Theoretical Suggestion of Policy-Based Wide Area Network Management System (wDACS system part-I)

Kazuya Odagiri [*†]
Yamaguchi University,
Yamaguchi, Japan
E-mail: odagiri@yamaguchi-u.ac.jp, kazuodagiri@yahoo.co.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

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

Received 15 August 2013

Accepted 19 August 2013

Abstract

In the current Internet system, there are many problems using anonymity of the network communication such as personal information leak 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 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 will realize the policy-based Internet system management. As the first step, the DASC System is extended to move on the Wide Area Network (WAN) in this paper. We call the extended DACS system the Wide Area DACS system (wDACS system).

Keywo[i]rds: policy-based netwok management; DACS Scheme; NAPT

Published by Atlantis Press

1. Introduction

In the current Internet system, there are many problems using anonymity of the network communication such as personal information leak 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 Intern [ii] et 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) 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 scheme. The first is the scheme of 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. It is difficult to apply the first scheme to Internet system management practically, because the communication control mechanism needs to be located on the course 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 been 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 [19], and security function [20]. After that, we implemented a DACS System to realize a concept of the DACS Scheme [21]. By applying this DACS Scheme to Internet system, we will realize the policy-based Internet system management. As the first step, the DASC System is extended to move on the Wide Area Network (WAN) in this research. We call the extended DACS system the Wide Area DACS system (wDACS system).

2. Motivation and Related Research

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] [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 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.

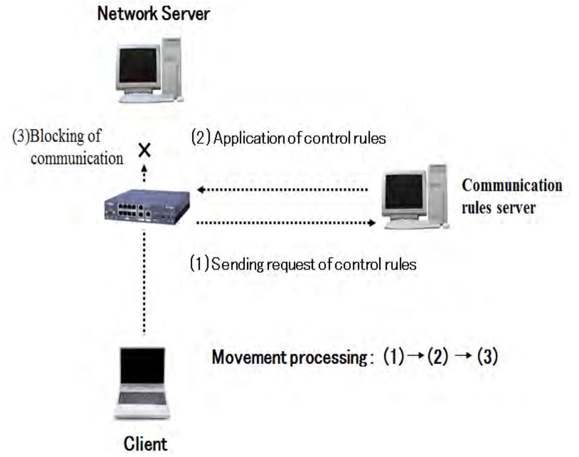
Network Server
(3)Blocking of communication
(2) Application of control rules
Communication rules server
(1) Sending request of control rules
Movement processing: (1)→(2)→(3)
Client

Figure 1 Principle in First Scheme

In policy-based network management, there are two types scheme. 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 [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.

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 [24], and was incorporated in the framework of DEN.

In addition, Resource and Admission Control Subsystem (RACS) [26] 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) [27] was established in International Telecommunication Union Telecommunication Standardization Sector (ITU-T).

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 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.

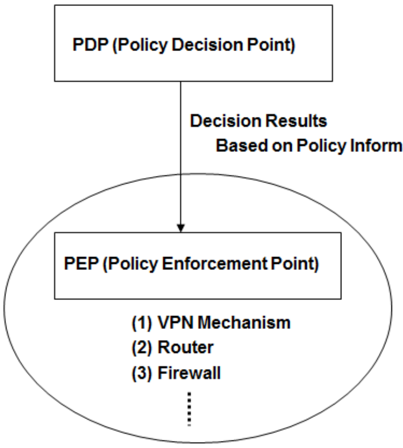
PDP (Policy Decision Point)
Decision Results
Based on Policy Information
PEP (Policy Enforcement Point)
(1) VPN Mechanism
(2) Router
(3) Firewall

Figure 2 Essential Principle

The principle of the second scheme is described in Figure 3 [28 29 30]. 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. 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.

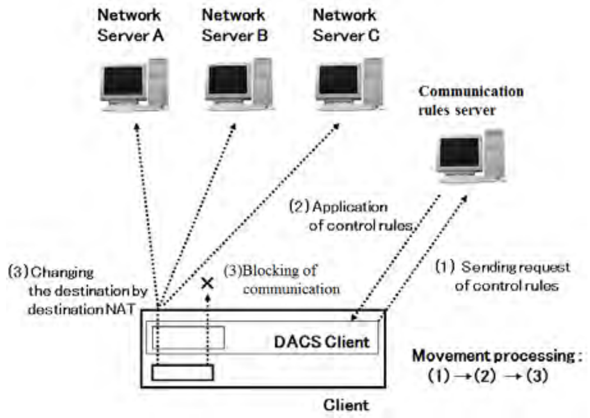
Network Server A
Network Server B
Network Server C
Communication rules server
(2) Application of control rules
(3) Changing the destination by destination NAT
(3)Blocking of communication
(1) Sending request of control rules
DACS Client
Movement processing : (1) →(2) →(3)
Client

