IPSec 기반 환경하에서 QoS 보장 가상 사설망 구현 방안 연구

김정훈* · 여현*

*순천대학교

A Study of Virtual Private Network On based Environment IP Security Simulations Quality of Service Guarantee

jeonghun kim* · hyun Yoe*

*Sunchon University

E-mail : yoehyun@dreamwiz.com

요 약

현재의 인터넷은 Best-Effort 서비스만을 지원한다. 그러나 지난 몇 년 동안 인터넷 환경의 지속적인 발전으로 인해 Best-Effort 서비스의 한계를 넘어선 새로운 형태의 Application들이 등장하게 되었고, 이러한 Application들은 end-to-end간에 QoS(Quality of Services)보장 및 보안을 요구한다.
본 논문에서는 IETF에서 제안한 QoS 보장 기술중 하나인 Differentiated Services를 이용하여 end-to-end 간의 QoS보장 및 IP Securtiy 적용한 가상사설망(VPN) 구현방안에 관해 연구하였다.

ABSTRACT

Today Internet is only Best-Effort service. During the past few years, new types of internet applications which require performance beyond the best-effort service that is provided by the current internet have emerged. These applications required QoS(Quality of Services) guarantee and Security between end-to-end. In this paper simulations Differentiated Services that IETF(Internet Engineering Task Force) has proposed one of QoS(Quality of Services) guarantee VPN(Virtual Private Network) using QoS(Quality of Services) guarantee and IP Security between end-to-end.

키워드

Virtual Private Network, Differentiated Services, IP Security

Ⅰ.서론

VPN(Virtual Private Network)은 기존은 사설망(Private Network)과 공중망(Public Network)의 중간 형태로서 이 두 망의 단점을 해소하고 장점을 활용하는데서 비롯됐다. 하지만 기업이나 공공기관 내부의 여러 가지 형태의 데이터가 존재하게된다. 따라서 다양한 형태의 VPN이 구성되어져야한다. 이러한 이유로 최근 다양한 형태의 VPN 대한 연구 및 개발이 활발히 이루어 지고 있다. 현재 표준으로 지정된 인터넷 기반의 VPN 기술은 Internet Protocol Security(IPSec) 표준이 있다. 이미 표준을 기반으로한 IP Sercurity VPN 제품이 출시되고있고, 이러한 제품들에 특징은 VPN의 취약한 보안문제 및 신뢰성 문제를 해결했다는 것이다. 하지만 최근에 멀티미디어 관련 응용프로그램(비디오-컨퍼런싱, VOD, etc)들 중 특히 실시간 관련 응용프로그램들은 고정된 대여폭을 요구함에 따라 VPN에서도 QoS문제를 고려하지 않을 수 없게됐다. 따라서 본 논문에서는 이러한 IP Security VPN에서의 QoS문제를 해결하기 위한 방안으로 Differentiated Services 적용한 VPN을 설계하였다.

II. VPN(Virtual Private Network)

VPN은 크게 다음과 같은 범위의 카테고리로 구분할 수 있다.

-. Intranet VPN
-. Remote VPN
-. Extranet VPN

2.1. 구성 범위에 따른 분류

▷ Intranet VPN - 인트라넷 VPN은 가장 단순한 형태의 VPN으로 기업내부의 부서를 모두 LAN으로 연결하고 , 지사들의 경우는 가까운 ISP까지만 접속한 후 인터넷망을 이용하여 물리적으로 떨어진 본사와 상호 연결하는 형태다.

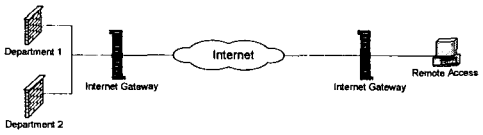

그림 2-1. Intranet VPN

▷ Remote VPN - 본사와 원격지간 이동 사용자의 연결을 지원하는 형태이다.

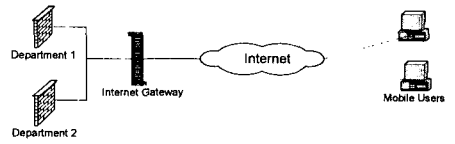

그림 2-2. Remote VPN

▷ Extranet VPN - 본사와 전략적인 파트너, 고객사 등을 연결하는 익스트라넷 VPN은 비즈니스 파트너들이 제공하는 다양한 솔루션들이 호환되어야 하기 때문에, 호환이 보장되는 정보 처리 상호 운용 표준에 적합한 지의 여부를 확인하는 작업이 요구된다.

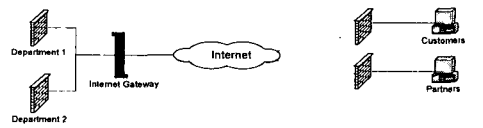

그림 2-3. Extranet VPN

▷ 통합 VPN - 인트라넷 VPN, 리모트 VPN, 익스트라넷 VPN의 3가지 형태를 통합한 VPN은 그림4와 같이 구성된다. 이 통합망은 기업의 업무 형태에 따라 네트워크 사용에 관한 모든 경우의 수를 포함하는 형태로서 내부 이용자, 외부 이용자 및 모바일 사용자까지 연결할 수 있는 폭넓은 망이다. 이렇게 구성되는 VPN은 각기 다른 형태의 VPN 구성으로 인해 발생하는 요구 부분이 모두 해결돼야한다.

