ISBN : 978-89-6211-376-1

2009 IPv6 보안 현황

IPv6 Security Status Report 2009

2009. 5. 15.

한국과학기술정보연구원

목 차

제 1 장 서 론 ····· **1**
1. IPv6 개요 ····· 1
2. IPv6 주요 특징 ····· 4
3. IPv6 보안 ····· 6

제 2 장 IPv6 보안현황 및 구축사례 ····· **8**
1. IPv6 지원 장비 동향 ····· 8
1.1 IPv6 지원 장비 개발현황 ····· 8
1.2 IPv6 지원 장비 동향 ····· 10
2. 국내·외 IPv6 구축 사례 ····· 28
2.1 국내 사례 ····· 28
2.2 해외 사례 ····· 37

제 3 장 IPv6 보안 고려사항 ····· **45**
1. IPv6 보안 위협 ····· 45
2. IPv6 보안정책 고려사항 ····· 46

제 4 장 결 론 ····· **51**

참고문헌 ····· **54**

약 어 ····· **55**

표 목 차

[표 1] IPv4주소 고갈 시기 예측 ····· 3
[표 2] IPv6 지원 국산 보안장비 비교 ····· 26
[표 3] IPv6 지원 외산 보안장비 비교 ····· 27

그 림 목 차

[그림 1] IPv4 Exhaustion Counter ····· 2
[그림 2] 한국천문연구원 IPv4/IPv6 네트워크 ····· 28
[그림 3] 한국기초과학지원연구원 IPv4/IPv6 네트워크 ····· 29
[그림 4] 국가핵융합연구소 IPv4/IPv6 네트워크 ····· 30
[그림 5] 한국항공우주연구원 IPv4/IPv6 네트워크 ····· 31
[그림 6] 한국표준과학연구원 IPv4/IPv6 네트워크 ····· 32
[그림 7] 강릉시청 IPv4/IPv6 네트워크 ····· 33
[그림 8] 공주시청 IPv4/IPv6 네트워크 ····· 34
[그림 9] 한국인터넷진흥원 IPv4/IPv6 네트워크 ····· 35
[그림 10] 한국과학기술정보연구원 IPv4/IPv6 네트워크 ····· 36
[그림 11] Internet2 IPv4/IPv6 네트워크 ····· 37
[그림 12] JGN2plus IPv4/IPv6 네트워크 ····· 38
[그림 13] CERNET2 IPv6 네트워크 ····· 39
[그림 14] TWAREN IPv6 네트워크 ····· 40
[그림 15] University of Southampton IPv4/IPv6 네트워크 ····· 41
[그림 16] GEANT2 백본 네트워크 ····· 43
[그림 17] KanREN IPv6 네트워크 ····· 44
[그림 18] 간단한 IPv6 아키텍쳐 ····· 46

제 1 장 서 론

1. IPv6 개요

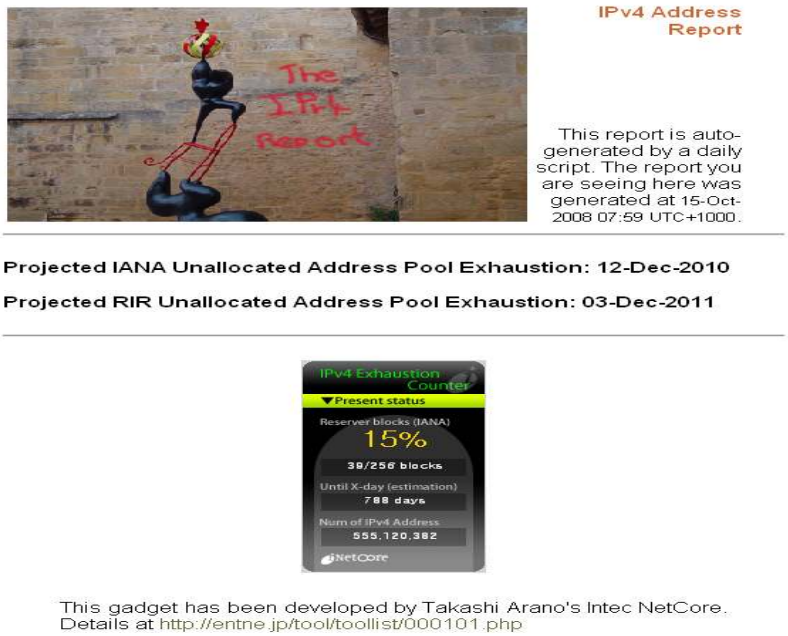
차세대인터넷프로토콜, 즉 IPv6는 크게 늘어난 IP 주소공간과 IPv4에 비해 많은 개선점을 제공함으로써 양적 질적인 측면 모두에서 인터넷의 계속적인 성장을 유지함을 목표로 개발되었다. 1994년에 IPng(The IP Next Generation)이라는 워킹그룹명으로 시작되어, 1998년 대부분의 주요 핵심표준의 개발이 완료되었으며, 현재는 IPv6 보급과 망관리 등을 위해 중요한 문제들에 대한 마무리 작업이 진행 중이다.

32bit로 구성되는 IPv4는 약 43억 개의 주소를 만들 수 있지만 오랜 시간 사용된 만큼 대부분이 소비되었으며, 더욱이 사설용으로 예약된 주소영역과 클래스 E는 연구용으로 사용되기 때문에 실제 사용할 수 있는 주소의 수는 훨씬 적다. 반면에 WWW(World Wide Web) 서비스의 개발로 인해 급격하게 증가한 호스트는 2008년 2월 현재 5억 4천여 개에 달하고 있으며, 향후 더욱 증가될 예정이다. 이에 반해 IPv4주소 자원은 80% 이상을 소비하고 있는 추세이고, 더욱이 지속적으로 인터넷을 활용하는 서비스 영역은 점점 더 확대되고 있으며, IP를 사용하는 기기 또한 점차 증가함에 따라 2013년경에 IPv4주소 자원은 전부 소진될 것으로 예측되고 있다.

IPv4주소 부족 문제는 NAT(Network Address Translation), CIDR(Classless Inter-Domain Routing), DHCP(Dynamic Host Configuration Protocol)나 RADIUS/PPP(Remote Authentication Dial In User Service/Point-to-Point Protocol) 등의 일시적 할당과 같은 주소 재활용 기술을 통해 보완되어 왔다. 이 기술들은 주소 공간을 늘려주고 전통적인 서버/클라이언트 환경을 만족하는 듯 보였으나 P2P 및 서버-to-클라이언트 응용 프로그램의 요구조건을 만족시키지는 못한다. 지속적인 연결 환경에 대한 필요가 충족되려면 이를 위한 IP

주소 변환, pooling 및 임시 할당 기술은 고려 대상이 될 수 없으며, 사용자용 인터넷 기기들의 플러그앤플레이(Plug & Play) 기능은 새로운 주소에 대한 요구를 더욱 증가시키고 있다.

IPv4는 주소 고갈 외에도 몇 가지 문제점을 내포하고 있다. IPv4는 인터넷 성장으로 인한 백본 라우터들의 대규모 라우팅 테이블 유지 능력 떨어지며, 단순하며 간단한 자동 설정 및 리넘버링(renumbering)에 대한 요구를 충족시키기가 어렵다. 또한 IP 수준에서의 보안을 위해 별개의 방안이 마련되어야 하며, QoS(Quality of Service)에 대한 지원을 고려하지 않고 개발되었다. 이로 인하여 현재의 IPv4는 홈 네트워크, 텔레매틱스, VoIP(Voice over Internet Protocol), 휴대 인터넷 서비스 등 현재 제공되고 있는 서비스들의 요구에 대한 충족은 물론 사용자 증가 및 인터넷 확장에 따른 지리적인 요구도 만족시킬 수 없다. IPv6는 이러한 요구를 만족시키고 네트워크의 주소지정 규칙이 다양한 서비스에 투명하게 제공될 수 있는 글로벌 환경을 위해 설계되었다.



[그림 2] IPv4 Exhaustion Counter

IPv6에는 IPv4의 주소 고갈에 대한 해결책을 제시하는 것을 기본으로 새로운 기능과 개선 사항을 추가하여 개발되었다. IPv6는 사용자, 응용 프로그램, 서비스의 요구사항을 만족시키기 위해 설계되었으며, 네트워크 운영을 보다 단순화시킬 수 있도록 하고 있다. IPv4 주소 고갈시기 예측에 대한 분석에 대해서는 다양한 각도에서 고갈시기를 예측하여 각종 보고서를 보고해오고 있다. APNIC 의장인 Geoff Huston이 작성한 리포트에서는 과거 BGP 라우팅 테이블, 각 RIR의 주소 할당보고서, IANA의 RIR로의 주소 할당 현황 등 수많은 IPv4주소 소비 현황 데이터를 분석하고 있다. 그림 1-1은 IPv4 Exhaustion Counter는 IANA에서 제공하는 "IPv4 Global Unicast Address Assignment"와 Geoff Huston의 "IPv4 Address Report"를 기반으로 IPv4주소의 고갈 시기를 제시하고 있다.

EC와 OECD는 IANA와 RIR의 주소 고갈 시기에 대한 예측을 기반으로 전체 IPv4주소 고갈 시기를 2011년 정도로 보고 있으며, 이에 대한 대책 마련을 각국 정부 및 산업체에 요구하고 있다. [표 1]은 IPv4주소 고갈 시기 예측에 대한 각 나라 및 기관의 동향을 정리한 표이다. 주소 고갈 등 IPv4에서 나타나는 다양한 문제점을 해결하기 위한 많은 연구가 진행되었으나 현재까지 IPv6의 도입을 대체할 수 있는 확실한 대안은 제시되지 못하고 있다. 즉 인터넷의 새로운 주소체계로써 IPv6가 사용될 것은 당연하게 인식되고 있으며, 많은 국가에서 빠르고 안정적으로 IPv6를 도입하기 위한 노력을 기울이고 있다.

[표 1] IPv4주소 고갈 시기 예측

국가/기관	IPv4 주소 고갈 시기 예측	예측 근거
IANA	2011년 4월	현재까지 미 할당된 주소 풀
RIR	2012년 5월	현재까지 미 할당된 주소 풀
EC	2011년	IANA와 RIR의 주소 고갈 시기
OECD	2010년 ~ 2011년	IANA와 RIR의 주소 고갈 시기
일본 총무성	2010년 중반 ~ 2012년 초	과거 IPv4 주소 보유 규모와 할당 규모를 기초로 분석

그러므로 국내에서도 IPv6 도입에 대한 해외 여러 국가들에 대한 움직임을 주시하고 이에 빠르게 대처할 수 있는 학술적, 정책적인 활동이 요구된다.

2. IPv6 주요 특징

첫째, IPv6의 주소비트는 IPv4의 32비트의 4배인 128비트로 설계되어 43억*43억*43억*43억 개의 주소가 가능하게 되어 거의 무한대의 주소를 가질 수 있다고 할 수 있다. 128비트는 지구상의 모든 사람마다 약 1030개(다른 교재의 경우 $5.4*10^{28}$로 나온다. 확인필요하다)의 주소를 할당할 수 있는 약 $3.4*10^{38}$ 개의 주소 노드를 제공한다.

둘째, 효율적인 패킷처리를 위해 헤더포멧이 보다 단순화되었다. IPv6주소의 증가된 비트 수는 IPv6 헤더 크기를 증가시키게 되지만 IPv6의 헤더 포맷은 IPv4의 헤더에 비해 더 간단하다. 기본적인 IPv4의 헤더 크기는 20옥텟이지만 옵션 필드의 변수 길이에 따라 IPv4 패킷의 전체 크기가 가변적이었다. 이에 반에 IPv6 헤더 크기는 40옥텟으로 고정되어 있다.

셋째, 효율적인 라우팅을 위한 계층적 네트워크 아키텍쳐를 가지고 있다. 대용량의 주소공간과 네트워크 프리픽스(prefix)는 유연한 네트워크 아키택처를 제공한다. 이러한 유연성은 조직이 전체 네트워크를 위해 오직 하나의 프리픽스(prefix)만을 사용할 수 있게 해준다. 더 커진 주소 공간은 ISP(Internet Service Provider)와 기타 다른 조직에게 대형화된 주소블록을 할당할 수 있게 해준다. 그 결과 ISP는 모든 고객들의 프리픽스(prefix)를 하나의 프리픽스(prefix)로 통합할 수 있으며 통합된 프리픽스(prefix)를 IPv6 인터넷에 알리게 된다.

넷째, 확장 가능한 라우팅을 위해 IPv6는 기존의 Interior Gateway Protocol(IGP)과 Exterior Gateway Protocol(EGP)을 지원한다. IPv6는 IPv4와 마

찬가지로 라우팅 알고리즘을 위해 가장 긴 프리픽스(prefix) 매칭을 이용한다. RIP2, OSPFv3, ISIS 그리고 멀티프로토콜 BGP4+까지 IPv6 라우팅을 위한 모든 기능적인 속성들을 제공하고 있다.

다섯째, IPv6 프로토콜내에서 내장된 주소 자동 설정 기능을 통하여 주소관리를 간편하게 하고 플러그 앤 플레이 지원을 제공함으로서 DHCP 서버가 필요없이 네트워크에 자동으로 접속할 수 있게한다. 이러한 특징으로 자동할당을 통한 ISP등의 리넘버링 정책이 비교적 간단하게 해결될 수 있다.

여섯째, NAT 장비를 설치할 필요가 없어지며 네트워크의 투명성이 증가하여 사용자와 사용자간의 네트워크 복잡성을 줄일 수 있다.

일곱 번째, 보안 기능이 임베디드 형태로 지원된다. 즉 IPSEC을 통한 보안을 강화함으로써 자연스럽게 암호와, 인증 그리고 VPN 등의 구현이 용이하게 되었다.

여덟 번째, 모바일 이동성이 보장되어 IPv6 노드는 연결을 유지한 상태에서 자유롭게 이동할 수 있다.

아홉 번째, IPv6의 가장 두드러진 특징 중의 하나는 브로드캐스트를 전혀 사용하지 않는다는 것이다. IPv4 브로드캐스트가 지원했던 라우터 탐색(Router Discovery) 및 라우터 요청 (Router Solicitation) 같은 기능들은 IPv6 멀티캐스트에 의해 처리된다. 멀티캐스트는 비디오 스트림 같은 IP 패킷이 동시에 여러 곳으로 보내질 수 있도록 하여 네트워크 대역폭을 절약시켜 준다.

열 번째, IPv6에서의 QoS(Quality of Service)는 IPv4에서와 같은 방식으로 처리된다. 서비스 클래스에 대한 지원은 IETF Differentiated Service(DiffServ) 모델을 따르고 있는 Traffic Class 필드를 통해 제공된다.

3. IPv6 보안

현재 개발된 IPv4/IPv6 전환 메커니즘에서의 중요한 고려사항 중 하나는 보안 문제에 있다. 또한 IP프로토콜이 처음 개발되어 제안된 1970년 이후, IP 보안에 대한 문제는 끊임없이 지속적으로 연구되어왔으며, 현재도 인터넷의 가장 취약한 문제점 중의 하나로 보안 문제를 꼽고 있을 정도로 많은 연구와 관심이 진행되고 있는 분야 중의 하나이다. IPv6 차세대 인터넷 프로토콜은 이러한 IP의 문제점을 개선하기 위해 IPsec의 구현을 기본(mandatory)으로 하는 등 보다 안전한 인터넷(secure Internet)을 구축하기 위한 설계 철학을 담기도 하였다. 그러나, 최근 IETF 내의 보안 그룹 등에서 IPv6 프로토콜에서의 확장 헤더의 사용, IPv4/IPv6 전환 메커니즘의 사용시 보안 문제가 발생할 수 있다고 연구결과를 발표하고, 이에 대한 보안 확인을 반드시 하도록 권고하고 있다. IPv6 도입에 따른 보안 위협 요소를 크게 두 가지로 구분할 수 있다. 첫째는 IPv6 프로토콜 자체에 대한 문제로 처음 설계 당시 기존의 IPv4와는 다른 확장된 프로토콜을 설계하고자 추가했던 기능들이, 보안 관점에선 문제가 되는 것으로 보고되고 있다. 물론 이러한 문제점들은 IPv6의 궁극적인 문제들은 아니며, 기존 IPv4 프로토콜 역시 해커들의 공격과 이에 대한 보안 문제의 해결이라는 반복을 통해 보다 안전한 프로토콜로 발전해 나갔던 것처럼 IPv6 역시, 이러한 보안 문제점들도 IPv6 프로토콜의 보안기능 수정과 방화벽, 침입방지시스템(IPS)에서의 관련 기능 추가 등으로 인해 해결될 수 있을 것으로 생각된다. 두번째 문제로는 IPv4/IPv6 연동 환경에 따른 보안 문제들로서, 실제 IPv4프로토콜, 혹은 IPv6 프로토콜 자체로는 문제가 없지만, 두 망이 혼재되는 상황에선 예상치 못했던 보안 위협 문제가 발생할 수 있다.

