Consideration of the User Authentication Processes in the Cloud Type Virtual Policy Based Network Management Scheme for the Specific Domain

Kazuya Odagiri[†], Shogo Shimizu[††], Naohiro Ishii[†††]
[†]Sugiyama Jogakuen University, 464-8662, 17-3Hosigaokamotomachi Chiksa-ku,Nagoya, Aichi, Japan
[††]Gakushuin Women's College, Tokyo, Japan
[†††]Advanced Institute of Industrial Technology, Tokyo, Japan

Summary
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. As one scheme, we have studied theoretically about the Destination Addressing Control System (DACS) Scheme with affinity with existing internet. By applying this DACS Scheme to Internet system management, we will realize the policy-based Internet system management. In this paper, to realize management of the specific domain with some network groups with plural organizations, the policy information decision processes applied for this scheme are considered and described.

Key words:
Policy-based network management; DACS Scheme; QOS

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)

Manuscript received June 5, 2019
Manuscript revised June 20, 2019

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 a step of the third 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, the policy information decision processes for the proposed scheme.is considered. 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, after the user authentication processes for the scheme are explained, the policy information decision processes are described.

2. Motivation and Related Researches

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.

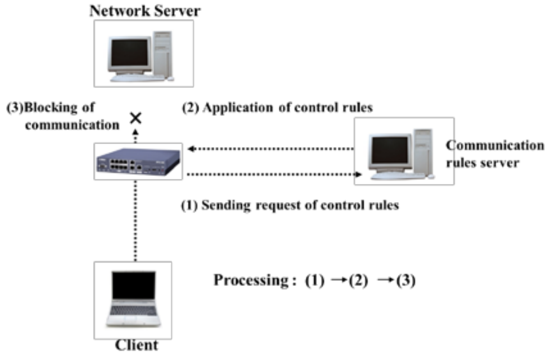
Network Server
(3)Blocking of communication
×
(2) Application of control rules
Communication rules server
(1) Sending request of control rules
Processing : (1) →(2) →(3)
Client

Fig. 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].

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.

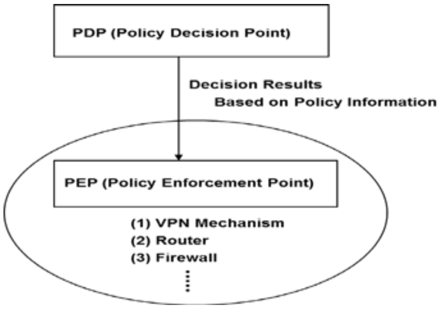
PDP (Policy Decision Point)
Decision Results
Based on Policy Information
PEP (Policy Enforcement Point)
(1) VPN Mechanism
(2) Router
(3) Firewall

Fig. 2 Essential Principle

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.

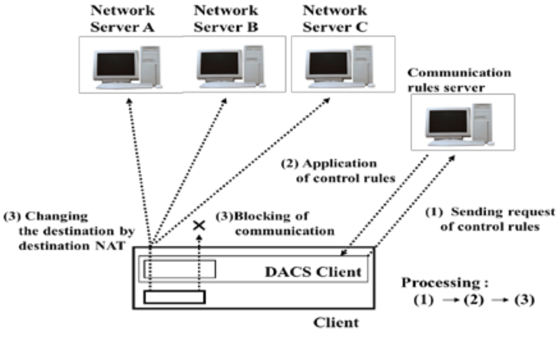
Network Server A
Network Server B
Network Server C
Communication rules server
(2) Application of control rules
(1) Sending request of control rules
(3) Changing the destination by destination NAT
(3)Blocking of communication
DACS Client
Client
Processing :
(1) → (2) → (3)

Fig. 3 Principle in Second Scheme

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. In order to improve it, we showed the cloud type virtual PBNM, which could be used by plural organizations. After it, to expand its application area, the scheme to manage the specific domain and the user authentication processes for that scheme are examined. In this paper, the policy information decision processes which are performed after the user authentication are examined.

3. Existing DACS SCHEME

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.

