가상사설망에서 터널링의 확장성과 모바일 클라이언트 지원

김영진* 이주연* 송주석*

*연세대학교, 컴퓨터과학 · 산업시스템공학과

Supporting Scalability of Tunneling and Mobile Clients in Virtual Private Network

Young-Jin Kim* Joo-Yeon Lee* Joo-Seok Song*

*Department of Computer Science and Industrial System Engineering Yonsei Univ.

요 약

VPN(Virtual Private Networks)을 적절히 설계하기 위한 필요조건은 확장성, 효율성, 신뢰성, 관리의 용이성, 상호운용성과 보안이다. 이러한 요구사항들을 지원하기 위한 중요한 기술이 tunneling 이 될 것이다. 본 논문에서는 현재 주로 사용되고 있는 VPN tunneling 기술에 대해 조사하고 VPN에서 문제시되는 확장성과 Mobile VPN 환경에서 Mobile Station 의 자원제한을 고려한 VPN 서비스 모델을 제안한다.

ABSTRACT

Requirements of a well-designed VPNs(Virtual Private Networks) are scalability, performance, reliability, ease of management, interoperability and security. Tunneling is a important technology to support these. This paper researches VPNs tunneling technologies used currently and proposes VPN service models for the scalability that is a problem in VPNs and for the resource limit of Mobile Station in Mobile VPNs environment.

I. Introduction

Building enterprise-class security goes far beyond antivirus protection, firewalls and VPN, yet many organizations are still struggling with the last element in this triad. Many companies implement VPNs because the alternative - private networks based on leased lines - would be the kind of recurring cost that companies want to avoid in today's difficult business climate.

VPNs use the power of the Internet to reduce networking costs and staffing requirements. It is the newest kind of outsourcing. Instead of using private lines or frame-relay links, a corporate VPN is effectively outsourced to Internet service providers

This paper researches VPNs tunneling technologies used currently and proposes VPNs service models for the scalability that is a problem in VPNs and for the resource limit of Mobile Station in Mobile VPNs environment.

II. Definition

- VPN : A secure connection between two segments of a network, with one end being your office's network gateway (an entrance to the network, such as a router), and the other end being your PC or a gateway to another network, say, in a remote office. Those two segments connect over a public network, usually the Internet. A VPN requires two technologies to create such a secure connection: tunneling and encryption.

- CE-based VPN : An approach in which (ignoring management systems) knowledge of the customer network is limited to customer premise equipment[1].

- PE-Based VPN : The customer network is supported by tunnels which are set up between PE devices. The tunnels may make use of various encapsulations to sent traffic over the SP network (such as, but not restricted to, MPLS, GRE, IPsec, or IP-in-IP tunnels) [1].

- Provider Provisioned VPNs (PPVPNs) : VPNs, whether CE-based or PE-based, that are actively managed by the SP and not the end customer[1].

Ⅲ. Requrements

- Traffic Types

PPVPN services must support unicast traffic and should support multicast traffic.

- Topology

A PPVPN should support multiple VPNs per customer site.

- User data security

PPVPN solutions that support user data security should use standard methods (e.g., IPsec) to achieve confidentiality, integrity, authentication and replay attack prevention.

- Access control

A PPVPN solution may also have the ability to activate the appropriate filtering capabilities upon request of a customer

- QoS

Ⅳ. Type of VPNs

The several types of VPNs correspond to the various networking layers : data link, network, transport, and application. The most common VPN in use provides secure dial-up (datalink) access [2].

1. MPLS (Multiprotocol Label Switching)

MPLS VPNs allow service providers to deploy scalable VPNs and build the foundation to deliver value-added services, including: [3]

- Connectionless Service - A significant technical advantage of MPLS VPNs is that they are connectionless. The Internet owes its success to its basic technology, TCP/IP. TCP/IP is built on packet-based, connectionless network paradigm. This means that no prior action is necessary to establish communication between hosts, making it easy for two parties to communicate.

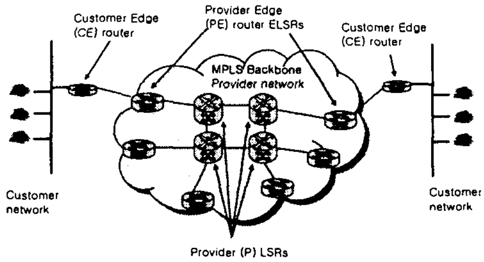
Customer Edge (CE) router
Provider Edge (PE) router ELSRs
Customer Edge (CE) router
MPLS Backbone Provider network
Customer network
Customer network
Provider (P) LSRs

Figure 1: MPLS VPN Terminology RFC 2547

- Centralized Service - Building VPNs in Layer 3 allows delivery of targeted services to a group of users represented by a VPN. A VPN must give service providers more than a mechanism for privately connecting users to intranet services.

