가설사설망 환경에서의 네트워크 보안 설계

김정태* · 류대현

목원대학교 · 한세대학교

Network Security Design for Information Security based on Virtual Private Network Environments

Jung-Tae Kim* · Dae-hyun Ryu

Mokwon University, Hansei University

E-mail : jtkim3050@mokwon.ac.kr

요 약

무선 통신망의 경우 기존의 유선망에 비해, 설치, 이동성 등이 우수하여 많은 기술적인 발전을 보이고 있다. 본 논문에서는 인터넷망에서 사용될 수 있는 가설 사설망 환경에서의 신뢰성을 가질 수 있는 네트워크의 구조에 대해 설명하였다. 또한, 안전한 네트워크의 가설사설망의 실현에 대해 제안하였다.

ABSTRACT

This paper describes an architecture how QoS-enabled virtual private network networks over the internet can be built and managed. The basic technologies for secure VPNs and for Qos support the introduced. Vision of a QoS-enabled VPN service over internet is described. We also presented the simplified implementation scenario and some implementation details in order to achieve secure and QoS-enable VPNs.

Key words

VPN, Virtual private network, Security

I. Introduction

A VPN is a communications environment in which access is controlled to permit peer connections only within a defined community of interested and is constructed through some form of partitioning of a common underlying communications medium, where this underlying communications medium provides to the network on a non-exclusive basis. Ferguson and Huston also provided a simpler, more approximate, and much less formal description. A VPN is a private network constructed within a public network infrastructure, such as the global internet. We want to focus on the case where the public network is the internet. For this case the above definitions are missing on key concept namely tunneling. VPN solutions, more often than not, set up tunnels to treat the internet as one hop between two friendly parties. The endpoints of a tunnel encapsulate a data packet into another one. Tunneling is a powerful technique used in many different are A to route packets of one protocol through a network using another one for mobile IP. Here is a compilation of the properties of the VPNs we want to focus on:

- The VPN uses the internet as a public communications infrastructure
- The VPN ensures privacy at the network layer. This means privacy is ensured per packet. The technical way to do so is by encapsulating IP packets and using cryptographic mechanism to authenticate and encrypt the contents.

- In contrast to current VPN implementations the propose method will support quality-of-service, thus eliminating the only real disadvantage of VPNs compared to real private networks using leased lines.

II. VPN Technology

IPSec evolved from the IPv6 development and is short of being finalized. It is an open architecture for IP-packet encryption and authentication, thus it is located in the network layer. IPSec adds additional headers/tailers ti an IP packet and can encapsulate IP packets in new ones. There are three main functionalities of IPSec separated in three protocols. One is the authentication through an Authentication Header the other is the encryption through an Encapsulating Security Payload and finally automated key management through the internet key exchange protocol. We will refer to these three mechanism as IPSec protocols. IKE is the most complex IPSec protocol and is still under study. Nevertheless, IPSec provides an architecture for key management, encryption, authentication and tunneling. Therefore all of the previously defined VPN business scenarios can be implemented with IPSec.

2.1 Integrated and differentiated services for QoS support

Resource Reservation Setup Protocol(RSVP) is main component of the integrated services architecture which is used to request QoS levels such as controlled load or guaranteed service for individual flows. RSVP operates on thop of IP in the transport layer, it is a control protocol comparable to internet control message protocol or internet gateway message protocol. RSVP alone is not sufficient to provide QoS. RSVP only sets up reservations for network resources, but enforcement of the reservation needs to be done by other components of the mechanism. RSVP provides the following features.

- Receiver orientation
- Simplex reservations
- Soft state
- Tunnels of non-RSVP clouds
- Unicast and Multicast support
- RSVP relies on underlying routing mechanism.

2.2 Interoperability between and Integrated Service and Differentiated services

Integrated Service and Differentiated services are approaches complementary to each other. Therefore, it is advisable to combine both of them. According to V.Bernet, the three alternatives for interoperability between Integrated Service and Differentiated services are as follow.

- Integrated Service over Differentiated services
- Aggregated Integrated Service states
- Parallel Operation

2.3 Basic model of Integrated Service over Differentiated services

In the basic model Differentiated services is used to allocate the network bandwidth in support of the Integrated Service networks which use RSVP end-to-end signaling. Figure 1 shows a network configuration where sub networks serve as customers of transit networks. The entire network consists of two Integrated Service capable sub networks which are interconnected by one large Differentiated services capable transit network. In this model, end systems in the sub network use RSVP as a signaling protocol to request a specific QoS, while Differentiated services is used in the transit network to support QoS with better scalability.

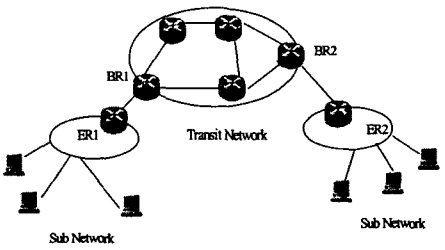

Fig. 1 Topology of a transmit network

The Integrated Service over Differentiated services consists of the following elements.

- Hosts

The hosts use RSVP signaling to request a specific QoS level. Some hosts are also able to provide traffic control functions.

- Edge routers(ER)

These routers consist of two parts, one part is RSVP capable and interacts with the intserv network and the other is diffserv capable and interacts with the diffserv admission control component to provide admission control feedback to the hosts generated RSVP signaling.

- Boundary routers(BR)

These routers provide traffic conditioning functions to ensure that the traffic conforms to the service level agreement

- Sub networks

The sub networks contain intserv capable hosts and a mesh of leaf router which are not explicity required to be intserv capable.