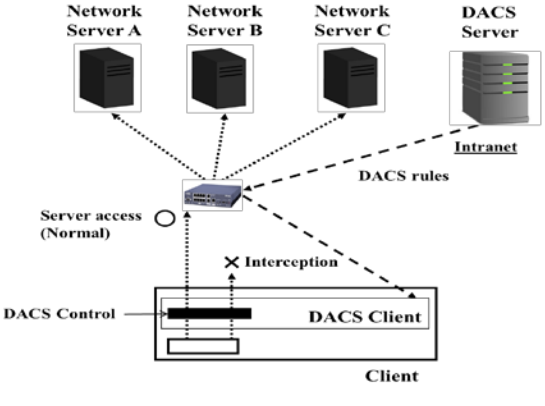

Fig. 4 Basic Principle of the DACS Scheme

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.
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.

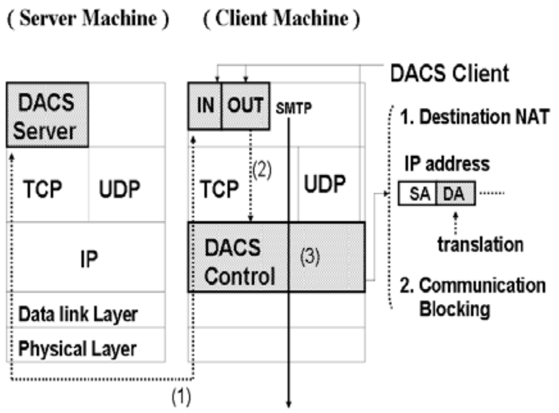

Fig. 5 Layer Setting of the DACS Scheme

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 of every user was given. However, it may be better to perform communication control 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 every client is described, and the coexistence method with the communication control of 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.

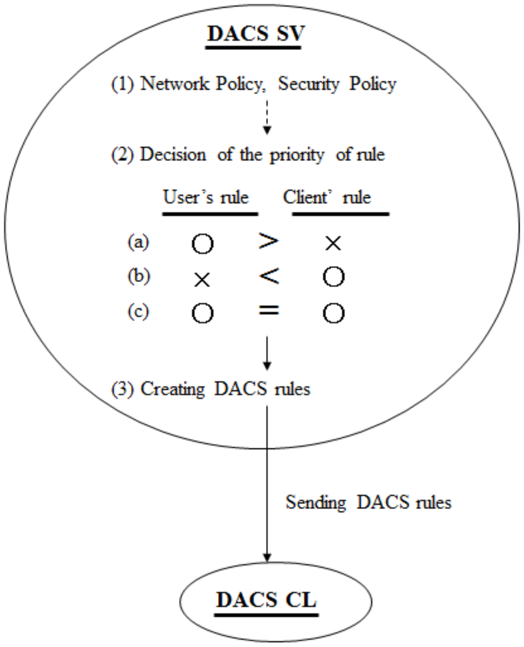

Fig. 6 Creating the DACS rules on the DACS Server.

When using the communication control of 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.

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 Secure Shell (SSH) [31]. 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 the 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, the local host (127.0.0.1) needs to be indicated on that client application as a communicating server. The transparent use of a client as the virtue of the DACS Scheme is lost. 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 does not fail the transparent use of a client is needed. The mechanism of that function is shown in Figure 7.

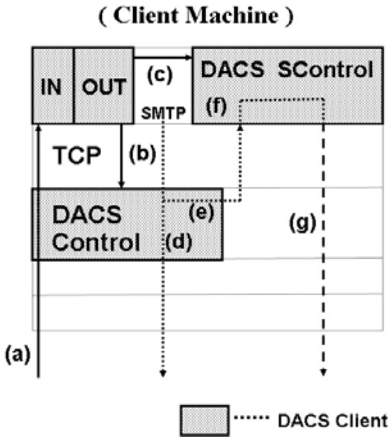

Fig. 7 Extend Security Function.

