글. 이선응 차장 / 김영준 과장 아이크래프트㈜ SNT본부 기술1팀

방송시스템의 보안강화 - 2

- Part 2. 방화벽과 VPN

연재 목차

지난 호에서 정보보안에 대한 다양한 분야를 살펴보았다. 이번 호에서는 네트워크보안 중 가장 기본이 되는 방화벽(Firewall)과 VPN(Virtual Private Network)에 대해 살펴보도록 하겠다.

우리가 일반적으로 알고 있는 방화벽은 [그림 1]과 같이, 건물과 건물 사이에 벽돌을 쌓아서 불이 옆 건물로 번지는 것을 막거나, 현대의 고층건물의 경우, 엘리베이터 옆 비상구에 설치된 방화 철문처럼 화재 시 고층에 있는 사람이 1층으로 대피할 때 사용하거나 계단실로 불이 번지는 것을 막아 안전을 확보하기 위한 용도로 사용된다.

그림 1. 건물 방화벽

방화벽의 용도가 불을 막거나 번지는 것을 차단하는 것이 주 용도인 것처럼 사이버공간에서의 방화벽은 불을 공격(Attack)으로 바꾸어 생각하면 된다. 즉 공격을 막거나 공격이 성공했더라도 다른 구역으로 공격이 확산되는 것을 막기 위한 용도가 주 목적이 되겠다.

계단실에 설치된 방화벽, 정확히는 방화 철문의 경우 평상시에는 사람의 통행이 가능하도록 되어 있으나, 화재가 발생한 경우 불이 철문을 통과할 수 없도록 동작하는 것처럼, 사이버공간에서의 방화벽도 사전에 정해진 규칙(보안정책)에 따라 트래픽을 통과시키거나 차단하는 동작을 수행하게 된다. 다음의 [그림 2]와 같이 보안정책으로 사전에 허용된 사용자만 내부 서버로의 접속을 허용하고, 허용되지 않은 사용자는 보안정책에 따라 접속을 차단하게 된다.

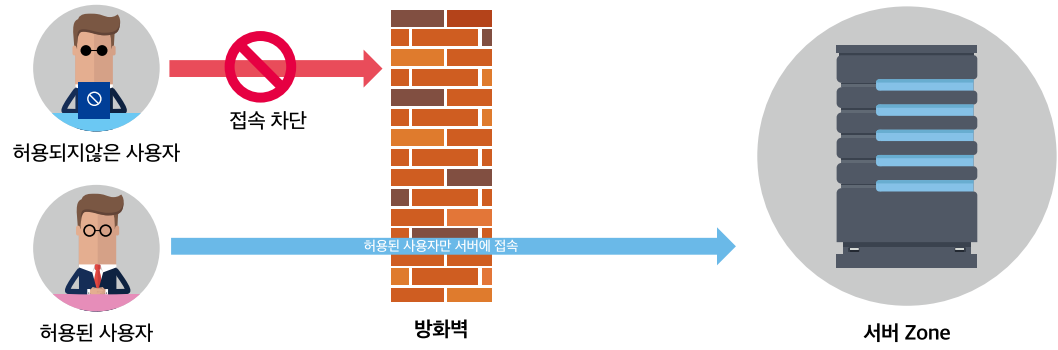

그림 2. 방화벽 동작방식

여기서 한가지 궁금한 점이 생긴다. 허용된 사용자만 접속이 되도록 보안정책이 설정되어 있는데 왜 해킹사고가 일어나는 것일까? 다양한 원인이 있겠지만 대략적인 유형은 아래와 같다.

