인터넷 방화벽 보안 정책

박진섭*, 김 강*, 신재호**, 이민섭***, 박정현****, 임휘성****, 임채호****

대 전 대학교 컴퓨터공학과*, 동 국 대학교 전자공학과**
단 국 대학교 수 학 과***, 한 국 정 보 보 호 센 터****

A Study on Internet Firewall Policy

Jinsub Park*, Kang Kim*, Jaeho Shin**, Min-surp Rhee***
JungHyun Park****, Hwi-sung Im****, Chaeho Lim****

*Taejon Univ., **Dongguk Univ., ***Dankook Univ., ****KISA

<요 약> 본고에서는 인터넷 방화벽 보안정책을 일반 정보 보안정책 수립 절차와 단계에 입각하여 분석하고, 위험처리 등급은 3 단계(낮음, 중간, 높음)로 구분하며, 보안정책 대상은 사용자, 관리자, 기술요원으로 나누어 각각의 방화벽 보안정책을 제시한다. 또한 네트워크 서비스를 방화벽에서 처리할 때 허용여부와 허용시에 사용 되어야할 인증 등의 보안정책을 제시한다.

1. 배 경 과 목 적

많은 기관은 자신의 LAN을 인터넷에 연결하고 그 사용자들은 인터넷 서비스를 편리하게 접근할 수 있기를 원한다. 전체적으로 인터넷을 신뢰하지 않기 때문에 자신의 사설 시스템은 외부 공격과 오용에 취약할 수 있다. 방화벽은 안전장치로 신뢰하는 네트워크와 덜 신뢰하는 네트워크 사이에 접근 제어를 하는 것이다. 방화벽은 단일 요소가 아니며 조직의 인터넷을 보호하기 위한 전략이다. 방화벽은 비신뢰 네트워크와 좀 더 신뢰하는 내부 네트워크 사이에 출입문 역할을 한다. 방화벽의 주 기능은 접근 제어를 집중화하는 것이다. 외부 혹은 원격 사용자가 방화벽을 통과하지 않고 내부 네트워크를 접근할 수 있다면 그 효용성은 희석된다.

방화벽은 조직의 인트라넷 세그먼트를 보호하기 위해 사용될 수 있다. 그러나 여기에서는 방화벽 정책의 인터넷 측면을 집중하여 다루고자 한다.

방화벽은 다양한 형태의 보호를 제공한다.

- 방화벽은 원하지 않는 트래픽을 막을 수 있다.
- 방화벽은 좀 더 신뢰하는 내부 시스템에 입력되는 트래픽을 안내한다.
- 방화벽은 인터넷으로부터 쉽게 보호될 수 없는 취약한 시스템을 숨긴다.
- 방화벽은 자신의 네트워크를 통과하는 트래픽을 로그 할 수 있다.
- 방화벽은 시스템 이름, 네트워크 토폴로지, 네트워크 장비형태, 인터넷으로부터 내부 사용자 ID를 감출 수 있다.
- 방화벽은 응용시스템에 보다 공고한 인증을 제공할 수 있다.

---

* 본연구는 '97년 정보통신 국책과제인 "정보시스템 침해사고 방지기술 개발" 과제로서 수행중 입니다.

2. 보안 정책 개발 기본 접근법

일반적으로 보안정책의 개발은 Fites[5]에 의해 제시된 단계로 이루어진다.
그 단계로는 다음과 같다.

(1) 보호대상을 명시하기.
(2) 무엇으로부터 보호할 것인지를 결정.
(3) 있음직한 위협을 결정.
(4) 경제적인 요소를 고려하여 자산(asset)을 보호할 수 있는 방법을 구현.
(5) 정기적인 재검토를 통하여 취약점 발견시 갱신.

효율적인 계획을 세우기 위해 어떤 단계도 간과해서는 안된다. 진부할 수 있지만 보안시, 예방비용이 회복하는데 드는 비용보다 덜 투자된다는 것을 염두해 두어야 한다. 이에 관련해서 비용은 실제 통화, 평판, 신용, 그 밖에 측정도구 등에 의해 나타나는 손실을 포함하게 된다. 보호대상과 가능한 위협에 대한 지식이 없이 이런 규칙을 적용해서는 안된다.

3. 위 험 평 가

3.1 일반적인 견해

보안정책을 만드는 가장 중요한 이유 중의 하나가 경제적인 요인에 의한 것이다. 그러나 보안의 대상을 잘못 파악할 수 있다. 예를 들어 시스템에 침입자에 대해 공표한 정책이 있다고 하자. 대부분의 기관에서, 보안에 대한 대부분의 검사는 오히려 내부자로부터 손실을 많이 받는다는 것을 보여준다.

위험 분석법은 보호대상, 무엇으로부터 보호해야 할 지를 그리고 보호방법을 결정하는 과정을 포함한다. 이 분석법은 모든 위험을 시험하고 보안단계에 의해 위험들의 순위를 매기는 과정이다. 그리고 보호대상에 대한 경제적인 요인을 고려하여 결정을 하는 것을 포함한다. 대개 실제로 가치 있는 것보다 임의의 것을 보안하는데 투자하기가 더 힘들다. 위험 분석법은 [5]와 [6]에 잘 나타나 있다.

보안의 기본 목표는 유효성, 기밀성, 무결성이다.

3.2 자산 명시

위험분석법의 한 단계는 보호되어야 할 대상들을 명시하는 것이다. 가치 있는 특허정보, 지적 자산 그리고 하드웨어의 다양한 부분들과 같은 대상들은 분명히 보호가 필요하다. 그러나 시스템을 실제로 사용하는 사람의 경우를 감시해야 한다. 기본적인 요지는 보안문제에 영향을 주는 모든 일들을 목록화하는 것이다.

다음의 리스트는 Pfleeger[6]가 제시한 것이다.