The changed point on network server side is shown as follows, in comparison with the existing DACS Scheme. SSH Server is located and activated, and communication, except, SSH is blocked. In Figure 7, the DACS rules are sent from the DACS Server to the DACS Client (a). On the DACS Client that accepts the DACS rules, the DACS rules are applied to the DACS Control in the DACS Client (b). These processes are same as the existing DACS Scheme. After functional extension, as shown in (c) of Figure 7, 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 7. When communication is tunneled and encrypted, destination of the communication is changed by the DACS Control to localhost, as shown in Figure 7. In Figure 7, the communication to localhost is shown with the arrows from (e) to the direction of (f). After that, by the DACS SControl which is used for the VPN communication, the communicating server is changed to the network server and tunneled and encrypted communication is sent as, shown in (g) of Figure 7, 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. 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. Distinguishing the control in the case of tunneling and encrypting or not tunneling and encrypting by a user unit is realized by changing the content of the DACS rules applied to the DACS Control and the DACS SControl. By tunneling and encrypting the communication for one network service from all users, and blocking the not tunneled 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, the communication to the network server from the client on which DACS Client is not installed in is permitted; each user can select whether the communication is tunneled and encrypted or not.

3.4 Application to cloud environment

In this section, the contents of wDACS system are explained. The system configuration of the wDACS system is described in Figure 8.

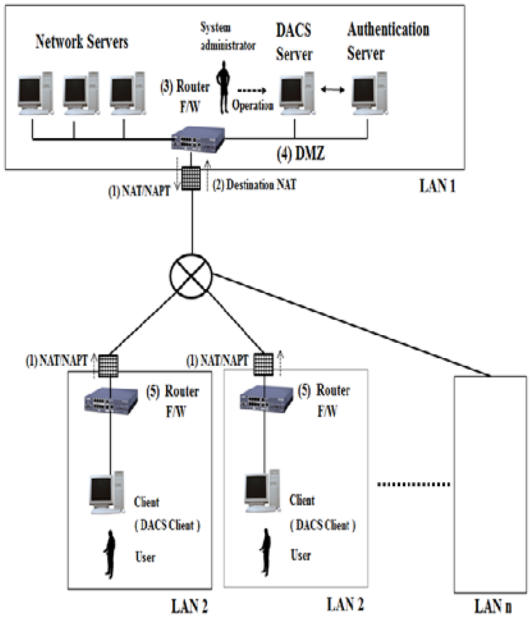

Fig. 8 Basic System Configuration of wDACS system

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.

3.5 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.

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.

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

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.

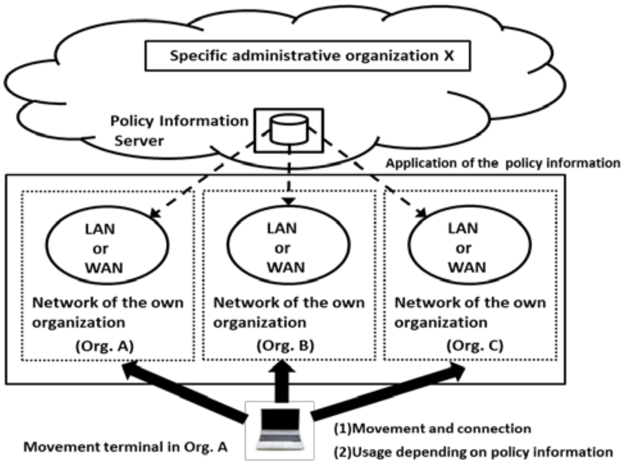
Specific administrative organization X
Policy Information Server
Application of the policy information
LAN or WAN
Network of the own organization
(Org. A)
LAN or WAN
Network of the own organization
(Org. B)
LAN or WAN
Network of the own organization
(Org. C)
Movement terminal in Org. A
(1)Movement and connection
(2)Usage depending on policy information

Fig. 9 Cloud Type Virtual PBNM for the Common Use between Plural Organizations

4. User Authentication Processes for the Scheme to Manage the Specific Domain

In this section, after the user authentication processes applied for the scheme to manage the specific domain was shown in Figure 10, the policy information decision processes are examined and described.

