Papers on UNIVERGE Hardware

SAFEBORDER as SSL VPN Uniquely Enables New Style of Business Communications by Connecting Corporate Intranets and the Internet Seamlessly

By Masaya NORIFUSA*

ABSTRACT SAFEBORDER is an SSL VPN appliance product that offers a unique remote access solution to any customer. The SSL VPN market in Japan was first addressed a year ago by several leading vendors including NEC, and has been growing very fast since. Many corporations are about to come up with new ways of business operations and models utilizing the Internet far more effectively than ever by taking advantage many benefits of SSL VPN and the rapid development of broadband communications. Many corporations have already moved to the new network environment for the next stage of their corporate IT activities. SSL VPN is expected to play important roles in connecting people with people and data sources instantly through the Internet. In this paper, basic technologies and benefits of SSL VPN are discussed, and SAFEBORDER's unique features are then explained to show how it can change corporate IT and business operations in their use of the Internet.

KEYWORDS **SSL VPN, Authentication, Encryption, One-time password, Remote access, Trusted security chains, SOCKS, Clientless**

1. INTRODUCTION

The Internet has grown tremendously and has become part of daily activities in information retrieval, data exchange, real-time and interactive communications in the business world as well as with PC users at home during this past decade. Along with this Internet development, each corporation has built an intranet, which may be described as a private version Internet, to ensure secure communications within the corporation.

A lot of applications are being used and run day and night on the Internet for pleasure and business, however, only for important internal businesses within the intranet. These two networks use the same networking technology, TCP/IP Suite, and thus are designed to interoperate with each other seamlessly at IP network layer in principle. In other words, any of applications intended originally for either of them should be able to function in the other, which is the beauty of TCP/IP design. However, this principle has been bent by many measures and devices due to various security considerations since the middle of 90's. Eventually, in the current IP network environment, networks connected by IP devices and communication lines do not guarantee that applications can work across the border of networks.

This situation has been created by firewalls, which currently operate at almost all corporations, NAT, of which function is now included in all IP router devices, and use of private IP addresses, which narrows the range of transparent IP routing. After many years of coping with difficulties and problems these technologies have introduced, network administration has learned to live with these technologies, which are almost impossible to either discard or replace, by creating a large security administration policy.

Now these two IP networks, which have grown with different identities, are in a way asked to become one though it is different from the way the Internet was created in the 80's. To accomplish this task, a new concept of Internet VPN was introduced with technologies such as IPSec and MPLS. These technologies use an IP tunneling method: They each create a logical tunnel between two IP devices, so-called VPN devices which must be IP reachable with each other. They carry IP packets from/to end user devices that are not IP reachable with each other. The

*Business Development Division

tunneling method has inherent limitations on its deployment range: As it requires interoperability and coordinated policy administration between VPN devices, and also requires a VPN device and an associated user device to be IP reachable, firewall and NAT can easily become obstacles in a large intranet.

On the other hand, however, the current generation of VPN has successfully enlarged a closed corporate intranet to a nationwide one by connecting network segments which used to be geographically separated. Users in the intranet have no big restrictions in accessing around within the widely extended intranet. However, it is still a closed-network to and isolated from the outside. With the growth of public network infrastructure and the advent of new applications, current user's interests and expectations have become much more focused on doing individual tasks free of time and location restrictions. Remote access is a typical demand from them and is considered as the most promising area in terms of utilizing the Internet and intranet to improve efficiency of internal business operations.

Well-managed remote access to VPN requires one indispensable feature, strong user authentication, because potentially any user can reach a VPN device and try logon anytime. Before making an intranet open to users by allowing their accesses from the Internet, we have to block anonymous communications first in order to ensure a following chain of trusted security enforcement measures, such as encrypted data communication, granular access control, and logging and auditing based on an individual user.