1. 허용된 사용자의 PC를 해킹하여 접속하는 경우
2. 보안정책을 너무 느슨하게 설정하여, 아무나 접속이 가능한 경우
3. 보안정책을 잘 설정하였으나, 해커가 실력이 좋은 경우

1번의 경우 클라이언트보안에 문제가 있어 해커가 허용된 사용자의 PC를 원격으로 조정하여, 방화벽을 무력화시키는 사례로 이런 경우 PC 보안을 강화하는 방법밖에는 없다.
2번의 경우가 가장 빈번한 경우인데, 방화벽관리자가 보안정책을 설정할 경우, 정책을 세분화해서 정교하게 설정해야 하나, 현실적으로 방화벽만 신경 쓸 수 없다 보니, 방화벽관리에 소요되는 업무시간을 줄이기 위해 허용범위를 넓게 잡아 발생되는 경우이다. 이런 경우는 조직 규모에 따라 다르겠지만, 보안을 전담으로 관리하는 전문인력을 배치하고, 보안정책을 규정에 맞추어 깐깐하게 설정하여야 해결이 가능하다.
3번의 경우는 규정에 맞추어 보안정책을 설정하고, 관리전담인력을 배치한다고 하더라도, 전문화된 해커의 경우 사용하는 방화벽의 보안정책을 정찰활동을 통해 추측하고 분석하여, 침투 가능한 조건을 찾아 접속을 하는 경우이다. 발생빈도는 낮지만, 이런 경우 여러 대의 방화벽을 다중으로 설치하거나, 다계층 보안구조로 방어를 해야 침입을 차단할 수 있다.

지난 호에서 물리적 보안과 정보보안을 비교할 때 은행을 예로 들었었다. 은행강도가 돈을 훔치기 위해 통과해야 하는 셔터 출입문, 안쪽 유리 출입문뿐만 아니라 금고실의 출입문이나 쇠창살까지 모두 뚫어야 최종 목적인 돈에 접근할 수 있듯이 정보보안에서도 방화벽을 하나만 두는 것이 아니라, 2차, 3차의 방화벽을 설치하여 보안구조를 강화할 수 있다.

[그림 3]과 같이 외부에서 침투할 경우 인터넷을 통해 접근하게 되며 이때, 제일 먼저 만나게 되는 외부방화벽(1차 방화벽)을 설치하고 내부의 ERP, 그룹웨어, DB 서버 앞에 별도의 내부방화벽(2차방화벽)을 설치할 수 있다. 이 경우 외부에서 1차 방화벽을 통과하더라도 2차 방화벽까지 통과해야만 정보에 접근이 가능하므로, 한층 시간과 노력이 많이 필요하게 되고, 내부에 있는 사내 PC도 내부 방화벽을 통과해야 업무서버에 접근이 가능하므로, 사내 PC가 해킹으로 인해 정보유출 등의 보안사고로 이어지는 경우를 일정 부분 차단이 가능하다.

이선응 차장/김영준 과장
아이크래프트㈜ SNT본부 기술1팀

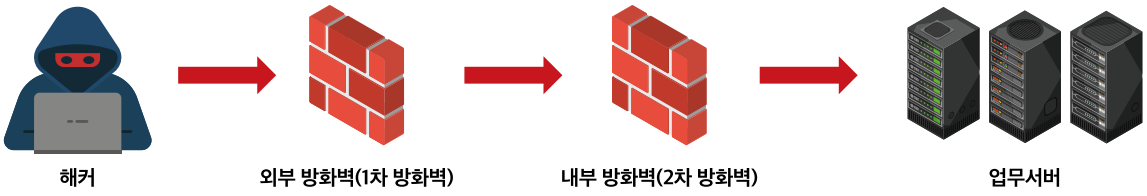

그림 3. 외부, 내부 방화벽

방화벽은 이렇게 내부와 외부를 구분하여 보안정책을 설정하게 되어 있다. 보통 외부는 비신뢰구역이라는 의미로 Untrust zone이라고 표시하고, 내부는 신뢰구역 즉, Trust zone으로 표시하여 구분한다. 방화벽이란 장비가 개발되어 사용되기 시작한 1990년대 중반부터 2010년 초반까지는 이런 구역 구분방식을 사용하더라도 문제가 없었지만 최근에는 이런 구분방식이 보안체계에 허점을 노출시키고 있다. 2010년 이전만 하더라도 휴대 가능한 기기 중 인터넷 등의 통신이 가능한 장비는 노트북이나 PDA, 초기형태의 스마트폰뿐이었으나, 최근에는 아이폰을 시작으로 안드로이드폰, 아이패드 등 고성능의 휴대기기로 페이스북 등의 SNS뿐만 아니라 메신저 서비스, 메일확인 전송, 인터넷검색이 가능한 환경이 되었다.

