8차시. 4차 산업혁명의 하이웨이를 지키는 네트워크 보안

01. 네트워크의 이해

OSI(Open System Interconnection) 7계층

- 1970년대 후반부터 IBM과 DEC 같은 메인 프레임을 공급하는 회사들이 시스템 간의 정보 교환을 하기 위한 네트워크 구조를 발표했는데, 그 당시에 발표된 네트워크는 타사의 네트워크 구조를 전혀 고려하지 않은 채 개발되어 상호 연동하는데 어려움이 많았다. 이에 국제표준화기구인 ISO(International Organization for Standardization)에서는 다양한 네트워크의 호환을 위해 OSI 7계층이라는 표준 네트워크 모델을 만들었다.
- OSI 7계층 모델은 네트워크에 연결된 시스템 간의 상호접속에 필요한 제반 통신절차를 정의하고 이 가운데 비슷한 기능을 제공하는 모듈을 동일계층으로 분할하여 모두 7계층으로 분할한 것이다. 이는 통신기능을 7개의 수직계층으로 분할하여 각 계층마다 다른 계층과는 무관하게 자신의 독립적인 기능을 지원하도록 구성하였다. 각각의 계층을 다른 계층과 독립적으로 구성한 것은 한 모듈에 대한 변경이 전체 모듈에 미치는 영향을 최소화하기 위해서이다. 즉, 일부 모듈의 변경이 있는 경우에 전체 모듈을 변경하는 대신 변경이 있는 해당 모듈만을 바꾸면 되도록 하였다.

- 이러한 계층은 크게 네트워크 기능을 제공하는 계층과 응용기능을 제공하는 계층으로 나누어지며 세부적으로는 최상위 계층인 응용계층(application layer)으로부터 시작하여 표현계층(presentation layer), 세션계층(session layer), 전송계층(transport layer), 네트워크 계층(network layer), 데이터 링크 계층(data link layer), 물리계층(physical layer)으로 구분되고, 각 계층마다 특정한 서비스를 제공함과 아울러 이를 위한 프로토콜들이 존재한다.

  - 물리 계층: 실제 네트워크 장치들을 연결하기 위한 전기적·물리적 세부 사항을 정의한 계층으로 케이블의 종류와 그 케이블에 흐르는 신호의 규격 및 신호를 송수신하는 장치의 인터페이스 회로와 제어순서, 커넥터 형태 등의 규격을 정하고 있다. 즉, 이 계층은 정보의 최소 단위인 비트 정보를 전송매체를 통하여 효율적으로 전송하는 기능을 담당한다.

  - 데이터 링크 계층: 포인트 투 포인트(Point to Point) 간 신뢰성 있는 전송을 보장하기 위한 계층으로 전송되는 비트의 열을 일정 크기 단위의 프레임으로 잘라 전송하고, 전 송 도중 잡음으로 인한 오류 여부(error control)를 검사하며, 수신측 버퍼의 용량 및 양측의 속도 차이로 인한 데이터 손실이 발생하지 않도록 하는 흐름제어(flow conrol) 등의 기능을 수행한다.

  - 네트워크 계층: 네트워크층은 패킷이 송신측으로부터 수신측에 이르기까지의 경로를 설정해주는 기능과 너무 많은 패킷이 한쪽 노드에 집중되는 병목 현상을 방지하기 위한 밀집제어(Congest control) 기능을 수행한다. 또한 상위 계층인 전송 계층이 요구하는 서비스 품질(QoS: Quality of Service)을 제공하기 위한 기능적, 절차적 수단을 제공하는 계층이다.

  - 전송 계층: 전송계층은 수신측에 전달되는 데이터에 오류가 없고 데이터의 순서가 수신측에 그대로 보존되도록 보장하는 연결 서비스(connection service)의 역할을 하는 종단간(end-to-end) 서비스 계층이다. 한편, 패킷의 순서에 무관하게 수신되며, 에러 처리도 하지 않는 비연결 서비스(Connectionless service)와 다중 목적지에 메시지를 전송하는 서비스도 있다. TCP와 UDP는 각각 연결지향 및 비연결지향 트랜스포트 프로토콜의 예이다.

  - 세션 계층: 양 끝단의 두 응용 프로그램(Applications) 간의 연결설정, 이용 및 연결해제 등 대화를 유지하기 위한 구조를 제공한다.

  - 표현 계층: 코드 간의 번역을 담당하여 응용 계층으로부터 사용자 시스템에서 데이터의 형식상 차이를 다루는 부담을 덜어주는 계층으로 전송되는 정보의 구문(syntax) 및 의미(semantics)에 관여하는 부호화 (encoding), 데이터 압축 (compression), 암호화 (cryptography) 등 3가지 주요 동작을 수행한다.

  - 응용 프로그램 계층: 네트워크 이용자의 상위 레벨 영역으로, 화면배치, 확장 비트열(escape sequence) 등을 정의하는 네트워크 가상 터미널 (network virtual terminal), 파일전송, 전자우편, 디렉토리 서비스 등의 유용한 작업을 할 수 있도록 한다.

