National Institute of
Standards and Technology
U.S. Department of Commerce

Special Publication 800-41
Revision 1 (Draft)

방화벽 구축 가이드라인

Guidelines on Firewalls and Firewall Policy (Draft)

Karen Scarfone

Paul Hoffman

NCHOVY 인터넷 스톰 센터 (http://nchovy.kr)

euan@nchovy.kr | 구형도 번역

xeraph@nchovy.kr | 양봉열 감수

8con@nchovy.kr | 구동언 감수

2008년 11월 17일 배포 버전

목차

핵심 요약

방화벽이란 서로 다른 보안 태세를 취하는 네트워크나 호스트 간의 네트워크 트래픽을 통제하는 프로그램이나 장비를 말한다.

초창기 대부분의 방화벽은 네트워크 경계에 배치되어 있었다. 이러한 방식은 내부 호스트를 보호하는 데에는 어느 정도 효과를 거둘 수 있었지만, 모든 유형의 공격을 탐지하는 것은 불가능했고, 내부 호스트 간에 이루어지는 공격은 종종 네트워크 방화벽을 우회하곤 했다. 이러한 이유들 때문에, 네트워크 설계자들은 네트워크 경계 및 기타 지역에도 방화벽 기능을 포함하여 보안을 한층 더 견고하게 하고, 나아가 외부 네트워크에 직접 배치되는 모바일 디바이스를 보호하려고 하고 있다. 또한, 네트워크의 위협은 네트워크 트래픽의 하위 계층에서 애플리케이션 계층으로 점진적으로 이동하였고, 이로 인해 하위 단 보호에 집중하는 방화벽의 효과는 줄어드는 결과를 가져왔다.

방화벽의 종류는 몇 가지가 있는데, 각각의 방화벽은 네트워크 트래픽 분석 능력이나 기존 정책과 트래픽 특성을 비교하여 특정한 예를 차단/허용하는 능력에 차이가 있다. 방화벽 종류별 기능 차이를 이해하고, 조직의 요구에 맞는 방화벽 정책을 설계하고 적절하고 효과적인 방화벽 기술을 적용하는 것은 네트워크 트래픽 보호에 있어 매우 중요한 전제 조건이다. 이 문서는 유형별로 방화벽 기술의 개요를 소개하고 각 기술의 보안 능력과 장/단점을 자세하게 다룬다. 또한 이 문서는 네트워크 안 어느 곳에 방화벽이 설치될 수 있는지, 특정 위치에 방화벽을

배치하는 것이 어떤 의미가 있는지 설명한다. 또, 이 문서는 방화벽 정책 수립 과정 및 방화벽 솔루션을 선정하고, 설정하고, 시험하고, 배치하고, 관리하는데 필요한 추천을 포함한다.

방화벽의 효과 및 보안을 증진시키려면 다음 추천 사항들을 실행해야 한다:

방화벽이 네트워크 트래픽을 어떻게 처리해야 하는지 명시한 방화벽 정책을 수립하라.

방화벽 정책은 조직의 정보 보안 정책을 기반으로 방화벽이 특정한 IP 주소 및 IP 주소 범위, 프로토콜, 애플리케이션, 컨텐츠 타입을 가진 네트워크 트래픽을 어 떻게 다루어야 하는지 정의한다. 조직은 위험 분석을 통해 조직 내에서 필요로 하는 트래픽 목록과 이런 트래픽들의 보안 유지 방안을 정리해야 한다. 이 위험 분석에는 어떤 형식의 트래픽이 어떤 조건 하에 방화벽을 통과할 수 있는가에 대한 정의가 포함된다. 정책 요구 사항의 예에는 필요한 IP 프로토콜만을 통과하도록 허가하는 것, 적절한 출발지와 목적지 IP 만 사용될 것, 특정한 TCP 와 UDP 포트가 접근 허용될 것, 특정한 ICMP 형식과 코드가 사용될 것 등이 있다. 일반적으로 방화벽 정책에 명확하게 언급되지 않은 모든 인바운드/아웃바운드 트래픽은 조직에서 필요로 하지 않는 트래픽이므로 허용되지 말아야 한다. 이러한 조치는 공격의 위험을 감소시키고, 네트워크에 걸리는 트래픽 부하 역시 감소시킬 수 있다.

어떤 방화벽을 사용할지 결정할 경우, 고려해야 하는 모든 요구 사항을 명시하라.

어떤 조직이 방화벽을 선정하고 계획하는 과정에는 수많은 고려 사항들이 존재한다. 조직은 어떤 네트워크 영역을 보호해야 하는지, 그리고 어떤 종류의 방화벽 기술이 조직에서 필요로 하는 보안을 위하여 가장 효과적인지 결정할 필요가 있다. 성능도 중요한 고려 사항이고, 기존 네트워크 및 보안 시설과 신규 방화벽의 통합도 신중하게 고려해야 한다. 방화벽 솔루션을 설계할 때는 물리적인 환경과 인적 환경에 관련된 요구 사항도 고려해야 한다. 마지막으로, IPv6 기술이나 VPN 등의 도입과 같은 미래의 요구 사항 역시 고려해야 한다.

방화벽 성능을 지원하면서 동시에 조직의 방화벽 정책을 잘 수행할 수 있는 룰셋을 만들어라.

방화벽 룰셋은 방화벽이 통제하는 네트워크 트래픽과 관련하여 가능한 한 구체적이어야 한다. 룰셋을 만드는 과정은 어떤 트래픽 유형이 필요한지 결정하는 과정을 포함한다. 여기에는 방화벽 자체를 관리하는데 필요한 프로토콜도 포함된다. 룰셋 설정의 상세한 부분은 방화벽의 종류와 상품에 따라 매우 다양하지만, 대부분의 방화벽은 방화벽 룰셋을 최적화함으로써 성능을 향상시킬 수 있다.

예를 들어, 어떤 방화벽은 일치하는 결과가 나올 때까지 규칙을 순차적으로 확인한다. 이러한 방화벽의 경우, 트래픽 패턴에 일치할 가능성이 가장 높은 규칙들을 최대한 규칙 목록의 상위에 위치시켜야 한다.

방화벽 솔루션 전반에 걸쳐 방화벽 구조, 정책, 소프트웨어, 그리고 기타 구성 요소를 관리하라.

방화벽 관리는 여러 가지 측면에서 바라봐야 한다. 가령, 정책 규칙은 새로운 애플리케이션이나 호스트의 추가 등 조직의 요구 사항이 변동됨에 따라 업데이트될 필요성이 있다. 방화벽 구성 요소의 성능 역시 잠재적인 자원 문제를 사전에 식별하고 해결할 수 있도록 모니터링 할 필요가 있다. 로그와 경고 역시 위협(성공적인 것과 성공적이지 못한 것 모두)을 식별할 수 있도록 지속적으로 모니터링 할 필요가 있다. 방화벽 룰셋 및 정책에 대한 변화는 보안에 영향을 줄 가능성이 있기 때문에, 정해진 절차를 따르도록 해야 한다. 이 절차는 조직의 보안 정책이 제대로 시행되고 있는지 확인하기 위한 것으로 룰셋 검토나 주기적인 시험을 실시하게 된다.

소개

담당자/담당 기관

미국 표준 위원회 (NIST) 는 2002 년의 연방 정보 보안 관리법 (FISMA), Public Law 107-347 에 의한 규정 제정 의무를 다하기 위하여 이 문서를 제작하였다.

NIST 는 모든 정부 기관 및 자산에 충분한 수준의 정보 보안을 제공하는데 필요한 최소한의 요구 조건을 포함하는 표준과 가이드라인을 개발할 책임이 있다. 그러나 이러한 표준과 가이드라인은 국가 보안 체계에는 적용되지 않는다. 이 가이드라인은 미 예산관리국 (OMB, Office of Management and Budget) 회람 A-130, 8b(3)절 "*Securing Agency Information Systems*"와 부록 4: *Analysis of Key Sections* 에서 분석된 요구 사항과 일치한다. 추가 정보는 동일 문서의 부록 3 에서 찾을 수 있다.

이 가이드라인은 연방 정부 기관용으로 만들어진 것이다. 원하는 경우에는 이 가이드라인을 비정부 기관에서 이용해도 좋다. 저작권법에 저촉되지는 않겠지만, 가급적 NIST 에서 제작한 문서라는 점을 명시하면 좋겠다.

기존 상무부, 예산 관리국 국장 및 기타 어떤 다른 연방 기관의 권한과 이 문서의 내용이 상충되는 경우, 이 문서는 기존 권한을 변경하거나 대체하는 것으로 해석될 수 없으며, 기존

권한이 항상 우선시된다. 또한 본 문서의 내용은 미 상무부 장관의 법적 권한에 의하여 각 연방 기관에 의무적으로 도입된 표준 및 가이드라인의 내용과 반하는 내용으로 다루어질 수 없다.

목적과 범위

이 문서는 조직이 방화벽 기술과 방화벽 정책을 이해하는 과정에 도움을 주도록 작성되었다. 이 문서는 방화벽 정책 수립과 방화벽 선정, 설정, 시험, 배치, 관리 과정에 실질적이고, 실제로 적용되는 지침을 제공한다.

독자

이 문서는 주로 네트워크, 보안, 시스템 엔지니어, 관리자 등 방화벽 설계, 선정, 배치, 관리를 책임지는 IT 기술 인력을 대상으로 쓰여졌다. 네트워크와 시스템 보안을 책임지는 다른 IT 인력 역시 이 문서를 유용하게 활용할 수 있다. 이 문서의 내용은 네트워킹과 네트워크 보안에 대한 어느 정도의 기반 지식을 전제로 쓰여졌다.

문서 구조

이 문서는 크게 4 부분으로 구성되어 있다.

- 2 부에서는 전반적으로 다양한 방화벽 기술을 설명한다 - 패킷 필터링, 상태 조사, 애플리케이션-프록시 게이트웨이를 포함하며, 호스트 기반 방화벽, 개인 방화벽, VPN, 그리고 특화된 방화벽 몇몇 종류를 다룬다.
- 3 부에서는 네트워크에 방화벽을 배치하는 데 대하여 언급한다.
- 4 부에서는 방화벽 정책과 금지 대상 트래픽 종류에 관한 권고 사항을 제시한다.
- 5 부에서는 방화벽 구축 계획과 실제 구축을 개략적으로 다룬다. 이 부분에서는 방화벽 솔루션 선정에서 고려해야 할 요소들을 제시하고, 방화벽 설정, 시험, 배치, 유지에 필요한 권고 사항을 제시한다.

문서 뒷부분에는 부록이 있다.

- 부록 A 와 B 는 용어사전, 두문자어, 약어 목록을 제공한다.
- 부록 C 는 방화벽 이해에 도움이 될 수 있는 온라인, 오프라인 자료 목록을 제공한다.

방화벽 기술 개관

방화벽은 각기 다른 보안 태세를 취하는 네트워크나 호스트간의 네트워크 트래픽을 통제하는 장비나 프로그램이다. 방화벽은 보통 인터넷 연결과 관련해서 언급되지만, 다른 네트워크 환경에도 적용될 수 있다. 예를 들어, 많은 사무용 네트워크는 내부 네트워크에서 회계나 인사 등 민감한 정보를 다루는 부서로의 접근을 차단하기 위해 방화벽을 적용한다. 방화벽으로 이런 구역의 접근을 차단하면, 조직은 인증 받지 않은 상태로 시스템과 자원에 접근하는 것을 방지할 수 있다. 방화벽이 추가적인 보안 계층을 제공하는 것이다.

사용 가능한 방화벽 기술에는 여러 가지가 있다. 방화벽 기술 간의 능력을 비교하는 한 가지 방법은 각 방화벽이 검사할 수 있는 TCP/IP 계층을 확인하는 것이다. TCP/IP 프로토콜 스택은 4 개의 계층으로 구성되어 있다. 사용자가 네트워크를 통하여 자료를 전송하면, 자료는 가장 높은 계층부터 중간 단계의 계층을 거쳐 가장 낮은 단계의 계층까지 전달된다. 그리고 각각의 계층에서 추가적인 정보가 덧붙여진다. 가장 낮은 단계의 계층은 축적된 자료를 물리적 네트워크에 전송하고, 수신 측에서는 전송 받은 자료를 목적지의 가장 높은 계층까지 전달한다. 간단하게, 한 계층에서 생산된 자료는 그보다 한 단계 아래의 계층에 의해 좀 더 큰 컨테이너에 포함된다.

4 개의 TCP/IP 계층은 표 1 에 표시된 것과 같다.

애플리케이션 계층. 이 계층은 DNS, HTTP, SMTP 등 특정한 애플리케이션을 위한 데이터를 송/수신한다.
전송 계층. 이 계층은 네트워크 간에 애플리케이션 계층 서비스를 수송하기 위한 연결-지향형 혹은 연결과 무관한 서비스를 제공하며, 통신의 신뢰성을 부가적으로 보장할 수 있다. 전송 계층 프로토콜로는 TCP 와 UDP 가 흔하게 사용된다.
IP 계층 (일명 네트워크 계층). 이 계층은 네트워크를 가로질러 패킷을 분배한다. TCP/IP 용 기반 네트워크 계층 프로토콜은 IPv4 이다. IPv4 외에 네트워크 계층에서 흔하게 사용되는 프로토콜은 IPv6, ICMP, IGMP 등이다.
하드웨어 계층 (데이터 링크 계층). 이 계층은 물리적인 네트워크 구성 요소 상의 통신을 관리한다. 가장 잘 알려진 데이터 링크 계층 프로토콜은 이더넷이다.

표 1 TCP/IP 계층

각 네트워크 인터페이스에 할당된 데이터 링크 계층의 주소는 MAC 주소라고 불린다. (하나의 이더넷 카드가 소유하고 있는 이더넷 주소가 좋은 예이다.) 방화벽 정책은 데이터 링크 계층과 거의 관련이 없다. 네트워크 계층의 주소는 IP 주소라고 불린다. 전송 계층은 특정한 네트워크 응용 프로그램을 식별하고, 네트워크 주소와 대조되는 통신 세션을 식별한다. 하나의 호스트는 같은 네트워크에 존재하는 다른 호스트들과의 관계에서 다수의 전송 계층 세션을 보유할 수도

있다. 이 때문에 전송 계층에 포트 개념이 포함되어 있다. (목적지 포트 번호는 일반적으로 목적지 호스트에서 응답 대기 중인 서비스를 식별하고, 출발지 포트는 일반적으로 목적지 호스트가 응답해야 할 출발지 호스트의 포트 번호를 식별한다. 출발지 IP 주소, 출발지 포트, 목적지 IP, 목적지 포트의 조합을 이용해서 세션을 정의한다. 가장 높은 단계의 계층은 최종 사용자 응용을 대표한다.)

방화벽은 응용 트래픽을 조사할 수 있고, 그 트래픽을 정책 결정 기반으로 사용할 수 있다. 일반적인 방화벽은 1 개 혹은 소수의 계층에서 작동한다. 반면, 조금 더 진보된 방화벽은 "표 1 TCP/IP 계층"에 등장하는 모든 계층을 조사한다. 더 많은 계층을 조사하는 방화벽은 좀 더 세밀하고 정확하게 검사를 수행할 수 있다. 응용 계층을 이해하는 방화벽은 고급 응용과 프로토콜을 포괄하고 사용자별 서비스를 제공할 수 있다. 예를 들어, 하위 계층만을 다루는 방화벽은 일반적으로 특정 사용자를 식별할 수 없으나, 응용 계층에서 작동 가능한 방화벽은 특정 사용자에게 사용자 인증과 이벤트 로깅을 강제할 수 있다.

방화벽 기술

이 부분에서는 방화벽 기술에 대한 개요와 흔히 사용되는 기술의 능력에 대한 기본적인 정보를 제공한다. 방화벽은 다른 시스템과 결합되는 경우가 많다. (주로 라우터) 방화벽과 관련된 기술들은 원래 다른 시스템의 일부인 경우가 많다. 예를 들자면, NAT 기술을 방화벽 기술로 생각하는 경우도 있지만, NAT 는 원래 라우팅 기술의 일종이다.

패킷 필터링

방화벽의 가장 기본적인 기능은 패킷 필터이다. 패킷 필터 기능만을 제공하는 방화벽 stateless inspection firewall 은 본질적으로 호스트 주소와 통신 세션에 대한 접근 통제 기능을 제공하는 라우팅 장비이다. 다른 진보된 필터와 달리, 패킷 필터는 패킷의 내용물에는 관여하지 않는다. 패킷 필터의 접근 통제 기능은 룰셋이라고 불리는 지시문 집합을 통해 좌우된다. 패킷 필터링 능력은 대부분의 OS 와 라우팅이 가능한 장비에 포함되어 있다; 순수한 패킷 필터링 장비의 가장 흔한 예는 접근 통제 목록을 운용하는 네트워크 라우터이다.

