通信情報保護學會誌
第6卷 第2號, 1996. 6

전산망 보호를 위한 방화벽 시스템 고찰

박 응 기*, 손 기 욱*, 정 현 철*

요 약

본 고는 인터네트와 내부(로컬) 네트워크 사이에 위치하여 내부 네트워크의 자원 및 중요한 정보를 해커 및 불법 침입자로부터 보호하기 위해서 사용되는 방화벽(Firewall) 시스템에 대해 분석하였다. 방화벽 시스템은 OSI 참조 모델의 계층 3과 계층 4에서 프로토콜 정보에 따라 패킷 필터링을 수행하는 스크리닝 라우터(Screening Router)와 OSI 참조 모델의 상위 계층에서 트래픽을 허가 및 거절하는 게이트웨이 혹은 proxy로 크게 나눌 수 있다. 이러한 방화벽 시스템들은 인터네트 등의 외부 네트워크와 내부 네트워크 사이에서 네트워크 트래픽을 감시하고, 허가 및 거절하는 역할을 수행한다. 인터네트 등 외부 네트워크에 연결된 내부 네트워크를 보호하기 위해서는 강력한 암호화 기법 및 정보보호 서비스를 내부 네트워크의 시스템에 구현하고, 방화벽 시스템을 사용하면 해커 등과 같은 불법 침입자로부터 내부 네트워크의 자원 및 정보를 보다 효율적으로 보호할 수 있다.

1. 서 론

세계 각국은 자국의 미래 정보통신의 사활이 초고속통신망 구축에 달려 있음을 인식하고 통신망 구축에 박차를 가하고 있다. 국내도 마찬가지로 국가의 정보통신 사활이 이에 있음을 인식하고 정부의 주도 하에 초고속통신망 구축을 진행 중에 있으며, 현재 일부 지역에 초고속통신망 시범 서비스를 실시하고 있다. 또한 앞으로의 각국은 정보통신의 발전이 초고속통신망 구축과 더불어 인터네트로의 발전을 예상하고 있으며, 세계 각국은 인터네트의 접속을 통하여 각종 최신의 정보를 수집하고, 서로 정보를 교환하고 있다[1]. 이러한 통신망으로의 발전에 힘입어 사용자들은 음성 및 비음성 등의 다양한 멀티미디어 정보 획득과 유통에 상당한 편익을 누리는 반면에 이의 역기능인 내부 네트워크의 자원 및 정보에 대한 해커들의 불법 침입 및 위협이 날로 증가하고 있다[1-3]. 인터네트에 연결하여 사용하는 내부 네트워크의 자원 및 중요한 정보 등을 해커로부터 보호하기 위해 방화벽 시스템에 대한 연구가 국내외에서 활발히 진행되고 있으며, 많은 상용 제품들이 시판되고 있다[2]. 따라서 인터네트 등과 같은 외부 네트워크에 연결된 내부 네트워크를 보호하기 위해서는 네트워크를 연결해주는 장치에서 입출력되는 패킷을 분석하여 패킷 트래픽을 제어 및 차단하는 방화벽 시스템[2,4-10]을 사용하면 네트워크를 보다 안전하게 보호할 수 있다.

* 한국전자통신연구소

제 2장에서는 방화벽 시스템에 대한 일반적인 개요 및 방화벽 시스템 구축 시 고려 사항에 대해 설명하고, 제 3장에서는 OSI 참조 모델과 방화벽 시스템과의 관계를 설명하며, 제 4장에서는 방화벽 시스템에서 제공해야 할 정보보호 서비스에 대해 설명하며, 제 5장에서는 방화벽 시스템의 종류, 이들의 기능 및 장단점을 제시하였으며, 제 6장에서는 현재 국내외의 방화벽 시스템에 대한 현황을 인터네트를 통하여 수집한 자료에 대해서 살펴보며, 제 7장에서는 결론을 맺는다.

2. 방화벽 시스템의 개요

가. 방화벽 시스템 구축 시 고려 사항

인터네트 등의 외부 전산망에 연결된 내부 네트워크를 보호하기 위해서 방화벽 시스템을 설계 및 구축하고자 할 경우 고려해야 할 사항은 다음과 같다[2,4-5].

1) 어떤 자원을 보호할 것인가?

보호하고자 하는 하드웨어, 소프트웨어, 각종 중요한 정보, 시스템 사용자, 시스템 관리에 대한 도큐먼트 등을 정의하고, 방화벽 시스템 구축 시 이를 고려하여야 한다.

2) 어떤 위협이 존재하는가?

보호하고자 하는 자원 및 정보들에 대한 위협이 어떤 것들이 있는가를 분석한다.

3) 자원이 얼마나 중요한가?

보호하고자 하는 자원의 중요성이 어느 정도인가를 분석한다.

4) 어떤 사용자를 인가할 것인가?

사용자 계정을 가진 사용자만이 네트워크를 사용하도록 할 것인지 비인가자라도 제한된 자원에만 사용하도록 할 것인지를 결정한다.

5) 요구되는 응용 및 서비스는 무엇인가?

보호하고자 하는 네트워크에서 사용 가능한 응용 및 서비스들이 어떤 것들이 존재하는지를 분석한다.

6) 비용 대 효과 측면에서 보호하기 위해 실현 될 수 있는 기법은 무엇인가?

화일이나 디렉토리 등은 액세스 제어에 의해 보호하고, 네트워크 장비 및 호스트의 보호는 방화벽 시스템 사용 등의 보호 기법을 고려한다.

7) 해커 등의 불법 침입 감지 시 취해야 할 행동은 무엇인가?

해커 등과 같은 불법 침입자가 시스템 내부에 침입했을 때 취해야 할 대응책을 마련해야 한다.

8) 정기적으로 시스템을 점검한다.

보호하고자 하는 네트워크 및 자원들에 변화가 일어났는지 정기적으로 점검하고 기록한다. 이러한 행위는 시스템 관리자 및 네트워크 관리 시스템에 의해 자동적으로 실행한다.

방화벽 시스템을 설계 및 구축할 때 상기와 같은 사항을 고려하여 보다 효과적으로 해커 등과 같은 불법 침입자로부터 내부 네트워크를 보호할 수 있도록 해야 한다. 일반적으로 방화벽 시스템을 설계 및 구축할 때 사용하는 패러다임은 두 가지로 구분되는데 첫째로는, 내부 네트워크로의 진입을 명확하게 허용하지 않는 트래픽은 내부 네트워크로의 진입을 방지하는 것이고, 둘째로는 첫 번째 패러다임의

반대 개념으로 명확하게 내부 네트워크로의 진입이 방지되지 않는 트래픽은 네트워크로의 진입을 모두 허용한다[2,6-7,9].

