SPX: New Group Communication System Based on Multi-VPN Association Model

Takeshi Yagi†, *Tsutomu Kondoh, Takeshi Kuwahara, and Junichi Murayama*

Abstract

This article describes a secure networking platform, called SPX (secure networking platform for group-oriented exchange), that can provide a new group communication system with global reachability like the Internet and the security of virtual private networks (VPNs). The key technology is a multi-VPN association function, which is effective at extending the reachability of users in each VPN. It enables SPX to provide secure group communication services based on a community network.

1. Introduction

The Internet can achieve global communication among a huge number of people economically, so it has rapidly become increasingly widespread all over the world. However, this feature results in security problems such as botnets [1], where malicious users invade hosts and servers illegally. Therefore, users who access the Internet by using their hosts and servers must limit access to themselves from the Internet, so usability is decreasing.

These problems can be solved by using virtual private networks (VPNs) [2], which are already used by many enterprises. A VPN is a logical closed network that provides reachability between only specific users. Therefore, security can be improved by managing the users who access each VPN. However, the global reachability of the Internet is lost.

To achieve both global reachability and security, we are developing SPX (secure networking platform for group-oriented exchange) [3], which utilizes a multi-VPN association function. In SPX, users can access multiple VPNs simultaneously, so they can expand their reachability while maintaining security by accessing appropriate VPNs. As a result, SPX can provide a secure communication service such as a community service.

In this article, we describe the service model and the network model of SPX and explain the implementation.

† NTT Information Sharing Platform Laboratories
Musashino-shi, 180-8585 Japan
Email: yagi.takeshi@lab.ntt.co.jp

2. Service model

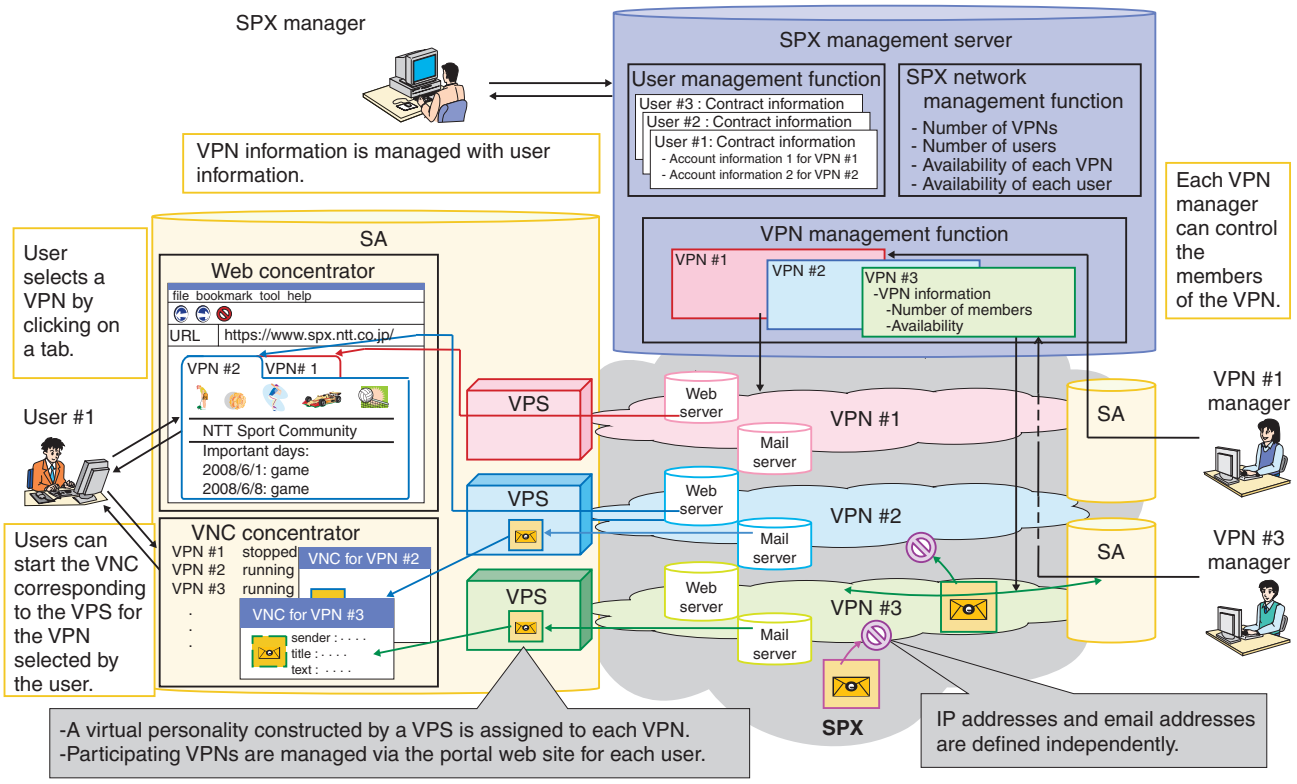
The service and network models of SPX are shown in **Fig. 1**. To make the features of the service model clear, we will explain the features of the network and the communication procedure and the benefits to users.