4.1 Management Scheme for the Specific domain

This is a scheme to manage the plural networks group. In Figure 10, the concept is explained. Specifically, as a logical range to manage organization A and organization B, network group 1 exists. Similarly, as a logical range to manage organization C and organization D, network group 2 exists. These individual network groups are existing methods listed in Figure 9. When plural network groups managed by this existing scheme exist, those plural network groups are targeted for management by this proposed method.

For example, when user A belonging to org. A in network group1 uses the network which org. C belonging to network group2 which is a different network group holds, administrative organization Y for network group2 refers for policy information of user A for administrative organization X of network group1 and acquires it. After it, in the form that policy information registered with Network Group2 beforehand is collated with the policy information, the final policy information is decided. As a result, the policy information is applied to the client that user A uses in network group2, and the communication control on the client is performed. When a user moves plural network groups as well as the specific network group, it is thought that the PBNM scheme to keep a certain constant management state is realized.

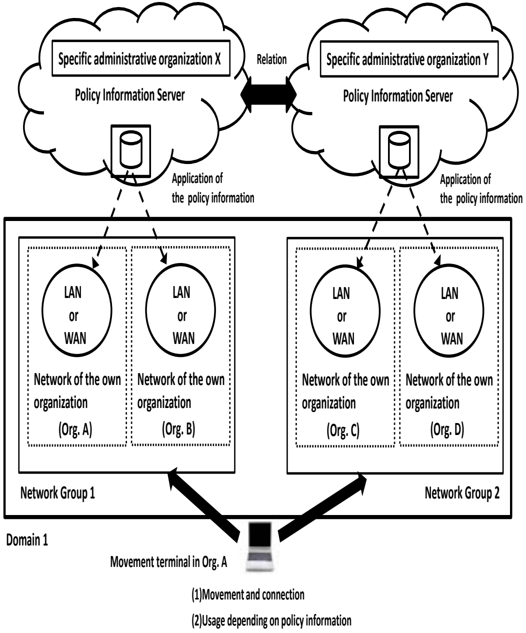
Specific administrative organization X
Relation
Specific administrative organization Y
Policy Information Server
Policy Information Server
Application of the policy information
Application of the policy information
LAN or WAN
Network of the own organization (Org. A)
Network of the own organization (Org. B)
Network of the own organization (Org. C)
Network of the own organization (Org. D)
Network Group 1
Network Group 2
Domain 1
Movement terminal in Org. A
(1)Movement and connection
(2)Usage depending on policy information

Fig. 10 Concept of the proposed scheme

To realize this scheme, it is necessary to consider the following three factors.

(Factor1) Method of user authentication
(Factor2) Determination method of the policy information
(Factor3) Distribution method of the policy information

Here, it is explained about the authentication processes when the client is connected to the network group2 by the user belonging to the network group1. First, between two administrative organization (organization X and Y), trust relationship is establised. As the result, the IP address of each other's DACS SV as policy information server are exchanged. This is done in advance before the authentication process. After it, authentication processes are performed as follows.

(1)Input of authentication information by the user
When the client is connected to the network group2, and the power of it is turned on. After an operation system was started up, the DACS CL is started up. In the middle process, the input pox for entering authentication information is displayed on the screen of the client. The user inputs user name and password, name or IP address of the authentication server in network group1.

(2)Authentication request from the client
By use of the authentication infotmation, authentication processes are performed in the form of encrypted communication by SSL. The authentication server is specified by the name of IP address the user inputs the input box.

(3)Authentication process at the authentication server side
Based on the user name and passwprd, the user authentication is performed. In this scheme, as the authentication server, the ldap server which is constituted by the openldap is used. The user name and password are compared with the user acount information. As a result of the comparison, when the authentication information matches, the IP address of the DACS SV in the network group 2 is notified to the client. When the authentication information does not match, the client is placed in a state in which no communication is possible based on the control by the DACS CL.

