通信情報保護學會誌
第5卷 第4號, 1995. 12

초고속 정보통신망과 인터네트의 접속에 따른 통신망 보안

Network Security on the Interworking with KII and Internet

문 필 주*, 고 병 도*, 전 문 석**, 이 철 희**

요 약

초고속 정보통신망상에서의 보안에 대한 중요성이 날로 증가하고 있다. 현재 통신망 보안을 위한 대책중의 하나가 바로 방화벽시스템의 설치이다. 방화벽시스템은 인터네트상에 공개되어있는 시스템들 중에서 보안이 요구되는 시스템들에 대하여 해커들의 침입을 사전에 예방하고 일단 침입에 성공하였다 하더라도 시스템의 피해를 최소로 줄이도록 하는 통신망 보안시스템이다. 본 논문에서는 이러한 방화벽시스템이 초고속 정보통신망과 인터네트이 접속된 상황하에서 어떻게 구성이 가능한지를 제시하였다. 이를 위하여 먼저 국내외 통신망 및 서비스 보안에 관련된 사항를 살펴보고, 초고속 정보통신망이 어떻게 기존의 인터네트에 접속할 수 있는지에 관한 방법과 인터네트상에서의 방화벽시스템 개념을 설명하였다.

1. 서 론

초고속 정보통신망은 디지틀정보를 언제, 어디에서나 광범위하게 접근 및 사용할 수 있도록 하는 하나의 거대한 시스템이며, 이 시스템은 고속통신망, 데이터 베이스, 고성능 컴퓨터들로 구성된다. 초고속 정보통신망은 21세기 정보화 사회에서 국가 경쟁력은 물론 개개인의 생활 즉, 가정, 직장, 학교 등에서 삶의 질을 향상시키는 중요한 역할을 할 것이다. 이러한 초고속 정보통신망의 중요성을 인식하여 전세계 모든 국가들이 이를 구축하기 위하여 최대의 노력을 기울이고 있다. 미국의 NII (National Information Infrastructure), 일본의 신사회 자본 정비 전략, 싱가폴의 IT2000 계획 등이 바로 그것이다. 국내에서도 이미 지난해부터 초고속 정보통신망구축기획단을 발족하여 초고속 정보통신기반 구축에 박차를 가하고 있다.

초고속 정보통신망의 구축은 방대한 정보를 모든 사람이 공유하고 활용한다는 의미에서 생활 형태의 전반적인 변화를 예고하고 있다. 특히, 기존의 문자 위주의 정보 공유 및 활용에서 문자, 그래픽, 이미지, 영상, 등을 모두 포함하는 멀티미디어 형태의 정보를 실생활에서 사용가능 하게 됨으로써 시간과 공간을 초월하는 가상현실(Virtual Reality)이나 가상 공간

* 한국전자통신연구소
** 숭실대학교 정보과학대학

(Cyber Space)의 세계를 직접 체험하게 될 것이다. 그러나 이러한 서비스의 효율적인 제공을 위해서는 초고속 통신망의 보안, 정보의 보안 그리고 서비스의 보안 문제가 먼저 해결되어야 한다.

초고속 통신망의 보안, 정보의 보안 그리고 서비스의 보안의 중요성이 더욱 대두되는 이유는 컴퓨터 보급과 이용의 확대 그리고 컴퓨터 통신망의 사용 증대에 따라 어느 누구나 쉽게 초고속 정보통신망에 접근할 수 있으며, 컴퓨터 및 통신망에 조금만 지식을 소유하고 있는 사람은 보안의 허술함을 이용하여 손쉽게 해커의 속성을 지니게 될 수 있기 때문이다. 이러한 해커들의 침입은 초고속 정보통신망 상에서 운용되는 공공 정보와 개인 정보의 중요성에 비추어 볼때 대단히 심각한 일이라고 아니할 수 없다. 따라서 초고속 정보통신망에 이러한 해커들의 침입을 미연에 방지하고, 일단 침입에 성공했더라도 정보 및 통신망의 피해를 최소로 줄일 수 있는 대책이 조속히 수립되어야 할 것이다. 현재 이러한 통신망 보안을 위한 대책중의 하나가 바로 방화벽시스템의 설치이다. 방화벽시스템이라고 하는 것은 인터네트상에 공개되어있는 시스템들 중에서 보안이 요구되는 시스템들에 대하여 해커들의 침입을 사전에 예방하고 일단 침입에 성공하였다 하더라도 시스템의 피해를 최소로 줄이도록 하는 보안 시스템이다.

본 논문에서는 이러한 방화벽시스템이 초고속 정보통신망과 인터네트이 접속된 상황하에서 어떻게 구성이 가능한지를 제시하였다. 이를 위하여 먼저 국내외 통신망 및 서비스 보안 관련 사항으로서, 미국의 NII를 구축함에 있어서 보안에 관한 사항을 다루는 조직체계와 정부의 역할를 살펴보고, 국내에서 진행중인 통신망 보안 및 안정성에 관한 연구개발 현황을 살펴보았다. 제3장에서는 초고속 정보통신망이 어떻게 기존의 인터네트에 접속할 수 있는지에 관하여 방법을 제시하였으며, 제4장에서는 인터네트상에서 사용되는 보안 장치로서 가장 안전한 보안 시스템이라고 할 수 있는 방화벽시스템의 개념 및 이들의 기능을 살펴보고, 초고속 정보통신망과 인터네트이 상호 연동될 경우에 방화벽을 어떻게 구성 및 설치 할 것인지에 관하여 기술하였다. 끝으로 제5장에서는 결론으로서 초고속 정보통신망상에서의 보안을 위해 정부가 해야할 일을 제시하였다.