- OSI 7 계층에서 사용되는 각 계층별 네트워크 장비에 대한 이해는 네트워크 보안을 이해하는데 도움이 된다. 즉, 네트워크 계층에 해당하는 장비로는 라우터와 멀티 레이어 스위치가 해당되며, 데이터링크층에 해당하는 장비로는 브리지와 스위치가 포함된다.

- 브리지(bridge): 하나의 네트워크 세그먼트를 2개 이상으로 나누어서 관리하기 위해서 만들어진 장비이다. 하나로 통합해서 관리하기 위한 허브와 비교될 수 있다. 동일한 지역 네트워크에 있는 부서에서 호스트들을 2개로 분리하여 상호 영향을 미치지 않도록 하기 위해서 사용된다.

- 허브(hub): 일반적으로 더미 허브(dumy hub)를 말하며, 허브 본래의 목적에 충실한 허브이다. A 호스트가 B 호스트에게 메시지를 보내고자 할 때, 메시지는 허브로 전달되고, 허브는 허브에 연결된 모든 호스트에게 메시지를 전달한다. 만일 수신자가 아닌 호스트가 메시지를 받은 경우 자신에게 보내어진 패킷이 아니라면 이 패킷은 버려지게 되고, 그렇지 않을 경우 최종적으로 애플리케이션 계층까지 전달되게 될 것이다.

- 리피터(repeater): LAN 영역에서 다른 LAN 영역을 서로 연결하기 위한 목적으로 사용된다. 2개의 LAN 영역을 하나의 LAN 영역으로 통합하고자 할 때 발생하는 문제는 데이타가 전달되어야 하는 망이 길어진다는 문제가 있는데 이에 따라서 데이터 전송매체인 전기적 신호가 감쇠되거나 잡음이 생길 수 있으므로 신호감쇠와 잡음을 처리하기 위한 장치를 필요로 하게 된다. 이러한 일을 해주는 네트워크 세그먼트 간의 연결 장치가 리피터이다.

- 스위치(switch): 일반적으로 스위칭 허브를 말하며, 더미 허브의 가장 큰 문제점인 LAN을 하나의 세그먼트로 묶어버린다는 점을 해결하기 위해서 세그먼트를 여러 개로 나누어준다. A 호스트에서 B 호스트로 패킷을 보내려고 할 때, 더미허브는 허브에 연결된 모든 호스트에 패킷을 복사해서 보내지만 스위칭 허브는 B 호스트에게만 패킷을 보낸다. 스위칭 허브는 MAC주소를 이용해서 어느 세그먼트로 패킷을 보내야할지를 결정할 수 있으며 이를 위해서 맥 테이블(MAC table)을 메모리에 저장하여 기능을 수행한다.

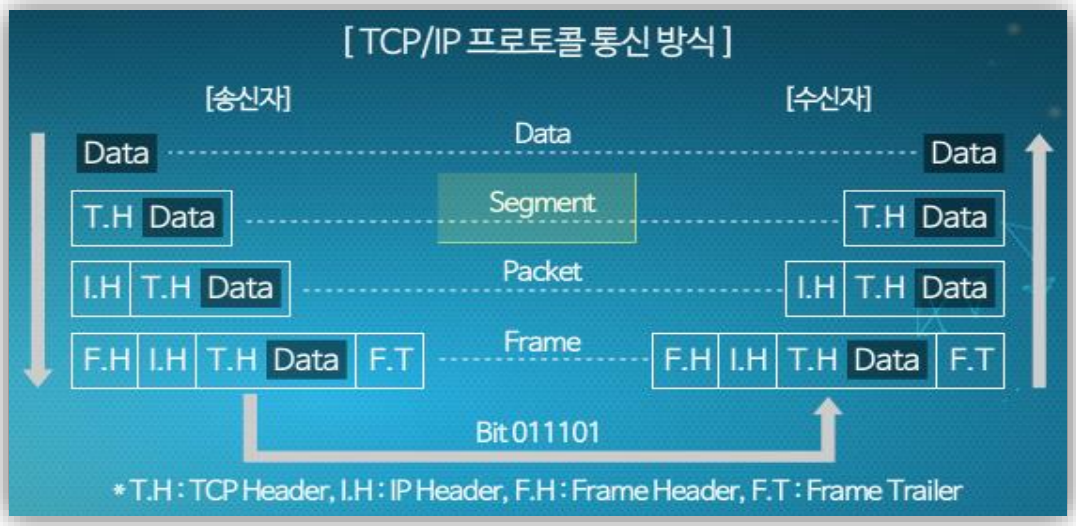
- L2(Layer 2) 스위치를 그냥 스위치라고 부르며, L3 스위치는 허브와 라우터의 역할, 즉 스위칭허브에 라우팅 기능을 추가한 장비이고 L4 스위치는 서버나 네트워크의 트래픽을 균형 있게 분배하는 로드밸런싱(load balancing)하는 기능을 포함한 장비이다. 멀티 레이어 스위치는 스위치 자체가 레이어2 장비였는데 비하여 상위 계층으로 점점 올라가면서 TCP, UDP 등의 프로토콜에 대한 컨트롤 역할을 수행하게 되면서 트래픽 제어 등의 기능이 추가되었다.