Another important requirement for managing secure remote access is to tie the security chains with a specific application that a user wants to access from somewhere outside of an intranet. Unfortunately many security technologies which have been applied to IP networks and applications so far have been implemented without any consideration for this requirement. For example, they may allow any application, once approved, to move around in the network; security measures applied to an application may require disabling or bypassing the network security; and so forth. SSL VPN, which was introduced to the market about a year ago, has the required facility and does not invite such fatal flaws. It provides a revolutionary solution to security management of both network and applications. In this paper, various SSL VPN architectures are discussed in detail, and SAFEBORDER, an SSL VPN appliance, is introduced to see real benefits to use SSL VPN products.

2. WHAT IS SSL VPN

The standardized definition of SSL VPN is not yet established, but is commonly understood to be a VPN created by using SSL technology in addition to other technologies such as HTTP, SOCKS, Java applet, ActiveX control, RADIUS, LDAP, and Digital Certificate. A SSL VPN product is basically an integration of these proven technologies to provide a trusted security chain, i.e. user authentication, data encryption, granular access control, and auditing. It uses network addresses such as IP address and port number for various judgments as firewalls do, but, for advanced and more rigorous security management, it relies more on a user ID and an actual application invoked.

A trusted security chain is one differentiation of SSL VPN products from other security products which function as stand-alones at one location, like a firewall. SSL VPN products are the first to facilitate a framework to integrate various security technologies within a security chain and can be considered as a new generation security products.

The most remarkable characteristic of SSL VPN is that it has achieved 'clientless' architecture, requiring neither software nor hardware to be installed on a user PC prior to establishing a VPN from a PC to an SSL VPN device. This revolutionary architecture differentiates SSL VPN from IPsec-based VPN, and creates a wider range of VPN-based applications, such as remote access VPN and B2B Internet VPN, which were once given up due to insufficient supporting technologies.

The clientless architecture provides the following benefits to users.

1) No VPN client software and hardware installation.
2) No VPN maintenance costs at end users.
3) No time wasted to get VPN service.
4) Centralized VPN device and access policy management.

With these beneficial characteristics, it results in a great reduction of TOC. For projects which are likely to require lots of resources, such as access from oversea operations, on-demand access from B2B partners, customer support, and confidential information service and remote access, SSL VPN can provide the best solution. These applications have one common characteristic: They do not need all day access, but when they do, they are likely to involve heavy traffics and have to be assured of a successful completion of VPN operations.

SSL VPN can provide very easy on-demand access

services and users, once registered in a user DB of the SSL VPN, can instantly get VPN service via SSL VPN product which is set up as in **Fig. 1**.

3. COMPARISON OF SSL VPN AGAINST IPSEC BASED VPN

When a VPN is simply interpreted as an encrypted data communication channel, there is not much difference between the two; both SSL and IPsec are well-proven technology to accomplish encrypted communication. However, there are lots of other differentiating factors between them.

1) SSL encrypts an application while IPsec does a network

An SSL negotiation is executed when an application needs to secure its communication session; an encryption key, so-called a session key, is generated for encrypting application data and the same key is never reused for another session. On the contrary, IPsec generates a key for encrypting IP packets between two devices, which is done totally independent of when and what application is executed. So, once the key is created, any communications between these devices are encrypted as long as the life of the key.

2) SSL protocol is self-closed in accomplishing security association

SSL relies on TCP and uses digital certificates for both client and server to accomplish not only mutual authentication but also key generation each time for further data encryption. Basically client and server do not need to contact any other server or device to accomplish these. On the contrary, IPsec needs PKI support and uses UDP to determine an encryption key, assuming that pre-setting a static key to either device is not desired option. IPsec communication requires UDP packet to be able to reach the PKI system other than two devices.

3) SSL is friendly to a proxy and NAT while IPsec is sensitive to both

SSL establishes its session via a SOCKS or HTTP proxy server by design and does not care about an execution of NAT as long as a NAT device maintains the SSL session. This nature comes from the fact that SSL relies on TCP. On the contrary, IPsec is sensitive to existence of NAT devices because its execution relies on IP address and IP routing. SSL allows either direct or indirect TCP session establishment, and IPsec requires direct IP reachability.