2. 국내외의 초고속 정보통신망 관련 보안 동향

2.1 미국의 NII

미국은 NII 구축을 위한 전담기관으로써 IITF(Infromation Infrastructure Task Force)라는 조직을 신설하고 이 기관을 통하여 NII 구축에 필요한 제반 사항을 모두 처리하고 있다. 특히 보안에 관한 사항을 다루기 위하여 IITF 산하에 "National Information Infrastructure Security Issues Forum(NIISF)"을 구성하였으며, 특히, 이 포럼에서는 NII 보안과 관련하여 연구개발, 법률적인 사항 그리고 기술적인 사항들을 분석, 종합하여 정부에 결과를 보고함으로써, NII 구축 정책에 이를 최대한 반영하게 하고 있다.

또한, IITF 와 더불어 NII 구축을 위한 미국자문위원회를 설치하였다. 이 자문 위원회는 통상부, 노동부, 주정부 그리고 공공 이익 단체를 대변하는 대표자들로 구성되어 있으며, NII에 관련된 사항들을 종합하여 상무성 장관에게 자문하는 역할을 한다. 자문위원회 산하 3개의 연구반 중에 하나인 Mega-Project III는 NII 와 관련하여 보안, 저작권, 사생활 보호에 관한 사항을 특히 강조하고 있다.

다음은 95년 5월에 NIISIF 에서 발표한 "NII SECURITY : THE FEDERAL ROLL"[2] 보

고서 중에서 NII 보안을 향상 시키기 위하여 제시한 연방정부의 4가지 역할을 요약하였다.

- 연방정부는 기업의 활동을 증진 시키기 위한 촉진자의 역할을 담당 하라
  - NII 보안 원리와 OECD(Organization for Economic Cooperation and Development) 보안 원칙을 발표
  - 보안의 위험성, 필요성, 해결책에 대한 의견과 의식을 조사
  - 연방정부가 NII 상에서 사용가능한 보안 제품과 기술 개발
  - 기업체에서 고품질의 보안 제품과 서비스 개발을 증진

- 연방정부는 공공의 이익과 일반 복지에 대한 관리자의 역할을 담당함에 있어서, NII 보안를 위한 법률과 정책을 수립시 지방정부와 기업체에게 협력하라
  - NII 상에서 적절한 비상응답능력를 보장
  - 현 관리 방식을 개정
  - 법률 검토
  - 국제 협력 증진

- 연방정부는 critical / high-risks 분야의 R&D에 자금을 지원함으로써 기업체가 필요한 기술을 개발하도록 지원하라
  - HPCCP, ARPA, NIST 등을 통하여 연구/개발를 증진 시켜라

- NII 의 사용자로서, 연방정부는 그들 자신의 정보가 안전하다는 것을 보장할 책임을 가짐
  - 효과적인 관리를 통하여 정보를 보호
  - 국가 보안/비상시 에 대한 준비 능력 향상
  - 연방정부가 사용하는 제품이나 서비스가 보안 요구사항을 만족한다는 것을 보장해야함
  - 보안 기반 기술개발

2.2 국내의 통신망 보안관련 연구개발 현황

국내에서는 초고속 정보통신망 상에서의 보안문제를 다룰 가시적인 조직은 아직 없는 상태이다. 다만 통신망의 보안/신뢰성/안정성 등에 대한 연구가 한국전자통신연구소, 한국전산원, 한국통신, 시스템공학연구소 등에서 개별적으로 수행되었다. 최근 초고속 정보통신망 상에서의 보안성 문제가 심각하게 대두되면서 정보통신부를 중심으로 가칭 정보보호센터의 설립이 구체적으로 논의되고있는 단계에 있다.

표 2-1에 국내 연구기관에서 추진중이거나 계획중인 통신망의 보안성, 신뢰성 그리고 안전성에 관한 연구개발의 주요 연구내용을 나타냈다.

표 2-1 보안관련 국내 연구개발 현황

기 관	과제 제목	주요연구내용
한국전자통신연구소	통신망 안전성/신뢰성 연구	• 비상통신 운용체계 연구 • 통신망 종합관리 DB 연구 • 통신망 종합관리 협의회 지원 • 재난대비 기술연구

	초고속정보통신망 안전성 기술연구	• 초고속망 안전성 요구사항 연구 • 안정선 보장 체계 수립 • 네트워크 신뢰성 확보 연구 • 네트워크 안전성 기술 연구 • 공통기반 서비스 안전성 연구
	통신정보보호 기술개발	• 암호알고리즘 및 장비 개발 • 정보보호 체계 구축 연구 • 안전한 KT-EDI 시스템 개발 • 전산망 보안평가 기준 및 방법 연구 • 컴퓨터 보안 연구(Secure OS / DBMS) • 정보보호 기술 연구 개발 (Access Control, Authenticaion, 등) • 정보보호 프로토콜 연구 개발
한국전산원	전산망 안전보안 연구	• 정보시스템 안전보안 사고 대응 연구 • 정보시스템 안전보안 홍보 및 교육연구 • 정보시스템 안전보안 평가 대책 연구 • 정보시스템 안전보안 관리 대책 연구 • 정보시스템 안전보안 기술 대책 연구
한국통신	재난대비 정보통신 종합대책 연구	• 방재관련 법규, 조직, 제도적 개선 보완대책 • 통신망 신뢰성 기준 제시 • 전송망 안정성 확보방안 제시 • 비상재해시 우회루트 확보방안 제시 • 공중 및 자가 통신시설 인력을 통합 활용하는 긴급통신 소통대책
	통신망 접속인증 및 유통 정보보호 기술연구	• 정보보호 기술 표준화 연구 • 인증 알고리즘 개발 및 응용, 표준화
시스템공학연구소	전산망 보안 연구	• 인터네트/유닉스 보안 취약성 분석 진단 연구 • 초고속정보화 추진을 위한 소프트웨어 기술개발(SOFTTECH 2015 중에서)