IPv6 입장에서 임베디드 IPSEC을 통한 기본적인 보안기능이 강화되어 있다. 하지만 실질적으로 망을 이용하는 기관의 입장에서 IPsec 만으로는 보안에 대한 홀 및 취약성에 대한 정확한 검증이 이루어지지 못한 상태이다. 이는 실질적인 망운영 및 기관차원에서 검토해야할 가장 중요한 이슈가 될 것이라 판

단된다. 이에 따라 본 보고서에서는 현재 진행되고 있는 보안장비의 개발현황과 실제 적용사례를 중심으로 보안의 필요성을 강조한다.

본 원고에서는 현재 우리나라를 포함하여 전세계에 걸쳐 개발되거나 개발되고 있는 보안장비에 대한 현황을 파악하고 보안장비의 기본 지원기능 등을 비교 분석한다. 또한 방화벽, 침입탐지시스템, 침입차단시스템, 웹방화벽 등 무수히 많은 네트워크 보안장비들의 현황을 파악함으로서 IPv6 현황 및 향후 IPv6 전환전략 수립 및 장비도입에 주요한 가이드라인으로 이용되기를 희망한다.

제 2 장 IPv6 보안현황 및 구축사례

1. IPv6 지원 장비 동향

1.1 IPv6 지원 장비 개발현황

최근 들어 수많은 정부부처 및 기관, 기업, 금융기관 등에서 네트워크를 업그레이드하면서, 해당 장비를 선정할 때 대부분 외산제품들을 찾고 있다. 이러한 현상은 기존의 IPv4망을 IPv6망으로 전환할 때에도 변하지 않고 있다. 이는 여러 가지 이유가 있지만 크게 세 가지로 나누어 볼 수 있다. 첫째, 국내에서 IPv6 라우팅을 완벽하게 지원하는 것으로 알려진 보안장비가 거의 전무한 실정이다. 둘째, 네트워크 관리자들은 기존에 구축된 외산장비들과의 호환성과 상호연동시 문제발생에 대한 염려로 인해 국산장비를 도입하는 것에 대해 거부감을 가지고 있다. 셋째, 대부분의 네트워크 관리자들은 국산장비들의 성능이나 안정성 그리고 도입후 유지보수 측면에서 외산장비들에 비해 질이 떨어진다고 생각한다. 이는 국산 장비업체들의 기술력 문제가 아니라 대부분의 국산 보안장비 업체들이 중소기업이기 때문이다. 또한 최근들어 국산보안장비 업체들이 IPv6를 지원하는 제품들을 출시하고 있지만, 실제로 IPv6 네트워크에 설치되어 운영된 사례가 없기 때문에 아직 검증이 된 제품은 없다고 볼 수 있다. 따라서, 트래픽이 흐르는 네트워크에 장비를 설치하여 운영하는 사용자 입장에서는 실제 IPv6 네트워크에 구축 및 연동되어서 많은 경험과 검증을 거친 외산장비를 선호할 수밖에 없다.

정부가 오는 2012년까지 국내 모든 상용 통신망의 가입자망을 차세대 인터넷 주소체계인 IPv6로 전환키로 함에 따라 국산 장비업계에도 특수가 일지 주목되고 있다. 특히 그동안 외산 네트워크 장비업체들이 주도해 온 IPv6 장비 시장에 국내 장비업체들이 국산화 바람을 일으킬지 주목된다.

업계 전문가들은 정부의 IPv6 전환 방침이 당장 네트워크 장비 특수로 이어지지는 않을 것으로 보고 있다. 이미 상당수 네트워크 장비업체들이 IPv6 전환을 염두에 두고 IPv4/IPv6 듀얼 장비를 개발·공급해 온 데다, 가장 큰 수요 발생이 예상되는 정부·공공기관의 경우도 시범사업 등을 통해 어느 정도 IPv6 주소체계를 갖춰가고 있다는 것이다.

하지만 장기적으로 볼 때 수혜는 분명해 보인다. 2010년 정부·공공기관에 이어 2012년까지 모든 상용 통신망의 인터넷 주소체계가 IPv6로 바뀔 경우, IPv6를 지원하지 않는 네트워크 장비는 교체가 불가피하기 때문이다.

한 업계 전문가는 "IPv6 주소체계가 본격화되면 일부 IPv4와 IPv6를 동시에 지원하는 듀얼스텍 장비를 제외하고 현재 인터넷 망에서 사용하고 있는 라우터와 단말기는 물론 허브, 스위치, 무선 공유기, 나아가 컴퓨터 운영체제(OS)까지 대부분 네트워크 장비의 사용이 불가능하다"며 "결국 장비를 교체하거나 소프트웨어를 업그레이드해줘야 하는 만큼, 분명 새로운 시장이 열릴 것"이라고 말했다.

이에 따라 네트워크 장비업체들이 IPv6 장비 상용화시범사업 등에서 국산 장비를 우선 채택하고 있는 만큼, 국내 네트워크 업체들의 IPv6 장비 출시가 이어질 것으로 전문가들은 보고 있다.

실제 국내 네트워크 장비 업체들은 올해 이후로 IPv6 장비시장이 본격화될 것으로 보고 있다. 향후에 이들은 스위치와 라우터뿐만 아니라, 유무선 통신단말기 분야에 이르기까지 IPv6 장비 개발 및 출시를 서두르고 있다. 또한 국내통신장비 업체들이 VoIP 시장을 겨냥하여 IPv6 기반의 IP-PBX(IP 사설교환기), 게이트웨이, 유무선 IP폰 출시가 이어질 전망이다.

이처럼 국산 장비업체들이 다양한 네트워크 장비들을 개발하여 향후 IPv6 네

트워크의 확산 및 전환에 대비하고 있지만, 보안 장비들의 경우에는 IPv6를 지원하는 장비들의 개발을 서두르지 않고 있다. 이는 정부가 주도적으로 IPv6의 전환 및 확산에 주력하고 있음에도 불구하고 아직까지 대부분의 네트워크들이 IPv6로 전환되기 위해서는 많은 시간이 걸릴 것으로 예상하고 있기 때문이다. 이러한 예상의 저변에는 IPv6 트래픽의 양이 많지 않다는 사실이 존재한다. 이는 현재 대부분의 국가에서 정부가 주도적으로 IPv6망으로의 전환을 유도하고 확산을 촉진하고 있지만, 획기적인 전환 및 확산 효과는 발생되지 않고 있는 것과 궤를 같이한다. 즉, IPv6를 이용하여야만 사용이 가능한 애플리케이션이 아직 없다는 것이 IPv6 네트워크 전환 및 확산에 가장 큰 걸림돌이 되고 있다. 이러한 애플리케이션이 개발되면 IPv6를 이용하는 트래픽이 증가하게 될 것이고, 이 트래픽을 통해서 악의적인 공격, 불법적인 자료획득 및 다양한 이상행위도 증가하게 될 것이다. 따라서, 이를 막기 위한 IPv6 지원 보안장비의 수요가 크게 증가할 것이다.

IPv6를 활용하는 킬러 애플리케이션으로 단기적으로는 가상사설망(VPN), 인터넷전화(VoIP), 게임, 브로드밴드, 3세대(3G) 이동통신 등이 중장기적으론 NGN, 원격제어, 휴대인터넷(와이브로), 홈 네트워크, 전력선 통신 등이 꼽힌다. [1]

이와 같이 IPv6를 활용할 솔루션들이 활성화 된다면 IPv6지원 국산 보안장비의 시장 및 보급률은 급속히 증가 될 수 있을 것이다.

1.2 IPv6 지원 장비 동향

1.2.1 외산 IPv6 지원장비 동향

○ 시스코

시스코 ASA(Adaptive Security Appliance) 5500 시리즈 [4]는 시스코의 지

능형 네트워크 보안 전략의 최신 단계인 '적응형 위협방어(Adopted Threat Defense)' 를 실현하기 위한 제품으로 웜, 바이러스, DoS 공격 등 유해한 요소가 네트워크를 통해 퍼지기 전에 미리 막아주는 하드웨어 일체형 통합 보안 솔루션이다.

이 제품군은 단일 플랫폼 상에서 방화벽, 가상사설망(VPN), 침입방지(IPS), 네트워크 및 애플리케이션의 트래픽 제어 등 보안에 필요한 모든 기능을 구현한다. 또한 서비스의 확장과 웹을 통한 통합적인 관리가 동시에 가능하여 복잡한 운영상의 절차 없이도 여러 종류의 보안 서비스를 동시에 운영할 수 있다. 시스코 ASA 5500 시리즈는 방화벽 성능으로 최대 20Gbps를 VPN 성능으로 최대 1Gbps를 보장한다. 세션 수는 방화벽일 경우에 최대 2,000,000세션과 VPN일 경우에 10,000세션을 동시에 지원한다. IPv4/IPv6 듀얼스택을 지원하며 2005년 8월 1일에 IPv6 Ready Phase-2 인증을 획득했고 2007년 10월말 에는 국가정보원의 보안적합성 검증을 통과함으로써 공공시장에서도 도입이 가능하다.

시스코 ASA 5500 시리즈의 보안 기능은 시스코의 PIX 보안 어플라이언스, IPS 4200 시리즈, VPN 3000 콘센트레이터 제품군의 최신 보안 기능에 기반을 두고 있다. 이 제품은 원격접속 IPSec, SSL VPN, 그리고 QoS가 보장되는 지점-대-지점(site-to-site) IPSec 서비스 등 일련의 VPN 서비스들을 제공하는 동시에 IP 통합, 라우팅, IPv6, 멀티캐스트를 지원하도록 디자인되어 기존 트래픽이나 애플리케이션 성능에 영향을 주지 않고 네트워크에 바로 삽입이 가능하다.

시스코 ASA 5500 시리즈는 고객의 보안망 구축에 소프트웨어와 하드웨어 모듈을 통한 서비스 확장, 이종 플랫폼 표준화, 통합 관리와 모니터링을 통한 운영의 간편함, 손쉬워진 문제해결과 고장 시스템의 격리 등의 강점으로 인해 경제적인 운영 효율성을 보장해 준다. 즉, 사이트 및 기능에 따라 맞춤화가 가능하여 고객들은 기존에는 이종의 플랫폼과 개별적 관리 체계를 필요로 했던

여러 종류의 보안서비스를 시스코 ASA 5500 시리즈의 단일 제품상에서 표준화할 수 있게 되면서 관리할 플랫폼 수는 줄이면서 동시에 공통의 운영 및 관리 환경은 보장받게 된다.

이러한 통합 관리서비스는 단일 장비 관리를 위한 '적응형 보안 디바이스 매니저 (Adaptive Security Device Manager)'와 복수 장비 관리를 위한 '시스코 보안관리 스위트(Cisco Security Management Suite)'를 통해 제공된다.

적응형 보안 디바이스 매니저(ASDM)는 통합된 웹 기반으로 방화벽과 침입차단을 포함한 모든 보안 및 VPN 장비 서비스의 구성이 가능하며, 통합된 장비의 상태와 서비스 모니터링 및 리포팅도 제공하기 때문에 10대 규모의 비교적 작은 구축에 적합하다. 시스코 보안관리 스위트(CSMS)는 규모가 더 큰 경우를 위한 것으로 정교한 정책 기반의 다중서비스, 다중기능, 다중 사이트 관리를 제공한다. 이는 어플라이언스, 라우터, 스위치들이 뒤섞여 있는 하이브리드 플랫폼 환경을 지원하며, 복수 사용자 또는 복수 부서 업데이트 제어 및 감사 기능을 제공한다.

시스코 ASA 5500 시리즈는 소형 기업군을 위한 ASA 5505, ASA 5510 및, ASA 5520, 중형 기업군을 위한 ASA 5520, 5540, 5550, 그리고 대형 기업군을 위한 ASA 5580으로 구분된다.

시스코 PIX 535 [4]는 4계층에서 7계층 까지의 데이터 플로우를 검사하는 30개의 애플리케이션 감지 엔진을 이용하여 강력한 애플리케이션 계층의 방화벽 기능을 수행하며 시스코의 침입방지 시스템과 통합하여 이상행위 노드들을 동적으로 차단할 수 있는 방화벽 장비이다. 고속의 VPN기능을 제공하며 HTTP, FTP, ESMTP, DNS, SNMP, ICMP와 같은 TCP/IP 기반의 프로토콜은 물론이고 SIP, SCCP, RTSP, GTP, ILS와 같은 프로토콜의 트래픽에 대해서도 검사가 가능하다. 또한 GUI 인터페이스를 통해 공격 및 감사, 보고활동을 손쉽게 수행할 수 있다.

시스코 PIX 535는 1.7 Gbps의 처리능력을 보장하며 500,000개의 동시세션을 지원한다. VPN 성능으로 최대 495 Mbps까지 지원하며 동시 세션수는 2000개이다. IPv4/IPv6 듀얼스택을 지원하며 CC인증과 FIPS 140-2 레벨 2 인증을 이미 마쳤다. 각각의 보안기능별 특성은 다음과 같다.

▪ 방화벽 기능

Stateful inspection기법을 통해 네트워크의 모든 통신을 감지하며, 100개 이상의 미리 정의된 애플리케이션은 물론 추가로 정의되는 애플리케이션들에 대해 인터페이스 기반 접근제어, 시간기반 접근제어, 사용자 혹은 그룹당 접근제어를 제공한다. 침입방지 시스템을 설치하면 기 구축된 침입패턴을 이용하여 다양한 침입들을 탐지해내고 이들로부터 네트워크를 보호한다. 하나의 장비에서 다양한 보안 컨텍스트를 생성하고 운용하는 것이 가능하고 각각의 컨텍스트 마다 자신의 보안정책, 논리적 인터페이스, 관리 도메인을 운영할 수 있다.

▪ VPN 기능

암호 알고리즘으로 168비트의 3DES와 256비트의 AES를 사용하며 하드웨어 기반의 VPN 가속기를 이용하여 높은 VPN성능을 보장하고 TACACS+와 RADIUS를 통한 AAA서비스 제공이 가능하다. 또한 시스코의 SACS(Secure Access Control Server)와의 밀결합을 통해 사용자 혹은 그룹기반의 정책을 지원하고 사용자 및 관리자 인증서비스를 제공할 수 있다.

○ 쥬니퍼

쥬니퍼 네트웍스의 ISG(Integrated Security Gateway) 시리즈 [5]는 기가비트의 성능과 모듈방식의 아키텍처, 그리고 다양한 가상화 기능을 보유하고 있으며 방화벽, VPN, IPS의 보안기능을 하나의 장비에 통합한 하드웨어 일체형 통합시스템이다. 침입탐지 및 방지기능을 통합하기에 용이한 추가모듈 슬롯을

보유하고 있으며 OSPF, BGP, RIPv2와 같은 동적라우팅을 지원하고 GUI를 통해 공격 및 사고조사, 감사, 보고활동을 손쉽게 수행할 수 있다.