Because MPLS VPNs are seen as private intranets, you may use new IP services such as:

- multicast

- QoS(Quality of Service)

- telephony support within a VPN

- centralized services including content and web hosting to a VPN

- Scalability -If you create a VPN using connection-oriented, point-to-point overlays, Frame Relay, or ATM VCs(Virtual Connections), the VPN's key deficiency is scalability. Specifically, connection-oriented VPNs without fully meshed connections between customer sites, are not optimal.

- Security - MPLS VPNs offer the same level of security as connection-oriented VPNs. Packets from one VPN do not inadvertently go to another VPN.

2. IPsec

IPsec evolved from the IPv6 movement and is promoted as a standard by the IETF. It is located in OSI-layer 3. IPsec is a broad-based open solution for encryption and authentication on a per-packet basis. IPsec can securely encapsulate IPv4 packets and tunnel them from one firewall to another. Thus it is an optimum solution for trusted LAN-to-LAN VPNs. IPsec can ensure authentication, privacy and data integrity. It is open to a wide variety of encryption mechanisms. IPsec is application transparent and a natural IP extension, thus ensuring interoperability among VPNs over the Internet. Router vendors and VPN hardware vendors support IPsec. Commercial implementations start to be introduced to the market in 1998 [4].

3. GRE (Generic Routing Emcapsulation)

It is a general encapsualtion protocol which was proposed aiming at some specific encapsulation schemes such as IPX encapsulated within IP, X.25 encapsulated within IP and so on. In this protocol, the encapsulating and encapsulated protocols both can be any network protocols. The general encapsulation form of GRE is (protocol Y(GRE(protocol X))) and when the encapsualting protocol is IP, its encapsulation form is (IP(GRE(protocol X))). GRE is used widely in various environments such as mobile IP, PPTP etc [5].

4. Point-to-Point Tunneling Protocol(PPTP)

PPTP, developed by a consortium of venders(Microsoft, Ascend, 3Com, ECI Telematics, and Copper Mountain Networks), is currently defined RFC 2637. Its purpose is to specify a protocol that encapsulates PPP packets inside an IP packet. PPTP can be broken down into two different components: the transport, which makes the virtual connection, and the encryption, which makes it private.

PPTP uses an extended version of GRE to transport PPP packets, allowing for low-level congestion and flow control. PPTP gets its multiprotocol support from PPP and GRE. It is easy to see where you can get confused on this issue, because the GRE protocol has multiprotocol support. However, GRE is only the transport used by PPTP to tunnel the packets to the VPN terminator.

As with any voluntary VPN, only two components exist: the VPN user, which is also the VPN initiator, and the VPN server [6].

V. Scalability of VPNs

1. Tunnel of IPsec

The concept of a SA(Security Association) IPsec is central to IPsec. The source IP address is not used to define an SA. This is because an SA is a security services agreement between two hosts or gateways for data sent in one direction. As a result, if two peers need to exchange information in both directions using IPsec, two SAs are required : one for each direction [7].

Although hosts(or gateways) have the same level of security or belong to reliable groups each other, different SAs are created in accordance with destination IP address , security protocol identifier and SPI(Security Parameter Index).

The more nodes are given to VPN, the more SAs to be manged will increase. It influences scalability and performance of IPsec.

SAs can be shared, classifying Several VPN networks(or hosts) according to security level. This method has an good effect on restraint of SAs creation, because SAD(Security Association Database) is managed efficiently.

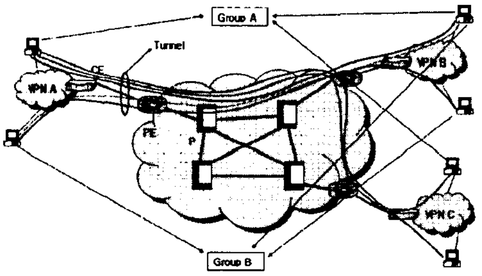

Figure 2: Sharing SAs in IPsec

2. Nomadic users environment

Nomadic users are wanderers, people on the move from place to place. The goal is to make information services and applications ubiquitous and flexibly available for such individuals as well as to small groups of them. Key requirements are the a) rapid service adaptation and customization and b) security.

Mobility places many demands on a system. Size and weight constraints limit the computing resources on a mobile client. Battery life is a nagging concern.

In spite of these challenges, mobile users need to access and update information at any time and from any place.

