

Opengate on Cloud

Kenzi Watanabe
Department of Information Science
Graduate School of Science and Engineering
Saga University
Saga, Japan
watanabe@is.saga-u.ac.jp

Makoto Otani
Computer and Network Center
Saga University
Saga, Japan
otani@cc.saga-u.ac.jp

Shin-ichi Tadaki
Computer and Network Center
Saga University
Saga, Japan
tadaki@cc.saga-u.ac.jp

Yoshiaki Watanabe
Department of Information Science
Graduate School of Science and Engineering
Saga University
Saga, Japan
watanaby@is.saga-u.ac.jp

Abstract—Opengate is an access control system of the captive portal type for mobile LAN users. Opengate has benefits such as simple user interface, easy administration and so on. It supports IPv6 and Shibboleth single-sign-on authentication. We have been operating Opengate over 10 years without serious problems. Opengate is running on virtual machine environments. Virtual machine environments enable Opengate to be a cloud system for user authentication. The cloud Opengate provides opportunities for small organizations to have their own access control systems without self-operations.

Keywords-Captive Portal, Authentication, Access Control, Single Sign-On, Cloud

I. INTRODUCTION

A lot of universities operate WiFi LAN for mobile users. These mobile LAN provide Internet connectivity wherever we needed in a campus.

However, everyone, including people who do not have relation with the university, can use the mobile LAN if it does not have access control systems. So, many universities introduce access control systems such as FEREC [1], IEEE802.1X [2].

We have been developing an access control system for mobile LAN users named “Opengate”[3]. Opengate is a captive portal type access control system. Opengate has benefits such as simple user interface, easy administration and so on. We started development of Opengate in 1999. We have been operating Opengate over 10 without serious problems. Since 2001, we started to operate the system for the whole WiFi LAN of Saga University. Opengate also has supported IPv6 protocol at [4] [5]. It has supported the Shibboleth single-sign-on authentication since 2009 [6].

Since 2010, Opengate has been running on virtual machine environment. Namely, Opengate becomes compatible

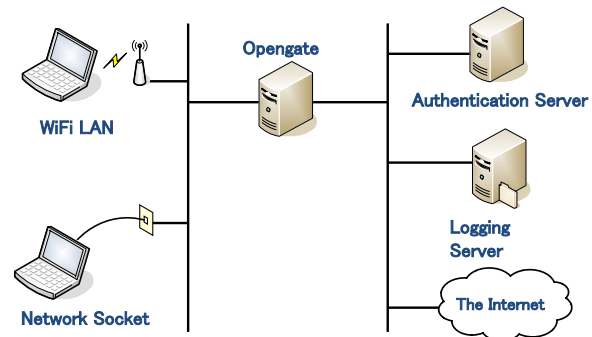


Figure 1. Configuration of Opengate.

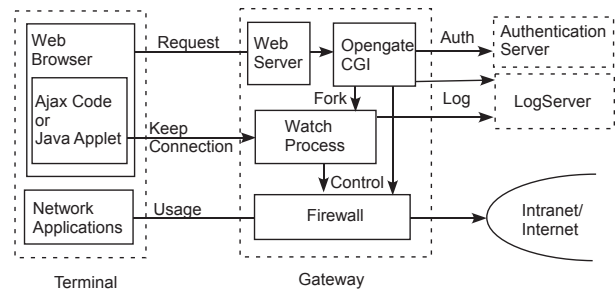


Figure 2. Block diagram of software.

to cloud services. We are able to provide user authentication services for any organizations as a cloud service.

In this paper, we will describe Opengate and Opengate with Shibboleth authentication. We propose cloud based user authentication service.

