제 19 회 한국정보처리학회 춘계학술발표대회 논문집 제 10 권 제 1 호 (2003. 5)

IP VPN 서비스의 출현과 ISP 보안 구조에 대한 연구

이 승 민, 남 택 용

한국전자통신연구원 네트워크보안구조연구팀 (대전광역시 유성구 가정동 161)

A Study on Emerging IP VPN Services and ISP Security Architecture

Seungmin Lee, Taekyong Nam

Network Security Architecture Research Team, ETRI,
161, Gajong-dong, Yusong-gu, Daejon 305-350 KOREA

요 약

현재 ISP 에서 제공하는 보안 서비스는 보안 솔루션이 적용되는 위치관점에서 개별 고객망 기반의 보안 구조로 볼 수 있다. 이는 확장성과 외부 공격에 대한 대응 등에 많은 한계점을 가지고 있다. 최근 이러한 문제점을 해결하고 보다 다양한 보안 서비스를 가능하게 하는 네트워크 기반의 보안 구조가 대두 되고 있다. 본 논문에서는 먼저 ISP 보안 구조의 변화에 많은 영향을 끼친 IP VPN 서비스의 출현에 대하여 살펴보고, 앞으로 ISP 의 주된 보안 구조가 될 네트워크 기반의 보안 구조에 대하여 논의해 보기로 한다.

1. 서 론

ISP 에서 제공하는 보안 서비스는 현재 단순 제품 위주의 보안 솔루션에서 정보보호 컨설팅 및 교육에서부터 시스템 구축과 관리대행 등의 종합 정보보호 서비스로 발전하여 왔다. 보안 솔루션이 적용되는 위치 관점에서 이는 개별 고객망 기반의 보안 서비스로 볼 수 있다.

최근 네트워크 기반의 IP VPN 서비스의 출현으로 인한 기업 환경의 변화는 보안 서비스에도 변화를 예고하고 있다.

또한 IP VPN 서비스는 대부분 ISP 의 에지에서 제공되므로 VPN 기능 이외에 기존 라우터에서 여러 고객 트래픽을 독립적으로 처리하는 가상 라우팅 기능과 침입차단 기능 등이 복합된 IP 멀티서비스 장비가 등장하기 시작하였다.

이와 같은 움직임은 ISP 입장에서 네트워크 기반의 보안 서비스로의 보안 구조를 변화시키는 데 적지않은 영향을 끼칠 것으로 보인다. 이에 따라 기존의 고객망 기반에서 제공되는 보안 구조의 한계점은 네트워크 기반의 보안 구조의 출현으로 많은 부분 해결 될 것으로 기대된다.

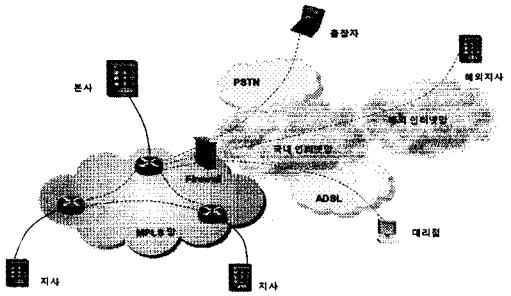
본 논문에서는 먼저 국내외 ISP 들의 IP VPN 도입 현황을 살펴보고, 이것과 ISP 보안 구조의 변화의 관련성에 대하여 논의해 보기로 한다.

2. IP VPN 서비스의 출현

네트워크 기반의 VPN 서비스로 불려지는 ISP 가 제공하는 VPN 서비스는 VPN 회선 제공과 함께 관리도 ISP 가 맡게 된다. 최근에는 네트워크 기반의 IP VPN 이라는 정의가 폭넓게 사용되며 그 안에는 IPSec VPN 과 MPLS VPN 이 포함된다(그림 1).

IPSec VPN 은 인터넷망을 이용하되 고객이 CPE 장비를 직접 구입하거나 ISP 에게 임대 받는다. 인터넷망을 이용하기 때문에 QoS 보장이 어렵다.

반면 MPLS VPN 은 ISP 가 대부분 MPLS 망을 따로 구성해 서비스를 제공하며 인터넷 연결을 원하는 고객에겐 두 망 사이에 침입차단시스템, NAT 기능을 하는 게이트웨이를 설치해 인터넷에 접속시켜 준다. 인터넷과 별개인 MPLS 망을 구성해 서비스하기 때문에 보안성이 좋고 QoS 도 보장해 줄 수 있다. 서비스 사업자가 MPLS VPN 을 적극 도입하는 이유는 수익성이 좋기 때문이다.



[그림 1] 네트워크 기반의 IP VPN 서비스
(MPLS VPN, IPSec VPN)

시장 조사기관에서는 MPLS VPN 서비스를 향후 서비스 사업자의 주력 상품이 될 것이라 예측하고 있다. 이미 세계 160 개 서비스 사업자들이 MPLS VPN 을 도입, 서비스 중이며 국내도 KT, 데이콤, 삼성네트웍스가 구축 운영 중이다.

