Customer Case Study

Japanese ISP Applies Service Control Solutions to Deliver Secure Broadband Services

Executive Summary

Customer Name

Plala Networks Inc.

- Headquarters: Tokyo, Japan
- 170 employees; 2 million users (1.53 million broadband users)
- Reputation for high level of customer satisfaction (ranked number 1 three years in a row)

Industry

Internet Service Provider

Business Challenges

- Increasing Internet threats created the need to protect users, especially those without security expertise.
- The Plala backbone network was experiencing congestion due to traffic associated with illegal distribution of copyrighted work (program-to-program file sharing).

Network Solution

- Cisco Service Control Engine (SCE) 2020 for URL filtering and packet filtering
- Elimination of need for client software on PCs

Business Results

- Gained protection from intrusions and viruses on an application level.
- Created an efficient, optimally performing broadband environment with the ability to restrict program-to-program file sharing.
- Reduced number of customer complaints related to security problems.
- Established foundation for providing transparent services to users.

Plala Networks relies on Cisco® technology to filter traffic, allowing its customers to use the Internet with "security and peace of mind."

Business Challenges

Over the past several years, the broadband market in Japan has expanded dramatically, which, in turn, has had a positive effect on service providers such as Plala Networks Inc. As its user base expanded to make it the one of the top five broadband providers in Japan, Plala noticed an increasing number of cases in which minors and novice Internet users were being affected by Internet threats. The Internet service provider, recently rated number one in customer satisfaction in Japan, has constantly provided services for customer convenience and security. The increase in threats raised concern at all levels of the company, especially considering the high ratio of broadband users and the nature of the increased exposure to users posed by always-on broadband connections. Of Plala's 2 million users, 1.53 million are broadband users (as of June 2005).

Based on the situation, Plala began working on a variety of security measures with the aim of enabling their customers to use the Internet "securely and with peace of mind." For establishing internal security, the company has continually reviewed all operational and system aspects as part of obtaining Information Security Management System and Privacy Mark certifications.

For building in security at the user service level, Plala already provided e-mail virus checking and encryption as optional services. However, the provider found that the optional services were being adopted only by customers with a certain degree of understanding about the dangers of the Internet. Novice customers, without knowledge of the Internet and related threats and, therefore, in the most need of protection, were not typically using the optional services. Katsumi Nagata, director of Plala Networks and general manager of the System Development Department and Network Engineering Department, says, "There is an increasing number of people who do not know what a virus is or what they should do to prevent children from accessing pornographic or violent sites. However, we would like such people to use the Internet more securely. To accomplish this goal, a potential solution is useless unless it is made the default or offered free of charge. We wanted to make a system in which our least-experienced users can be protected from the outset."

Network Solution

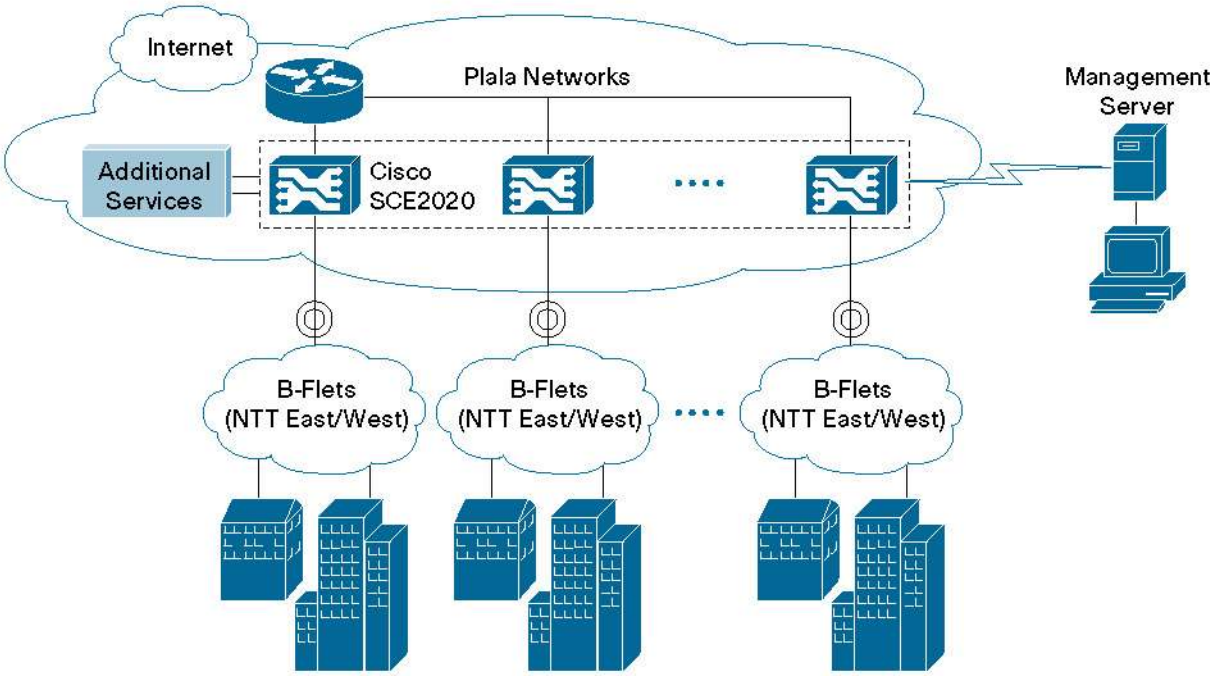
Since November 2003, Plala has controlled bandwidth of peer-to-peer (P2P) traffic using the Cisco Service Control Solution (formerly a P-Cube offering). With this solution, Plala eliminated the problem of the entire Plala backbone network being congested due to traffic from Internet users other than Plala members, typified by users of P2P file-sharing services. The improvement in traffic flow has greatly raised the overall experience for all users.