나. 방화벽 시스템의 방어 범위

방화벽 시스템은 인터네트와 같은 외부 네트워크와 내부 네트워크 사이에 놓이며, 외부 네트워크로부터 내부 네트워크로 혹은 역으로의 트래픽을 감지하여 내부 네트워크의 정보 및 자원들을 보호한다[1,5,9]. 즉, 외부 네트워크에서 내부 네트워크로 액세스하기 위해서는 방화벽 시스템을 통과하여야만 내부 네트워크로 진입할 수 있도록 하여 내부 네트워크에 존재하는 정보 및 자원들에 대한 트래픽을 사전에 방어하고, 내부 네트워크에서 지정된 인터네트로의 트래픽을 제어[1,5]하는 것이다.

그러나 방화벽 시스템은 내부 사용자가 내부 네트워크에 존재하는 중요한 정보를 디스크 혹은 테이프와 같은 매체를 통해 가지고 나가는 것은 방어하지 못한다. 또한 외부 네트워크로부터 내부 네트워크로 비인가된 다이얼 모뎀을 통한 접근을 방어하지 못하며, 바이러스 혹은 정보 지향적인 공격에 대해서는 방어하지 못한다[2,6]. 따라서 방화벽 시스템은 보호하고자 하는 네트워크의 자원이나 정보들을 완벽하게 불법 침입자로부터 보호할 수 없으며, 다만 외부 네트워크에서 내부 네트워크로의 진입을 1차로 방어해주는 기능을 수행한다.

다. 위험 지역의 축소

인터네트 및 외부 네트워크에는 많은 해커가 존재하며, 이들은 언제 어느 통신망에 접속하여 내부 네트워크에 존재하는 자원 및 중요한 정보를 파괴, 변경, 갈취 등을 할지 예측할 수 없다. 따라서 인터네트 등 외부 네트워크에 연결된 모든 내부 네트워크는 해커들이 침입할 수 있는 위험 지역(Zone of Risk)에 놓이게 된다. 이러한 위험 지역으로부터 내부 네트워크를 분리시키고자 하는 것이 방화벽 시스템이다[2,5,8-9].

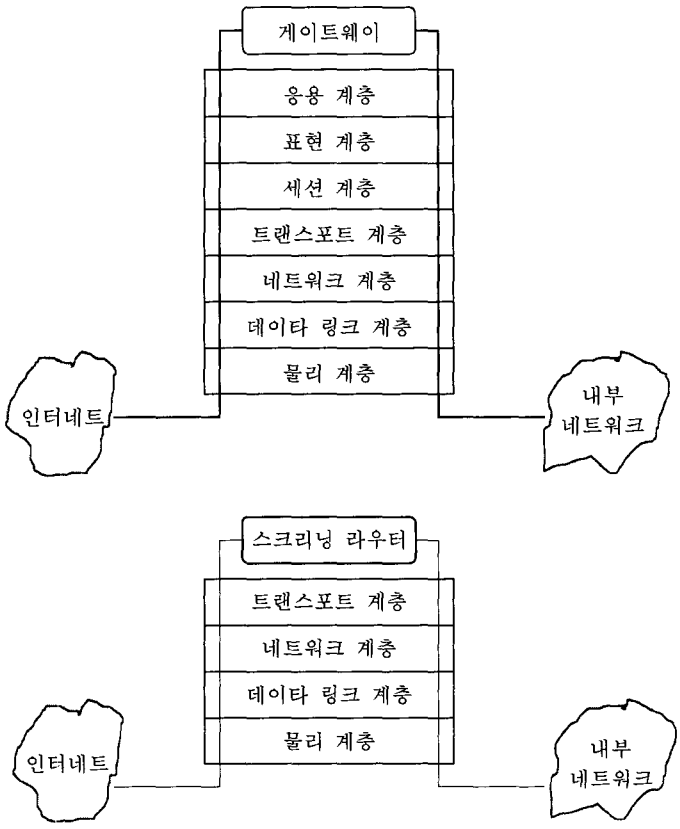
라. 방화벽 시스템의 특성

인터네트와 내부 네트워크 사이에 위치하여 이들 사이의 트래픽을 감시 및 제어하는 방화벽 시스템의 특성은 다음과 같다[2,6].

첫째, 인터네트에서 내부 네트워크로 그리고 내부 네트워크에서 인터네트로의 모든 트래픽은 방화벽 시스템을 거쳐야만 한다. 둘째, 보안 정책에 따라 결정한 인가된 트래픽만이 방화벽 시스템을 안전하게 통과할 수 있다. 세번째, 방화벽 시스템 자체는 불법 사용자에 의한 침투를 허용하지 않는다.

3. 방화벽 시스템과 ISO의 OSI 참조 모델

[그림 1]은 ISO의 OSI 참조 모델과 방화벽 시스템의 관계를 보여주고 있다[2]. 스크리닝 라우터는 ISO의 OSI 참조 모델의 계층 3인 네트워크 계층과 계층 4인 트랜스포트 계층에서 동작하며, 외부 네트워크에서 내부 네트워크로 진입하는 그리고 내부 네트워크에서 외부 네트워크로 나가는 패킷 트래픽을 필터링하는 기능을 수행한다. 게이트웨이 방식의 방화벽 시스템은 ISO의 OSI 참조 모델의 모든 계층에서 동작하며, 내부 네트워크로 진입하고 외부 네트워크로 나가는 패킷 트래픽을 필터링하는 기능과 인증 기능 및 로그 기능 등을 수행한다. 전형적인 게이트웨이 방식의 방화벽 시스템은 ISO의 OSI 참조 모델의 계층 7인 응용 계층에서 응용 서비스에 따라 각각 처리를 수행하는데 많은 상용 제품들도 여기에 해당된다.



[그림 1] 방화벽 시스템과 ISO의 OSI 참조 모델과의 관계

4. 방화벽 시스템의 정보보호 서비스

방화벽 시스템은 인터네트 등과 같은 외부 네트워크와 연결하여 사용하는 내부 네트워크의 자원 및 중요한 정보를 해커 및 불법 침입자로부터 보호하기 위해서 사용되며, 방화벽 시스템의 기능을 지원하기 위해서는 다음과 같은 정보보호 서비스가 필요하다.

가. 사용자 인증

정보를 교환하는 상대방을 확인하고 접근 자격 유무를 확인하는 절차를 말하는데, 패스워드 및 Kerberos와 같은 강력한 인증 프로토콜[3]를 사용하여 내부 네트워크에 접근하는 사용자를 인증한다. 게이트웨이 방식의 방화벽 시스템을 사용할 경우 사용자 인증을 실현하는 것이 중요하다. 방화벽 시스템을 구축하여 내부 네트워크로의 접근을 방지하기 위해서는 강력한 인증 방법을 도입하여야 하는데, 이를 위해 One-Time 패스워드를 사용하는 방법[1,3,11]과 Kerberos 인증 방법[3] 등이 많이 사용된다.