이런 기기가 개인적인 용도뿐만 아니라 회사업무에도 같이 활용되고 있고, 출근 후 사내 무선망에 연결되어 업무에 적용되는 경우가 많아지고 있다. 또한 인터넷을 통해 홈페이지에 방문하거나, 메일로 오는 첨부파일을 열어 보기만 해도 악성코드에 감염되어 해킹의 도구로 활용되는 경우가 빈번하게 발생되고 있어, 옛날과 같이 대부분의 침입이 외부에서 내부로 이루어지던 것이, 최근에는 공격 시작 위치가 내부에서 시작되는 경우가 대부분이 되었다. 이제는 내부구간인 Trust zone이 무한정 신뢰할 수 없는 구간이 된 것이다.

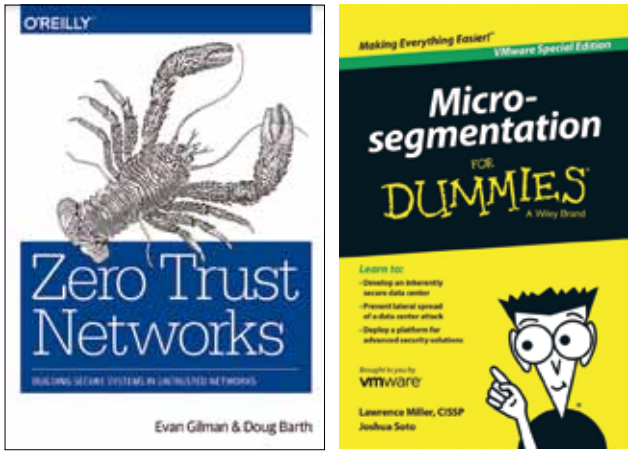

그림 4. Zero Trust Networks, Micro-segmentation 기술서적

최근에 이런 현상을 Zero Trust라고 표현하고 있다. 더 이상 안전하고 신뢰 가능한 공간은 존재하지 않으니, 여기에 맞추어 보안체계를 새롭게 설계해야 한다는 것이다. 이제 사내에 있는 PC라도 무한정 내부 시스템에 접근하는 것을 허용하지 않고, 모두 잠재적인 해커로 상정하고 내부에서 접근하더라도 다양한 보안시스템을 통해 감시하고 차단하며, 외부(인터넷)로 접속하더라도 무조건 허용하지 않고 사전에 지정한 서비스만 사용할 수 있도록 제한하는 보안설계철학이 권장되고 있다.

앞에서 설명한 1차, 2차 방화벽에서 좀 더 개념을 발전시켜 이제는 극단적으로 서버 1대에 방화벽을 1대씩 설치하여, 아무리 권한이 높은 회사 CEO나 전산 책임자라도 접근할 필요가 없는 서버에는 접근을 차단할 수 있도록 굉장히 세밀하게 접근을 제어하여 설계하는 방식을 Micro segmentation이라고 말한다. 즉, 아주 조밀하게 방화벽을 서버 사이사이에 배치하여, 허가되지 않은 사용자의 접근을 이중 삼중으로 막겠다는 보안설계철학이다.

또한, 최근 CPU 성능이 향상되면서 듀얼코어, 쿼드코어라는 용어를 많이 들어 보았을 것이다. 즉 독립적으로 동작가능한 코어(Core)라는 두뇌 역할의 칩을 물리적인 하나의 CPU에 2개, 4개 혹은 8개, 16개를 설치하여, 동시에 여러 가지 일을 시킬 수 있게

만들었다. “서버 가상화”라고 하여 하나의 CPU만 있으면 가상의 서버를 동시에 여러 개 동작시킬 수 있게 된 것이다. 과거에는 서버 한 대에 당연히 하나의 OS만 구동시킬 수 있었고, 윈도우서버, 리눅스서버 등으로 구분하여 사용하였다면, 최근에는 한 대의 서버에 윈도우서버와 리눅스서버를 혼용하여 동시에 10대씩 운영하는 것도 어렵지 않게 되었다.