III. IPsec

IPsec은 인터넷에서 필수적인 암호화와 인증 서비스를 구조적으로 제공하면서 안전한 키교환이나 replay 공격등을 방어할 수 있는 메카니즘도 제공하고 있다. IETF IPsec과 IPsp 워킹그룹에서는 패킷 기반의 비연결형 정보보호 서비스를 제공하기 위하여 두 개의 확장 헤더를 정의하였고, 헤더 처리를 위한 키교환 및 인증 프로토콜, 정보보호 정책기술, 그리고 정보보호 서비스 관리를 위한 MIB들을 정의하였다.

현재 IPsec은 VPN(Virtual Private Network)가장 활발하게 적용되고 있고, IPsec을 엔터프라이즈 네트워크에 적용 시 확장성 및 호환성을 해결할 수 있는 유일한 정보보호 프로토콜로 여기고 있다.

IV. Diffserv

인터넷에 VoIP, 사설가상망(VPN)과 같은 응용서비스들의 등장함에 따라 IP의 QoS 문제가 발생하게 되었다. 그래서 이를 해결하기 위한 방안으로써 DiffServ가 등장하게 되었다.

Diffserv 다음과 같은 요소 기능으로 구성된다.

4.1 트래픽 조절(Traffic Conditioning)

SLA(Service Level Agreement)에 의해 DS망(DiffServ망)의 경계라우터는 내부라우터에서 패킷전달방식을 결정하기 위해 marking을 해야하는데 이러한 것은 traffic-controling이라고 한다. 이 traffic-controling에는 그림4-1에서 보는 것과 같이 트래픽분류(classifier), 측정(meter), 표시(marker), 쉐이핑(shaping), 폐기(drop)의 기능들이 있다. IPv4에서는 ToS(Type of services)의 6bit를 사용하여 서비스의 Class를 구별하게된다.

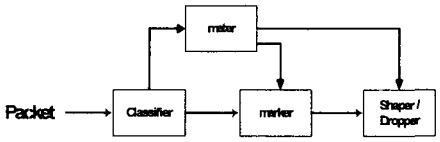

그림 4-1. 트래픽 조절기의 기능과 상호관계

트래픽분류는 DS byte만을 가지고 하는 BA(Behavior Aggregate)분류와 주소필드 등을 함께 고려하는 MF(Multi-Field)분류로 나뉜다. 트래픽 측정기는 라우터를 거쳐가는 패킷을 측정하여 SLA에 의거해 프로필을 준수하는지 위반하는지를 알아보고 다음 기능요소에 전달한다. 트래픽표시기는 특정 패킷전달방식에 해당하는 코드를 DS 바이트에 기록하여 패킷을 트정BA에 속하게 한다. 트래픽 쉐이퍼는 트래픽 폐기와 함께 프로필을 준수하지 않는 트래픽들에 큐를 이용하여 적절한 조취를 취한다.

4.2 PHB(Per-Hop Behavior)

패킷이 DS망의 내부라우터에서 BA형태로 단순하게 전달되기 위해서는 경계라우터에서 어떠한 방식으로 전달될지를 결정하여 DSbyte에 표시하게 된다. IPv4에서는 ToS 영역을 이용하여 다음 그림 5에서와 같이 6bit의 DS 코드포인트[5]로 할당한다. 이 코드포인트를 이용하여 라우터는 각 패킷의 전달순서와 버퍼할당 같은 망 내부의 패킷 전달방식을 결정하는데 이것을 PHB라고 한다.

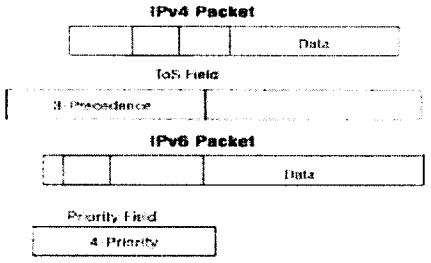

그림 4-2. IPv4 와 IPv6 ToS 필드

DE(Default) PHB는 이러한 PHB중에 디폴트이다. DiffServf를 사용하지 않는 서비스를 위해서 최소한의 자원을 할당해 놓아야 하고, 반드시 수용되어져야 한다. EF(Expedited Forwarding) PHB는 제어 트래픽과 같은 가장 우선 순위가 높은 패킷에 전달방식이다. 이것은 최소한의 손실, 지연, 지연변이를 얻게 하기 위해 입력 큐에 속도의 최대값보다 출력큐에 속도의 최소값을 항상 크게 함으로서 구현할 수 있다. AF(Assured Forwarding) PHB는 패킷을 그림 6에서와 같이 4개의 클래스와 3개의 폐기 우선순위로 구분하여 망의 혼잡상황에서 패킷을 패기하는 순서를 결정한다.