- 라우터: 리피터(repeater)와 브릿지(bridge), 허브(hub)가 비교적 근거리에서 네트워크(LAN)를 통합하거나 분리하기 위해서 사용하는 반면, 라우터는 원거리에서 네트워크 간 통합을 위해서 사용되는 장비이다. 라우터를 이용해서 거미줄처럼 얽혀있는 인터넷상에서 원하는 목적지로 데이타를 보낼 수 있으며, 원하는 곳의 데이터를 가져올 수 있다.

TCP/IP 프로토콜 동작원리

- TCP/IP(Transmission Control Protocol/Internet Protocol) 프로토콜은 1960년대 후반 이기종 컴퓨터간의 원활한 데이터통신을 위해 미 국방성에서 개발한 통신 프로토콜이다. TCP/IP는 보안 기능dl 취약하고 IP주소 자원이 부족한 제한성에도 불구하고 전 세계적으로 가장 널리 사용하는 인터넷 표준 프로토콜이다. 그림 2는 TCP/IP 프로토콜과 OSI 7계층과의 대응 관계와 함께 계층별 프로토콜을 도시한 것이다.

- TCP/IP 프로토콜은 4개의 계층으로 구성되며 각 계층에서 처리되는 메시지는 애플리케이션 계층에서는 데이터, 트랜스포트 계층에서는 세그먼트, 인터넷 계층에서는 패킷 그리고 네트워크 인터페이스 계층에서는 프레임 및 비트라는 명칭을 사용한다(그림 3 참조). 송신자의 최상위 계층에서 하위계층으로 내려 보내면서 각각의 계층에 해당하는 헤더정보를 삽입하여 최하위 계층에서 물리적 전송을 수행한다. 수신자의 최하위계층에서는 해당 계층의 헤더를 확인하면서 최상위 계층에서 데이터를 최종적으로 확인하는 과정을 거친다. 즉, 해당 계층의 헤더를 통하여 동등한 계층 간의 통신이 수행되는 것이다.



- 여기서 네트워크 계층의 유일한 주소인 IP 주소가 각 호스트와 TCP/IP를 이용하여 통신을 수행하는 모든 네트워크 컴퍼넌트에 필요하다. IP 주소는 마치 집주소를 이용하여 집을 찾는 것과 같은 방식으로 네트워크상에서 특정 시스템의 위치를 찾는 역할을 한다. IP 주소는 32비트로 구성되고 네트워크 ID와 호스트 ID로 구성되며 네트워크 ID는 IP 라우터에 의해 묶여져 있는 동일한 물리적 네트워크에 존재하는 시스템을 구분한다. 동일한 물리적 네트워크상에 존재하는 모든 시스템은 반드시 동일한 네트워크 ID를 가져야 한다. 그리고 외부망에서는 네트워크 ID는 반드시 유일해야 한다.

- 호스트 ID는 네트워크 내에서 워크스테이션, 서버, 라우터, 기타 TCP/IP 호스트를 구분한다. 각 호스트의 주소는 반드시 네트워크 ID에 대해 유일해야 한다.
- CP/IP에서는 애플리케이션의 상호 통신을 위해서 포트 번호를 사용한다. 포트번호는 IP 주소와 함께 쓰여 해당하는 프로토콜에 의해 사용되고 그 범위는 0 ~ 65535이다. 포트 번호에는 인터넷 주소 관리 기관(ICANN: Internet Corporation for Assigned Names and Numbers)이 애플리케이션용으로 지정한 알려진 포트 번호(well-known port numbers), 회사용의 등록 포트 번호(registered port numbers), 그리고 개별용의 동적 포트 번호(dynamic port numbers)가 있다. 그 범위는 각각 0 ~ 1023, 1024 ~ 49151, 49152 ~ 65535이다. 예를 들면, 5는 원격 작업 입력용, 80은 하이퍼텍스트 전송 규약용 등이다.

포트번호의 범위는 각각 0~1023, 1024~49151, 49152~65535

21번: FTP	22번: 보안 텔넷(SSH)	23번: 텔넷
25번: SMTP(메일 발송)	42번: 호스트 네임 서버	53번: 도메인 메인 서버
70번: 고퍼(Gopher)	79번: 핑거(Finger)	80번: 웹(HTTP)
88번: 커베로스 보안 규격	110번: POP3(메일 수신)	161번: SNMP(네트워크 관리)

주요 프로토콜의 이해

- **ARP(Address Resolution Protocol)**

  ARP는 인터넷 IP 주소를 이용하는 네트워크 계층 주소를 이더넷 하드웨어, 즉 어댑터 주소 또는 MAC 주소인 물리 주소로 변환하기 위해 사용되는 프로토콜이다. 즉, ARP는 상대방의 IP 주소를 알고 있지만 MAC 어드레스를 알지 못하는 경우 ARP 프로토콜에 의해서 수신자 MAC 어드레스를 가져올 수 있는 프로토콜이다.

