이것만은 알아야 할 네트워크 보안 이야기

Part 1. 방화벽 - 1 (방화벽의 역할, 보안정책)

글. 이선응 아이크래프트 수석

대략 2년 전 필자는 '방송시스템의 보안 강화'란 제목으로 '방송과기술'에 글을 연재하여 정보보안에 대한 개요 및 네트워크 보안에 대해 '수박 겉핥기' 식으로 다양한 장비를 소개해 드린 적이 있다. 이번 연재는 네트워크 보안에 대해 좀 더 심화시켜 전문적인 내용을 소개하면서 되도록 알기 쉽게 풀어서 설명해 드리도록 하겠다.

첫 번째 글에서는 네트워크 보안에서 가장 필수적이며, 대표적인 장비인 방화벽(Firewall)을 주제로 소개해 드리도록 하겠다. ICT 분야에 종사하지 않는 분이라도 방화벽이라는 용어는 한 번쯤은 들어보셨을 것이다. 그만큼 정보시스템을 운영하는 환경에서는 거의 필수적으로 사용되는 장비로써 서버와 서버 간 혹은 서버와 단말 간 통신을 제어하고, 보안을 강화하기 위한 목적으로 사용되고 있는 장비이다.

방화벽은 정보보안 분야에서 사용되기 전에 실생활에서 먼저 사용되기 시작하였다. 용어를 풀어 쓰면 한자어로 막을 '방', 불 '화' 즉 '불을 막는 벽'을 의미한다. 아래 [그림 1]과 같이 건물과 건물 사이에 불에 타지 않는 불연재로 돌을 이용하여 벽을 쌓은 것을 볼 수 있다. 옛날에는 대부분 나무로 건물을 세워서 화재에 무척 취약했었다. 한 집에서 불이 나면 마을 전체가 잿더미가 되는 경우가 흔했었다. 이를 막기 위해 건물과 건물 사이에 돌로 방화벽을 세워 불이 나더라도 옆 건물로 불이 번지는 것을 막아 피해를 최소화하는 용도로 사용했었다.

그림 1. 전통적인 방화벽

정보시스템에서의 방화벽도 전통적인 방화벽과 사용 목적은 동일하다. 단지 불을 막는 용도가 아니라 외부에서의 침입을 차단하는 목적으로 변경되었을 뿐이다. 즉 불을 침입 혹은 공격으로 대치하면 동일한 역할을 한다고 볼 수 있다. 아래 [그림 2]는 일반적으로 정보시스템 방화벽을 표현할 때 사용하는 그림이다. 왼쪽 그림과 같이 바깥쪽에서 난 불이 내부로 번지는 것을 막는 벽돌벽으로 표현되거나, 가운데 그림과 같이 지구본에서 출발하는 다양한 접속 시도를 화살표로 표현해서 녹색은 정상적인 접속 시도로 내부 시스템에 접속된 것을 표현하고, 빨간색 화살표는 허가되지 않은 접속 시도로 방화벽에서 해당 접속을 차단한 것을 표현한 것이다. 지구본은 인터넷을 통합 접속을 의미하는 것으로 전 세계에서 인터넷 연결이 된다면 어디 서든지 접속이 가능한 것을 표현한 것이며, 마지막 그림은 일반적인 방화벽 장비의 사진이다.