뿐만 아니라, 방화벽도 물리적인 방화벽을 구매하는 것이 아니라, 방화벽 프로그램만 구매하여 서버에 설치하면, 동작시킬 수 있는 개념으로 발전하게 되었고, 가상서버 한 대 당 가상방화벽을 한 대 씩 설치하는 것도 더 이상 어려운 일이 아니게 되었다.

다음으로 VPN을 설명하도록 하겠다.

VPN은 Virtual Private Network의 약자로써 가상 사설망으로 번역할 수 있다. 즉 실제로는 존재하지 않는 사설망을 인터넷을 통해 가상으로 구성하여, 본사와 지점 간 혹은 출장, 재택근무자의 PC에서 본사 간 사설망을 구축하는 효과를 낼 수 있는 장비를 말한다.

우리가 일반적으로 말하는 인터넷은 누구나 이용 가능한 공용망이라고 할 수 있다. 이런 공용망은 쉽고, 빠르며 저렴하게 이용이 가능하다는 장점이 있는 반면, 악의적인 사용자가 나의 통신내용을 훔쳐보거나, 내용을 조작하여 보낼 수 있는 단점이 존재한다. 그에 비해 사설망을 사용할 경우는 반대로 우리 회사만 사용하는 전용망이기 때문에 보안은 강력한 반면에 비용이 많이 발생되고 가격에 비해 속도도 그리 빠르지 않는 문제가 있다. 2000년대 중반까지만 하더라도 규모가 있는 기업의 경우 본사와 지사 간 이런 사설망을 구성하여 많이 사용하고 있으며, 은행 같은 보안이 생명인 기업군의 경우에는 아직도 주 라인을 사설망으로 이용하고 보조라인으로 VPN을 많이 이용하고 있는 실정이다.

여기서 공용망의 장점만 살리면서 단점을 제거할 수 있는 방법이 없는지 장비제조사들은 고민하게 되었고, 그 결과물로 VPN이 개발되었다. 공용망인 인터넷을 이용하면서도 보안을 강화하기 위해 보내는 정보를 암호화하여 보내면, 중간에 내용을 가로채서 보더라도 원본 내용을 확인할 수 없도록 만들고, 받는 쪽에서는 암호화된 내용을 풀어서(복호화) 원본 내용을 확인할 수 있도록 만드는 것이다. [그림 5]와 같이 정보를 암호화하고 복호화해주는 VPN Router를 왼쪽의 본사와 오른쪽 지사 건물의 인터넷이 나가는 길목에 설치하고 두 장비 간 터널(Tunnel)이라는 가상의 통로를 만들어 정보를 주고받는 방식으로 동작한다.

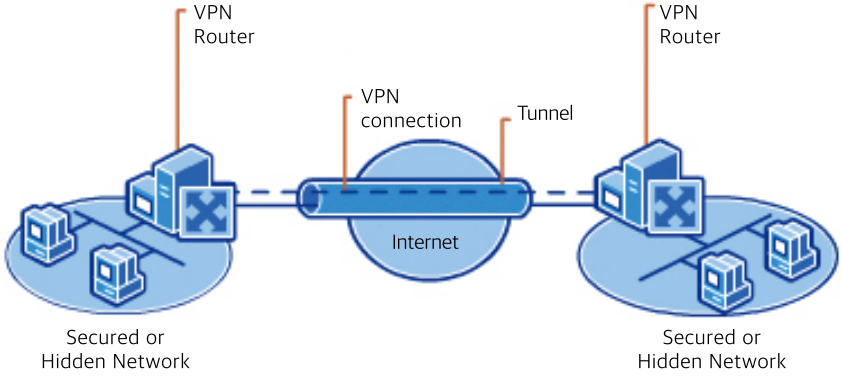

그림 5. VPN의 동작방식

앞에서 소개한 방화벽의 경우도 통상 인터넷이 나가는 길목에 위치하고, VPN도 같은 위치에 놓이기 때문에, 초창기에는 방화벽과 VPN이 각각 설치되었지만 이제는 방화벽과 VPN 기능이 하나의 장비에서 동작하는 제품이 시장의 대부분을 차지하게 되었다.

