인터넷에서 사용되는 여러 기술 : VPN(Virtual Private Network)

조인준 KBS 미디어기술연구소 차장

지난 연재까지 HTTPS(Hypertext Transfer Protocol Secure)를 구현하기 위해 사용되는 보안기술인 SSL/TLS(Secure Sockets Layer/Transport Layer Security)에 대해 설명했습니다. 이번 편에서는 SSL/TLS 등과 같은 보안기술을 바탕으로 몇 년 전부터 일상 속에서 친근해지고 있는 VPN(Virtual Private Network, 가상 사설망)에 대해 이야기해보겠습니다. 아마 독자 여러분들도 이런저런 이유로 VPN을 많이 사용하고 계실 것 같습니다. 우선 기술 자체의 목적을 소개하자면 VPN은 사용자의 인터넷 연결을 보호하고 프라이버시를 강화하기 위한 기술입니다. Virtual Private Network라는 이름 속의 단어 하나하나를 통해 기술의 속성이 좀 더 구체적으로 다가오도록 설명하면 다음과 같습니다.

- **Virtual**
  - VPN에서는 실제로 케이블이나 전용 회선 등을 사용해 두 네트워크를 물리적으로 연결하지 않음
  - 기존의 공용 네트워크(예: 인터넷)를 통해 암호화된 터널을 만들어 사용자가 사설 네트워크에 안전하게 접근할 수 있게 함
  - 터널은 네트워크의 가상적인 연결을 의미하며 네트워크의 연결 방식이 물리적이지 않고, 논리적이고 소프트웨어적으로 구현된 가상 네트워크임을 나타냄

- **Private**
  - VPN 연결을 통해 다른 사용자가 내 데이터 또는 검색 활동을 볼 수 없기 때문에 Private 한 특성을 가짐

- **Network**
  - VPN을 사용하면 공용 네트워크를 통해 연결된 여러 기기가 마치 같은 사설 네트워크에 있는 것처럼 작동
  - 이 논리적인 네트워크는 물리적으로 존재하지 않지만 사용자가 그 네트워크 내에서 안전하게 데이터를 주고받을 수 있는 환경을 제공

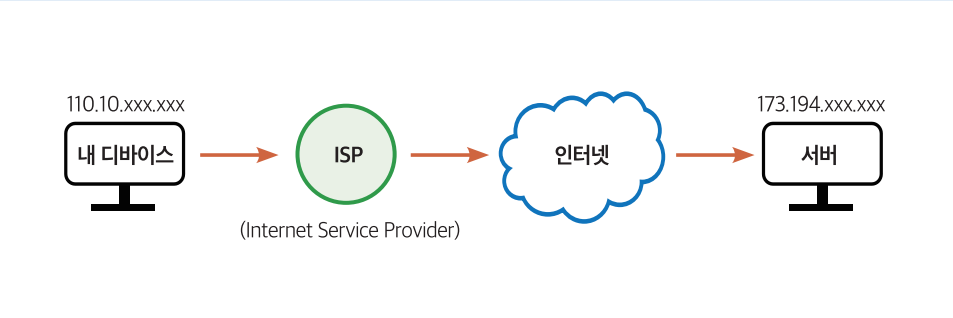

그림 1

[그림 1]과 같이 우리는 가정이나 회사에서 ISP(Internet Service Provider, 인터넷 서비스 제공자)를 통해 인터넷에 연결된 서버들에 접속하여 데이터를 주고받습니다. ISP는 개인이나 기업에 인터넷 서비스를 제공하는 회사나 조직을 가리키며 가장 가까운 예로 인터넷 서비스를 제공하는 통신사, 케이블 TV 회사 등이 있습니다.

ISP를 이용하여 인터넷의 서버에 접근하여 요청을 보내고 응답을 받는 과정에서 데이터는 [그림 2]의 IP 패킷 형태로 전달됩니다. IP 패킷의 IP 헤더에는 패킷을 보내는 디바이스의 IP 주소(Source Address)와 패킷을 받는 디바이스의 IP 주소(Destination Address)가 적혀 있습니다. 이는 중간에 누군가 패킷을 볼 수 있다면 누가 누구에게 데이터를 보내고 있는지 알 수 있다는 이야기가 됩니다. 더욱이 Payload가 암호화되어 있지 않다면 누가 누구에게 무엇을 보내는지 누군가가 중간에 볼 수 있고 이용도 할 수 있습니다. 이는 프라이버시의 노출 및 침해를 의미합니다.