- **UDP(User Datagram Protocol)**

  UDP는 신뢰를 보장하지 않는 비연결형 데이터그램 서비스를 제공한다. 즉, UDP는 데이터그램의 전송을 100% 보장하지 않으며, 전송된 패킷의 순서가 정확하다는 것을 보장하지 못한다는 것하며 손실된 데이터를 재전송을 통해 복구하지 않는다.

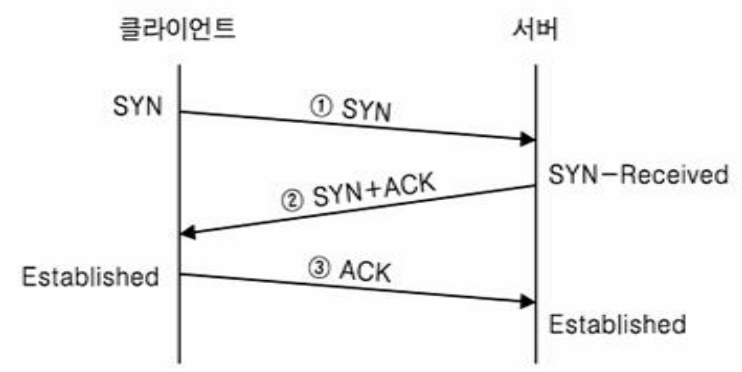
  UDP는 데이터 전달을 확인할 필요가 없거나 한 번에 작은 양의 데이터를 전송하는 애플리케이션에 주로 사용된다. SNMP(Simple Network Management Protocol)나 DNS(Domain Name Service)등이 UDP를 사용하는 애플리케이션의 대표적인 예이다.

- **TCP(Transmission Control Protocol)**

  TCP는 신뢰할 수 있고, 연결 지향의 전달 서비스이다. 데이터는 세그먼트 단위로 전송된다. 연결 지향(Connection-oriented)이란 호스트가 데이터를 교환하기 이전에 연결이 반드시 이루어져야 함을 말하며 전송되는 모든 세그먼트에 순번을 지정하여 신뢰성을 확신할 수 있게 된다.

- **ARP(Address Resolution Protocol) TCP 3-way 핸드쉐이크(Handshake)**

  TCP/IP 네트워크에서 클라이언트와 서버 간의 연결을 만드는데 사용되는 방법으로 실제 데이터 통신이 시작되기 전에 클라이언트와 서버는 SYN와 ACK(수신 확인) 패킷을 교환하는 3 단계 방법이다. 그 절차는 아래와 같다.



① 단계 : 두 시스템이 통신을 하기 전에, 클라이언트는 포트가 닫힌 Closed 상태, 서버는 해당 포트로 항상 서비스를 제공할 수 있는 Listen 상태

② 단계 : 통신 개시를 위하여 임의의 포트 번호가 클라이언트 프로그램에 할당되고 클라이언트는 서버에 연결하고 싶다는 의사 표시로 SYN 전송

③ 단계 : 클라이언트의 연결 요청을 받은 서버는 SYN Received 상태가 되고 클라이언트에게 연결을 해도 좋다는 의미로 SYN1) + ACK2) 패킷을 전송

④ 단계 : 클라이언트는 연결을 요청한 것에 대한 서버의 응답을 확인했다는 표시로 ACK 패킷을 서버로 전송

02. 네트워크 보안 유형

- 올해 초 미국에서는 인공심장박동기의 해킹 가능성이 대두됐으며, 스마트TV의 도감청 의혹도 불거진 바 있다. 초 연결로 특징 지워지는 4차 산업혁명 시대에서 우리의 일상에 밀접하게 연관되어 있는 각종 기기의 해킹은 일반인들에게 사이버 위협이 자신의 생활과 생명에 직접적 영향을 끼칠 수 있다는 불안을 야기한다. 따라서 보안에 취약한 기기 자체의 방어력을 높이는 것도 물론 중요하지만 외부에서 쉽게 기기에 접속하지 못하도록 네트워크 보안에 관심을 기울일 필요가 있다. 침입자들의 길목 곳곳에 두껍고 무거운 문을 설치하는 것이다. 4차 산업혁명의 핵심인 기기의 연결과 기술의 융합이 해커들에게 침입과 정복의 발판이 되지 않기 위해 네트워크 보안에 대한 경각심을 더욱 키워야 하는 이유다.

- **네트워크 보안 이란?**

  데이터 처리장치가 보급 이전에는 그 기관의 중요 보안 문제를 거의 물리적인 방법이나 행정적인 수단으로 처리했다. 즉, 물리적인 방법은 문서 서류함에 자물쇠를 달아 놓는 것이고, 행정적 수단이라는 것은 사람을 활용하여 보안 검사를 실시하는 등의 절차를 의미한다.

