"Access Authentication Solutions" - Providing Flexible and Secure Network Access

KAWAI Hideki, OMINO Takayuki, SHIBAHARA Hideo, SAKAMOTO Daichi, KANAMORI Ichiro, SONODA Kentaro

Abstract

In order to avoid information leakage, strict security such as sliced network access is essential for departments and projects. Because they need to process highly confidential information such as customer details and component design data, etc. Providing a granular access control may improve security efficiency, however, such a tight access control system sometimes poses issues, e.g., high system management costs and difficulties in quickly coping with the ever changing company organization environments. This paper introduces NEC's "Access Authentication Solutions," which reduce system management costs while also improving security. This is achieved by providing automated settings to server networks based on user's human resource information. Software-Defined Networking (SDN) technology is an essential feature in effecting this approach.

Keywords

information security, information leakage, targeted threats, BYOD, VLAN, SDN, OpenFlow

1. Introduction

In recent years, the risk of information leakage has become one of the biggest threats for business managers. Even though, network access controls, which are a significant countermeasure against information leakage, are not generally provided to a satisfactory degree. This issue occurs because the provision of satisfactory access controls may entail significant management costs as well as difficulties in dealing effectively with an ever changing company organization environment. This paper introduces the "Access Authentication Solutions" that provides flexible access control while ensuring firm security and reducing system management cost. The key concept of the solution is linking between human resource information and the access control function by Software-Defined Networking (SDN), which allows users to control networks via software-based operations.

Human resource information includes various employee data, such as their belonging departments, projects, their positions in the company and working location, etc. Access control is decided by referring to human resource information, such as which person is allowed access to which information on the company network. This means that the human resource information and the network access controls are operated together so that any unauthorized access may be prevented without setting manual network access controls. Moreover, the network environment is maintained so that only appropriate person can access to appropriate information. When this solution is applied to the network together with a file access control function such as Information Rights Management (IRM), a more robust security regime may be implemented.

2. Company Issues: Information Leakage and Access Control

Incidents of information leakage occurring in companies or governmental offices have increased in recent years. These incidents have focused social attention on how to protect personal or confidential information. In a society in which the IT infrastructure is highly developed, companies are facing new risks of information leakage. Therefore it is essential that they are capable of providing management systems that can rigorously protect such information.

The first step in protecting confidential information and in preventing incidents such as information leakage is to provide strict access controls and to limit the number of persons that may access confidential information. Companies belonging to

the finance, insurance and securities industries adopt the guidelines provided by The Center for Finance Industry Information Systems (FISC), which recommends the creation of an independent network for each department. In addition, banks are requested by law that they must provide information blocking countermeasures, such as those for physically blocking network systems or limiting access permissions, and install them between departments that have conflict of interests. Building independent network systems is also important for industries other than the finance industries. Such independent network systems may contribute, for example, to localizing virus infections in a certain network should a targeted attack occur, and to preventing its spreading to an entire company.

However, countermeasures that support network access controls are not yet adequately implemented in many companies even though many company managers have a strong sense of crisis regarding information leakage issues. This is because the network management costs are likely to be enormous for implementing satisfactory network security systems by localizing networks for individual departments or projects, and for providing strict access controls.

In a case where a Sales Dept. employee is transferred to the Planning Dept., various network connection change procedures related to the transfer will be necessary. These will include connection change requests and network settings, etc., and both the network users and the administrators will have to conduct these procedures. Also, in a case where an employee is on a business trip and desires to access their department network from the branch office, it will be necessary to establish the relevant network settings in advance before leaving. Moreover, when a LAN cable is replaced due to office room layout change, department relocation, etc., it will also be necessary to change the network settings. Even when a project is expected to have its own independent network in order to prevent information leakage, a network setting change will also be required. As described above, the work involved in the network setting changes occurs at various timings and for various reasons. Therefore, the requisite network operations management will consume much labor and many hours to achieve completion satisfactorily.

NEC's "Access Authentication Solution" makes it possible to automate the network setting changes while separating networks more specifically and linking the access control function and the relevant human resource information. This procedure will eliminate deficient setting procedures such as any missed setting changes or setting errors, so that a flexible and secure access control system may be effectively achieved.

3. Access Authentication Solution

Fig. 1 shows an outline of the "Access Authentication Solution." This solution brings significant advantages to companies which demand for strict security controls for departments and projects dealing with highly confidential information such as customer data, company management data, new product planning data, component design data and product manufacturing process data, etc.

The three key advantages of this solution are;

(1) Network-level access control
(2) Access restriction between client PCs
(3) Automated network settings for linking with human resource information

(1) The network-level access control is provided so that more detailed records may be logged, such as for who has accessed from where and when. With the network system of the server-level access control, a malware attack can target the entire server. However, if the network is isolated per department, a virus attack can be limited to the targeted department.

(2) SDN controls the traffic according to a node linked to the network and then enables to provide an access restriction between client PCs. This strategy prevents the spreading of malwares inside client PCs even when vulnerable client PCs are attacked by a targeted thread.