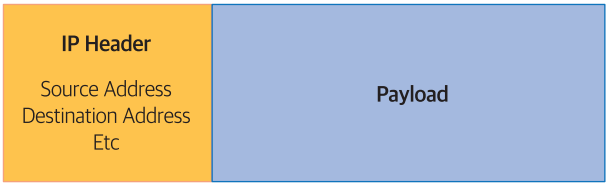

그림 2

하지만 [그림 3]과 같이 VPN을 이용하면 내 디바이스와 VPN 서버 사이에 VPN 터널이라는 것을 형성하고 VPN 서버를 통해 인터넷의 서버에 요청을 보내거나 응답을 받을 수 있습니다. 거의 대부분 암호화가 적용되는 VPN 터널을 이용하기 때문에 ISP는 내 디바이스와 VPN 서버 사이에 무언가 오고 간다는 것을 알 수 있지만 내 디바이스가 인터넷의 어느 서버에 접속하는지는 알 수 없습니다. 다시 말해 내가 인터넷에서 무엇을 하고 있는지 ISP는 알 수 없다는 것이 됩니다. 또한 인터넷에서 패킷을 들여다보고 있는 누군가가 있다고 해도 VPN 서버와 인터넷상의 서버 사이에 무언가 오간다는 것만 알 수 있을 뿐 실제 누가 인터넷상의 서버에 접속하고 있는지 알 수가 없습니다. 이렇듯 VPN을 통해 프라이버시를 안전하게 보호하는 것이 가능합니다.

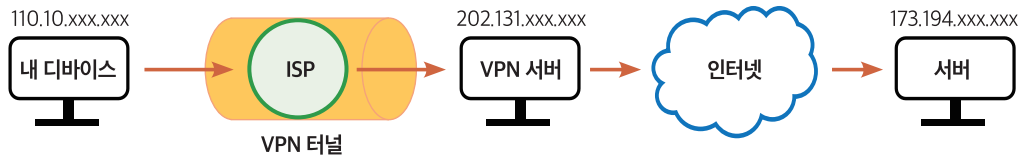

그림 3

그렇다면 VPN 터널에 관해 조금 더 자세히 알아보겠습니다. 지금 설명하는 내용은 전반적인 개념에 관한 것으로 실제 구현 기술들은 세부적으로 더 복잡한 내용을 포함하고 있습니다. [그림 1]에서와 같이 일반적으로 ISP를 통한 인터넷 통신에서 주고받는 IP 패킷은 [그림 4]의 엽서로 비유할 수 있습니다. 이 엽서에는 보내는 주소와 받는 주소가 노출되어 있고 전달되는 데이터의 내용인 Payload는 암호화되어 있을 수도 안 되어있을 수도 있습니다. Payload가 암호화되어 있지 않다면 누가 누구에게 무엇을 보내는지 그대로 중간에서 다 볼 수 있는 것이 됩니다. VPN 터널은 이렇게 중요한 정보가 노출된 상태로 패킷을 직접 보내지 않고 [그림 5]와 같은 형태로 바꾸어 VPN 서버에 전달합니다. 엽서로 비유된 [그림 5]에서 보내는 주소는 My Address(내 디바이스의 주소)이고 받는 주소는 VPN Server Address(VPN 서버 주소)입니다. 그리고 전달 내용은 암호화되어 있으며, 여기에 이용되는 암호화/복호화 방식은 VPN 터널 생성 시에 VPN 서버와 약속이 되어있어서 VPN 서버가 암호화된 데이터를 풀어서 볼 수 있습니다.