(1) 하드웨어 : CPU, board, keyboard, terminal, workstation, PC, printer, disk drive, communication line, terminal server, router
(2) 소프트웨어 : 소스프로그램, 목적프로그램, 유틸리티, 진단프로그램, 운영 체제, 통신 프로그램 등등
(3) 데이터 : 실행하는 동안 통신 매체를 통과한 저장된 온-라인 , 수행된 오프-라인, 백업, 감시기록, 데이터베이스 등등
(4) 인적자원 : 사용자, 관리자, 하드웨어 유지보수자 등등
(5) 문서화 : 프로그램과 하드웨어 시스템, 부분적인 관리 절차 등에 대한 것
(6) 공급매체 : 종이, 형식, 리본, 자기 매체 등등

3.3 위협 명시

보호를 요구한 자산들이 명시될 때, 그 자산에 대한 위협을 명시해야할 필요가 있다. 그런 후에 위협이 잠재적인 손실을 갖고 있는지를 시험하게 된다. 그 결과는 자산을 보호하기 위해 어떤 위협이 있는지를 알 수 있게 한다. 특정의 사이트에 대한 특정의 위협이 있을 것이다.

(1) 권한 없는 자원과 정보에 대한 접근
(2) 고의가 아닌 또는 권한이 없는 정보의 노출
(3) 서비스의 거부

4. 형식화된 정책의 사용자와 사용시기

적당하고 효과적인 보안정책을 위해, 조직 안의 모든 피고용인의 수용과 지지가 필요하다. 특히 공동관리에 피고용인들이 영향을 줄 수 있는 보안정책절차를 지지하는 것이 중요하다. 아래의 내용은 생성과 관련된 개인목록이고, 보안정책문서의 개관이다.

(1) 사이트보안 관리자
(2) 정보기술 기술스탭진(계산소의 스텝진)
(3) 조직 안의 거대한 사용자그룹의 관리자(사업 분야, 대학 안의 컴퓨터과학과)
(4) 보안사고 대응팀
(5) 보안정책에 영향을 받은 사용자그룹의 대표자
(6) 책임 있는 관리
(7) 법적 자문

4.1 좋은 보안 정책

좋은 보안 정책의 특징은 다음과 같다.

(1) 수용 가능한 사용법 또는 접근 가능한 방법을 발표한 시스템 관리절차를 통해 구현이 가능해야 한다.
(2) 적절한 보안기법이 적용되어야 하고, 보호책이 기술적으로 실행 불가능한 곳에서는 사용에 제약을 가해야 한다.
(3) 사용자, 관리자, 기술요원의 책임영역이 명확히 정의되어야 한다.

좋은 보안 정책의 구성 요소는 다음과 같다.

(1) 컴퓨터기술 도입지침서 - 획득되거나 우선권이 있는 보안 요소를 명시한 구매정책과 지침서가 있는 부록이다.
(2) 프라이버시 정책 - 전자우편의 청취, 키 입력의 등록, 사용자 화일의 접근 등의 문제를 언급한 개인이 사용할 수 있는 권리를 정의한 것임.
(3) 접근 정책 - 사용자와 운영스탭진과 관리에 대한 사용지침을 명시함으로써 접근권리와 손실 또는 발표에 의해 자산을 보호하는 특권을 정의함.
이 정책은 장치와 네트워크를 연결하고 새로운 소프트웨어와 시스템을 추가함으로써 외부 접속과 데이터 통신에 지침을 제공한다.
(4) 계정 정책 - 사용자, 운영 스탭진, 관리에 대한 책임을 정의함.
이 정책은 감시능력을 명시하고, 사고을 다루는 지침을 제공한다.
(5) 인증 정책 - 원거리 위치 인증의 지침과 인증 장치의 사용을 설정함으로써 효과적인 패스워드 정책을 통해 신뢰를 인증함.

(6) 자원의 유용성에 대한 언급 - 이 언급은 작동시간과 유지보수, 고장시간을 명시함으로써 복구문제에 역점을 두어 설명한다.

(7) 정보기술시스템과 네트워크 유지정책- 내·외부의 유지보수요원이 어떻게 기술을 다루고 접근하는지에 대해 표현을 함. 여기에서 다루는 중요한 주제는 원격에서의 유지보수의 허용여부와 어떻게 이러한 접근을 통제하는가에 대한 것이다. 또 고려해야할 대상은 외부에서 구입하여 조립하는 것이 어떻게 관리되는 지에 대한 것이다.

(8) 위반 보고 정책 - 침해 형태와 보고서 작성자에 의해 침해를 보고하는 정책. 대부분 위협이 되지 않는 상황과 가능한 한 익명의 보고서로 침해발견을 보고할 것이다.

(9) 각 정책위반형태에 대한 정보를 사용자, 스텝, 관리자에게 제공하는 정보 - 보안사건이나 비밀스럽거나 소유권이 요구되는 정보에 대한 외부로부터의 질문을 어떻게 다룰 것인가에 대한 지침서.
그리고 보안절차와 회사 정책이라든가 정부 법안과 규칙과 같은 관련된 정보를 알기 위해서는 이 책을 참조해야 한다.

보안정책은 사용자와 스텝, 관리간에 의사소통을 하기 위해 시작되었다. 정책을 따르기 위한 과정은 개별적인 표시를 가져야 한다. 정책은 성공적으로 보안요구를 충족시킬수 있다는 조건하에서 법적 근거를 가지고 검토하여야 한다.

5. 인 증

방화벽을 기반으로 한 라우터는 사용자 인증을 제공하지 않는다. 따라서 더 향상된 보안을 위해서 방화벽을 기반으로 한 방어거점(Bastion)호스트를 두어 다음과 같은 종류의 인증을 제공할 수 있다.

- 사용자 이름/패스워드 : 그 정보가 반복 시행으로 노출될 수 있기 때문에 가장 취약한 종류이다.
- 1회용 패스워드 : 소프트웨어나 하드웨어 토큰을 사용한 1회용 패스워드는 매 세션마다 새로운 패스워드를 생성한다. 이것은 과거 패스워드가 재사용 될 수 없어 노출되거나 도둑맞을 염려가 없음을 의미한다.
- 전자서명 : 공개키 암호를 사용하여 생성된 서명을 사용한다.

6. 방 화 벽 타 입

방화벽은 다양한 방법으로 구현될 수 있다.

표 1 은 다양한 방화벽 구조를 나타내며 그 등급은 **"낮음", "중간", "높음"**이라는 위험처리 환경으로 분류된다.