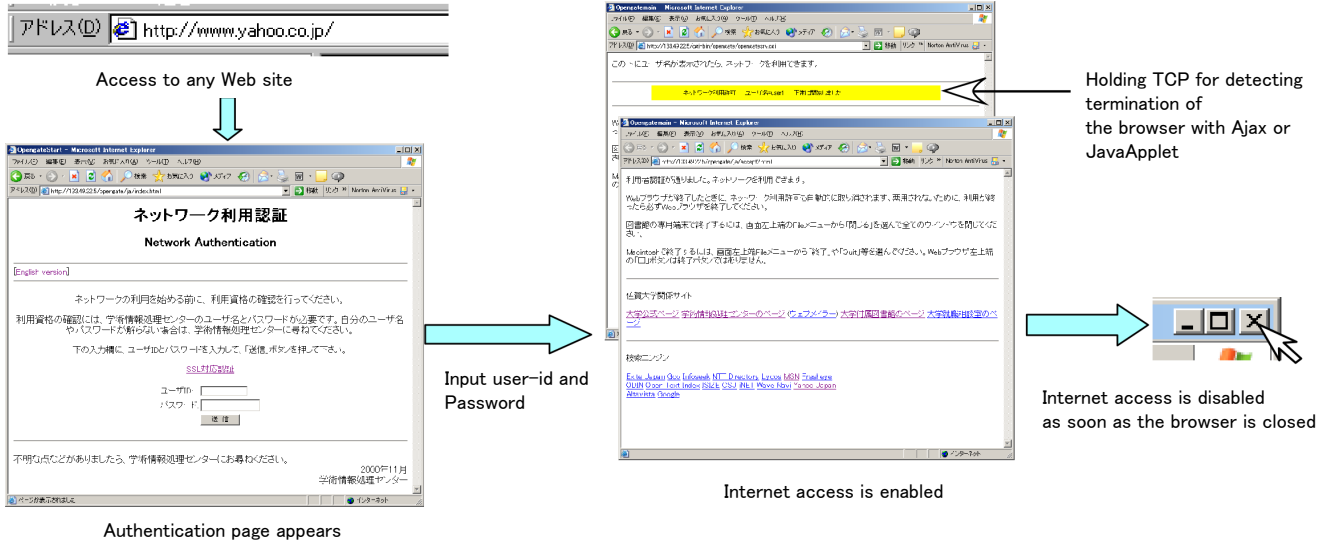


Figure 3. Use flow of Opengate.

II. OPENGATE

Opengate is a captive portal type access control system for mobile LAN.

Opengate is configured as a gateway of a LAN for terminals (Figure 1). Authentication is provided by an external server, which uses one of FTP, POP3, Radius, and LDAP protocols. Operation logs can be sent to an external syslog server.

The block diagram of the software is shown in Figure 2. Opengate consists of four components: local Web server, Opengate CGI, watch process and firewall.

Figure 3 shows use flow of Opengate. When a user wants to connect to the Internet, the user only needs to launch Web browser on his/her PC. Opengate catches HTTP access from the users' Web browser. The Opengate CGI returns an Web page for user authentication. After user inputs his/her user-id and password, Opengate CGI tries to authenticate the user with the authentication server. During the process above, Opengate gets IPv4 and IPv6 addresses of the user's PC. If the authentication succeeds, Opengate inserts allow rules into the firewall for both IPv4 and IPv6 addresses. After that, Internet access become enabled for the user. The Watch process establishes and holds a TCP connection between the Opengate server and user's Web browser using Ajax or JavaApplet. Opengate watches this TCP connection. When the user closes his/her Web browser or LAN connection, the watch process recognizes the end of the use. Then Opengate removes the corresponding firewall rules. The Internet access is turned to be disabled for the user.

Opengate records all information such as authenticated user-id, firewall open and close time and so on into log files using the syslog function. The administrator can track users'

usage history from this log files.

Opengate is running on FreeBSD with ipfw [7] and Apache [8]. Opengate is distributed as open source software on the Opengate's Web [9].

III. OPENGATE WITH SHIBBOLETH

Shibboleth is a Single Sign-On mechanism for Web based systems developed by MACE (Middleware Architecture Committee for Education) of Internet2 [10]. Shibboleth has two components: IdP (Identity Provider) and SP (Service Provider). IdP provides user authentication function for SP. SP provides services for users.

We have implemented Shibboleth functions into Opengate. We call shibbolized Opengate "SSO-Opengate".

Figure 4 shows system configuraton of SSO-Opengate. SSO-Opengate works as SP of Shibboleth.

A user launches Web browser on his/her PC. This HTTP request is diverted to Opengate. The directory containing Opengate system is protected by Shibboleth. As the result, the HTTP request is forwarded to the IdP. IdP shows the authentication page (Figure 5). The user inputs his/her user-id and password. After the authentication, Opengate shows two pages. The one is authentication notification page (Fig. X), which contains user ID and time stamps of checking the connection. The second is a university portal site. Opengate starts watching the use of the network. To close this authentication notification page, SSO-Opengate understands the user finish to use network. SSO-Opengate closes the firewall immediately.

After authentication with SSO-Opengate, users can use SPs without requiring any additional authentication procedures.