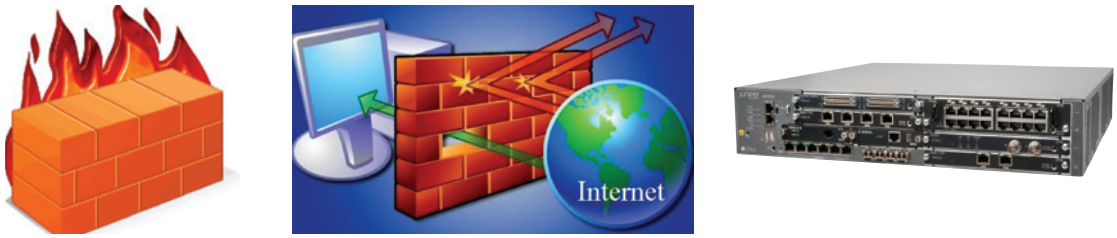

그림 2. 정보시스템 방화벽

그럼 다음으로 방화벽이 어떻게 구성되고 동작하는지 알아보자.
방화벽의 용도가 외부에서 내부로 접속을 시도할 때 내부시스템으로 접속을 허용하거나 차단하는 용도로 사용되기 때문에 언제나 외부와 연결된 위치에 설치되는데, 일반적으로 외부에서 들어오는 인터넷회선과 내부시스템으로 접속되는 사이에 설치된다. 통상 그 위치를 게이트웨이(Gateway) 구간이라고 표현하는데, 말 그대로 외부에서 들어오는 대문까지 연결된 길을 의미한다.

회사에서 인터넷을 사용하기 위해서는 KT, SK, LG라는 인터넷회선제공업체(ISP, Internet Service Provider)에서 제공하는 회선을 통해 서비스를 받는다. 라우터(Router)라는 통신장비를 전산실에 설치하고, 여기에 ISP 사업자의 광케이블을 연결해서 인터넷 접속이 가능하게 서비스하고 있다. 즉, 방화벽은 라우터에서 내부 네트워크로 연결되는 사이에 설치되는 것이다. 아래 [그림 3]과 인터넷 회선(Untrust zone)을 받아서 연결하고 내부 구역(Trust zone)과 완충구역(DMZ zone)으로 구분하여 각 구역을 연결시킨다.

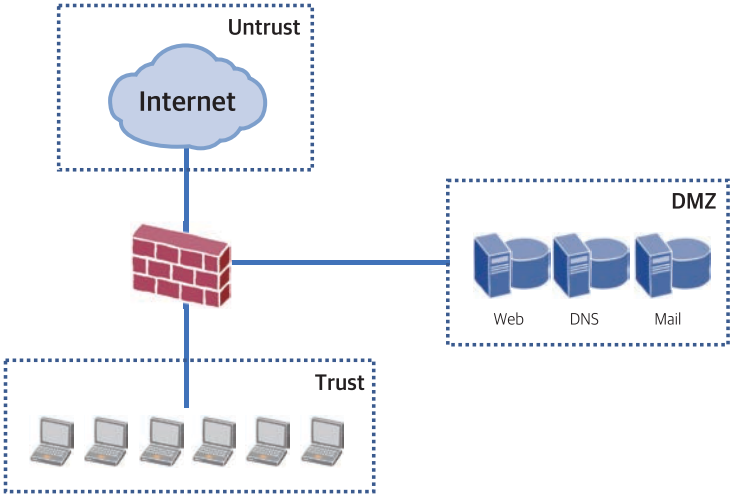

그림 3. 방화벽 구역 구성 예

방화벽은 연결되어 있는 네트워크의 위치 및 성격에 따라 이름을 부여하는데 보통 Untrust, Trust, DMZ 등을 할당한다. Untrust는 영어로 신뢰하지 않는 구간 즉 외부와 연결된 네트워크 구간을 의미하며, Trust는 신뢰구간 즉 사용자 내부 네트워크 구간을 의미한다. 그럼 DMZ는 어떤 구간을 의미하는 것일까?

그림 4. DMZ / 출처 : 위키피디아

DMZ라는 용어는 우리나라 사람들에게는 무척 친숙한 단어이다. 2000년대 초반 외산 방화벽업체에서 작성한 기술문서에서는 DMZ를 설명하기 위해 [그림 4]와 같이 우리나라의 비무장지대를 예로 들어 설명한 자료가 있었다. 북한과 남한을 구분하는 경계선에서 각각 2Km 범위에 완충지대를 두어 우발적인 군사충돌을 방지하기 위한 용도로 사용된 공간이다.

방화벽의 DMZ 구역은 남북이 아니라 외부(Untrust)와 내부(Trust)를 구분하고 그 중간지점을 지정한 구간이다. 이런 공간이 필요한 이유는 내부에서도 접근이 가능해야 하지만, 외부에서도 접근이 가능해야 하는 서버가 있는데, 이런 서버를 어느 구역에 놓을지 애매할 경우에 위치시킬 구역이 필요하기 때문이다.