2.1 Network

A lot of VPNs are created over the SPX network. Each VPN is operated as an independent closed network and these VPNs do not connect with each other. So IP addresses and email addresses can be defined independently in each VPN. Although these addresses may be known to malicious users who do not belong to the VPN, malicious users cannot access the VPN by using them because these addresses are invalid outside the VPN. Consequently, malicious users cannot gain access to legitimate users.

2.2. Users

Users are permitted to access multiple VPNs simultaneously, so they can access multiple VPNs corre-



VNC: virtual network computing, VPS: virtual private server, SA: security agent

Fig. 1. Service and network models.

sponding to their interests. Consequently, users can control their reachability as desired, so usability is improved. In this user access model, we introduce logical user entities, called virtual personalities, to prevent communication across VPNs via users who belong to several VPNs.

The virtual personality is a virtual terminating device prepared by the VPN to which a user belongs. Each user has one or more virtual personalities, one for each VPN to which he or she belongs. Logically, each user is composed of multiple virtual personalities. Each virtual personality terminates a VPN to which the virtual personality is assigned. At present, a virtual personality cannot communicate with the other virtual personalities of the same user but communicates with other users and other virtual personalities in the user's VPN.

2.3. Communication procedure

Users will be provided with an access service composed of an SPX layer and a VPN layer. The access procedures are explained below.

First, the user must join the SPX service. At this time, the user is given a portal web site and secure means to access it. The site supports user access to VPNs.

After the user is permitted to join the SPX service, he or she can log in to the portal web site. At that time, the user can search for VPNs and ask to join an interesting-looking one. The user can join the VPN if the VPN's manager gives permission.

After the user is permitted to join the VPN, his or her portal web site displays a login window for that VPN, enabling further access as desired.

Users can access multiple VPNs simultaneously according to their interests. At present, different graphical user interfaces (GUIs) are provided to users for different services.

Users will log out from a VPN when the purpose of the communication in the VPN has been achieved. In addition, if the user has no intention of accessing the VPN again, the user can unregister from the VPN.

Users log out from their portal web sites after logging out from all VPNs. In addition, if the user has no intention of using the portal web site again, he or she can unregister the SPX by an off-line process.

3. Network model

To achieve the service model of the SPX, we used a network model composed of two kinds of devices. First, we allocated a logical edge router, called a security agent (SA) for each user. We also deployed an SPX management server to manage the whole SPX network and all the VPNs in a hierarchical manner.

3.1 SA

Each SA manages a user terminal and the virtual personalities assigned to the VPNs to which that user belongs. An SA provides functions for selecting and associating multiple VPNs as a portal web site only for that user. It concentrates the information from each VPN via each virtual personality and sends the information to the user with separate information for each VPN. SAs have two access functions that can improve security by enabling users to access the VPN without storing data on their own terminals.

(1) Web concentrator

Web concentrators [4] can concentrate information from multiple VPNs by using only a web application. Each virtual personality receives information for one VPN as a web terminal. In addition, the web concentrator preserves the information for each VPN in the browser tab assigned to each virtual personality. By displaying multiple tabs, a web concentrator can provide functions for selecting and associating multiple VPNs by using one web browser window.