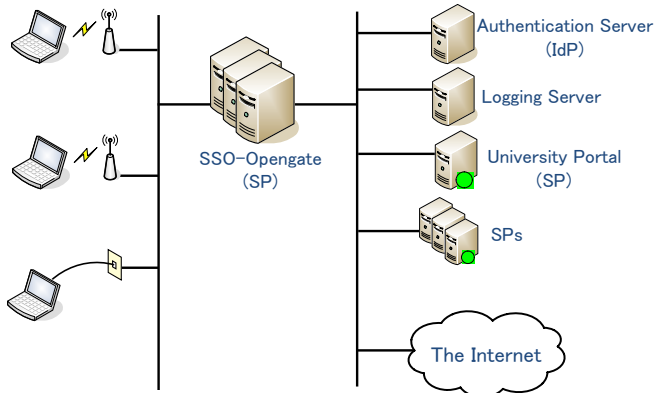


Figure 4. Configuration of SSO-Opengate.

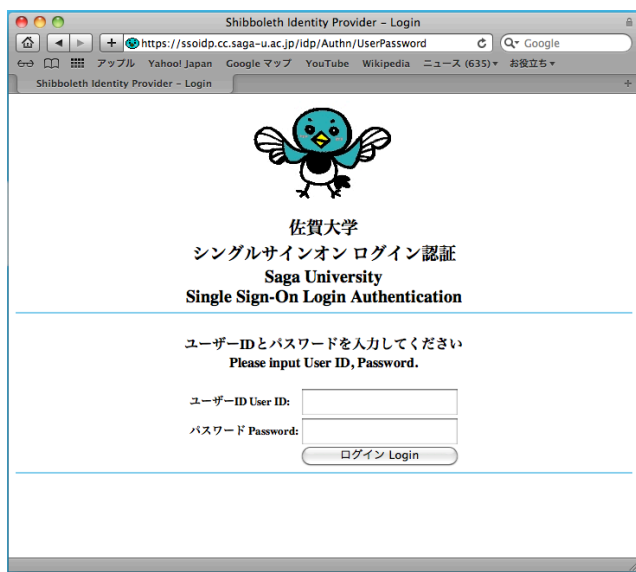


Figure 5. Window for Shibboleth authentication.

IV. OPENGATE ON VIRTUAL ENVIRONMENT

Recently, virtual machine technologies are growing rapidly. Many operating systems are running on virtual environment on a single physical machine. Each operating system connected to virtual networks with virtual switches. Physical networks and virtual networks are integrated.

We have been operating SSO-opengate on a virtual environment with virtual networks. We are using VMWare ESX 4.0 as the virtual environment in Saga University's network systems. Nine SSO-Opengates are running on one physical machine with Xeon E5540 2.53GHz (Quad Core) × 2 CPU, 20GB main memory, 2 ports of CNA (Converged Network Adapter) and 2 ports of 10/100/1000BASE-T Ethernet. Figure 6 shows virtual machine status for SSO-opengate.

Even though SSO-Opengate is running on virtual machine, the performance of SSO-Opengate is entirely satis-

| 名前 | 状態 | 使用領域 | ホスト CPU - MHz | ホスト 大抵 - MB | ゲスト 大抵 - % | アラーム アクション |
|--------------|-------|----------|---------------|-------------|------------|------------|
| Opengate1 | パワーオン | 34.00 GB | 50 | 2085 | 4 | 有効 |
| Opengate2 | パワーオン | 34.00 GB | 50 | 2085 | 4 | 有効 |
| Opengate3 | パワーオン | 34.00 GB | 101 | 2083 | 9 | 有効 |
| Opengate4 | パワーオン | 34.00 GB | 101 | 2084 | 5 | 有効 |
| Opengate5 | パワーオン | 34.00 GB | 50 | 2084 | 4 | 有効 |
| Opengate6 | パワーオン | 34.00 GB | 126 | 2086 | 4 | 有効 |
| Opengate7 | パワーオン | 34.00 GB | 50 | 2086 | 4 | 有効 |
| Opengate-fed | パワーオン | 34.00 GB | 75 | 2085 | 4 | 有効 |

Figure 6. Status of SSO-Opengates on virtual environment.