패킷 필터를 장착한 방화벽은 기본적으로 네트워크 계층에서 작동한다. 이런 장비는 패킷에 포함된 몇몇 정보를 기반으로 네트워크 접근 통제 기능을 제공한다. 정보는 다음과 같다:

- 패킷의 출발지 IP 주소 - 네트워크 패킷이 출발한 호스트의 주소 (예:192.168.1.1)

- 패킷의 목적지 IP 주소 - 네트워크 패킷이 도달하려고 하는 호스트의 주소 (예:192.168.2.1)
- 출발지와 목적지의 통신에 사용된 네트워크 프로토콜. TCP, UDP, ICMP 등
- 세션 출발지 및 목적지 포트
  (예: TCP 80 은 웹 서버 목적지 포트, TCP 1320 은 웹 서버에 접근하는 PC 의 출발지 포트)
- 패킷이 사용하는 인터페이스 및 방향 (인바운드 또는 아웃바운드)

패킷 필터 기능만을 가진 방화벽은 속도와 유연성이라는 두 가지 장점을 가지고 있다. 패킷 필터가 네트워크 계층 이상의 데이터를 조사하는 일은 거의 없기 때문에, 패킷 필터 방화벽은 매우 빠르게 작동할 수 있다. 그리고 근래 대부분의 네트워크 프로토콜이 네트워크 계층 혹은 그 이하의 계층에 포함되고 있기 때문에, 패킷 필터는 거의 모든 종류의 네트워크 통신 및 프로토콜에 대해 어느 정도의 보안을 제공할 수 있다. 패킷 필터 방화벽은 단순하기 때문에 회사 네트워크 망 어느 곳이나 배치하기 편하고, 패킷 필터 방화벽은 빠르기 때문에 신뢰할 수 없는 네트워크와 맞닿은 최-외곽 경계, 혹은 경계선에 배치하여 유입되는 트래픽을 차단하는 이상적인 수단으로 활용할 수 있다. 이러한 작업을 유입 필터링 ingress filterling 이라고 한다. 경계 라우터 boundary router 라고 불리는 이러한 패킷 필터는 특정한 저수준 계층 공격을 막을 수 있고, 정책 설정으로 간단한 접근 통제를 수행할 수 있으며 (원하지 않는 프로토콜을 차단하고 나머지를 통과시키는 등의 정책), 패킷 필터에서 통과된 트래픽을 더 강력한 방화벽으로 전달해서 더 높은 계층에서의 접근 통제와 필터링을 수행하도록 할 수 있다. 이러한 기본적인 필터링을 수행함으로써, 경계 라우터는 다른 방화벽의 처리 부담을 경감시킨다. 아래의 그림 1 은 경계 라우터로 사용되는 패킷 필터를 보여주고 있다.

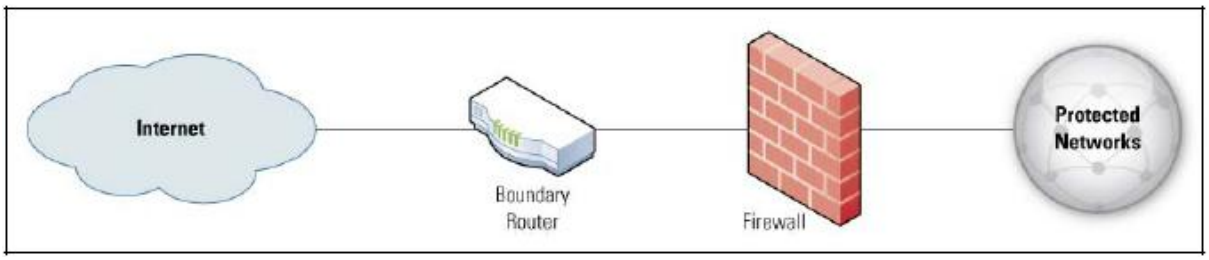

그림 1 경계 라우터로 사용되는 패킷 필터

외부로 나가는 트래픽도 유출 필터링 egress filtering 이라 불리는 작업을 통하여 필터링 할 수 있다. 조직은 외부의 FTP 서버 이용을 차단하거나, 조직 내부에서 외부로 이루어지는 DoS 공격을 예방하는 등의 제한 조치를 조직 내부의 트래픽에 적용할 수 있다. 조직은 유출 트래픽 중 조직에서 실제로 사용 중인 IP 주소를 출발지 IP 로 사용하는 트래픽만 허용해야 한다. 이렇게

하면 다른 네트워크의 주소로 변조된 트래픽을 차단할 수 있다. 이렇게 변조된 주소를 가진 트래픽은 악성 코드에 감염되거나 해킹 당한 호스트, 혹은 설정 실수 등에 의해 발생할 수 있다.

패킷 필터만 사용하는 방화벽은 신속성과 유연성을 제공하지만, 태생적인 한계도 역시 지니고 있다. 패킷 필터가 상위 계층의 데이터를 조사하지 않기 때문에, 패킷 필터는 응용 프로그램의 특정한 취약점이나 함수를 활용하는 공격을 차단할 수 없다. 예를 들어, 패킷 필터 방화벽은 특정 응용 프로그램 명령어를 차단할 수 없다. 만약에 패킷 필터가 특정 응용 트래픽을 허가할 경우, 해당 응용 내에서 이뤄지는 모든 기능과 함수 역시 허가되는 것과 같기 때문이다. 상위 계층 데이터 조사가 불가능한 점은, 고급 사용자 인증 구조를 지원하지 못하게 하고, 의미 있는 로그를 남기기 어렵게 만든다. 대부분의 로그가 똑같은 정보(출발지 주소, 목적지 주소, 트래픽 타입)만 기록되기 때문이다.

패킷 필터는 일반적으로 TCP/IP 스펙과 프로토콜 스택의 문제점을 이용한 공격과 익스플로잇에 취약하다. 예를 들어, 많은 패킷 필터는 패킷의 네트워크 계층 주소 정보가 변조되었는지 탐지할 수 없다. 대개 방화벽 플랫폼으로 구축된 보안 통제를 우회하려는 침입자들이 변조 공격을 시도한다. 상위 계층에서 작동하는 방화벽은 세션이 수립되었는지 확인하거나 트래픽 허용 이전에 사용자 인증을 하는 등의 방법으로 일부 변조 공격을 저지할 수 있다.

이러한 한계 때문에 패킷 필터 방화벽은 대개 네트워크의 최-외곽에서 기본적인 트래픽 필터링을 수행하는 1 차 방어선으로 이용된다. 추가적인 기능을 보유한 방화벽은 대개 패킷 필터 방화벽 뒤에 위치하게 된다. 일반적으로 이러한 방화벽은 패킷 필터 방화벽만큼 신속하게 패킷을 처리하지는 못한다. 만약 추가적인 기능을 보유한 방화벽의 트래픽 처리 속도가 충분히 빠르다면, 패킷 필터 방화벽 대신 네트워크 최-외곽에 배치하고 운용할 수 있다.

상태 기반 감시

상태 기반 감시 stateful inspection 는 연결 상태를 추적하고, 정상 상태에서 벗어난 패킷을 차단하는 방법으로 패킷 필터의 능력을 향상시킨다. 이러한 작업은 전송 계층에 대한 심층적인 분석 기능을 통합시킴으로써 가능하게 된다. 패킷 필터링과 마찬가지로, 상태 기반 감시는 네트워크 계층의 패킷이 기존 방화벽 규칙에 의해 허용되는지 검사한다. 그러나 패킷 필터링과는 다르게, 상태 기반 감시는 상태 표에 각 연결의 상태를 추적하고 기록한다. 상태 표의 세부 내용은 각 방화벽 제품에 따라 다양하지만, 일반적으로 출발지 IP 주소, 목적지 IP 주소, 포트 번호, 그리고 연결 상태 정보를 포함한다.

TCP 트래픽에는 크게 연결 성립, 사용 중, 그리고 연결 종료 (연결 종료는 연결 종료 요청에 의한 것과 장시간 사용되지 않은 연결 모두를 포함한다.) 3 가지의 상태가 존재한다. 방화벽의 상태 기반 감시는 각 연결의 상태를 감시하기 위하여 TCP 헤더에 포함된 특정한 값을 검사한다. 방화벽은 패킷이 정상적인 상태인지 아닌지를 확인하기 위하여 모든 새 패킷을 방화벽의 상태 표와 비교한다. 예를 들어, 공격자는 이미 연결된 세션으로 표시한 헤더를 가진 패킷을 만들어 방화벽을 통과하려고 시도할 수 있다. 만약 해당 방화벽이 상태 기반 감시를 사용하는 경우, 방화벽은 가장 먼저 해당 패킷이 상태 표에 등재된 연결의 일부인지 아닌지를 검증할 것이다.

아래의 표 2 는 상태 표 예제이다. 만일 내부 네트워크에 위치한 장비(여기서는 192.168.1.100)가 방화벽 외부의 장비(192.0.2.71)에 연결하려고 시도할 경우, 방화벽은 먼저 이 연결 시도가 방화벽 룰셋에 의해 허용되었는지 확인한다. 만약 허용되었을 경우, 방화벽은 새 세션이 시작되었음을 표시하는 항목으로 시작됨 Initiated 을 상태 표에 추가한다. (표 2 의 첫 번째 열) 여기서 192.0.2.71 과 192.168.1.100 이 3 단계 TCP 접속을 완료하게 되면, 연결 상태는 연결됨 Established 으로 변경되고, 이후에 해당 항목과 일치하는 모든 트래픽은 방화벽을 통과할 수 있도록 허용된다.

출발지 주소	출발지 포트	목적지 주소	목적지 포트	연결 상태
192.168.1.100	1030	192.0.2.71	80	시작됨
192.168.1.102	1031	10.12.18.74	80	연결됨
192.168.1.101	1033	10.66.32.122	25	연결됨
192.168.1.106	1035	10.231.32.12	79	연결됨

표 2 상태 표 예제

UDP 같은 일부 프로토콜은 연결이라는 개념과 연결 시작, 수립, 종료 등의 절차가 존재하지 않기 때문에, TCP 와 같은 방법으로 전송 계층에서 상태를 추적하는 것이 불가능하다. 상태 기반 감시 기능을 보유한 대부분의 방화벽은 이러한 프로토콜에 대하여 단지 목적지, 출발지 IP 주소와 포트를 추적하는 것만이 가능하다. UDP 패킷은 출발지 IP, 목적지 IP, 포트 정보를 기반으로 작성된 상태 표 항목과 일치해야 한다. 따라서 이런 시스템에서 외부에서 들어오는 DNS 응답은, 방화벽이 그에 대응하는 내부에서 외부로 나가는 DNS 쿼리를 이전에 처리하였을 경우에 한하여 허용될 것이다. 방화벽이 세션의 종료 여부를 식별할 수 없기 때문에, 해당 항목은 미리 설정된 시간 제한에 도달한 이후 상태 표에서 삭제된다. DNS 를 인식할 수 있는 응용 수준 방화벽 Application-level firewall 은 시간 제한을 사용하지 않고도 DNS 응답이 수신된 이후 바로 세션을 종료시킬 수 있다.

상태 기반 감시의 최근 추세는 상태 기반 프로토콜 분석 능력을 추가하는 것으로, 일부 제조사는 이를 *심층 패킷 분석* deep packet inspection[1]이라고 이름 붙였다. 상태 기반 프로토콜 분석은 기본적인 침입 탐지 기술을 추가함으로써 표준 상태 기반 감시 기능을 향상시킨다. 이 검사 엔진은 네트워크, 전송, 응용 계층에 있는 프로토콜을 분석하고, 제조사가 개발한 정상 프로토콜 행위 프로필과 비교하여 프로토콜이 정상적으로 작동하는지, 비정상적으로 작동하는지 판단한다. 이 기능은 같은 명령어가 반복적으로 실행되거나, 선행 명령어 없이 실행되는 명령어 등 예측되지 않은 명령어 조합을 식별할 수 있다. 보통 버퍼 오버플로우, DoS, 악성 코드, 그리고 HTTP 같은 응용 프로토콜을 이용하는 형태의 공격이 이런 의심스러운 명령어를 전송한다. 또 다른 흔한 기능은 인수의 최소, 최대값 등을 이용하여 각 명령의 적합성을 검사하는 것이다. 예를 들어, username 인수의 길이가 1000 글자에 달할 경우 (게다가 바이너리 데이터까지 포함하고 있다면 더욱 더) 수상한 값이라 할 수 있다.

상태 기반 감시 및 상태 기반 프로토콜 분석 능력을 모두 보유한 방화벽이라도 완벽한 침입 탐지/방지 시스템(IDPS)으로 취급할 수 없다. IDPS 는 좀 더 광범위한 공격 탐지 및 방지 능력을 보유하고 있다. 예를 들어, IDPS 는 서명 기반이나 비정상 행위 분석을 활용하여 네트워크 유해 트래픽을 더 정교하게 찾아낼 수 있다.[2]

애플리케이션-프록시 게이트웨이

애플리케이션-프록시 게이트웨이는 하위 계층 접근 통제 기능을 상위 계층 기능과 통합하는 고급 방화벽 기능 중 하나이다. 이러한 방화벽은 서로 통신을 시도하는 호스트 사이에 위치한 중계 프록시 에이전트를 포함하는데, 이 에이전트는 두 호스트 간의 직접 연결을 허용하지 않는다. 접속이 성공하면 실제로 2 개의 연결을 만들어진다. 하나는 클라이언트와 프록시 서버 간의

---

[1] 이 문서에서는 *상태 기반의 프로토콜 분석* *stateful protocol analysis* 이라는 용어를 사용하는데, 그 이유는 네트워크 기반의 활동에만 적용되는 *심층 패킷 분석* *deep packet inspection* 과 달리, 이 용어가 네트워크 기반 및 호스트 기반 활동을 다루는 데에 모두 적절하기 때문이다. 역사적으로, 보안 커뮤니티 내에서 심층 패킷 분석이라는 용어의 정의에 대한 합의가 이루어진 적은 없다.

[2] IDPS 에 대한 추가적인 정보는 NIST 특별 저작물 (SP) 800-94, IDPS 가이드 (http://csrc.nist.gov/publications/nistpubs/)를 참조할 것.

연결이고, 다른 하나는 프록시 서버로부터 실제 목적지까지의 연결이다. (그림 2 참조). 각 호스트가 프록시의 존재를 식별하지 못하도록 설계되기 때문에, 각각의 호스트는 상호 간의 직접적인 연결에 성공했다고 여기게 된다. 외부 호스트는 오로지 프록시 에이전트와 통신을 하기 때문에, 내부 IP 주소는 바깥 세상에 전혀 알려지지 않는다. 프록시 에이전트는 방화벽 룰셋과 직접 통신하는 방식으로 네트워크 트래픽을 통과시킬지 말지 결정한다. 이와 더불어 각각의 프록시 에이전트는 각 네트워크 사용자에게 인증을 요구할 수 있는 능력이 있다. 이 사용자 인증은 ID 와 암호, 하드웨어나 소프트웨어 토큰, 출발지 주소, 생체 인식 등의 여러 가지 형태를 취할 수 있다.

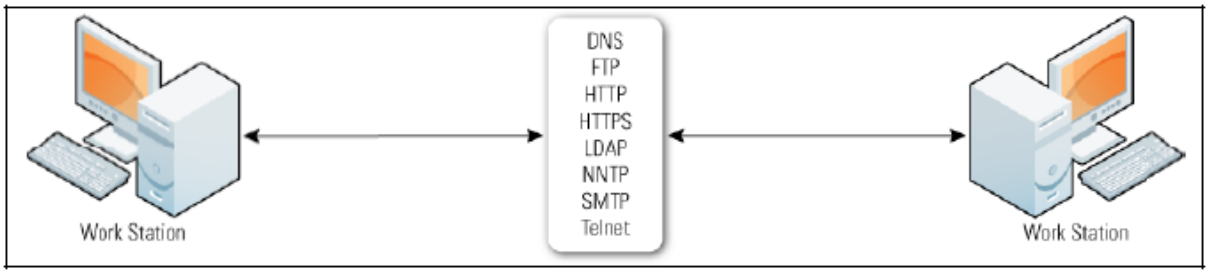

그림 2 일반적인 프록시 에이전트

프록시 에이전트는 응용 계층에서 작동하며, 트래픽의 실질적인 내용을 조사한다. 특정 트래픽이 주로 특정 트래픽이 프로토콜 정의와 일치하는지 검증하는 상태 기반 프로토콜 분석과 달리, 애플리케이션-프록시 게이트웨이는 데이터를 분석하여 패킷의 내용을 좀 더 철저하게 조사한다. 알려진 결함을 이용하는 익스플로잇을 포함할 가능성이 있는 트래픽과 일반적인 트래픽을 구분해낸다. 이와 동시에, 게이트웨이는 출발지의 시스템과 TCP 접속을 처리하고 연결의 각 단계에서 익스플로잇에 대한 보호를 수행할 수 있다. 또한, 게이트웨이는 응용 프로토콜의 헤더나 페이로드 정보를 기반으로 트래픽의 허용 여부를 결정할 수 있다. 예를 들어, 게이트웨이는 특정 이메일이 조직에서 허가하지 않은 특정 종류의 첨부 파일(실행 가능한 파일 등)을 첨부하고 있는지, 혹은 인스턴트 메신저가 80 번 포트(HTTP)를 경유하여 사용되고 있는지 알아낼 수 있다. 게이트웨이는 특정한 작업의 수행을 제한할 수 있고(사용자는 FTP 에서 put 명령을 사용하지 못할 수도 있다), ActiveX 나 자바 등 특정한 종류의 동적 컨텐츠를 포함한 웹 페이지를 허용하거나 차단하는 목적으로 사용할 수 있다. 게이트웨이가 해당 데이터를 허용하도록 결정하면, 비로소 데이터가 목적지 호스트로 전달된다.