네트워크 보안 이란?

- 컴퓨터가 등장한 메인 프레임의 시대에서는 컴퓨터에 저장된 정보나 파일을 보호하는 자동화 도구가 필요하게 되었다(그림 5 참조). 따라서 외부의 해커의 침입을 차단하거나 저장된 데이터를 보호하기 위해 설계된 모든 도구를 총망라하여 컴퓨터 보안(Computer Security)이라고 하였다.

[메인 프레임 시대의 보안 개념: 문지기 역할]

- 인터넷의 보급과 함께 분산 네트워크의 시대가 확산되면서 네트워크를 통해 전송중인 데이터에 대한 보안은 더욱 중요하게 되었고 이를 네트워크 보안(Network Security)이라 한다. 사실 모든 기업, 정부, 교육기관의 데이터 전송이 하나의 네트워크가 아니라 네트워크들의 네트워크로 연결된 인터넷에서 이루어지므로 인터넷 보안이라는 용어를 사용하는 것이 적절하다. 네트워크 보안을 본격적으로 학습하기 전에 몇 가지 보안 위배 사례를 통해서 네트워크 보인의 중요성을 인식하도록 한다.

사례 1

철수가 영희에게 파일을 전송. 파일은 기관 내 구성원의 봉급내역으로 비밀이 요구됨. 파일을 볼 권한이 없는 도청자가 통신과정을 지켜보고 있다가 해당 파일을 몰래 가로채 복사

사례 2

네트워크 관리자인 밥이 관리하고 있는 네트워크 내의 컴퓨터 A에게 권한 파일 갱신 명령이 담긴 메시지를 전달. 즉, 새로운 사용자의 신원을 권한 파일에 포함시켜 컴퓨터 A에 접근을 허용하라는 명령. 공격자가 이 메시지를 가로채서 다른 사용자를 추가, 또는 일부 사용자를 제외시키도록 수정한 후 메시지를 컴퓨터 A에게 전송. 컴퓨터 A는 이 메시지가 밥이 보낸 것으로 믿고 그 메시지 명령에 따라 권한 파일을 갱신.

사례 3

사례 2에서 메시지를 가로채는 대신 공격자가 자신이 원하는 사용자의 신원이 포하된 메시지를 따로 작성하여 마치 이 메시지가 관리자 밥이 보낸 것처럼 꾸며 컴퓨터 A에 전송. 컴퓨터 A는 해당 메시지가 관리자 밥에게서 온 것으로 여기고 권한파일을 갱신.

- 위의 사례들은 금전적인 손실을 유발하는 비즈니스 거래나 금융거래 등에서 발생할 수 있기 때문에 네트워크 보안에서는 매우 많은 사항을 고려해야만 한다.

네트워크 보안 유형

- 조직이나 기관에 따라 네트워크 자체는 많은 장치와 소프트웨어로 구성되어 있지만 해커들의 관점에서는 네트워크에 어떤 네트워크 장비가 설치되어 있는지, 사용하고 있는 네트워크 프로토콜의 보안 취약점은 없는지 등이 주요 관심사이다. 즉 설치되어 있는 허브, 스위치 및 라우터의 설정, TCP/IP 프로토콜 구현상의 오류, 자원 공유/접근제어의 허점, 네트워크 기반의 인증 서비스 허점, 네트워크 서비스 데몬의 취약점 및 보안 관리의 허점 등을 살피게 된다. 현실세계에서 도둑이 행위를 하기 앞서 사전탐색을 하듯이 다양 방법으로 대상 네트워크를 스캐닝하고 사용 중인 서비스에 대한 포트 스캐닝 등을 먼저 시작한다. 그것을 바탕으로 스니핑(Sniffing), 스푸핑(Spoofing), 세션 하이재킹 및 서비스 거부 공격 등 다양한 유형의 네트워크 공격을 실해하게 된다.
- **네트워크 스캐닝**

  실질적인 네트워크 공격을 감행하기 이전에 네트워크 스캐닝을 하는데 그 목적은,

  - 시스템 정보 획득: 해킹을 위한 초석 작업으로 현재 운영 중인 시스템의 정보를 비롯한 다양한 정보를 취득하는 목적

  - 네트워크연결에 대한 보안취약점 검색: 특정 호스트의 작동유무와 제공 중인 서비스 확인

  - 포트 스캔(Port Scanning) : 서비스 중인 포트 및 서비스 종류, OS 종류 및 버전 파악

  - 취약점 스캔(Vulnerability Scanning) : 특정 네트워크 서비스(서버 어플리케이션)의 취약점 탐지

  포트 스캐닝은 어떤 서비스 포트가 열려 있는지를 확인하기 위해서 행위지는 작업으로

  - 네트워크 스캐닝에 의해서 시스템의 존재 유무가 확인되고 그를 통해 그 시스템의 IP 주소를 획득할 수 있고 이어서 그 시스템에 무슨 서비스가 존재하는지를 확인할 수 있다.