이선응 차장/김영준 과장
아이크래프트㈜ SNT본부 기술1팀

[그림 5]와 같이 한 장소에서 머무는 사용자가 있는 사무실 등에는 고정형 장비를 설치하여 사용 가능하지만, 출장이나 외근, 재택근무를 하는 사용자들의 경우 별도의 장비를 가지고 다니기 힘들기 때문에, 다른 형태의 장비가 필요하다. 이런 경우에는 본사에만 VPN 장비가 위치하고, 사용자 PC에 VPN 접속프로그램이 설치되어, 사용자가 PC에 설치된 VPN 접속프로그램을 동작시켜 ID, Password를 입력하면, 본사 VPN 장비에 접속할 수 있게 된다. 이런 경우 PC에 설치된 접속프로그램이 정보를 암호화, 복호화를 처리하게 되고, 본사의 VPN 장비는 동시에 다수의 사람이 접속하기 때문에, 동시 접속자를 고려하여 장비의 용량을 결정하게 된다.

방화벽과 VPN을 조합해서 보안을 강화할 수 있는 방식이 있다. 단순한 홍보목적의 홈페이지 서버는 불특정 다수의 고객을 대상으로 서비스 하기 때문에 방화벽에서 접속 제한을 할 수 없다. 고객이 어떤 IP 주소를 이용해서 접속할지 모르기 때문이다. 그러나 임직원을 대상으로 하는 서비스는 접속하는 사람이 제한되어 있기 때문에 방화벽에서 이런 서비스의 접속을 처음부터 차단한다. 그러면 일반고객이나 해커들은 임직원용 서비스에 접근할 수가 없게 되어 완벽한 접근보안이 가능하다. 여기서 접속이 필요한 임직원을 위해 VPN 장비를 설치한 후에 ID와 Password를 발급하고, VPN 장비의 주소를 알려주게 되면, VPN 장비를 통해서만 임직원용 서버에 접속할 수 있게 된다. 이렇게 되면, 허용된 사용자만 접근할 수 있을 뿐만 아니라, 전송되는 회사 메일이나 문서가 암호화되어 회사정보가 유출될 위험성이 낮아지게 된다.

요즘에는 VPN 장비 이외에 웹서버에서도 트래픽을 직접 암호화하여 고객 PC와 통신하는 방식이 늘어나는 추세이다. [그림 6]과 같이 홈페이지 주소(URL)를 입력할 때 http:// 대신에 s를 추가한 https:///(https://)를 입력하게 되면 데이터가 암호화되어 전달되게 된다. 이런 방식을 보통 SSL이라고 부르며, Daum 메일이나 Gmail 등을 이용할 경우 주소창에 녹색 자물쇠모양과 함께 안전함이라는 표시가 나오게 된다. 즉 전달받는 정보가 암호화되어 있기 때문에 해커가 나의 메일 정보를 엿보거나, 유출되는 위험에서 안전하다는 것을 나타내는 표시이다.

그림 6. 메일서비스 SSL 접속 화면

그런데, 이렇게 좋은 기능을 해커들도 이용하려고 시도하게 되었다. 최근의 보안장비는 방화벽처럼 단순하게 설정한 규칙에 따라 정보를 허용 또는 차단하는 동작 이외에도 허용하는 트래픽 내용을 계속 지켜보고 있다가 이미 알려져 있는 공격방식과 유사한 패턴이 보이면 공격으로 인식하여 해당 트래픽을 차단할 수 있는 기능이 있다. 당연히 이런 기능은 트래픽이 암호화되어 있지 않아야 사용이 가능하다.