애플리케이션-프록시 게이트웨이는 패킷 필터나 상태 기반 감시에 비해 많은 장점을 지니고 있다. 첫째, 애플리케이션-프록시 게이트웨이는 좀 더 높은 수준의 보안을 제공하는데, 이는 두 호스트 사이의 직접 연결을 방지할 뿐 아니라 정책 위반 여부를 판단하기 위해 트래픽 내용을 검사하기

때문이다. 둘째, 게이트웨이는 네트워크 주소와 포트만이 아닌 패킷 전체를 검사할 수 있기 때문에 좀 더 세세하게 로그를 기록할 수 있는 능력이 있다. 예를 들어, 애플리케이션-프록시 게이트웨이 로그는 네트워크 트래픽 내의 특정 애플리케이션 명령어를 기록할 수 있다. 또한, 애플리케이션-프록시 게이트웨이 구조 상 사용자 인증 능력이 우수하다. 또 다른 장점은 일부 애플리케이션-프록시 게이트웨이의 경우 암호화된 패킷(SSL 로 보호된 페이로드 등)을 해독하고, 검사한 후, 목적지 호스트로 전송하기 전에 다시 암호화를 할 수 있다는 점이다. 게이트웨이가 해독할 수 없는 데이터는 응용 프로그램에게 전달되지 않는다. 마지막으로, 애플리케이션-프록시는 주소 변조 공격을 탐지하는 능력이 더 뛰어나다.

그러나 애플리케이션-프록시 게이트웨이가 적용된 고급 방화벽은 패킷 필터링, 상태 기반 감시 방화벽과 비교했을 때 몇 가지 단점을 가지고 있다. 첫째, 애플리케이션-프록시 게이트웨이가 "모든 패킷"을 처리하기 때문에, 방화벽은 패킷 해독과 분석에 더 많은 시간을 소모하게 된다. 이 때문에, 일부 게이트웨이는 높은 대역폭이 필요하거나 실시간 애플리케이션을 사용하는 경우에는 부적합하다. 그러나 높은 대역폭에도 적합한 애플리케이션-프록시 게이트웨이가 존재하기도 한다. 방화벽의 부하를 줄이려면, 전용 프록시 서버를 이용해서 이메일이나 웹 트래픽 등 응답 시간에 덜 구애 받는 서비스를 처리하게 하면 된다. 또 다른 단점은 애플리케이션-프록시 게이트웨이가 신규 네트워크 응용이나 프로토콜에 대한 지원이 제한적인 경향이 있다는 것이다. 방화벽을 통과하려면 각 네트워크 트래픽 종류별로 전용 애플리케이션-프록시 에이전트가 필요하다. 많은 애플리케이션-프록시 게이트웨이 제조사들은 정의되지 않은 네트워크 프로토콜과 애플리케이션을 처리하는 프록시 에이전트를 제공한다. 이런 에이전트는 트래픽이 "터널"을 거쳐 방화벽을 통과하도록 단순히 허가하는 경우가 많기 때문에, 애플리케이션-프록시 게이트웨이 구조의 능력을 크게 저하시키는 요인이 된다.

회로 수준 게이트웨이

회로 수준 게이트웨이 circuit-level gateway 는 프록시의 다른 형태로, 간혹 회로 수준 프록시 circuit-level proxy 로 불리는 경우가 있다. 회로 수준 게이트웨이는 내부 시스템을 외부로부터 방어하는 프록시 기능과 함께, 상태 기반 감시와 비슷한 방법으로 연결이 수립되기 전에 각각의 연결을 검증한다. 연결 시도가 수신되면, 회로 수준 게이트웨이는 룰셋을 확인하여 연결의 허용 여부를 결정한다. 규칙은 일반적으로 목적지 IP 와 포트, 출발지 IP 와 포트, 요청된 애플리케이션 프로토콜 등에 기반하여 구성된다. 일부 회로 수준 게이트웨이는 사용자 인증이나 시간 제한 등을 추가로 규칙 설정에 적용할 수 있다.

연결이 허용되면, 상태 정보를 동시에 포함하고 있는 가상 회로 표에 항목이 추가된다. 표에 목록으로 표시된 패킷들은 추가 검증 없이 방화벽을 통과하게 된다. 연결이 종료되었거나 사전에 설정된 시간 동안 비활성화되어 있을 경우, 해당 항목은 표에서 제거된다. 회로 수준 프록시는 상태 기반 감시 방화벽과 유사한 기능을 많이 제공하는데, 여기에 방화벽의 서로 다른 측에 위치한 호스트 사이의 직접 연결을 차단하는 프록시 기능을 추가한 형태이다. 회로 수준 게이트웨이는 일반적으로 애플리케이션-프록시 게이트웨이 방화벽보다 신속하게 작동하는데, 이는 애플리케이션-프록시 게이트웨이가 데이터 내용을 검증하는 것과 달리 회로 레벨 게이트웨이는 데이터를 가지고 처리하는 검증 절차가 조금 더 단순하기 때문이다.

전용 프록시 서버

전용 프록시 서버는 애플리케이션-프록시 서버 및 회로 레벨 게이트웨이와 다른 종류의 프록시로, 트래픽에 대한 프록시 통제를 유지하면서 방화벽 기능이 제외된 형태이다.

방화벽에 포함되지 않지만, 전용 프록시 서버는 애플리케이션-프록시 게이트웨이 방화벽 및 회로 수준 게이트웨이 방화벽과 매우 가까운 관계이기 때문에 본 절에서 다루기로 한다. 많은 프록시는 애플리케이션에 특화되어 있으며, 일부는 실제로 HTTP 와 같은 흔한 애플리케이션 프로토콜에 대한 분석과 검증을 수행한다. 전용 프록시 서버가 방화벽 기능을 가지고 있지 않기 때문에, 이러한 서버는 주로 전통적인 방화벽 플랫폼 뒤에 배치된다. 일반적으로, 주 방화벽이 유입 inbound 트래픽을 접수하고, 어떤 애플리케이션이 목표인지를 결정하고, 적절한 프록시 서버 (이메일 프록시 등) 에 트래픽을 전달하게 된다. 이 서버는 트래픽에 대한 필터링과 로깅 작업을 마친 후, 내부 시스템에 트래픽을 전달하게 된다. 마찬가지로 내부 시스템에서 외부로 나가는 outbound 트래픽도 프록시 서버가 받아서, 필터링이나 로깅을 마친 후, 방화벽에 전달하여 외부로 나가도록 할 수 있다. 이 과정의 예로는 방화벽 뒤에 위치한 HTTP 프록시 서버가 있다. 사용자가 외부의 웹 서버에 접속하려면 이 프록시 서버에 먼저 연결되어야 한다. 전용 프록시 서버는 방화벽의 처리 부하를 줄이고 방화벽이 직접 처리하기 어려운 특화된 필터링과 로깅 작업을 처리할 목적으로 널리 사용된다.

최근에는 인바운드 프록시 서버의 사용이 극적으로 감소하였다. 인바운드 프록시 서버는 자신이 보호하는 진짜 서버의 기능을 흉내내어야 하는데, 많은 기능을 보유한 서버의 경우 프록시 서버가 제대로 흉내내는 것이 거의 불가능하기 때문이다. 서버의 모든 기능을 흉내내지 못하는 프록시 서버를 사용하게 되면, 프록시 서버에서 미처 흉내내지 못하는 기능의 경우 사용 불가능한 상태가 되고 만다. 게다가 인바운드 프록시 서버가 보유해야 하는 필수 기능들(로깅,

접근 통제 등)이 운영 서버에 포함되는 경우가 많아졌다. 현재 사용되는 대부분의 프록시 서버는 아웃바운드 프록시 서버로, 가장 흔한 것은 역시 HTTP 프록시이다.

아래의 그림 3 은 HTTP 와 이메일 전용으로 다른 방화벽 체계 뒤에 배치된 전용 프록시 서버의 운용을 보여준다. 이메일 프록시는 송신, 수신 이메일을 모두 관리하는 메일 게이트웨이가 될 수 있다. 모든 메시지와 통신은 내부에 위치한 다른 메일 서버로 전달되기 전에 반드시 이 프록시를 거쳐야 한다. 이렇게 인터넷과 내부 메일 서버의 직접 연결을 차단해 놓으면 메일 서버에 대한 공격이 더욱 어려워진다. 공격자는 메일 게이트웨이만 직접 공격할 수 있다. HTTP 프록시는 외부 웹 서버 접속을 관리한다. 관리 대상으로 동적 컨텐츠를 포함할 수도 있다. 많은 조직들은 네트워크 트래픽을 줄이고 반응 시간을 단축할 목적으로 자주 사용되는 웹 페이지를 프록시에서 캐시할 수 있도록 설정한다.

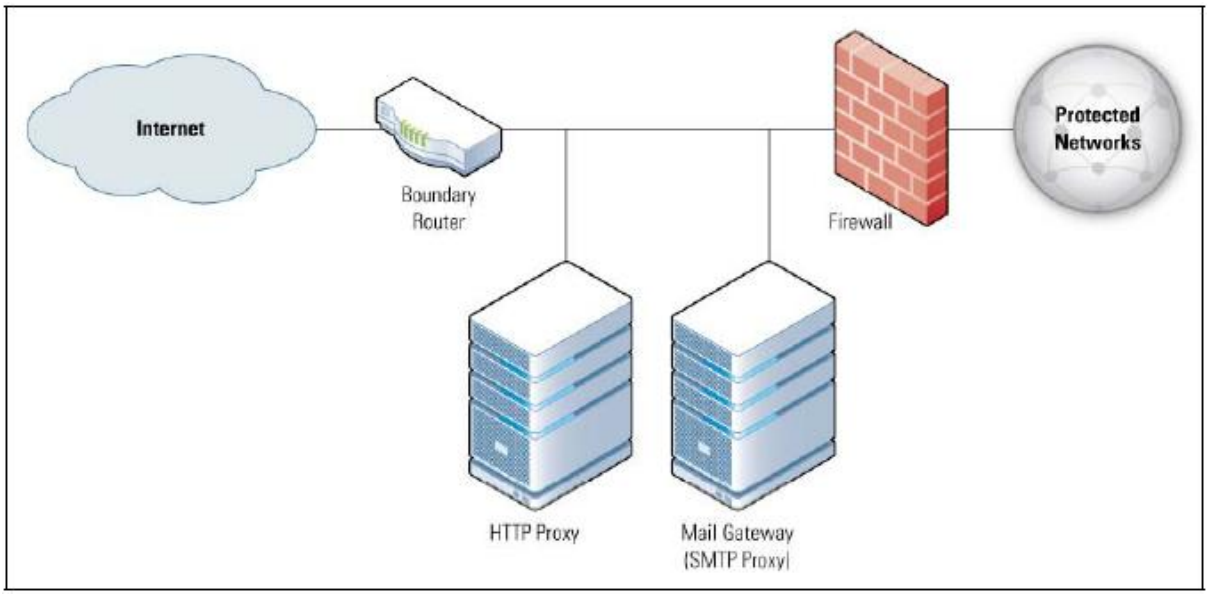

그림 3 애플리케이션 프록시 설정

가상 사설망

네트워크 경계에 위치한 방화벽 장비는 종종 원하지 않는 트래픽을 차단하는 것 이상의 일을 해야 할 때가 있다. 바로, 보호되는 네트워크와 외부 네트워크 간의 특정 네트워크 트래픽 트래픽을 암호화하고 다시 해독하는 일이다. 이는 트래픽을 암호화하고 사용자 인증과 무결성 검사에 필요한 추가 프로토콜을 제공하는 VPN 을 포함한다는 뜻이다. VPN 은 대개 신뢰할 수 없는 네트워크를 경유하는 보안 네트워크 연결을 제공할 때 사용된다. 예를 들어, VPN 기술은 여러 장소에 위치하는 조직의 보호된 네트워크를 인터넷을 경유하여 연장하는 데에 광범위하게

사용되고, 사용자가 인터넷을 경유하여 조직 내부 네트워크에 원격 보안 접속을 할 수 있도록 한다. 보안 VPN 에서 사용되는 가장 흔한 두 가지 옵션은 Internet Protocol Security (IPSec)[3]와 Secure Sockets Layer (SSL)/Transport Layer Security (TLS)이다.[4]

가장 흔한 VPN 구조 3 가지는 게이트웨이-게이트웨이, 호스트-게이트웨이, 호스트-호스트이다.[5] 게이트웨이-게이트웨이 구조는 가장 많이 사용되는 것으로, 다수의 고정된 위치에 VPN 게이트웨이를 설치하고 인터넷을 경유하여 망을 연결한다. 예를 들면, 조직의 본사에서 지사를 연결할 때 사용한다. VPN 게이트웨이는 보통 방화벽이나 라우터 등 다른 네트워크 장비의 일부이다. 일단 VPN 연결이 두 게이트웨이 사이에 성립되면, 원격지에 위치한 사용자들은 VPN 연결을 거의 인식할 수 없을 뿐만 아니라 추가적으로 컴퓨터에 어떤 조작도 할 필요가 없다. 두 번째로, 호스트-게이트웨이 구조는 집이나 호텔 등 조직 외부에 위치한 개별 사용자들(원격 사용자)에게 보안 연결을 제공한다. 여기서는 사용자 컴퓨터에 설치된 클라이언트가 조직의 VPN 게이트웨이와 보안 연결을 수립하게 된다. 세 번째 구조는 호스트-호스트 구조로 사용되는 빈도가 가장 낮다. 이 설정은 대개 단일 서버의 원격 관리를 가능하게 한다.

게이트웨이-게이트웨이 및 호스트-게이트웨이 VPN 의 경우에는 VPN 기능이 방화벽 자체에 포함되는 경우가 많다. 방화벽 뒤에 배치하는 경우, VPN 트래픽은 암호화된 채로 방화벽을 통과하며, 방화벽이 해당 트래픽을 검사하지 않도록 한다. 모든 VPN 은 방화벽 관리자로 하여금 어떤 사용자가 어떤 네트워크 자원에 접근할 수 있는지 결정할 수 있다. 이 접근 통제는 기본적으로 사용자별로 시행된다. 따라서 VPN 정책은 어떤 사용자들이 어떤 네트워크 자원들에 접근할 수 있는지 큰 그림을 그린다고 할 수 있다. VPN 은 대개 RADIUS(RFC 2865, Remote Authentication Dial In User Service)와 같은 인증 프로토콜에 의존한다. RADIUS 는 사용자 이름과 암호, 디지털 서명, 하드웨어 토큰 등 여러 종류의 인증 증명서를 사용한다.

---

[3] IPSec 에 대한 추가 정보는 NIST SP 800-77, IPsec VPNs 가이드를 참조하라 (http://csrc.nist.gov/publications/nistpubs/).

[4] SSL 과 TLS 에 대한 추가 정보는 NIST SP 800-52, TLS 도구 선정 및 사용에 대한 가이드라인과 NIST SP 800-113, SSL VPNs 가이드를 참조하라 (http://csrc.nist.gov/publications/nistpubs/).

[5] VPN 구조에 대한 추가 정보는 NIST SP 800-77, IPsec VPNs 가이드와 NIST SP 800-113, SSL VPNs 가이드를 참조하라 (http://csrc.nist.gov/publications/nistpubs/).

방화벽에서 VPN 기능을 실행하려면, VPN 을 통해 오가는 트래픽의 양과 사용되는 암호화 종류에 따라 추가적인 자원이 필요하다. 일부 환경에서는 VPN 으로 인한 트래픽 때문에 처리 용량과 자원이 더 필요할 수 있다. 방화벽 구축 계획에는 포함할 VPN 의 종류(게이트웨이-게이트웨이나 원격 접속)도 포함되어야 한다.

방화벽의 위치

네트워크 경계에 위치한 방화벽의 경우 내부 호스트를 어느 정도 보호하긴 하지만, 대부분의 경우 추가적인 네트워크 보호가 필요하다. 네트워크 방화벽이 모든 형태의 공격과 모든 공격 시도를 인지하는 것은 불가능하기 때문에, 종종 일부 공격이 방화벽을 뚫고 내부 호스트까지 도달하는 경우가 있다. 그리고, 내부 호스트가 다른 내부 호스트를 노리고 시작한 공격은 보통 네트워크 방화벽을 거치지 않는다.

