Star VPN 구조에서 CPE VPN GW간 직접 터널을 이용한 성능 향상 방안

변해선*, 이미정*, 안상준**
*이화여자대학교 컴퓨터학과
**(주)타오네트웍스
e-mail: {ladybhs, lmj}@ewha.ac.kr, sjahn@taonetworks.com

Approach with direct tunnels between CPE VPN GWs in star VPN topology

Hae-Sun Byun*, Mee-Jeong Lee*, Sang-Joon Ahn**
*Dept of Computer Science & Engineering,
Ewha Womans University
**Taonetworks.com

요 약

현재 운용중인 대부분의 VPN은 모든 CPE(Customer Premise Equipment) VPN GW(Gateway)들이 Center VPN GW에 연결되어 있는 Star 구조를 취하고 있다. 이러한 구조에서는 모든 트래픽들이 항상 Center VPN GW를 거쳐서 전송되므로 비효율적인 트래픽 전송이 이루어진다. 또한 대용량의 멀티미디어 트래픽 전송이 빈번하거나 다수의 지점을 갖고 있는 기업의 경우 Center VPN GW에서의 오버헤드가 증가하게 된다. 이러한 문제를 해결하기 위한 방법으로는 IPSec의 IKE(Internet Key Exchange) 메커니즘을 이용하여 CPE VPN GW간 직접 터널을 맺어 줄 수 있으나, 터널 설립에 앞서 원격지 CPE VPN GW의 주소, 요구되는 보안 등급 등의 터널 설정에 필요한 정보를 관리자가 직접 설정해 주어야 한다. 이는 현재 DHCP와 같은 동적 IP 환경에서 운용되는 ADSL 기반의 VPN 환경에서 관리 오버헤드를 증가시키는 요인이 된다. 이에 본 논문에서는 CPE VPN GW 간 직접 터널 연결이 필요할 시에 자동적으로 제반 기능들이 수행될 수 있게 하는 주문형 터널 생성(On-demand Tunnel Creation) 메커니즘 제안한다. 시뮬레이션을 통해 제안하는 방안에 대하여 성능을 조사하였고, 이와 함께 기존의 Star VPN 구조, Full-mesh VPN 구조와 성능을 비교하였다. 시뮬레이션 결과, 제안하는 방안이 기존의 Star VPN 구조보다 확장성과 트래픽 전송효율성, Center VPN GW의 오버헤드 측면에서 우수한 성능을 보였으며 Full-mesh 구조의 VPN과 거의 비슷한 종단간 지연시간과 처리율을 보였다.

1. 서론

인터넷을 기반으로 하는 기업 활동이 증대됨에 따라 제한된 LAN의 구성에서 벗어나 멀리 떨어진 본·지점 간 네트워크를 구성하기 위해 VPN (Virtual Private Network)을 구축하는 기업이 늘어나고 있다. VPN은 공중망에서의 물리적인 구성과 무관하게 논리적으로 망을 구성하여 특정 사용자 그룹에게 보안을 제공해주는 가상사설망이다. 현재 운용중인 대부분의 VPN은 모든 CPE VPN GW들이 Center VPN GW에 연결되어 있는 Star 구조를 취하고 있다. Star VPN 구조는 CPE VPN GW들이 Center VPN GW와 터널을 유지하므로 확장성이 우수하며 CPE VPN GW의 오버헤드가 적다는 장점을 가지고 있다. 그러나 이 구조에서는 CPE VPN GW에서 발생하는 모든 트래픽들이 항상 Center VPN GW을 거쳐서 전송된다. 이는 트래픽 전송을 비효율적이게 할 뿐 아니라, 대용량의 멀티미디어 서비스의 이용이 많은 기업이나 수많은 지점을 갖고 있는 대규모 기업의 경우 Center VPN GW에서의 오버헤드가 증가하게 된다. 따라서 트래픽의 효율적인 전송과 Center VPN GW의 오버헤드를 줄이기 위해서는 CPE VPN GW간 직접 터널을 설립할 수 있도록 해야 한다. CPE VPN GW간 직접 터널은 IPSec의 IKE(Internet Key Exchange)라는 표준 키 교환 메커니즘을 이용하여 설립되어질 수 있으나, 이러한 방법은 터널 설립 절차를 수행하기 이전에 원격지