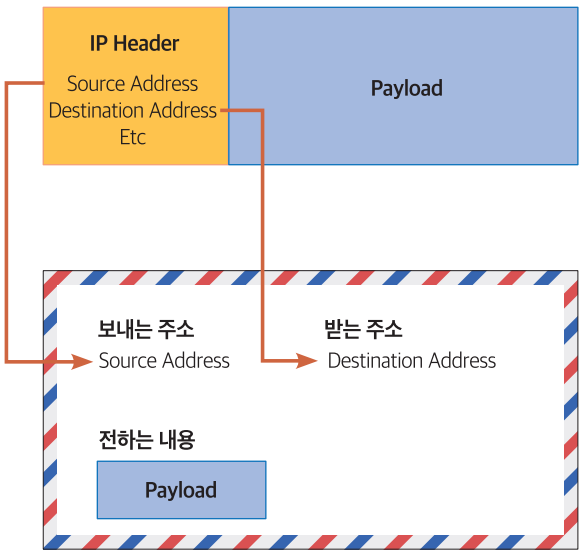

그림 4

그림 5

[그림 5]의 엽서가 ISP를 통해 VPN 서버에 전달되기까지 그 중간에 있는 ISP는 내가 VPN 서버에 무언가 보낸다는 것은 알아도 이 엽서가 최종적으로 어디로 향하는지, 무슨 내용을 전달하는지 알 수가 없습니다. 이를 알기 위해서는 VPN 터널에 적용된 암호화를 풀 수 있어야 하는데 사실상 계산이 불가능합니다.

[그림 5]와 같은 엽서로 비유된 데이터를 받은 VPN 서버는 VPN 터널 생성 시에 약속된 암호화/복호화 방식으로 전달 내용을 열어서 실제로 내 디바이스가 어디에 무슨 내용을 보내는지 알 수 있으며, 내 디바이스를 대리해서 인터넷상의 서버에 접속하여 요청을 보내거나 응답을 받습니다. VPN 서버가 인터넷상의 서버들로부터 받은 응답을 다시 내 디바이스에 돌려줄 때는 [그림 5]의 엽서와 같이 보내는 주소를 VPN 서버 주소로 하고, 받는 주소는 내 디바이스 주소로 한 후 전달 내용은 암호화하여 VPN 터널을 통해 회신합니다. VPN 터널은 ISP를 거쳐서 형성되어 있지만 앞서와 같이 ISP가 최대한 알 수 있는 내용은 내 디바이스가 VPN 서버와 무언가 주고받고 있다는 것뿐이고, 인터넷상에서 패킷을 훔쳐보는 이들도 VPN 서버와 인터넷상의 서버들이 무언가 주고받고 있다는 것뿐, 그 내용이 내 디바이스로 전달되고 있다는 것을 알 수가 없습니다. 이런 익명성을 이용해서 특정 국가에 한정된 인터넷을 통한 서비스도 그 서비스에 접근 가능한 VPN 서버를 통해 우회함으로써 이용이 가능합니다. 서비스 제공자에게 보이는 것은 VPN 서버뿐이고 실제로 그 서비스를 이용하고 있는 내 디바이스는 보이지 않기 때문입니다. 물론 이 모든 것을 알고 있는 VPN 서버가 패킷이 어디로 향하는지에 대해 비밀을 유지해주기 때문에 가능한 일입니다.

VPN 터널을 만들고 VPN 서버를 통해 통신하려면 VPN 프로토콜을 이용해야 합니다. VPN 프로토콜은 데이터를 암호화하고 내 디바이스와 VPN 서버 사이에 데이터를 전송하는 방식을 결정합니다. 현재 다양한 VPN 프로토콜이 사용되고 있으며 각 프로토콜의 장단점을 간략히 소개하면 다음과 같습니다.

- **OpenVPN**
  - OpenVPN은 많은 VPN 서비스 공급자가 사용하고 있으며 보안 수준이 높은 오픈소스 기반의 프로토콜
  - TCP 또는 UDP 프로토콜 기반으로 작동하며 TCP 기반은 데이터 전송의 안정성에, UDP 기반은 빠른 통신 속도에 초점이 맞추어져 있음
  - 오픈소스 기반이므로 누구나 보안 약점이나 다른 취약점이 있는지 확인할 수 있음
  - 다양한 설정과 기능을 지원하다 보니 복잡도가 높은 편임

- **WireGuard**
  - OpenVPN과 같은 오픈 기반의 프로토콜로 매우 높은 수준의 보안을 제공
  - 가장 최신 VPN 터널링 프로토콜인 만큼 OpenVPN과 IPsec을 능가하는 첨단 암호화 방식을 제공
  - OpenVPN 대비 코드의 복잡성이 낮고 빠름
  - 비교적 최신 오픈소스 프로토콜이라서 여전히 개선의 여지가 있지만 장래성은 매우 밝게 여겨지고 있음