Figure 3 Principle in Second Scheme

However, it is difficult to manage the whole Internet system by using a policy-based thinking from the beginning. We assume an enormous number of problems. Therefore, in this study, the mechanism of managing the WAN which connects some LANs is shown as a stage before managing whole Internet system. To be concrete, by extending the DACS Scheme, the scheme for the WAN management is examined. Because the DACS system to realize the DACS Scheme was implemented in the previous studies, this system is extended so as to move on the WAN. The examples of the technical problem to make the DACS system move on the WAN are as follows.

(Problem 1)

When private IP addresses are assigned to the network servers and clients in the different LANs, same IP address may be assigned to them. In addition, same user name may be user in the different LANs. In that case, the correct communications may not be guaranteed.

(Problem 2)

When network servers and clients send the network communications to each other, network communications may be obstructed by the translation mechanism such as NAT/NAPT.

(Problem 3)

There is no mechanism to hand over the key for encrypting the network communication from the clients to each client or each user.

In this paper, the contents of the DACS Scheme are explained in Section 3. In Section 4, the mechanisms of the existing implemented DACS system are described. Then, the DACS system moving on the WAN called wDACS system is shown in Section 5.

3. Existing DACS Scheme

In this section, the content of the DACS Scheme is described.

3.1. *Basic Principle of the DACS Scheme*

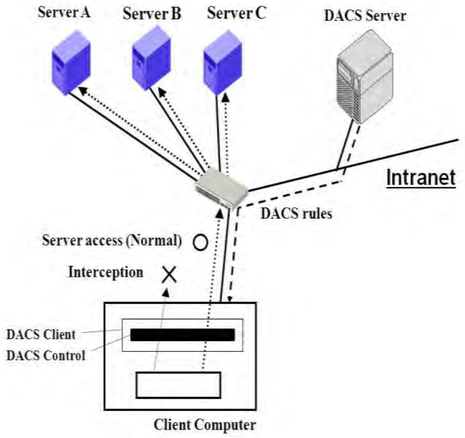

Figure 4 Basic Principle of the DACS Scheme

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.

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. 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.

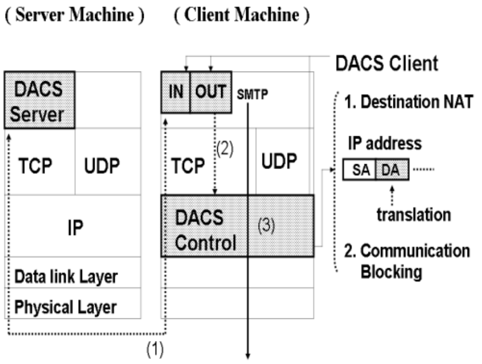

Figure5 Layer Setting of the DACS Scheme

3.2. *Communication Control on the Client*

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

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

When using communication control on every user and every client, communication control may conflict.

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

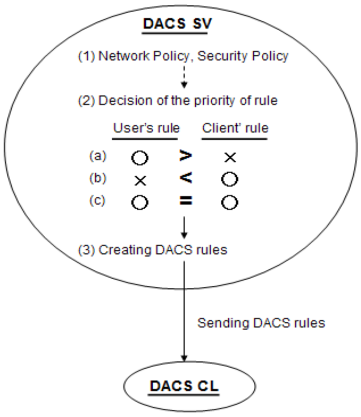

Figure 6 Creating the DACS rules on the DACS Server

3.3. *Security Mechanism of the DACS Scheme*

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

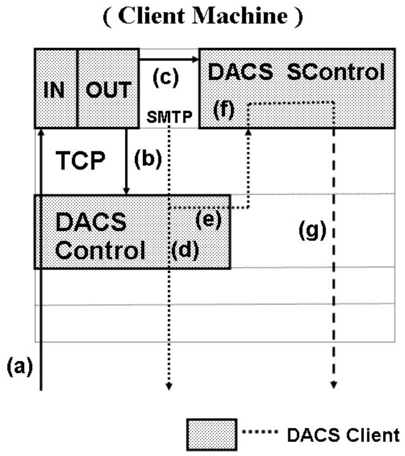

Figure 7 Extend Security Function

4. Specification of the DACS System

4.1. *Security Mechanism of the DACS Scheme*

(A) Technical Points

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

The Communications between the DACS Server and the DACS Client such as sending and accepting the DACS rules 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 8 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().