VPN GW의 주소, 요구되는 보안 등급과 같은 터널 설정에 필요한 기본적인 정보를 관리자가 직접 설정해 주어야 한다. 특히, 현재 VPN 장비의 근간을 이루는 ADSL 기반의 VPN 장비들은 DHCP(Dynamic Host Configuration Protocol)와 같은 동적 IP 환경에서 운용되므로 장비의 기본 환경설정의 잦은 업데이트가 요구되는데, 관리자가 이러한 정보를 매번 수동으로 입력해야 하는 것은 관리 오버헤드를 증가시키는 요인이 된다. 대규모의 VPN 망을 구성하고자 할 경우 이와 같은 관리 오버헤드는 VPN 운용에 심각한 문제점이 될 수 있으므로 현실적으로 운용되는 망에서는 Center VPN GW를 거치는 기본적인 구성을 그대로 사용하고 있는 실정이다. 따라서 CPE VPN GW 간 터널 설립에 위한 관리적인 측면에서의 오버헤드를 최소화 할 수 있는 지능화(Intelligent) 된 터널 생성 메커니즘이 연구되어야 한다.

이에 본 논문에서는 Star VPN 구조에서 CPE VPN GW간 직접 터널 설립을 위한 주문형 터널 생성(On-demand Tunnel Creation) 메커니즘을 제안한다. 이는 관리자의 수동적인 설정을 거치지 않고 자동적으로 제반 기능들을 수행함으로써 네트워크 관리를 용이하게 한다. 또한 CPE VPN GW간 직접 터널을 설립함으로써 CPE VPN GW에서 발생하는 트래픽들이 Center VPN GW를 거치지 않아도 되므로 Center VPN GW에서의 오버헤드를 줄일 수 있으며 효율적인 트래픽 전송이 이루어진다. 시뮬레이션을 통해 기존의 Star VPN 구조(앞으로 Basic Star VPN이라 명함), Full-mesh VPN 구조와 함께 성능을 조사하였다. 시뮬레이션 결과, 제안하는 방안이 Basic Star VPN 구조보다 확장성, 트래픽 전송 효율성, Center VPN GW의 오버헤드에서 우수한 성능을 보였으며, Full-mesh VPN 구조와 거의 비슷한 종단간 지연시간과 처리율을 보였다.

2. 제안하는 방안

그림 1은 모든 CPE VPN GW들이 Center VPN GW와 연결된 Star VPN 구조의 환경에서 Customer Site 3의 CPE VPN GW와 Customer Site 4의 CPE VPN GW간 직접 터널을 설립한 형태를 보여주고 있다. Center VPN GW는 CPE VPN GW들이 VPN 망 내에서 유기적으로 동작할 수 있도록 해주는 TDS(Tunnel Directory Service) 서버와 연결되어 있다. CPE VPN GW는 상대 CPE VPN GW와 직접 터널의 연결이 필요할 시에 이를 판단하여 TDS 서버에게 터널 설립을 위한 정보를 요구한다.