• **IKEv2/IPsec(Internet Protocol Security)**
- IPsec은 네트워크 통신을 보호하기 위해 사용되는 프로토콜 모음으로 IP 계층에서 데이터를 인증하고 암호화하여 보안을 제공
- 암호화 키를 안전하게 교환하기 위해 강력한 암호화 및 인증을 제공하는 IKE(Internet Key Exchange) 프로토콜 사용
- IKEv2는 IKE 버전 2를 의미
- 설정과 관리가 복잡할 수 있음

• **L2TP/IPsec(Layer 2 Tunneling Protocol / Internet Protocol Security)**
- L2TP와 IPsec의 두 가지 프로토콜이 결합되어 동작
- L2TP는 터널링 프로토콜로 두 네트워크 간에 가상 터널을 설정하여 데이터를 전송하는 부분을 담당
- L2TP는 자체 암호화 기능이 없기 때문에 IPsec을 사용해 암호화 및 인증을 제공
- IPsec는 데이터 암호화 및 무결성 보장, 상대방에 대한 인증을 수행
- 역설적으로 L2TP는 보안을 전혀 제공하지 않기 때문에 여러 다른 암호화 프로토콜을 수용할 수 있어 안전함
- L2TP와 IPsec 두 가지 프로토콜을 사용하므로 상대적으로 느린 속도는 단점

• **SSTP(Secure Socket Tunneling Protocol)**
- 마이크로소프트가 만들었으며 안정성 및 활용성이 높은 VPN 프로토콜
- HTTPS(TCP 기반으로 SSL/TLS 사용) 기반으로 암호화된 데이터를 전송
- HTTPS 프로토콜에서 사용하는 443 포트를 이용하기 때문에 방화벽과 NAT을 쉽게 통과할 수 있음
- 마이크로소프트에 의해 개발되었으므로 Windows 중심으로 최적화되어 있는 것으로 알려져 있으며 OpenVPN과 같이 코드가 공개된 것이 아니어서 다양한 보안 관련 기술 점검에 집단 지성을 이용할 수 없음

• **PPTP(Point-to-Point Tunneling Protocol)**
- 1999년에 만들어졌으며 전화 접속 트래픽을 터널링하도록 설계된 VPN 프로토콜
- VPN 프로토콜 중 가장 약한 암호화 방식을 사용하여 보안에 취약
- 1999년에 만들어진 만큼 당시 하드웨어 수준으로 인해 많은 컴퓨팅 리소스를 사용하지 않도록 설계되어 실행이 빠름
- 오래된 만큼 다양한 운영체제에서 지원되고 널리 사용되어왔음
- 구식이라 보안에 취약하고 방화벽을 통해 차단되기가 쉬워서 권장되지 않음

지금까지 VPN의 기술적 내용에 대한 간략한 설명을 드렸습니다. 개념적인 수준의 설명이지만 동작 원리를 이해할 수 있었을 것 같습니다. 지금까지 설명 드린 내용을 기반으로 다음과 같은 VPN의 다양한 유형 또한 쉽게 이해할 수 있을 것 같습니다.

• **Remote Access VPN(원격 액세스 VPN)**

- 원격 사용자가 인터넷과 같은 공용 네트워크를 통해 회사 등의 내부망에 안전하게 접속할 수 있음
- 재택근무나 출장 중에도 회사 네트워크에 접근할 수 있음

• **Site-to-Site VPN(사이트 간 VPN)**

- 본사와 지사 등 두 개 이상의 네트워크를 인터넷을 통해 안전하게 연결
- 대규모 조직에서 지리적으로 분산된 거점 간의 연결을 지원

• **Mobile VPN(모바일 VPN)**

- 모바일 사용자를 위한 VPN으로 이동 중에도 연결이 끊이지 않고 안전하게 인터넷에 접속할 수 있도록 함

• **Clientless VPN(클라이언트리스 VPN)**

- VPN 클라이언트를 설치하지 않고 브라우저를 통해 VPN에 접속할 수 있는 방식으로 소프트웨어 설치 없이도 사용 가능
- 브라우저를 통하지 않는 디바이스 내의 다른 연결들에 대해 VPN을 지원하지 않음 보충 필요

P.S.

C군이 여러분께 전하는 내용 중 전문적 성격이 짙은 것은 엄밀한 언어를 사용하여 설명하기에는 한계가 있습니다.
본 내용은 설명하는 대상에 대한 전체적 맥락의 이해에만 이용하시고, 그 이상은 권위 있는 전문자료를 참고하시기 바랍니다.