6.1 패킷 필터링 게이트웨이

패킷 필터링 방화벽은 매우 저가격의 최저 보안을 제공하고 **"낮음"** 위험환경에서 선택될 수 있다. 이것은 빠르고 유연성이 있으며 투명하다. 필터링 규칙은 라우터 상에서 쉽게 유지되지 않는다. 따라서 규칙을 유지하고 생성하는 일을 간단히 하기 위해 툴(Tool)이 존재한다. 필터링 게이트웨이는 타고난 위험을 가지고 있다.

즉, - IP 패킷 헤더에 포함된 소스, 목적지 주소와 포트가 유일한 정보로 내부 네트워크에

트래픽 접근을 허용할 것인지 여부를 결정한다.
- IP 혹은 DNS 주소 속임수에 대해 방어하지 못한다.
- 공격자는 방화벽에 의해 일단 승인되면 내부 네트워크에 접속된 어떤 호스트로의 접근도 가능하다.
- 강력한 사용자 인증이 많은 패킷 필터링 게이트웨이에서 지원되지 않는다.
- 아주 미미하거나 거의 쓸모없는 로깅을 제공한다.

6.2 응용 게이트웨이

응용 게이트웨이는 방화벽 상에서 수행하는 서버 프로그램(Proxy)을 사용한다. 이들 프록시는 외부의 요청에 대하여 그들을 시험하고 적절한 서비스를 제공하는 내부 호스트에 적법한 요구를 전달한다. 응용 게이트웨이는 사용자 인증과 로깅 같은 기능을 제공할 수 있다. 응용 게이트웨이가 안전한 방화벽으로 여겨지기 때문에 이 구성은 **"중간-높음"**의 위험 사이트에 많은 장점을 제공한다.

- 방화벽이 네트워크 외부에서 볼 때 단지 하나의 호스트 주소로 구성된다.
- 다양한 서비스를 위한 프록시들의 사용은 불안전하거나 잘못구성된 내부호스트를 가진 기업을 보호하기 위하여 내부 네트워크 상에 있는 서비스를 직접 접근하지 못하도록 방어 한다.
- 강력한 사용자 인증이 응용 게이트웨이에 장착될 수 있다.
-프록시는 응용수준에서 자세한 로깅을 제공할 수 있다.

응용레벨 방화벽은 트래픽이 방화벽에서 출발한 것처럼 나타나게 구성될 수 있다(즉 단지 방화벽만이 네트워크 외부에 보여진다)..

Telnet, FTP, HTTP, RLOGIN 등과 같은 다양한 네트워크 서비스를 받기위해 들어오는 모든 요청은 방화벽 상의 적절한 프록시를 통과해야만 한다.

응용 게이트웨이는 방화벽을 통하여 지원되는 각 서비스(FTP, HTTP 등)마다 프록시를 요구한다. 프록시에 의해 지원되지 않는 서비스가 요청될 때 그 조직은 3가지 선택이 가능하다.

- 안전한 프록시를 방화벽 공급자가 공급할 때까지 서비스를 거부하는 방법
- 사용자가 프록시를 개발하는 방법
- 방화벽을 통과시켜 서비스를 제공하는 방법

"낮음"

프록시에 의해 지원되지 않는 인터넷 서비스가 방화벽 통과를 요구할 때 방화벽 관리자는 요구된 서비스를 허락할 구성과 플러그를 정의해야만 한다. 방화벽 공급자로부터 프록시가 제공될 때는 그 플러그를 제거하고 프록시가 운용하게 한다.

"중간-높음"

방화벽의 프록시 소프트웨어에 의해 인터넷 서비스가 처리되어야만 한다. 만약 새로운 서비스가 요청된다면 그 서비스는 프록시가 확보되고, 관리자에 의해 테스트 될 때까지 연기하여야 한다.

6.3 복합 게이트웨이

복합 게이트웨이는 앞서의 방화벽 형태를 두 개 이상 결합한 것이며 병렬이 아닌 직렬의 형태로 구현된다. 직렬로 연결된다면 보안은 더욱 강화된다. 반면에 병렬로 연결된다면 네트워크 보안 척도는 가장 낮은 보안 척도의 방화벽으로 보호될 것이다. **"중간-높음"**의 위험 환경에서 복합 게이트웨이는 이상적인 방화벽 구현이 될 수 있다.

6.4 등 급

다양한 방화벽 형태에 대한 등급은 다음과 같이 나타낼 수 있다.

표. 1. 방화벽 보안 위험

방화벽 구조	"높음" 위험 환경 예 : 병원	"중간" 위험 환경 예 : 대학	"낮음" 위험 환경 예 : 꽃집
패킷 필터링	0	1	4
응용 게이트웨이	3	4	2
복합 게이트웨이	4	3	2

0 : 부적합, 1 : 최소 보안, 2 : 대체로 적합, 3 : 효율적 선택, 4 : 권고되는 선택

7. 방 화 벽 구 조

각 기관은 자신의 위험에 따라 방화벽 구조형태를 선택해야만 한다.
다음은 전형적인 방화벽 구조를 설명하고 정책 예문을 제시한다.

7.1 Multi-homed host

Multi-homed host는 하나 이상의 네트워크 인터페이스를 가지는 호스트(이 경우에 방화벽)이다. 이 때 각 인터페이스는 논리적, 물리적으로 분리된 네트워크에 연결된다.
Dual-homed host (두개의 인터페이스를 가진 호스트)는 가장 보편적 Multi-homed host이다. Dual-homed 방화벽은 두 개의 네트워크 인터페이스 카드를 가지는 방화벽으로 서로 다른 네트워크에 연결된다.

" Dual-homed 방화벽에 의한 라우팅은 임의의 네트워크로부터 들어온 IP 패킷을 직접 다른 네트워크에 라우트 하지 않는다."

7.2 Screened host

Screened host 방화벽 구조는 모든 외부 호스트가 내부 호스트에 직접 연결되지 않고 중간 호스트(베스천 호스트라함)에 연결하여 사용한다. 이렇게 하기 위해서는 필터링 라우터가 구성되어 외부 네트워크로부터 내부 네트워크로의 모든 연결이 베스천 호스트를 향하도록 구성한다.