These are essential differences between the two technologies, and lead to different capabilities of the products based on them and requirements to IP

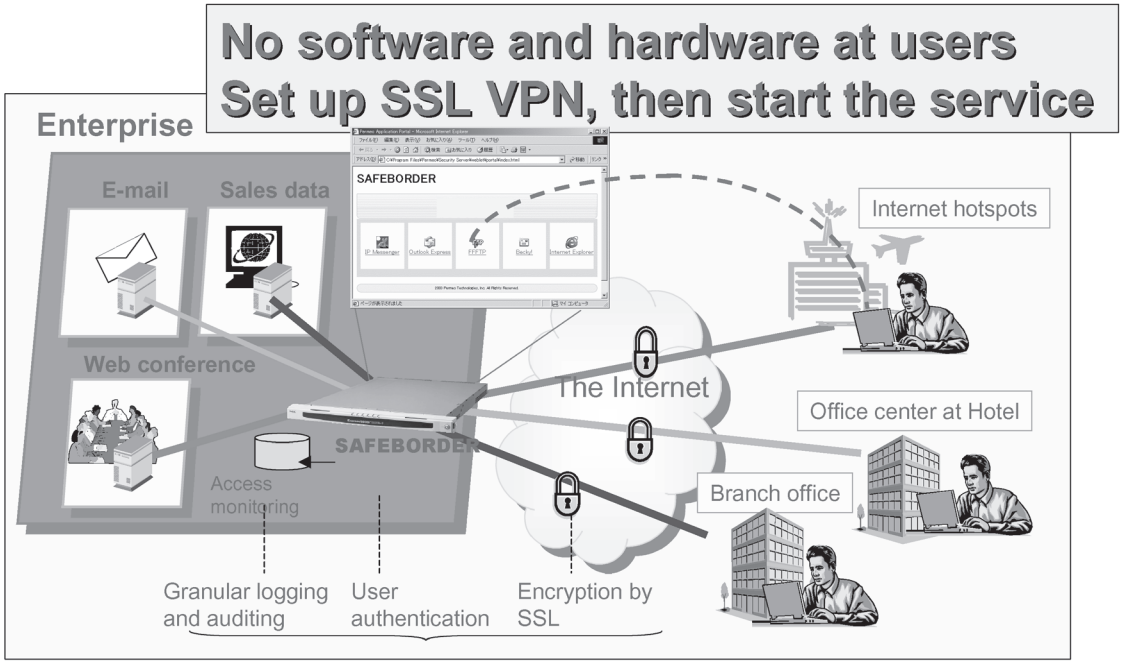

Fig. 1 Client-less architecture as the most powerful feature of SSL VPN.

infrastructure level conditions such as IP address. Here is the summary of the resulting products.

The SSL VPN product has the following benefits:

- Security administration is easy because; only client and server are involved in performing SSL; client is almost administration free; and applications used are restricted.
- There is no need for IP network reconfiguration, especially with border gateways in DMZ, such as firewalls, proxy servers, and NAT devices.
- By issuing unique certificates to client and server, strong mutual authentication is achieved each time when an application needs to be started.
- Traversal of networks, i.e. traversal from a partner intranet, via proxy server, firewall, and ISP network, to your firewall, SSL VPN, and intranet, is easy without opening ports at border gateways.

The IPSec-VPN product has the following benefits:

- Performance is better than SSL VPN which uses SSL layer.
- More applications, especially UDP applications, can use its encrypted tunnel.

One more important fact to be understood is that SSL works with IPsec without technical conflict. Because of this, SSL VPN products can be used in a network where IPsec is already used. Outside of that network or access to from other networks, SSL VPN products work independently from IPsec to provide on-demand VPN service and thus can widen a range of VPN applications.

4. SAFEBORDER

SAFEBORDER is an SSL VPN appliance which includes SSL VPN software, hardened OS, and hardware platform integrated in one, and offers an easy administration, higher security, and stable communication services to any user equally. It has combined SOCKS and SSL technologies to create a SSL-based VPN without installing SOCKS client on PC and with keeping best of each technology, i.e. firewall traversal and strong security. This integration of proven technologies achieves unique benefits that other technologies or methods, such as reverse HTTP proxy and Java-based port forwarding, cannot provide.