ISG시리즈는 방화벽 성능으로 최대 4Gbps를 보장하고, VPN 성능으로 2Gbps를 보장한다. 세션 수는 방화벽일 경우에 최대 512,000세션과 VPN일 경우에 10,000세션을 동시에 지원한다. IPv4/IPv6 듀얼스택을 지원하며 CC인증과 국정원 보안적합성 검토를 이미 마쳤다. 각각의 보안기능별 특성은 다음과 같다.

▪ 방화벽 기능

ASCI모듈을 통한 패킷 포워딩으로 패킷 크기와 상관없이 안정적인 성능을 보장하며 분산 하드웨어기법을 이용하여 서비스 추가에 따른 성능저하 현상이 발생하지 않는다. 또한 침입탐지 및 방지모듈을 장착하면 웜 바이러스, 트로이 목마, 악성 프로그램과 같은 다양한 애플리케이션 레벨의 공격을 차단할 수 있으며 가상화 시스템, 시큐리티 존, 가상 라우터, VLAN과 같은 네트워크 세그먼트 분할기능을 제공한다.

▪ VPN 기능

암호 알고리즘으로 DES, 3DES, AES를 해쉬 알고리즘으로 MD-5와 SHA-1을 지원하며 하드웨어 기반의 VPN 가속기를 이용하여 높은 VPN성능을 보장하고 웹기반 인증, XAUTH 기반의 VPN인증, 그리고 RAIDUS 및 LDAP을 이용한 ID기반의 인증을 제공한다.

▪ IPS 기능

침입탐지 및 방지모듈을 부착하면 약 3600여개의 침입패턴을 이용하여 다양한 침입들을 탐지해내고 시그니처 기반의 오용탐지와 프로토콜, 트래픽 기반의 비정상 행위 탐지를 수행하여 오탐율 및 미탐율을 낮춘다. TCP/IP 기반의 프로토콜인 HTTP, FTP, SMTP, POP3, IMAP, DNS등에 대해 지원이 가능하고 500여개의 접근제어 선택항목을 통해 사용자의 환경에 가장 적합한 접근

제어 설정이 가능하다.

쥬니퍼 네트웍스의 NetScreen 5000시리즈 [5]는 ASIC 기반구조를 채택하여 VoIP나 멀티미디어 스트리밍 서비스와 같은 지연에 민감한 응용에 대해 높은 성능을 제공하는 방화벽 장비이다. NetScreen 시리즈는 하나의 네트워크가 여러개의 논리적 보안 도메인으로 분리되어 각각의 도메인별로 가상라우터, 정책집합, 주소록, VPN들을 가지는 가상화 시스템을 500개 까지 지원한다. 이 제품군은 다양한 시그니쳐와 프로토콜 기반 이상행위 탐지 기법을 이용하는 침입방지 소프트웨어를 설치할 경우에 다양한 애플리케이션 레벨 공격들이 네트워크에 영향을 미치지 못하게 할 수 있으며 OSPF, BGP, RIPv2와 같은 동적라우팅 및 RPF, IGMP, PIM SM, PIM SSM과 같은 멀티캐스트 프로토콜들을 지원한다.

NetScreen 시리즈는 방화벽 성능으로 최대 30Gbps를 보장하고, VPN 성능으로 최대 15Gbps를 보장한다. 세션 수는 방화벽일 경우에 최대 2,000,000세션과 VPN일 경우에 25,000세션을 동시에 지원한다. IPv4/IPv6 듀얼스택을 지원하며 CC인증과 FIPS 140-2 레벨 2 인증을 받았다. 각각의 보안기능별 특성은 다음과 같다.

▪ 방화벽 기능

ASIC모듈을 통한 패킷 포워딩으로 성능향상과 멀티미디어 응용에 대한 지원성을 향상시켰다. DoS 보호, DDoS 보호, SYN 쿠키 보호, Brute force 공격 효과 절감, 영역기반 IP 스푸핑 방지와 같은 기능을 제공하며 침입방지시스템을 설치하면 시그니쳐와 프로토콜상의 이상행위 탐지를 혼용하여 침입을 방지할 수 있다. 추가적인 웹 필터링 소프트웨어를 설치하면 URL 필터링도 가능하다.

▪ VPN 기능

암호 알고리즘으로 DES, 3DES, AES를 해쉬 알고리즘으로 MD-5와 SHA-1

을 지원하며 IKEv2와 IPSec NAT traversal을 지원한다. 인증으로 웹기반 인증, XAUTH 기반의 VPN인증, 그리고 RAIDUS 및 LDAP을 이용한 ID기반의 인증을 제공한다.

○ 체크포인트

체크포인트사가 제공하는 Power-1 [6]은 하드웨어 기반의 세가지 가속화 기술을 적용하여 방화벽, VPN, 그리고 IPS기능을 고속으로 구현한 기가비트 성능의 일체형 통합 보안 시스템이다. Power-1은 OSPF, BGP, RIP v1 과v2와 같은 동적라우팅을 지원하고 PIM-SM, PIM-DM, DVMRP와 같은 멀티캐스트 프로토콜을 지원한다. 또한 Power-1은 여러 사이트들의 중앙집중적 보안정책 관리를 위해 단일 콘솔을 두고 이를 통해 통합된 보안정책 정의 및 수정, 그리고 중앙에서 감사를 수행할 수 있다.

Power-1은 방화벽 성능으로 최대 14Gbps를 보장하고, VPN 성능으로 3.7Gbps, 그리고 IPS 성능으로 6.1 Gbps를 보장한다. 동시세션 수로 최대 1,100,000세션을 동시에 지원하며 사용자수에 제한을 받지 않는다. IPv4/IPv6 듀얼스택을 지원하며 CC EAL4 인증을 받았다. 각각의 보안기능별 특성은 다음과 같다.

▪ 방화벽 기능

CoreXL, SecureXL, ClusterXL과 같은 3개의 가속화 기법들을 사용하여 보안검사를 신속하게 수행하며 고가용성을 제공한다. 200여개의 다양한 프로토콜들에 대해 보호하며 SIP, H.323, MGCP와 같은 VoIP 프로토콜은 물론 Gnutella, BitTorrento와 같은 P2P 프로토콜을 지원한다.

▪ VPN 기능

암호 알고리즘으로 3DES, AES를 해쉬 알고리즘으로 MD-5와 SHA-1을 지원하며 하드웨어 기반의 가속기를 이용하여 높은 VPN성능을 보장하고 패스

워드기반 인증, RAIDUS 및 LDAP을 이용한 ID기반의 인증, 그리고 X.509기반의 인증을 제공한다.

▪ IPS 기능

침입탐지 기능에서는 시그니처 기반의 오용탐지와 프로토콜, 트래픽 기반의 비정상 행위 탐지를 수행하여 오탐율 및 미탐율을 낮춘다. TCP/IP 기반의 다양한 프로토콜들에 대해 지원이 가능하고 DNS cache poisoning, FTP bounce, 부적절한 명령들을 차단할 수 있다.

○ F5 네트웍스

F5네트웍스가 제공하는 BIG-IP [7]는 입증된 L7 스위치 본연의 로드 밸런싱 기능 외에 단일의 포인트 장비 수준의 높은 보안 성능과 가속 기능 및 애플리케이션 스위칭을 제공하는 통합 솔루션이다. BIG-IP는 최대 12Gbs의 L7 처리용량과 초당 58,000 SSL 트랜잭션 및 초당 8Gb의 하드웨어 압축을 수행한다. IPv6 Gateway모듈을 통해 IPv4주소와 IPv6 주소의 동시사용을 지원하며 IPv4 종단노드와 IPv6 종단노드 간의 트래픽 변환을 수행할 수 있다. 또한 BIG-IP는 RIP, RIPv2, OSPF, OSPFv3, IS-IS와 같은 다양한 동적 라우팅 프로토콜들을 지원한다.

BIG-IP는 네트워크 단의 보안 기능으로 대량 공격을 막아 기업 내 보안을 개선시킨다. 특히 유니버설 인스펙션 엔진(Universal Inspection Engine)과 F5 솔루션의 강력한 기능중의 하나인 iRules를 통해 각 기업의 보안 정책을 인텔리전트하게 관리하고 구현할 수 있게 해준다. DoS와 DDoS 공격 및 프로토콜 탬퍼링 공격과 같은 일반적인 네트워크 공격에 대한 보호 기능은 BIG-IP의 패킷 필터링 기능과 결합해 기업들이 생산성과 수익 및 낮은 TCO를 달성할 수 있도록 해준다.

BIG-IP는 다음과 같은 특성들로 기업 내 네트워크 인프라의 보안성을 만족시

킨다.

▪ Deny-by-default(디폴트에 의한 거부)

BIG-IP는 서버 및 애플리케이션 단에서 디폴트로 차단하는 고유의 디폴트 아키텍처로 인지할 수 있는 종류의 트래픽을 제외한 모든 트래픽은 거부된다. BIG-IP를 통해 통과할 수 있도록 허가되는 트래픽을 제어할 수 있기 때문에 극히 엄격한 보안성을 제공한다.

▪ 자동 방어

BIG-IP는 일반적인 공격 형태에 대해 네트워크를 보호할 수 있도록 다양한 빌트인 프로세스를 보유하고 있다. BIG-IP는 스머프(smurf)와 프래글(fraggle) 공격을 시작하는 브로드캐스트 ICMP 에코에 반응하지 않으며 서브넷 상으로 브로드캐스트되어지는 공격을 차단한다. BIG-IP의 커넥션 테이블은 기존의 연결과 함께 LAN 공격과 같은 스푸핑 연결이 서버로 통과되지 않도록 해준다. BIG-IP는 일반적인 Teardrop, Boink, Bonk, Nestea와 같은 분산 공격을 막을 수 있도록 proper-frame alignment를 위해 체크하는 기능을 갖추고 있다. WinNuke, Sub7, Back Orfice와 같은 다른 위협들도 포트의 디폴트 차단을 통해 막을 수 있다. BIG-IP는 또 중복되는 TCP 분할과 IP 조각을 다시 모으는 기능을 제공해 기업들은 오늘날 더 기승을 부리고 있는 새로운 공격에 대해서도 네트워크를 보호할 수 있도록 해준다.

▪ 씬 체크(SYN CHECK)

씬 플러딩은 시스템의 리소스를 고갈시켜 합법적인 연결을 방해하는 DoS 공격의 한 형태다. BIG-IP의 씬 체크 기능은 서버 대신 BIG-IP에서 클라이언트 리퀘스트의 응답에 쿠키를 보냄으로써 씬 플러딩을 완화시킨다. 이 독특한 기능은 공격은 배제시키고 서버들에게 합법적인 연결만 진행시키도록 하고 일반적인 TCP 커뮤니케이션을 지속할 수 있도록 해준다. 씬 체크 기능은 BIG-IP의 다이내믹 리핑(Dynamic Reaping) 기능을 이용해 확인된 연결 플러딩을 처리한다. 씬 체크는 고성능 씬 캐시(SYN-cache)와 함께 실행되어 TCP

옵션의 손실없이 씬 쿠키를 사용할 수 있도록 해준다.

▪ DoS와 DDoS 방어

BIG-IP는 손쉽게 적용할 수 있는 립(reap) 연결을 사용할 수 있도록 해주는 두 종류의 글로벌 셋팅을 제공한다. DoS 공격을 막기 위해 리핑 연결을 위한 낮은 감지 수준과 높은 감지 수준을 규정할 수 있으며 또한 요즈음 기승을 부리고 있는 다양한 형태의 애플리케이션 레벨의 공격을 매우 효과적으로 차단해준다.

▪ 가상화 서버 상에서의 연결 제한

BIG-IP는 가상화 서버로의 최대 연결 수를 제한할 수 있다. 이로써 DoS와 같은 사용 공격에 대한 또 다른 방어 계층을 제공할 수 있다.

▪ 프로토콜 검열

BIG-IP의 프로토콜 검열 기능으로 서버 리소스를 장악해 사이트를 다운시키는 공격을 실행하는 IP 프로토콜 탬퍼링을 사용하는 해커들로부터 네트워크를 보호할 수 있다. BIG-IP는 클라이언트와 서버 사이의 모든 TCP 연결을 방어하고 차단하는 최초의 라인이 되어 적절치 않은 패킷 플러드, MSS tiny 패킷 플러드 및 TCP 윈도우 탬퍼링과 같은 공격들을 차단할 수 있다. BIG-IP는 또 BIG-IP ASM, PSM 장비와 함께 HTTP 헤더 평가, RFC 침입 매치, 프로토콜 집행, URL 메타 캐릭터 및 캐릭터 셋 평가 등을 포함한 검사가 가능할 수 있도록 확장할 수 있다.

▪ 패킷 필터링

BIG-IP의 개선된 패킷 필터 엔진은 딥 패킷 인스펙션을 제공하고 강화된 패킷 필터링 규정을 기반으로 트래픽을 허용, 폐기 또는 거부할 수 있도록 해준다. 이러한 규정은 신뢰할 수 있는 트래픽만 허용하는 L4 필터링을 실행하고 보안 정책에 따라 특수한 트래픽 형태를 관리할 수 있도록 한다. 또 기본적인 방화벽 기능을 제공하여 IPv4와 IPv6를 함께 패킷 필터링 할 수 있어 보안의

수준을 한 단계 높일 수 있다.

▪ 감사와 로깅

BIG-IP는 예외적인 경우 또는 랜드(Land) 공격, 스머프 공격, 배드 체크섬(bad checksums), 제어가 불가능한 IP 프로토콜 번호나 버전 등 효력이 없는 매개변수에 기인해 폐기된 패킷과 관련된 이벤트를 로깅한다. BIG-IP의 보안 리포트는 권한이 없는 접근 시도의 소스 IP 주소, 사용된 포트, 그러한 시도의 빈도를 모니터링해 권한이 없는 접근 시도를 받아들이는 서비스와 포트를 인지한다. 이 정보는 보안 네트워크에 생긴 틈을 발견하고 공격 소스의 기준을 정하는 데 유용하다.

▪ 레이트 쉐이핑(Rate Shaping)

이 기능은 대역폭을 고갈시키는 공격에 대해 강력하고 유연한 해결책을 제시한다. 전송률 분류와 전송률 필터를 함께 사용해 네트워크와 애플리케이션을 무력화시키는 트래픽을 차단하고 네트워크 리소스를 고갈 시키는 불량한 사용자들과 네트워크 공격을 통제한다.

1.2.2 국산 IPv6 지원장비 동향

○ 안철수 연구소

Absolute 1000 [8]은 다양한 보안 기능(Firewall, IDS/IPS, IPsec VPN, Anti-virus, Anti-Spam, QoS)을 단일 장비(Appliance)에서 구현한 하드웨어 일체형 통합보안시스템으로 자체 개발한 전용 장비 및 전용 OS를 사용하며, 보안 정책 개수 및 동시 접속 세션 수에 독립적인 성능을 보장한다. 또한, 웹 UI를 통한 편리한 운영 및 LED/LCD를 통한 시스템 상태 정보 및 성능 파악이 가능하며, Firmware Update시 OS 재설치가 불필요하다.

Absolute 1000은 방화벽 성능으로 최대 2Gbps를 보장하고, 세션 수는 방화벽

일 경우에 1,500,000세션과 VPN일 경우에 15,000세션을 동시에 지원한다. IPv4/IPv6 듀얼스택을 지원하며 2007년 1월 15일에 IPv6 Ready Phase-2 인증을 획득했고 CC인증과 국정원 보안적합성 검토를 이미 마쳤다. 각각의 보안 기능별 특성은 다음과 같다.

▪ 방화벽 기능

고속 패킷 분류 알고리즘을 이용하여 보안정책 개수 및 동시접속 수에 무관한 성능을 지원하며 부하분산기법을 이용하여 애플리케이션 프록시로 동작 시에도 고속의 패킷처리 및 안정적인 서비스를 제공한다. 또한 트래픗 쉐이핑, 폴리싱을 동시에 제공하여 QoS 서비스 제공시에 다양한 보안정책 수립이 가능하다. 또한 한 기관에 여러대의 동일장비를 도입하는 경우에 설정동기화 기능을 제공하며 링크 집약(Link Aggregation) 및 VLAN 등을 구성하기에 적합하다.