3. 초고속 정보통신망과 인터네트의 접속

전세계적으로 초고속 정보통신망의 구성 형태는 ATM 통신방식을 기반으로 하는 B-ISDN 임에는 의심의 여지가 없다. ATM 기술은 현재 ATM-FORUM 을 중심으로 사설망 분야에서는 표준화가 급진전되고 있으며 이에 따라 상용화 제품들이 속속 출현하고 있다. 이들의 제품군을 살펴보면 ATM Adaptor Card, ATM 사설 교환기, ATM 라우터, ATM WAN 교환기 등의 형태로 다양하게 나타나고 있다.

초고속 정보통신망은 이러한 장치들을 기반으로 ATM WAN 교환기를 서로 연결하여 ATM backbone 망을 구성하고, 이 ATM backbone 을 중심으로 ATM 사설 교환기를 기반으로한 ATM LAN 과 ATM 호스트들이

접속된다. 또한 데스크탑의 컴퓨터 시스템의 입장에서 보면 다양한 ATM Adaptor Card 의 개발로 UNIX 나 Windows NT를 운영체제로 하는 워크스테이션으로 155 Mbps의 고속 통신 인터페이스를 사용할 수 있게 되었으며 개인용 컴퓨터를 위한 ATM Adaptor Card 의 개발도 조만간 이루어질 전망이다.

이러한 ATM을 기반으로한 초고속 정보통신망을 사용하는 이용자는 기존의 TCP/IP 프로토콜을 기반으로하는 인터네트을 접속하는데 어려움이 있다. 이는 ATM 통신방식이 cell을 기본단위로 하는 연결형 서비스인데 반하여 인터네트는 패킷을 기본단위로 하는 패킷통신망으로서 TCP/IP 프로토콜을 사용하기 때문이다. 따라서 초고속 정보통신망과 기존의 인터네트을 접속하기 위해서는 ATM 망 내부에서 혹은 외부에서 비연결형 서비스를 지원해야 한다. ATM 망에서 비연결형 서비스의 지원은 비연결형 서버를 사용함으로써 가능하다. 비연결형 서비스를 원하는 이용자, 즉 인터네트에 접속하고자 하는 사용자는 호 설정시 PVC(Permanent Virtural Channel) 나 SVC(Switched Virtural Channel) 를 이용하여 비연결형 서버에 연결되고 이때 비연결형 서버는 패킷통신에서 주소를 할당해주는 ARP 서버의 역할을 수행함으로써 ATM cell의 해더에

