Deploying User-based Extranet without Global Addresses

Koichi Okada koichi@isl.ntt.co.jp
Eric Y. Chen eric@isl.ntt.co.jp
Teruyuki Komiya komiteru@isl.ntt.co.jp
Hitoshi Fuji fuji@isl.ntt.co.jp

NTT Information Sharing Platform Laboratories
1-1, Hikarinooka, Yokosuka-shi, Kanagawa 239-0847 Japan
tel: +81-468-59-2133 fax: +81-468-59-3365

Extranet is known to pose a number of threats to the confidential data exchanged among partner sites. End-to-end VPN network solutions are sometimes deployed to cope with both the external threats from the Internet and the internal threats within the mutual sites. However, because existing end-to-end VPN technologies require all participating hosts to have a global address, it is often speculated that the limited address space of IPv4 would eventually thwart their acceptance. Although we can wait for the arrival of IPv6 to alleviate this problem, in this paper we propose a method for deploying an end-to-end VPN using only private addresses by incorporating the Twice-NAT into our VPN-Exchange System (a star-type end-to-end VPN that we have proposed).

Keywords: End-to-end-VPN, extranet, Twice-NAT, IPv6, Security inside a corporate network

グローバルアドレスを使用しない個人単位エクストラネットの実現

岡田 浩一
Eric Y. Chen
小宮輝之
冨士 仁

NTT 情報流通プラットフォーム研究所
〒239-0847 神奈川県横須賀市光の丘 1-1
tel: 0468-59-2133 fax: 0468-59-3365

通信先サイトにおける安全性の保証が困難なエクストラネット通信において、インターネット上だけでなく、互いのサイト内における脅威に対処するためには、end-to-end VPN を利用することが有効である。しかし、そのためには全てのエンド端末がグローバルアドレスを持つ必要がある。これはアドレスが枯渇しつつある IPv4 では困難であり、十分なグローバルアドレスが確保できる IPv6 の普及を待つ必要があると考えられていた。我々は本稿において、スター型 end-to-end VPN を実現する「VPN-exchange 方式」に Twice-NAT を組み合わせることにより、グローバルアドレスなしで end-to-end VPN を実現する方法を提案し、IPv4 環境における end-to-end VPN の普及を可能にする。

キーワード: End-to-end-VPN, エクストラネット, Twice-NAT, IPv6, 社内セキュリティ

1 Introduction

Until recently, data encryption within an extranet (inter-organizational network) was performed from gateway of the sending party to the gateway of the receiving party. Because internal leaks caused by malicious users within the same organization are also possible [1], end-to-end VPN (user-based VPN) network solutions are sometimes adopted to completely seal the sensitive information exchanged between two parties. However, in order to construct direct encryption channels across the public network, most existing end-to-end VPN technologies require all participating hosts to have a global address directly. It is therefore speculated that the limited address space of IPv4 would thwart the acceptance of end-to-end VPN. In addition, NAT (Network Address Translator) technology commonly used in IPv4 may thwart the acceptance of end-to-end VPN because it affects the integrity of encrypted packets.

Although we can wait for the arrival of IPv6 to alleviate the address problem, it is certain that IPv6 and IPv4 will co-exist for