  - 서비스를 제공하는 서버 데몬의 종류를 확인하여 웹 서버의 종류와 버전을 확인하고 이어서 이미 알려져 있는 버그(취약점)가 데몬에 있는지를 확인할 수 있다. - 스캐닝 도구: nmap(Network mapper), mscan, sscan, portscan, HakTek, 등또한 사용하고 있는 운영체제를 확인하는데 이는 시스템의 운영체제 종류를 알면 존재하는 취약점 파악할 수 있고, 그 취약점을 악용할 방법을 도출할 수 있기 때문이다.

- **네트워크 스캐닝**

  취약점 스캐닝은 컴퓨터, 네트워크 및 통신 장비의 보안 취약성을 스캔하여 발견된 취약점에 대한 패치를 하지 않은 경우에는 그것을 이용하여 공격을 위한 시나리오 구성에 활용한다.

- **스니핑(Sniffing)**

  스니핑은 스니퍼를 이용하여 네트워크를 도청하는 행위를 말한다. 스니핑 공격을 수동적(passive) 공격이라고도 말하는데 그 이유는 공격할 때 아무 것도 하지 않고 조용히 있는 것만으로도 충분하기 때문이다. 도청 내용으로는

  - ID/패스워드를 포함하는 민감 데이터를 도청: ID/Password, credit card 번호, 이메일 내용

  - 인증 정보

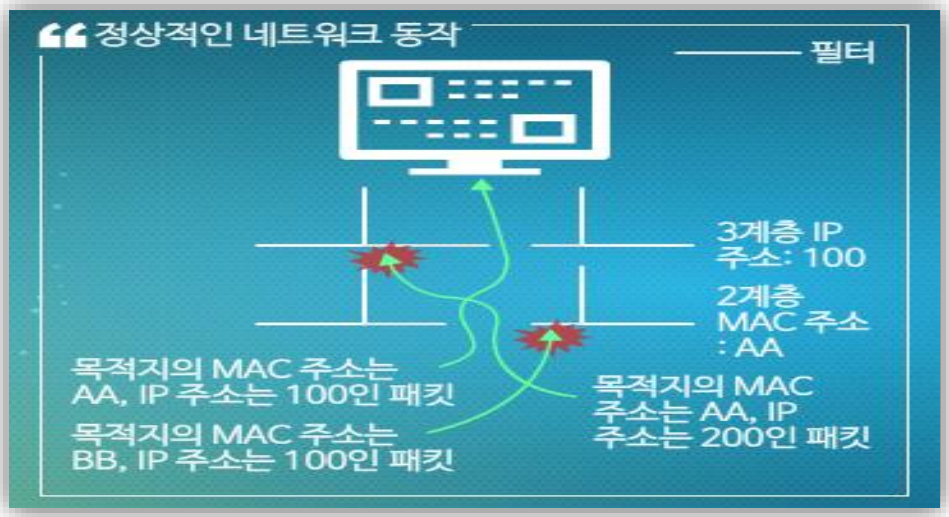
  - 기타 네트워크 트래픽

  . 내부자의 정보 유출 감시

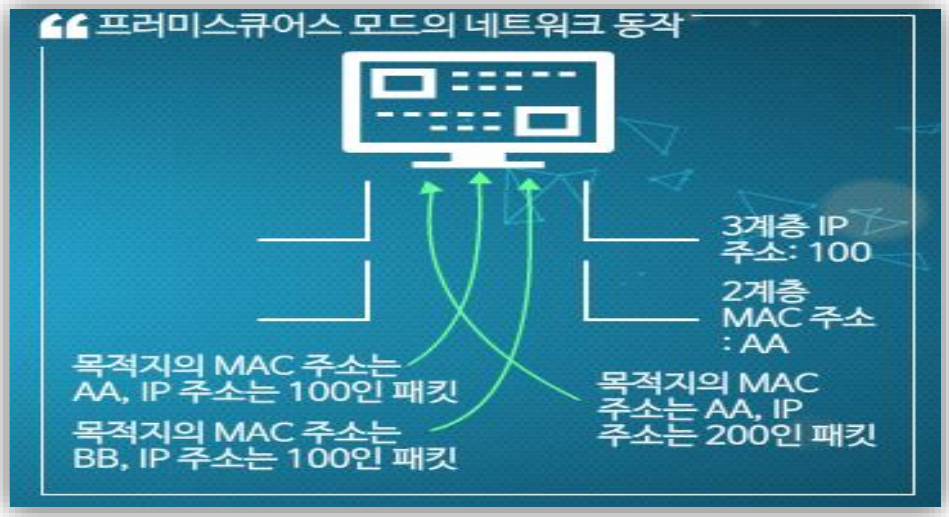
  . 트래픽의 내용 보다는 주로 트래픽 통계 및 네트워크 사용량 모니터링