▪ VPN 기능

암호 알고리즘으로 3DES, AES, SEED를 해쉬 알고리즘으로 SHA-1, HAS-160을 지원하며 하드웨어 기반의 VPN 가속기를 이용하여 높은 VPN성능을 보장하고 기본으로 IKEv2를 지원한다.

▪ IDS 기능

1400여개의 침입탐지 패턴을 통해 침입을 감지하고 대응하며 패턴의 자동업데이트를 통한 신속한 대응체계를 가지고 있다. 모든 TCP/IP 기반의 프로토콜 및 NetBIOS 프로토콜에 대해 지원이 가능하고 우회공격에 대한 탁월한 탐지율을 보이며 트래픽 임계치에 의한 패턴에 없는 이상징후를 감지해 낸다.

Absolute 1000은 IPv6 포럼의 Phase-2인증을 받았기 때문에 장비자체는 IPv6를 지원가능 하지만, 그 장비가 실제로 IPv6 트래픽이 유통되는 망에 연동된 사례는 없다. 따라서, 해당장비를 도입하여 IPv6망을 구축할 때에는 보다 면밀한 조사와 테스트가 필요할 것으로 사료된다.

○ 시큐아이 닷컴

NXG 2000 SE [9]는 하드웨어 일체형으로 국가정보원 및 Tolly 그룹으로부터 인증을 획득한 기가비트 방화벽이다. 독자적인 Classification Algorithm을 적용하여 Rule과 Session 수에 관계없이 기가비트 네트워크 성능를 유지한다. Active-Active High Availability로 안정성 향상 및 이중화와 동시에 로드밸런싱으로, 네트워크를 안정적이며 효과적으로 운영 가능하다. Firewall 및 VPN 기능이 결합된 통합 네트워크 보안 솔루션으로 분산된 보안 요구사항을 하나의 장비에서 구현하였다. 전용 암호화 가속칩을 탑재함으로써 IPSec 통신의 고성능 처리가 가능하다.

NXG 2000 SE는 방화벽 성능으로 최대 2Gbps를 보장하고, VPN성능으로 최대 1.5Gbps를 보장한다. 세션 수는 방화벽일 경우에 1,500,000세션과 VPN일 경우에 20,000세션을 동시에 지원한다. IPv4/IPv6 듀얼스택을 지원하며 2005년 8월 1일에 IPv6 Ready Phase-2 인증을 획득했고 CC인증과 국정원 보안적합성 검토를 이미 마쳤다. 각각의 보안기능별 특성은 다음과 같다.

▪ 방화벽 기능

고속 패킷 분류 알고리즘을 이용함으로써 높은 성능을 보장하며 동적 규칙 집합의 적용으로 융통성이 뛰어나다. 동적 포트를 이용한 응용 프로그램과의 안전한 채널확보가 가능하며 내부 및 외부 DNS를 분리할 수 있는 기능을 제공한다.

▪ VPN 기능

암호 알고리즘으로 3DES, AES, ARIA, SEED를 해쉬 알고리즘으로 SHA-1, HAS 160을 지원하며 IPSec의 L2TP와 NAT Traversal을 지원한다.

Absolute 1000의 경우처럼 NXG 2000 SE도 IPv6 포럼으로부터 Phase-2인증

을 받았고 장비 자체는 IPv6를 지원한다. 하지만, 해당장비를 이용해서 실제 IPv6 망을 구축하고 다른 IPv6망과 연동된 사례가 없다. 즉, IPv6 트래픽이 흐르는 망에 연동된 경험이 없으므로, 아직은 확실한 검증이 안된 상태이다.

○ 퓨쳐시스템

2005년부터 한국정보사회진흥원이 KOREAv6 시범 서비스 사업의 일환으로 추진하는 "홈네트워크 IPv6 시범 서비스"의 사업자로 선정된 퓨쳐시스템은 2005년 11월까지 시범서비스를 수행했으며, 정보보호 업계에서는 처음으로 2005년 6월 국제 IPv6포럼이 부여하는 'IPv6 Ready Logo'를 획득했다.

또한 퓨쳐시스템은 TTA로부터 IPv6 Home Gateway 제품과 시큐웨이게이트 6000제품에 대해서 Conformance & Interoperability 운용시험을 받아 TTA Verified 인증서를 수령하여 IPv6에 대한 적합성 시험도 검증 받았다.

최근에, 퓨쳐시스템이 개발한 WeGuardia XTM 시리즈 [10] 는 멀티코어를 기반으로 개발된 확장형 통합위협관리 제품으로 자체적인 하이브리드형 소프트웨어 프레임워크(FOHSAM: Future's Optimum Hybord Software Architecture for Multicore environment)를 적용하여 다양한 암호화 알고리즘을 고속으로 처리한다. 가상화 기술을 적용함으로써 확장형 보안플랫폼을 제공하여 추가 보안장비의 구입 없이 다양한 보안기능을 구현가능하고 이에 따라 고가용성 및 관리효율성을 높인다. IPv6 기능으로 IPv4/IPv6 듀얼스택, IPv6-in-IPv4 터널링, NAT-PT, 6-to-4와 같은 IPv6 전환기술을 모두 지원한다.

WeGuardia XTM 시리즈는 방화벽 성능으로 최대 10Gbps를 보장하고 IPS성능으로 최대 5Gbps를 제공한다. 세션 수는 방화벽일 경우에 최대 2,000,000세션과 VPN일 경우에 최대 20,000세션을 동시에 지원한다. 현재 WeGuardia XTM 시리즈는 IPS와 VPN기능의 CC인증을 신청한 상태이며 향후에 국정원 보안적합성 검토를 거칠 예정이다. 각각의 보안기능별 특성은 다음과 같다.

▪ 방화벽 기능

가상방화벽 기능을 제공함으로써 VLAN별 방화벽 정책적용이 가능하고 독립적인 방화벽으로 운영이 가능하다. 동적인 필터링 기능, Stateful Inspection 기반 패킷필터링, 사용량 기반 필터링, 패턴기반 필터링 등을 지원하여 정교한 패킷제어를 지원한다. RADIUS와 LDAP에 연동되는 사용자 기반 보안정책을 통해 정책관리의 용이성 및 내부해킹자를 용이하게 탐지한다.

▪ VPN 기능

암호화 알고리즘으로 3DES, SEED, AES, FACE를 지원하며 해쉬 알고리즘으로 MD5, SHA-1, HAS-160을 지원한다. 다중 SA를 지원하여 다중 IPSec터널 구성이 가능하고 IKEv2를 지원한다.

▪ IPS 기능

시그니처 기반의 오용탐지와 프로토콜, 트래픽 기반의 비정상 행위 탐지를 수행하여 오탐율 및 미탐율을 낮춘다. 다중 패턴매칭 알고리즘을 사용하고 하드웨어 기반의 패턴매칭 가속기를 통해 빠른 탐지 및 대처를 지원한다. 실시간 시그니처 업데이트를 통해 새로운 침입패턴에 대한 신속한 대응방안 마련 및 적용이 가능하도록 지원한다.

WeGuardia XTM 시리즈는 다른 국산 통합보안 장비들과는 다르게 방화벽 기능은 물론 IPS와 VPN까지도 IPv6를 지원한다. 또한, 이 장비들은 다양한 시험환경을 통해 IPv6 트래픽 테스트를 거쳤으므로, 어느 정도는 검증되었다. 그러나 이러한 테스트들은 IPv6 Lab 환경 구축에 의한 테스트이므로 이들이 실제 IPv6 망에 연동되어 운영될 때에도 완벽한 기능을 지원할지 혹은 문제가 발생하지 않을지는 아직 미지수이다. 따라서, 이 장비군의 실제 망구축 및 운영에 따른 검증을 위해서는 IPv6 트래픽이 흐르는 망에 연동시켜 테스트해볼 필요가 있다.

1.2.3 IPv6 지원장비 요약 및 비교

본 절에서는 IPv6 지원 장비들의 성능, IPv6 지원여부, CC인증 및 국정원 보안성 검토 획득여부, 침입방지 및 탐지기능 구현여부 등을 국산 및 외산장비별로 비교하고 2개의 표로 정리·요약 한다.

[표 2]과 [표 3]에서 보는 것처럼, 국산장비들은 처리능력, 동시지원 세션수, 지원 인터페이스 수, 그리고 침입탐지 및 방지지원 기능 등이 모두 외산장비들에 비해 더 뛰어나다. 즉, 기술적인 면에서는 국산 장비들에 외산 장비들에 비해 결코 떨어지지 않고 오히려 더 우수한 성능을 보인다는 것이다. 그러나, 문제는 이러한 국산장비들이 실제로 IPv6망과 연동되어서 동작할 때에도 원활하게 동작할지는 알 수 없다는 것이다. 몇몇 장비 업체들은 자신들의 장비가 자체적인 IPv6 시험테스트를 모두 통과했으므로 문제가 없을 것이라고 주장하고 있다. 하지만 그러한 테스트들은 단순한 수준의 네트워크 환경을 구축하고 테스트를 수행한 것이므로 충분한 신뢰성을 가진다고 보증할 수 없다. 따라서, 보다 완벽하고 실질적인 IPv6 지원여부 확인을 위해서는 실제 IPv6 트래픽이 유통되는 망에 연동시켜 테스트를 수행할 수 있는 환경이 제공되어야 한다. 국산장비들이 이러한 실질적인 망 연동 테스트를 통과한 경우에는 기술적으로 외산장비보다 더 높은 경쟁력을 가지므로, 국내시장의 점유율을 크게 늘리는 효과를 가져올 것이다. 향후에 IPv6를 지원하는 장비 개발업체들에게 실질적인 테스트 환경이 제공된다면, 개발한 장비들의 실질적 검증이 가능하므로 장비자체의 고도화 및 경쟁력 측면에서 외산장비에 비해 우위를 점하게 될 것이다. 이를 통해 국산장비산업을 활성화시키고 관련 정보보호산업의 발전을 견인할 것으로 기대된다.

[표 2] IPv6 지원 국산 보안장비 비교

구 분		Absolute 1000	NXG2000 SE	WeGuardia XTM 8000
제 조 사		안철수연구소	시큐아이닷컴	퓨처시스템
Throughput	Firewall	2Gbps	2Gbps	4Gbps
	VPN	-	1.5Gbps	-
Session	Firewall	1,500,000	1,500,000	500,000
	VPN	15,000	20,000	10,000
CPU/메모리	프로세서	Dual Xeon	Dual Xeon 2.8Ghz	Intel Core2Quad
	메모리	4G	1G	1G
	플래쉬메모리	-	-	1G
인터페이스	10/100/1000	4	1(10/100B-T) 4(1000B-T)	6(10/100/1000)
	1G(optic)	8	4(1000B-SX)	4(1000B-SX)
	10G(optic)	-	-	-
라우팅 프로토콜	BGP	-	×	○(IPv4)
	OSPF	-	○	○
VLAN 지원		-	○	○
WAF 지원		-	-	○
IPv6	듀얼스택	○	○	○
	IPv6 주소변환	-	○	○
	6 to 4 터널링	-	○	○
	매뉴얼 터널링	-	○	○
	NAT_PT 지원	-	×	○
	DHCPv6	-	×	○
	DNSv6	-	×	○
인증	IPv6 포럼	Phase-2	Phase-2	-
	CC 인증	○	○	진행중
모니터링		SNMP/Syslog	SNMP/Syslog	WebSMC/Syslog
IDS/IPS 지원		○	○	○
QoS 지원		○	○	○
장비 사진				

[표 3] IPv6 지원 외산 보안장비 비교

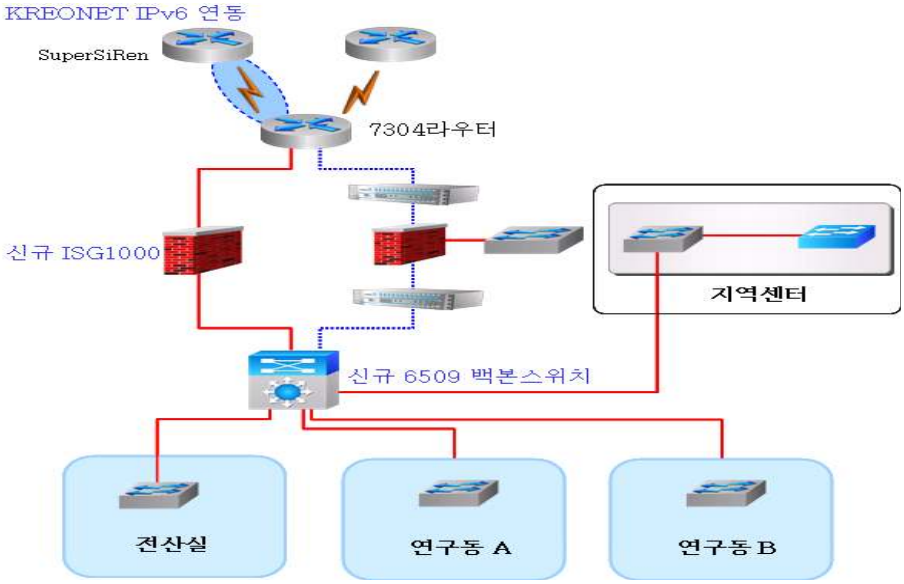
구 분		ASA 5550	ISG1000	Power-1 5070
제 조 사		시스코	쥬니퍼	체크포인트
Throughput	Firewall	1.2Gbps	2Gbps	9Gbps
	VPN	425Mbps	1Gbps	2.4Gbps
Session	Firewall	650,000	500,000	1,100,000
	VPN	5,000	2,000	-
CPU/메모리	프로세서	-	-	-
	메모리	4G	-	-
	플래쉬메모리	64Mbyte	128M or 512M	-
인터페이스	10/100/1000	1(10/100B-T) 8(1000B-T)	Fixed 4(10/100/1000)	8+4 (optional)
	1G(optic)	4(SFP)	최대 8(SFP)	-
	10G(optic)	-	-	2 (optional)
라우팅 프로토콜	BGP	×	○	○
	OSPF	○	○	○
VLAN 지원		○	○	○
WAF 지원		×	×	○
IPv6	듀얼스택	○	○	○
	IPv6 주소변환	○	○	○
	6 to 4 터널링	○	○	○
	매뉴얼 터널링	○	○	○
	NAT_PT 지원	○	-	-
	DHCPv6	○	○	-
	DNSv6	○	-	-
인증	IPv6 포럼	Phase-2	-	-
	CC 인증	-	○	○
모니터링		SNMP/Syslog	SNMP/Syslog	-
IDS/IPS 지원		Option	○	○
QoS 지원		○	○	○
장비 사진				

2. 국내·외 IPv6 구축 사례

2.1 국내 사례

2.1.1 한국천문연구원

한국천문연구원은 천문우주를 연구하고 관련된 연구 장비와 시설을 개발하는 전문연구기관이다. 이런 천문연의 IPv4/IPv6망으로의 전환을 위해 외부망 인입 라우터의 IPv6 설정을 통해 외부 IPv6망과의 연동 기반을 마련하였고, 연구원 내 백본장비를 IPv6 지원가능한 장비로 교체함으로써 일부 영역이나 제한된 구역이 아닌 모든 호스트 장비에 대한 IPv6 설정 및 활용이 가능하게 구축하였다. 또한, IPv6 전용 방화벽을 구축하여 IPv6 서비스 외부 제공서비스의 보안성을 강화하였다.