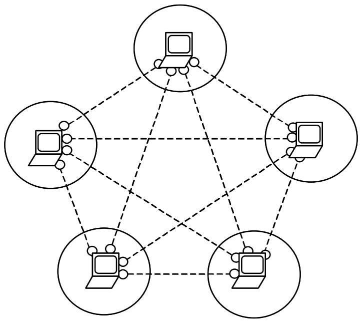

Fig.1 Conventional end-to-end VPN

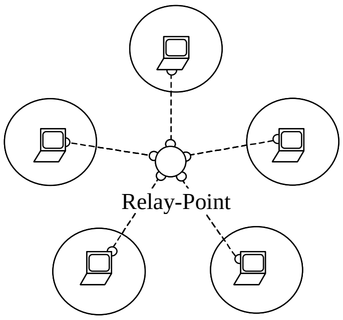

Fig.2 Basic VPN-Exchange

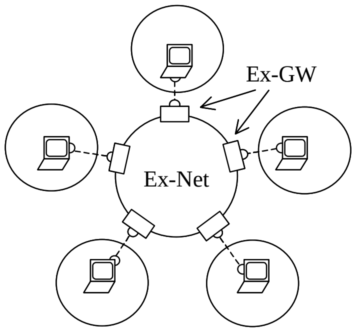

Fig.3 Scalable VPN-Exchange

many years to come. We need viable solution to support such heterogeneous network environment.

In this paper, we propose a method for deploying an end-to-end VPN between organizations without using any global address. This method is to be adopted on the network provider's side rather than the user's side.

In section 2, we briefly explain the VPN-Exchange System, which we proposed in the past. In section 3, we describe our proposed method in detail. We then evaluate our proposal in section 4 and outline our future work and conclusion in the last section.

2 Deploying End-to-end VPN using VPN-Exchange

We have proposed the VPN-Exchange System, in order to solve the inherent problems with the conventional end-to-end VPN [2].

2.1 Problems with the Conventional End-to-end VPN

Problems with the conventional end-to-end VPN are listed as follows:

(1) Since the contents of the communication cannot be investigated on the fly, it is impossible to enforce network security policy using a firewall.

(2) Interconnections between different encryption systems or different authorization systems are difficult.

(3) Since the number of encrypted communication channels can amount up to a square order of the number of users, the cost of management is extremely high in large-scale settings.

(4) Since the packet header is not encrypted, the communication partner can be easily identified by sniffing a packet.

(5) Global addresses are required for all communication hosts.

Note that this paper focuses on tackling the last issue listed above.

2.2 The VPN-Exchange System

We have proposed the VPN-Exchange System to solve the problems (1), (2), (3) and (4) listed in section 2.1. To establish an end-to-end VPN, the VPN-Exchange System does not adopt the conventional mesh-type connection model (Fig. 1), but instead the star-type connection model, which places a VPN relay point in the center (Fig. 2). Each user establishes one VPN tunnel to the relay point respectively. At the relay point, access control is performed based on the result of the user authentication, which is performed prior to the establishment of a VPN tunnel. This mechanism ensures secure communications within the specified user groups. Although this VPN model is not exactly end-to-end since data packets are decrypted at the relay point, it practically prevents internal leaks since there is no way to sniff the data packets inside the same user's network. Moreover, by sharing the relay point among mutually unfamiliar users, the extranet can be easily reconstructed by changing the access control rules at the relay point.

2.3 Achieving High Scalability

The VPN-Exchange System introduced in the previous section suffers scalability problems because the traffic converges at the relay point. In [3], we have made a proposal to address this issue. In order to achieve high scalability, the relay point was considered as a wide area backbone network (called "Ex-Net"), and the functions of the relay point are offered by the distributed gateways (called "Ex-GWs") placed on the boundary of the Ex-Net and the exterior network (Fig. 3). The relay point of the VPN-Exchange System has two basic functions: (1) establish a VPN tunnel upon a successful user authorization; (2) perform access control on all communication in VPN tunnels according to the results of the user authentications. These two functions are offered in Ex-GW. However, when two or more Ex-GWs have been placed, the gateway that performs user authentication and the gateway that performs access control may be different. In this case, information of user authentications needs to be delivered between Ex-GWs. In our proposal, Ex-GW assigns each user an