- **스니핑의 원리: 초창기 스니핑**

  정상적인 네트워크에 접속하는 모든 시스템은 설정된 두 가지 정보인 IP 주소(3계층)와 기기에 고유한 MAC 주소(2계층)를 가지고 있는데 통신할 때 네트워크 카드(NIC: Network Interface Card)는 이 두 가지 정보를 가지고 자신의 랜 카드에 들어오는 패킷 헤더의 주소 값을 인식하고 자신의 버퍼에 저장할지를 결정한다. 즉, 네트워크 카드에 인식된 2계층과 3계층 정보가 자신의 것과 일치하지 않는 패킷은 무시한다(그림6에서 패킷의 IP 주소가 100, MAC 주소가 BB인 경우만 버퍼에 저장)



[정상적인 네트워크 동작]



[프러미스큐어스 모드의 네트워크 동장: 네트워크 필터링이 해제]

그러나 스니핑을 수행하는 공격자는 자신이 가지지 말아야 할 정보까지 모두 보기 위하여 IP주소와 MAC주소를 기반으로 하는 정상적인 필터링을 해제해야 한다(그림 7 참조). 이때 IP 주소와 MAC 주소에 의한 필터링을 해제하는 랜 카드의 모드를 프러미스큐어스(Promiscuous) 모드라고 하는데, 프러미스큐어스 모드는 간단한 설정 사항이나 스니핑을 위한 드라이버 설치를 통해 바꿀 수 있다.

- **스위치 재밍(Switch Jamming) 공격**

스위치 재밍 공격은 스위치가 MAC 주소 테이블을 기반으로 패킷을 포트에 스위칭할 때 정상

적인 스위칭 기능을 마비시키는 스니핑 공격을 말한다. 스위치 재밍 공격은 MACOF 공격이라고도 부른다. 스위치 재밍 공격과정은

- 스위치에 랜덤으로 생성한 MAC 주소 프레임을 대량 전송

- 스위치 MAC 테이블은 MAC 주소로 용량 초과(flooding): 용량을 초과하면 스위치는 기능을 잃고 더미 허브같이 작동

- 실제 패킷이 도착하면 스위치 메모리에는 목적지 MAC 주소가 없게 됨

. 이 경우 스위치는 모든 링크로 실제 패킷을 내보냄: 이때 스니퍼는 모든 패킷을 도청

- **ARP 손상(Poisoning) 스니핑**

ARP 손상 스니핑은 스위치 재핑 스니핑에서 사용하는 MAC flooding에 의한 공격이 작동하지 않는 스위치 환경에서 사용한다. 즉, 공격 대상자의 ARP 테이블을 손상시키는 방법을 이용한다. ARP 손상 스니핑의 특징은 공격대상의 트래픽이 공격자에 전송된다는 점이다. 공격 시나리오는 다음과 같다.

- 가짜 ARP 응답을 전송, 공격자의 MAC 주소로 대입

- 손상된 ARP 테이블에 의해 트래픽은 공격자로 전송

- 도착하는 모든 프레임을 스니프. 공격대상에서 오는 IP 패킷은 라우터로 보내도록 설정

- 패킷은 공격자에서 라우터로 전송

- **스니핑 탐지 및 대응(Sniffing Detection & Defense)**
- **스니핑 탐지(Sniffing Detection)**

-스니핑 공격은 스니퍼를 설치한 이후에는 네트워크에 별다른 이상 현상을 만들지 않기 때문에 사용자가 이를 인지하는 것이 어려워 능동적인 탐지를 통해서만 잡아낼 수 있다.

- Ping을 이용한 탐지: 위장 MAC 주소 전송에 대해 응답하면 스니핑
- ARP를 이용한 탐지: 위조 ARP 요청에 응답이 오면 프로미스큐어스 모드의 스니퍼
- 유인을 이용한 탐지: 가짜 ID/패스워드 이용(Honey-pot)
- Honey-pot: 가짜 계정을 생성하여 패스워드를 네트워크에 노출 후 그 패스워드를 사용 하는 공격자를 색출

- **스니핑 대응**

스니핑을 예방할 수 있는 가장 좋은 방법은 데이터를 암호화 하는 것이다.

- HTTPS(암호화된 HTTP)를 사용하여 웹 트래픽을 암호화
- SSH(Secure Shell) 를 사용하여 로그인 세션을 암호화
- S/MIME 이나 PGP를 사용하여 이메일 암호화

* S/MIME: Secure/Multipurpose Internet Mail Extensions, PGP: Pretty Good Privacy

- 무선이나 케이블 채널도 암호화

스니핑에 취약한 Telnet 사용을 피하고, 네트워크 내의 Hub는 스위치 네트워크로 전환하는데 좋다.