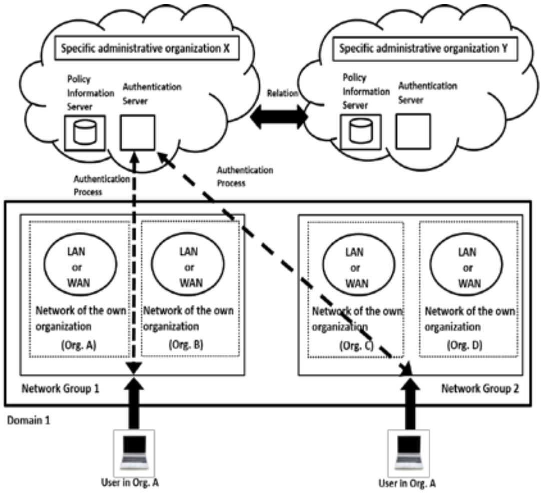
Specific administrative organization X
Policy Information Server
Authentication Server
Relation
Specific administrative organization Y
Policy Information Server
Authentication Server
Authentication Process
Authentication Process
LAN or WAN
Network of the own organization (Org. A)
Network of the own organization (Org. B)
Network of the own organization (Org. C)
Network of the own organization (Org. D)
Network Group 1
Network Group 2
Domain 1
User in Org. A
User in Org. A

Fig. 11 The proposed user authentication method

4.2 User Authentication Processes

Here, it is explained about the authentication processes when the client is connected to the network group2 by the user belonging to the network group1.
First, between two administrative organization (organization X and Y), a trust relationship is establised. As the result, the IP address of each other's DACS SV as policy information server are exchanged. This is done in advance before the authentication processes. After it, authentication processes are performed as follows.

(1)Input of authentication information by the user
The client is connected to the network group2, and the power of it is turned on. After an operation system was started up, the DACS CL is started up. In the middle process, the input pox for entering authentication information is displayed on the screen of the client. The user inputs user name and password, name or IP address of the authentication server in network group1.

(2)Authentication request from the client

By use of the authentication infotmation, authentication processes are performed in the form of encrypted communication by SSL. The authentication server is specified by the name of IP address the user inputs the input box.

(3)Authentication process at the authentication server side

Based on the user name and passwprd, the user authentication is performed. In this scheme, as the authentication server, the ldap server which is constituted by the openldap is used. The user name and password are compared with the user acount information. As a result of the comparison, when the authentication information matches, the IP address of the DACS SV in the network group 2 is notified to the client. When the authentication information does not match, the client is placed in a state in which no communication is possible based on the control by the DACS CL.

5. Conclusion

In this paper, the authentication processes for the proposed scheme are examined and described. Considering affinity with the Internet system, because the distributed authentication method was proposed, these processes were examined. As the future study, we will examine determination and distribution method of the policy information applied for this scheme.

Acknowledgments.

This work was supported by the research grant of JSPS KAKENHI Grant Number 17K00113, and the research grant by Support Center for Advanced Telecommunications Technology Research, Foundation (SCAT). We express our gratitude.

Acknowledgement

This work was supported by KDDI Foundation. We express our gratitude

References

[1] V. CERF and E. KAHN, “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 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, 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.

[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), Vol.1, No.4, November 2013, pp.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,” Proc of Int. Conf. on International Conference on Network-Based Information Systems (NBiS-2015),pp.180-186,Septmber, 2015

Kazuya Odagiri received the degree of B.S in 1998 from Waseda University. He is an Associate Professor in Sugiyama Jogakuen University now. In addition, he got his Ph.D. in Aichi Institute of Technology. He engages in a study of network management.

Shyogo Shimizu received the degree of B.S in 1996 from Osaka University and the degree of M.S in 1998 from Nara Institute of Science and Technology, Nara. He got his Ph.D. in Nara Institute of Science and Technology in March 2001. He is now Associate Professor in Gakushuin Women’s College.

Naohiro Ishii received the B.E., M.E. and Dr. of Engineering degree from Tohoku University, Japan in 1963, 1965 and 1968, respectively. He was a professor in Department of Intelligence and Computer Science at Nagoya Institute of Technology. From 2003, he was a professor in Department of Information Science at Aichi Institute of Technology until 2019. He belongs to Advanced Institute of Industrial Technology now. His research interest includes computer engineering, artificial intelligence, and human interface.