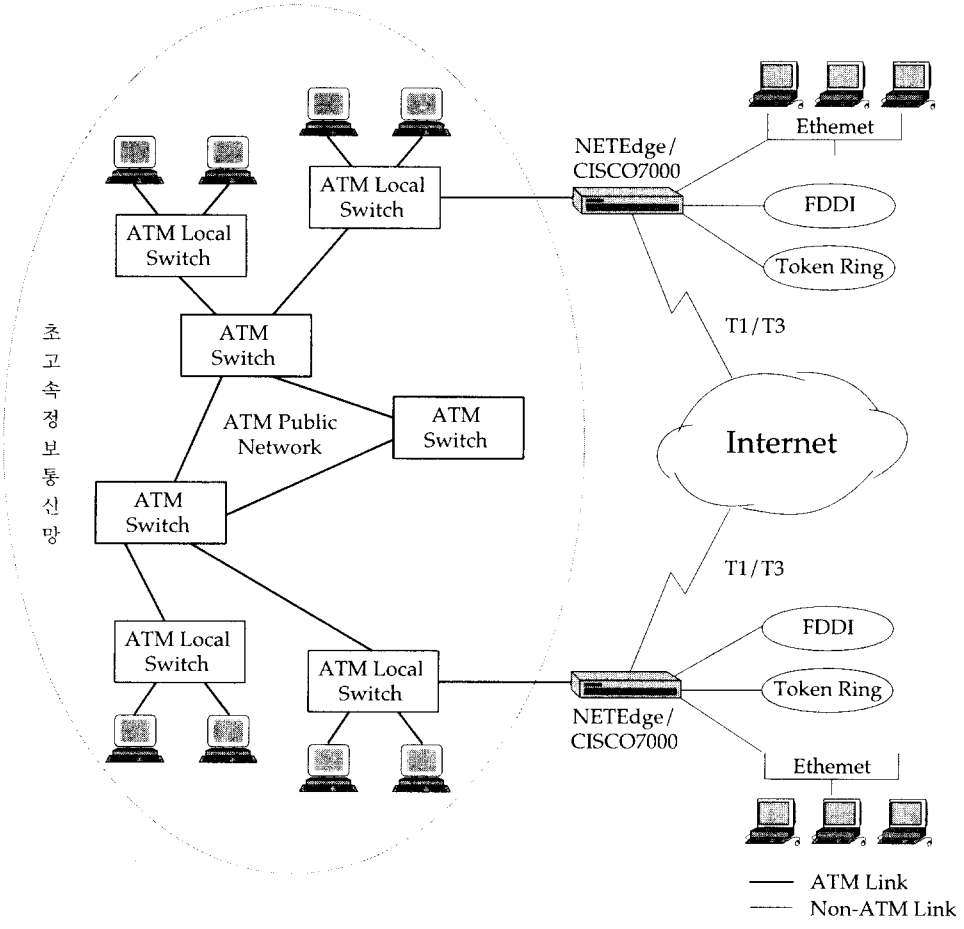


그림 3-1 CISCO 7000/NETEdge를 이용한 초고속정보통신망과 인터네트와의 연결

있는 목적지 주소를 IP 프로토콜상의 IP 주소로 변환한다. 이를 위하여 비연결형 서버는 ATM 사용자가 보낸 ATM cell을 IP protocol에 맞게 mapping 시키는 역할(IP over ATM 기능)과 인터네트로 패킷을 전송하기 위한 라우팅 기능을 담당한다.

따라서 초고속 정보통신망상의 ATM 사용자는 인터네트을 접속하기 위하여 비연결형 서버와 라우팅 역할을 하는 게이트웨이에 PVC나 SVC 를 이용하여 경로를 설정하고 이 게이트웨이의 IP over ATM 기능을 통하여 인터네트에 접속하여 패킷을 통신할 수 있다.

현재 이러한 기능을 수행할 수 있는 대표적인 제품으로는 CISCO 사의 CISCO 7000 시스템과 NETEdge System 사의 NETEdge 시스템이 있다. 이러한 장비들을 이용하여 어떻게 초고속 정보통신망과 인터네트의 접속이 가능한지를 그림 3-1에 나타냈다. CISCO 7000 과 NETEdge 시스템은 기존의 LAN 즉, Ethernet, Token Ring, FDDI 등은 물론 ATM LAN 및 ATM 호스트를 위한 인터페이스를 제공한다. 따라서 CISCO 7000 에 연결된 사용자는 자신이 속한 LAN의 종류에 관계없이 상대방과 통신이 가능하다. 또한 라우팅 기능을 통하여 인터네트와의 통신도 가능하다. 이를 위한 WAN 인터페이스로서 56kbps, 64kbps, T1급(1.5Mbps) 그리고 고속통신을 위한 T3 (45Mbps) 등의 전송속도를 지원한다. 표 3-1에 CISCO 7000과 NETEdge 시스템의 기능을 인터페이스와 S/W 측면에서 비교하여 나타냈다.

표 3-1 CISCO 7000과 NETEdge의 기능 비교

	NETEdge	NETEdge
Serial Interface	• ANSI / EIA RS-232 • ITU-T V.35 • ANSI / EIA RS-449 • ANSI / EIA RS-530 • ITU-T X.21 • ANSI / EIA RS-612(HSSI) • T1 / E1, T3	• ANSI / EIA RS-232 • ITU-T V.35 • ANSI / EIA RS-422 • T1 / E1
LAN Interface	• Token Ring : 4 / 16 Mbps • Ethernet • FDDI(multimode or single mode)	• Token Ring : 4 / 16Mbps • Ethernet • FDDI(multimode or single mode)
ATM Interface	• 100Mbps 4B / 5B TAXI(multimode) • 155Mbps SONET / SDH (multimode or single mode) • 45Mbps DS3(coax) • 34Mbps E3(coax)	• 100Mbps 4B / 5B TAX(multimode) • 155Mbps SONET / SDH (multimode or single mode)
S / W Spec.	• Routed Protocols - TCP / IP, OSI CLNS, OSI CMNS - DECnet, Novell IPX, AppleTalk - Banyan VINES, 3Com XNS - Xerox XNS, Apollo Domain	• Routed Protocols - TCP / IP - AppleTalk

	- Ungermann-Bass XNS • WAN Support - HDLC, PPP, X.25, DDN X.25 - Frame Relay, SMDS - ATM DXI • Bridging Technologies - IEEE 802, 1d Spanning Tree - Source-Route Bridging - Translational Bridging - Source-Route Transparent Bridging	• WAN Support - PPP - Frame Relay • Bridging Technologies - IEEE 802, 1D Spanning Tree - Source-Route Bridgin - Source-Route Transparent Bridging

4. 초고속 정보통신망상에서 통신망 보안

4.1 인터네트상에서의 방화벽시스템 설치

4.1.1 방화벽시스템의 개념

인터네트 방화벽 시스템은 사설 네트워크를 보호하기 위한 통신망 보안 방법을 말하며, 외부네트워크와 사설 네트워크의 경계에 패킷 필터링 기능을 하는 라우터나 응용게이트웨이를 두어 모든 정보의 흐름이 이들을 통해서만 이루어지도록 하는 개념이다. 즉, 사설네트워크를 보호하기 위해 외부에서의 불법적인 트래픽 유입을 막고, 허가되고 인증된 트래픽만을 허용하려는 적극적인 방어대책이다.