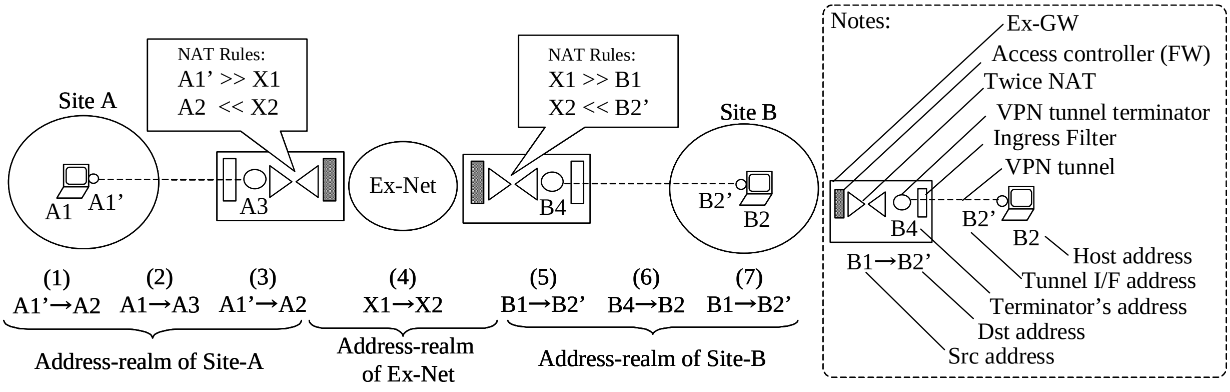

Fig.4 Proposed Method (Ex-GW with Twice-NAT)

address upon a successful user authentication. We call this function “address-mapping.” When a user who has been assigned an address by address-mapping sends a packet, he can be identified by the source address. In other words, the information of user authentication is delivered on a per-packet basis between two gateways to ensure security. The address-mapping can be implemented by assigning a tunnel interface address [4]. In order to prevent unauthorized uses of addresses reserved for the address-mapping function, ingress filtering [5] can be implemented in Ex-GW.

2.4 Evaluation of the VPN-Exchange System

Table 1 shows a comparison of the VPN-Exchange System with the conventional mesh-type end-to-end VPN.

3 Deploying user-based extranet without Global addresses

This section describes our proposed mechanism of deploying the VPN-Exchange System for hosts without a global address.

3.1 The Basic Idea

We propose a method of using private addresses as the source address and the destination address of a packet in a shared backbone network (a Ex-Net of VPN-Exchange System). When these private addresses overlap with private addresses used in the user’s network, the Twice-NAT function, explained in the next section, is performed at the Ex-GW to convert the addresses into non-overlapped addresses. It is then possible to identify the same host by a different private address respectively in each address-realms, that is, each of user networks and the Ex-Net (Fig. 4).

3.2 Twice-NAT

Our proposed mechanism uses Twice-NAT [6] on the boundary of different address-realms that may have overlapped private addresses.

The regular NAT (Network Address Translator) converts an internal address into an external one to allow hosts access to the public networks, such as the Internet. Therefore, each host behind the NAT can be recognized by a global address in public network. However, in our proposed mechanism, global addresses are not required since private addresses are assigned as the source address and the destination address of every packet in the shared backbone network (a Ex-Net of VPN-Exchange System). If the assigned private address is already in use by the users’ networks, this address is converted into another private address on the boundary of the user sites and the Ex-Net. Because conversion of both the source address and the destination address is required, two NATs are required for each site： the outbound NAT converts the address of the host inside the user site in the same way as a regular NAT, while the inbound NAT changes the address of the host outside the user site. The mechanism, which combines these two NAT, is commonly called “Twice-NAT”. Each site connected to the Ex-Net deploys Twice-NAT in its Ex-GW. Communication across the Ex-Net traverses two Twice-NATs on a single direction course.

Since it is difficult to convert the address of encrypted packet [7], Twice-NAT is performed right after the decryption process, or right before the encryption process at Ex-GW.

Each Ex-GW have NAT rules for conversion between addresses used in the user’s site and addresses used in the Ex-Net. In fact, the source address of a packet sent directly from a VPN

Table.1 Comparison of the conventional end-to-end VPN (Transport-mode IPsec) and our proposed system (VPN-Exchange).
Note: A - Good, B - Fair, C -Poor.