패킷 필터링 게이트웨이가 사용된다면 외부 네트워크로부터의 모든 연결은 회사 네트워크와 외부세계 사이에 직접 인터넷 연결을 방지하기 위해서 베스천 호스트를 통하도록 한다.

7.3 Screened Subnet

Screened Subnet 구조는 본질적으로 Screened host 구조와 같으나 내부 네트워크로부터 분리되어 베스천 호스트가 위치한 네트워크(Perimeter network라고 함)를 생성시켜 보안 등급을 더 추가한 것이다. 이것은 베스천 호스트를 성공적으로 공격한다 할지라도 그 공격자는 내부와 주변 네트워크 사이에 연결된 스크린 라우터에 의해 주변 네트워크를 보호한다.

8. 인 트 라 넷

방화벽이 내부 네트워크와 외부 네트워크 사이에 항상 위치하더라도 대규모 회사 혹은 기관에서 방화벽은 네트워크의 다른 서브네트 사이에 종종 사용된다(Intranet이라 함). 인트라넷 방화벽은 전체 조직의 네트워크로부터 특정 서브넷을 고립시키기 위함이다. 네트워크 세그먼트의 고립화 이유는 "알 필요가 있는" 특정 고용인만 이 방화벽의 승인에 의해 서브넷

을 접근할 수 있도록 하기 위함이다. 그 예는 기관의 예산 회계 부서만을 위한 방화벽이다. *"회사의 중요한 응용이나 민감하거나 기밀한 정보에 접근을 제공하는 시스템 호스트 경우에 내부 방화벽 혹은 필터링 라우터가 감사와 로깅을 지원하고 강력한 접근통제를 제공하기 위해 사용되어야 한다. 이들 통제는 정보 설계 소유자에 의해 개발된 접근 정책을 지원하기 위하여 내부 회사 네트워크를 세그먼트 하기 위해 사용되어져야 한다".*

9. 방 화 벽 관리

다른 네트워크 장치와 마찬가지로 방화벽은 누군가에 의해 관리되어야 한다. 보안정책은 방화벽 관리책임이 누구인지 언급해야 한다. 두명의 방화벽 관리자(주, 보조)는 정보보안 부서장에 의해 지명될 수 있다. 주 관리자는 방화벽을 변경할 수 있고, 보조 관리자는 단지 주 관리자 유고시에만 조작해야 하며 동시에 접근해서는 안된다. 각 방화벽 관리자는 그 집 전화번호, 삐삐번호, 휴대폰 번호, 기타 번호나 코드로 지원이 요청될 때 접속 할 수 있어야 한다.

9.1 방화벽 관리자 자질

일상적 방화벽 관리를 위해 일반적으로 두명의 경력자를 권고한다. 이와같은 방법으로 방화벽 관리기능의 가용성은 극대화된다.

사이트 보안은 그 기관의 일상 업무행위에 중요하다. 그러므로 방화벽의 관리자는 네트워크 개념과 구현의 이해를 하고 있을 것이 요구된다. 예를 들면 대부분의 방화벽은 TCP/IP 기반이기 때문에 이 프로토콜의 전체적인 이해가 필수적이다.

" 방화벽 관리 직무를 할당받은 개인은 네트워크 개념, 설계, 구현 경험을 가지고 있어야 한다. 이는 방화벽이 적절히 관리되고 정확히 구성되어지기 위함이다. 방화벽 관리자는 네트워크 보안 원리와 실제 그리고 사용에 있어서 방화벽에 대한 정기적 훈련을 받아야 한다."

9.2 원격 방화벽 관리

방화벽은 공격자에게 보이는 1차 방어선이다. 방화벽은 일반적으로 직접 공격하기가 어렵다. 공격자는 방화벽에 대하여 종종 관리 계정을 목표로 한다. 관리 계정의 사용자 이름/패스워드는 엄격히 보호되어야 한다. 이러한 공격으로부터 가장 안전한 보호방법은 방화벽 호스트 주위에 강력한 물리적 보안을 하는 것이며, 접속된 터미널로만 방화벽 관리를 허용하는 것이다. 그러나 운영상 종종 방화벽 관리가 원격 접근 형식으로 이루어진다. 이때 강력한 인증 형식 없이 비신뢰 네트워크를 통해 방화벽에 대한 원격접근이 되어서는 안된다.

또한 도청을 예방하기 위하여 세션 암호화가 원격 방화벽 연결시 사용되어야 한다.

"낮음"

방화벽 관리를 위해 비신뢰 네트워크를 통한 원격접근은 1회 패스워드 혹은 하드웨어 토큰 같은 강력한 인증을 사용해야만 한다.

"중간"

방화벽 관리를 위해 위에 언급한 방법이 직접 접속된 터미널로 이루어져야 한다. 방화벽 터미널에 대한 물리적 접근은 방화벽 관리자와 백업 관리자에게만 국한한다. 방화벽 관리의 원격 접근이 허락되어야만 할 때는 회사 내부 네트워크 상의 다른 호스트로만 접근이 제한된다. 그러한 내부 원격 접근은 강력한 인증 방법이 사용되어야 한다. 인터넷 같은 비신뢰 네트워크를 통한 원격접근은 양단에서의 암호화와 강력한 인증이 요구된다.

"높음"

모든 방화벽 관리는 지역 터미널에서만 수행되어야 한다. 방화벽 운영 소프트웨어에 대한 접근이 원격 접근으로는 허용되지 않는다. 방화벽 터미널에 대한 물리적 접근은 방화벽 관리자와 백업 관리자에만 국한한다.

9.3 사용자 계정

방화벽은 결코 일반목적 서버로 사용되어서는 안된다. 단지 방화벽에 대한 사용자 계정은 방화벽 관리자와 백업 관리자에게만 주어져야 한다. 또한 단지 이들 관리자들은 시스템 수행을 갱신하거나 기타 시스템 소프트웨어에 대한 권한이 주어진다.

" 방화벽 관리자와 백업 관리자에게만 회사 방화벽에 사용자 계정을 준다. 방화벽 시스템 소프트웨어의 수정은 방화벽 관리자 혹은 백업 관리자에 의해서만 수행되어야 하고 네트워크 서비스 관리자의 인가를 요구한다."