방화벽시스템의 기본 목표는 사설네트워크에 불법 사용자들이 접근하여 컴퓨팅 자원들을 엑세스 하는것을 방지하고 자산(Proprietray) 정보들이 뜻하지 않게 혹은 불법적으로 외부로 유출되는 것을 방지하는 것이다.[3] 다음 그림 4-1은 일반적인 인터네트와의 접속을 하고 있는 네트워크를 나타냈다. 인터네트와의 투명성으로 인하여 사설 네트워크 전체에 접근 가능함을 보여주고 있으며, 그림4-2의 경우에는 인터네트와 사설 네트워크사이에 방화벽시스템을 둠으로서 인터네트를 통하여 들어오는 모든 트래픽은 방화벽시스템을 반드시 통과하도록 구성되어 있기때문에 불법적인 트래픽을 거부하거나 막을 수 있다.[6]

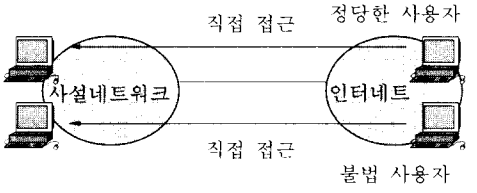


그림 4-1 직접접근으로 인한 위험지대

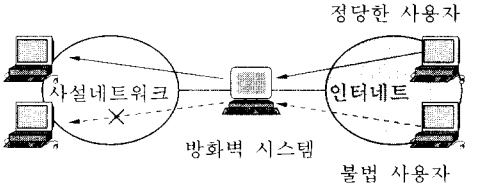


그림 4-2 방화벽시스템으로 사설네트워크의 안전지대화

그러나 그림 4-2에서와 같이 방화벽시스템을 구축하였다 하여 완벽하게 안전하다고 할 수 없다. 왜냐하면 불법침입자들은 사설 네트워크에 직접 접근하기는 어려워도 간접적으로 방화벽시스템에 접근하여 사설네트워크에 접근하려고 할 것이기 때문이다. 따라서 방화벽

시스템은 시스템 내부를 침입자가 들어올 수 없도록 가능한 안전시스템으로 구성되어야 한다. 이를 위하여 불필요한 네트워크 응용을 없애고 각종 에디터, 컴파일러, 명령어 등을 없애 기본적인 방화벽시스템 기능만 수행하도록 운영한다.

방화벽시스템이 구축되면 이를 운용할 정책이 요구된다. 이러한 정책은 기본적으로 네트워크 정책과 서비스 접근 정책으로 나눌 수 있다. 네트워크 접근 정책은 어떠한 네트워크와 호스트를 접근하게 할 것인지를 결정하는 것으로써 인터네트에서 사설네트워크로 혹은 사설네트워크에서 인터네트로 통신이 허용된 네트워크와 호스트를 정하는 것이다. 서비스 접근 정책은 어떠한 네트워크 서비스를 허용할 것인가를 결정하는 것으로써 예를들면 "전자우편, 화일전송, 월드와이드웹(WWW) 등의 서비스는 허용하고 그외의 서비스는 허용하지 않는다"와 같이 결정하여 운용할 수 있을 것이다.

이러한 방화벽시스템의 운용 정책은 사설네트워크를 운용하는 기관의 특성에 따라 상이하며 사용자의 요구에 따라 지속적인 서비스가 제공되어야 한다.

4.1.2 방화벽시스템의 구성요소

일반적으로 방화벽시스템을 구성하는 요소는 스크린라우터, 베스천호스트, 이중네트워크 게이트웨이, 스크린호스트 게이트웨이, 스크린 서브네트, 응용게이트웨이 등이 있으며, 이들의 개념은 다음과 같다.

- 스크린라우터(Screening Router)

방화벽시스템을 구성하는 가장 기본적인 요소로서 사설네트워크가 인터네트에 접속할때 일반적으로 사용하는 라우터(Router)이다. 이 라우터는 인터네트 패킷을 전달하고 경로배정(Routing) 기능을 담당하는 장비이다. 이러한 라우터는 패킷의 헤더 내용을 보고 필터링(스크린)할 수 있는 능력을 가지고 있다. 네트워크 수준의 IP(Internet Protocol) 데이타그램에서는 출발지주소 및 목적지 주소에 의한 스크린 기능을 제공하며, TCP(Transmission Control Protocol) 수준의 패킷에서는 네트워크 서비스을 식별해주는 포트(Port) 번호에 의한 스크린, 프로토콜별 스크린 등의 기능을 제공한다. 이 스크린라우터만을 가지고도 어느정도 수준의 보안 접근제어를 갖는 방화벽시스템을 구현할 수 있다.

- 베스천호스트(Bastion Host)

베스천호스트는 방화벽시스템이 가지는 기능 중 가장 중요한 기능을 제공한다. 따라서 방화벽시스템 관리자는 베스천호스트를 중점적으로 관리하여야다. 방화벽시스템의 주요 기능으로서는 접근제어 및 응용 게이트웨이로서 가상서버(Proxy Server)의 설치, 인증, 로그등을 담당하게 된다. 이 호스트는 외부로부터의 침입대상이기 때문에 일반 사용자의 계정을 만들지 않고 해킹의 대상이 될 어떠한 조건도 두지 않는 가장 완벽한 시스템으로서 운영되어야 한다.