전체적인 IT 경기 침체에도 불구하고 VPN 시장이 낙관적으로 전망되는 가장 큰 이유로 비용절감 효과를 들 수 있다. 전용회선에 비해 평균 40~50%에 불과한 요금은 불황에서 더욱 매력적일 수밖에 없고, 기술 발달로 강화된 보안성도 전용회선에서 VPN 으로 옮기게 되는 주요 원인이 되고 있다. 그러나 특히 국내에서 최근 VPN 이 급부상하는 요인으로 ISP 에서 제공하는 MPLS VPN 의 출현과 발달된 초고속 인터넷(xDSL) 인프라를 꼽을 수 있다.

Nikkei communications 지에 따르면, 일본내 3000 개 회사를 대상으로 조사한 결과 IP VPN 서비스의 도입 비율이 작년에 비해 4 배가 증가한 3 할에 이르렀으며, 2003 년에는 일본 기업의 5 할이 IP VPN 이 될 것이라는 분석이다. 일본내 IP VPN 서비스 점유율 1 위는 NTT 의 Arcstar IP VPN 이며, 다음으로 KDDI 의 KDDI IP VPN 이 차지하고 있다. 상위 4 개의 서비스의 제공 방식은 모두 MPLS 를 이용한 서비스이다.

이와 같이 ISP 에 의해서 주도적으로 전개되는 네트워크 기반의 IP VPN 서비스는 세계적으로 확대되는 추세에 있으며, Yankee group 의 분석에 따르면 2005 년쯤 50 억달러의 규모로 성장할 것이라는 전망이다.

3. ISP 보안 구조의 변화

3.1. 현재의 보안 구조

네트워크를 소유하고 있는 ISP 에서 보안 서비스를 제공하고 관리까지 대행해 주는 보안 관리형 서비스는 업체마다 약간의 차이는 있지만 현재 주류를 이루고 있는 Managed security services 와 보안 컨설팅, 솔루션 구축 및 관리를 포함한다. 보안 솔루션이 적용되는 위치 관점에서 이와 같은 서비스는 대부분 고객망 기반의 보안 서비스로 볼 수 있다.

국내의 경우 데이콤이 2001 년 말부터 이와 같은 보안 서비스를 제공하기 시작하였으며 KT, 하나로통신, 한솔 아이글로브 등의 경우에는 자사의 인터넷데이터센터 고객을 대상으로 다양한 종류의 보안 서비스를 제공하고 있다. 외국의 경우 NTT, WorldCom, AT&T, PSINet 등에서 Managed security services 개념의 보안 서비스를 제공하고 있다

그러나 고객망 기반의 보안 구조는 서비스를 받는 고객 입장에서 볼 때, 망 확장에 따른 확장성 부족과 관리 비용의 증가, 그리고 글로벌한 보안 서비스 부재로 인한 외부 공격에 대한 대응의 한계점을 가지고 있다.

3.2 네트워크 기반의 보안 구조의 등장

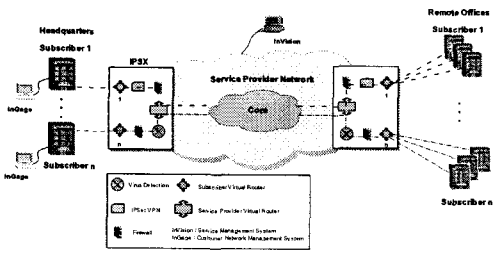
네트워크 기반의 IP VPN 서비스로 인한 기업 환경의 변화는 네트워크 기반의 보안 서비스의 출현을 예고하고 있다. 즉, ISP 에서 제공하는 VPN 을 이용하고 있는 고객이 인터넷 서비스를 이용하고 자 할 때, VPN 망을 경유하여 인터넷 망에 접속 되므로 인터넷망과의 연결 부분에 보안 기능을 제공하기 시작

하였다.

그리고 ISP 의 에지 부분에 위치하여 VPN 기능으로부터 출발한 네트워크 장비는 대규모의 고객을 한 장비에서 독립적으로 처리하는 가상 라우팅 기능과 함께 침입차단 기능을 포함한 다양한 보안 기능을 갖춘 IP 멀티서비스 장비로 발전하고 있다. 이 또한 네트워크 기반의 보안 서비스의 출현을 가속화 시킬 것으로 보인다.

이와 같은 복합 보안 기능을 수행하는 장비를 제조하는 업체는 대표적으로 보안 업체인 CoSine communications 와 네트워크 장비 업체인 Cisco 등이 있다.

CoSine communications 는 IP 멀티서비스 장비 IPSX9500/3500 으로 IP VPN 기반 MPLS 게이트웨이와 MPLS 프로바이더 에지(PE) 시장을 공략하고 있다(그림 2). IPSX9500 은 VPN 서비스를 위한 MPLS 와 인터넷망 연결시 침입차단시스템, IPSec 터미네이션, NAT 역할을 하는 게이트웨이이다.