9.4 방화벽 백업

고장이나 자연재해 발생시 복구하기 위해 다른 네트워크 호스트와 마찬가지로 방화벽은 시스템 백업을 정의하는 어떤 정책을 가지고 있어야만 한다. 시스템 구성 파일과 마찬가지로 데이터 파일은 방화벽 고장의 경우에 백업 계획을 가질 필요가 있다.

방화벽(시스템 소프트웨어, 구성 데이터, 데이터 파일 등)은 일일, 주간, 월간 백업이 되어야만 하며, 시스템 고장의 경우에 데이터와 구성파일이 복구할 수 있어야 한다. 백업파일은 읽기전용 매체에 안전하게 저장되어야 하며, 저장된 데이터는 부주의에 의해 덮어쓰기가 되지 않도록 해야 하며, 단지 적절한 사람에게만 접근되어야 한다.

또 다른 백업은 현재의 방화벽 고장시 안전하게 운용할 수 있도록 또 다른 방화벽을 더 구축하는 것이다. 이와같은 백업 방화벽은 앞서의 방화벽 고장시, 고장 수리시간 동안에 대체될 수 있다.

"적어도 하나의 방화벽이 구성되어야 하며, 방화벽 고장시 대체 될 수 있는 백업 방화벽이 있어야 하며, 이 백업 방화벽은 네트워크를 보호하기 위하여 주 방화벽 고장시 스위치 되어야 한다."

10. 네트워크 신뢰 관계

업무 네트워크는 자주 다른 업무 네트워크 연결을 요구한다. 그러한 연결은 WAN, VAN, 인터넷 같은 공공 네트워크를 통한 임대회선으로 할 수 있다. 예를 들면 많은 기업은 국가간의 업무를 연결하기 위해 상업 VAN을 사용한다. 결합된 다양한 네트워크 세그먼트가 다른 조직의 통제하에 있을 수 있으며, 다양한 보안정책하에서 운영될 수 있다. 그러한 경우로 네트워크가 연결될 때 전체 네트워크의 보안은 가장 취약한 네트워크 수준으로 저하된다.

네트워크 연결을 결정할 때 신뢰관계가 결합된 모든 네트워크의 보안성 감소를 피하기 위해 정의되어야만 한다. 신뢰 네트워크는 공통 보안서비스를 제공하도록 같은 보안 정책, 보안통제 구현, 절차를 공유하는 네트워크로 정의된다. 비신뢰 네트워크는 보안수준이 알려지지 않은 곳, 예측 불가일 때, 공통의 보안통제를 구현하지 않은 것을 말한다.

"높음"

회사 네트워크로부터 외부 네트워크로의 모든 연결은 네트워크 서비스 관리자에 의해 인가되고 관리되어져야만 한다. 연결은 받아들일 수 있는 보안 통제와 절차를 가지고 있다고 확

인된 외부 네트워크에만 허용되어야 한다. 인가된 외부 네트워크에 대한 모든 연결은 회사에서 인가한 방화벽을 통과해야만 한다.

"낮음-중간"

회사 네트워크로부터 외부 네트워크로의 모든 연결은 네트워크 서비스 관리자에 의해 인가되어야만 한다. 인가된 외부 네트워크에 대한 모든 연결은 회사의 인가된 방화벽을 통해 이루어져야만 한다.

주요 취약점을 제거하기 위하여 외부 네트워크 연결과 관련한 모든 연결과 계정은 정기적으로 검토되고 더 이상 필요가 없는 것은 삭제하여야 한다. 외부 네트워크 연결과 관련한 감사추적과 로그는 매주 단위로 검토되어야 한다. 월 단위로 사용되지 않는 연결 계정은 삭제되어야 한다. 네트워크 서비스 관리자는 주단위 연결이 필요한지의 타당성을 담당 관리자에게 문의해야 한다. 네트워크 시스템 관리자에 의해 특정 네트워크에 더 이상 연결이 필요없다고 통지되면 그 연결과 관련한 파라메터는 1일 이내에 삭제되어야 한다.

11. 가상 사설 네트워크 (VPN)

가상 사설 네트워크 (Virtual Private Network)는 신뢰된 네트워크가 인터넷같은 비신뢰 네트워크를 통하여 다른 신뢰 네트워크와 통신하는 것을 허용한다.
몇몇 방화벽은 VPN 능력을 제공하기 때문에 VPN 구축을 위해 정책을 정의할 필요가 있다. 공공 네트워크 간의 방화벽 사이의 모든 연결은 공공 네트워크 상을 통과하는 데이터의 사적인 보호와 무결성을 보장하기 위해 암호화된 가상 사설 네트워크를 사용할 것이다.
모든 VPN 연결은 네트워크 서비스 관리자에 의해 허가되고 관리되어야 한다. 적절성이라는 것은 암호키를 분배하고 관리하는 것이 VPN 사용 전에 구축되어야만 함을 의미한다.
VPN을 기반으로 한 방화벽은 많은 다양한 구성으로 구축될 수 있다.

12. D N S 와 메일 문제

인터넷에서 DNS는 도메인 이름을 IP 주소로 매핑하고 변환을 제공한다. 몇몇 방화벽은 주, 부, 혹은 캐쉬 DNS서버로서 수행되도록 구성될 수 있다. DNS서비스를 어떻게 관리하느냐의 결정은 일반적으로 보안 결정은 아니다. 많은 기관이 인터넷 서비스 제공자(ISP)같은 제 3자가 자신의 DNS운영을 하도록 한다. 이 경우에 방화벽은 DNS 캐쉬 서버로서 사용될 수 있다. 그 기관이 자신의 DNS 데이터베이스 관리를 결정한다면 방화벽은 DNS 서버로서 작용할 수 있다. 방화벽이 DNS 서버로서 구성된다면 다른 보안 예방조치가 필요하다. DNS 서버로서 방화벽을 구현하는 장점은 사이트의 내부 호스트 정보를 감추도록 구성할 수 있다는 것이다. 바꾸어 말하면 DNS 서버로 동작하는 방화벽을 가지면 내부 호스트가 내·외부 DNS 데이터를 제한없이 볼 수 있다. 반면에 외부 호스트는 내부 호스트 기계에 대한 정보에 접근할 수 없다.
외부로부터 숨겨진 호스트 정보로서 공격자는 인터넷에 서비스를 제공하는 내부 호스트의 호스트 이름과 주소를 알 수 없을 것이다.
DNS 숨김을 위한 보안정책 : 방화벽이 DNS 서버로서 동작한다면 방화벽은 네트워크에 대

한 정보를 숨기도록 구성되어야만 하며, 그것은 내부 호스트 데이터를 외부 세계에 노출되지 않도록 할 것이다.