- Transit network

The transit network can provide different QoS levels by applying appropriate per-hop-behaviors.

III. QoS Enabled VPN Mechanism

A major competitor of IP-VPNs are private leased line(frame relay, ISDN). While the leased lines are more expensive because the user has to pay even when not using the line, the usually come with guaranteed QoS. Enhancing todays VPN solutions with QoS will eliminate the VPNs only real disadvantage compared to the leased line solutions. External Differentiated services seems to be the technology that is simple enough to enhance VPNs without restricting the global reachability of the internet. Another problem of VPNs is the relative high expertise necessary for managing a VPN. Mismanagement leads either to loss of privacy or loss of connectivity. An Internet service provider(ISP) has control over a part of the internet. Using emerging technologies it can offer QoS guarantees. It has the expertise and the financial resources to build up a VPN service, as well. Furthermore, in order to service its customers and to lower costs the ISP must try to automate as much of its services as possible. Currently, the most promising technologies for such a service bundle are Differentiated services and IPSec. In order for these technologies to work together it must be assured, that the tunnel endpoints and the ISP ingrwss nodes are located in the same machines. Else, the tunneling and encryption of the VPN and Differentiated service may hide information necessary for Differentiated services. But given that an ISP provides the VPN and Differentiated service together, it can place the tunnel endpoints accordingly. Although Differentiated services and VPNs are two different services, they have similar concepts and can enhance each other:

- Differentiated services provide QoS commitments for a VPN as a whole or it can be used to differentiated the treatment of traffic classes within a VPN.

- VPNs are traffic aggregations with known traffic destination points. Differentiated services also operate on traffic aggregations. The known destination points can furthermore ease the specification of necessary service levlel agreements.

- Differentiated services and VPNs both need enhanced functionality of border routers of the ISP but not of intermediate routers. Both share some similar functionality in the border router, the traffic classification.

- The simplicity and the coarse grained traffic classification make Differentiated services a scalable technology. Differentiated services is therefore suitable for the QoS support between different ISPs. On the other hand, a VPN tunnel that crosses intermediate ISPs is transparent to them and therefore does not allow fine grained QoS support.

IV. Security Issues

The higher we climb in the component hierarchy the more critical is the security of a component. A corrupt CD can only directly impact one machine. Once the corruption is detected, the reestablishment of correct service can be done relatively quickly. A corrupt ISB will affect the whole ISB network. A corrupt ESB will also directly affect neighbor ESBs. This case represents an extreme high threat potential, since the ESBs have the authority to handle payments automatically. The more intelligence a component has the higher is collation with other ISPs. It is difficult to reestablish correct service handing in that case.

While the interactions between components of the same ISP can be secured in a more statical manner with local key management, the ESB-ESB interaction needs to be secured using a trusted third party and public key cryptography. From what we said above we can draw the following conclusions:

- Not all components need the same levle of protection. ESB must be protected using the highest level of security available. The

interactions could be secured with an encryption algorithm allowing for long keys. The key material must be refreshed automatically and in short terms.

- ESB-ISP interactions need also strong protection mechanism but shorter keys with frequent key refreshment can suffice
- ISP-CD interactions need protection but shorter keys and a less frequent key refreshment can suffice.
- CD-network equipment interactions may be protected using a dedicated cable or application layer security such as secret shells

V. Implementation

This paper describes the implementation scenario derived from the general scenario described. It discusses which configuration steps a configuration setup has to trigger for the demonstrator of a QoS enabled VPN service. We presents examples for the establishment of VPN tunnels and for hardware based QoS support. The establishment module of CD establishes secure tunnels between two peers. Any tunneling mechanism can be used in architecture, but we will assume that IPSec will be used in most cases since this the recommended mechanism by IETF. Using IPSec implementation, traffic between two peers is protected by configuring access lists and enabling the access lists to interfaces by crypto map sets. Traffic selection can be based on source and destination address. Crypto access lists are used to define which IP traffic will be protected by crpyto and which traffic will not be protected by crypto. For example, access lists can be created to protect all IP traffic between subnet A and subnet Y or telnet between host A and Host B. Crypo map sets are accumulation of crypto map entries in a group. When crypto map sets are applied ti interfaces then all IP traffic passing through the interface is evaluated against the applied crypto map set. If a static map entry sees outbound IP traffic that should be protected and the crypto map specifies the use of IKE, a security association is negotiated with the remote peer according to the parameters include in the crypto map entry.

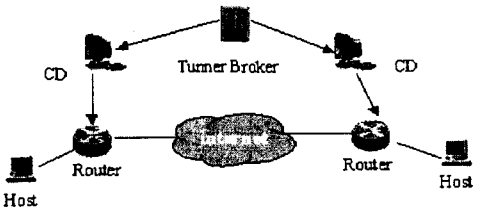

Fig. 2 Setup of Tunnelling

VI. Conclusion

This paper described an architecture that allows to implement QoS-enabled VPNs. The architecture is based on an generalization of the bandwidth broker concept introduced in the Differentiated services environment. The architecture framework includes service broker hierarchy that allows for automated service configuration. An instantiation of the frame allows a user to set up, change, and modified VPNs including parameters such as security and QoS related parameters.

References

[1] St. Kent, R. Atkinson: Security Architecture for the Internet Protocol, November, 1998

[2] Cisco System: Cisco Service Management System,

[3] B, Bchneir, Applied Cryptography, 2nd edition, John Wiley&Sons, 1996

[4] R. Yavatkar et al, "SBM: A protocol for RSVP-based admission control over IEEE 802-style networks," RFC2814, May 2000