(2) VNC concentrator

In the SPX, each virtual personality is constructed by a virtual private server (VPS) in an SA to store VPN information outside the user terminal. The VNC concentrator can send the window from the VPS to the user terminal by using virtual network computing (VNC). A VPS is a logical computer, so many kinds of application can be deployed. Thus, VNC concentrators do not concentrate windows from multiple VPSs but unify selected windows from multiple VPSs.

3.2 SPX management server

The SPX management server manages users, VPNs, and the whole SPX network. It has three management functions.

(1) User management function

This function can be used by only the SPX manager to manage the relationships between users and virtual personalities. It manages contract information given by users when they join the SPX network, such as real name, real address, phone number, global IP address, and email address. It also manages account information for virtual personalities, such as information about the VPN to which the virtual personality is assigned. The contract and account information is used not only for charging the user but also for identifying malicious and unauthorized users.

(2) VPN management function

This function is provided for each VPN, so each VPN manager has management information for his or her VPN, such as the age limit, member account information, and private IP address.

(3) SPX network management function

This function can be used by only the SPX manager to manage information about the whole SPX network, such as the number of VPNs in the network and the availability of each VPN. It can also advertise VPNs to users according to their interests.

4. Implementation

We implemented a prototype system of the SPX. Screen shots of a portal web site and web concentrator are shown in **Fig. 2**. The system is actually implemented in Japanese; the English is shown only for reference. In the portal web site, the VPNs to which the user belongs are shown as a list. Users can set account information for each virtual personality according to the VPN to which the virtual personality is assigned. For example, a user can set his or her real name as account information for only a specific virtual personality.

When a user logs in to a VPN on his or her portal web site, a tab showing the VPN name is generated automatically and a window showing information about the VPN whose name is on the tab appears. This window shows application tabs prepared by each VPN for using web applications. These application tabs are generated automatically in response to commands from the VPN manager, so different information is displayed when the user uses the same application in different VPNs.

The VNC concentrator of the prototype system is shown in **Fig. 3**. A window of the VNC concentrator can be displayed by clicking the tab on the portal web site. From this window, the user can start up windows of multiple VPSs to which the user belongs simulta-