어떤 서버들이 DMZ에 위치해야 할까? 인터넷을 사용할 때 필요한 서비스가 있다. 바로 DNS 서버(Domain Name Server)와 Web 서버(HTTP Service), 전자우편서버(Mail Service) 등이다. 인터넷을 사용하기 위해 웹브라우저(익스플로러, 크롬)의 주소창에 www.naver.com을 입력하게 되면, PC는 naver.com이라는 도메인 이름의 서버가 가지고 있는 IP 주소를 찾게 된다. 이때 도메인 이름을 질문하면 IP 주소로 알려주는 서버가 DNS 서버이며, 이렇게 확인한 IP 주소를 가지는 웹 서버에서 웹 페이지 정보를 불러오게 된다. 메일 서버도 동일한 방법으로 메일을 보내거나 받는 용도로 사용되는 서버이다.

그런데 이런 서버들은 반드시 인터넷을 통해 외부에서 접속하는 사용자와 통신이 가능해야 한다. 회사 홈페이지에 접속하거나 임직원에게 메일을 보내는 사람은 임직원뿐만 아니라 불특정 다수 즉, 인터넷에 연결된 모든 사람이 접속 가능해야 문제없이 서비스가 가능하다. 문제는 내외부의 모든 사람에게 접속을 허용해야 하므로 공격의 위험도 그만큼 증가하는 것이다.

만약 이런 공개된 서버가 내부 구역(Trust)에 설치되어 있다면 어떤 문제가 생길까? 이 서버가 해킹당하게 되면, 같은 내부 구간에 있는 일반 PC뿐만 아니라 사내에서만 사용되는 서버까지 위험하게 된다. 해킹된 서버에서 사내 전산 자원으로 접속하는 데 아무런 제약이 없어 공격이 확산하는 것을 막을 수가 없게 되는 것이다.

이런 외부에 공개된 서버가 DMZ 구간에 있을 때, 같은 구역의 서버들은 공격을 당할 위험이 높아 지지만 최소한 방화벽으로 구역이 분리된 내부 전산자원으로의 침입은 방어가 가능하게 된다. 즉 불이 번지는 것을 막을 수 있는 것이다. DMZ 구역뿐만 아니라, 사용자가 임의로 구역을 추가로 만들고 같은 성격의 서버를 위치시킬 수 있다. 예를 들어 외부에서 취재한 사진과 기사를 인터넷을 통해 본사 서버로 송고할 경우 어쩔 수 없이 취재자료서버는 외부에 공개되어야 한다. 그러나 이런 서버를 방화벽에서 특정 구역으로 분리하면, 이 서버가 혹시 해킹되더라도, 이 서버를 통해 사내의 전산자원으로 공격이 이루어지는 것을 차단할 수 있다.

이론적으로는 모든 서버 앞에 방화벽을 각각 한 개씩 설치하면 좀 더 완벽한 방어가 가능하다. 기존에는 물리적인 방화벽의 도입이나 관리문제로 불가능했지만, 최근에는 가상 서버(VM, Virtual Machine)를 많이 사용하기 때문에, 가

상 서버 앞에 논리적으로 가상방화벽을 한 개씩 설치하는 것에 문제가 없을 정도로 기술이 발전하였다. 이런 설계방식을 Micro-segmentation이라고 하여 굉장히 잘게 구역을 쪼개서 세밀하게 서버 접근을 제어할 수 있게 설계하는 방식도 존재한다.

방화벽은 사전에 설정한 규칙에 따라 서버와 단말(PC, 스마트폰) 간 연결을 시키거나, 혹은 연결을 차단하는 역할이 주요 기능이다. 이런 규칙을 보통 보안정책(Security Policy)이라 하며, 이 정책은 방화벽 관리자가 사전에 설정하여 모든 전산 자원에 대한 통신을 제어할 수 있다. 모든 전산 장비가 마찬가지겠지만, 방화벽의 경우에도 보안정책을 어떻게 설정하느냐에 따라 조직의 보안 수준을 굉장히 높일 수도 있고, 반대로 방화벽이 없는 것이나 마찬가지인 결과를 낼 수도 있다.