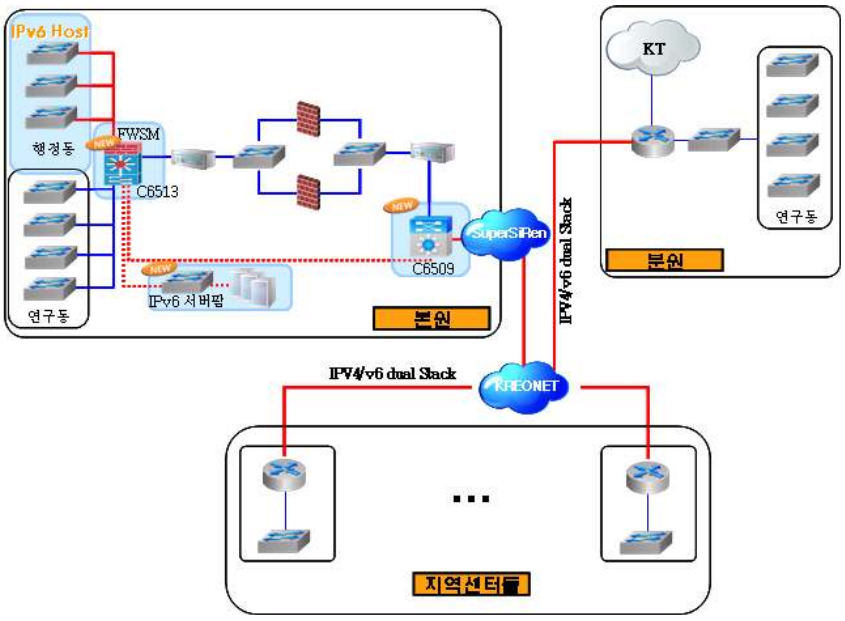
[그림 3] 한국천문연구원 IPv4/IPv6 네트워크

IPv6 외부망과의 접속을 위하여 외부망 인입라우터는 OS 업그레이드를 통해 IPv6를 설정하여 외부 IPv6망과의 연동 기반 마련하였으며, 원내 기존 백본스

위치를 Cisco Catalyst 6509로 교체함으로써 원내 망의 일부 영역이나 제한된 구역이 아닌 모든 호스트 장비에 대한 IPv6 설정 및 활용이 가능하게 하도록 하였다. 또한, IPv6 네트워크 보안을 위하여 Juniper ISG-1000 설치 및 운영하고 있다. 또한, Windows Server 2003으로 IPv6 전용 DNS를 구축하였다. [2][3]

2.1.2 한국기초과학지원연구원

한국기초과학지원연구원은 IPv4/IPv6 듀얼스택 망을 지원하기 위하여 한국기초과학지원연구원 대덕본원의 주요 네트워크 장비를 IPv6 지원가능 장비로 교체하였으며, 지역센터의 네트워크 시스템 IPv6 지원토록 변경하였다. 대덕본원 및 지역센터들를 연계하는 IPv6망을 구축하였다.



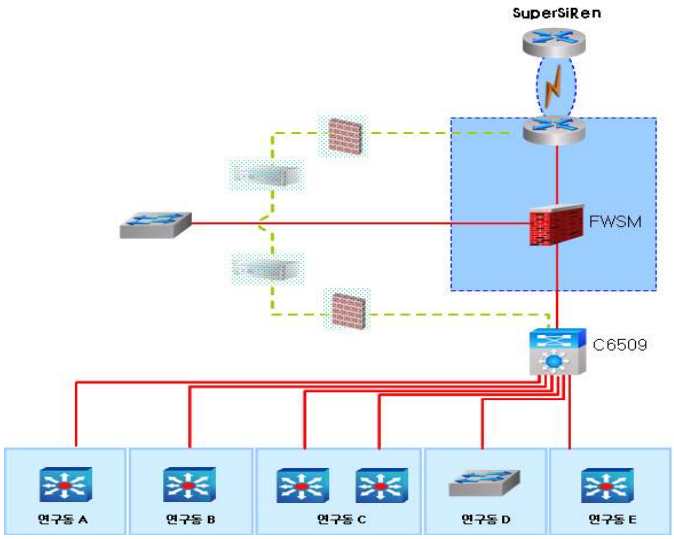
[그림 4] 한국기초과학지원연구원 IPv4/IPv6 네트워크

기존 운영중인 백본스위치(Cisco Catalyst 6509)에 IPv6 스택을 올려 IPv6를 지원하게 하였고, 기존 Cisco Catalyst 6509에 모듈형 IPv6 방화벽인 FWSM를 탑재하여 보안을 강화하였다. 또한, 대전 본원을 비롯한 지역센터간의 IPv6

지원을 가능하게 구성하여 전국적인 규모의 IPv6 네트워크 구축하였고, IPv6 주소 할당은 지역센터별로 /64단위로 분할하여 할당하였다. 아울러 본원 및 지역센터간에는 IPSec VPN를 통한 암호화 통신체계를 구축 운영하고 있다. [2][3]

2.13 국가핵융합연구소

급속히 성장하고 있는 핵융합분야의 인프라의 확충에 따라 분석데이터와 각종 연구결과물의 저장 및 처리와 국내/외 원격공동연구를 위한 인프라로 활용하기 위하여 IPv6 전환망을 구축하고자 하는 국가핵융합연구소는 IPv4/IPv6 전환망을 구축하였으며, KSTAR 운전상황 모니터링 서비스를 IPv6 용으로 구축하였으며, IPv6 DNS를 구축하였다.

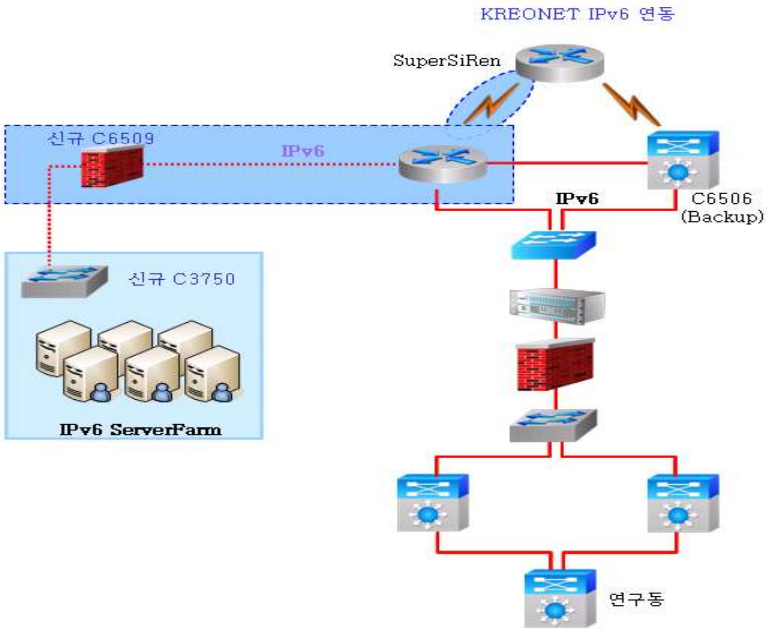


[그림 5] 국가핵융합연구소 IPv4/IPv6 네트워크

IPv6 전환 계획은 연구소내 일부구간에만 IPv6를 적용하려 하였으나 적용 범위를 확대하여 현재 연구소 전체에 IPv6망을 사용할 수 있는 환경으로 구축하였다. Cisco Catalyst 6509 라우터와 모듈형 방화벽인 FWSM를 이용하여 IPv6 전환망을 구축하였다. [2][3]

2.1.4 한국항공우주연구원

우리나라 항공우주 분야의 연구개발을 주도하는 항공우주연구원은 신기술인 IPv6 기술의 선도적 도입으로 대덕특구내의 타 연구기관으로의 IPv6 기술 확산의 기반과 향후 항공우주분야에 활용하고자 IPv6 전환망을 구축하였다. 이를 위하여 IPv4/IPv6 듀얼스택 전환망을 구축하였으며, IPv6용 항공우주연구원 홈페이지를 구축하였다.



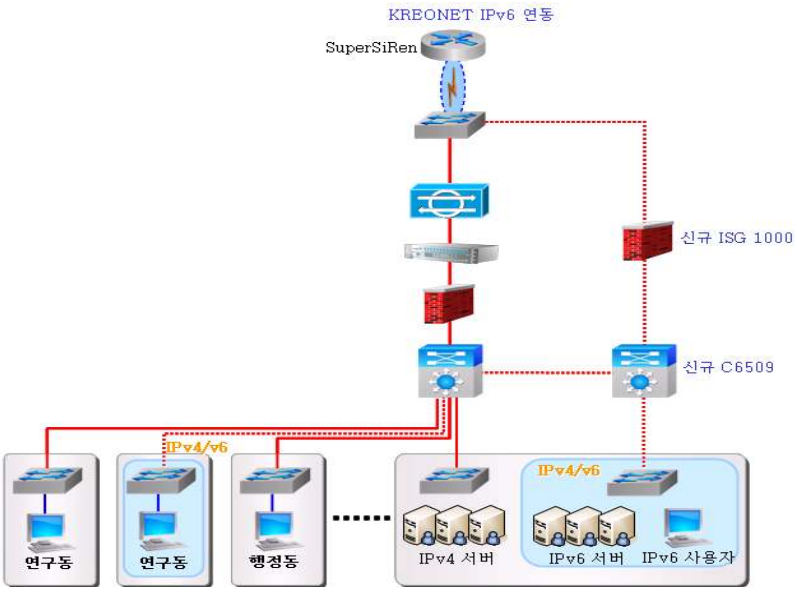
[그림 6] 한국항공우주연구원 IPv4/IPv6 네트워크

내부망은 Cisco Catalyst 6509 및 모듈형 방화벽인 FWSM를 이용하여 IPv6망을 구축하였다. 중국으로부터 해킹을 방지하고자 발신지가 중국으로 되어있는 IP를 차단하였다. [2][3]

2.1.5 한국표준과학연구원

국가측정표준 확립 및 유지, 국가측정표준 보급, 표준과학기술 연구개발, 측

정표준 국제보증 등의 국가로부터 부여받은 임무와 시대의 변천 과학기술의 발전에 따라 새롭게 요구되는 임무들을 IPv6망을 활용하여 보급하고자 선도적으로 IPv6 도입을 추진하였다. 표준과학연구원내 연구동 및 전산센터내 IPv4/IPv6 듀얼스택 망을 구축하였다.



[그림 7] 한국표준과학연구원 IPv4/IPv6 네트워크

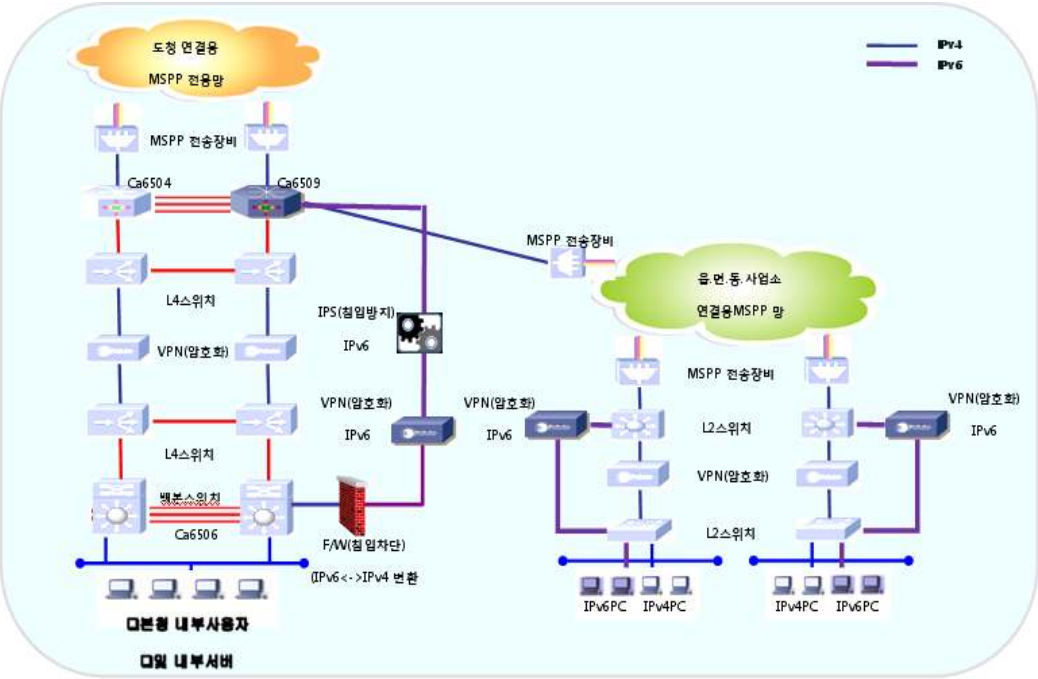
표준연구원 Cisco Catalyst 3750 L3 Switch에 IPv4/IPv6 듀얼스택을 올린 후 KREONET과 연동하고, 신규 Cisco Catalyst 6509 백본 스위치를 IPv6로 연결을 구성하였다. 신규 Cisco Catalyst 6509 백본 스위치에서 라우팅을 하고 각 서버 및 네트워크 장비를 연결할 수 있도록 구성하였다. 네트워크의 보안을 위하여 Juniper ISG-1000를 연동하였다. [2][3]

2.1.6 강릉시청

차세대 인터넷 주소(IPv6) 확보가 유비쿼터스 전략의 새로운 화두로 떠오르면서 강릉시는 차세대인터넷 주소관리체계의 시급성을 인식하고, 새로운 IPv6 기반 u-city 특화형 도시전략구축을 위해 2005년부터 2007년까지 IPv6 시범사

업에 참여하였다. 그리하여 전국 지자체 최초 3년 연속 IPv6 인프라를 구축하고 IPv6 시범 특화도시 이미지를 쌓아왔다.

2008년 강릉시청은 강릉시 내·외부망 및 행정망 내 IPv6 지원 장비 도입 및 보건소·문화교육센터·주민센터(13개동) 등 15개소에 IPv6 인프라 구축, 강릉시 홈페이지에 IPv6 적용, IPv6 무선 Mesh망 이용 인터넷 무료서비스 존(경포해수욕장· u-문화스포츠타운) 이용 확산유도 등을 목표로 '공공기관 IPv6 장비 지원 사업'에 참여하였다.



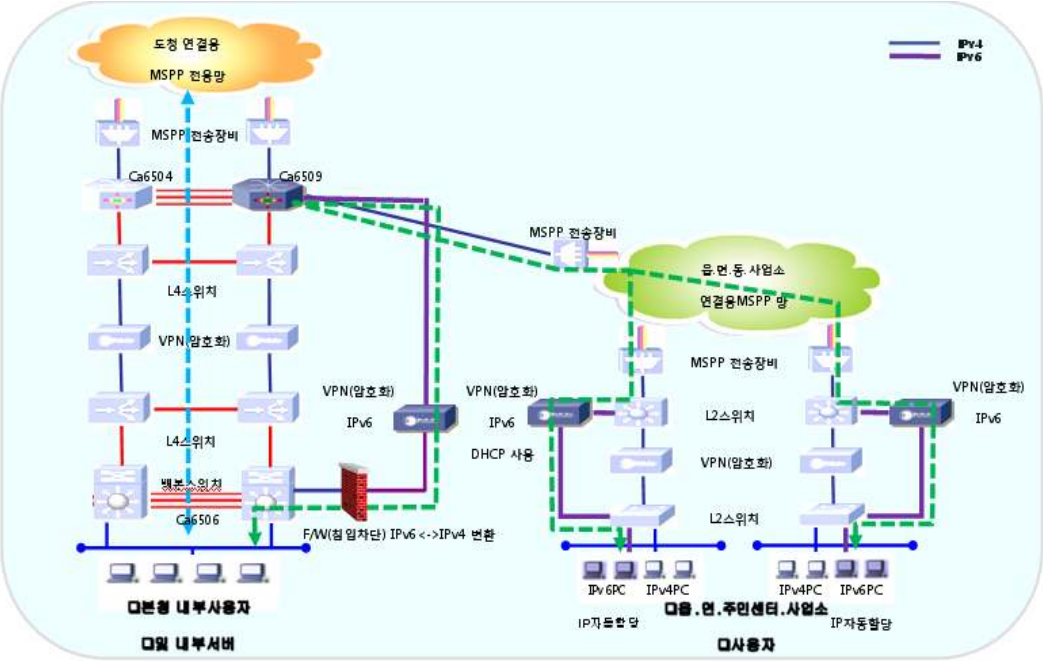
[그림 8] 강릉시청 IPv4/IPv6 네트워크

강릉시청은 내·외부망에 IPv6를 도입하기 위해 인터넷 연동 라우터를 신규 도입하고 시청과 동사무소 사이에 IPv6로 VPN 통신을 하도록 구축하였다. IPv6 IPS 장비를 구축하였고 향후의 IPv6 트래픽의 증가에 대비하여 IPS 패턴의 업데이트가 가능하도록 구성하였다. 또한 시청 내부에 IPv6↔IPv4로 변환

하는 NAT-TP 기능을 Future Systems사의 WeGuardia XTM를 사용하여 구축하였으며, 무엇보다도 KT 측에 IPv6 인터넷 접속을 요구하여 상용망인 KT Pubnet에 IPv6를 적용하였다. [2]

2.1.7 공주시청

공주시청은 내부 업무 처리를 위한 행정망과 외부 인터넷 연동망에 IPv6를 도입하였다. 공주시청은 행정망에 IPv6를 도입하기 위해 IPv6 암호화 장비 및 침입방지시스템을 신규 도입하여 본청과 읍·면 주민센터 등 26개소에 설치하고 라우터와 스위치를 IPv4/IPv6 듀얼모드로 구성하였다.