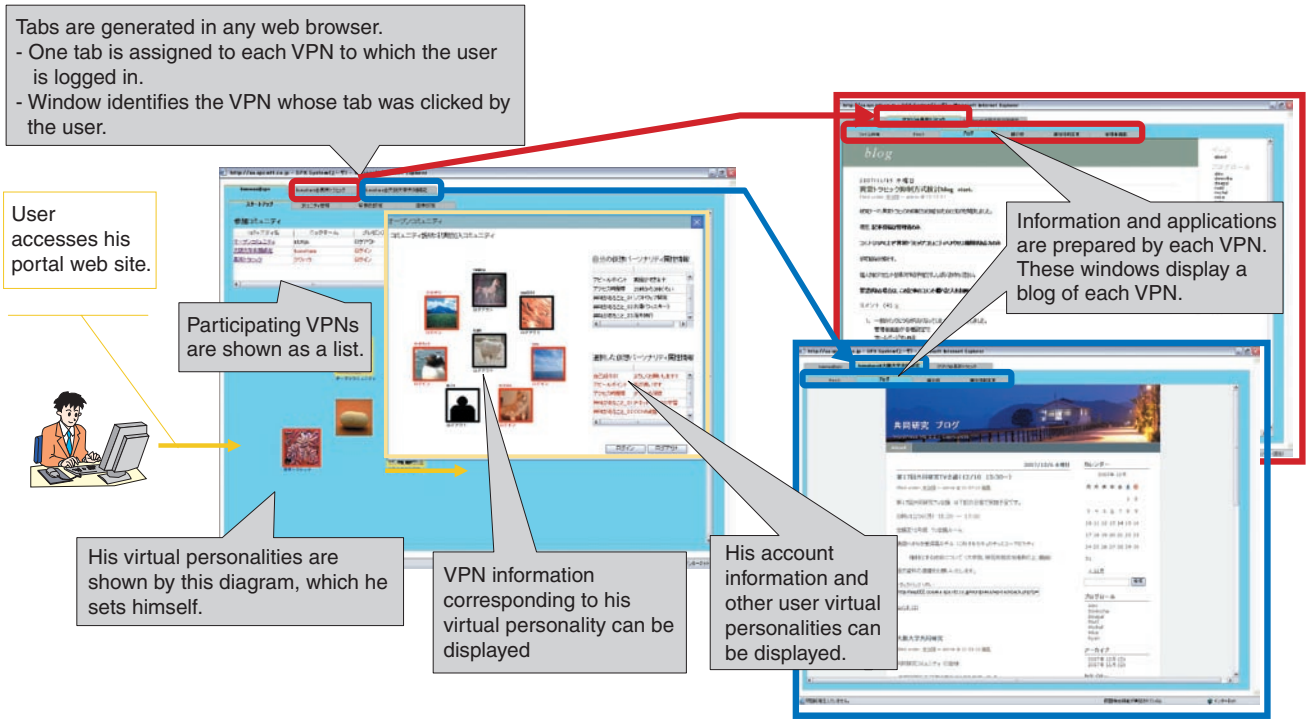


Fig. 2. Portal web site and web concentrator.

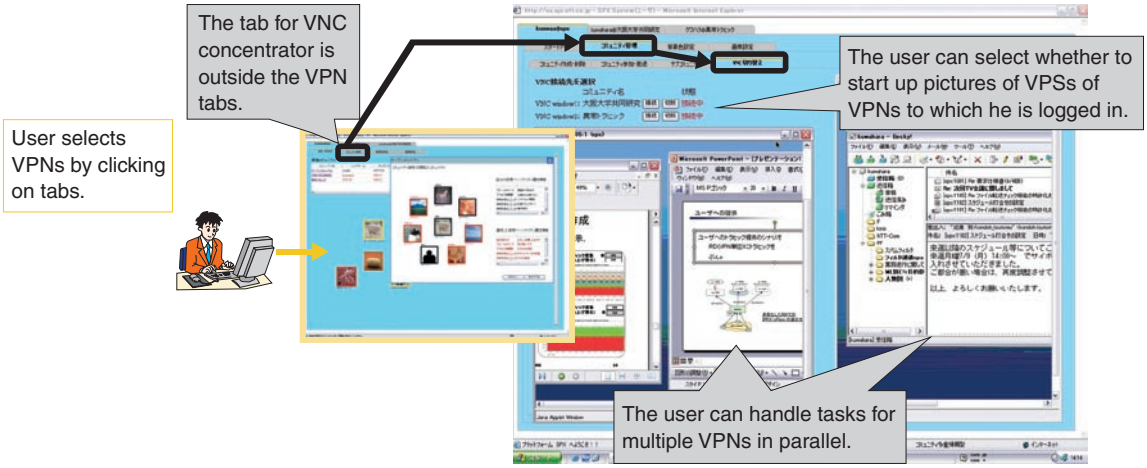


Fig. 3. VNC concentrator.

neously. Consequently, the user can handle tasks for multiple VPNs in parallel while preventing information being accidentally sent to different VPNs.

Finally, management windows for the two kinds of manager are shown in **Fig. 4**. The manager for each VPN can be set individually. The VPN manager, who is a member of the VPN, can increase/decrease the number of members in the VPN and applications used in it. Then, by registering the URL of conventional application servers that have already been used, the VPN manager can generate application tabs for accessing these conventional application servers. On the other hand, the SPX manager, who works for the service provider, manages the whole SPX network by using not only the windows for all VPN managers, but also ones that describe maps and lists for displaying the availability of each user and VPN. In addition, the SPX manager can read windows that describe the