우선 보안정책은 어떤 내용으로 구성되어 있는지 알아보자. 보안정책을 설정할 때 필요한 요소는 아래 5가지이다.

요소	내용	예제
방향	어느 구역에서 출발해서 어느 구역으로 가나요?	Untrust → DMZ
출발지 주소	어디서 왔나요?	ANY
목적지 주소	어디로 갈 건가요?	10.10.10.10
서비스 포트	어떤 서비스를 이용하나요?	TCP80 (HTTP-Web)
액션(허용/차단)	위의 4가지 조건이면 해당 연결은 허용/차단합니다.	허용(Permit)

위의 표에 있는 예제를 풀어서 설명해 보면 다음과 같다.

> "인터넷에서 DMZ 구역으로 가려는 트래픽이네요, 그럼 출발지는 안 볼게요, 당신의 IP 주소가 무엇이든지 상관하지 않겠습니다. 목적지 IP 주소가 10.10.10.10이고 접속하려는 서비스 포트가 TCP 80을 사용하는 웹서비스이면 접속 요청을 허가하여 트래픽을 서버로 전달해 드릴게요."

이런 보안정책은 홈페이지 서버 혹은 웹 기반의 서비스를 하기 위해 필요한 전형적인 보안정책이다. 이러한 보안정책을 방화벽의 성능에 따라 수백 개에서 수만 개까지 만들 수 있으나, 보통 조직의 규모에 따라 수십 개에서 2~300개 정도를 사용하고 있다.

웹 서비스 이외에 DNS(UDP 53), Mail(TCP 25, 110), HTTPS(TCP 443) 등 다양한 포트를 조합해서 다양한 보안정책 설정이 가능하다. 그럼 가장 전형적인 방화벽의 구성 예를 들어보자. 다음 [그림 5]는 아래 조건에 맞추어서 설계된 구성도이다.

1. 회사를 들어오는 인터넷회선을 방화벽을 통해 제어가 가능해야 한다.
2. 인터넷을 통한 서비스를 위해 DMZ와 Upload 구역을 만들어 공개되는 서버를 위치시켜야 한다.
3. 방화벽 내부는 스위칭허브를 통해 사내 서버 및 사무실 단말을 연결시켜야 한다.
4. 지역 방송국, 외부 스튜디오, 재택근무자, 현장 취재기자들은 인터넷을 통해 공개된 서버 혹은 사내 서버에 접근이 가능해야 한다.