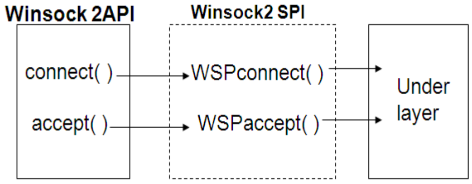

Figure 8 Winsock2 SPI

(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.

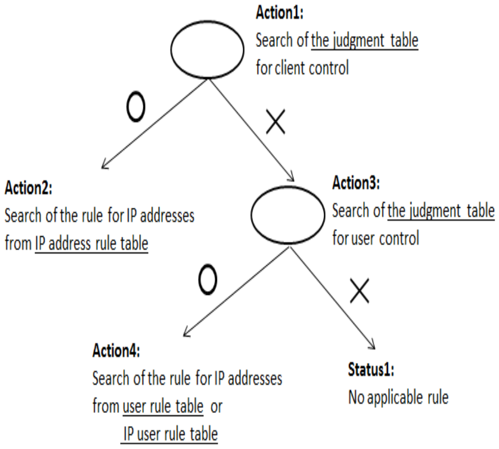
Action1:
Search of the judgment table for client control
O
X
Action2:
Search of the rule for IP addresses from IP address rule table
Action3:
Search of the judgment table for user control
O
X
Action4:
Search of the rule for IP addresses from user rule table or IP user rule table
Status1:
No applicable rule

Figure 9 Used Algorism

4.2. *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 9, 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 control rules every user are searched and extracted from the user rule table or IP user rule table.

5. WDACS SYSTEM

In this section, the contents of wDACS system are explained in the form including three problems introduced in Section 2.

5.1. *System Configuration of wDACS system*

The system configuration of the wDACS system is described in Figure 10.

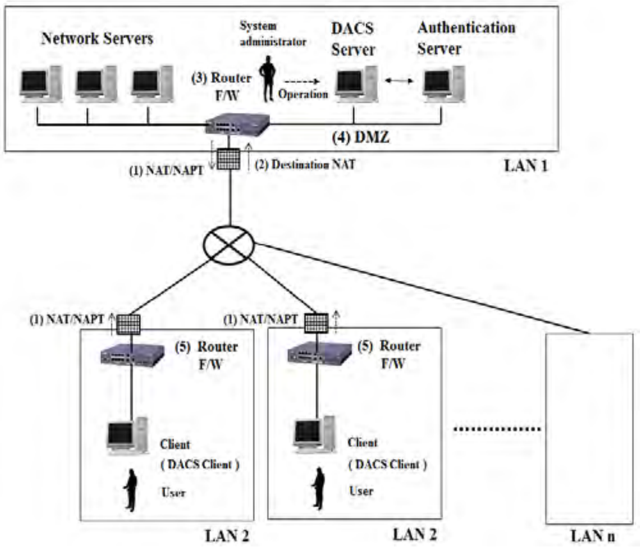

Figure 10 Basic System Configuration of wDACS system

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 thorugh 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.

5.2. *Solving Method of Technical Problem*

Here, solving methods of three problems described in Section 2 are shown.

(A) Solving method of Problem 1

The following two methods are thought.

(Method 1) Corresponding method by system operation

In the form of using the current DACS system, only one IP address and IP address are used in multiple LANs. As the result, they are distinguished uniquely.

(Method 2) Corresponding method by system improvement

Identification information such as domain name and sub domain name is assigned to each LAN. The control rules as the DACS rules are set in the form of distinguishing the same user name and IP address in the different LAN by adding the above identification information.

Because the wDACS system examined in this research has the premise of managing the network which interconnects multiple LANs in same one organization, the method 1 is used. The method 2 needs to be used for interconnects of wDACAS system in different organization. We recognize this point as a future research task.

(B) Solving method of Problem 2

By adopting the system configuration described in Figure 10, the problem 2 is solved. When the private IP addresses are set on the servers and clients on the interconnect LANs, the communications form the clients in the LANs except the LAN 1 do not reach the servers in LAN1. By adding the mechanism of the destination NAT to LAN 1, the communications sent form the LANs except the LAN 1 can get to the DACS Server in the LAN 1.