- 이중 네트워크 게이트웨이(Dual-Homed Gateway)

이중네트워크 게이트웨이는 2개 이상의 네트워크에 동시에 접속된 호스트를 말한다. 2개의 네트워크은 즉 사설네트워크와 인터네트를 의미하고 사설네트워크와 인터네트간의 유일한 경로를 제공한다. 즉 동적인 경로배정과 경로정보전달을 배제하므로 모든 트래픽은 이 호스트를 통과하도록 한다. 따라서 베스천호스트의 기능을 여기에 구현하면 되는 것이다.

• 스크린호스트 게이트웨이(Screened Host Gateway)

스크린호스트 게이트웨이는 가장 많이 사용되는 방화벽시스템 구성 방식으로 이 스크린호스트을 사설네트워크에 내부에 설치하여 스크린라우터가 내부로 들어가는 모든 트래픽을 스크린호스트에게만 전달되도록 구성하는 것이다. 또한 스크린라우터는 사설네트워크에서 인터네트로 나가는 모든 트래픽에 대해서도 스크린호스트에서 출발한 트래픽만 허용하고 나머지는 거부한다. 이 스크린호스트도 결국 베스천호스트, 이중네트워크 게이트웨이의 개념이 집합된 시스템이다.

• 스크린서브네트(Screened Subnet)

스크린 서브네트는 일명 "Secure Subnet"이라고도 하며, 완충지대의 역할을 하는 서브네트를 인터네트와 사설인터네트 사이에 두는 것이다. 따라서 인터네트와 사설 네트워크에서 서브네트로 접근이 가능하지만, 인터네트에서 서브네트를 직접 통과하여 사설 네트워크에 접속할 수 없다. 다만 스크린라우터를 이용하여 필터링된 패킷만 사설 네트워크에 접근할 수 있다. 그러므로 어떤 기관에서 외부로 공개할 정보서버 즉, 익명의 FTP서버, 고퍼(Gopher) 서버, 월드와이드웹(WWW)서버 등을 서브네트에 설치하여 운영하면 된다.

• 응용 게이트웨이(Application Gateway)

인터네트 상에서 많은 소프트웨어들은 중간전달 (Store-and-Forward) 방식으로 동작한다. 예를들면 e-mail 시스템이나 USENET 의 뉴스 등이다. 이 응용 게이트웨는 가상서버(Proxy Server)라는 클라이언트/서버 기능을 제공한다. 예를 들면 인터네트상에서 임의의 전자우편 클라이언트가 사설네트워크의 어떤 호스트내 전자우편 서버와 접속 하기를 원한다면 중간에 가상서버가 이를 받아 다시 사설네트워크의 서버에게 전달하는 방식이다.

4.1.3 방화벽시스템의 구축

방화벽시스템의 구축은 기관의 정책과 사용의 용이성 그리고 안전성의 중요도에 따라 결정된다. 방화벽시스템을 설치하여 운영할때 제공할 서비스에 대한 기본방침은 다음과 같다.

- 허가 사항에서 명시적으로 밝히지 않은 것외에는 모두 금지 한다 : 방화벽시스템은 모든것을 일단 차단하도록 설계되어야 하며, 서비스 요구와 내재된 위험성 정도에 따라 서비스를 제공한다. 이 방식은 사용자들에게 직접적인 영향을 주게되며 방화벽시스템이 방해물로 인식될 수도 있다.
- 금지 사항중에서 명시적으로 밝힌것 이외에는 모두 허가한다. : 시스템 관리자가 수신 모드에서 사용자들이 방화벽시스템의 안전에 위협하는 종류의 행위들이 무엇인가를 예측하여 이를 방어하는 대책을 강구하도록 한다. 이는 필수적으로 방화벽 관리자가 끊임 없는 악의의 사용자들과 대응하게 된다.

위의 두가지 기본방침에 따라 보호하고자 하는 사설네트워크의 서비스 및 위협의 정도를 고려하여 방화벽시스템을 구성하고 이를 운용해야 한다. 그림4-3은 베스천호스트와 스크린서브네트를 이용하여 구성한 방화벽시스템의 한 예를 나타냈다. 인터네트와는 스크린라우터로 연결하며 인터네트와의 접속점에는 스크린서브네트가 구성되어 하나의 완충지대를 만들고 여기에 외부로 공개하는 FTP서버, WWW 서버, Gohper 서버 등를 운영할 수 있다. 그리고 내부로 들어가는 모든 트래픽은 베스천호스트를 거쳐야 하며 베스천호스트에서는 허용된 네트워크 서비스별로 가상서버를 운영하고 있다.

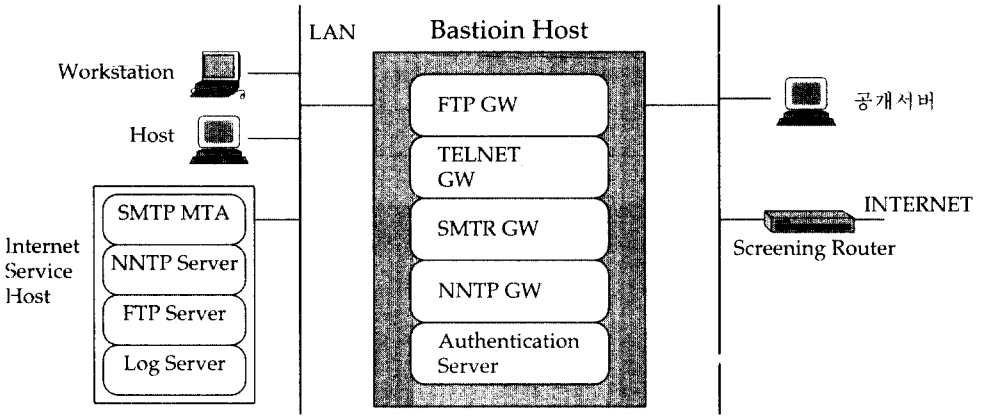


그림 4-3 방화벽시스템 구축예[6]