나. 접근제어

외부의 사용자가 내부 네트워크로 혹은 내부 사용자가 내부 네트워크에서 인터네트 등과 같은 외부 네트워크로 통신하기 위해 방화벽 시스템에 접근할 때, 허용된 시스템에서 접근 요청을 하는지 그리고 통신 대상인 목적지

시스템이 원하는 곳인지 검사하고 허용 여부를 결정하며, 네트워크의 특정 자원에 대해서 액세스할 자격이 있는가를 검사한 후 접근 여부를 결정함으로써 불법 침입자에 의한 불법적인 자원 접근 및 파괴를 방지한다[2,3].

다. 트래픽 암호화

외부 사용자가 인터네트를 통해 내부 네트워크로 허용하는 트래픽이나 또는 내부 네트워크의 사용자가 인터네트에 접속하여 사용하고 있는 다른 사용자에게 트래픽을 전송할 경우 인터네트에 존재하는 제 3자에게 트래픽의 노출을 방지하기 위해 전송되는 트래픽을 암호화한다. 트래픽을 암호화하기 위한 암호 알고리즘은 DES, RSA, IDEA 등이 많이 사용된다[2,3].

라. 트래픽 로그

외부 네트워크와 내부 네트워크 사이에 존재하는 모든 트래픽에 대해서 로그 화일에 기록한다[2].

마. 감사 추적 기능

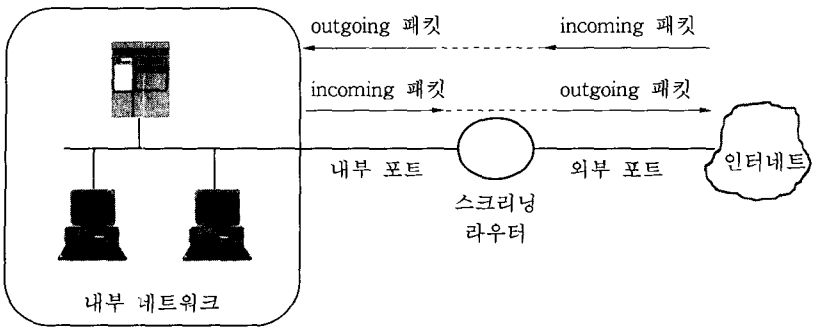
내부 네트워크에 대한 감사 추적 기능[2]을 수행하기 위해 누가, 언제, 어떤 호스트에 접근하여, 어떤 정보를, 어떻게, 얼마동안 접근하였는가에 대한 정보를 기록한다. 이러한 정보는 내부 네트워크에 해커 및 외부의 불법 침입자들이 시스템내의 침입 여부를 파악할 수 있으며, 침입했을 때 대처할 수 있게 한다.

5. 방화벽 시스템의 종류

방화벽 시스템은 ISO의 OSI 참조 모델과 관련하여 방화벽 시스템이 동작하는 프로토콜 계층에 따라 분류[2,6]될 수 있다. 계층 3인 네트워크 계층과 계층 4인 트랜스포트 계층에서 패킷 필터링 기능을 수행하는 스크리닝 라우터와 응용 계층에서 패킷 필터링 기능과 인증 기능 등을 수행하는 응용 계층의 게이트웨이로 분류할 수 있다. 일반적으로 스크리닝 라우터를 구축할 경우 「명확하게 내부 네트워크로의 진입이 방지되지 않은 트래픽은 네트워크로의 진입을 허용하는 패러다임[2,6-7,9]을 사용하고, 게이트웨이 혹은 proxy 서버의 경우 「내부 네트워크로의 진입을 명확하게 허용하지 않은 트래픽은 내부 네트워크로의 진입을 방지」하는 패러다임[2,6-7,9]에 입각하여 설계한다.

가. 스크리닝 라우터[2,6-10]

스크리닝 라우터는 OSI 참조 모델의 계층 3과 계층 4에서 동작되기 때문에 계층 3과 4에서 동작하는 프로토콜인 IP(Internet Protocol), TCP(Transmission Control Protocol) 혹은 UDP(User Datagram Protocol)의 헤더에 포함된 내용을 분석해서 동작한다. 스크리닝 라우터란 네트워크에서 사용하는 통신 프로토콜의 형태, 근원지 주소와 목적지 주소, 통신 프로토콜의 제어 필드 그리고 통신 시 사용하는 포트 번호를 분석해서 내부 네트워크에서 외부 네트워크로 나가는 패킷 트래픽을 허가 및 거절하거나 혹은 외부 네트워크에서 내부 네트워크로 진입하는 패킷 트래픽의 진입 허가 및 거절을 행하는 라우터를 말한다. 이러한 진입 허가 혹은 거절하는 결정은 패킷 필터 규칙에 따른 라우팅 테이블에 의해 결정된다. 이렇게 일반 패킷과 특수한 프로토콜에 입각한 포트로 전송되는 패킷을 구별하는 라우터의 능력 때문에 패킷 필터 라우터라고도 한다. [그림 2]는 스크리닝 라우터(패킷 필터 라우터)의 위치 및 기능을 보여준다[2].



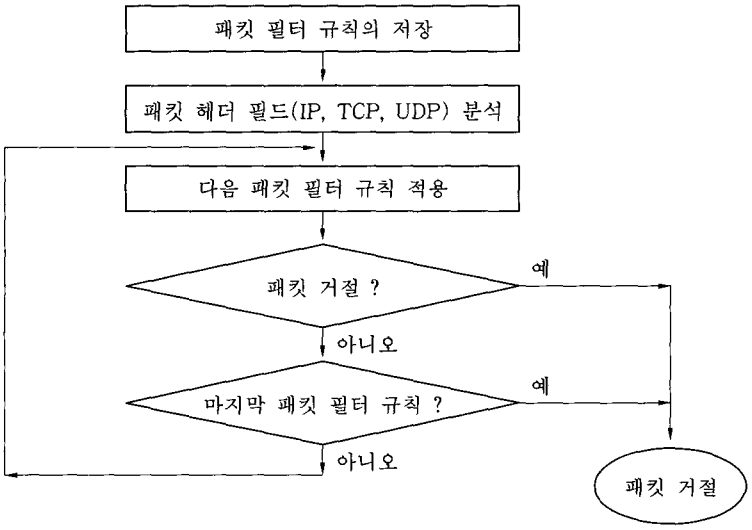
[그림 2] 스크리닝 라우터의 위치

1) 패킷 필터의 동작

[그림 3]은 스크리닝 라우터가 동작하는 흐름도를 도시하고 있다[2]. 스크리닝 라우터로 연결에 대한 요청이 입력되면 IP, TCP 혹은 UDP의 패킷 헤더를 분석하여 근원지/목적지의 주소와 포트 번호, 제어 필드의 내용을 분석하고, 이들을 패킷 필터 규칙에 적용하여 계속 진입시킬 것인지 아니면 거절할 것인지를 판별한다. 연결 요청 패킷의 진입이 허가되면 이후의 모든 패킷은 연결 단절이 발생할 때까지 모두 허용된다.