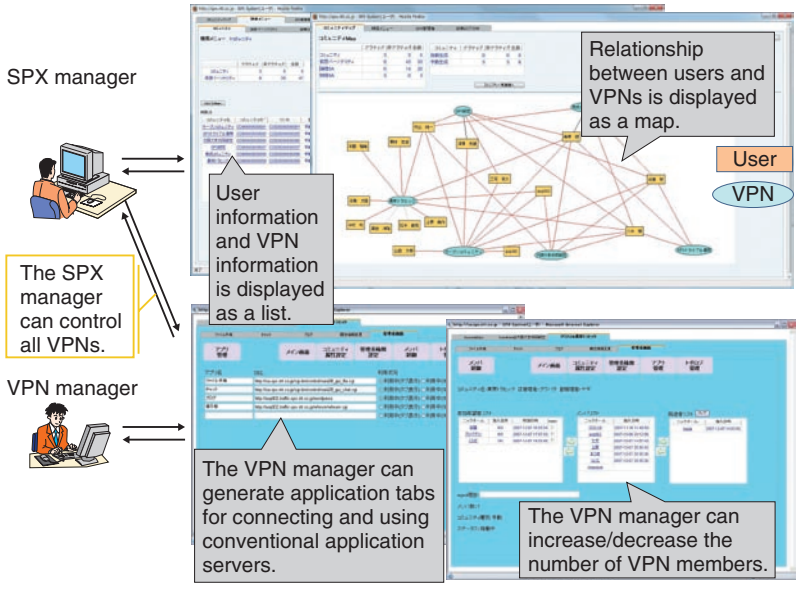


Fig. 4. Management windows.

relationship between users and VPNs in the whole SPX network. By using these windows, the SPX manager can easily check the status of the whole SPX network.

5. Conclusion

SPX can provide a new group communication system that combines global reachability like the Internet and the security of VPNs. It lets users generate VPNs easily and register applications for them as they wish. Additionally, users can access multiple VPNs simultaneously from the same user terminal while maintaining security. The SPX manager can manage the whole SPX network hierarchically by providing a VPN management function to each VPN manager. Thus, the SPX system enables the sharing of information with acquaintances or enterprises while maintaining security. In future, we will evaluate the network architecture of the SPX by performing tests on the prototype system.

References

[1] http://www.sans. org/reading_room/whitepapers/malicious/1299.php
[2] E. Rosen & Rekhter Informational, "BGP/MPLS VPNs," IETF RFC 2547, Mar. 1999.
[3] T. Yagi, T. Kondoh, T. kuwahara, J. Murayama, H. Ohsaki, and M. Imase, "Architecture Design for SPX: Secure networking Platform for group-oriented eXchange," 7th Asia-Pacific Symposium on Information and Telecommunication Technologies (APSITT2008), Apr. 2008.
[4] Y. Takahashi, K. Sugiyama, H. Ohsaki, M. Imase, T. Yagi, and J. Murayama, "On Network Architecture for Realizing Group-Oriented Communication," 7th Asia-Pacific Symposium on Information and Telecommunication Technologies (APSITT2008), Apr. 2008.

Takeshi Yagi
Secure Communication Project, NTT Information Sharing Platform Laboratories.

He received the B.E. degree in electrical and electronic engineering and the M.S. degree in science and technology from Chiba University, Chiba, in 2000 and 2002, respectively. He joined NTT in 2002. Since then, he has been engaged in R&D of technologies for IP VPNs, IP routing and forwarding, traffic monitoring, multilayer cooperation, virtual networks, and secure group communication. He is a member of the Institute of Electronics, Information and Communication Engineers (IEICE) of Japan and the Institute of Electrical Engineers of Japan (IEEJ).

Tsutomu Kondoh
Secure Communication Project, NTT Information Sharing Platform Laboratories.

He received the B.E. degree in applied physics from Keio University, Tokyo, in 2004. Since joining NTT Communications in 2004, he has been engaged in the development of optical networks. His current research interests include networking technologies and applications based on closed communities.

Takeshi Kuwahara
Research Engineer, Secure Communication Project, NTT Information Sharing Platform Laboratories.

He received the B.E. and M.E. degrees in electrical engineering from Waseda University, Tokyo, in 1995 and 1997, respectively. Since joining NTT in 1997, he has been engaged in R&D of ATM networks, IP VPNs, VPS systems, and network security. He is a member of IEICE.

Junichi Murayama
Senior Research Engineer, Supervisor, Secure Communication Project, NTT Information Sharing Platform Laboratories.

He received the B.E. and M.E. degrees in electronics and communication engineering from Waseda University, Tokyo, in 1989 and 1991, respectively. Since joining NTT in 1991, he has been engaged in R&D of ATM networks, IP VPNs, IP/optical multilayer networks, and traffic control systems. He is a member of IEICE and IEEJ.