	Transport-mode IPsec		VPN-Exchange	
Realizing extranet without global addresses	B	- Special system, which perform UDP-encapsulation, is required on each end host. - Some protocols (FTP etc.) bring problems.	A	- No Special system is needed on end host. - Application level translation can be performed.
Policy enforcement on gateway	B	- Since the data portion is encrypted, there is no way to enforce policy on the communication contents. - Since the IP header is not encrypted, policy on the destination addresses can be enforced.	A	- Since a packet is fully decrypted at the relay point, policy on both the contents and destination addresses can be enforced.
Inter-connectivity	C	- In order to establish secure connections with partners using different encryption methods, a terminal needs to support all encryption methods.	A	- By equipping Ex-GW with multiple encryption methods, VPN-exchange facilitates communication between hosts using different methods.
Ease of configuration	C	- A user need to provide a lot of parameters in proportion to the number of partners. - When there are n hosts, the secure connections at number of $o(n^2)$ are used.	A	- A terminal can establish safe communication with many partners only by setting up one secure connection. - Even when there are n hosts, the secure connections at number of only o(n) are used.
Destination concealment	C	- Since the addresses of each packet is not encrypted, the destination can be easily sniffed.	A	- Since all packets are destined to an end terminal of Ex-GW in appearance, the actual destination is well concealed.
Third party requirement	A	- The contents of communication cannot be monitored by any third party, therefore there is no need for a trusted third party.	B	- Need a trusted third party since administrators of the relay point can monitor the contents of communication.
Communication delay	A	- Since only one encryption is performed on one-way, delay is comparatively small.	B	- Since two-time encryptions and additional access control processing are performed, delay is comparatively large.
Overhead of connection establishment	C	- Establishment of secure connection takes several seconds. The overhead occurs at every time to establish a connection to new partners.	A	- Establishment of secure connection takes several seconds. However, since the overhead occurs only once, it is not affected by the number of partners.

tunnel is the address of the tunnel interface. Also, the destination address of a packet forwarded into VPN tunnel used by the destination host must be the address of the tunnel interface of destination host. Therefore, an address of a user of VPN tunnel configured in NAT rules is the tunnel interface address. Note that conversion between an address in a user’s site and an address in other user’s site does not appear directly as a NAT rule because the address of each packet must be translated into an address in the Ex-Net once, instead of directly translating into an address that belongs to the partner’s site.

3.3 An Example

Figure 4 illustrates an example of a communication process using our mechanism.

Each site is directly connected to Ex-Net, without traversing the Internet. Host A1 with a private address A1 resides in Enterprise A, while Host B2 with a private address B2 resides in Enterprise B. VPN tunnel terminators at the Ex-GWs of Enterprise A and Enterprise B have private addresses A3 and B4 respectively. Between each host and the Ex-GW, a VPN tunnel is established after user authorization. A1' and B2' are assigned as the addresses of the tunnel interfaces to Host A1 and Host B2 respectively according to address-mapping.

In Enterprise B, Host A1 is recognized by the private address B1. On the other hand, Host B2 is recognized by the private address A2 in Enterprise A. In the Ex-Net, Host A1 and B2 are recofnized by private addresses X1 and X2 respectively.

These assignments are configured as the NAT rules for Ex-GWs. As described in previous section, these rules involve tunnel interface address. As the NAT rules of Ex-GW for Enterprise A, two rules appear in Figure 4: a rule for conversion between inside address A1’ and outside address X1 on outbound NAT (denoted as “A1’ >> X1”); a rule for conversion between inside address A2 and outside address X2 on inbound NAT (denoted as “A2 << X2”). Moreover, as the NAT rules of Ex-GW for Enterprise B, two rules appear: a rule for conversion between outside address X1 and inside address B1 on inbound NAT (denoted as “X1 >> B1”); a rule for conversion between outside address X2 and inside address B2’ on outbound NAT (denoted as “X2 << B2’ ”). Note that the direction of these expressions are in accordance with the topology in Figure.4.