(3) Network setting change operations are necessary each time that members of staff are transferred, or travelling between branch offices, etc. The automated setting operations linking with the human resource information is achieved by connecting the human resource information database and the OpenFlow[*1] switch. This procedure enables efficient automated network setting change operations by eliminating issues caused by any missing or erroneous settings.

As discussed above, our solution will enable network security improvements as well as system management cost reductions, both of which have hitherto been difficult to achieve.

3.1 System Configuration

Fig. 2 shows a system configuration example of the "Access Authentication Solution." The solution adds the OpenFlow switch and a management server to the existing network so that the network and the human resource information are linked to each other.

An "Open vSwitch" is employed for the OpenFlow switch as a software switch and this is installed in the general-purpose server. The OpenFlow switch is also available to be used as a hardware switch for the UNIVERGE PF series.

[*1] OpenFlow is a foundational element to implement SDN. It is a communications protocol that enables centralized network control by decoupling the network control function and a switch device, and then integrating it into a controller. NEC is a member of the Open Networking Foundation (OFN), a non-commercial organization that is dedicated to the standardization of OpenFlow.

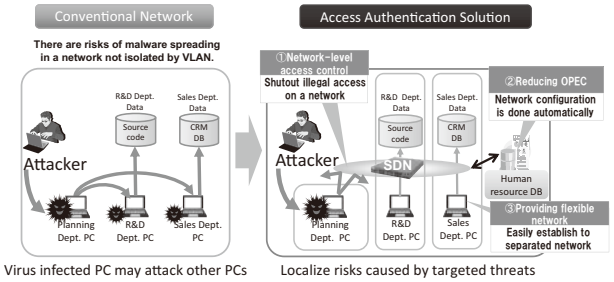


Fig. 1 Outline of the "Access Authentication Solution."

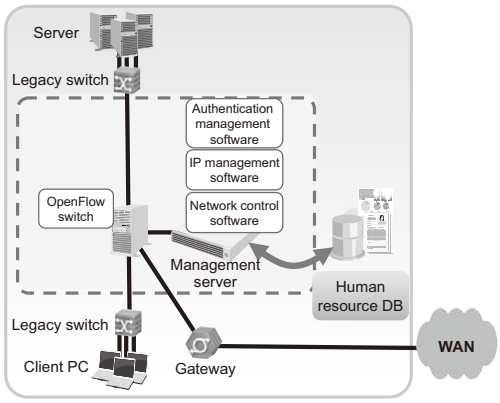


Fig. 2 System configuration of the "Access Authentication Solution."

NEC's originally developed OpenFlow controller is employed as the network control software to be operated on the management server. Also, DHCP is employed as the IP management software that allocates the IP addresses, and OpenLDAP as the authentication management software. Even with some limitation in applicable scales and performances, our solution has the advantage that it can be provided to the user's existing network system just by adding a single server. This is achieved by operating the software-based OpenFlow switch on the management server. Three types of authentication system are supported: a terminal authentication, 802.1X authentication (RADIUS server is optional) and a Web authentication. The authentication management combining these three types is also available with our proposed solution.

When these solutions are introduced in two or more offices, OpenFlow switches and management servers are added to the existing networks installed in each office (Refer to Fig. 2). The network setting information linking with the human resource information can be shared among management servers, so that once the system is installed in an office, it is not necessary to link between the network system and the human resource when it is installed in a second office or later. A "Small Start" using an existing network is available so that step-by-step scaling out of the configuration becomes possible; e.g., by firstly introducing it to a department that must be isolated from other networks because it deals with confidential information, and secondly by introducing the same solution system configurations to other offices.

3.2 Features of the Access Authentication Solution

In this section, three features of our "Access Authentication Solution" are described: (1) network-level security, (2) reduction of the system management costs and (3) flexible network systems.

(1) Network-level security

Our "Access Authentication Solution" allows the management server to acquire the human resource information and automatically set the access information of individual users to the OpenFlow switch (**Fig. 3**). This results in preventing deficient network access rights settings (missing or erroneous settings) when an employee relocates to another department. At the same time, it also enables the blocking of illegal access at the network-level environment. Moreover, communications between client PCs are easily controlled so that countermeasures can be provided to deal with security risks that might occur in the intranet such as via targeted threads or information leakages, etc.

(2) Reduction of management costs

Conventional network systems are not able to conduct a linkage operation between the network access control system and the human resource information. Additional work is therefore required when a company organization is changed or if an employee is transferred to a different department. When a network user applies his/her network access right modifications it will in consequence be necessary for a network administrator to carry out the requisite access control setting change operations, etc. (**Fig. 4**). However, our "Access Authentication Solution" automatically sets the access control settings by linking the network system with the human resource information,

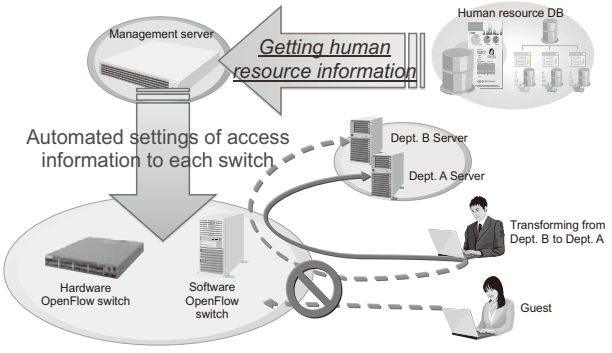


Fig. 3 Network-level security.