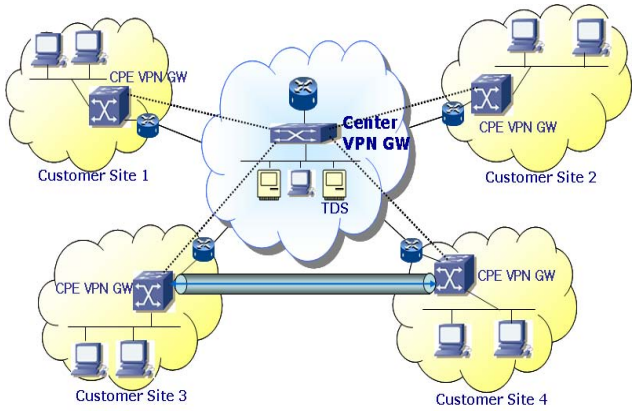

그림 1. Star VPN 구조의 환경에서
CPE VPN GW 간 직접 터널 설립

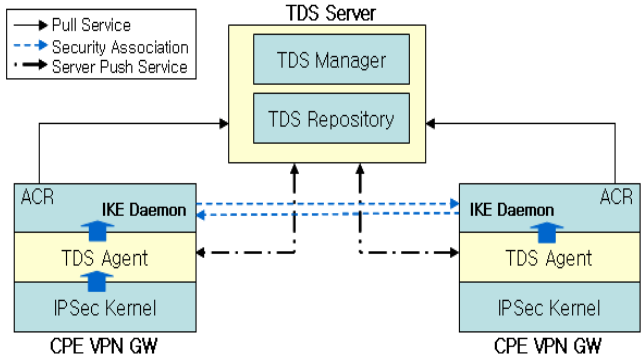

그림 2. CPE VPN GW 간 터널 설립 과정

그림 2는 제안하는 방안에서 사용되는 VPN 시스템의 구성요소들의 CPE VPN GW간 터널 설립을 위한 메시지 전달과정을 보여주고 있다. CPE VPN GW에는 IPSec Kernel 모듈, TDS Agent, ACR(Auto Configuration Registration) 등으로 구성되어 있다. IPSec Kernel은 원격지의 CPE VPN GW에 대하여 직접 터널을 연결할 필요가 있을 때 이를 판단하여 주문형(On-demand) 터널을 생성할 수 있게 한다. 만약 직접 터널이 연결되어 있는 경우에는 해당 터널의 SA(Security Association)를 이용하여 패킷을 전송하고, 직접 터널이 없는 경우에는 Center VPN GW로 패킷을 전송 한 후 TDS Agent로 하여금 직접 터널 연결을 위한 제반 작업을 수행하게 한다. TDS Agent는 IPSec 커널로부터 새로운 터널을 생성하라는 요청을 받았을 때 TDS 서버의 TDS Manager에게 상대 CPE VPN GW와의 터널 설립에 필요한 CPE VPN GW 주소 및 제반 정보에 대한 질의(Query)를 실행한다. TDS

Server의 TDS Manager는 TDS Repository에서 해당 VPN GW의 정보를 찾아 TDS Agent로 전송한다. 이때 전송되는 정보는 상대편 VPN GW의 IP 주소, 서브넷 정보, SA을 맺는데 필요한 부가정보가 전달된다. TDS Agent는 TDS Manager로부터 받은 정보를 이용하여 IKE 메커니즘이 효과적으로 동작할 수 있는 제반 환경을 자율적으로 구성한다. 한편, TDS Manager는 터널을 맺을 상대편 CPE VPN GW에게 Tunnel Notification Message를 보냄으로써 두 개의 CPE VPN GW가 유기적으로 동작할 수 있도록 한다. 정보를 받은 CPE VPN GW은 상대편 CPE VPN GW와 터널을 설립하기 위해 IKE(Internet Key Exchange)를 활성화하고, 두 CPE VPN GW의 IKE 간에 터널 생성에 필요한 자료 교환이 이루어진 후에 터널이 생성된다. ACR은 자신의 IP 주소, 서브넷 주소 등 제반 설정 정보가 변한 것을 감지하게 되면 이를 TDS 서버의 TDS Manager에게 등록하고, TDS Manager는 CPE VPN GW의 ACR 모듈로부터 받은 변경사항을 TDS Repository에 업데이트 한다.

3. 성능평가

제안하는 방안의 성능평가를 위해 캘리포니아 버클리 대학에서 개발된 NS-2를 이용하여 시뮬레이션을 수행하였다. 본 시뮬레이션에서는 CPE VPN GW의 수 변화시켜보면서 확장성, 트래픽 전송에 대한 효율성, Center VPN GW에서의 오버헤드를 측정하였다. 시뮬레이션에서 사용된 네트워크 모델은 그림 3과 같으며, 트래픽 전송은 UDP를 이용한 CBR(Constant Bit Rate)을 가정하였다.

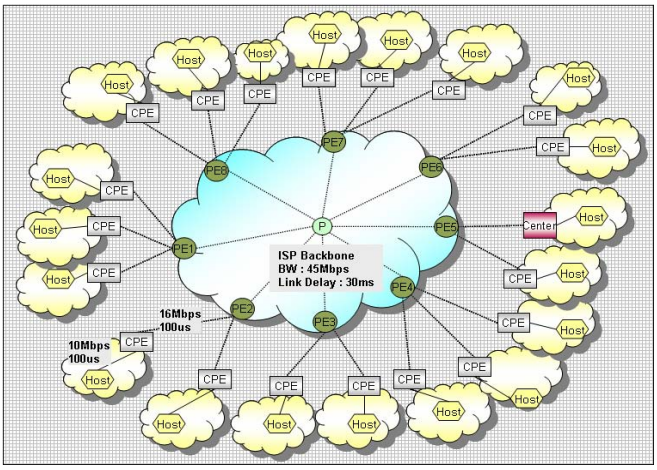

그림 3. 시뮬레이션 토폴로지

실험에서 사용된 CPE VPN GW의 수와 플로우 발생빈도, 패킷 전송률은 표 1과 같다.