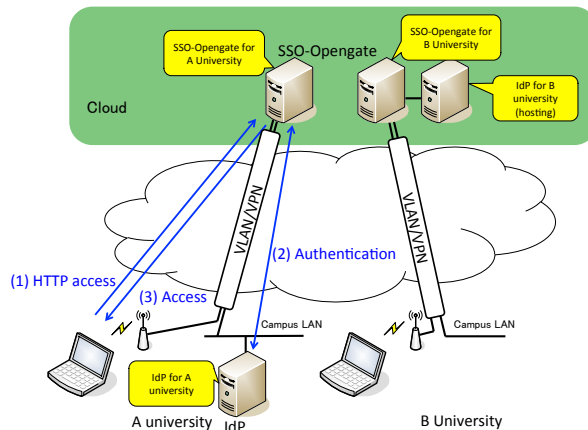


Figure 7. Opengate on cloud.

factory for providing services for some hundred PCs.

V. OPENGATE ON CLOUD

Virtual networks can be expanded flexibly with VLAN or L2VPN technologies.

We propose “Opengate on Cloud” in Figure 7, which is a cloud based user authentication system for mobile LAN for any organizations.

The advantage of this style of the service is that any organizations need not to operate SSO-Opengate by themselves. This style reduces cost for installation and operation. We think this is good for small organizations. This style may have the disadvantage of long turn around time if clients use slow network connection.

VI. CONCLUSION

In this paper, we described Opengate and its extension with Shibboleth authentication. We also proposed cloud type services with Opengate.

Among various access control systems of a captive portal type, Opengate has advantages: simple user interface, easy administration, flexible authentication, quick disconnection responding user's finish of use, expandability, and so on. The

expandability enables us to introduce IPv6 and Shibboleth single-sign-on features into Opengate.

Currently, we operate Opengate gateways on a virtual machine environment. Namely Opengate can be exported as a cloud base service. The cloud-based Opengate provides user authentication for organizations without having their own Opengate systems. User organizations do not need to pay their cost for installation and operation for user authentication.

SSO-Opengate is ready to be SP in the GakuNin project led by NII [11]. The cloud base SSO-Opengate must be benefit for joining GakuNin.

ACKNOWLEDGMENT

Opengate and SSO-Opengate are developed by the Opengate development team [9].

REFERENCES

- [1] NetSpring Inc., *FEREC*, <http://www.ferec.jp/> (05/01/2012 access).
- [2] Institute of Electrical and Electronics Engineers, Inc., *IEEE802.1X-2004*, <http://www.ieee802.org/1/pages/802.1x-2004.html> (05/01/2012 access).
- [3] Yoshiaki Watanabe, Kenzi Watanabe, Hirofumi Eto and Shin-ichi Tadaki, *An User Authentication Gateway System With Simple User Interface, Low Administration Cost And Wide Applicability*, IPSJ Journal, Vol. 42, No. 12, pp. 2802 - 2809 (2001.12) (In Japanese).
- [4] Makoto Otani, Katsuhiko Eguchi, Hirofumi Eto, Kenzi Watanabe, Shin-ichi Tadaki and Yoshiaki Watanabe, *Implementation of IPv6 Functions for a Network User Authentication System Opengate*, ACM SIGUCCS 2005 Fall Conference (held in Monterey, California, November 6 - 9, 2005), pp.283-286 (2005.11).
- [5] Makoto Otani, Katsuhiko Eguchi and Kenzi Watanabe, *Development of a Network User Authentication System for IPv4/IPv6 Dual Stack Network*, IPSJ Journal, Vol. 47, No. 4, pp. 1146 - 1156 (2006.4) (In Japanese).
- [6] Makoto Otani, Hirofumi Eto, Kenzi Watanabe, Shin-ichi Tadaki and Yoshiaki Watanabe, *Development of the Network User Authentication System Supporting Single Sign-On*, IPSJ Journal, Vol. 50, No. 3, pp. 1031 - 1039 (2010.3) (In Japanese).
- [7] The FreeBSD Documentation Project, *IPFW, FreeBSD Handbook*, http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/firewalls-ipfw.html (06/01/2012 access).
- [8] The Apache Software Foundation, *Apache HTTP SERVER PROJECT*, <http://httpd.apache.org/> (06/01/2012 access).
- [9] Yoshiaki Watanabe, *Opengate Home Page*, <http://www.cc.saga-u.ac.jp/opengate/index-e.html> (06/01/2012 access).
- [10] Internet2, *Shibboleth*, <http://shibboleth.internet2.edu/> (05/01/2012 access).
- [11] National Institute of Informatics, *GakuNin - Academic Access Management Federation in Japan* <https://www.gakunin.jp/docs/en/fed/about> (06/01/2012 access).