2) 패킷 필터 규칙

패킷 필터 규칙은 〈표 1〉과 같이 근원지 주소, 근원지의 포트 번호, 목적지 주소, 목적지의 포트 주소, 프로토콜 플래그, 행위(허가/거절) 등으로 구성된다[2,6,10]. 이러한 패킷 필터 규칙이 정해지면 인터네트 주소에 적용하는 허가/거절하는 조건의 순차적인 액세스 집합인 액세스 리스트를 정의한다. 스크리닝 라우터는 이러한 액세스 리스트를 가지고 프로그램 되며, 패킷을 허가 혹은 거절할 것인지를 액세스 리스트에 있는 행위에 대해서 순차적으로 결정하며,



[그림 3] 패킷 필터의 흐름도

패킷에 해당하는 액세스 리스트가 나타날 때까지 혹은 마지막 액세스 리스트에 도달할 때까지 순차적으로 점검한다. 방화벽 시스템을 실현할 경우 액세스 리스트의 점검 순서는 매우 중요하기 때문에 액세스 리스트의 점검 순서를 신중히 검토하여 사용한다.

◆ 장 점

- 필터링 속도가 빠르고, 비용이 적게든다.
- 네트워크 계층에서 동작하기 때문에 클라이언트와 서버에 변화가 없어도 된다.
- 사용자에 대해 투명성을 유지한다.
- 하나의 스크리닝 라우터로 보호하고자 하는 네트워크 전체를 동일하게 보호할 수 있다.

◆ 단 점

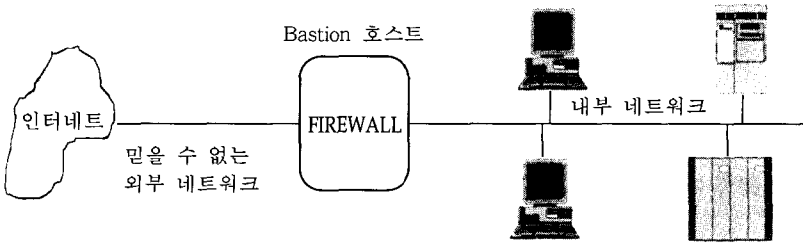
- 네트워크 계층과 트랜스포트 계층에 입각한 트래픽만을 방어할 수 있다.
- 패킷 필터링 규칙을 구성하여 검증하기 어렵다.
- 패킷내의 데이터에 대한 공격을 차단하지 못한다.
- 스크리닝 라우터를 통과 혹은 거절당한 패킷에 대한 기록(log)을 관리하기 힘들다.

나. Bastion 호스트[2,9]

Bastion 호스트는 통신망을 보호하는데 중요한 방화벽 시스템으로 사용되며, 네트워크 관리자가 정기적으로 주의 깊게 감시 및 점검하여야 한다. Bastion 호스트로는 상용 제품인 SPARCstation, IBM/AIX 등이 사용될 수 있으며, 이들은 방어 기능이 철저히 구현된 호스트이다. 이러한 Bastion 호스트는 인터네트 등의 외부 네트워크와 내부 네트워크를 연결해 주는 방화벽 시스템 역할을 한다. 인터네트의 사용자가 내부 네트워크로의 액세스를 원할 경우 우선 Bastion 호스트를 통과하여야만 내부 네트워크를 액세스하여 자원 및 정보를 사용할 수 있다. 해커 및 불법 침입자가 Bastion

〈표 1〉 패킷 필터 규칙

규칙번호	행위	근원지 주소	근원지 포트	목적지 주소	목적지 포트	프로토콜 플래그	설명
1	허가	129.254.128.0	1024	129.254.128.1	25	TCP	
2	거절	129.254.0.0	0	129.254.128.1	25	TCP	
..							



[그림 4] Bastion 호스트

호스트에 있는 중요한 정보를 악용하여 내부 네트워크로의 접근하는 것을 방지하기 위해서는 Bastion 호스트 내에 존재하는 모든 사용자 계정을 지워야 하며, 중요하지 않은 화일이나 명령 및 유티리티, IP forwarding 화일 그리고 라우팅 정보 등을 삭제하여야 한다. Bastion 호스트로의 입력 시 강력한 인증 기법을 구현하여야 하며, Bastion 호스트는 내부 네트워크로의 접근에 대한 기록(log), 감사 추적을 위한 기록 및 모니터링 기능을 가지고 있어야 한다. [그림 4]는 방화벽 시스템으로 동작하는 Bastion 호스트를 이용하여 외부 네트워크의 불법 사용자들로부터 내부 네트워크로의 접근을 방지하는 구성도를 나타낸 것이다.

◆ 장 점

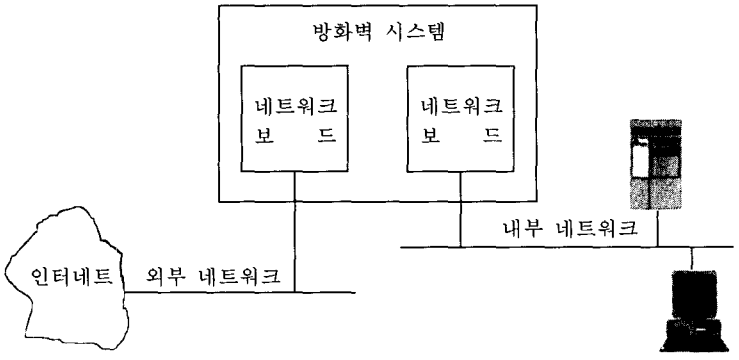
- 응용 서비스 종류에 보다 종속적이기 때문에 스크리닝 라우터보다 안전하다.
- 정보 지향적인 공격을 방어할 수 있다.
- 각종 기록(logging) 정보를 생성 및 관리하기 쉽다.

◆ 단 점

- Bastion 호스트가 손상되면 내부 네트워크를 보호할 수 없다.
- 로그인 정보가 누출되면 내부 네트워크를 보호할 수 없다.