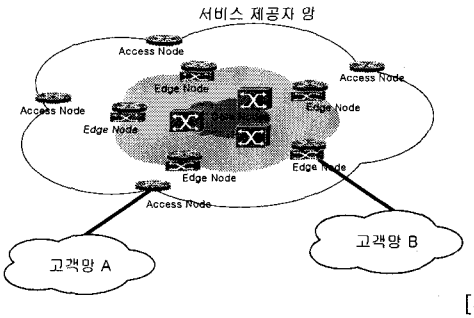


[그림 2] CoSine communications IPSX 를 이용한 보안 서비스

한편, 보안 업체와 비교하여 네트워크 업체인 Cisco 는 최근 새롭게 강화된 멀티기가비트 네트워크 보안 시스템을 발표 하였는데, 이는 기존의 시스코 카탈리스트 6500 시리즈 스위치에 카탈리스트 침입차단 서비스 모듈, IPSec VPN 서비스 모듈, SSL 서비스 모듈, 강화된 네트워크 분석 모듈 등의 4 가지의 고성능 보안 서비스 모듈을 선택적으로 채택할 수 있다. 이 모듈은 시스코 7600 시리즈의 라우터에도 적용될 수 있다.

이와 같은 IP 멀티서비스 장비는 CoSine communications 와 같이 ISP 의 에지 부분에 위치하여 한 장비에서 여러 보안 기능을 제공하며 하나의 부가적인 기능으로 IP VPN 을 지원하는 IP service switch (IPSS)와, 시스코등과 같이 에지 라우터에 IP VPN 기능은 결합하지만 IPSS 와 같은 다양한 보안 기능은 포함하지 않는 Multiservice edge router(MER)로 개발되어 왔다. 이 같은 IPSS 와 MER 기술은 향후 상호 결합되어 네트워크 기반의 IP 서비스를 제공할 것으로 보인다.

IP VPN 서비스로부터 시작된 네트워크 기반의 보안 구조는 향후 다양한 보안 기능을 갖춘 IP 멀티서비스 장비의 개발에 따라 ISP 보안 구조의 변화를 주도할 것으로 예상된다(그림 3). 다만, ISP 마다 자사의 전략에 부합한 장비의 도입과 기존의 네트워크 서비스와의 관계를 고려한 보안 구조의 정립, 그리고 타 망 사업자와의 협력 관계를 고려한 깊이 있는 연구가 선행되어야 할 것이다.



[그림 3] 네트워크 기반의 보안 구조

네트워크 기반의 보안 구조는 기존의 고객망 기반의 보안 구조와 비교하면, 고객망에 변화를 주지 않고 네트워크 기반의 확장성 있는 보안 서비스를 가능하게 할 뿐만 아니라, 외부 공격에 대하여 글로벌 대응이 가능하며 유해 트래픽에 대해서 사전에 차단이 용이하다는 이점이 있다(표 1).

[표 1] 보안 구조 비교

구분	기존 보안 구조	네트워크기반 보안구조
적용망	고객망	기간망, 공중망
서비스	보안컨설팅, 취약성 점검을 포함한 보안 관제 서비스	네트워크 기반의 IP VPN 를 포함한 침입차단, 항 바이러스 등

보안 장비	IDS, Firewall, Anti-virus, vpn appliance, ESM 등의 보안 솔루션	CoSine, Quarry, Cisco, Nortel 등에서 개발한 에지형 IP 복합 멀티 서비스 장비
장점	ISP 네트워크 구조의 변화가 필요 없음.	확장성이 용이하며 비용 절감, 고객망의 변화가 필요 없음
단점	고객망 확장에 따른 확장성 부족과 비용 증가, 글로벌 보안 서비스 부재	ISP 네트워크 구조의 변화가 필요함.
방향	네트워크 기반의 보안 서비스화	기술적으로 성숙된 복합 보안 장비 개발, 체계적인 운용 및 관리에 대한 연구 필요

4. 결론

현재 IP VPN 을 중심으로 한 네트워크 기술의 변화와 네트워크 장비의 개발 등으로 인하여 네트워크 기반의 보안 구조로의 진화는 자연스럽게 진행될 것으로 전망된다.

ISP 는 이러한 추세를 고려하여 네트워크 기반의 보안 구조를 구축함에 있어서, 무엇보다 기존의 네트워크 구조를 고려하여 타당성 있는 전략을 수립해야 할 것이다.

참고 문헌

[1] 데이콤, http://www.dacomisg.com

[2] NTT, http://www.ntt.com

[3] Cosine, http://www.cosinecom.com

[4] Cisco, http://www.cisco.com

[5] Strategies & Issues - IP VPNs : The Next Wave, http://www.networkmagazine.com

[6] 기업내 IP VPN, Nikkkei Com., 2002. 08.