Strassner et al., " Policy Core Lightweight Directory Access Protocol (LDAP) Schema," IETF RFC 3703, 2004.
[20] D. Durham et al., "The COPS (Common Open Policy Service) Protocol, " IETF RFC 2748, 2000.
[21] S. Herzog et al., "COPS usage for RSVP", IETF RFC 2749, 2000.
[22] K. Chan et al., "COPS Usage for Policy Provisioning (COPS-PR), " IETF RFC 3084, 2001.
[23] M. Wahl et al., "Lightweight Directory Access Protocol (v3)," IETF RFC 2251, 1997.
[24] CIM Schema: Version 2.30.0, 2011.
[25] 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.
[26] 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", April 2006.
[27] K. Odagiri, R. Yaegashi, M. Tadauchi, and N.Ishii, "Efficient Network Management System with DACS Scheme : Management with communication control, " Int. J. of Computer Science and Network Security, vol. 6, no. 1, pp. 30-36, January, 2006.
[28] K. Odagiri, R. Yaegashi, M. Tadauchi, and N.Ishii, "Secure DACS Scheme," Journal of Network and Computer Applications," Elsevier, vol. 31, Issue 4, pp. 851-861, November 2008.
[29] K. Odagiri, S. Shimizu, R. Yaegashi, M. Takizawa, and N. Ishii, "DACS System Implementation Method to Realize the Next Generation Policy-based Network Management Scheme," Proc. of Int. Conf. on Advanced Information Networking and Applications (AINA 2010), Perth, Australia, Japan, IEEE Computer Society, pp. 348-354, May 2010.
[30] K. Odagiri, G. D. Marco, R. Yaegashi, M. Tadauchi, N. Ishii "The Processing Workload Evaluation in two Network Management Models of IP Networks, " Journal of Convergence Information Technology, Volume 4, Number 3, pp.7-16, September 2009.
[31] K. Odagiri, S. Shimizu, N. Ishii, "Technical points in the implementation of the support system for operation and management of DACS system," Proc. of Int. Conf. on Networking and Services (ICNS2013), IEEE Computer Society, pp.16-21, May, 2013.