13. 시 스 템 무 결 성

방화벽 구성의 불법 수정을 방지하기 위하여 무결성 보장 처리의 어떤 형식이 사용되어야만 한다. 전형적으로 체크섬, 순환잉여검사, 암화해쉬가 런타임 이미지로부터 만들어지고 보호된 매체에 저장되어야 한다. 매번 방화벽 구성은 권한을 가진 자(보통 방화벽 관리자)에 의해 수정되며, 시스템 무결성 온라인 데이터 베이스가 네트워크나 분리된 매체의 파일 시스템에 갱신되고 저장될 필요가 있다. 시스템 무결성 검사로 방화벽 구성 파일이 수정되었다는 것을 알면 시스템이 위태롭게 되었다는 알려야 한다.
방화벽의 시스템 무결성 데이터 베이스는 방화벽이 구성되고 수정되어질 때 갱신될 것이다. 시스템 무결성 파일은 읽기 전용 매체나 오프-라인 저장장치에 저장되어야만 한다. 시스템 무결성은 모든 파일의 리스트를 생성하기 위해 관리자가 수정하고, 교체하고, 삭제하는 방법으로 방화벽은 규칙적으로 검사될 것이다.

14. 문 서 화

방화벽 운영절차와 구성 파라메터가 잘 문서화되고 갱신되고 안전한 위치에 안전하게 유지되는 것은 중요하다. 이것은 방화벽 관리자가 사임하거나 유고 시에 경험자가 그 문서를 읽고 신속하게 방화벽 관리를 맡을 수 있음을 보장한다.
그러한 문서는 또한 보안사고를 야기하는 사건을 수습하도록 지원한다.

15. 물리적 방화벽 보안

방화벽에 대한 물리적 접근은 방화벽 구성 혹은 운영상태에 대한 어떤 권한 있는 변경도 엄격히 통제되어야만 한다.
또한 예방조치로 적절한 경보가 취해질 수 있어야 하고 백업 시스템은 방화벽이 온라인으로 유지되도록 해야 한다. 회사 방화벽이 네트워크 서비스 관리자, 방화벽 관리자, 방화벽 백업 관리자에게만 제한적으로 접근되는 통제된 환경에 위치되어야 한다.
물리적으로 방화벽이 위치한 방은 냉난방기, 가스 경보기 등이 갖추어져야만 한다. 소화기의 위치와 재충전 여부가 규칙적으로 검사되어야 한다. 무정전 서비스가 인터넷에 연결되어진다면 그러한 서비스는 방화벽에도 제공되어야 한다.

16. 방화벽 사고 처리

사고의 보고는 어떤 비정상이 방화벽에 나타나고 로그되는 과정이다. 정책은 생성된 로그 보고가 어떤 형태의 로그이고 무엇을 해야 하는 지를 결정할 것이 요구된다. 이것은 일반 보안 사고 처리 방법과 같다. 다음 정책은 모든 위험 환경에 적용된다. 방화벽은 매일, 주간, 월간으로 모든 기록이 보고되도록 구성되어 필요할 때 네트워크 동작이 분석될 수 있어야

한다. 방화벽 로그는 공격이 검출되는지를 결정하기 위해 주단위로 검사되어야 한다. 방화벽 관리자에게는 E-메일, 삐삐, 혹은 기타의 방법으로 즉시 알려져야 하고 그는 그러한 경고에 즉시 응답해야 한다.

방화벽은 어떤 종류의 스캐닝 도구도 직접 접속되어서는 안되며, 이는 보호되어야 할 정보가 방화벽 외부에 누출되지 않게 한다.

유사한 방법으로 방화벽은 네트워크 보안을 보다 강화하기 위해 Active X와 JAVA같은 네트워크 보안 위협으로 알려진 모든 종류의 소프트웨어 형태와 단절시켜야 한다.

17. 서비스의 복구

일단 사고가 검출되면 방화벽을 다운하고 재구성할 필요가 있다. 만일 방화벽을 다운시킬 필요가 있다면 인터넷 서비스가 중단되거나 예비 방화벽이 운용되어져야 한다. 내부 시스템은 방화벽 없이 인터넷에 연결되지 않아야 한다. 재구성이 완료된 후에 방화벽은 운전상태로 복귀되어야 한다.

방화벽이 중지되었다가 작업 상태로 복귀되기 위한 정책이 필요하다. 방화벽이 중지된 경우에 방화벽 관리자는 어떤 취약성이 있는지 찾고 재구성할 책임이 있다.

18. 방화벽 업 그레이드

방화벽 소프트웨어와 하드웨어 요소가 방화벽 성능을 향상시키기 위하여 업그레이드 될 필요가 있다. 방화벽 관리자는 어떤 하드웨어, 소프트웨어 오류가 있으며 이를 인식해야만 하고 공급자에 의해 업그레이드 되도록 해야 한다.

업그레이드가 필요하다면 고수준의 보안을 유지하기 위해서는 어떤 예방조치가 있어야만 한다. 업그레이드를 위해 작성될 수 있는 정책에는 다음을 포함해야 한다.

방화벽의 성능을 최적화하기 위해서 프로세서와 메모리 용량을 공급자 권고에 따라야 한다. 방화벽 관리는 업그레이드가 요구되는지를 결정하기 위해 방화벽 신규 공급 소프트웨어를 평가해야 한다. 방화벽 공급자에 의해 권고되는 모든 보안 패치는 적기에 구현되어야 한다. 하드웨어와 소프트웨어 요소는 공급자 권고 자료 목록으로부터 얻을 수 있다. NFS가 하드웨어와 소프트웨어 요소를 얻는 수단으로 사용되어서는 안된다. 공급자 사이트의 FTP 혹은 바이러스 검사된 CDROM의 사용은 적절한 방법이다.