다. Dual-Homed 게이트웨이[2,6,9]

Dual-Homed 게이트웨이는 [그림 5]와 같이 두개의 네트워크 인터페이스를 가진 Bastion 호스트를 말하며, 하나의 네트워크 인터페이스는 인터네트 등 외부 네트워크에 연결되며, 다른 하나의 네트워크 인터페이스는 보호하고자 하는 내부 네트워크에 연결되며, 양 네트워크간의 라우팅은 존재하지 않는다. 따라서 양 네트워크간의 직접적인 접근은 허용되지 않는다. 만약 라우팅이 가능하면 외부 네트워크로부터 내부 네트워크로의 액세스가 가능하다. 라우팅이 없는 Dual-Homed 게이트웨이를 이용하여 인터네트 혹은 내부 네트워크의 정당한 사용자들이 응용 서비스를 제공받는 방법은 두 가지로 구분되는데 첫째 방법은, Dual-Homed 게이트웨이 상에서 실행되며 서비스를 제공하는 proxy 서버를 사용하는 것이고, 두 번째 방법은 응용 서비스를 제공해주는 Dual-Homed 게이트웨이에 직접 로그인 한 다음 다시 내부 네트워크로 접근하는 것인데, 이 경우 강력한 인증 방법이 게이트웨이에 구현되어야 한다. 따라서 해커나 불법 침입자가 악용할 소지가 있



[그림 5] Dual-Homed 게이트웨이

는 명령어(suid, sgid 등), 유티리티 및 불필요한 서비스, 프로그래밍 도구(컴파일러 등)를 이들이 사용할 수 없도록 Dual-Homed 게이트웨이에서 삭제하여야 하며, 라우팅이 되지 않도록 하여야 한다. 또한 로그인에 대한 기록 정보 및 감사 추적에 필요한 기록을 정확히 유지 관리하여야 한다. 외부 네트워크로부터 내부 네트워크로 진입하기 위해서는 Dual-Homed 게이트웨이를 통과하여야 한다.

◆ 장 점

- 응용 서비스 종류에 좀더 종속적이기 때문에 스크리닝 라우터보다 안전하다.
- 정보 지향적인 공격을 방어할 수 있다.
- 각종 기록(logging) 정보를 생성 및 관리하기 쉽다.
- 설치 및 유지보수가 쉽다.

◆ 단 점

- 제공되는 서비스가 증가할수록 proxy 소프트웨어 가격이 상승한다.
- 게이트웨이가 손상되면 내부 네트워크를 보호할 수 없다.
- 로그인 정보가 누출되면 내부 네트워크를 보호할 수 없다.

라. 스크린 된(Screened) 호스트 게이트웨이[2,6,9]

스크린 된 호스트 게이트웨이는 Dual-Homed 게이트웨이와 스크리닝 라우터를 혼합하여 사용한 방화벽 시스템이다. 방화벽 시스템의 구성 방법은 [그림 6]과 같이 인터네트와 Bastion 호스트 사이에 스크리닝 라우터를 접속하고, 스크리닝 라우터와 내부 네트워크 사이에서 내부 네트워크 상에 Bastion 호스트를 접속한다. 인터네트와 같은 외부 네트워크로부터 내부 네트워크로 들어오는 패킷 트래픽을 스크리닝 라우터에서 패킷 필터 규칙에 의해 1차로 방어하고, 스크리닝 라우터를 통과한 트래픽은 모두 proxy 서버를 구동하는 Bastion 호스트에서 입력되는 트래픽을 점검하며, 스크리닝 라우터 혹은 Bastion 호스트를 통과하지 못한 모든 패킷 트래픽은 거절된다. 내부 네트워크로부터 인터네트 등으로 나가는 트래픽은 1차로 proxy 서버를 구동하는 Bastion 호스트에서 점검한 후 통과된 트래픽을 스크리닝 라우터로 보내고 스크리닝 라우터는 Bastion 호스트로부터 받은 트래픽을 인터네트 등의 외부 네트워크로 송신을 할 것인지 결정한다. Bastion 호스트와 스크리닝 라우터를 통과한 트래픽만이 외부 네트워크로 전달된다. Bastion 호스트는 외부 네트워크로 또는 외부 네트워크로부터의 서비스 요청을 허용할 것인지 아니면 거절할 것인지를 결정하기 위해서 응용 계층의 proxy 서버를 구동한다. 스크리닝 라우터의 라우팅 테이블은 외부 트래픽이 Bastion 호스트로 입력되도록 구성되어야만 하며, 이 스크리닝 라우터의 라우팅 테이블은 침입자로부터 안전하게 보호되어야 하고 비인가된 변환을 허용해서는 안된다. 만약 라우팅 테이블이 변환되어 외부 트래픽이 Bastion 호스트로 입력이 되지 않고 곧바로 내부 네트워크로 진입할 수 있다면 해커 및 불법 침입자는 내부 네트워크의 자원 및 정보를 변환, 파괴 등을 할 수 있다. 이와 같은 방화벽 시스템의 스크리닝 라우터에서는 정적 라우팅 테이블을 사용하는 것이 안전하다.

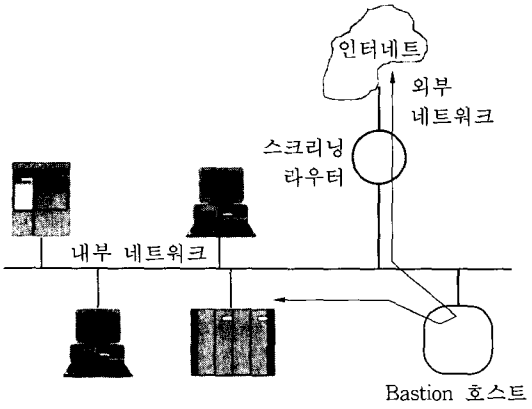
◆ 장 점

- 2단계로 방어하기 때문에 매우 안전하다.
- 네트워크 계층과 응용 계층에서 방어하기 때문에 공격이 어렵다.
- 가장 많이 이용되는 방화벽 시스템이며, 융통성이 좋다.

- Dual-Homed 게이트웨이의 장점을 그대로 가진다.

◆ 단 점

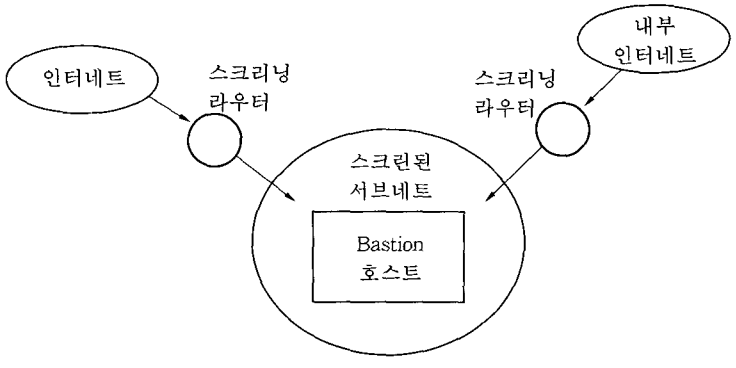
- 해커에 의해 스크리닝 라우터의 라우팅 테이블이 변경되면 이들을 방어할 수 없다.
- 방화벽 시스템 구축 비용이 많이 든다.
- 서비스 속도가 느리다.