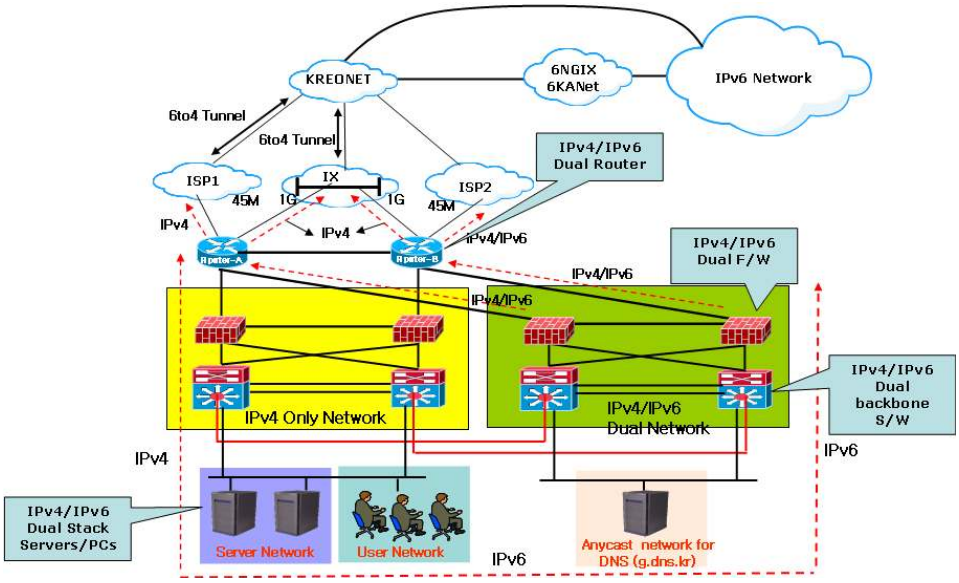
[그림 9] 공주시청 IPv4/IPv6 네트워크

공주시청은 시청과 읍·면 주민센터 등의 IPv6 단말에서 본청 서버로 접근시 해당 사업소에 있는 Future Systems사의 WeGuardia XTM 장비를 사용하여 VPN으로 암호화를 수행하고 본청의 IPv6 암호화 장비에서 복호화를 수행한 후 백본스위치에서 IPv4로 변환하여 본청 서버로 전달한다. 또한, 읍·면 주

민센터 등에서 타 시군구의 정보를 조회할 때는 본청 시군구서버로 요청을 하고 본청 시군구서버는 타시군구 서버의 정보를 검색하여 읍·면 주민센터 등에 정보를 전달하는 방식을 취하였다. [2]

2.1.8 한국인터넷진흥원

한국인터넷진흥원은 공공부문 IPv6 전환·확산 사업의 전담기관으로써 내부 네트워크 및 홈페이지에 자발적으로 IPv6를 적용함으로써 공공부문 IPv6 전환을 선도하였다. 2008년 2월에 사용자 및 서버 네트워크의 IPv6 적용을 완료하였고, 3월에 기관 대표 홈페이지 웹서버의 IPv6 전환, IPv6 DNS 구축, .KR 네임서버에 IPv6 주소 할당 및 적용을 완료하였다. 현재 IPv4/IPv6 듀얼스택으로 운영되고 있으며, 네트워크 보안을 위하여 NOKIA IP530 방화벽을 사용하고 있다. [2][16][17]

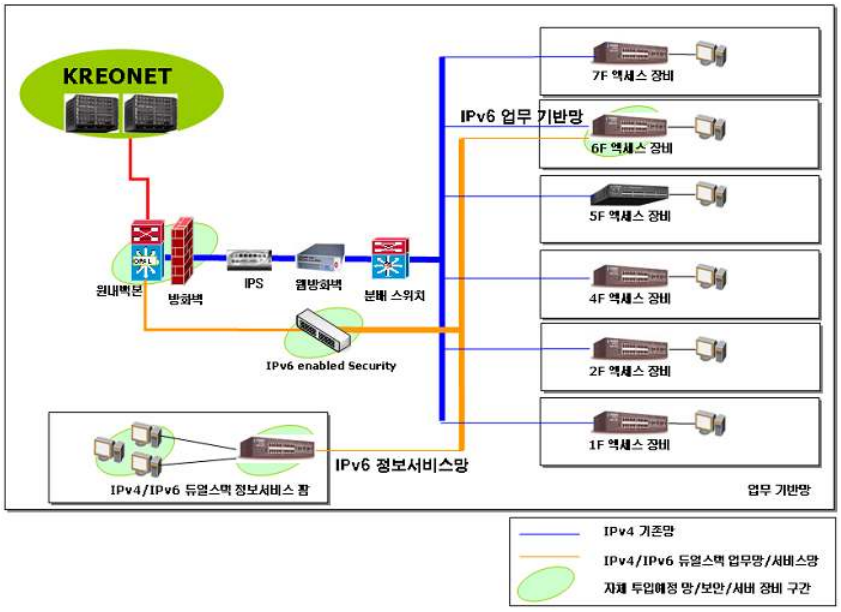


[그림 10] 한국인터넷진흥원 IPv4/IPv6 네트워크

2.1.9 한국과학기술정보연구원

한국과학기술연구원은 과학기술정보분야의 데이터베이스 및 콘텐츠 제공은

물론, 슈퍼컴퓨팅 자원, 네트워크 자원 등의 정보자원 인프라를 보유하고, 서비스를 제공 하는 기관이며, 과학기술분야의 정보제공 인프라의 선도 기관으로서, 전국 백본 및 국제 게이트웨이에 IPv6 전용 네트워크를 구축하였으며, 연구원 내의 내부망도 IPv4/IPv6 듀얼스택으로 구축하였다.



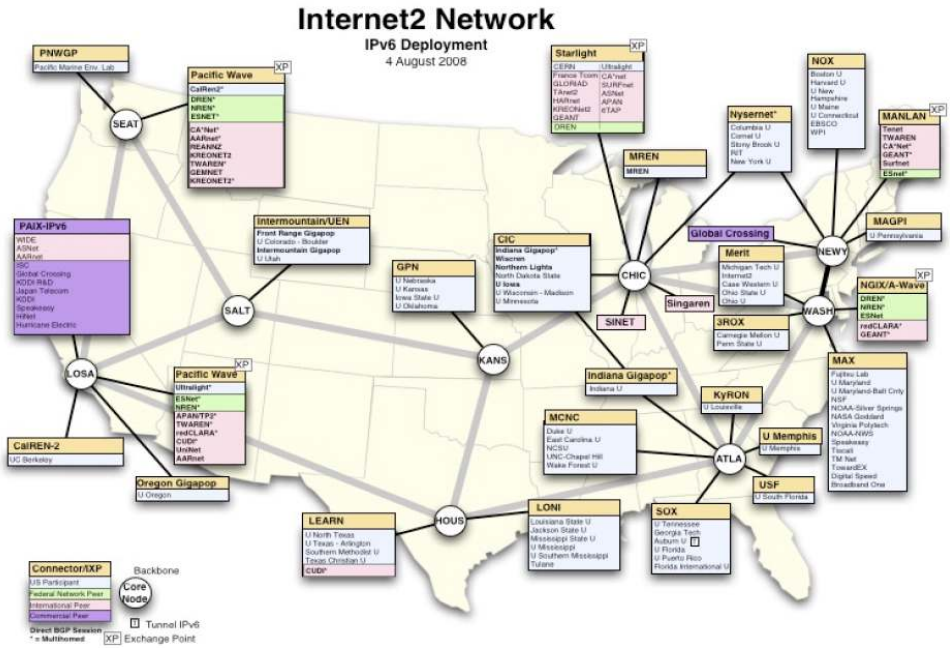
[그림 11] 한국과학기술정보연구원 IPv4/IPv6 네트워크

한국과학기술정보연구원은 Cisco Catalyst 6509 라우터 및 모듈형 방화벽인 FWSM을 이용하여 원내 백본 네트워크를 IPv4/IPv6 듀얼스택으로 전환하고, IPv6 백본 스위치를 구성하여, IPv6 정보서비스망을 구축하고, 연구원 업무망의 일부를 IPv4/IPv6 듀얼스택이 가능한 구성으로 전환하였다. [1][2][18]

2.2 해외 사례

2.2.1 Internet2 (미국)

Internet2(www.internet2.edu)는 미국 내 140 여개의 대학들이 업계 및 정부 기관과의 협력 하에 진보된 연구, 교육을 지원하는 차세대 인터넷 기술과 응용을 개발하기 위한 대학연합 주도의 공동연구 사업이다.



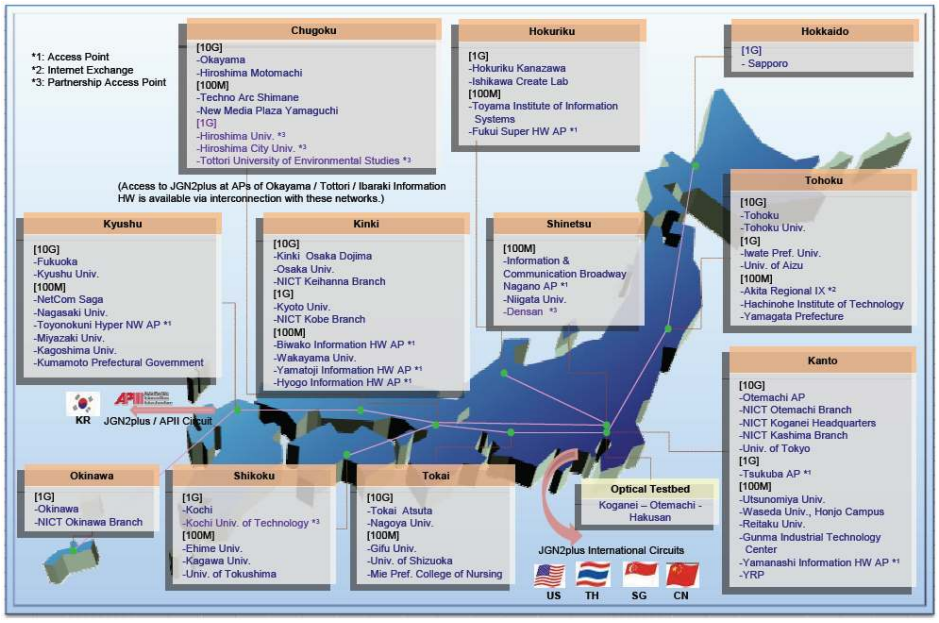
[그림 12] Internet2 IPv4/IPv6 네트워크

Internet2는 지속적으로 IPv6망을 확대 구축하고 있으며, Juniper T640 라우터를 이용하여 IPv4/IPv6 듀얼스택망을 구축하고 있다. 또한 LA의 PAIX 라우터를 통해 상용망과 상호 연동하고 있다. 향후에 상용망과의 연동은 시카고, 뉴욕, 시애틀로 확대할 예정이다. 아울러, Juniper 라우터에 설치된 방화벽 필터링을 통하여 IPv6 트래픽을 모니터링 하고 있다. [11]

- http://vixen.grnoc.iu.edu/jfirewall-viz/index-bits.html
- http://vixen.grnoc.iu.edu/jfirewall-viz/

2.2.2 JGN2plus (일본)

일본은 IPv6를 포함한 차세대 네트워크 환경을 구축하기 위하여 2000년부터 2004년까지 ATM 기반의 JGN1을 구축·운영하였으며, 이후 2004년부터 2008년까지 이더넷기반의 JGN2로 업그레이드하였다. 최근에는 2008년부터 2011년까지 운영할 JGN2plus로 업그레이드하였다. JGN2plus는 IPv4/IPv6 듀얼스택, IPv6-native 서비스를 제공할 뿐만 아니라, Layer 2 이더넷 서비스(1Gbps ~ 10Gbps)제공하며, 미국, 태국, 싱가폴, 중국, 한국과 국제적으로 연동하고 있다. [12]



[그림 13] JGN2plus IPv4/IPv6 네트워크

2.2.3 CERNET2 (중국)

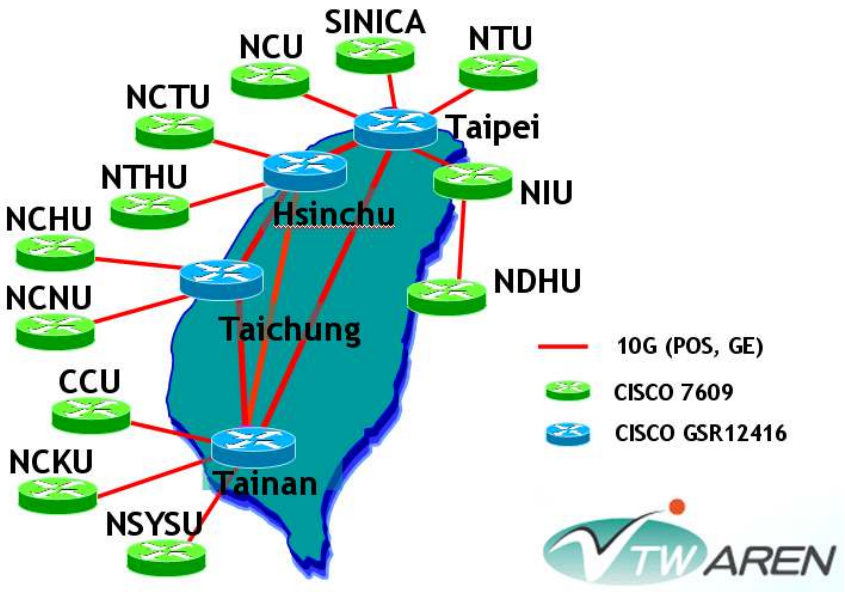
2003년에 중국 정부는 '973 프로젝트' 내에 '미래 인터넷 아키텍처 연구'의 프로젝트로 CERNET을 CERNET2로 명명하여 추진하였다. CERNET2는 순수한 native-IPv6 트래픽을 지원하도록 하고 있다.