V. DiffServ적용 VPN(IPSec) 설계

기본적인 IPSec VPN은 다음과 같다.

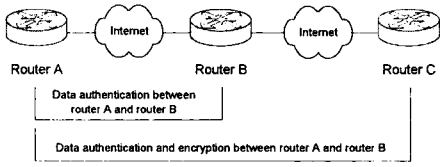

그림 5-1 IP Security VPN

그림에서 라우터 A와 C사이에서 데이터 인증과 암호화가 이루어지는 것을 보여준다.

5.1 DiffServ 지원 Linux router 구현

DiffServ를 지원하기 위해 각각의 라우터들이 DiffServ지원 기능을 가진 하나의 PHB가 된다. 이러한 PHB 기능을 가진 라우터는 Linux router로 구현하였다.

▷ DiffServ + IPSec VPN Linux Router

Router	Setting
Router A	eth0 : 210.110.81.147 eth1 : 210.110.89.20
Router B	eth0 : 210.110.89.21 eth1 : 210.110.89.22
Server	IP address : 210.110.81.145
clinet 1	IP address : 210.110.89.30
client 2	IP address : 210.110.89.31

표 1 Linux router IP table

-. Linux router 간에 IPSec tunnel 설정
-. 논리 인터페이스인 ipsec0는 DiffServ를 지원
-. Max tunnelling rate(IPSec tunnel bandwidth) : ~ 3.2 Mbps

5.2 DiffServ 지원 VPN(IPSec)구현

소스와 목적지 사이에 두 대의 Linux 라우터를 연결하고, 라우터간에는 IPSec 터널링을 하였다.

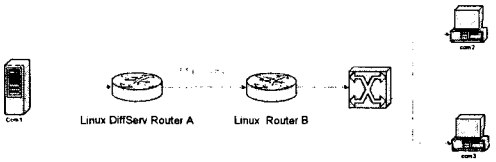

그림 5-2 DiffServ+VPN(IPSec) Router IP tunnelling test

5.3 Test

DiffServ+VPN tunnel 대여폭 테스트는 SnifferPro와 Ping으로 하였다.

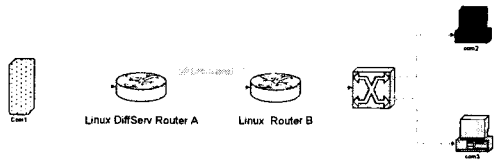

그림 5-3 Com1 -> Com2 IP tunnelling test

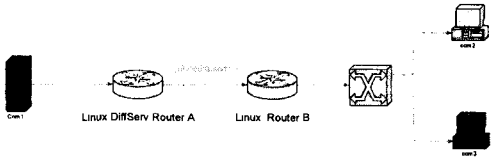

그림 5-4 Com1 -> Com2 IP tunnelling test

5.4 DiffServ 지원 VPN(IPSec) 설계

최근에 IP Security를 이용한 VPN이 제품으로 출시되고 있다. 이러한 모델을 기반으로 DiffServ 지원 VPN(IPSec)을 설계했다.

위의 그림에서 보듯이 기업 가상사설망은 IPSec를 이용하여 구축하고, 백본은 DiffServ 지원 라우터로써 구현함으로써 Enterprise Network에서도 충분히 적용 가능하다.

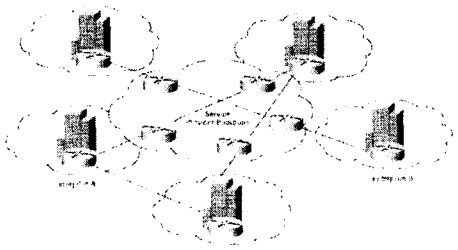

그림 5-5. 통합 DiffServ 지원 VPN(IPSec)

VI. 결론

본 논문에서는 IPsec 기반 가상 사설망에서 다양한 형태의 트래픽에 대한 QoS보장을 위해 Differentiated Services를 적용한 망을 설계하였다. 이러한 망 설계를 통해 VPN 내에서 QoS 보장 및 IP Security 문제를 해결하였다. 그러나 IPSec을 적용함에 있어서 대여폭이 감소하는 문제점이 발생하였다.

향후 연구에서는 대여폭 감소 문제를 해결하기 위해서 스케쥴링 알고리즘에 따른 망 성능 분석 및 가장 효율적인 망 구현을 위한 스케쥴링 알고리즘을 제안할 예정이다.

참고문헌

[1] Spiridon Bakiras and Victor O.K.Li, "Quality of Service Support in Differentiated Services Packet Networks"

[2] S. Blacke, D. Black, M. Carlson, E. Davis, Z. Wang, and W. weiss, "An architecture for differentiated services," *Internet RFC 2475, December 1998*

[3] S. Kent, R Atknson, "Security Architecture for the Internet Protocol", *Internet RFC2401 November 1998*

[4] Paul Ferguson and Geoff Huston, "What is a VPN ?," Cisco, April 1998