이상의 이유와 또 다른 요소들로 인해, 네트워크 설계자들은 추가적인 보안 계층을 제공하기 위하여 네트워크 경계는 물론 다른 장소에도 방화벽 기능을 포함시키기 마련이다.

호스트 기반 방화벽과 개인용 방화벽

서버용 호스트 기반 방화벽과 데스크탑과 랩탑 컴퓨터를 위한 개인용 방화벽은 네트워크 기반 공격을 더 잘 방어할 수 있도록 추가적인 보안 계층을 제공한다. 이러한 방화벽은 소프트웨어 기반으로, 방화벽이 보호하는 호스트에 존재한다. 각 방화벽은 단일 호스트의 유입, 유출 네트워크 트래픽을 감시하고 통제한다. 이런 방화벽들은 특정 호스트의 환경에 최적화 할 수 있기 때문에 네트워크 방화벽보다 더 나은 보안을 제공할 수 있다.

호스트 기반 방화벽은 리눅스나 윈도우 등 서버 운영체제의 일부일 수도 있고, 간혹 다양한 운영체제에 설치되는 서드파티 애드온의 형태로 설치될 수 있다. 필요한 트래픽만 허용하도록 호스트 기반 방화벽을 설정하면 모든 호스트 및 서브넷(네트워크 방화벽으로 구분되지 않은 내부 서브넷 포함)에서 발생하는 악의적인 동작으로부터 보호받을 수 있다. 호스트에서 외부로 향하는 트래픽을 제한하면 다른 호스트로 전염되는 맬웨어를 차단하는 데 도움이 될 수 있다.[6] 호스트

[6] 만약 공격자가 이미 호스트를 장악하고 관리자 레벨의 권한을 획득한 경우, 공격자는 호스트 기반 방화벽을 비활성화하거나 우회할 수 있다.

기반 방화벽은 일반적으로 로그를 남기도록 되어있으며, 주소 기반 접근 통제를 수행하도록 설정할 수도 있다.

개인용 방화벽은 윈도우나 Mac OS X 등의 사용자 중심 운영체제를 탑재한 랩탑이나 데스크탑 컴퓨터에서 동작하는 소프트웨어이다. 개인용 방화벽은 호스트 기반 방화벽과 유사하지만, 보호 대상이 되는 컴퓨터가 최종 사용자 대상이기 때문에 일반 사용자가 이해하기 더 쉬운 인터페이스를 제공한다. 개인용 방화벽은 네트워크 경계 방화벽 내부나 외부 어디에 있더라도 랩탑이나 데스크탑 컴퓨터에게 추가적인 보안 계층을 제공한다. 개인용 방화벽은 인바운드와 아웃바운드 통신을 제한할 수 있는데, 이것은 랩탑이나 데스크탑을 외부로부터의 공격에서 보호하는 것은 물론, 감염된 컴퓨터로부터 시작되는 맬웨어의 확산이나 P2P 파일 공유 프로그램 등 허가되지 않은 프로그램을 다운로드하거나 사용하는 것 등을 차단할 수도 있음을 의미한다. 개인용 방화벽은 종종 안티바이러스 소프트웨어, 침입 탐지 소프트웨어 등 기타 보안 유틸리티와 패키지로 제공되기도 한다.[7]

개인용 방화벽은 조직의 보안 정책에서 허가된 종류의 통신만을 허가하고 나머지는 모두 차단하도록 설정되어야 한다. 많은 개인용 방화벽은 웹 서버와 통신하는 웹 브라우저나 이메일을 송수신하는 이메일 클라이언트 등을 비롯한 인증된 애플리케이션 목록에 의거하여 통신을 허가하고, 그 외 모든 애플리케이션과 관련된 통신은 차단하도록 설정할 수 있다.

개인용 방화벽의 유지 관리가 중앙에 집중되면 손쉽게 모든 사용자와 그룹을 대상으로 하는 보안 정책을 설정하고, 분배하고, 강제할 수 있다. 이렇게 하면 사용자가 조직의 컴퓨팅 자원에 접근하려고 할 때마다 항상 조직의 보안 정책이 적용된다. 그러나 개인용 방화벽의 유지 관리가 중앙 관리자 소관인지, 개별 사용자의 소관인지와는 무관하게, 모든 경고 메시지가 사용자에게 알려져야만 발견된 문제점을 쉽게 수정할 수 있다.

개인용 방화벽 장비

개인용 컴퓨터에 개인용 방화벽을 사용하는 것과 더불어, 일부 재택 근무자들은 방화벽 장비 혹은 방화벽 라우터라고 불리는 작고 저렴한 장비를 사용하여 가정 내 네트워크의 컴퓨터들을 보호하기도 한다. 개인용 방화벽 장비는 개인용 방화벽과 비슷한 기능을 구현하고, VPN 과 같이

[7] 개인용 방화벽에 대한 추가 정보는 NIST SP 800-114, *Securing External Devices for Telework and Remote Access* 사용자 가이드를 참조하라 (http://csrc.nist.gov/publications/nistpubs/).

이 문서의 앞에서 언급한 일부 고급 기능을 포함하기도 한다. 만약 가정 내 네트워크에 위치한 컴퓨터들이 각각의 개인용 방화벽을 사용하고 있다 하더라도, 방화벽 장비는 여전히 유용한 추가적 보안 계층으로 작동한다. 컴퓨터에서 작동하는 개인용 방화벽이 오작동하거나, 비활성화되거나, 잘못 설정되더라도 방화벽 장비는 여전히 외부로부터 유입되는 인증되지 않은 네트워크 연결로부터 컴퓨터를 보호한다.[8]

분산형 방화벽

분산형 방화벽 Distributed Firewalling 은 방화벽 배치 분야에서 급부상하고 있는 보안 기술로, 보안의 중심점을 네트워크 경계에서 각 네트워크 장비의 종점으로 이동시킨다. 이 기술은 방화벽을 모든 종점 혹은 기타 적절한 네트워크 장비의 앞이나 혹은 종점/네트워크 장비에 바로 배치하는 것으로 구현할 수 있다. 분산형 방화벽은 이론적으로 그간 네트워크 접속에서 전통적인 주요 취약점이었던 경계 방화벽이나 내부 방화벽의 부하를 줄일 수 있다. 분산형 방화벽 기술이 발전하면, 경계 방화벽이나 내부 방화벽의 필요성은 거의 사라질 것이다. 그러나, 현재 분산형 방화벽을 사용하고 있는 조직은 매우 적다.

분산형 방화벽은 각 장비에서 작동하는 방화벽과 보안 정책을 지시하는 중앙 정책 서버로 구성된다. 분산형 방화벽은 각 네트워크 장비에게 인증서를 발급하고, 여기에 설치된 호스트 기반 방화벽들을 중앙에서 관리한다는 개념을 확장시킨 것이다. 인증서는 어떤 장비가 어떤 자원에 접근할 권한을 가지고 있는지 식별하는 용도로 사용할 수 있다. 예를 들어, 내부 웹 서버에는 특정한 인증서를 보유한 워크스테이션만 접근을 허용하도록 하는 보안 정책이 적용될 수 있다.

이 개념은 워크스테이션(인트라넷 내•외부를 모두 포함)과 내부 자원 간의 접근 통제를 제공하며, 다수의 모바일 사용자로 구성된 환경에서도 네트워크의 규모를 쉽게 확장할 수 있다. 공격자가 주소를 변조하지 못하도록 하려면, 분산형 방화벽 시스템은 네트워크의 각 종점에 신원을 보장하는 인증 절차를 포함해야 한다. 그렇지 않을 경우, 공격자는 인증서에 접근할 수 있는 권한을 획득하고 허가 없이 네트워크 자원에 접근할 수 있게 된다.

특수 방화벽

[8] 개인 방화벽 장비에 대한 추가 정보는 NIST SP 800-114, *Securing External Devices for Telework and Remote Access* 사용자 가이드를 참조하라 (http://csrc.nist.gov/publications/nistpubs/).

방화벽이 PBX 시스템 (Private Branch eXchange, 사설 교환기) 같은 특수한 시스템에 내장되는 경우도 있다. 상태 기반 프로토콜 분석이나 애플리케이션 필터링 등의 기존 방화벽 기술을 XML 이나 이메일 등 특정한 프로토콜이나 기술에 적용하는 경우도 있다. 이러한 방화벽들은 흔히 해당 프로토콜이나 기술에 특화된 안티바이러스 기술과 침입 탐지 시스템(IDS) 기능과 같이 사용된다. 이러한 종류의 방화벽의 예는 아래와 같다.

PBX 방화벽

전통적으로, PBX 자원은 텍스트 터미널이나 제조사 전용의 유지 관리 콘솔로 관리되어 왔다. 그러나 최근에는 PBX 시스템이 소형화되고 모듈화되면서 PBX 노드 간 네트워킹 모듈과 네트워킹을 필요로 하는 관리 소프트웨어가 흔해지고 있다.

PBX 방화벽은 일반적으로 인터넷 방화벽과 비슷한 기능을 제공한다. 예를 들면, 조직 내에서 사용 중인 전화선에 대한 사용자별 보안 정책 적용 같은 것들 말이다. 방화벽은 전화 회선에 아래와 같은 정책을 적용할 수 있다:

1. 비상 전화(911 등)은 항상 허용
2. 걸려오는 모뎀 통신 차단
3. 거는 모뎀 통신 차단
4. 그 외 모든 트래픽 허용

패킷 필터링 방화벽과 유사하게, PBX 방화벽은 통화의 방향(걸려온 것인지 외부로 거는 것인지), 걸려 온 전화번호, 목적지 전화번호, 전화 종류 (긴급 전화 혹은 수신자 부담 1-800 등), 그리고 통화 시작 시간 등의 특성을 통해 통화를 필터링하는 방식으로 동작한다. 관리자는 이러한 정보들을 로그로 저장하거나, 특정한 종류의 통화를 차단하거나, 사전에 지정된 통화 규칙 위반이 발생했을 때 실시간 경보를 발령하도록 설정할 수 있다.

방화벽으로 PBX 자원에 대한 접근을 통제하는 경우 감사 추적 로그가 기록된다. PBX 와 방화벽 모두 관리 세션을 로그로 저장한다.

XML 방화벽

일명 XML 게이트웨이로 알려진 XML 방화벽은 XML 에 포함된 모든 내용을 검사할 목적으로 설계되었다. 이 방화벽은 대개 웹 서비스를 제공하는 서버 앞에 위치하며, 일반적으로 SOAP 헤더와 XML 메시지 본문을 검사하여 트래픽 허용 여부를 결정한다. 이 방화벽은 인증, 접근 통제,

암호화, 서명 검증, 로깅, 경고, 변조된 메시지나 기타 의심스러운 컨텐츠 탐지 등을 수행할 수 있다.[9]

이메일 방화벽

많은 제조사들은 이메일 서비스를 보호할 목적으로 특별히 고안된 방화벽을 제공한다. 이 장비들은 수신되는 이메일을 검사하여 이메일에 포함되어 있을 수 있는 맬웨어를 탐지하고, 본문을 검사하여 스팸이나 피싱 공격의 징후를 찾도록 설계되었다. 이 방화벽은 동시에 알려진 스팸 사이트에서의 트래픽을 차단하고, 비정상적으로 큰 트래픽 볼륨 등 비정상적인 이메일 패턴을 추적한다. 부가적으로, 이메일 방화벽이 발신 메시지에 대한 추가적인 통제 기능을 제공할 수도 있다. 예를 들면, 이메일을 스캔하여 조직의 정책에 반하는 내용이 포함되어 있는지 판단할 수 있다. 이러한 방화벽들은 암호화나 향상된 로깅 등 추가 보안 기능을 제공할 수도 있다.[10]

방화벽과 네트워크 구조

방화벽은 인터넷과 민감한 정보를 담은 서버가 운용되는 내부 네트워크 등 서로 다른 보안 요구조건을 가진 네트워크를 구분하는데 사용된다. 조직은 내부 네트워크나 시스템이 외부 네트워크나 시스템과 상호작용하는 곳이면 어디든지, 그리고 내부 네트워크 간의 보안 요구조건이 상이한 곳이라면 방화벽을 운용해야 한다. 이 절은 조직이 방화벽 배치 위치를 결정하고 방화벽과 관련된 다른 네트워크와 시스템이 어디에 배치되어야 하는지 결정하는데 도움을 주기 위하여 작성되었다.

방화벽의 주 기능 중 하나가 네트워크로 유입되는 (경우에 따라서는 안에서 밖으로 향하는) 원하지 않는 트래픽을 차단하는 것이기 때문에, 방화벽은 물리적인 네트워크의 경계에 배치되어야 한다. 이것은 일반적으로 방화벽이 네트워크가 여러 경로로 분배되는 분배점이나, 단일 경로 네트워크인 경우에는 인라인으로 설치된다는 것을 의미한다. 라우팅되는 네트워크의 경우, 보통 방화벽은 라우터로 유입되기 직전에 (경우에 따라 라우터와 같은 단에) 위치한다.

---

[9] XML 과 XML 방화벽에 대한 추가 정보는 NIST SP 800-95, *Secure Web Services* 가이드를 참조하라 (http://csrc.nist.gov/publications/nistpubs/).

[10] 이메일 보안에 대한 추가 정보는 NIST SP 800-45 Version 2, *Electronic Mail Security* 가이드라인을 참조하라 (http://csrc.nist.gov/publications/nistpubs/).

방화벽을 라우터 뒤에 배치하게 되면 감시할 경로가 늘어나게 되므로, 이런 식으로 방화벽을 배치하는 경우는 거의 없다. 하드웨어 방화벽 장비 중 대다수는 라우터 기능을 가지고 있고, 스위치 네트워크에서 방화벽은 종종 스위치 그 자체의 일부로서 가능한 한 많은 네트워크 세그먼트를 보호한다.

방화벽은 검사되지 않은 트래픽을 받아들이고, 방화벽의 정책에 부합하는가를 확인한 후, 결과에 따라 동작을 취한다. (즉, 트래픽을 통과시키거나, 차단하거나, 약간의 수정을 거쳐 통과시키는 등의 동작을 취한다.) 네트워크의 모든 트래픽이 목적지를 가지고 있기 때문에, 정책은 트래픽의 목적지에 기반하여 수립된다. 이 문서에서는 아직 확인되지 않은 트래픽이 방화벽의 "보호되지 않는 쪽"으로 유입되어 "보호되는 쪽"으로 향한다고 가정한다. 일부 방화벽은 양쪽 모두의 트래픽을 확인한다. 예를 들어, 조직의 내부 망에서 인터넷으로 나가는 특정한 트래픽을 막을 용도로 방화벽이 설정된 경우를 들 수 있다. 이러한 경우, "보호되고 있는 쪽"은 외부 네트워크를 접하고 있는 쪽을 의미한다.

2 부에서는 다양한 종류의 방화벽을 다룬다. 네트워크 방화벽은 대부분 다수의 NIC 가 장착된 하드웨어 장치이다. 호스트 기반 방화벽과 개인 방화벽은 단일 컴퓨터에서 구동되는 소프트웨어로 구성되어 있다. 개인용 방화벽 장비는 단일 PC 나 소규모의 사무실/재택 사무실 네트워크를 보호할 목적으로 설계되었다. 다른 종류의 방화벽에는 네트워크 토폴로지 이슈가 없으므로 이 절에서는 네트워크 방화벽에 집중한다.

방화벽이 적용된 네트워크 배치

그림 4 는 라우터로 작동하는 하드웨어 방화벽 장비가 설치된 일반적인 네트워크 배치의 예이다. 방화벽으로 보호되지 않은 쪽은 "WAN"이라 명명된 단일 경로에 접속되고, 보호되고 있는 쪽은 "LAN1", "LAN2", "LAN3" 로 명명된 3 개의 경로에 접속된다. 이 방화벽은 WAN 과 LAN 경로 사이에서 라우터 역할을 한다.