방화벽 관리자는 공급자의 방화벽 우편목록 혹은 다른 접촉 방법 등에 주목해야 한다.

19. 방화벽 정책의 개정과 갱신

신기술이 급속히 소개되고 조직은 계속적으로 새로운 서비스가 개시되는 경향이어서 방화벽 보안 정책은 규칙적으로 재검토되어야 한다. 네트워크 요구가 변경되는 만큼 보안정책도 마찬가지이다.

20. 로그와 감사 추적

대부분의 방화벽은 트래픽 로깅과 네트워크 사건에 대한 폭넓은 영역의 능력을 제공한다. 보안 관련사건은 방화벽의 감사 추적 로그에 기록되어야 한다. 포함되어야할 정보는 하드웨어와 디스크 매체 오류,. 로그인/로그아웃 행위, 연결시간, 시스템 관리자 권한의 사용, E-메일 트래픽의 송수신, TCP 네트워크 연결시도, 프록시 트래픽 형의 이동 등이다.

21. 정 책 예

모든 기관은 적어도 "낮음" 수준 정책은 있어야 한다. "중간" 수준은 중간 수준 정책을 추가하고, "높음" 수준은 낮음, 중간, 높음 수준 정책을 추가해야 한다.

"낮음"

사용자

- *인터넷 서비스에 접근하고자 하는 모든 사용자는 회사에선 인준한 소프트웨어와 인터넷 게이트웨이를 사용하여야만 한다.*
- *방화벽은 자신의 개별 네트워크와 인터넷 사이에 우리 시스템을 보호하기 위해 위치하고 있다. 어떤 프로토콜은 동작되지 않거나 반송된다. 만약 업무에 특정 프로토콜이 필요하다면 당신 관리자와 인터넷 보안 담당자에 요청해야만 한다.*

관리자

- *방화벽은 비신뢰 네트워크가 회사 네트워크를 접근하지 못하도록 회사 네트워크와 인터넷 사이에 위치되어야 한다. 방화벽은 NSM에 의해 선택되고 운영될 것이다.*
- *회사 WAN에 접속된 사이트로부터 모든 다른 형태의 인터넷 접근(예 : 전화모뎀)은 금지한다.*
- *인터넷 서비스에 대한 접근을 요구하는 모든 사용자는 회사에서 인준한 소프트웨어와 인터넷 게이트웨이를 사용하여야만 한다.*

기술요원

- *모든 방화벽은 그 구성이 모든 서비스를 거부하는 고장이 있을 수 있으며, 고장 후에 재가동은 방화벽 관리자가 하도록 요구된다.*
- *소스라우팅은 모든 방화벽과 외부 라우터를 무력하게 할 수 있다.*
- *방화벽은 내부 네트워크 주소를 가지고 나타나는 외부 인터페이스 상의 트래픽을 받아들이지 말아야 한다.*
- *방화벽은 모든 세션의 자세한 감사로그를 제고하여 이 로그가 비정상 상태를 찾게 해줄 수 있어야 한다.*
- *보안매체가 로그 기록을 보관하기 위해 사용되어야 하며 이 매체에 대한 접근은 그 권한을 가진 자로만 국한되어야 한다.*
- *방화벽은 오프-라인으로 테스트되며 적절한 구성 검증이 되어야 한다.*
- *방화벽은 모든 외부 서비스를 위해 투명성 있게 구성되어야 한다. 네트워크 서비스 관리자에 의해 인준되지 않는 한 모든 내부 서비스는 방화벽에 의해 가로채기 되어지며 처리*

되어져야 한다.

- *적절한 방화벽 문서가 항상 오프-라인 저장소에 유지되어야 한다. 그러한 정보는 네트워크 다이어그램 뿐 아니라 모든 네트워크 장비의 모든 IP 주소와 외부뉴스서버, 라우터, DNS 서버 등과 같은 인터넷 서비스 제공자(ISP)의 관련 호스트의 IP주소, 패킷 필터 규칙 같은 기타 모든 구성 파라메터 등을 포함해야 한다. 그러한 문서는 방화벽 구성이 변경될 때 마다 갱신되어야 한다.*

"중간"

사용자

- *회사에서 인준한 1회용 패스워드와 하드웨어 토큰을 사용한 강력한 인증이 방화벽을 통하여 내부 시스템으로의 모든 원격 접근에서 요구된다.*

관리자

- *네트워크 보안정책은 방화벽 관리자와 그 밖의 최고위 정보(보안) 관리자에 의해 정기적(최소 3개월마다)으로 검토되어야 한다. 네트워크 연결과 서비스 변경이 요구될 때 그 보안 정책은 갱신되고 인준되어야 한다. 변경이 이루어진다면 방화벽 관리자는 그 변경이 안전하게 구현되고 정책이 수정되도록 해야 한다.*
- *회사 내부의 신뢰 네트워크의 자세한 사항을 방화벽 외부에서 볼 수 없도록 해야 한다.*

기술요원

- *방화벽은 허용되지 않은 모든 서비스를 거부하도록 구성하고 침입자 혹은 사용 잘못을 탐지하기 위해 정기적으로 감사되고 감시될 것이다.*
- *방화벽은 시스템 관리자에게 실시간으로 네트워크 중단, 디스크 공간 부족, 기타 즉각적 조치를 취해야 하는 관련 메시지 같은 즉각적 대처가 필요한 사항을 알려야 한다.*
- *방화벽 소프트웨어는 전용 컴퓨터 상에서 수행되어야 하며 방화벽과 관련없는 컴파일러, 편집기, 통신 소프트웨어 등과 같은 소프트웨어는 삭제되거나 동작시키지 말아야 한다.*

"높음"

사용자

- *회사 시스템으로 업무와 관련없는 인터넷 사용은 금지한다. 인터넷 서비스에 대한 모든 접근은 기록된다. 이 정책의 위반자는 징계 사유에 해당한다.*
- *귀하의 브라우저는 금지된 사이트에 대한 어떠한 접근시도도 귀하의 관리자에게 보고될 것이다.*

관리자

- *회사 시스템으로 업무와 관련없는 인터넷 사용은 금지한다. 인터넷 서비스에 대한 모든 접근은 기록된다. 이 정책의 위반자는 징계 사유에 해당한다.*

기술요원

- *인터넷 서비스에 대한 모든 접근은 기록된다.*

22. 특정 서비스 정책 예

어떤 기관은 강력한 인증없이 몇몇 서비스를 지원할 수도 있다. 예를 들면 Anonymous FTP 서버는 모든 외부 사용자에게 개방된 정보를 다운로드 하도록 허락 할 수 있다. 이 경우에 그러한 서비스는 방화벽 외부의 호스트나 중요한 자료를 갖는 회사 네트워크에 연결되지 않은 서비스 네트워크에 있는 호스트에 있어야 한다.