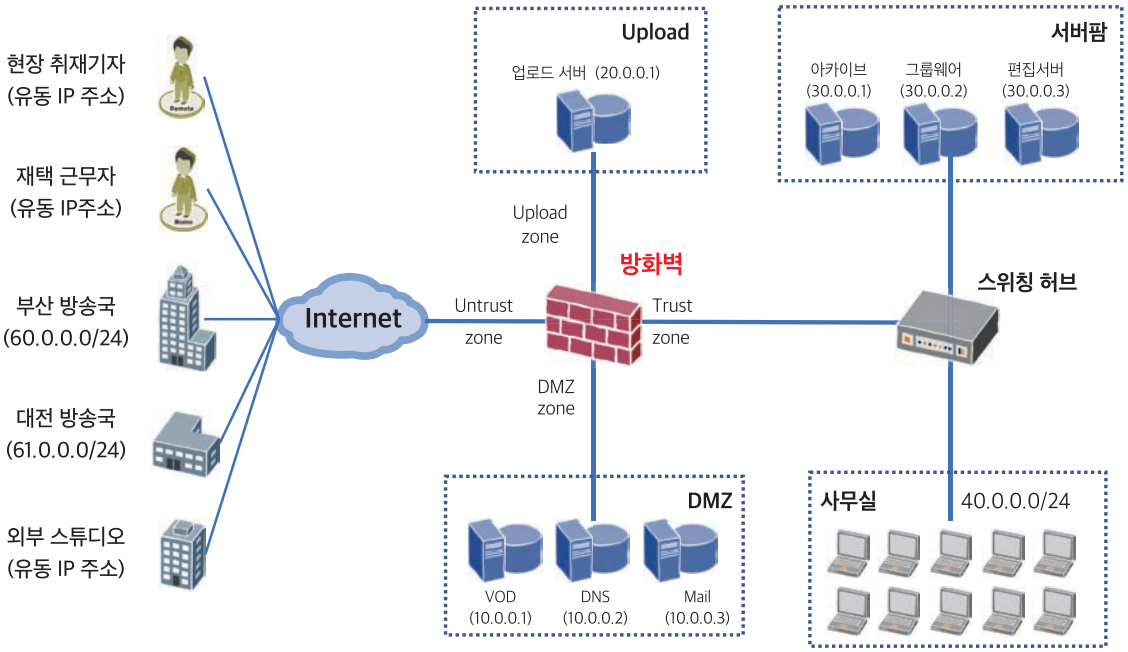

그림 5. 방화벽을 이용한 네트워크 구성도

위의 방화벽 구성도를 참고하여 다음과 같은 고객의 요구사항이 있다고 할 때 방화벽에서 어떻게 서비스가 가능하게 보안정책을 반영하는지 알아보자. 보안정책 표시는 (출발지 IP, 목적지 IP, 서비스 포트, 액션)으로 하였다.

	요구 사항	보안정책 반영 내용
1	일반 시청자들이 인터넷을 통해 VOD 서버에서 영상 검색과 시청이 가능해야 하며 서비스가 계속 증가하므로 서비스 포트는 모두 열어주어야 한다.	**Untrust → DMZ** ANY, 10.0.0.1/32, ANY, Permit
2	인터넷을 통해 VOD, Mail, 업로드 서버의 도메인 주소로 접속이 가능해야 하고, 사내에서 인터넷 사용 시 DNS 서버 사용에 문제가 없어야 한다.	**Untrust → DMZ** ANY, 10.0.0.2/32, UDP53, Permit **Trust → DMZ** 40.0.0.0/24, 10.0.0.2/32, UDP53, Permit
3	회사 내부에서 업무용 메일을 받고(SMTP) 보낼 (POP3) 있어야 하고, 사내에서뿐만 아니라 출장이나 재택근무 중에도 메일을 사용할 수 있어야 한다.	**Trust → DMZ** 40.0.0.0/24 10.0.0.3/32, TCP25(SMTP)/TCP110(POP3), Permit **Untrust → DMZ** ANY, 10.0.0.0.3/32, TCP25(SMTP)/TCP(POP3), Permit
4	그룹웨어 서버는 보안을 위해 외부에서 인터넷을 통한 접속은 못 하고 본사 사내와 지역 방송국에서만 접속이 되어야 한다.	**Untrust → Trust** 60.0.0.0/24, 30.0.0.2/24, TCP80, Permit 61.0.0.2/24, 30.0.0.2/24, TCP80, Permit
5	현장에서 취재한 사진과 기사는 인터넷을 통해 업로드 서버로 전송이 가능해야 하고, 서버에 전송된 사진과 기사는 사내에 있는 편집 서버에서 FTP로 사진과 기사를 가져갈 수 있어야 한다.	**Untrust → Upload** ANY, 20.0.0.1/32, TCP80, Permit **Trust → Upload** 30.0.0.3/32, 20.0.0.1/32, FTP, Permit

	요구 사항	보안정책 반영 내용
6	사무실에 있는 노트북에서 인터넷 사용이 가능해야 한다.	**Trust → Untrust** 40.0.0.0/24, ANY, TCP80, Permit
7	코로나 사태 등으로 재택근무가 필요할 경우 인터넷을 통해 사내에 있는 그룹웨어에 접속이 가능해야 한다.	**Untrust → Trust** ANY, 30.0.0.2/32, TCP80, Permit