Each site and Ex-Net is an independent address-realm. A private address in respective address-realm referes to exactly one host. However, a same private address in different address-realms may refer to different hosts. For example, it is possible that addresses A3, B1 and X2, each of which refers to a different host, are the same private address.

Next, we explain the proposed mechanism by considering a scenario in which a packet is delivered from Host A1 to Host B2. In the explanation below, a packet is expressed as "S -> D", where S is the source address and D is the destination address of the packet.

(1) Since Host B2 is recognized as A2 in Site A, the packet transmitted towards host B2 from Host A1 is generated as a packet "A1' -> A2." Note that the source address is the tunnel interface address A1'.
(2) Inside Host A1, this packet is encrypted and encapsulated as a packet directed to the gateway (A3), the packet is expressed as "A1 -> A3". Note that the source address of this packet is the host address A1 because of encapsulation.
(3) This packet arrives at the gateway (A3). Then after decapsulation and decryption, it is restored to "A1' -> A2".
(4) This packet is changed into a packet "X1 -> X2" by the Twice-NAT in Ex-GW of Enterprise A.
(5) On the route towards the destination address X2, this packet is delivered inside the Ex-Net, and reaches Ex-GW of Enterprise B, and is then changed into "B1 -> B2' " by the Twice-NAT of the gateway. Note that the destination address becomes the interface address B2' of the tunnel for the encrypted communication.
(6) This packet is encrypted and encapsulated as "B4 -> B2" when it goes through the VPN tunnel established between the Ex-GW and Host B2.
(7) Finally, this packet arrives at Host B2. After decapsulation and decryption, the Host B2 receives the packet from Host A1 as "B1 -> B2' ".

3.4 Utilizing DNS and Dynamic Address Assignment

If the Twice-NAT has a DNS-application-level-gateway function shown in [8], it is then possible to make an inquiry of DNS across borders of different address-realms.

In our proposal, each site reserves a set of private addresses to distinguish every host in the partner networks, and registers them as NAT rules for Ex-GW. However, it is possible that most of the private addresses are already in use by the hosts inside. Although it is difficult to reserve additional private addresses for partner hosts under such circumstance, by registering address to NAT rules dynamically according to the DNS query, it is possible to communicate with many partners with only a few reserved private addresses. This is shown in [9] in more detail.

If it is not necessary to distinguish each host accessing from outside of a user site, all unregistered external hosts can be assigned a same address by NAPT (Network Address and Port Translator) on the inbound NAT of the Twice-NAT. Access control according to the user authentication can still be performed because it is performed in the address-realm of Ex-Net.

4 Reasons for using the VPN-Exchange System

Twice-NAT comes in handy when there are address-overlapping problems in communications across different address-realms. However, end-to-end encryption is difficult to perform with the conventional VPN solutions since encrypted packets cannot traverse a NAT. The VPN-Exchange System gives us a clear technical advantage: NAT can be performed on decrypted packets since packets are decrypted at the relay point.

Other than the VPN-Exchange System, the VPN system described in [9] and [10] allows encrypted packets of transport-mode IPsec to traverse a NAT. By using Twice-NAT and Ex-Net as described in this paper, it is possible to deploy an end-to-end VPN without global addresses (Fig.5). However, interconnectivity can be lost because this proposal requires the special VPN systems on the end-hosts. Because the conversion of an encrypted payload is technically impossible, some protocols (such as FTP) that require payload conversion in addition to header translation would make address translation difficult. Furthermore, this VPN system also has the various problems with the conventional end-to-end VPN shown in Table 1.