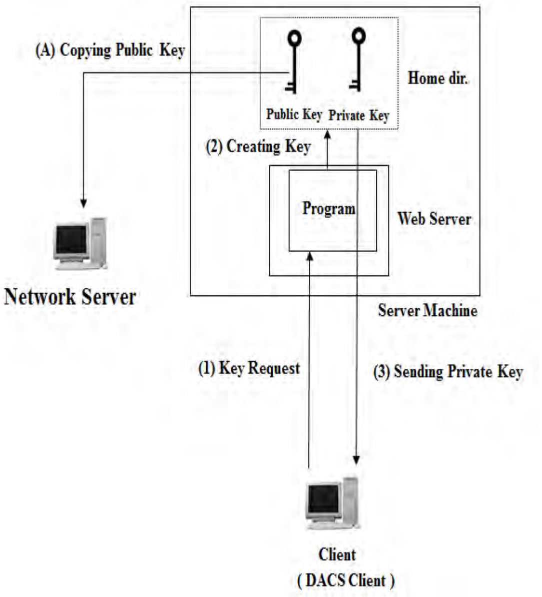

Figure 11 Mechanism of Key Setting

(C) Solving method of Problem 3

The existing DACS system has the function of encrypting the communications between network servers and clients by using SSH. Because it is used in a LAN restrictively, it is not necessary to apply the authentication using the public key (client authentication). However, it is necessary for the wDACSsystem to apply the authentication using the public key because of security enhancement. When the existing DACS system is moved on the WAN without extensions, both a system administrator and users need to make and set the key to the servers and clients as a part of the system operation. Because it is easy to support the users in the organization which can post system administrators on each LANs, there is no problem. When it is difficult to support the users by the telephone and e-mail, the system administrator can go to the user's place and support them. However, in the organization which cannot post system administrators on each LANs, the system administrator cannot go to the user's place in the different LAN and support users. In the case of introducing the wDACS system, such a form may be taken.

Therefore, it is necessary to introduce the mechanism for acquisition and management of the key without doing something at the user side in particular with keeping the security of a certain uniformity standard. To be concrete, the mechanism described in Figure 11 is introduced newly.

This mechanism is incorporated at the last part of the initialization process of the DACS Client. The preconditions are as follows.

(a) The communications between the DACS Client and the Web Server are encrypted by the https.

(b) The communications between the Server Machine moving the Web Server and network servers are encrypted by SSH.

(c) This mechanism is located on the Server Machine which is separated physically with DACS Sever for the management of a large-scale network with many clients.

Next, the movements of this mechanism are described. First, the key request is performed from the DACS Client (1). The program on the Web Server receives the request, and creates two kinds of keys which are a public key and a private key (2). Then, the program sends the private key to the client (3).The public key stored in the home directory on the Server Machine is copied and stored on the network server by mirroring through SSH. To be concrete, network commands such as rsync and rdiff-backup are used. The mirroring process is performed just before the transmission of the private key.

6. Conclusion

In this paper, we showed the policy-based wide area network management system called wDACS system. This system is realized by the extension of the policy-based network management system called DACS system which manages the LAN. To be concrete, after showing the three problems for moving the existing the DACS system through the WAN, the concepts of the wDACS system were described and the solving method of the three problems were explained. As the result, the wDACS system which moves in the form of keeping the security of a certain uniformity standard for the purpose of managing the WAN which multiple LANs interconnected. As a future study, the DACS system will be implemented to manage the WAN practically and evaluations will be performed.

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.MILLS,"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. In SIGCOMM'88, 1988.
4. http://tools.ietf.org/html/rfc2453
5. http://www.ietf.org/rfc/rfc2328.txt
6. http://tools.ietf.org/html/rfc4271
7. Alex X. Liu, Mohamed 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
9. M.S. Ferdous, F. Chowdhury, 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, 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 at el., "A Framework for Policy-based Admission Control", IETF RFC 2753, 2000.
17. B. Moore at el., "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 at el., " Policy Core Lightweight Directory Access Protocol (LDAP) Schema", IETF RFC 3703, 2004.
20. D. Durham at el.,"The COPS (Common Open Policy Service) Protocol", IETF RFC 2748, 2000.
21. S. Herzog at el.,"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. CIM Core Model V2.5 LDAP Mapping Specification, 2002.
24. M. Wahl at el.,"Lightweight Directory Access Protocol (v3)", IETF RFC 2251, 1997.
25. CIM Schema: Version 2.30.0, 2011.
26. 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.
27. ETSI ETSI ES 283 026: Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control; Protocol for QoS reservation information exchange between the Service Policy Decision Function (SPDF) and the Access-Resource and Admission Control Function (A-RACF) in the Resource and Protocol specifica-tion", April 2006.
28. 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.
29. 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.
30. K. Odagiri, S. Shimizu, R. Yaegashi, M. Takizawa, 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 (AINA20010), Perth, Australia, Japan, IEEE Computer Society, pp.348-354, May, 2010.