4.2 초고속 정보통신망 상에서의 방화벽 설치

현시점에서 초고속 정보통신망과 인터네트과의 접속방법은 앞에서 제시한 대로 ATM을 기반으로 하는 초고속 정보통신망과 TCP/IP를 기반으로 하는 인터네트 프로토콜을 상호 매핑 시켜주는 CISCO 7000 이나, NETEdge 시스템를 사용할 수 밖에 없다. 이는 통신망 진화의 특성상 기존의 통신망을 수용하기 위한 최선의 대안일 것이다. 따라서 초고속 정보통신망의 최대 장점인 고속의 전송속도를 제공하는데 있어서 인터네트와 접속되는 지점에서 병목현상이 발생하는 단점도 있으나 기존의 인터네트 사용자들을 그대로 수용하는 잇점도 있다.

초고속 정보통신망과 인터네트이 접속된 상황하에서 통신망 보안을 위한 방화벽 설치는 기존의 인터네트상에서 사용한 방식을 응용하면 가능하다. 즉, 그림 4-4에 나타낸 바와 같이 CISCO 7000 나 NETEdge 시스템을 스크린라우터로 이용하고 각각의 LAN종류에 따라 베스천호스트를 독립적으로 구성하면 방화벽시스템을 설치할 수 있다. CISCO 7000 장치는 사설 네트워크 내부로 유입되는 패킷의 헤더를 보고 각각의 IP 주소에 맞게 전달되고 이 시점에서 불법침입자에 대한 스크린 기능을 수행한다. 스크린라우터를 통과한 패킷은 베스천호스트에서 네트워크 서비스의 보안을 위하여 가상서버(Proxy Server)를 운용하고 어떠한 네트워크 서비스를 제공할지 결정된다. 외부 인터네트과의 접속은 T1(1.5 Mps) 나 T3(45 Mbps) 급의 전송속도로 스크린라우터를 통하여 연결하고 외부 인터네트과의 접속점에는 스크린 서브 네트워크를 구성하여 하나의 안전지대를 만든다. 이곳에 외부로 공개하는 각종 서버들 즉, WWW, FTP, Gopher 서버등을 운용한다.

그리고 내부로 유입되는 모든 트래픽은 LAN 의 종류에 따라 각각의 베스천호스트를 통과함으로써 베스천호스트에서 허용하는 네트워크 서비스만을 제공한다. 베스천호스트에서 네트워크 서비스에 대한 보안을 위하여 가상서버를 운영한다. 현재 널리 사용되는 가상서버들은 Telnet 가상서버, Rlogin 가상서버, FTP 가상서버, WWW 가상서버, TCP Wrapper, SMTP Wrapper, 인증 서버 등이 있다.