Authentication, encryption and decryption are not processed in Mobile Station but in Security

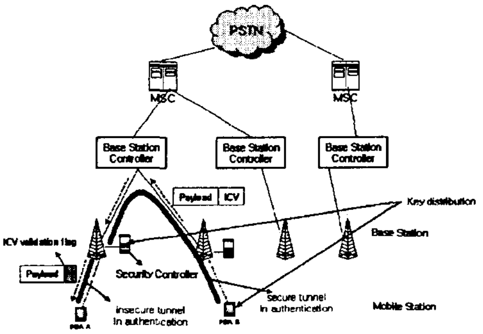

Figure 3: Supporting mobile clients

Controller. Mobile Station is related only to communication and Security Controller is charged with security processes. Therefore mobile clients do not have to acquire overall knowledge of security and the amount of work done is also reduced.

In case Mobile Station processes authentication directly, sender's Mobile Station transfers data and ICV(Integrity Check Value) to receiver's one. The receiver's Base Station validates integrity after calculating ICV. If the data is modified, the receiver's Base Station informs the sender of the result. If the data is normal, it transfers the data and the flag that proves ICV validation to receiver's Mobile Station. In this method, Authentication can be trusted between sender's Mobile Station and receiver's Base Station. The use of the resource of receiver's Mobile Station is also reduced.

Ⅵ. Conclusion

When SA is shared in IPsec, it must be considered that the addition of the classification of security and the module which manages reliable groups among its members. It should be added the process of recreating SA parameters and of correctly redistributing them to members in the group when the event is occurred such as change or deletion of member. So these functions must be resided on PE routers.

In Mobile VPN, the problem of IPsec is that IPsec adds extra and unnecessary overhead to packets that are short and it is very strict in the use of its services and modes, which makes it difficult to be optimized for Mobile IP. IPsec is also not optimized for wireless case, where the number of packets should be kept as low as possible. Because traditional IKE(Internet Key Exchange) protocol is complex and has repeatedly-worked part, there are many problems which should be solved such as increasing of the amount of computation.

It should be considered the problem of key distribution between Mobile Station and Base Station, when authentication and encryption/decryption are processed in Security Controller not in Mobile Station. And Base Station needs a processing to manage and maintain the key which is used to communicate securely with Mobile Station. Also it should be considered that there is a interval where authentication was not guaranteed, when it is processed between Base Station and Mobile Station.

MPLS technology comes into the spotlight to current VPN service providers. MPLS VPNs provide not only more excellent scalability and cost-effectiveness than traditional IPsec VPNs but also additional services easily such as voice, video service including data when VPN is implemented with MPLS traffic engineering, QoS.

However MPLS VPN service providers assume that MPLS core is secure. Also the traffic between CE and PE router is not protected. In an MPLS VPN, privacy doesn't come from encapsulation or encryption. In fact, there is no encryption at all. Privacy comes from segregating packets based on their MPLS labels. Traffic for a particular label is read only by the LSRs(Label Switch Routers) along that LSP(Label Switch Path).

In the future study, the architecture should be researched that minimizes complexity and the amount of computation of IPsec in implement Mobile VPN and advances security keeping scalability without combination of IPsec in implement of MPLS VPN.

References

[1] R. Callon (Ed.), "A Framework for Layer 3 Provider Provisioned Virtual Private Networks", <draft-ietf-ppvpn-framework-05.txt>, April 2002

[2] William Yurcik and David Doss, "A Planning Framework for Implementing Virtual Private Networks", IEEE IT Pro, pp. 41-44, May|June 2001.

[3]http://www.cisco.com/univercd/cc/td/doc/pro

duct/software/ios120/120newft/120t/120t5/vpn.htm

[4] Manuel Gunter, "Virtual Private Networks over the Internet", August 1998

[5] Zhao Aqun, Yuan Yuan, Ji Yi, Gu Guangqun,"Research on tunneling techniques in virtual private networks", IEEE, pp. 691-697, 2000

[6] Adam Quiggle, "Implementing Cisco VPNs", Osborne McGraw-Hil, pp. 365-366, Feb. 2001

[7] Yuan, Ruixi/ Strayer, W. Timothy, "Virtual Private Networks", Addison-Wesley, 2001

[8] Stamatis Karnouskos, "Supporting Nomadic Users within Virtual Private Networks", Proceedings of GLOBECOM Workshop on Service Portability, San Francisco, U.S.A. Dec. 2000

[9] Vesselin Tzvetkov Erika Sanchez Sheffield University, "Mobile Virtual Private Network", Mobile IP Working Group Internet Draft, 15 Sep. 2000

[10]http://www.datanet.co.kr/search/search_view.html?cd=1752&cate=trend&kw=mpls

[11]http://www-2.cs.cmu.edu/afs/cs/project/coda-www/ResearchWebPages/index.html

[12] Elsevier Science Ltd, "Information Security Technical Report", vol. 6, no. 1, 2001