표. 2 보안 정책의 요약

정 책	Non-Anonymous FTP 서비스	Anonymous FTP 서비스
서버를 방화벽 외부에 위치시킨다.	N	Y
서버를 서비스 네트워크에 위치시킨다.	N	Y
서버를 보호된 네트워크에 위치시킨다.	Y	N
서버를 방화벽 자체에 위치시킨다.	N	N
서버는 누구에게나 인터넷 접근을 허용.	N	Y

표 2. 는 FTP와 같은 서비스를 위해 그러한 정책을 기술하는 방법을 요약한 것이며, 인터넷 서비스별 방화벽 보안정책은 부록에 나타낸다.

23. 결 론

방화벽의 주 기능은 접근 제어를 집중화하는 것이다. 또한 방화벽은 내부 네트워크에 있는 여러 가지 자산을 보호하기 위한 단편적 수단이다. 보호해야 할 다양한 자산의 위험성과 그 가치를 고려한 비용-효과적인 보안정책의 수립이 요구된다. 따라서 보호해야 할 자산에 따라 정보 보안정책은 다양한 형태와 종류로 구성되어진다. 본고에서는 방화벽 보안정책에 대하여 고찰하고 그 정책 예를 제시하였다. 본고에서 정의한 위험의 수준은 "낮음", "중간", "높음"으로 분류하였으며, 정책 적용대상은 사용자, 관리자, 기술요원으로 구분하여 각각의 정책을 제시하였다. 아울러 네트워크 서비스 종류 각각에 대하여 네트워크 내부에서 외부로, 또 외부에서 내부로의 서비스 지원이 현재의 보안기술을 바탕으로 사용자에게 허용가능 여부와 이때 필요한 인증을 제시하였다. 그러나 네트워크 응용서비스가 계속 개발되고 있으며, 새로운 취약점도 계속 나타나고 있으며, 이에따른 보안기술도 급속하게 발전되고 있어 보안기술을 기반으로한 정보 보안 정책들은 적어도 3개월마다 재검토되고 갱신되어져야 한다고 사료된다.

< 참 고 문 헌 >

[1] S. Bellovin, "Security Problems in the TCP/IP Protocol Suite", Computer view, Vol 19, 2, pp. 32-48, April 1989.

[2] B. Chapman and E. Zwicky, "Building Internet Firewalls", O'Reilly and Associates, Sebastopol, CA, 1995.

[3] W.Cheswick and S.Bellovin, "Firewalls and Internet Security: Repelling the Wily Hacker", Addison-Wesley, MA, 1994.

[4] NCSA, "NCSA Firewall Policy Guide", 1995.

[5] M. Fites, P. Kratz, and A. Brebner, "Control and Security of Computer Information Systems", Computer Science Press, 1989.

[6] C. Pfleeger, "Security in Computing", Prentice-Hall, Englewood Cliffs, NJ, 1989.

[7] M. Ranum, "An Internet Firewall", Proceedings of World Conference on Systems Management and Security, 1992.

[8] NIST, "Internet Security Policy : A Technical Guide", 1997, 7

[9] NIST, "Site Security Handbook", 1997, 7

[10] 한국정보보호센터, "Firewall 시스템 총서", 1996, 10

[11] 한국정보보호센터, "방화벽 FAQ", 기술문서 CERT-KR-TG-96-002, 1996

" 부록 " 인터넷 서비스들에 대한 방화벽 보안 정책 예

서비스	정책				정책 예
	내부에서 외부로		외부에서 내부로		
	상태	인증	상태	인증	
FTP	Y	N	Y	Y	FTP접근은 내부 네트워크에서 외부로 허락된다. 외부로부터의 접근은 강력한 인증이 요구된다.
Telnet	Y	N	Y	Y	Telnet접근은 내부에서 외부로 허락된다. 외부에서 내부로 접근은 인증이 요구된다.
Rlogin	Y	N	Y	Y	외부로부터 회사 호스트에 rlogin은 NSM 으로부터 서면 허가가 요구되며 강력한 인증이 요구된다.
HTTP	Y	N	N	N	외부 사용자 접근이 예정된 모든 WWW서버는 회사 방화벽 외부의 호스트에 있어야 한다.
SSL	Y	N	Y	Y	SSL 세션은 SSL세션이 회사 방화벽을 통과할 때 고객 서명이 요구된다.
POP3	N	N	Y	N	회사 POP서버는 회사 방화벽 내부에 위치해야 한다. APOP의 사용이 요구된다.
NNTP	Y	N	N	N	NNTP 서버에 대한 외부 접근은 허용되지 않는다.
Real Audio	N	N	N	N	현재 회사 방화벽을 통과해야 하는 오디오 세션 지원 업무 요구는 없다. 그러한 지원을 요구하는 사업장은 NSM과 협의 해야 한다.
lp	Y	N	N	N	lp 서비스는 회사 방화벽에서 제거된다.
finger	Y	N	N	N	finger 서비스는 회사 방화벽에서 제거된다.
gopher	Y	N	N	N	gopher 서비스는 회사 방화벽에서 제거된다.
whois	Y	N	N	N	whois 서비스는 회사 방화벽에서 제거된다.
SQL	Y	N	N	N	외부호스트에서 내부 DB로의 연결은 NSM의 허가가 필요하며 인증된 SQL 프록시 서비스가 요구된다.
rsh	Y	N	N	N	rsh 서비스는 회사 방화벽에서 제거된다.
기타 (NFS 등)	N	N	N	N	언급하지 않은 기타 서비스 접근은 거부한다.