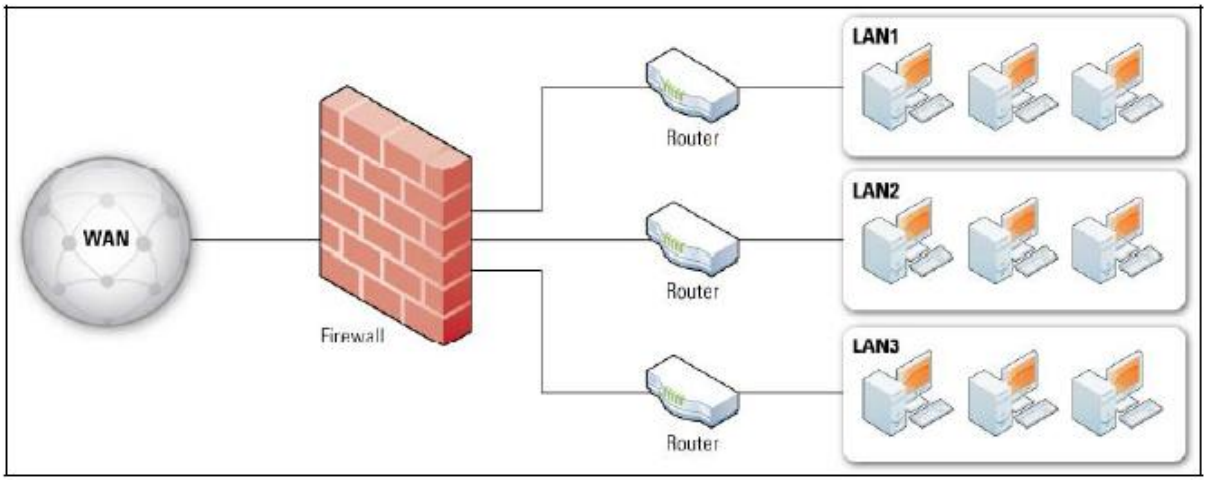

그림 4 방화벽 장비가 설치된 간단한 라우팅 네트워크

많은 하드웨어 방화벽 장비는 DMZ 라 불리는 기능을 가지고 있는데, DMZ 는 비무장지대의 약자로, 전쟁 중인 국가 사이에 선언되는 지대를 의미한다. 방화벽 DMZ 에 대한 유일한 기술적 정의가 존재하지는 않지만, DMZ 는 대개 라우팅 방화벽의 인터페이스로, 방화벽에서 보호되고 있는 쪽의 인터페이스와 유사하다. 가장 큰 차이점은 DMZ 와 보호되고 있는 쪽에 위치한 다른 인터페이스 간에 오고 가는 트래픽도 역시 방화벽을 지나기 때문에, 방화벽 정책이 적용될 수 있다는 점이다.

그림 5 는 이런 경우의 예로, DMZ 가 존재하는 방화벽이 적용된 단순한 네트워크이다. 인터넷에서 들어온 트래픽은 방화벽으로 향하며, 이 트래픽은 방화벽으로 보호되고 있는 쪽 혹은 DMZ 에 위치한 시스템들로 라우팅된다. DMZ 의 시스템들과 보호되고 있는 쪽의 시스템들은 방화벽을 지나며, 선택적으로 방화벽 정책이 적용될 수 있다.

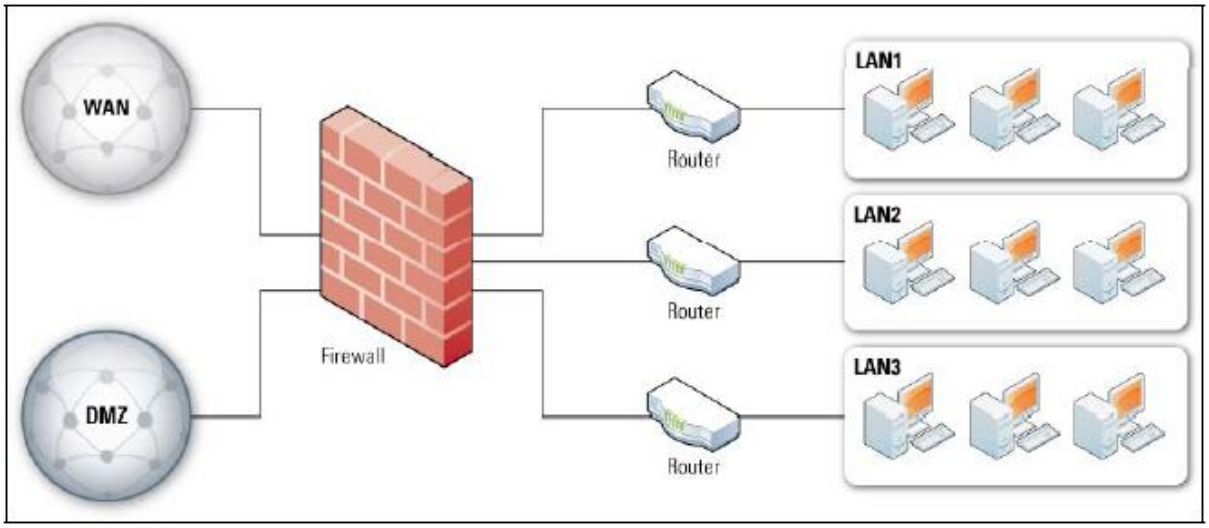

그림 5 DMZ 가 적용된 방화벽

대부분의 네트워크 구조는 계층적인데, 이는 외부에서 유입되는 단일 경로가 내부 네트워크로 들어가면서 다수의 경로로 나누어진다는 것을 의미한다. 그리고 대개 경로가 나누어지는 곳에 방화벽을 배치하는 것이 가장 효과적이다. 이는 방화벽을 "외부"인지 "내부"인지 고민할 필요가 없는 곳에 배치할 수 있다는 장점이 있다. 그러나, 내부의 컴퓨터들을 다른 컴퓨터들로부터 보호하려는 경우처럼 추가로 내부 방화벽을 보유해야 할 때도 있을 수 있다.

만약 어떤 네트워크의 구조가 계층적이지 않다면, 모든 네트워크의 입구에 동일한 방화벽 정책이 적용되어야 한다. 대부분은 네트워크로 유입되는 경로가 하나뿐이지만, 전체 정책에서 허용하지 않는 방법으로 임시 네트워크 ad-hoc network 유입 경로를 만드는 경우가 있다. 이 때 적절하게 설정된 방화벽이 입구에 배치되지 않은 상태라면, 주 유입 경로에서 차단되는 수상한 트래픽이 다른 경로를 통하여 네트워크에 유입될 수 있다.

그림 6 의 네트워크는 그림 4 의 네트워크와 유사하지만, 한 사용자가 LAN2 에 허락 없이 연결을 추가하였다는 점이 다르다. 이것이 우연히 이웃에서 운영하고 있는 무선 망에 연결된 경우일 수도 있고, 방화벽의 특정 정책을 회피하려고 의도적으로 추가한 연결일 수도 있다. 이유가 어찌 되었든, 이 연결 때문에 방화벽을 통하지 않고도 네트워크를 가로질러 LAN1, LAN2, LAN3 에 접근하는 것이 가능해졌다.

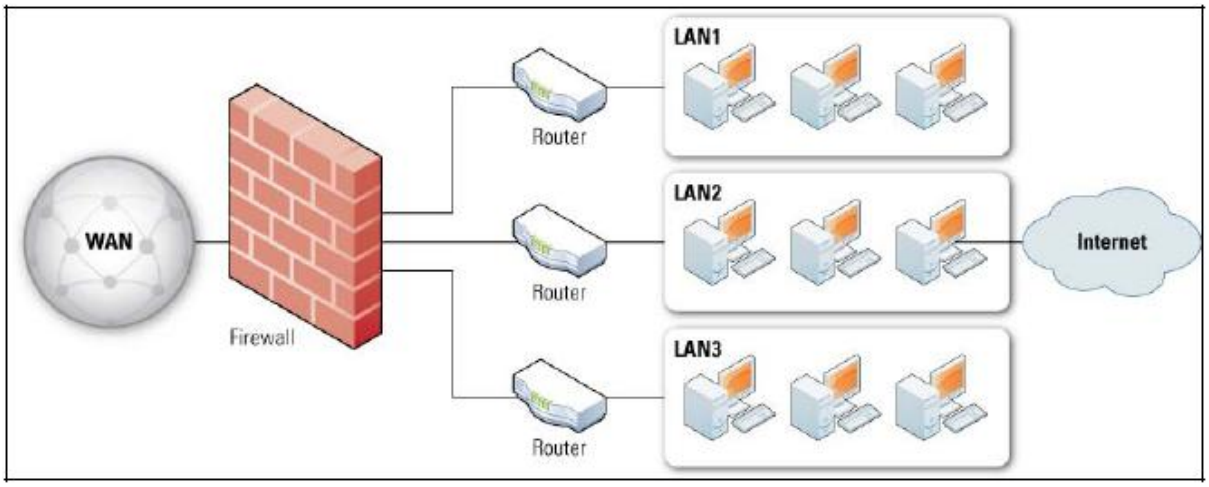

그림 6 외부로 통하는 제 2 의 연결이 추가된 네트워크

다수의 방화벽 계층이 적용된 구조

방화벽은 네트워크 어디에나 배치될 수 있다. 일반적으로는 방화벽이 물리적인 네트워크 경계에 위치하고, 그럼으로써 방화벽의 양쪽에 "안쪽"과 "바깥쪽" 이라는 개념을 생성하지만, 네트워크 관리자가 네트워크 내부에 추가적인 경계를 구축할 수도 있다. 다수의 방화벽 계층을 이용하여 종심 방어 defense-in-depth 를 구축하는 것은 꽤 흔한 일이다. 이미 앞에서 호스트 기반 방화벽이 설치된 호스트 바로 앞에 경계를 만들고 네트워크 구조에 추가적인 방화벽 정책 집합을 추가하는 예를 다룬 적이 있다. 다수의 네트워크 방화벽 계층을 사용하는 것 역시 흔한 기법이다.

다수의 네트워크 방화벽 계층을 필요로 하는 일반적인 상황은 내부 사용자마다 보안 등급이 서로 다른 경우이다. 예를 들어, 조직에서는 회계 부서와 관련이 없는 사용자가 회계 관련 데이터베이스를 열람할 수 없도록 보호하고 싶을 것이다. 이는 인터넷으로부터의 일반적인 접근을 막기 위한 방화벽을 네트워크 경계에 배치하고, 추가적인 방화벽을 회계 부서 네트워크의 경계에 배치하는 방법으로 구현할 수 있다. 내부 방화벽은 회계 부서 네트워크 내부가 아닌 다른 사용자의 회계 데이터베이스 서버 접근을 모두 차단할 수 있다. 그러면서 회계 부서 네트워크의 다른 자원에 제한적인 접근을 허용하는 것도 가능하다.

네트워크 내부에서 방화벽을 운용하는 또 다른 일반적인 상황은 조직 소속이 아닌 방문자의 인터넷 접속이 필요한 경우이다. 많은 조직들은 네트워크 내부에 무선 AP 를 운용하면서 인터넷 접속을 방문자에게 제공하고 있다. 각 AP 와 내부 네트워크 사이에 위치한 방화벽은 방문자가 조직 구성원과 똑같은 권한으로 로컬 네트워크에 접근할 수 없도록 차단한다.

이미 경계 방화벽이 배치된 네트워크에 추가적으로 방화벽을 배치하는 과정에서 발생할 수 있는 보안 오류를 방지하려면 철저한 계획 수립과 정책 협조가 필요하다. 내부 방화벽 정책을 설계할 때, 관리자는 잘못된 정책 선정으로 인해 초래될 수 있는 결과를 생각해 봐야 한다. 예를 들어, 내부 방화벽 관리자가 외부 방화벽이 이미 특정 트래픽의 내부 방화벽 도달 시도를 차단하고 있다고 가정하고 별다른 조치를 하지 않은 상황에서, 후에 외부 방화벽 관리자가 관련 정책을 수정하게 될 경우, 내부 방화벽 뒤에 있는 호스트들은 추가적인 위협에 그대로 노출되어 버릴 수 있다. 이러한 사태를 방지하려면 개별 내부 방화벽 정책에, 외부 방화벽 정책 중 내부 방화벽과 관련이 있는 부분을 그대로 복제하여 적용하면 된다. 만약 방화벽들이 자동적으로 정책을 동기화 시킬 수 없을 경우 이러한 작업은 매우 어려워지는데, 특히 방화벽이 동일한 제조사에서 제조된 것이 아닌 경우 이런 상황이 흔하게 발생한다.

다수의 네트워크 방화벽 계층을 사용할 때 흔히 발생하는 또 다른 문제는 방화벽 문제를 추적하기 더 어려워진다는 점이다. 사용자와 서버 사이에 단 하나의 방화벽만 설치된 상황에서 사용자가 서버에 접속할 수 없다면, 해당 방화벽의 로그를 점검하여 접속 허용 여부만 확인하면 사태가 쉽게 해결된다. 그러나 다수의 방화벽이 연관되어 있을 경우, 관리자는 모든 방화벽의 로그를 순서대로 확인하면서 어느 방화벽에서 문제가 시작되었는지 확인해야 하기 때문에 이 작업은 더 복잡해진다. 다수의 애플리케이션 계층 게이트웨이(Application Layer Gateways, ALG)가 설치된 경우에는 더 골치 아파지는데, 각각의 ALG 가 메시지를 변경하면서 디버깅을 더욱 더 어렵게 만들기 때문이다.

방화벽 정책

방화벽 정책은 방화벽이 조직의 정보 보안 정책에 기반하여 특정 IP 주소, IP 주소 범위, 프로토콜, 애플리케이션, 컨텐츠 종류(예를 들면, 액티브 컨텐트)에 해당하는 네트워크 트래픽을 어떻게 다루어야 하는지 명시한다. 방화벽 정책이 수립되기 전에, 조직에서 필요로 하는 트래픽 종류를 목록으로 만들고 어떻게 보호되어야 하는가 분류를 나누고, 어떠한 종류의 트래픽이 어떤 조건에서 방화벽을 통과할 수 있는지 설정하려면 위험 분석이 선행되어야 한다.[11] 위험 분석은

[11] 위험 평가를 수행하고 체크리스트를 만드는 과정에 대한 자세한 설명은 이 문서에서 언급하지 않는다. 더 알아보려면 NIST SP 800-30, *Risk Management Guide for Information Technology System* 과 SP 800-18 Revision 1, *Guide for Developing Security Plans for Federal Information Systems* 문서를 참조하라 (http://csrc.nist.gov/publications/nistpubs/).

위협, 취약점, 취약점 완화를 위한 대책, 시스템이나 데이터가 감염되었을 경우의 피해 등에 대한 평가를 기반으로 진행되어야 한다.

새로운 공격 방법이나 취약점이 계속 발생하고 조직에서 사용하는 네트워크 애플리케이션의 요구가 변할 수 있기 때문에, 방화벽 정책은 주기적으로 관리되고 갱신되어야 한다. 이 과정에서 방화벽 룰셋을 애플리케이션 매트릭스와 비교해 볼 수 있으므로, 좀 더 검증 가능하고 에러가 덜 발생하는 방화벽 룰셋 설정 절차가 될 수 있다. 그리고 룰셋 변경 사항을 어떻게 기록해야 하는가에 대한 자세한 지침도 정책에 포함해야 한다.

일반적으로, 방화벽은 방화벽 정책에 의해 명시적으로 허용되지 않은 모든 인바운드/아웃바운드 트래픽(조직에서 필요로 하지 않는 트래픽)을 차단해야 한다. "기본적으로 불허 deny by default" 라고 불리는 이 방식은 공격 위험을 감소시킬 뿐만 아니라 조직의 네트워크에 걸리는 트래픽 부하를 줄일 수 있다. 호스트, 네트워크, 프로토콜, 애플리케이션이 태생적으로 역동적이고 다양하기 때문에, "기본적으로 불허" 방식은 명시적으로 금지하지 않은 모든 트래픽을 통과시키는 방식에 비하여 훨씬 더 안전한 접근 방식이다.

본 절의 나머지 부분에서는 어떤 종류의 트래픽이 차단되어야 하는가에 대한 자세한 정보를 제공한다. 4.1 부는 IP 주소와 IP 특성에 기반한 패킷 필터링과 상태 기반 감시 정책을 다루며, 4.2 부에서는 애플리케이션 트래픽에 관련된 정책을 다룬다.

IP 주소와 프로토콜에 기반한 정책

방화벽 정책은 필요한 IP 프로토콜만 통과시키도록 해야 한다. 주로 사용되는 IP 프로토콜의 예로는 ICMP (1), TCP (6), UDP (17)가 있다. (괄호 안의 숫자는 IP 프로토콜에 할당된 번호이다.[12]) IPsec ESP Encapsulating Security Payload (50), AH Authentication Header (51), 라우팅 프로토콜 같은 다른 IP 프로토콜 역시 방화벽을 통과하도록 설정할 수 있다. 방화벽 정책은 프로토콜 사용을 원하는 조직 내의 특정 호스트와 네트워크만 허용하도록 최대한 구체적으로 설정되어야 한다. 필요한 프로토콜만 허용하고, 그 외 모든 불필요한 IP 프로토콜은 기본으로 차단한다.

IP 주소와 기타 IP 특성

[12] IP 프로토콜 번호 할당은 http://www.iana.org/assignments/protocol-numbers 에 정의되어 있다.

방화벽 정책은 적절한 출발지 및 목적지 IP 주소만 사용되도록 허가하여야 한다. IP 주소에 대해서는 아래 사항을 추천한다.