SOCKS is the IETF standard for implementing generic proxy services and has the following unique features.

1) User authentication process is embedded within the protocol.
2) Not only TCP but UDP proxy methods are included, and SOCKS is the only standard for implementing generic UDP proxy.
3) Domain name (FQDN) is used to set up an entire proxy in a case where an IP address cannot be used to specify a destination server.
4) SOCKS protocol repeats a proxy operation via multiple SOCKS servers.

As described in the previous section, SSL provides the most secure communication to an application. By combining SOCKS and SSL technologies together, following unique features materialize.

1) Web browser and server have SSL built-in, but there are many applications that have neither SSL nor security mechanism built-in. SOCKS provides generic proxy feature to these applications. Therefore, SSL-embedded SOCKS instantly enable SSL capability to those applications. Thus, applications that do not have any security feature become secure applications without any extra development work.

2) One disadvantage of using SSL is that SSL is not designed to be implemented with UDP-based application protocols, such as RTP while SOCKS is designed to proxy UDP applications. Therefore, SSL-embedded SOCKS can transport encrypted UDP packets to an application server via SOCKS server.

3) SSL authenticates client and/or server with their digital certificates, but not a user. SOCKS takes user authentication before establishing an application session, and thus SSL-embedded SOCKS always carry out an encrypted and granular user authentication. Since SOCKS initiates different user authentication methods when needed, such as OTP and CRAM with incorporating RADIUS and LDAP, all of user names, passwords, and other information managed by these methods are also securely carried on the Internet.

4) Using domain names and proxy chains extends a workable range of SSL across an unlimited number of IP network borders (**Fig. 2**). This is not achievable by other proxy technologies including HTTP proxy.

In addition to the above, there are many other

important factors that make SAFEBORDER a very useful product in a real network environment where user's conventional business situations can pose challenging requirements. The following are some of its practical features.

1) Group concept is introduced that associates each ACL with the user authentication process. For example, the user authentication is done strictly based on each user information without introducing any vulnerable, shared password for his/her group, and a group is determined by a user ID which is determined by the authentication process, and finally the authorization process takes place by picking up an ACL associated with the group which was just determined. (**Fig. 3**)

2) Log and audit management is implemented by a separate server. This is because there are industry requirements on log data, such as to maintain logs for three years. Logs collected by SAFEBORDER are periodically transferred to this server in order