1번 요구사항은 인터넷을 통해 시청자가 VOD 서버에 접근이 가능하게 하는 것이다. 방화벽 입장에서는 시청자는 Untrust 구역에서 들어오는 출발지 IP 주소를 지정할 수 없는 사용자이기 때문에 ANY 즉 모든 IP가 접근이 가능하게 설정한 것이다. 목적지는 DMZ 구역에 있는 VOD 서버이며, 서비스 포트도 어떤 포트를 요청하더라도 접속을 시도하면 허용하여 접속 요청을 VOD 서버로 전달하게 된다.
2번 요구사항은 외부에 공개된 서버의 도메인 주소로 접근을 시도하면 도메인 주소의 IP 주소를 알려 주는 DNS 서버가 외부 DNS 서버의 질의 요청에 응답을 주어야 한다. 이때 외부 DNS 서버는 불특정 다수 서버이기 때문에 출발지 IP 주소는 ANY로 설정하였다. 사내 임직원이 인터넷을 사용할 경우에도 사내 DNS를 이용할 경우 Trust 구역에서 DMZ 구역 방향으로 임직원 IP 주소 대역인 40.0.0.0/24에서 DNS 서버 IP 대역의 DNS 서비스 포트인 UDP53 포트를 오픈해야 정상적인 DNS 질의를 통해 웹브라우저에서 인터넷 접속이 가능하다.
3번 요구사항은 외부 및 내부에서 DMZ 구간에 있는 메일 서버에 접근이 가능해야 하기에 Untrust 구간에서 접근할 때는 출발지 IP를 지정할 수 없어 ANY로 지정하였으며, Trust 구간인 사내에서 접근할 때는 사무실 IP 대역을 출발지 IP로 지정하였다.
4번 요구사항은 그룹웨어와 같은 서비스는 임직원들만 접근이 가능해야 하며, 인터넷을 통한 불특정 다수의 접속은 차단되어야 한다. 그러나 본사에 근무하지 않는 지역방송국 임직원의 경우도 접근이 가능해야 해서 지역방송국의 IP 대역을 출발지 IP로 지정하여 접근이 가능하게 보안정책을 설정하여야 한다.
5번 요구사항은 외부에서 인터넷을 통해 취재한 사진과 기사를 송고하여야 하므로 해당 기자의 스마트폰 등을 통해 인터넷 접속을 해야 한다. 이때 할당받는 공인 IP 주소는 무작위로 할당되기 때문에 사전에 출발지 IP를 지정할 수 없으므로 ANY로 사용하여야 한다. 이렇게 업로드된 자료는 사내의 편집 서버에서 자료를 받아 가기 위해 FTP 서비스를 통해 접근이 가능하게 설정이 필요하다.
6번 요구사항은 사내 임직원들의 인터넷 접속을 위해서 Trust 구역에서 Untrust 구역으로 접근하는 것으로 출발지는 사무실 대역을 지정할 수 있지만 목적지는 임직원이 어떤 인터넷서비스에 접속할지 알 수 없어 임의로 지정할 수가 없어 ANY를 설정하여야 한다. 서비스 포트는 웹 접속을 위해 TCP 80을 오픈하여야 한다.
7번 요구사항은 출장 중이거나, 코로나 사태 등으로 재택근무를 시행할 경우 외부에서 인터넷을 통해 그룹웨어와 같은 사내 서버에 접근이 필요할 경우가 있다. 스마트폰을 이용하거나 집에서 인터넷을 사용할 경우에는 공인 IP가 임의로 할당되기 때문에 출발지 IP는 ANY를 지정할 수밖에 없다.

1번 요구사항과 같이 인터넷을 통해 접근할 때 출발지 IP가 ANY이면서 서비스 포트를 ANY로 지정할 경우, 해커가 해당 서버의 모든 포트에 접근 가능해져 사용 중인 서비스 포트 이외에 불필요하게 열려 있는 서비스 포트를 통해 침투당할 위험이 존재하게 된다. 방화벽을 운영하면서 가장 큰 문제점이 바로 출발지 혹은 목적지, 서비스 포트를 ANY로 사용하는 것이다. ANY를 사용하는 가장 큰 이유는 방화벽 관리자가 바쁘기 때문이다. 서비스가 추가 혹은 변경될 때마다 보안정책을 일일이 손봐야 하는데 담당자가 방화벽 이외에도 해야 할 업무가 많을 경우에는, ANY로 설정하게 되면 업무가 줄어들기 때문이다.