- 방화벽의 위치와 관계없이 올바르지 않은 출발지 주소나 목적지 주소를 가진 트래픽은 반드시 차단되어야 한다. 비교적 흔하게 사용되는 올바르지 않은 IPv4 주소는 127.0.0.1(로컬호스트 주소)와 0.0.0.0(일부 운영체제에서 로컬호스트나 브로드캐스트 주소로 인식)이다. 이 두 주소는 네트워크에서 일반적인 용도로 사용되는 주소가 아니다.
- 올바르지 않은 출발지 주소를 가진 인바운드 트래픽이나 올바르지 않은 목적지 주소를 가진 아웃바운드 트래픽("외부" 주소)은 네트워크 경계에서 차단되어야 한다. 이러한 트래픽은 보통 맬웨어, 변조, DoS 공격, 혹은 잘못 설정된 장비에 의해 유발된다. 올바르지 않은 외부 주소의 예 중 두 가지는 다음과 같다:
  - RFC 1918 에 정의된 범위 안에 있는 IPv4 주소. 이 주소 대역은 사설 네트워크용으로 할당되어 있다. 주소 범위는 10.0.0.0 부터 10.255.255.255 까지 (10.0.0.0/8), 172.16.0.0 부터 172.31.255.255 까지 (172.16.0.0/12), 192.168.0.0 부터 192.168.255.255 까지(192.168.0.0/16)다.
  - IANA Internet Assigined Numbers Authority 에서 제정한 할당 범위 안에 없는 주소.[13] 여러 단체에서 bogon 리스트(인터넷에서 유효하지 않은 주소 범위를 명시한 목록)를 배포[14] 하는데, 이를 이용하면 조직에서 올바르지 않은 IPv4 주소를 필터링하는데 도움이 된다. 훌륭한 단체에서 배포하는 Bogon 리스트는 IANA 에서 할당하는 IP 범위를 긴밀하게 모니터링하면서 만들어낸다. 이러한 리스트들을 기반으로 트래픽을 차단할 경우, 반드시 주 1 회 이상 리스트를 업데이트해야 한다. 업데이트에 소홀할 경우, 사용자가 새로 만들어진 합법적인 사이트에 접속하지 못하는 상황이 발생할 수 있다.
- 유입되는 트래픽 중 목적지 주소가 사설 주소이거나, 유출되는 트래픽 중 출발지 주소가 사설 주소인 경우("외부" 주소), 해당 트래픽은 네트워크 경계에서 차단되어야 한다. 네트워크 경계에 위치한 장비는 사설 주소를 가진 내부 호스트가 네트워크 경계를 통해

---

[13] IPv4 주소 범위 할당 목록은 http://www.iana.org/assignments/ipv4-address-space 에서, IPv6 할당 목록은 http://www.iana.org/assignments/ipv6-address-space 에서 확인할 수 있다.

[14] bogon 리스트를 받을 수 있는 곳 중 하나는 http://www.cymru.com/Bogons/index.html 이다. 이 사이트는 IP 주소 필터링에 대한 추가적인 정보도 포함하고 있다.

외부와 교류할 수 있도록 주소 번역 서비스를 수행할 수 있지만, 사설 주소가 네트워크 경계 밖으로 유출되어서는 안 된다.

- 목적지 주소가 방화벽인 유입 트래픽은, 방화벽 자체가 서비스를 제공하고 있지 않은 한 (가령 방화벽이 애플리케이션 프록시로 기능할 경우) 반드시 차단되어야 한다.

다음 종류의 트래픽도 네트워크 경계에서 차단해야 한다.

- IP 출발지 라우팅 정보를 포함한 트래픽. 이런 패킷이 노출되면 출발지로부터 목적지까지 라우팅되는 과정을 알아낼 수 있다. 이는 공격자로 하여금 네트워크 보안 통제를 우회하는 패킷을 구현하도록 허용할 가능성이 있다. IP 출발지 라우팅은 근래의 장비에서는 거의 사용되지 않는 기술이고, 인터넷에서 이를 사용하는 응용 프로그램을 찾기란 더욱 힘들다.
- 다이렉트된 브로드캐스트 주소(브로드캐스트 주소가 출발지와 다른 서브넷에 있을 때)를 포함한 트래픽. 어떤 시스템이든 다이렉트된 브로드캐스트에 대한 응답으로, 출발지 시스템 대신 출발지에서 지정한 시스템으로 답신을 보내게 된다. 이러한 패킷들은 DoS 공격을 목적으로 거대한 네트워크 트래픽 "폭풍"을 일으킬 때 사용될 수 있다.

네트워크 경계 방화벽은 외부 네트워크에서 접근이 허가되어서는 안 되는 네트워크나 호스트에 대한 모든 유입 트래픽을 차단하여야 한다. 이러한 방화벽은 조직의 네트워크와 호스트 중 외부 네트워크와의 접근이 허용되지 않은 네트워크와 호스트에서 외부로 향하는 모든 트래픽을 차단하여야 한다. 보통 방화벽 IP 정책 수립 과정에서 어느 주소가 차단되어야 하는지 결정하는 과정에 시간을 가장 많이 소모한다. 이는 또한 가장 오류가 발생할 가능성이 높은 부분인데, 원하지 않은 대상의 IP 주소가 시간이 지남에 따라 변화하기 때문이다.

IPV6

IPv6 는 IP 의 새 버전으로, 최근 급속하게 보급되고 있다. IPv6 의 내부 포맷과 주소의 길이가 IPv4 의 그것과는 매우 상이하지만 그 외 기능은 대부분 이전과 유사하며, 일부는 방화벽과 관련이 있다. IPv4 에서 IPv6 로 가면서 달라지지 않은 기능의 경우, 방화벽은 똑같이 작동해야 한다. 예를 들어, 방화벽에서 명시적으로 허용하지 않은 모든 유입, 유출 트래픽을 차단하도록 설정되어 있다면 해당 트래픽이 IPv4 인지 IPv6 인지 여부와는 관계없이 차단이 이루어져야 한다.

이 문서를 작성하고 있는 현재, 일부 방화벽 제품은 IPv6 트래픽을 전혀 처리하지 못한다. 일부 방화벽은 IPv6 패킷을 제한적인 방법으로만 필터링 할 수 있다. 다른 방화벽은 IPv6 트래픽도

IPv4 와 같은 수준이나 품질로 필터링 할 수 있다. 조직 내부로 IPv6 트래픽이 조금이라도 유입될 가능성이 있는 조직은 반드시 이러한 종류의 트래픽을 필터링 할 수 있는 방화벽을 필요로 한다. 이러한 방화벽들은 반드시 아래의 능력을 보유해야 한다.

- 방화벽은 IPv4 주소를 사용하는 모든 필터링 규칙에서 IPv6 주소를 사용할 수 있어야 한다.
- 관리 인터페이스는 관리의 편의를 위하여 IPv4 규칙을 IPv6 주소에 복제할 수 있도록 지원해야 한다.
- 만일 방화벽이 도메인 이름도 DNS 조회를 이용하여 필터링 할 수 있다면, IPv4 에서 사용하는 A 레코드와 같은 방식으로 AAAA(Ipv6 주소 레코드)를 사용해야 한다.
- 방화벽은 RFC 4890(방화벽에서의 ICMPv6 메시지 필터링 추천 사항)에 명시된 대로 ICMPv6 를 필터링 할 수 있어야 한다.
- 많은 사이트에서 IPv6 패킷을 IPv4 패킷에 터널링해서 전송한다. 이 방법은 특히 IPv6 를 시험적으로 적용하고 있는 사이트들에서 흔하게 사용되는데, ISP 로부터 네이티브 IPv6 변환기 transit 를 제공받는 것보다 v6-to-v4 터널을 이용하여 IPv6 주소를 변환하는 것이 훨씬 쉽기 때문이다. 이 과정을 수행하는 방식은 여러 가지가 존재하며 터널링 표준 역시 계속 증가하고 있다. 만약 방화벽이 IPv4 패킷의 컨텐츠를 검사할 수 있다면, 방화벽은 해당 조직에서 어떤 방식의 터널링 방식을 사용하더라도 터널링 된 트래픽을 검사할 수 있어야 한다. 그러므로 조직에서 IPv6 트래픽의 유입/유출을 차단할 목적으로 방화벽을 운용하고 있다면, 해당 방화벽은 모든 종류의 v6-to-v4 터널링을 인식하고 차단할 수 있어야 한다.

IPv6 사용을 허가하는 방화벽의 경우, 올바르지 않은 출발지나 목적지 IPv6 주소를 가진 트래픽은 언제나 차단되어야 한다. 이것은 올바르지 않은 IPv4 주소를 가진 트래픽을 차단하는 것과 유사하다. 지금까지 IPv6 주소보다 IPv4 주소에서 올바르지 않은 주소의 목록을 만드는 일에 더 많은 노력을 기울여 왔기 때문에, IPv6 용 차단 대상 주소 목록을 구하는 것이 어려울 수 있다. 게다가 IPv6 는 네트워크 관리자로 하여금 할당 받은 범위 안에서 다양한 방식으로 주소를 배정할 수 있게 해준다. 따라서 한 조직에 할당된 특정한 주소 범위 안에서 글자 그대로 수 조개의 유효하지 않은 IPv6 주소가 존재할 수 있고, 극히 소수만이 올바른 주소일 수 있다. 이런 이유 때문에, 유효하지 않은 IPv6 주소 목록은 IPv4 목록에 비하여 훨씬 더 세세한 목록이어야 한다. 이런 IPv6 목록을 사용하는 방화벽 규칙은 IPv4 목록을 사용하는 방화벽의 경우에 비해 효과가 적을 것이다.

TCP 와 UDP

TCP 와 UDP 는 응용 프로그램에서 사용된다. 응용 프로그램 서버는 일반적으로 고정된 TCP/UDP 포트를 사용한다. 반면 응용 클라이언트는 일반적으로 광범위한 포트 중 임의의 포트를 사용한다. 그리고 다른 경우와 마찬가지로, TCP/UDP 트래픽에도 "기본적으로 거부" 정책이 적용되어야 한다. 일반적으로 외부로 향하는 TCP/UDP 트래픽에는 덜 엄격한 정책이 사용되는데, 이는 대부분의 조직에서 사용자들이 수백만의 외부 호스트에 위치한 광범위한 외부 애플리케이션을 사용할 수 있도록 허가하기 때문이다.

애플리케이션 트래픽 매트릭스는 구체적으로 어떤 활동이 허용되고 차단되었는지 기록하는 데에 사용될 수 있다. 표 3 은 외부에서 DMZ 로 진입을 시도하는 트래픽 매트릭스의 일부를 보여준다. (즉, 외부 네트워크에서 외부 방화벽을 거치는 경우)

서비스[15]	출발지	목적지	허용 여부
HTTP	인터넷	공개 웹 서버	허용
HTTPS	인터넷	웹 메일용 웹 서버	허용
DNS	인터넷	외부 DNS 서버	허용
메일	인터넷	외부 메일 서버	허용
NTP	인터넷	NTP 서버	허용
VPN 터널	지점	VPN 서버	허용
기타 트래픽	모든 출발지	모든 목적지	거부

표 3 방화벽 애플리케이션 트래픽 룰셋 매트릭스

UDP 와 TCP 트래픽을 허용하고 차단하는 것과 더불어, 많은 방화벽은 보호되고 있는 호스트나 방화벽 자체를 향하는 변형된 UDP 와 TCP 트래픽을 보고하거나 차단할 수 있다. 이런 트래픽은 호스트를 스캔하는데 주로 사용되고, 특정한 종류의 공격에 사용될 수도 있다. 방화벽은 이러한 활동들을 막을 수 있다. 그렇지 않더라도 최소한 이러한 사태가 벌어질 때 관리자나 담당자에게 보고할 수 있다.

[15] 방화벽에 따라 서비스 제공에 구체적으로 필요한 내용은 달라질 수 있다. 예를 들면, 일부 방화벽은 일반적인 서비스(TCP 포트 80, HTTP)가 사용하는 기본 프로토콜과 포트를 설정해 둔다. 그 외의 방화벽은 관리자가 직접 포트의 종류(TCP, UDP)와 포트 번호(80)를 입력하도록 되어 있다.

ICMP

공격자들은 네트워크 트래픽의 흐름을 정찰하거나 조작하는 용도로 다양한 ICMP 타입과 코드를 사용할 수 있다.[16] 그러나 ICMP 는 인터넷에서 적정 수준의 성능을 얻으려고 하는 경우 등 많은 경우에 사용된다. 일부 방화벽 정책은 모든 ICMP 트래픽을 차단하는데, 이렇게 하면 네트워크 진단이나 성능에 문제가 발생하기 쉽다. 일반적인 정책은 모든 유출 ICMP 트래픽을 허용하고, 유입 ICMP 트래픽은 MTU 측정과 Ping 에 필요한 ICMP 타입과 코드만 허용되도록 제한하는 것이다.

수상한 활동을 방지하기 위하여, 네트워크 경계 방화벽은 조직에서 명시적으로 허용한 타입과 코드를 제외한 모든 유입, 유출 ICMP 트래픽을 차단해야 한다. IPv4 에서 ICMP 타입 3 메시지 (목적지 도달 불가 destination unreachable)는 네트워크 진단 용도로 사용되기 때문에 필터링 되어서는 안 된다. IPv6 ICMP 에서 다양한 IPv6 기능을 활성화하려면, 많은 종류의 메시지를 허용해야 한다. 특정한 종류의 방화벽에서 어떠한 종류의 ICMPv6 트래픽을 차단하거나 허용해야 하는가에 대한 추가 정보는 RFC 4890 (Recommendations for Filtering ICMPv6 Messages in Firewalls)을 참조하기 바란다.

IPSEC 프로토콜

ESP 와 AH 프로토콜은 IPsec VPN 에 사용된다. 이 프로토콜을 통과시키지 않으면 IPsec VPN 을 사용할 수 없게 된다. ESP 를 차단하면 민감한 정보를 암호화하는 것을 방해하게 되지만, 그 대신 방화벽(상태 기반 감시 방화벽이나 애플리케이션-계층 게이트웨이)이 패킷을 검사할 수 있게 된다. (일반적으로 암호화 된 패킷은 검사가 불가능하다.)

조직은 내부 네트워크의 특정 주소에서 출발하거나 특정 주소를 향하는 경우를 제외한 모든 ESP 와 AH 프로토콜을 차단해야 한다. 특정 주소는 IPsec 게이트웨이에 포함된 주소로서 VPN 종점 endpoint 으로 사용될 수 있도록 허가된 주소를 의미한다. 이러한 정책을 강제하면 조직 내부의 인원이 ESP 나 AH 프로토콜을 이용하려고 할 때 적절한 정책 승인을 획득해야만 해당 작업이 가능하도록 할 수 있다. 이는 동시에 네트워크 내부에서 검사할 수 없는 암호화된 트래픽의 양을 줄일 것이다.

---

[16] ICMP 종류와 코드 번호는 http://www.iana.org/assignments/icmp-parameters 에 정의되어 있다.

애플리케이션에 기반한 정책

초창기 방화벽의 역할은 대부분 네트워크 경계에서 원하지 않은 트래픽이나 수상한 트래픽을 단순히 차단하는 정도였다. 인바운드 애플리케이션 프록시는 다른 방식을 취하고 있다. 네트워크 내의 특정한 서버로 향하는 트래픽의 경로 중간에, 포트 기반 방화벽처럼 트래픽을 감시하는 서버가 개입한다. 이 애플리케이션 프록시 접근 방식은 목표 서버로 트래픽이 도달하기 전에 트래픽의 일부를 검증하기 때문에 유입 트래픽을 대상으로 추가적인 보안 계층을 제공한다. 이론적으로 인바운드 애플리케이션 프록시의 추가적 보안 계층은 서버가 스스로를 보호하는 것보다 더 나은 보안을 제공할 수 있다. 게다가 의심스러운 트래픽은 서버에 도달하기 전에 제거하므로 서버의 부하를 줄일 수 있다. 애플리케이션 프록시는 서버보다 더 강력한 필터링 능력을 보유하고 있기 때문에, 서버에서 처리할 수 없는 트래픽을 제거할 수 있다. 그리고 애플리케이션 프록시는 서버가 외부 네트워크에 직접 노출되는 것을 막는다.

가능하다면 인바운드 애플리케이션 프록시는 애플리케이션 특정 공격에서 스스로를 보호할 충분한 보안 능력을 보유하고 있지 않은 모든 서버 앞에 설치되어야 한다. 인바운드 애플리케이션 프록시의 사용 여부를 결정하는데 주로 고려해야 할 사항은 다음과 같다:

- 적당한 애플리케이션 프록시를 사용할 수 있는가?
- 해당 서버가 기존 방화벽에 의해 이미 충분히 보호되고 있는가?
- 주 서버가 애플리케이션 프록시만큼 효과적으로 의심스러운 컨텐츠를 제거할 수 있는가?
- 프록시로 인한 지연 시간 latency 이 애플리케이션 사용에 문제를 일으키지 않을 정도인가?
- 신규 위협에 대응할 때 주 서버와 애플리케이션 프록시의 필터링 규칙을 업데이트 하는 것이 얼마나 간단한가?