표 1. 실험모델

CPE VPN GW의 수(개)	하나의 CPE VPN GW에서의 flow 발생빈도(flow/s)	flow 별 패킷 전송률(Mbps)
5,10,15,20	0.1	0.5 ~ 2

그림 4는 Star VPN 구조에서 Center VPN GW를 지나는 데이터 패킷의 수를 구한 결과이다. Basic Star VPN 방법의 경우 CPE VPN GW의 수가 늘어날수록 Center VPN GW를 지나는 패킷의 수가 크게 증가한다. 이는 Center VPN GW에서의 오버헤드가 증가하게 됨을 의미하며 확장성 측면에서도 고려해야 할 문제가 된다. 제안하는 방안에서는 통신하고자 하는 CPE VPN GW와 직접 터널이 설립된 이후에는 CPE VPN GW에서 발생하는 트래픽 Center VPN GW를 지나지 않으므로 Basic Star VPN보다 Center VPN GW에서의 오버헤드가 훨씬 적다.

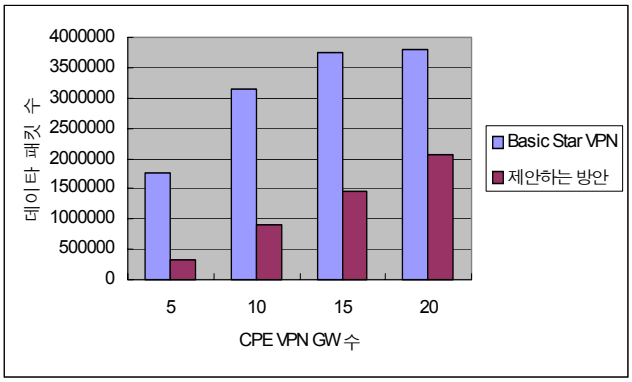

그림 4. Star VPN 구조에서 Center VPN GW를 지나는 데이터 패킷의 수

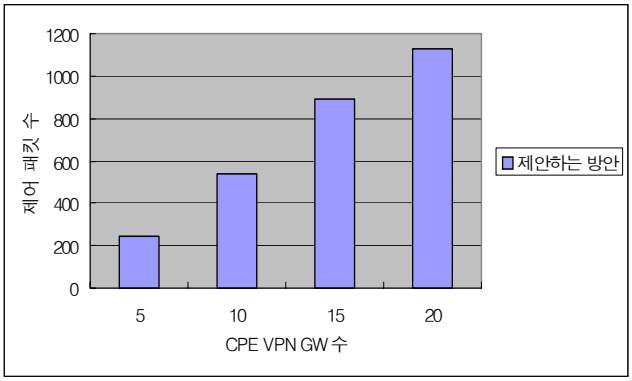

그림 5. CPE VPN GW의 터널설립 요청 메시지의 수

그림 5는 터널 설립을 위하여 CPE VPN GW가 Center VPN GW에게 보낸 시그널링 메시지의 수를 구한 결과이다. Basic Star VPN에서는 VPN 초기구성 시에만 Center VPN GW와 터널정보를 교환하면

되지만 제안하는 방안의 경우 CPE VPN GW간 직접 터널 설립이 필요할 때마다 Center VPN GW에게 터널 설립 정보를 요청한다. 그림 6과 7은 트래픽 전송의 효율성 측정을 위해 종단간 지연시간과 Goodput을 구한 결과이다. Basic Star VPN에서는 트래픽이 항상 Center VPN GW를 거쳐서 목적지 CPE VPN GW에게 전달되기 때문에 종단간 지연시간이 길다. 제안하는 방안이 Full-mesh VPN 구조보다 종단간 지연시간은 길었지만 CPE VPN GW의 수에 관계없이 두 스킴에서의 차이가 0.02ms정도인데 반해 Basic Star VPN과는 0.04ms의 차이를 보였으며 CPE VPN GW의 수가 증가할수록 간격이 더 벌어졌다.