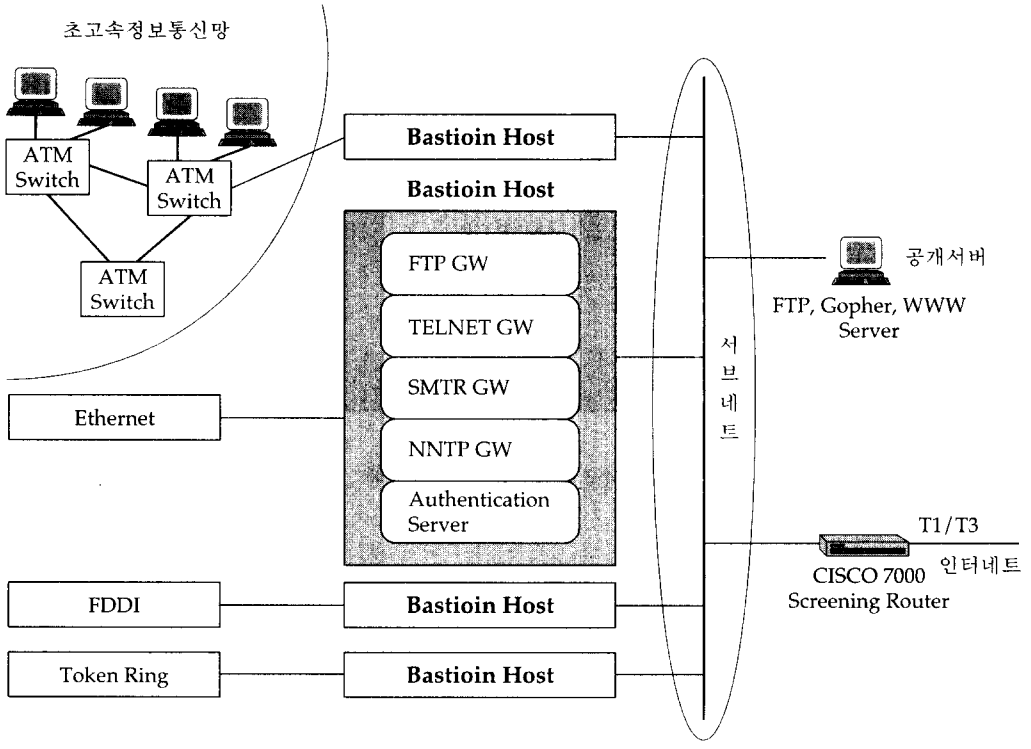


그림 4-4 초고속정보통신망과 인터네트 접속하에서 방화벽 구축 예

5. 결 론

지금까지 초고속 정보통신망 상에서의 통신망 보안에 관한 국내외의 현황을 살펴보았으며, 초고속 정보통신망과 인터네트이 접속되었을때 통신망 보안을 위한 방화벽시스템 구성 모델을 제시하였다. 이 모델은 통신망의 백본이 초고속 정보통신망 즉, ATM 을 기반으로 하는 망으로 구성이 되지않고, 인터네트와의 접속을 위하여 저속의 인터페이스를 그대로 수용하는 상황하에서 구성되었다. 이 모델은 방화벽시스템을 구성할 수 있는 여러방식들 중에 하나이며 최상의 해결책이 아닐수도 있다. 그러나 초고속 정보통신망으로 진화하는 중간 단계에서 방화벽시스템을 구축을 위한 해결책으로서 사용될 수 있을 것이다.

끝으로 초고속 정보통신망상에서의 보안을 유지하기 위해 정부가 해야할 일을 제시하고자 한다. 첫째, 현재 추진중인 가칭 정보보호센터의 설립을 촉진하여 국가적 차원에서 체계적인 통신망, 정보, 서비스 등의 보안 작업이 이루어져야 한다. 둘째, 통신망 사용자에게 보안의 중요성을 확산 시키는 작업이 요구된다. 세째, 초고속 정보통신망 보안과 관련된 연구개발의 다양화와 대폭적인 지원이 필요하다. 네째, 민간기업이 스스로 통신망 보안 및 서비스 보안의 중요성을 인식하여 보안관련 기술들을 개발할 수 있도록 유도해야 할 것이다.

참 고 문 헌

[1] John P. Wack, Lisa J. Carnahm,

"Keeping Your Site Comfortably Secure : An Introduction to Internet Firewalls", http: / / www.tis.com / Home / NetworkSecurity / Firewalls / Firewalls.html

[2] Lawrence J. Haas, National infornation infrastructure security issues From Release "NII Security : The Federal Role", http: / / iitf.doc.gov, June 14, 1995

[3] Marcue J. Ranum, "Thinking About Firewalls", http: / / www.tis.com / Home / NetworkSecurity / Firewalls / ThinkingFirewalls.html

[4] Marcue J. Ranum, "A Network firewalls", http: / / www.tis.com / Home / NetworkSecurity / Firewalls / Thinking Firewalls.html

[5] TIS, Firewalls FAQ, http: / / www.lib.ox.ac.uk / internet / news / faq / archive / firewalls-faq.html

[6] "인터네트 방화벽시스템의 개념과 구현", http: / / nms.etri.re.kr / pub / security / doc / firewall.doc

[7] 임채호, 정진욱, "인터네트 방화벽시스템의 구축방법과 연구개발 현황", 정보보호학회지 제4권 제3호 1994.9

□ 著者紹介

문 필 주

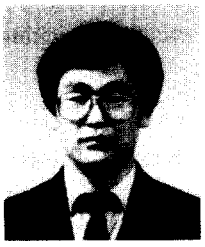
1988년 2월 숭실대학교 전자계산학과 학사
1991년 8월 숭실대학교 전자계산학과 석사
1993년 8월 ~ 현재 숭실대학교 전자계산학과 박사과정
1988년 2월 ~ 현재 한국전자통신연구소, 선임연구원

※ 관심분야 : B-ISDN, ATM 트래픽 제어, 통신망 보안

고 병 도

1981년 2월 숭실대학교 전자계산학과 학사
1983년 2월 숭실대학교 전자계산학과 석사
1993년 3월 ~ 현재 충남대학교 전자계산학과 박사과정
1983년 3월 ~ 현재 한국전자통신연구소,광대역서비스연구실장

※ 관심분야 : 데이타베이스, 망관리, 정보통신망구조



전 문 석

1980년 2월 숭실대학교 전자계산학과 학사
1986년 12월 University of Maryland at College Park, 전산학 석사
1989년 12월 University of Maryland at College Park, 전산학 박사
1989년 1월 ~ 1989년 7월 Morgan State University 전산수학과 조교수
1989년 7월 ~ 1991년 2월 New Mexico State University Physical Science Lab 책임연구원
1993년 3월 ~ 현재 숭실대학교 정보과학대학 부교수

※ 관심분야 : 병렬 컴퓨터설계, 병렬알고리즘, 암호화 설계

이 철 희

1958년 2월 육군사관학교 이학사
1962년 2월 Purdue University, 전자공학과 석사
1988년 2월 중앙대학교 전산학과 박사
1962년 9월 ~ 1973년 4월 육군사관학교 전자공학과 조교수
1988년 3월 ~ 1994년 2월 숭실대학교 정보과학대학원 원장
1988년 11월 ~ 1990년 12월 한국정보과학회 회장
현재 숭실대학교 정보과학대학 교수

※ 관심분야 : 데이터 통신, 전산망 구성, 통신망 프로토콜