처음부터 외부에 공개할 서버는 해킹당할 위험이 항상 존재하기에 사내 네트워크와 완전히 분리하여 별도의 격리된 공간인 DMZ 혹은 Upload 구역으로 구분하여 설치해야 한다고 앞에서 설명해 드렸다. 문제는 여러 가지 이유로 인터넷을 통해 사내 서버에 다이렉트로 접속해야 하는 경우에 해킹당할 위험성이 높아지는 것이다. 앞의 요구사항 중 4번, 7번과 같이 Untrust 구역에서 Trust 구역으로 접근하는 보안정책이 바로 이에 해당한다. 이런 정책은 비유하자면 집안 가장 안전한 장소에 있어야 할 금고가 집 앞 길거리에 놓여 있는 것이나 마찬가지인 것처럼 위험한 보안정책이라고 할 수 있다.

4번 요구사항에 맞추어서 출발지를 부산, 대전 방송국 IP 주소로 지정한 경우는 그나마 출발지 IP가 제한되어 있어 안전한 편이나 7번 요구사항과 같이 출장 중이나 재택근무자를 위해 출발지를 ANY로 설정할 수밖에 없는 정책의 경우 인터넷을 통해 아무나 해당 서버로 접근이 가능하므로 문제가 있는 정책이라고 할 수 있다. 만에 하나 해커가 해당 서버에 관리자권한으로 접근 가능한 권한을 획득하게 되면 어떤 일이 일어날까? 해킹당한 서버와 사내에 있는 모든 서버, PC, 노트북 사이에는 방화벽이 없어 다른 사내 서버나 단말들이 해킹당할 위험이 매우 높아지게 된다.

다음에 연재될 예정인 VPN(Virtual Private Network, 가상 사설망)이란 기술을 이용하면, 4번 7번 요구사항에 대해 안전하게 서비스가 가능하게 구성이 가능하다. 간단히 설명드리면, 외부에서 사내의 중요 서버에 접근이 필요한 지역방송국에는 VPN 장비를 설치하거나, 개인 단말의 경우 VPN 프로그램을 설치하여, VPN 장비를 통해서만 접속이 가능하게 하는 것이다. 그리고, 단말에서 VPN 프로그램을 실행해서 인증(아이디/패스워드)을 통해서만 접속이 가능하게 접근 절차를 추가하면, 인터넷을 통해 데이터가 전송될 경우 데이터를 암호화해서 전송 하므로 혹시 데이터가 탈취되더라도 내용을 확인할 수 없게 만드는 기술을 사용하여 이런 문제를 해결할 수 있다.

보안 정책에 있는 서비스 포트의 경우 일반적으로는 표준으로 정의된 번호를 사용하게 된다. 이런 포트를 'well known port'라고 부르는데, 인터넷 초기인 1980~2000년 중반까지는 표준을 대부분 준수하여 사용하였으나, 이후부터는 여러 가지 이유로 표준을 준수하지 않고 임의로 포트를 지정하여 사용하는 경우가 증가하게 되었다. 예를 들면 웹을 사용하기 위한 HTTP 프로토콜의 표준 포트가 TCP 80번인데 8080, 8090번 등을 이용하거나, 메신저, P2P 등의 파일공유서비스 등도 TCP 80 포트를 이용하게 되면서, 포트 넘버로 서비스를 구분할 수 없게 되어, 기존 방화벽을 통해서는 정확한 트래픽 제어가 불가능하게 되었다. 새로운 방화벽이 필요한 시점이 된 것이다.

또한, 방화벽의 보급이 많이 되어서 거의 대부분의 조직이 보안정책을 통해 실제로 사용하는 포트만 오픈하여 서비스를 하기에 외부에서 공격을 시도하는 해커 입장에서 침투할 수 있는 통로가 많이 줄어드는 상황이 되었다. 많은 서비스들이 웹을 기반으로 통합되어 광범위하게 사용되게 되면서 대부분의 조직은 인터넷을 통해 불특정 다수가 접근 가능한 웹 서비스를 위하여 방화벽 보안정책을 통해서 TCP 80 포트만 오픈하게 되었다.

다음 시간에는 이러한 전통적인 방화벽의 한계를 극복하기 위해 등장한 차세대방화벽과 웹 방화벽에 대해 알아보도록 하겠다.