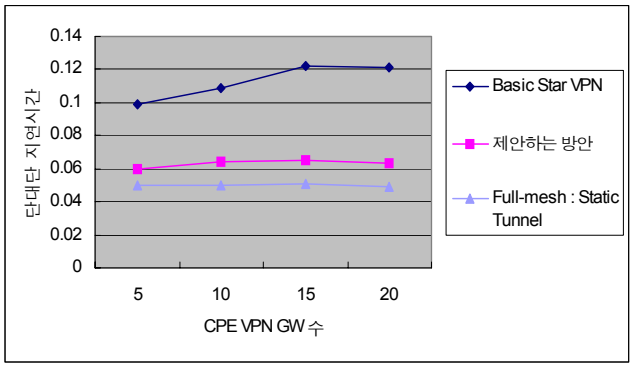

그림 6. End-to-End Delay

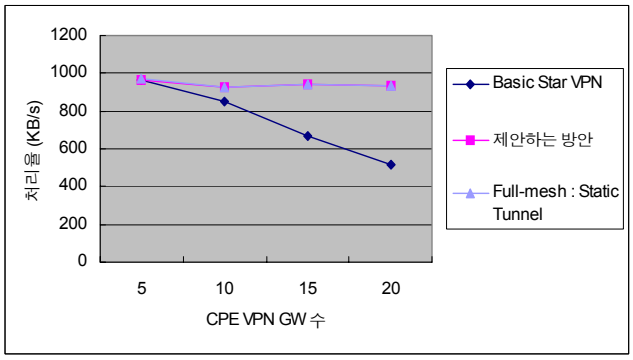

그림 7. Goodput

그림 8과 9는 VPN 확장성 측정을 위해 모든 VPN GW에서 유지하는 터널의 수와 CPE VPN GW에서 유지하는 터널의 수의 합을 구한 결과이다. 그림 8의 Full-mesh VPN 구조의 Static Tunnel 방법의 경우 CPE VPN GW의 수가 늘어날수록 VPN GW에서 유지하는 터널 정보도 크게 증가함을 알 수 있다. 제안하는 방안에서는 필요에 따라 터널을 설립하고 해제하므로 VPN GW에서 유지하는 터널 정보는 Basic Star VPN 구조와 비슷함을 알 수 있다. 그림 9의 Basic Star VPN 구조와 Full-mesh VPN 구조에서는 이미 터널의 엔드 포인트(Endpoint)가 지정되어 있기 때문에 유지하고 있는 터널의 수가 일정하다. 제안하는 방안에서는 CPE VPN GW에서 터널 설립이 필요할 때 상대 CPE VPN GW와 터널 설립을 하기 때문에 Center VPN GW에 대한 터널 정보 이외에 통신하는 CPE VPN GW의 터널 정보가 요구되지만 각 CPE VPN GW에서 유지하고 있는 터널 정보는 Basic Star VPN 구조와 크게 차이가 나지는 않았다.

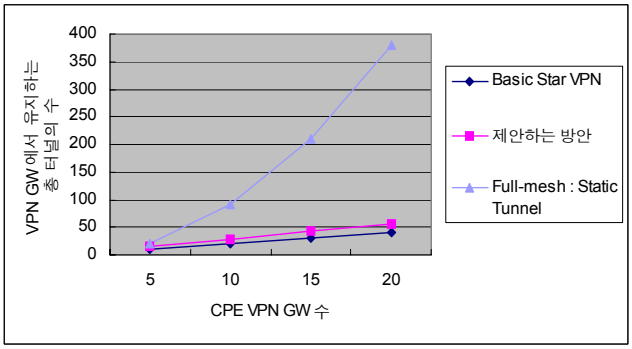

그림 8. VPN GW에서 유지하고 있는 터널 수의 합

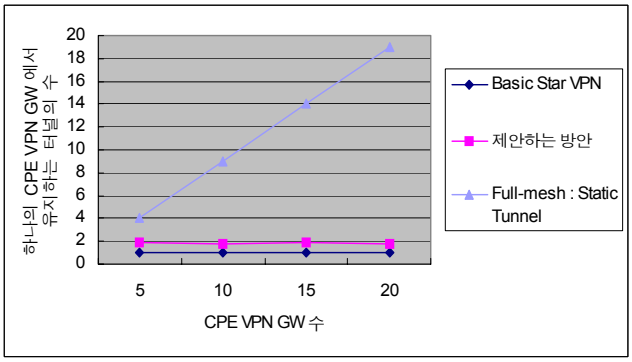

그림 9. CPE VPN GW에서 유지하는 평균 터널의 수

4. 결론

본 논문에서는 Star VPN 구조에서 CPE VPN GW간 직접 터널을 설립하기 위한 방법으로써 주문형 터널 생성(On-demand Tunnel Creation) 메커니즘 제안하였다. 시뮬레이션을 통해 제안하는 방안이 Basic Star VPN 구조보다 확장성, 트래픽 전송 효율성, Center VPN GW의 오버헤드에서 우수한 성능을 보였으며, 종단간 지연시간과 처리율에 있어서는 Full-mesh VPN 구조와 거의 비슷한 성능을 보였다.

참고문헌

[1] B. Gleeson, A. Lin, J. Heinanen, G. Armitage A. Malis, "A Framework for IP Based Virtual Private Networks", RFC 2764, Informational