[그림 6] 스크린 된 호스트 게이트웨이

마. 스크린 된 서브네트 게이트웨이[2,6,9]

인터네트와 내부 네트워크를 스크린 된 게이트웨이를 통해서 연결하며, 일반적으로 스크린 된 서브네트는 방화벽 시스템이 설치되어 있으며, 인터네트와 스크린 된 서브네트 사이 그리고 서브네트사이와 내부 네트워크 사이에는 스크리닝 라우터를 사용한다. 이와 같은 방화벽 시스템의 구성도는 [그림 7]과 같다. 스크리닝 라우터는 인터네트와 스크린 된 서브네트 그리고 내부 네트워크와 스크린 된 서브네트 사이에 각각 놓이며 입출력되는 패킷 트래픽을 패킷 필터 규칙을 이용하여 트래픽을 필터링 기능을 수행하며, 스크린 된 서브네트에 설치된 Bastion 호스트는 proxy 서버(응용 게이트웨이)를 이용하여 명확히 진입이 허용되지 않은 모든 트래픽은 거절하는 기능을 수행한다. 이러한 구성에서 스크린 된 서브네트에 대한 액세스는 Bastion 호스트를 통해서만 가능하기 때문에 침입자가 스크린 된 서브네트를 통과하는 것은 어렵다. 만약 인터네트를 통해 내부 네트워크로 침입하려고 한다면 침입자는 자기가 자유롭게 내부 네트워크를 액세스할 수 있도록 인터네트, 스크린 된 서브네트 그리고 내부 네트워크의 라우팅 테이블을 재구성해야만 가능하다. 그러나 스크리닝 라우터가 존재하기 때문에 이는 힘들다. 비록 Bastion 호스트가 침해되었더라도 침입자는 내부 네트워크 상에 존재하는 호스트로 침입해야 하고 그리고 스크린 된 서브네트를 액세스하기 위해서 스크리닝 라우터를 통과해야 한다.



[그림 7] 스크린 된 서브네트

◆ 장 점

- 스크린 된 호스트 게이트웨이 방화벽 시 스템의 장점을 그대로 가진다.
- 융통성이 뛰어나다.
- 해커들이 내부 인터네트를 공격하기 위해서는 방화벽을 통과할 것이 많아 침입이 어렵다.
- 매우 안전하다.

◆ 단 점

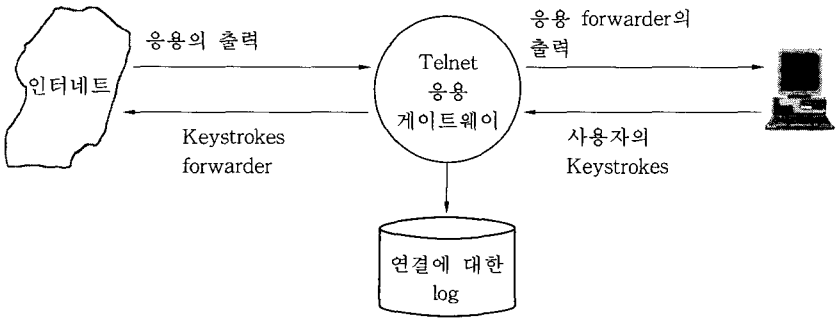
- 다른 방화벽 시스템들 보다 설치하기 어렵고, 관리하기 어렵다.
- 방화벽 시스템 구축 비용이 많다.
- 서비스 속도가 느리다.

바. Proxy 서버 / 응용 게이트웨이[2,4-7,9]

응용 게이트웨이 혹은 proxy 서버는 방화벽 시스템(일반적으로 Bastion 호스트)에서 구동되는 응용 소프트웨어를 말하는데 store-and-forward 트래픽 뿐만 아니라 대화형의 트래픽을 처리할 수 있으며, 사용자 응용 계층(OSI 참조 모델의 계층 7)에서 트래픽을 분석할 수 있도록 프로그램 된다. 따라서 이것은 사용자 단계와 응용 프로토콜 단계에서 액세스 제어를 제공할 수 있고, 응용 프로그램의 사용에 대한 기록(log)을 유지하고 감사 추적을 위해서도 사용될 수 있다. 응용 게이트웨이는 사용자 단계에서 들어오고 나가는 모든 트래픽에 대한 기록을 관리하고 제어할 수 있으며, 해커 및 불법 침입자를 방어하기 위해서 강력한 인증 기법이 필요하다. 응용 게이트웨이는 사용되는 응용 서비스에 따라 각각 다른 소프트웨어를 구현하여 사용하기 때문에 고수준의 보안을 제공할 수 있다. 네트워크에 첨가되고 보호가 필요한 새로운 응용이 생기면 이를 위해 새로운 특수 목적용 코드를 생성해야 한다. 응용 레벨 게이트웨이를 사용하기 위해서 사용자는 응용 게이트웨이 장치에 로그인 하거나 서비스를 이용할 수 있는 특수한 클라이언트 응용 서비스를 실현해야 한다. 각각 응용에 따라 다르게 사용하는 특수한 게이트웨이는 제각기 내부에 관리 도구와 명령 언어를 가지고 있다. 응용 게이트웨이는 실제 서버의 관점에서 볼 때 클라이언트처럼 동작하며, 클라이언트 관점에서 볼 때는 실제 서버처럼 동작한다. 응용 게이트웨이의 실현예는 TELENT 게이트웨이, FTP 게이트웨이, Sendmail, NNTP News Forwarder 등이 있다.

◆ 장 점

- 응용 서비스마다 각각 다른 응용 게이트웨이를 구현하므로 보다 안전하게 보호할 수 있다.



[그림 8] TELNET 게이트웨이

- 응용 사용에 따른 기록(log) 및 감사 추적을 유지 관리 가능하다.
- 융통성이 좋다.
- 정보보호 서비스를 응용 게이트웨이에 구현 가능하다.

◆ 단 점

- 응용 서비스마다 제각각 다른 응용 게이트웨이가 필요하다.
- 사용되는 응용 서비스가 증가할수록 구축 비용이 증가한다.

6. 방화벽 시스템의 현황

인터네트에 연결하여 사용하는 내부 네트워크의 자원 및 중요한 정보 등을 해커로부터 보호하기 위해 사용되는 방화벽 시스템에 대한 연구가 국내외에서 활발히 진행되고 있으며, 많은 상용 제품들이 시판되고 있다. 본 장에서는 국내외에서 시판 및 개발된 제품들에 대해 소개하고자 한다.