[그림 14] CERNET2 IPv6 네트워크

CERNET2는 CNGI(China Next Generation Internet)의 백본 네트워크로서, 중국의 차세대 인터넷망이다. 중국 20개 도시에 20개의 기가팝을 운영하고 있으며 100개 이상의 대학교와 연구소들이 1Gbps ~ 10Gbps의 속도로 연동되어 있으며 국제적으로는 북미, 유럽, 아시아 지역과 2.5Gbps로 연동되어 있다. 특히 청화대학에서 자체 연구개발한 라우터 장비들을 활용하여 구축하는 등 자국 라우터설비의 사용률이 80%에 이르고 있다. [13]

2.2.4 TWAREN (대만)

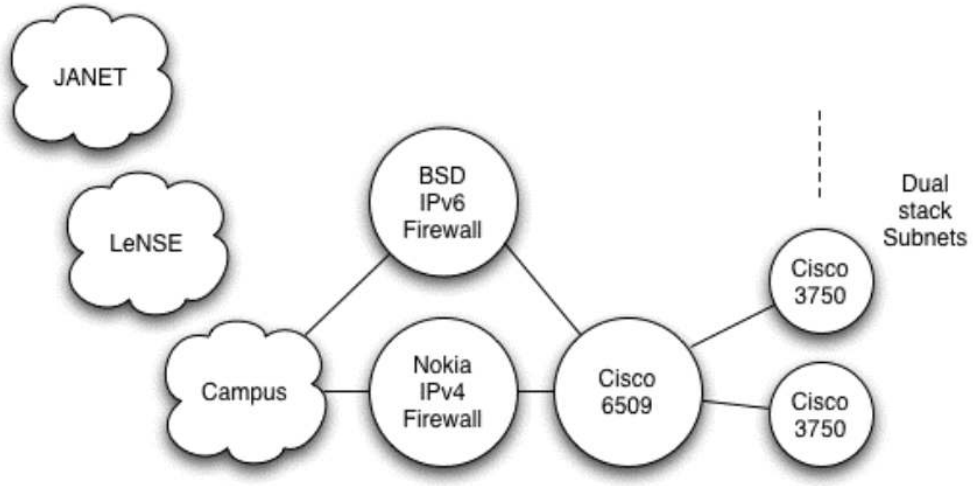
대만은 e-Taiwan 프로젝트를 통해 IPv6 개발 및 전환을 도모하고 있으며 7개 주요 ISP업체들이 IPv6 주소를 할당받아 운용하고 있고 그중에 1개 업체(HiNet)은 IPv6 기반의 상용서비스를 제공하고 있다. 또한 IPv6 교육용 네트워크인 TANet(Taiwan Academic Network)를 구축하여 학교와 연구기관들에게 IPv6 서비스 제공하고 있다. 아울러 20G급의 광 네트워크를 기반으로 한 TWAREN을 구축하여 IPv6 관련 연구개발을 진행하고 있다. TWAREN을 구축하기 위해 Cisco Catalyst 7609 라우터와 GSR 12416 장비를 사용하였다. [14]



[그림 15] TWAREN IPv6 네트워크

2.2.5 University of Southampton (영국)

총 4200명의 사용자와 1900개의 IPv4 주소를 사용하고 있는 Southampton 대학교는 기존의 IPv4망에 IPv6를 올려 IPv4/IPv6 듀얼스택 네트워크를 구축하였다. 총 50대의 Cisco Catalyst 3750 스위치/라우터를 사용하였으며, 외부용 라우터 장비로 Catalyst 6509를 이용하여 구축하였다. 기존의 IPv4망에서는 Checkpoint사의 방화벽을 사용하였으나, 구축당시 본 장비는 IPv6를 지원하기 않는 관계로 IPv6용 방화벽으로 BSD IPv6 방화벽을 사용하였다. 또한, Snort v2.8.0를 이용하여 IDS를 구축하였으나, 현재 특정한 룰이 적용되어 있지는 않은 상태이다. 아울러, DNS, www, login 등과 같은 핵심 서비스들에 듀얼스택을 올려 서비스 제공하고 있다.



[그림 16] University of Southampton IPv4/IPv6 네트워크

2.2.6 GEANT (유럽)

GEANT은 유럽 30개국의 26개 주요 국가 연구교육망(NREN)을 상호 연동하여 멀티 기가비트 범유럽 데이터 통신 네트워크를 구축하는 프로젝트이다. 2004년 9월부터는 GEANT2로 발전하여 현재 34개국 국가 연구교육망들이 연동되어 있다. GEANT은 Juniper Networks사의 M160과 M40 라우터와 Cisco Systems사의 Catalyst 7500 장비로 IPv4/IPv6 듀얼스택망을 구축하고 운영하고 있다.

NREN으로서는 2003년 1월에 RedIRIS(스페인), RENATER(프랑스)가 처음으로 GEANT IPv6에 연동하였고, 2003년 9월까지 대부분의 NREN들이 GEANT IPv6에 연동하였다. 이후 2004년 8월에는 4개의 추가적인 NREN과 CANARIE 및 SINET이 연동되었다. 현재 대부분의 NREN이 IPv6-tunneling보다는 IPv6-native 방식으로 연동되어 있다. 주요 NREN의 IPv6 연동방식은 다음과 같다. [15]

○ European NRENs

Peer	Connection Type	Connection Date
ACONET	Tunnel	13/05/2003
ARNES	Native	22/07/2003
BELNET	Native	29/07/2003
CARNET	Native	10/03/2004
CERN	Native (since 02/09/2004)	09/05/2003
CESNET	Native	30/07/2003
CYNET	Native	10/12/2004
DFN	Tunnel	16/09/2003
EEnet	Native	09/05/2003
FCCN	Native	22/04/2003
GARR	Native	29/04/2003
GRnet	Native	31/07/2003
HEAnet	Native	23/04/2003
HUNGARNET	Native (since 19/04/2004)	10/06/2003
IUCC	Native (since 05/01/2004)	29/04/2003
ISTF	Native	17/03/2005
JANET	Native	10/06/2003
SigmaNet	n/a	n/a
LITNET	Tunnel	06/05/2003
University of Malta	Native (since 26/1/2006)	29/03/2005
NORDUnet	Native	25/08/2003
PSNC	Native	06/05/2003
RBnet	Native	17/09/2003
RedIRIS	Native	10/04/2003
RENATER	Native	15/04/2003
RESTENA	Native	18/06/2003
RoEduNet	Native	09/05/2003
SANET	Native	18/10/2004
SURFnet	Native	22/04/2003
SWITCH	Native (since 09/03/2004)	09/05/2003
Ulakbim	Native	30/05/2003

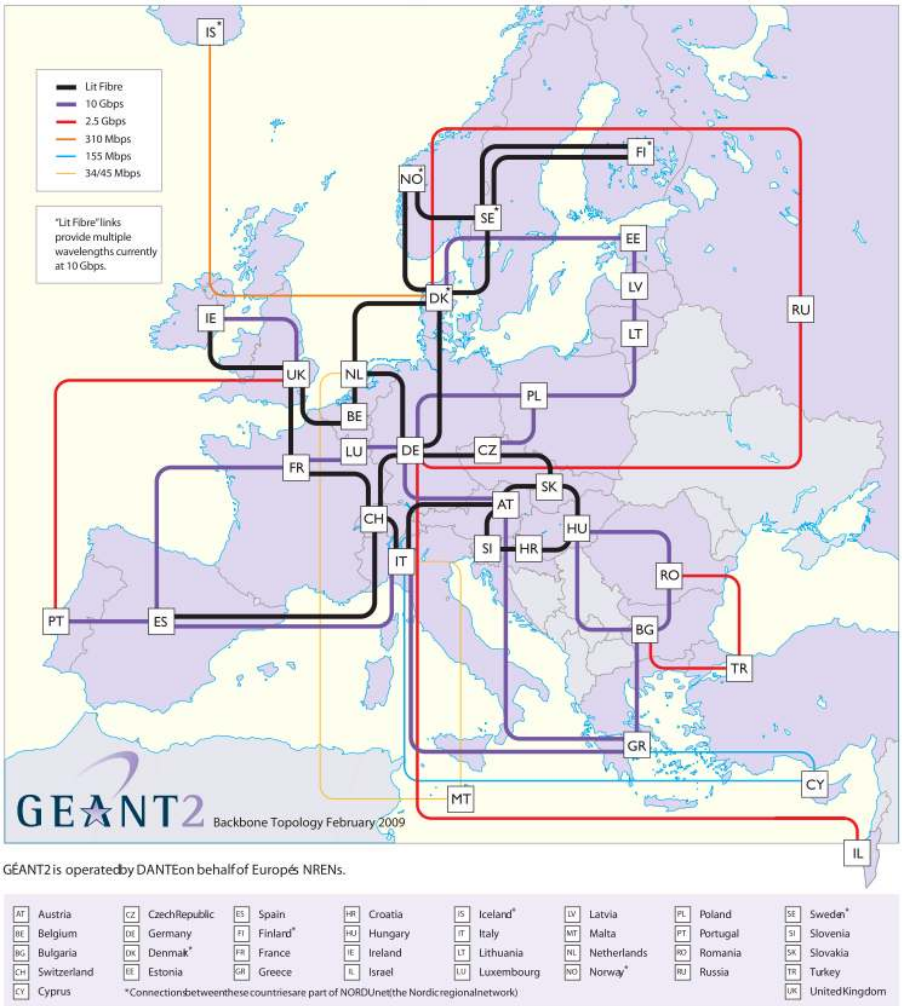
○ International Peerings

Peer	Connection Type	Connection Date
Abilene	Native (DE-Washg.)	05/05/2003
	Native (NY)	10/06/2003
	Native (NL)	07/10/2003
CANARIE	Native	09/07/2003
ESnet	Native	27/05/2003

SINET	Tunnel to NY (since 20/05/04)	03/06/2003

○ Commerical Peerings

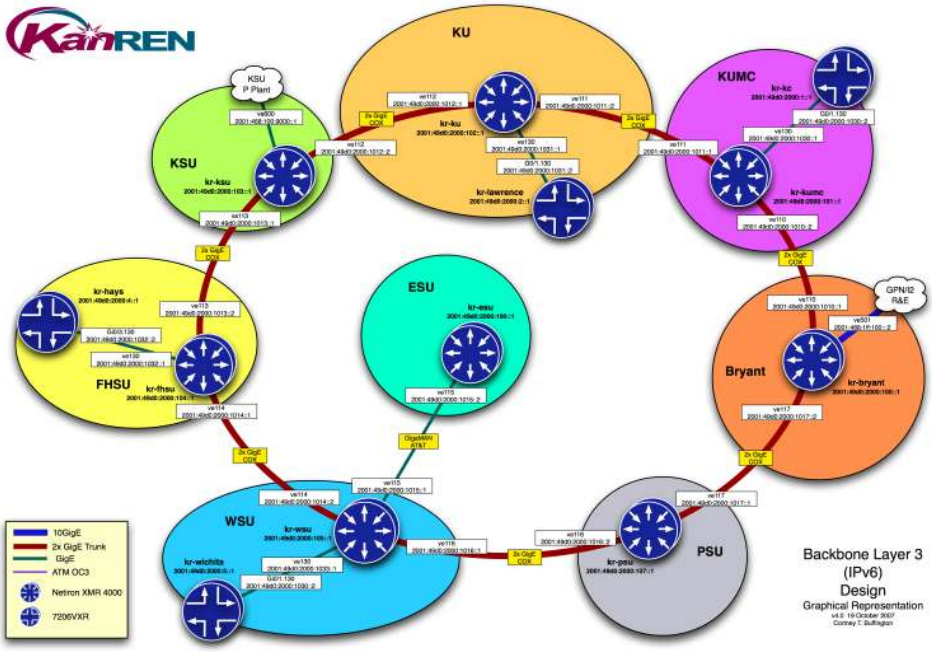
Peer	Connection Type	Connection Date
GlobalCrossing	Tunnel (Frankfurt)	25/07/2003
Telia	Tunnel	12/05/2003



[그림 17] GEANT2 백본 네트워크

2.2.7 KanREN (미국)

KanREN은 미국 캔사스주의 대학교 및 비영리 연구기관을 연결하는 연구교육망으로써 Internet2의 연구교육망의 멤버로써 활동하고 있으며, IPv6 구축에 있어서 선도적인 역할을 하고 있는 연구망이다. 특히 KanREN의 Barton County Community College는 IPv6망 전환 및 보안 정책을 구축하였고, Ft. Scott Community College는 본교 캠퍼스 및 6개 분교 캠퍼스에 IPv4/IPv6 듀얼스택을 지원하는 망을 구축하였다. Fort Hays State University는 DNS, email, Web 서비스를 학내 핵심 네트워크 및 외부 네트워크에 구축을 마쳤으며, Pittsburg State University와 Emporia State University는 두 학교간 IPv4/IPv6 듀얼스택을 지원하는 노력을 진행중에 있다. [19]



[그림 18] KanREN IPv6 네트워크

제 3 장 IPv6 보안 고려사항

IPv6 보안은 많은 방식에서 IPv4의 보안과 유사한 점이 많다고 할 수 있다. 네트워크를 통해서 패킷전송을 수행해야하는 메커니즘은 거의 변화되지 않았기 때문이다. 그러나 IPv6가 IPsec을 기본 탑재하였기 때문에 임베디드 보안이 강화되었다고 볼 수 있다.

IPv6에 대한 일반적인 보안에 대한 고려사항은 일부 특정한 프로토콜이나 어플리케이션에 대한 사항 등에 한정되어 IETF 등에서 다루어지고 있다. 이는 실제 사용되는 인터넷 노드가 많지가 않기 때문일 것이다. 하지만 IPv6 역시 IPv4가 가지고 있는 대부분의 보안에 대한 이슈가 그대로 적용될 수 있을 것이다. 본 장에서는 IPv6에서 생성이 가능한 보안이슈에 대해 살펴본다.

1. IPv6 보안 위협

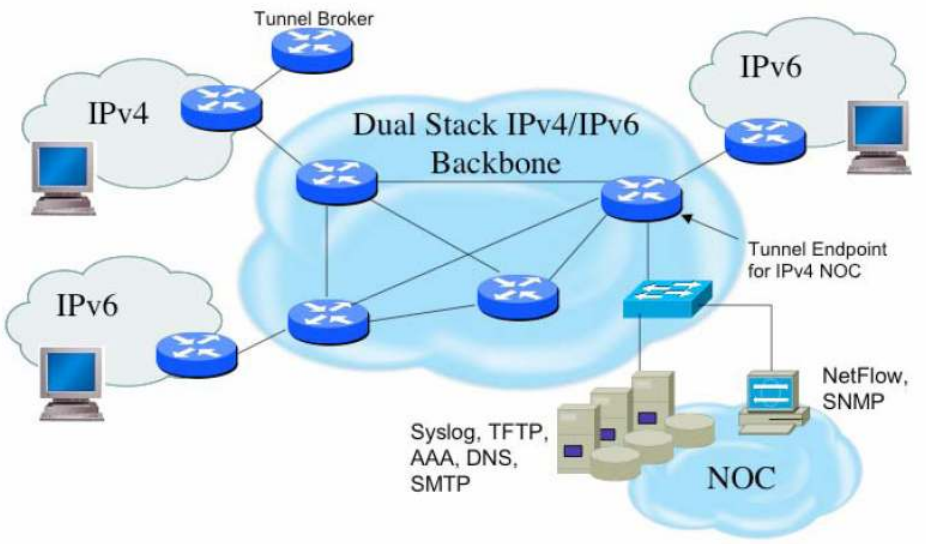
기본적으로 IPv4나 IPv6의 위협에 대한 비교자료는 시스코의 S.Convery와 Darrin Miller가 제시한 문서 등에 잘 제시가 되어 있으며 간단히 요약하자면 다음과 같다[20]. 다음의 9가지 공격이슈가 IPv6 월드로 향하는 특징적인 위협이라 볼 수 있다.

- 정찰(Reconnaissance)
- 비인가 접근(Unauthorized access)
- Header manipulation and fragmentation
- 스푸핑 공격(Layer 3 and Layer 4 spoofing)
- Address Resolution Protocol (ARP) and Dynamic Host Configuration Protocol (DHCP) attacks
- 스머프공격(Broadcast amplification attacks (smurf))
- 라우팅공격(Routing attacks)
- 바이러스와 웜공격(Viruses and worms)
- Transition, translation, and tunneling mechanisms

물론 위와 같은 형태의 위협은 IPv4에 대부분 존재하는 공격에 대한 기술이며 이는 IPv6가 IPv4를 계승하는 차원의 보안이 적용되어야한다는 점이다. 듀얼스택을 활용한 네트워크로의 전개를 계획하고 있다는 이 두 가지 기능에 모두 부합하는 방화벽이나 VPN 등의 장비의 도입을 신중히 검토해야한다.