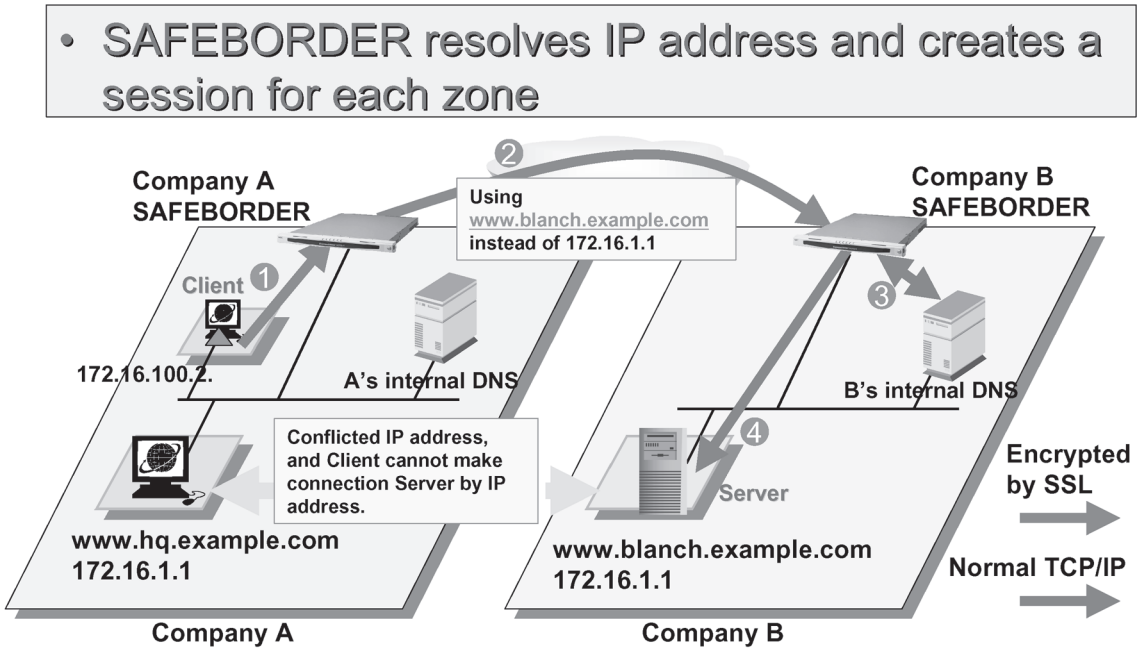

Fig. 2 Private IP independent proxy chaining by domain name.

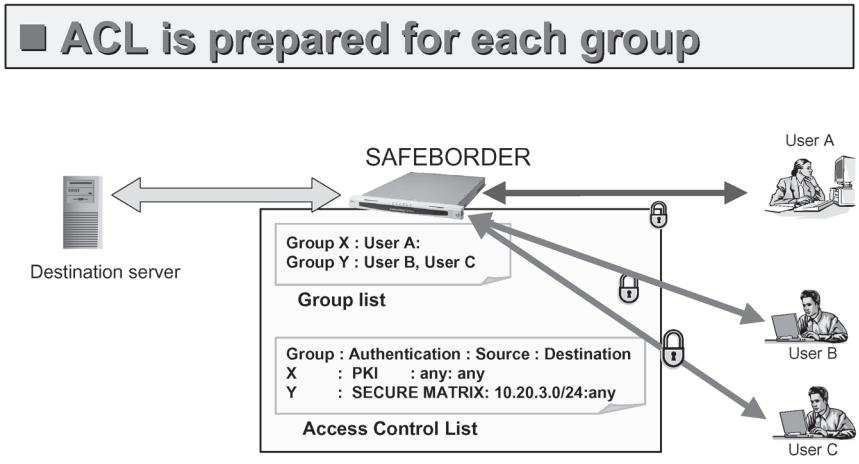

Fig. 3 User-based authentication and group-based access control.

to keep large volume of data for a long period and also to analyze the logs to find out who did what and when.

5. USAGE EXAMPLE

NEC uses SAFEBORDER for remote access service to its employees in the NEC global intranet. This service applies to all the NEC subsidiaries that use this intranet. Since many users are stationed nationwide in domestic and overseas, there was one indispensable requirement on the user authentication method: In order to offer client-less VPN service to the entire intranet users, the user authentication method should not require any client.

Among several alternatives, OTP (One Time Password) method based on random number matrix was selected to be worked with SAFEBORDER. This method requires only Web browser to pick up OTP from the matrix table generated each time of authentication. User information and OTP accepted by the OTP system are given to SAFEBORDER securely without involving user interaction. With this integration, simple but secure, and pure client-less VPN service has been made available (**Fig. 4**)

Currently about 5,000 users have participated in this service within two months, and hundreds of employees are constantly using the service to perform important internal business tasks without any delay from anywhere. This is start of new business style for coming broadband network era.

6. MARKET TRENDS

The SSL VPN market in Japan showed up about a year ago, and client-less feature of SSL VPN products has attracted many network integrators, system integrators, and IT administrators who have been struggling with difficulties of managing the other type of VPN for their users.

There is another reason why SSL VPN suddenly attracted so many users. In the past two years, public broadband network infrastructure, i.e. xDSL and FTTH, has penetrated into homes to provide LAN level performance at inexpensive costs, and not only individuals but local corporate offices now can easily get these lines and instantly be a part of the Internet. These users, therefore, started looking at new style of business communication, at real-time, on-demand, faster, and cost-effective, that once they wished to get but could not. Remote access and B2B are typical ones at the starting line.