가. 국내 현황

인터네트 등 외부 네트워크에 연결하여 사용하고 있는 내부 네트워크를 해커 및 불법 침입자들로부터 보호하기 위해 방화벽 시스템에 대한 연구가 활발히 진행되고 있다. 국내에서는 아직 자체 개발하는 업체는 소수이며, 대부분 외국 업체의 방화벽 시스템을 수입 판매하고 있는 실정이며, 현재까지 방화벽 시스템을 도입 구축한 업체는 많지 않으나 금년 하반기부터는 본격적으로 시장 도입기에 들어갈 전망이다. 본 절에서는 국내 업체들의 방화벽 시스템에 대한 동향을 소개하고자 한다.

1) 대정정보통신

국내 업체로는 최초로 방화벽 시스템을 개발해 경찰청, 대구 상공회의소, 대우조선에 공급하였다. 대정정보통신이 개발한 방화벽 시스템은 네트워크를 통한 해커 침입 시 방화벽 시스템의 구조를 변경할 수 있고, 소스 레벨의 수정을 통해 즉각 대처할 수 있을 뿐 아니라 최단 시간 내에 시스템을 원상 복구, 피해를 최소화하는 게 특징이다.

2) 두산정보통신

캐나다의 BNT사의 방화벽 시스템인 '보더웨어'의 국내 공급 계약을 체결하고 시판에 나섰다. 보더웨어는 해커 등 외부의 침입으로부터 내부 인터네트의 시스템 및 중요한 정보를 보호하는 외부 방화벽 시스템과 사내 사용자들의 자료 유출을 제어하는 내부 방화벽 시스템으로 구성되어 있다.

3) 삼성전자

캐나다의 밀키웨이사의 '블랙홀' 제품을 들여와 국내 실정에 맞는 제품으로 개발하고 삼성 그룹 전체를 보호하는 방화벽 시스템을 구축하고 있으며, 사내의 구축이 완료되면 외부 용역에 나설 계획이다.

4) 싸이버텍홀딩스

이스라엘의 체크포인트사의 '파이어월 1' 제품을 국내 공급 계약을 체결하고 삼보 컴퓨터 등 5개 업체에 공급하였다.

5) 한국컴퓨터

NSC사의 상용 라우터에 방화벽 시스템인 '엣센트리'를 탑재하여 공급하고 있다. ERS, SR, BAR 등 라우터에 '엣센트리'를 탑재해 체공함으로써 별도의 방화벽 시스템 호스트없이 라우터 기반의 패킷 필터링 방식을 채택하고 있다.

6) 한일정보통신

미국 네트워크 전문회사인 TIS사의 '건틀릿' 방화벽 시스템을 국내 공급 계약을 체결하고 국내 공급에 나섰다.

이들 업체이외도 국내 대기업인 현대, LG 등도 그룹 전체에 방화벽 시스템을 구축하고 이를 바탕으로 판매에 나설 계획이다. 또한 국내의 외국 업체 등에서도 본사에서 개발한 방화벽 시스템을 국내에 공급할 계획을 세워 놓고 있다.

나. 국외 현황

인터네트에 내부 네트워크를 연결하여 안전하게 사용할 수 있도록 하기 위해 많은 통신 전문 업체 및 소프트웨어 회사들이 방화벽 시스템에 대한 연구를 진행하고 있으며, 이들 회사들은 상용 제품을 개발해 세계 각국으로 수출하고 있다. 본 절에서는 외국 회사들의 대표적인 상용 제품들을 소개한다.

1) LanOptics Ltd.(영국)

가) 제품명 : Guardian Firewall

나) 특징

- Guardian 관리자와 대리자(Agent)를 통해 인터네트 연결에 대한 보호를 제공
- 보호 기능으로는, 네트워크 관리자가 근원지 및 목적지 주소, 날짜, 시간, 트래픽 로드 등을 포함하는 규칙을 정의하여, Guardian의 필터링 시스템을 제어한다.
- 관리 기능으로 Guardian은 네트워크 관리자가 네트워크 접근에 대한 제한, 특정 시간대에 접근하는 것에 대한 제한, 특정 서비스에 대한 제한을 할 수 있는 기능을 제공한다.
- Guardian Firewall은 대리자 플랫폼으로써 OS/2를 지원하고(WINDOWS NT도 지원 예정), 관리 플랫폼으로써 WINDOWS-3.xx/95/NT를 지원한다.
- 하드웨어 요구 조건 : Intel 486/66에서 586/133, 16 Mbytes memory, 2 LAN adapters, 500 Mbytes Hard Disk를 필요로 한다.

2) SunSoft (미국)

가) 제품명 : Soltice FireWall-1

나) 특징

- 플랫폼 : SPARCS and Intel
- 운영체제 : Solaris 2.3 이상, SunOS 4.1.3 이상
- 윈도우 시스템 : X11R5/OPEN LOOK
- 디스크 용량 : 15 MB
- 메모리 : 24 MB
- 네트워크 인터페이스 : Standard Solaris Network Interface
- 라우터 관리 : Cisco IOS ver. 9.x 또는 10.x, Bay Network/Wellfleet ver. 8
- 암호화 기능과 인증 기능을 제공
- 네트워크와 사용자 레벨의 보호 기능 제공
- 통합된 네트워크 보호

3) Harris Computer System(미국)

가) 제품명 : CyberGuard Firewall

나) 특징

- 해커 및 불법 침입자로부터 내부 네트워크를 보호
- NCSC의 B1 레벨 운영체제 제공
- 요구된 서비스에 대한 패킷 필터링 기능 수행
- HTTP, FTP, rlogin, telent, SOCKS, SNMP 등에 대한 응용 Proxy 제공
- 가상의 Private 네트워크를 제공

- 강력한 인증 기법 제공
- 네트워크 액세스와 트래픽에 대한 감사 기능
- Mandatory Access Control(MAC) 제공
- GUI 제공

4) Mazama Software Labs(미국)

가) 제품명 : Mazama Packet Filtering MPF

나) 특징
- 비인가된 모든 서비스를 차단
- ICMP Redirect 패킷의 차단
- rlogin, X window, openwindow등과 같은 위험 요소를 갖는 서비스의 차단
- 모든 TCP 연결의 방향성 점검 기능
- 보호 취약 지점 점검을 위한 자체 시험 기능
- 사용하는 포트 인식 기능

5) SOS Corporation(미국)

가) 제품명 : Brimstone

나) 특징
- Multiple Mutually secured Interface
- 클라이언트/서버로 동작
- 사용자 단위의 접근 제어 지원 : 날짜, 주, 근원지 및 목적지 주소, 근원지 및 목적지 포트 등
- 다양한 프로토콜 지원 : Telent, ftp, SMPT, X11
- 비인가된 변경에 대한 자동적인 검사 기능
- SunOS 4.1.3, BSD 1.1, IRIX 5.3에서 구동