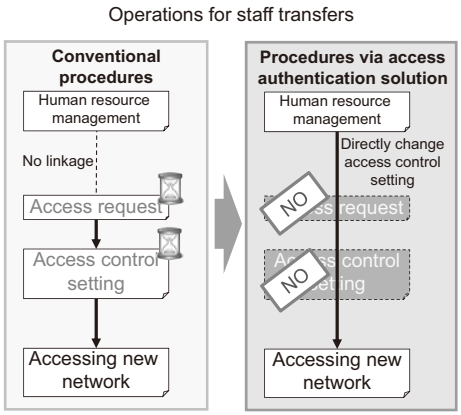


Fig. 4 Management cost reduction.

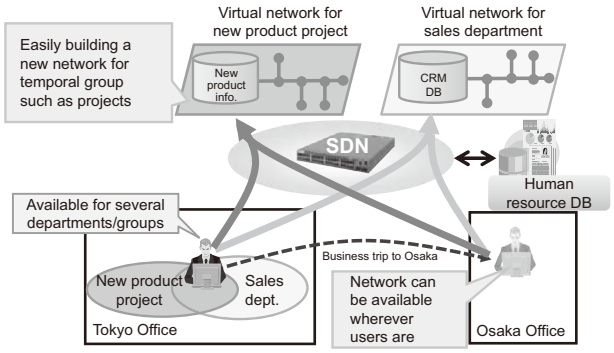


Fig. 5 Flexible network system.

so that manual setting change operations will not now be necessary. The required time to complete the network access modification request and the relevant control setting operations is 10 to 20 minutes per user. Although this may seem to be rather a short amount of time, there could be a significant amount of time and costs accruing in a year from these operations each time that organization changes occur; e.g., staff transfers, travelling between offices, office room layout modifications, creating exclusive networks for different projects, etc. With our solution system in place, a company with 3,000 employees can expect to reduce approximately 60% of the network management costs in five years. Even after deducting the cost of introducing the solution, a 30% cost reduction in total may be expected.

(3) Flexible network system

Our "Access Authentication Solution" employs a virtual network system based on SDN and builds independent networks. Various network configurations are thereby enabled; such as creating a flexible network system for a certain project or sharing a network between different departments, etc. Moreover, users can access the network from different locations without applying a network access right in advance. This means that the network can easily cope with staff transfers between offices. **Fig. 5** illustrates an example in which an employee who belongs to the Sales department and deals with a new product development project, is on a business trip from the Tokyo office to the Osaka office, and is able to access the virtual network of his/her Tokyo office from Osaka.

4. Conclusion

This paper has introduced our "Access Authentication Solution" that achieves secure and flexible network access control. Control is enabled by employing SDN and linking the human resource information and the access control function. Our solution achieves network control operations based on OpenFlow technology, a strategy that has made it possible to have the authentication function linked to the human resource information. Therefore, our solution can provide (1) network-level security, (2) management costs reductions and (3) a flexible network system. These provisions are highly suitable for enterprises that demand strict security control in their departments and projects that handle highly confidential information.

* OpenFlow is a trademark or registered trademark of Open Networking Foundation.

Authors' Profiles

KAWAI Hideki
Expert
SDN Strategy

OMINO Takayuki
Assistant Manager
SDN Strategy

SHIBAHARA Hideo
Senior Expert
SDN Strategy

SAKAMOTO Daichi
Assistant Manager
Service Platform Division
Network Service Business Unit
NEC Networks & System Integration Corporation

KANAMORI Ichiro
Common Platform Development Division
Network Software Development Business Unit
NEC Communication Systems, Ltd.

SONODA Kentaro
Assistant Manager
Cloud System Research Laboratories

Information about the NEC Technical Journal

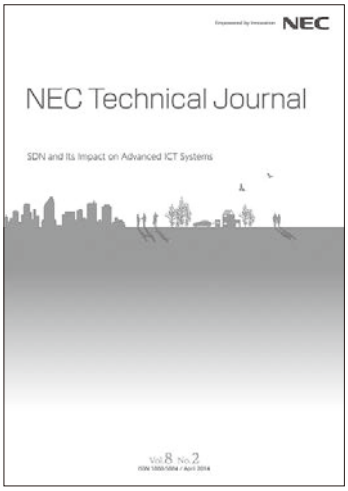
Thank you for reading the paper.
If you are interested in the NEC Technical Journal, you can also read other papers on our website.

Link to NEC Technical Journal website

Japanese

English

Vol.8 No.2 SDN and Its Impact on Advanced ICT Systems



Vol.8 No.2
April, 2014

Special Issue TOP