2. IPv6 보안정책 고려사항

보안정책은 주어진 보안환경에서 가장 효과적인 아키텍쳐로 전환되기 위해서 필요한 기술이다. IPv6는 단순화와 자동화 네트워크 구현 등 많은 능력을 보유하고 있다. 하지만 이러한 많은 형태의 기술들은 반드시 주의깊게 고려되어야한다. 즉 주어진 각 기관이나 ISP 등 그들의 보안정책에 어떠한 영향을 미칠 것인가? 를 고려해야한다는 점이다.



[그림 19] 간단한 IPv6 아키텍쳐

이 절에서는 실질적인 IPv6 구축을 위한 운영관점에서 보안 고려사항을 다루고자한다. [그림 18]은 간단한 IPv6 네트워크 아키텍쳐를 보여준다. IPv6 보안

아키텍쳐를 구현하기위해서는 다음과 같이 몇 가지 사항을 먼저 고려하여야 한다. 보안정책 고려사항, 단말호스트 보안 , 네트워크 인프라 보안 등이 이에 해당한다.[21]

2.1 보안 정책 고려사항

모든 네트워크 보안을 수행하기위해 우선해야하는 것은 어떠한 철학으로 보안을 구축할 것인가에 대한 중요한 결정이다. 보안정책은 반드시 IPv6 통신 환경을 제어할 수 있도록 만드는 절차가 선행되어야한다. 이러한 정책은 그 해당기관이나 네트워크에 대한 위험평가 분석(RA: Risk Assessment)과 많은 양의 비즈니스 그리고 운영실무 등이 총망라된 결과물이 될 것이다. 그러므로 모든 환경에 대한 보안정책을 입안하는 것은 불가능하지만 보안정책의 주요한 목표는 기밀성, 무결성, 책임성 그리고 가용성 등을 보존하는 것이 주목적일 것이다. 위험평가를 수행함에 있어서 IPv6로의 안정적인 전환을 위한 현재의 정책을 어떻게 수행할 것인가는 매우 중요한 이슈가 될 것이다. 이런 관점에서 보안 정책은 IPv4와 거의 같지만 추가적으로 다음의 고려사항을 염두에 두어야한다.

- 대부분의 장비들은 인터페이스마다 많은 수의 IPv6 주소를 가질 수 있기에 정책은 효율적인 필터링과 검사가 되어야 한다.
- IPv6는 IPsec을 이용한 임베디드 형태로 구현이 되었기에 다양한 보다 안전한 P-to-P 통신이 가능하다. IPv6 노드들 사이에 모든 통신이 IPsec을 이용하여 얼마나 정책적으로 인증과 무결성을 보장할 수 있을까? 이것은 IPv6 클라이언트와 서버들 뿐만 아니라 듀얼스택 라우터나 터널브로커와 같은 디바이스역시 포함한다.
- 기밀성 서비스를 재검토할 필요가 있다. 만약 필터링과 감사가 네트워크 인프라내부거나 단대단 기밀성 대신에 호스트수준으로 수행될 수 있다면 IPsec을 사용하여 보안정책을 위임할 수 있다.
- Native IPv6가 최종적인 목표지만, 이를 이행하는 것은 쉽지않다. 모

든 터널링 솔루션을 이용할 경우 터널 스푸핑 등의 보안요구사항을 검토하여야한다. 터널이 설정된 위치와 정적 또는 동적 터널을 사용할 것인지가 결정되어야한다.

- 방화벽 정책에 IPv6 시나라오를 적극 수용하기 위해 수정할 수 있어야한다. 더 구체적인 내용에서 찾을 수있는 섹션에서 '네트워크 인프라 보안'에서 다룰 예정이다.
- IPv6는 매우 DNS에 의존적이다. 특히 FQDN(fully qualified domain names)의 이용하는 정책에 매우 신중해야한다. 이러한 것은 DHCPv6 (server and client) 와 DNS의 Dynamic Updates시 필요하다.

어떤 효과적인 보안 정책은 항상 기술적으로 실현가능하여야 하고, 운영 적인 측면에서도 구축과 집행이 가능해야한다 것을 주지하여야한다.

2.2 단말 호스트 보안

단말호스트 보안은 IPv6가 이용이 가능한 클라이언트와 서버를 그 대상으로 한다. 이러한 관점에서 주요한 관심사는 다음과 같다.

- 주소 할당이 신뢰할 수 있고 스푸핑 공격을 대비해야한다.
- 단말 호스트를 향한 트래픽은 변조, 삭제 그리고 스푸핑에 방어가 가능하여야한다.
- 악의적인 공격을 감지할 수 있도록 해야한다.

이러한 기본적인 단말에 대한 호스트 공격을 차단하는 방법은 IPv4나 IPv6 모두에 해당되는 기술일 것이다. 특히 IPv6는 autoconfiguration 기능이 사용되기 때문에 정책적으로 DHCPv6와 DNS 등이 잘관리 되어야한다. 최소한 다음과 같은 정책으로 수행되어야한다.

- 개인에게 클라이언트 또는 인증 및 권한을 서버에 대한 액세스를 제한
- 모니터 및 클라이언트와 서버에 접근에 대해 관제와 감사 강화
- 말단 노드에서 사용하지 않은 서비스 전원차단
- 호스트 방화벽 기능을 사용하여 상위 계층 프로토콜에 의해 처리하고 트래픽을 제어한다.
- 바이러스 스캐너를 사용하여 악성 프로그램을 감지

2.3 네트워크 인프라 보안

네트워크 인프라 보안은 이를 구성하는 요소인 DNS, AAA, Syslog, DHCP, SNMP 그리고 NTP와 같은 네트워크 서비스뿐만 아니라 라우터, 스위치, 네트워크 방화벽, 네트워크 침입 탐지 시스템을 포함하는 네트워크 인프라와 관련된 요소들에 대한 보안을 말한다.

2.3.1 네트워크 인프라 보안

네트워크 인프라 보안에서 네트워크 서비스 서버, 터널브로커, 방화벽, 감사시스템 그리고 라우터나 스위치 등의 장비는 다음과 같은 보안 고려사항을 지켜야한다.

- 텔넷과 SSH를 위한 IPv6를 액세스에 대한 통제 제한
- 장비에 대한 인증 및 권한에 대한 액세스를 제한
- 모니터와 정기적인 액세스를 감사
- 미사용 서비스 차단 및 작동 정지
- 바이러스 스캐너를 통한 악의적인 활동 감지 (DNS, DHCP, 네트워크 서비스 등 서버 등)에 적용
- 통신상호간의 인증 및 무결성 서비스를 제공하기 위해 NULL 암호화를 이용한 IPSec ESP 사용

2.3.2 라우팅 프로토콜 보안

라우팅 프로토콜 보안은 전통적으로 MD5 인증과 필터링의 조합을 이용해서 보안을 수행하였다. MD5 인증은 피어링을 유지하는데 이용되며 대부분의 라우터들은 IPv4와 IPv6 모두 MD5 인증을 통해 라우팅 프로토콜 보안을 수행한다. 즉 패스워드(KEY 값)을 통한 메커니즘을 이용하며 이는 운영상 필요한 요소이다. IKE를 이용한 IPsec은 MD5의 인증과 기밀성 검증에 대한 대안 옵션으로 고려될 필요가 있다.

Ingress/egress traffic filtering은 효과적으로 소스 어드레스 스푸핑과 같은 DDoS 트래픽을 경감하는 기술로서 IPv4에서 뿐만아니라 IPv6에서도 이용될 수 있다. 비록 이러한 기술들이 IPv4에 이용되지만 IPv6 인프라에서도 적용될 수 있다. IPv6를 위해서는 다음과 같은 것을 포함한다.

- 0::/16 (compatible, mapped addresses, loopback, unspecified, ...)
- fe80::/10 (link-local)
- fec0::/10 (site-local)
- ff00::/8 (any multicast)

BGP 라우팅의 경우에 IPv6 라우팅 정보의 전달을 위한 제한사항으로 다양한 정책들이 적용될 수 있다. 추천되는 BGP 라우팅 정책은 다음의 문서 참고문헌을 참조한다. [22] http://www.space.net/~gert/RIPE/ipv6-filters.html

2.3.3 방화벽/필터링 보안

필터링이란 패킷에 대한 파라미터들에 대한 분석을 통해 트래픽을 허용할 것인가 차단할 것인가를 결정하는 기술이며 이는 대부분의 네트워크 인프라스트럭쳐에서 중요한 부분이다. 필터링 룰들은 현재 추천되는 IPv6 트래픽에 대한 네트워크 방화벽의 내용은 참고문헌 참조한다.[21]

제 4 장 결 론

모든 안전한 네트워크에서 진정한 목표는 네트워크에서 악의적인 스푸핑, 훼손, 변경, 파괴 등 데이터나 서비스의 불능을 미연에 방지하는 것이 그 주목적이다. 이러한 방어는 모든 장비에서 필요한 사항이며 네트워크에 연결되고 참여하는 모든 장치는 보안을 위한 방어전략이 부가되어 있어야한다. IPv6 네트워크는 IPv4 네트워크의 계승적인 성격이 강하므로 IPv4에서 부가하는 보안기능이 모두 구현되는 것이 바람직하다고 할 수 있다. 하지만 가장 큰 차이점은 필수 인증, 기밀성, 무결성을 제공하기위해 IPsec이 제공된다는 점이다. 추가적으로 로깅과 네트워크 감사 등이 추가적으로 수반되어야할 부분이다.

본 고에서는 IPv6 지원 장비들의 성능, IPv6 지원여부, CC인증 및 국정원 보안성 검토 획득여부, 침입방지 및 탐지기능 구현여부 등을 국산 및 외산장비별로 비교하고 2개의 표로 정리·요약하였다. 국산장비들은 처리능력, 동시지원 세션수, 지원 인터페이스 수, 그리고 침입탐지 및 방지지원 기능 등이 모두 외산장비들에 비해 더 뛰어나다. 즉, 기술적인 면에서는 국산 장비들에 외산 장비들에 비해 결코 떨어지지 않고 오히려 더 우수한 성능을 보인다는 것이다. 그러나 문제는 이러한 국산장비들이 실제로 IPv6망과 연동되어서 동작할 때에도 원활하게 동작할지는 알 수 없다는 것이다. 몇몇 장비 업체들은 자신들의 장비가 자체적인 IPv6 시험테스트를 모두 통과했으므로 문제가 없을 것이라고 주장하고 있다. 하지만 그러한 테스트들은 단순한 수준의 네트워크 환경을 구축하고 테스트를 수행한 것이므로 충분한 신뢰성을 가진다고 보증할 수 없다. 따라서, 보다 완벽하고 실질적인 IPv6 지원여부 확인을 위해서는 실제 IPv6 트래픽이 유통되는 망에 연동시켜 테스트를 수행할 수 있는 환경이 제공되어야 한다. 국산장비들이 이러한 실질적인 망 연동 테스트를 통과한 경우에는 기술적으로 외산장비보다 더 높은 경쟁력을 가지므로, 국내시장의 점유율을 크게 늘리는 효과를 가져올 것이다. 향후에 IPv6를 지원하는 장비 개발업체 들에게 실질적인 테스트 환경이 제공된다면, 개발한 장비들의 실

질적 검증이 가능하므로 장비자체의 고도화 및 경쟁력 측면에서 외산장비에 비해 우위를 점하게 될 것이다. 이를 통해 국산장비산업을 활성화시키고 관련 정보보호산업의 발전을 견인할 것으로 기대된다.

국내에서 IPv6 트래픽이 직접 유통될 수 있는 ISP는 현재 거의 없다고 할 수 있다. 국가과학기술연구망(KREONET)과 같은 소수의 연구망과 전세계의 유수의 연구망들이 현존하는 IPv6 트래픽을 전세계적으로 유통하고 있을 뿐이다. 이는 IPv6의 고갈에 대한 인식과 실질적인 수요의 비즈니스적인 사항이 실제로 부합하지 않아서 일 것이다. 산업은 곧 비즈니스적인 미래가 보여야 급진적으로 발전한다는 것이다. 특히 보안적인 측면에서 기관망에 대한 중소규모의 네트워크를 IPv6로 전환하는 관점에서도 매우 심각한 어려움이 존재하고 있다.

Transition 기술적인 면에서 듀얼스택으로 망을 구축해야 저비용으로 완전한 망전환이 가능하지만 기존의 망을 운영하는 기관의 운영자의 IPv6에 대한 신뢰가 아직 형성되지 않았다는 점에서 인식제고에 대한 홍보도 필수적일 것으로 생각된다. 유선망의 경우는 기존 IPv4에서 운영중인 방화벽, IPS, 침입탐지시스템, 관제시스템, 망관리시스템 등 무수히 많은 네트워크 장비 및 보안장비가 필요하다. 하지만 현 시점에서 방화벽의 필터링 기능과 일부 IPv6 기능 정도는 어느 정도 IPv6의 성능이 보장되는 실정이지만 그 외의 많은 보안 장비의 경우 거의 대부분 IPv6 기능이 보완이 되어 있지 않다. 각 기관의 경우 최소한 망운영을 위한 보안장비 즉 방화벽, 침입차단/방지시스템, 망관리시스템 정도는 IPv6에 대한 보안기능이 모두 수행이 가능하여야한다. 하지만 현 시점에서 트래픽이 생성되지 않고 있기에 실질적인 IPS룰과 같은 시그네이쳐 등이 개발되지 않았기는 현재는 지극히 초보적인 보안 솔루션이 동작하고 있다고 할 수 있다. 기관입장에서 곧 대부분의 망운영을 수행하는 엔지니어나 관리자 그리고 CEO가 어려움과 안전성이 보장되지 않은 IPv6망으로의 전환을 심각하게 고려하기는 정말로 어려운 실정인 것이다. 하지만 이러한 어려

운 시점이 오히려 국가적인 측면이나 산업적인 선점 측면에서 중요한 시점이라 판단된다. 특히 IPv6 보안장비의 시장은 현재 일부 국산방화벽과 대다수의 외산장비들로 대변이 되고 있으며 만약 이러한 시장이 고갈시점인 2011년경부터 급속적인 발전을 이룩한다면 국내에서도 선투자를 통한 경쟁력확보 관점에서 현 시점이 보안솔루션에 대한 IPv6 적용 및 전개를 매우 필수적으로 고려할 시점인 것으로 판단된다.

참고문헌

[1] 2008 IPv6 동향, 한국인터넷진흥원

[2] 2008 공공부문 IPv6 전환·확산 보고서, 한국인터넷진흥원

[3] 2008 대덕특구 IPv6 클러스터 구축 사업보고서 (한국과학기술정보연구원)

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

[5] Juniper Homepage, http://www.juniper.net

[6] Checkpoint Homepage, http://www.checkpoint.com

[7] F5 Networks BIG-IP Homepage,
http://www.f5.com/products/hardware/big-ip.html

[8] Ahn Lab Homepage, http://home.ahnlab.com/

[9] Secui.com Product Homepage, http://www.secui.co.kr/

[10] Future Product Homepage, http://www.future.co.kr/01/0102.php

[11] http://ipv6.internet2.edu/

[12] http://www.jgn.nict.go.jp/english/index.html

[13] http://www.cernet2.edu.cn/en/6ix.htm

[14] http://www.twaren.net/english

[15] http://www.geant2.net/

[16] http://www.nida.or.kr/english/

[17] http://www.vsix.kr/english/index.jsp

[18] http://www.kreonet.net/english/

[19] http://www.kanren.net

[20] http://www.cisco.com/web/about/security/security_services/ciag/documents/v6-v4-threats.pdf

[21] NAv6TF www.nav6tf.org IPv6 Network Security Architectures V1.0

[22] http://www.space.net/~gert/RIPE/ipv6-filters.html

약 어

BSD : Berkeley Software Distribution

CNGI : China Next Generation Internet

DNS : Domain Name Service

FWSM : Firewall Services Module

IPv4 : Internat Protocol version 4

IPv6 : Internat Protocol version 6

IPS : Intrusion Prevention System

JGN : Japan Gigabit Network

KanREN : Kansa Research and Education Network

KREONET : Korean Research Environment Open NETwork

NREN : National Research & Education Network

TWAREN : Taiwan Advanced Research & Education Network

VPN : Virtual Private Network

XTM : eXtensible Threat Management