6) Cohesive System(미국)

가) 제품명 : CENTRI

나) 특징
- 내부 네트워크를 인터네트에 안전하게 연결할 수 있도록 보장
- 응용 레벨의 proxy 서비스
- IP 주소 변환 기능 제공
- 안전한 메일 서비스 기능 제공
- 사용자 인증 서비스 제공
- 단 대 단 암호화 기능 제공

7) Trusted Information Systems(미국)

가) 제품명 : Gauntlet Internet Firewall

나) 특징
- 선택적인 암호화 기능 제공
- GUI를 통한 방화벽 시스템 관리
- 응용 레벨 게이트웨이로 안전한 WWW 및 FTP 서버를 제공
- POP3과 프린터 Proxy를 통한 원격지 사용자의 기능 향상
- SSL과 SHTTP Proxy를 통한 private WWW 트래픽 가능

8) Global Technology Associates Inc.(미국)

가) 제품명 : GFX family (GFX-E, GFX-S, GFX-R)

나) 특징
- 두 개의 ethernet 인터페이스를 제공 (AUI, BNC)
- 하나의 ethernet 인터페이스로 56K-T-1 DSS, X.25, Frame Relay를 제공
- TCP/IP를 통해 외부 네트워크에 대한 투 명한 접근을 제공함으로써 TCP/IP를 사용하는 응용은 모두 수용
- One Time 패스워드를 사용
- 주소 변환 기능을 제공
- 패킷 필터링 기능을 통해 비인가된 포트에 대한 접근 제한
- SATAN을 통한 보호 기능의 안전성 검증

9) Raptor Systems Inc.(미국)

가) 제품명 : Eagle V3.0 Firewall

나) 특징

- 사용자 인증을 통해 불법 사용자의 접근 제한
- 응용 레벨의 방화벽 시스템이며 GUI 환경 제공
- EagleConnect Encryption을 통해 암호화된 비밀 통신을 제공하고, 두 개의 호스트 사이에 안전한 네트워크 통로를 제공
- Sun의 SunOS 4.1.x, HP의 HP-UX ver. 9.x, IBM AIX ver. 3.2에서 구동

이들 업체 이외도 많은 회사의 상용 제품이 시판되고 있으며, 해커들의 수법도 날로 지능화되고 고도화됨에 따라 이들로부터 내부 네트워크를 보다 안전하게 사용할 수 있도록 방화벽 시스템의 기능을 고도로 향상시키고 있다.

7. 결 론

본 고에서는 인터네트와 내부 네트워크 사이에 위치하여 내부 네트워크의 자원 및 중요한 정보 등을 해커로부터 보호하기 위해 사용되는 방화벽 시스템의 종류를 살펴보고 이들의 기능 및 성능을 분석하였으며 각각의 장단점을 제시하였다. 또한 방화벽 시스템의 기능을 향상시키기 위해 필요한 정보보호 서비스를 설명하였다. 주어진 환경에 가장 적합한 방화벽 시스템을 구축하는 것은 많은 고려사항으로 인하여 쉬운 일은 아니다. 이를 선택하기 위해서는 구축 비용 대 효과, 사용하는 네트워크 기술, 보호해야 할 정보, 보안 정책, 조직의 네트워크에 대한 정책 등을 신중히 고려하여 자신의 네트워크에 가장 적합한 방화벽 시스템을 선택하여야 한다. 그러나 방화벽 시스템이 해커 및 불법 침입자로부터 내부 네트워크의 모든 자원 및 정보를 보호해준다고 믿어서는 안되며, 단지 방화벽 시스템은 내부 네트워크를 보호하기 위한 1차 방어선으로 생각하고 암호화 기법 및 강력한 인증 서비스 등과 같은 안전한 정보보호 서비스를 구현하여야 하며, 이와 더불어 사용자 및 관리자들에게 보안 교육 등을 꾸준히 실시해야 하고, 관리자는 내부 네트워크 시스템을 정기적으로 점검하여야 한다.

참 고 문 헌

[1] J. Ellis, B. Fraser and L. Pesante, Keeping Internet Intruders Away, Unix Review, pp35-44, September 1994

[2] K. Siyan and C. Hare, Internet Firewalls and Network Security, Indianapolis, IN:New Riders Publishing, 1995.

[3] W. Stalling, Network and Internetwork Security : Principles and Practice, Englewood Cliffs, NJ:Prentice-Hall, 1995.

[4] G. W. Treese and A. Wolman, X Through the Firewall and Other Application Relays, proceedings of USENIX Summer Conference, 1993.

[5] R. Braden, D. Clark, S. Crocker and C. Huitema, Report of IAB Workshop on Security in the Internet Architecture-February 8-10, 1994. RFC 1636, June 1994.

[6] D. LaBar, Packet Filtering in Internet Firewalls, Available at http::/www.willamette.edu/~dlabar/firewall.html.

[7] F Avolio and J. Sebes, Application Gateways and Filtering Gateway : A Comparison of Firewall Designs, Data Security Letter #59 Trusted Information Systems, 1995.

[8] Marcus J. Ranum, A Network Firewall, Proceedings of the World Conference on System Administration and Security, July 1992.

[9] Marcus J. Ranum, Thinking About Firewalls, Proceedings of Second International Conference on Systems and Network Security and Management (SANS-II), April 1993.

[10] D. Brent Chapman, Network (In) Security Through IP Packet Filtering, Proceedings of the Third USENIX UNIX Security Symposium, September 1992.

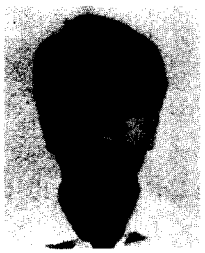
[11] N. M. Haller, The S/Key One-Time Password System, Proceedings of the Internet Society Symposium on Network and Distributed System Security, Feburary 1994.

□ 著者紹介

박 응 기

1986년 중앙대학교 컴퓨터공학과(학사)
1988년 중앙대학교 대학원 컴퓨터공학과(석사)
1988년 ~ 현재 한국전자통신연구소 선임연구원

※ 주관심 분야 : 컴퓨터 보안, 통신망 보안



손 기 욱

1990년 성균관대학교 정보공학과(공학사)
1992년 성균관대학교 대학원 정보공학과(공학석사)
1992년 ~ 현재 한국전자통신연구소 연구원

※ 주관심 분야 : 데이타 통신, 통신망 정보보호

정 현 철

1989년 계명대학교 전산학과(공학사)
1991년 경북대학교 대학원 컴퓨터공학과(공학석사)
1991년 ~ 현재 한국전자통신연구소 연구원

※ 주관심 분야 : 계산이론, 통신망 보안