Speaking on this topic, Shinya Adachi, manager of the Network Engineering Department of Plala Networks, says, “Everyone is affected when some users consume large amounts of bandwidth for illegally distributing copies of copyrighted content. With the Cisco Service Control Solution, we were able to create an environment that allows everyone to share resources fairly.”

Approximately six months since Plala first began using the Cisco Service Control Solution, URL filtering and packet filtering functions were announced by Cisco for its higher-end models. Plala immediately began considering the provision of services based on these capabilities. The direction of services using the Cisco Service Control Engine (SCE) 2020, which is the flagship model for the Cisco Service Control Solutions, was decided upon in the summer of 2004. The system configuration was finalized in November, and development began in December.

Today, Plala’s system configuration (see Figure 1) includes a Cisco SCE 2020 implemented at each point where regional access is concentrated. Adachi commented on the management server connected to the SCE 2020 saying, “IP addresses change each time a user connects, so the management server performs the role of identifying each customer even when the IP address changes, and sends the customer’s settings to the SCE 2020 to provide services.” The establishment of this mechanism has made it possible to provide services without requiring users to install client software on their PCs.

Figure 1
The Plala Network



"Since the Cisco SCE 2020 can make judgments on an application level, it is possible to block traffic that is spoofing the port number. With this ability, we can protect our network from performance degradations – high performance is a vital contributor to our reputation for leading customer satisfaction."
– Yasuhiro Horike, Manager, System Development Department, Plala Networks Inc.

On the SCE 2020 foundation, the company introduced its "Net Barrier Basic" URL filtering and packet filtering service. The service is being offered free of charge to all users. Net Barrier Basic provides transparent URL and packet filtering services, making it possible to protect users from network threats regardless of each individual's knowledge or skills. Net Barrier Basic relies on three major features gained from the Cisco SCE 2020:

- **High performance.** Yasuhiro Horike, manager of the System Development Department at Plala Networks, says, "Since we first used the Cisco SCE 1010 (formerly SE 1000) for bandwidth control, we have valued the ability to deliver extremely high throughput. Now that we have moved to the SCE 2020, we do not experience any reductions in performance even when using URL filtering and packet filtering."
- **Packet control on a Layer-7 application level.** For Plala, the most common packet filtering is port-number-based control. For example, use of port 80 is deemed to be a Web service. However, SCE 2020 makes judgments on an application level. Even if there is a Website on a port other than 80, flexible responses can be made to allow packets to pass as long as it is a Website. Horike explains, "The Cisco SCE 2020 can make judgments on an application level, making it possible for us to block traffic that is spoofing the port number. With this ability, we can protect our network from performance degradations – high performance is a vital contributor to our reputation for leading customer satisfaction."
- **System architecture.** The SCE 2020 is purpose-built to support per-subscriber application-based services, enabling the transparent provision of services tailored to suit each subscriber.

Business Results

The Cisco SCE 2020 has enabled Plala to provide customers with multiple benefits:

- **Consistent broadband environment.** By controlling network bandwidth consumed by P2P file sharing and optimizing network bandwidth, Plala provides an environment in which users can predictably and fairly use resources.
- **Predictable broadband access.** With the Net Barrier Basic service implemented on the SCE 2020, intrusions and viruses can be blocked at the application level. The use of URL filtering and the provision of these functions as default capabilities make it possible for novice Internet users to receive services in a protected environment.
- **Optimization of support services.** In the past, Plala's customer center addressed many issues regarding virus infections and security problems. As more people become covered by Net Barrier Basic, Nagata predicts, "User inquiries will undoubtedly decrease. These support resources will be redirected to other services such as service guidance and instructions."
- **Foundation for providing services tailored to each user.** The combination of the management server and the SCE 2020 enables each user to be identified, which has enabled the construction of a foundation for providing optional services tailored to suit the needs of each customer. With regard to this point, Nagata says, "In a way, this is a uniform service. The main theme was to provide the service by default and free of charge, but some users want a more advanced service. For example, with URL filtering, there are some people who want greater customization and basically wish to block violence and pornography but allow certain items. We are currently considering such services with a greater degree of customization. The system that we have created will provide the necessary foundation for this level of customized service."

Next Steps

Regarding Plala's desire to provide more advanced security measures in addition to the optional services mentioned above, Nagata says, "Although the service offerings are still in the conceptual stage, we would like to provide security measures that allow us to logically determine responses for any discovery of a security problem or vulnerability. We would also like to offer a system that provides even greater protection by warning customers of infection by worms and viruses, and notifying them of how to respond to the situation. By providing more secure services, we would like to let people use the Internet with a greater sense of peace of mind."

For More Information

For more information on the Cisco Service Control solution, visit: http://www.cisco.com/en/US/products/hw/cable/products_promotion0900aecd801cac91.html.

For more information about Plala, go to: http://www.plala.or.jp.

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on **the Cisco Website at www.cisco.com/go/offices.**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica Croatia • Cyprus • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Printed in the USA C36-331385-00 01/06