애플리케이션 프록시가 서버에 비하여 확실히 견고하고 업데이트된 상태로 유지하기가 간편하지 않은 한, 보통 애플리케이션 서버만 단독으로 운영하는 것이 최선이다. 그러나 서버의 자원도 고려할 필요가 있다. 만약 서버가 공격을 방어하는데 충분한 자원을 보유하고 있지 않다면, 프록시를 일종의 방패로 사용할 수 있다.

인바운드 애플리케이션 프록시가 방화벽이나 방화벽의 DMZ 뒤에 있는 경우, 방화벽은 애플리케이션 프록시에 걸리는 부하를 줄일 수 있도록 IP 주소 기반으로 트래픽을 선별하고 차단하여야 한다. 이러한 작업은 더 많은 주소별 정책을 한 장소(주 방화벽)에 적용하게 되고, 애플리케이션 프록시에 유입되는 트래픽의 양을 감소시켜 필터링에 필요한 자원 확보에 도움을 준다.

아웃바운드 애플리케이션 프록시는 보호된 내부 네트워크에서 외부로 향하는 부적절하거나 위험한 연결을 시도하는 시스템을 탐지할 때 유용하다. 가장 흔한 종류의 아웃바운드 프록시는 단연 HTTP 이다. 아웃바운드 HTTP 프록시는 조직으로 하여금 위험한 컨텐트가 해당 컨텐트를 요청한 PC 에 도달하기 이전에 필터링 할 수 있도록 한다. HTTP 프록시는 특정 웹 페이지가 사용자에게 필터링 대상인 내용을 전송하는 경우 경고할 수 있다. HTTP 프록시에서 보안을 제외한 가장 큰 장점은 웹 페이지를 캐싱하여 속도를 향상시키고 대역폭 사용을 줄일 수 있다는 것이다. 대부분의 조직은 HTTP 프록시를 운영해야 한다.

방화벽 계획과 구축

이 절은 기업에서의 방화벽 계획과 구축에 초점을 맞춘다. 어떤 종류의 신기술 배치에도 대응할 수 있도록, 방화벽 계획과 구축은 단계적 접근 방식으로 기술되어야 한다. 명확하고 단계적인 계획과 구축 절차를 통해 성공적으로 방화벽 배치를 달성할 수 있다. 방화벽 배치 과정에서 단계적 접근 방식을 사용하면 예측하지 못한 이슈의 발생을 최소화하고, 잠재적인 취약점 발생을 최소화할 수 있다. 이 절은 방화벽 계획과 구축의 각 단계에 대해 자세히 언급한다. 각 단계는 다음과 같다:

1. **계획**. 방화벽 계획과 구축 단계의 첫 번째 과정으로, 방화벽을 선정하는 과정에서 고려되어야 할 모든 요구 조건을 명시한다.
2. **설정**. 다음 단계는 방화벽 플랫폼 환경 설정 과정의 모든 면을 다룬다. 이 절은 방화벽 규칙 설정은 물론 하드웨어 및 소프트웨어 설치에 관련된 내용도 포함한다.
3. **시험**. 다음 단계는 연구실이나 시험 환경에서 설계된 프로토타입을 구축하고 시험하는 것과 관련이 있다. 시스템 시험의 주 목적은 해당 솔루션의 기능성, 성능, 확장성, 보안 등을 평가하고 기존 구성 요소와의 상호 호환성 등 발생할 수 있는 문제점을 식별하는 것이다.
4. **배치**. 시험 운용이 완료되고 모든 문제점이 해결되면, 다음 단계는 방화벽을 실제로 기업에 배치하는 것에 초점을 맞춘다.
5. **관리**. 방화벽이 실제로 배치되고 나면, 방화벽은 구성요소 유지보수와 운용 과정의 문제점 해결 지원 등을 통해 생명주기 끝까지 관리된다. 이러한 생명주기는 솔루션에 추가 사항이나 중요한 변화 사항이 있을 때마다 반복된다.

계획

방화벽 선정과 구축을 위한 계획 단계는, 조직이 보안 정책을 강제하는데 방화벽이 필요하다고 결정한 이후에 시작될 수 있다. 이는 일반적으로 시스템 전반에 대한 위험 평가를 수반한다. 위험 평가는 (1) 위협 및 정보시스템의 취약점 식별, (2) 식별된 취약점으로 공격이 가해졌을 때 기밀성, 무결성, 혹은 조직의 자산이나 운용(임무, 기능, 이미지, 평판 등을 포함)에 가해질 가능성이 있는 잠재적 충격이나 피해 범위 명시, (3) 정보 시스템을 위한 보안 통제에 대한 식별 및 분석 등을 포함한다.[17]

방화벽 배치 계획 단계에서 사용되는 기본 원칙은 다음과 같다.

- **장치를 원래 용도에 맞게 사용할 것**. 방화벽은 방화벽용으로 설계되지 않은 장비로 구성되어서는 안 된다. 예를 들어, 라우터는 라우팅을 위하여 설계된 장비이므로, 복잡한 필터링 규칙을 사용하면 라우터의 프로세서에 과도한 부하를 가할 수 있다. 추가로, 방화벽이 방화벽 본연의 기능 외에 웹 서버, 이메일 서버 등 추가적인 서비스를 제공할 것으로 기대해서는 안 된다.
- **종심 방어를 구축할 것**. 종심 방어 defense-in-depth 라 함은 다단계 보안 계층을 생성한다는 의미이다. 이렇게 하면, 만약 한 보안 계층이 뚫리더라도 그 다음 순서의 계층이 공격에 대응하기 때문에, 위험을 더 잘 통제할 수 있다. 방화벽의 경우, 종심 방어는 조직 전반에 걸쳐 다수의 방화벽(네트워크 경계, 중요 정보를 다루는 내부 부서, 개별 컴퓨터 등)을 배치하는 방법으로 구현할 수 있다. 종심 방어가 제대로 효과를 발휘하려면 방화벽이 안티바이러스 및 침입 탐지 소프트웨어 등을 포괄하는 전반적인 보안 프로그램의 일부로 작동해야 한다.
- **내부 위협에 주의를 기울일 것**. 외부 위협에만 집중하다 보면, 네트워크를 내부의 위협에 무방비 상태로 노출하게 된다. 이러한 위협들은 꼭 내부자의 소행이 아니더라도, 맬웨어 등으로 내부 호스트가 외부 공격자에게 감염되면서 발생할 수 있다. 중요한 내부 시스템은 내부 방화벽이나 DMZ 환경 뒤에 배치되어야 한다.

방화벽을 구축할 때, "모든 규칙은 깨지라고 있는 것이다"는 말을 기억하기 바란다. 방화벽 구축자는 방화벽 구축 과정에서 위의 규칙들을 항상 염두에 두고 있어야겠지만, 각 네트워크와 조직마다 특유의 요구사항과 개성을 가지고 있으므로 이를 수용하면서 예외가 생길 수 있다.

---

[17] 위험 평가에 대한 추가 정보는 NIST SP 800-30, *Risk Management Guide for Information Technology Systems* 문서(http://csrc.nist.gov/publications/nistpubs/)를 참조하라.

방화벽 솔루션을 구매하고 구축할 때는 다음 사항을 고려하라.

- 보안 능력
  - 조직의 어떤 부분이 보호되어야 하는가? (경계, 내부 부서, 원격 사무소, 개별 호스트, 이동형 클라이언트, 기타 등등)
  - 어떤 종류의 방화벽이 필요로 하는 보호에 가장 최적인가? (패킷 필터링, 상태 기반 감시, 상태 기반 프로토콜 분석, 애플리케이션/회로 프록시 게이트웨이, 기타)
  - 방화벽이 추가로 제공해야 할 필요성이 있는 추가적인 보안 기능에는 무엇이 있는가? (침입 탐지 능력, VPN, 컨텐츠 필터링, 기타)
- 성능 (일반적으로 네트워크 방화벽에만 해당됨)
  - 방화벽이 현재 네트워크 트래픽 및 향후 예상되는 트래픽을 병목 현상 없이 원활하게 처리하기 위하여 충족되어야 하는 처리량, 최대 동시 접속 수, 초당 접속 수, 지연 시간은 얼마인가?
  - 가용성을 극대화하는 로드 밸런싱이나 장애 조치 기능이 필요한가?
  - 하드웨어 기반의 방화벽과 소프트웨어 기반의 방화벽 중 어느 쪽을 선호하는가?
- 통합
  - 방화벽이 조직의 네트워크에 적절하게 통합되려면 특정 하드웨어가 필요한가? (특정한 전원 용량, 특정한 네트워크 인터페이스 카드의 종류, 특정한 백업 장치 등)
  - 방화벽이 네트워크 내에서 보안이나 기타 서비스를 제공하는 다른 장비와 호환성을 가져야 하는가?
  - 방화벽 설치가 네트워크의 다른 영역에 변화를 초래하는가?
- 물리적 환경 (호스트 기반 방화벽이나 개인 방화벽 적용 과정의 중앙 집중화된 구성 요소에 적용될 수도 있으나, 일반적으로 네트워크 방화벽에 해당됨)
  - 물리적 보안과 재난에서 보호하려면 방화벽은 물리적으로 어디에 배치되어야 하는가?
  - 방화벽이 설치될 곳에 적당한 선반이나 랙 rack 공간이 있는가?
  - 추가적으로 전원, 백업 전원, 공조 장치, 네트워크 연결 등이 해당 물리적 공간에 필요한가?
- 인사
  - 방화벽 관리의 책임은 누가 맡을 것인가?
  - 방화벽이 배치되기 전에 시스템 관리자들이 훈련을 받아야 하는가?
- 미래의 요구 사항

- 방화벽이 조직의 차후 요구 사항을 충족시킬 수 있는가? (IPv6 로의 전환, 필요한 대역폭 증가 예측, 미래에 시행될 것으로 예상되는 법적 규제 등)?

호스트 기반 및 개인 방화벽을 구매하고 구축할 때 고려해야 하는 사항들은 다음과 같다.

- 워크스테이션이나 서버가 방화벽 평가의 최소 시스템 사양을 만족하는가?
- 방화벽이 워크스테이션이나 서버에서 사용되고 있는 다른 보안 프로그램(백신 등)과 호환되는가?
- 방화벽이 중앙에서 관리가 가능하고, 조직의 보안 정책을 사용자에게 강제적으로 전달할 수 있는가?
- 방화벽이 보안 정책 위반 사항을 중앙 서버에 보고할 수 있는가?
- 관리자 외에는 아무도 방화벽 설정을 변경할 수 없도록 차단할 수 있는가?

설정

설정 단계는 방화벽 플랫폼 설정의 모든 면과 관련되어 있다. 여기에는 하드웨어와 소프트웨어의 설치, 룰셋 설정, 로깅과 경고 설정이 포함된다.

하드웨어 및 소프트웨어

일단 방화벽이 선정되고 구입되면, 소프트웨어 기반 방화벽의 경우에는 하드웨어, 운영체제, 방화벽 소프트웨어가 설치되어야 한다. 다음으로, 소프트웨어 기반 방화벽 및 하드웨어 기반 방화벽 모두 제조사에서 제공하는 패치와 업데이트를 시스템에 설치해야 한다. 이 단계를 통해 방화벽의 보안을 강화하여 취약점의 위험을 감소시키고, 비인가 접근으로부터 시스템을 보호해야 한다. 원격 접근에 필요한 콘솔 소프트웨어도 이 단계에서 설치되어야 한다.

네트워크 방화벽은 해당 제품의 권장 환경 필요 조건(온도, 습도, 전력 등)을 충족시키는 방에 설치되어야 하고, 장비 사이에 적절한 공간이 필요하다. 또한 이 방은 비 인가자의 방화벽 접근을 막을 수 있도록 물리적으로 보호되어야 한다.

룰셋 설정

하드웨어와 소프트웨어가 설치되고 보안이 확보된 이후, 관리자는 방화벽의 룰셋을 설정할 수 있다. 이 룰셋은 4 부에서 언급된 바와 같이 조직의 방화벽 정책을 포함하여야 하고, 방화벽이 통제하게 될 네트워크 트래픽을 고려하여 최대한 구체적으로 작성되어야 한다. 룰셋을

설정하려면 조직에서 허용된 애플리케이션을 사용할 때 어떤 종류의 트래픽이 필요한지 (프로토콜, 출발지 및 목적지 주소 등) 먼저 결정해야 한다. 여기에는 방화벽 자체가 필요로 하는 프로토콜도 포함되어야 한다. (DNS, SNMP, 로깅 등).

룰셋 설정의 세세한 부분은 방화벽의 유형과 상품별로 차이가 있다. 예를 들어, 많은 방화벽은 트래픽이 규칙을 어기는지를 판단할 때 일치하는 항목이 나올 때까지 순차적으로 비교한다. 이러한 방화벽의 경우, 성능 향상을 위해 높은 빈도로 나타나는 트래픽 패턴에 대한 룰을 리스트의 상단에 위치시켜야 한다. 다른 방화벽들은 룰셋을 처리하는 조금 더 복잡한 방법을 사용하는데, 여기에는 먼저 "거부" 규칙을 확인한 다음에 "허용" 규칙을 확인하는 방법 등이 있다. 관리자는 방화벽의 룰셋 설정 관련 문서를 참조하여 룰셋을 최적화하고, 비인가 트래픽이나 원하지 않는 트래픽을 허용하는 "허점"을 만들지 않도록 설정 오류에 주의해야 한다.

최소한 다음 규칙들이 정의되어야 한다.

- 포트 필터링은 네트워크의 외부 경계에 활성화되어야 하며, 경우에 따라 네트워크 내부에도 활성화될 필요가 있을 수 있다.
- 컨텐트 필터링은 가능한 한 컨텐트 수신자 가까이에서 처리되어야 한다.

룰셋 설정에 정답은 없다. 룰을 정의하는 방법은 다양하기 마련이다. 특정한 트래픽을 필요로 하는 모든 조직이나 개인은 룰셋 설정에 참여해야 한다.

로깅과 경고 설정

다음 단계는 로깅과 경고를 설정하는 것이다. 로깅은 실패를 방지하고 복구하는 과정에 필수적인 단계로서, 보안 설정이 제대로 되었는지 확인하는 것만큼이나 중요하다. 그리고 적절한 로깅은 이후 보안 사고에 대응하는데 필요한 아주 중요한 단서를 제공할 수도 있다. 방화벽 로그는 로컬에 저장하도록 설정되어야 한다 그리고 만약 가능하다면, 중앙 집중화된 로그 관리 시설에 로그를 전송하도록 한다.

방화벽에 중요한 이벤트가 발생했을 때, 관리자에게 알려줄 실시간 경고 역시 설정되어야 한다. 알림은 다음 내용을 포함할 수 있다:

- 방화벽 룰에 대한 모든 변경 사항이나 비활성화
- 시스템 재시작, 디스크 공간 부족 및 기타 운영 이벤트
- 가능한 경우, 보조적인 시스템 상태 변화

시험

신규 방화벽의 정상 작동 여부를 확인하려면 실제 배치 이전에 시험되고 평가되어야 한다. 시험은 실제 사용되는 네트워크에서 단절된 시험용 네트워크에서 완료해야 한다. 이 시험 네트워크는 방화벽을 통과할 가능성이 있는 네트워크 토폴로지와 네트워크 트래픽을 포함하여 최대한 실제 배치할 네트워크와 비슷하게 구성해야 한다. 평가 요소는 다음을 포함한다:

- **연결성**. 사용자는 방화벽을 통하여 연결을 수립하고 유지할 수 있다. 보안 정책에서 명시적으로 허용한 트래픽은 허용되어야 한다.
- **차단**. 보안 정책에 의해 허용되지 않은 다른 모든 트래픽은 차단되어야 한다.
- **애플리케이션 호환성**. 호스트 기반 방화벽이나 개인 방화벽 솔루션은 다른 소프트웨어 애플리케이션과 충돌하거나 간섭하지 않아야 한다. 애플리케이션 사용에는 애플리케이션 구성 요소 사이의 네트워크 통신도 포함된다.
- **관리**. 관리자가 방화벽 솔루션을 안전하고 효과적으로 설정하고 관리할 수 있어야 한다.
- **로깅**. 로깅과 데이터 관리는 조직의 정책과 전략에 일치해야 한다.
- **성능**. 솔루션은 일반 상황 및 최대 부하 상황에서 모두 충분한 성능을 제공해야 한다. 대부분의 경우에 견본 설치 상태에서 부하 상황 성능 테스트를 시행하는 가장 좋은 방법은 트래픽 생성기를 이용하여 예상되는 트래픽과 특성이 비슷한 트래픽을 테스트 네트워크에서 시뮬레이션 하는 것이다. 시험은 방화벽을 통과할 다양한 애플리케이션을 포함해야 하며, 특히 네트워크 처리량이나 지연 시간에 영향을 받을 가능성이 높은 애플리케이션들은 꼭 포함되어야 한다.
- **자체 보안**. 방화벽이 공격자들이 악용할 수 있는 취약점을 가지고 있을 수 있다. 높은 수준의 보안이 필요한 조직에서는 방화벽 구성요소에 대한 취약점 평가를 수행할 수도 있겠다.
- **구성 요소 상호 운용성**. 방화벽의 구성 요소들은 원활하게 함께 구동되어야 한다. 이는 다양한 제조사의 다양한 구성 요소가 함께 사용될 때 가장 주의해야 할 부분이다.
- **추가 기능**. 방화벽에서 향후 이용될 추가 기능 (VPN, 안티바이러스 기능 등)이 정상적으로 작동되는지 시험해야 한다.