Since SSL VPN has strong framework to integrate other security technologies, i.e. user authentication, PC integrity check, and application control, it will be covering multiple security market segments in

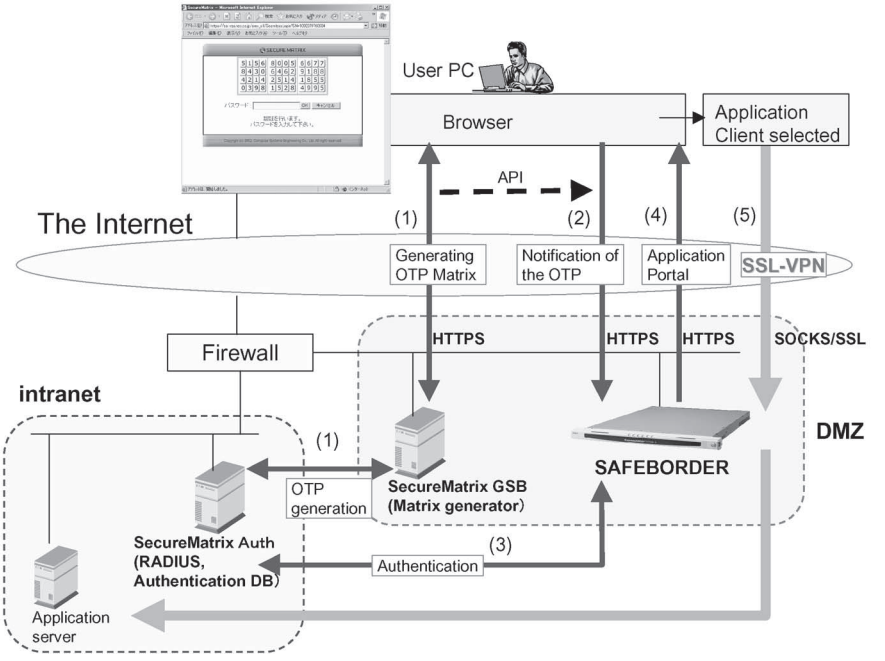

Fig. 4 One-Time Password system (SecureMatrix) and SAFEBORDER integration.

addition to the VPN market.

7. CONCLUSION

In this paper, SSL VPN and related technologies have been overviewed, and as an example of applying these technologies to real world requirements, SSL VPN product, the SAFEBORDER was explained with its unique features and benefits.

SSL VPN is very easy to start VPN service once after understanding of its essential technologies and basic IP networking issues surrounded. With its client-less architecture, setting up SSL VPN server with a list of users registered for authentication is the major task to be done at the beginning. Then, VPN service could be on-line instantly.

However, despite of its simplicity, many users tend to look at SSL VPN with pre-established knowledge of IPsec-based VPN. This attitude occasionally causes confusion such that all applications could be used by SSL, however allowing any application passing through the VPN leads the most dangerous application security vulnerability. Expectation to SSL VPN should focus on its strong security, managed application use, and NAT friendly communications.

SAFEBORDER has been designed and built based on this philosophy. It instantly embeds SSL capability to many insecure applications but manages security and communications at the most granular level by always taking trusted security chains starting from user authentication until user-based auditing. As described in the paper, the market has expectation to SSL VPN to integrate other important security technologies, and SAFEBORDER has already achieved some as exampled in the paper, such as OTP system and audit system integration. This direction will be enhanced along the market requirement growth to provide the most useful security product on time to the growing broadband network community.

Received September 27, 2004

* * * * * * * * * * * * * * * * *

Masaya NORIFUSA joined NEC Corporation in 1980 and had engaged in technology and product development on Internet and security area since 1989 to 2002 in NEC US subsidiaries. Currently he belongs to Business Development Division, Broadband Solution Business Unit of NEC and works on security solution business development. He holds CISSP (Certified Information Systems Security Professions) and NCP (NEC Certified Professional), and is a member of IPSJ and ISSA.

* * * * * * * * * * * * * * * * *