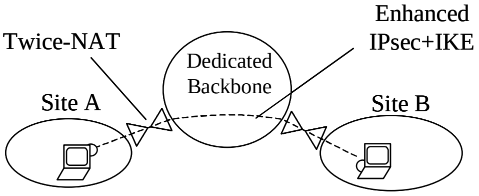

Fig.5 Alternative method of end-to-end-VPN without global addresses

5 Future Work and Conclusion

5.1 Using the Internet

Our current proposal is to be deployed on a dedicated backbone network (Ex-Net). However, because most enterprises are connected to the Internet, we should consider bridging the Ex-Net to the Internet. The relevant subjects to be studied are:

(1) Connection between Ex-Net and a customer network on the Internet
(2) Remote access to Ex-GW from a host on the Internet

(3) Remote access to Ex-GW from a host with a private address in a corporate network on the Internet.

5.2 Migration to IPv6

Although users can be distinguished in Ex-Net by private addresses using our proposal, private addresses themselves are limited, too (about 18 million). Therefore, the scalability is limited by the size of the private address space. Eventually, we will still need the enormous address space that IPv6 can offer. Therefore we should consider supporting IPv6 in the Ex-Net. Some possible solutions include the use of V4-V6 translator (SIIT [11] and NAT-PT [12]) instead of the Twice-NAT. This method does not require any change to the user network, so end user will not be aware of the Ex-Net's migration to IPv6.

Moreover, since end users will eventually use IPv6 directly, we should fully support IPv6.

Using both IPv6-supported Ex-GW and v4-v6-translator-supported Ex-GW will make it possible to relay end-to-end-VPN between IPv6 user and IPv4 user without an IPv4 global address (Fig. 6). Therefore, we believe that this VPN-Exchange System can be effectively deployed in networks where IPv4 and IPv6 co-exist.

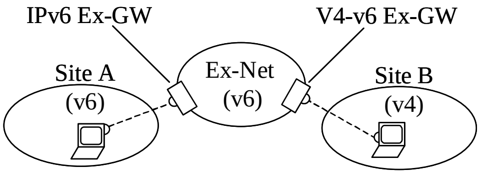

Fig.6 Extranet across
IPv4 and IPv6 Environment

5.3 Conclusion

This paper proposes a mechanism of deploying user-based extranet by establishing end-to-end VPN without global addresses. This proposal is useful for networks where IPv4 is deployed. Using this mechanism, network service providers are able to offer a new network service to their customers.

References

[1] "2001 Computer Crime and Security Survey", CSI and FBI, 2001.

[2] Okada and Fuji, "VPN-exchange: A Network Service Providing User-based VPN" (In Japanese), Computer Security Symposium 2001 (CSS2001), Morioka, Japan, pp.67-72, 2001.

[3] Okada and Fuji, "Achieving High Scalability in VPN-exchange, a Method of Constructing Star-type End-to-end VPN" (In Japanese), the 16th Meeting of Computer Security Group (CSEC-16), Information Processing Society of Japan, 2002.

[4] Dukes et al, "The ISAKMP Configuration Method", draft-dukes-ike-mode-cfg- 02.txt, 2001.

[5] Fergunson et al, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Address Spoofing", RFC2267, 1998.

[6] Srisuresh et al, "IP Network Address Translator (NAT) Terminology and Considerations", RFC2663, 1999.

[7] Aboba, "IPsec-NAT Compatibility Requirements", draft-ietf- ipsec-nat-reqts-01.txt, 2002.

[8] Srisuresh et al, "DNS extensions to Network Address Translators (DNS_ALG)", RFC2694, 1999.

[9] Huttunen et al, "UDP Encapsulation of IPsec Packets", draft-ietf-ipsec-udp-encaps-02, 2002.

[10] Kivinen et al, "Negotiation of NAT-Traversal in the IKE", draft-ietf-ipsec-nat-t-ike-02, 2002.

[11] Nordmark, "Stateless IP/ICMP Translator (SIIT)", RFC2765, 2000.

[12] Tsirtsis et al, "Network Address Translation - Protocol Translation (NAT-PT)", RFC2766, 2000.