배치

시험이 완료되고 모든 이슈가 해결되면, 방화벽 계획과 구축의 다음 단계는 배치이다. 방화벽 배치는 조직의 정책에 따라 진행되어야 한다. 방화벽을 배치하기 전에, 관리자는 방화벽 배치

계획에 의해 영향을 받을 가능성이 있는 시스템의 소유자나 사용자에게 미리 공지하고, 문제를 발견할 경우 누구에게 알려야 하는지 주지시켜야 한다. 기본 게이트웨이 변경 등 다른 장비에 변경이 필요한 경우, 이것 역시 방화벽 배치 계획의 일부로 통합해야 한다.

다수의 방화벽(개인 방화벽 혹은 여러 지사 사무실에 설치되는 경우 포함)이 배치되는 경우, 조직은 점진적이거나 단계적인 접근 방식을 고려해야 한다. 이는 관리자에게 방화벽 솔루션의 영향을 평가할 기회를 제공함은 물론, 전사적으로 방화벽을 배치하기 이전에 문제를 해결할 수 있는 기회도 제공한다.

관리

관리 단계는 방화벽 계획과 구축의 마지막 단계로 가장 오래 지속되는 단계이다. 그 이유는 방화벽 솔루션 관리에 방화벽 구조, 정책, 소프트웨어, 그 외 다른 구성 요소의 유지보수가 포함되기 때문이다.

일반적인 유지보수 작업의 한 예로는 패치를 시험하고 방화벽 장비에 적용하는 작업이 있다.[18] 정책 규칙은 새로운 애플리케이션이나 호스트가 네트워크에 추가된 경우처럼 요구 조건이 변경될 때마다 갱신되어야 할 필요가 있고, 변경된 규칙이 보안 정책을 위배하지 않는지 확인할 수 있도록 주기적으로 재검토 해야 한다. 구성 요소가 과부하에 시달리기 전에 미리 잠재적인 자원 이슈를 식별하고 대응할 수 있도록 방화벽 구성 요소의 성능을 모니터링 하는 것도 중요하다. 로그와 경고 역시 시스템에 가해진 위협(성공/실패 모두 포함)을 식별하려면 지속적으로 모니터링 해야 한다. 방화벽 규칙이 의도된 대로 작동하는지 주기적으로 시험하여 검증하는 것 역시 중요한 일이다.

방화벽 룰셋이나 네트워크 보안에 영향에 미치는 정책을 변화시켜야 할 경우 공식적인 절차에 따라 관리해야 한다. 많은 방화벽은 관리자 인터페이스의 일부로 변화 감시 기능을 가지고 있으나, 이는 정책 변화를 충실하게 추적하지 않는다. 최소한 모든 정책 결정과 룰셋 변화에 대한 로그가 기록되어야 한다. 그리고 이 로그는 어떤 방법으로든 방화벽과 연계되어 있어야 한다. 예를 들어, 로그는 물리적으로 연결된 장치에 저장되거나, 조직의 자산 관리 시스템에 방화벽 항목으로 보관될 수 있다.

---

[18] 패치 관리에 대한 추가 정보는 NIST SP 800-40 버전 2, *Creating a Patch and Vulnerability Management Program* (http://csrc.nist.gov/publications/nistpubs/)를 참조하라.

방화벽 룰셋은 시간이 지날수록 기하급수적으로 복잡해질 수 있다. 예를 들어, 새로 배치된 방화벽의 룰셋은 외부로 향하는 사용자 트래픽과 유입되는 이메일 트래픽 (TCP/IP 에 의해 요구된 리턴 인바운드 연결을 허용하는 것과 같이) 정책을 포함할 것이다. 하지만 방화벽이 배치된 지 1 년이 되었을 무렵에는, 훨씬 더 많은 규칙을 포함하고 있을 가능성이 높다. 일반적으로 새로운 사용자나 새로운 비즈니스 요구사항이 이러한 변화를 주도하지만, 조직 내의 다른 요소나 영향을 반영한 결과일 수도 있다. 네트워크 환경의 전반적인 보안 태세를 평가하는 침투 테스트의 시행도 생각해보기 바란다. 이 시험은 네트워크 트래픽을 생성하고, 해당 트래픽이 방화벽에서 어떻게 처리되는가를 예측되는 반응과 비교하는 방법으로 방화벽 룰셋이 의도대로 작동하는지 검사한다. 침투 테스트는 반드시 통상적 감사 프로그램과 함께 수행되어야 한다.[19]

일반 추천 사항

다음 추천 사항들은 관리자들이 방화벽 배치와 방화벽 정책 설정 계획을 수립하는 데에 도움이 될 것이다.

- 위치와 배치
  - 조직 내의 독립된 네트워크 경계마다 패킷 필터링 방화벽을 배치하라.
  - 하나 혹은 그 이상의 하위 네트워크가 경계 방화벽이 지원하지 못하는 특별한 보안 요구 조건을 가지는 경우, 해당 내부 노드에 방화벽을 배치해야 한다.
  - 네트워크의 두 지점 간에 기밀 트래픽 운용이 필요한 경우, VPN 기능을 탑재한 방화벽을 사용하라.
  - 경계에 가깝게 배치된 방화벽이 제공할 수 있는 보안 능력 이상의 보안을 요구하는 사용자 시스템이 있는 경우, 해당 시스템에 개인 방화벽을 배치하라.
- 방화벽 정책
  - 신뢰할 수 있는 조직 내부 네트워크 밖에서 사용될 가능성이 있는 모든 이동식 컴퓨터에 개인용 방화벽을 배치하라.
  - 방화벽 정책이 네트워크에 배치되기 전에, 각각의 방화벽 정책 발전 및 설정에 대해 계획을 먼저 수립하라.

---

[19] 침투 테스트에 대한 자세한 정보는 NIST SP 800-115 (Draft), *Technical Guide to Information Security Testing* (http://csrc.nist.gov/publications/nistpubs/) 문서를 참조하라.

- 네트워크의 모든 방화벽 정책을 통합하고, 조직의 보안 정책과 방화벽 정책이 일치하는지 확인할 수 있도록 모든 방화벽 정책을 대상으로 정기적인 재검토를 수행하라.
- 방화벽을 통과하는 모든 트래픽 중 적절한 출발지, 목적지 IP 주소를 가진 트래픽만 허용하라.
- 인증되지 않은 모든 TCP/UDP 포트를 차단하여 보호된 네트워크 외부에서 접근할 수 있는 애플리케이션의 종류를 제한하라.

■ ICMP 타입 3 메시지가 방화벽을 통과할 수 있도록 하라.

부록 A - 용어사전

이 문서에서 사용된 용어는 다음과 같이 정의된다.

애플리케이션-프록시 게이트웨이 방화벽: 상위 계층 기능과 하위 계층 접근 통제 기능을 통합한 개선된 기능의 방화벽이며, 서로 통신하기를 원하는 두 호스트 간에서 중개 역할을 하는 프록시 에이전트를 포함한다.

경계 라우터: 조직 네트워크와 신뢰할 수 없는 외부 네트워크 간의 경계에 위치하는 라우터. 이 문서에서 경계 라우터는 패킷 필터 방화벽으로 설정된다.

회로 수준 게이트웨이: 상태 기반 감시와 매우 유사한 방법으로 각각의 연결이 수립되기 전에 검증을 수행하는 프록시 서버의 종류.

전용 프록시 서버: 방화벽 기능이 탑재되지 않은 프록시 서버의 종류.

비무장지대 (DMZ): 방화벽으로 보호되고 있는 주 네트워크와 별개로 보호되고 있는 네트워크로 유도하는 라우팅 방화벽의 인터페이스. DMZ 를 향하는 트래픽은 여전히 방화벽을 통과하며, 방화벽의 보호 정책이 적용될 수 있다.

기본으로 거부: 방화벽 정책에 명시적으로 허용된 트래픽을 제외한 다른 모든 트래픽을 차단하는 정책

분산형 방화벽: 방화벽 기능을 네트워크 경계에서 장비 종점으로 이동하는 것으로, 네트워크 내의 모든 종점 및 기타 적절한 위치에 방화벽을 배치하는 것 등을 의미함

유출 필터링 Egress Filtering: 외부로 나가는 네트워크 트래픽에 대한 필터링.

방화벽: 서로 다른 보안 태세를 적용하는 네트워크나 호스트간의 네트워크 트래픽 흐름을 통제하는 장비나 프로그램

방화벽 플랫폼: 방화벽이 탑재되는 시스템을 의미. 예를 들어, 개인용 컴퓨터에서 구동되는 상용 운영체제 등이 있음.

호스트 기반 방화벽: 서버로 유입되거나 서버에서 외부로 나가는 네트워크 트래픽을 모니터링하고 통제하기 위하여 서버에 설치되는 소프트웨어 기반의 방화벽

유입 필터링 Ingress Filtering: 유입되는 네트워크 트래픽에 대한 필터링

인트라넷: 인터넷과 유사하게 서비스, 애플리케이션, 프로토콜 등을 운용하지만 외부 접속 가능성이 없는 네트워크. 인트라넷 외부에 정보가 공개될 우려 없이 조직 내에서 정보를 공유할 수 있게 함.

맬웨어: 시스템의 무결성, 기밀성을 해치거나 데이터, 애플리케이션, 운영체제, 혹은 서버에 위해를 가하기 위한 목적으로 시스템에 은밀하게 침투하는 프로그램.

네트워크 주소 변환 (NAT): 외부 네트워크에서 주소 스키마 addressing schema 를 이용하여 내부 시스템의 주소를 파악하지 못하도록 숨기는 데 사용됨

패킷 필터 방화벽: 호스트 주소와 연결 세션을 위한 접근 통제 기능을 포함한 라우팅 장치

개인용 방화벽: 유입되거나 나가는 트래픽을 모니터링하고 통제하기 위하여 데스크탑이나 랩탑 컴퓨터에 설치되는 소프트웨어 기반 방화벽

개인용 방화벽 장비: 가정용 네트워크에 포함된 일군의 컴퓨터를 위한 장비로, 개인용 방화벽과 유사하게 기능함

프록시 에이전트: 방화벽이나 전용 프록시 서버에서 구동되는 소프트웨어 애플리케이션으로, 프로토콜을 필터링하거나 장치의 인터페이스간에 전달하는 기능이 있음

룰셋: 방화벽의 접근 통제 기능을 제어하는 일련의 지시문 모음. 방화벽은 이 지시문들을 사용하여 패킷들이 방화벽의 인터페이스간에 어떻게 전달되어야 하는가를 결정함

상태 기반 감시 방화벽: 패킷을 필터링하고, 연결 상태를 추적하고, 예측되는 상태에서 어긋난 상태의 패킷들을 차단할 수 있는 기능이 있는 방화벽

상태 기반 프로토콜 분석 방화벽: 상태 기반 감시 방화벽의 일종으로, 네트워크, 전송, 애플리케이션 계층상의 프로토콜을 분석할 수 있는 감시 엔진을 포함한다.

부록 B - 두문자어와 약어

이 문서에서 사용된 두문자어와 약어를 정의한다.

AH	Authentication Header
ALG	Application Layer Gateways
CIDR	Classless Interdomain Routing
DMZ	Demilitarized Zone

DNS	Domain Name System
DoS	Denial of Service
ESP	Encapsulating Security Payload
FISMA	Federal Information Security Management Act
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
IDPS	Intrusion Detection and Prevention System
IDS	Intrusion Detection System
IGMP	Internet Group Management Protocol
IM	Instant Messaging
IP	Internet Protocol
IPsec	Internet Protocol Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISP	Internet Service Provider
IT	Information Technology
ITL	Information Technology Laboratory
LAN	Local Area Network
MAC	Media Access Control
MTU	Maximum Transmission Unit
NAT	Network Address Translation
NIC	Network Interface Card
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OMB	Office of Management and Budget
PBX	Private Branch Exchange
PC	Personal Computer
RADIUS	Remote Authentication Dial In User Service
RFC	Request for Comment
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SP	Special Publication
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol

TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
URL	Uniform Resource Locator
VPN	Virtual Private Network
VPNC	Virtual Private Network Consortium
WAN	Wide Area Network
XML	Extensible Markup Language

부록 C - 참고 문헌

유용한 자료들을 아래 첨부한다.

출판물

Allen, Julia H, The CERT Guide to System and Network Security Practices, Addison-Wesley, 2001

Chapman, Brent, et al, Building Internet Firewalls, 2nd Edition, O'Reilly Media, Inc., 2000.

Cheswick, William R., et al, Firewalls and Internet Security: Repelling the Wily Hacker, 2nd Edition, 2003.

Deal, Richard A, Cisco Router Firewall Security, Cisco Press, 2005.

Noonan, Wes and Dubrawsky, Ido, Firewall Fundamentals, Cisco Press, 2006.

Northcutt, Stephen, et al, Inside Network Perimeter Security, 2nd Edition, Sams, 2005.

Rash, Michael, Linux Firewalls: Attack Detection and Response with iptables, psad, and fwsnort, No Starch Press, 2007.

Shimonski, Robert J., et al, Building DMZs for Enterprise Networks, Syngress Publishing, Inc., 2003.

Shinder, Thomas, W., et al, The Best Damn Firewall Book Period, Second Edition, Syngress Publishing, Inc., 2007.

NIST 문서와 위치

제목	URL
NIST National Checklist Program	http://checklists.nist.gov/
NIST SP 800-18 Revision 1, Guide for Developing Security Plans for Federal Information Systems	http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf
NIST SP 800-30, Risk Management Guide for Information Technology Systems	http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
NIST SP 800-40 Version 2, Creating a Patch and Vulnerability Management Program	http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf
NIST SP 800-44 Version 2, Guidelines on Securing Public Web Servers	http://csrc.nist.gov/publications/nistpubs/800-44-ver2/SP800-44v2.pdf
NIST SP 800-45 Version 2, Guidelines on Electronic Mail Security	http://csrc.nist.gov/publications/nistpubs/800-45-version2/SP800-45v2.pdf
NIST SP 800-46, Security for Telecommuting and Broadband Communications	http://csrc.nist.gov/publications/nistpubs/800-46/sp800-46.pdf
NIST SP 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations	http://csrc.nist.gov/publications/nistpubs/800-52/SP800-52.pdf
NIST SP 800-61 Revision 1, Computer Security Incident Handling Guide	http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf
NIST SP 800-70, Security Configuration Checklists Program for IT Products – Guidance for Checklists Users and Developers	http://csrc.nist.gov/checklists/docs/SP_800-70_20050526.pdf

기타 기술 문서와 위치

제목	URL
Achieving Defense-in-Depth with Internal Firewalls	http://www.sans.org/reading_room/whitepapers/firewalls/797.php?portal=a4d358dbd051422110d917753a0ebb7c
An Introduction to Network Firewalls and the Firewall Selection Process	http://www.more.net/technical/netserv/tcpip/firewalls/
Best Practices for Managing Firewall Logs	http://www.zdnet.com.au/insight/print.htm?TYPE=story&AT=120265680-139023731t-110000100c
Comparison of Firewall, Intrusion Prevention, and Antivirus Technologies	http://www.juniper.net/solutions/literature/white_papers/200063.pdf
Defense in Depth: Foundations for Secure and	http://www.cert.org/archive/pdf/Defense_in_Depth09

Resilient IT Enterprises	2106.pdf
Firewall Evolution – Deep Packet Inspection	http://www.securityfocus.com/infocus/1716
Handbook of Firewall Architectures	http://www.securecomputing.com/pdf/SIDE--Ch-ExamFirewallTP.pdf
How do Circuit-Level Gateways and Application-Level Gateways Differ?	http://searchsecurity.techtarget.com/expert/KnowledgebaseAnswer/0,289625,sid14_gci1197999,00.html
IPv6 Transition Guidance	http://www.cio.gov/documents/IPv6_Transition_Guidance.doc
National Vulnerability Database	http://nvd.nist.gov/
The Perils of Deep Packet Inspection	http://www.securityfocus.com/infocus/1817
RFC Editor Homepage	http://www.rfc-editor.org/
Security Implications of IPv6	http://www.iss.net/documents/whitepapers/IPv6.pdf
Transparent, Bridging Firewall Devices	http://www.securityfocus.com/infocus/1737
Trusted Computing Group: Trusted Network Connect	https://www.trustedcomputinggroup.org/groups/network/
The Web Services Advisor: XML Firewalls	http://searchwebservices.techtarget.com/tip/1,289483,sid26_gci855052,00.html