해커는 이런 보안장비가 계속 자기의 공격행위를 지켜보고 있다는 것을 알고 있기 때문에, 이를 무력화시키기 위해 자기의 공격행위를 SSL 기술을 이용하여 암호화시켜 버린다. 이렇게 되면, 보안장비는 암호화된 트래픽을 더 이상 확인할 수 없기 때문에 공격행위를 탐지할 수 없게 되고 공격성공률이 올라가게 된다. 이런 식으로 유용한 보안기술이 나오면, 이를 공격에 악용하는 사례가 반복되고 있다.

공격자의 이런 악용사례를 방어자 입장에서는 그저 바라만 볼 수 없게 되고, 다시 보안장비에 암호화된 트래픽을 복호화시켜, 공격여부를 검사할 수 있는 기능을 추가하는 방식으로 대응하였다. 물론 복호화시키기 위해 별도의 장비를 추가하고, 장비의 성능을 높이기 위해 추가적인 하드웨어를 설치하겠지만, 보안수준을 향상시키기 위해서는 감수해야 하는 사항이다. 이렇게 보안 분야에

는 창과 방패의 싸움이 무한 반복되고 있다. 방패의 성능을 높이면, 이 방패를 뚫기 위해 좀 더 날카로운 창이 나오게 되고, 다시 이를 막기 위해 방패의 성능을 높여야 하는 일이 반복될 수밖에 없다.

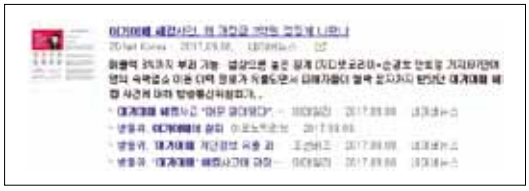

그림 7. 숙박 예약사이트 해킹사고 기사

과거보다 프로그램을 개발하는 방식이 쉬워지고, 이렇게 만든 프로그램을 간편하게 찾고 다운로드할 수 있는 환경으로 바뀌다 보니, 요즘은 중고등학생이 단순한 호기심에서 인터넷에 있는 해킹툴 혹은 공격프로그램을 다운로드 받아 공격하더라도, 쉽게 홈페이지가 해킹되는 사고가 빈번히 발생되고 있다. 얼마 전 숙박예약사이트의 경우 기본적인 공격 방식 중 하나인 SQL Injection이라는 공격으로 인해 97만 명의 개인정보 및 숙박예약 정보가 유출되었다고 한다.

이런 공격은 대부분의 웹서버를 운영하는 조직에서는 일상적으로 발생하는 공격이며 이런 종류의 공격을 막기 위해 웹방화벽이라는 보안장비를 많이 이용하고 있다. 문제는 TV에 광고를 할 정도의 규모를 가지고 있는 사업체에서 이런 기본적인 보안장비가 없거나 있더라도 정상적으로 관리가 되어 있지 않았다고 추측해 볼 수 있다.

정보보안의 목적을, 공격을 완벽히 막는 것에 두지 말고, 공격이 들어오면 공격자의 시간과 노력을 최대한 투입하게 만들어 침입을 지연시키고, 이렇게 침투에 성공했더라도, 투입한 시간과 노력에 비해 얻는 이득이 없게 만드는 것을 목적으로 하는 것이 올바른 방향이라고 생각한다. 보안장비를 구비할 충분한 여력이 있고 인터넷으로 매출을 대부분을 얻는 조직이 단순히 인터넷으로 다운로드 받은 공격프로그램으로 단 시간 내에 중요정보가 쉽게 유출되는 것을 차단할 수 없는, 기본적인 보안체계조차 갖추지 못하는 것은 법적으로 처벌받을 수 있는 사안이다.

다음 시간에는 최근 언론에 많이 언급되고 있는 DDoS 공격과 APT 공격에 대해 소개하도록 하겠다.