- **스푸핑(Spoofing)**

스푸핑(위장) 이란 시스템과 서비스에 접근하기 위해 타인의 신분으로 위장하는 것으로 매체 접근 제어(MAC) 주소, 인터넷 프로토콜(IP) 주소, 포트(port), 전자우편(이메일) 주소 등을 이용한다. 예를 들어, TCP/IP 프로토콜의 인증 메커니즘에 존재할 수 있는 결함을 이용하거나 공격자 시스템의 정보(IP 주소, DNS 이름, Mac 주소 등)를 신뢰성 있는 호스트로 위장하여 역추적을 어렵게 만든다. 스푸핑은 패킷 스니퍼링이나 서비스 거부 공격, 세션 하이재킹(Session Hijacking) 등의 다른 여러 가지 공격의 사전 공격 행위의 일환으로 진행된다. 스푸핑 공격에는 어떤 정보를 속이느냐에 따라 IP 스푸핑, ARP 스푸핑, DNS 스푸핑, 이메일 스푸핑 등으로 분류된다.

- **IP 스푸핑**

IP 스푸핑은 트러스트(trust) 접속의 서버-클라이언트 구조에서 IP 주소를 속이는 행위를 기반으로 진행된다. 즉 트러스트(trust) 접속의 서버-클라이언트 구조에서는 클라이언트 정보(주로 IP 정보)를 미리 서버에 저장 후, ID/패스워드 입력 없이 트러스트 로그인을 한다. 따라서 트러스트 접속은 패스워드를 이용하지 않아 스니핑 공격에 효과적인데, 해커에게는 접속과정에서 인증을 IP로 수행하기 때문에 패스워드를 알아내야 하는 스니핑 노력이 불필요한 장점이 있다. IP 스푸핑은 1995년 케빈 미트닉이 미 의회 시스템을 뚫고 들어간 방법이다.

- **IP 스푸핑**
  - 트러스트 관계의 클라이언트에 DoS 공격으로 연결 차단
  - 클라이언트의 IP 주소 확보
  - 실제 클라이언트로 위장하여 서버에 접근
- **IP 스푸핑 대응책**
  - IP 스푸핑은 DoS 공격이 시작이기 때문에 DoS 공격 대응 방안이 필요
  - IP 주소를 인증으로 사용하는 응용(application)을 피함
  - 인증으로 비밀번호, PKI나 Kerberos를 사용(불편함을 감수)
  - 패킷의 시퀀스 번호를 랜덤하게 생성하여 시퀀스 번호조작을 어렵게 함
  - 패킷 필터링 기능, 보안 취약성이 보강된 라우팅 프로토콜 사용 장비
  - 암호화된 프로토콜을 사용하면 IP 스푸핑 공격을 상당히 차단할 수 있지만 속도가 느려지는 단점이 있어 아직 보편화 되어 있지 않음.
- **이메일 스푸핑**

  이메일 스푸핑은 메일 프로토콜에 인증 메커니즘이 없는 취약점을 악용한 것으로 스팸메일이나 바이러스 감염메일을 보낼 때 악용되는 기법이다. 즉, 메일이 스푸핑되어 답장이 나에게 오도록 원래 메일발송자가 답장 받을 주소로 내주소를 위조한다. 따라서 이메일 스푸핑의 증상은

  - 내 계정에서 보낸 것처럼 보이는 메일이 반송되었다는 메일을 수신
  - 스팸함에 '내'가 보낸 메일이 들어 있는 경우
  - 보낸 적이 없는 메일에 대한 답장을 받은 경우이다.
- **세션 하이재킹**

  인터넷으로 계좌이체를 하는데 수신자 계좌 번호가 바뀐다면? 또는 FTP를 통해 파일을 다운로드하는데 파일의 내용이 바뀐다면? 생각하기조차 싫겠지만 세션 하이재킹을 통해서 가능한 상황이다. 세션 하이재킹은 허가 없이 활성화된 TCP/IP 세션을 가로채는 행위이다.

  세션 하이재킹에는 적극적 방식과 소극적 방식으로 구분된다. 적극적 세션 하이재킹은 정상 이용자의 세션을 차단하고 대신 공격자가 통신에 참여하는 경우이며, 새로운 계정을 생성하여 나중에 하이재킹 공격 없이 통신에 참여하기도 한다.

  소극적 세션 하이재킹의 경우 공격자는 클라이언트와 서버 간의 트래픽을 모니터링하면서 의미 있는 정보나 패스워드를 탐색한다.

- **세션 하이재킹 과정**

  TCP/IP 통신을 위해서는 양단간의 통신 요소인 IP 주소, 퍼트반호, 패킷의 시퀀스 번호가 필요한데, IP 주소와 포트번호는 스캔닝을 통해 쉽게 획득가능하다. 따라서 패킷의 시퀀스 번호를 추측할 경우 세션 하이재킹은 성공할 수 있다. 즉, 공격자는 시퀀스 번호를 예측하는 등 아래의 단계로 세션 하이재킹을 시도한다.

  - Step 1 - 공격대상 위치 탐지
  - Step 2 – 활성화 세션 탐지
  - Step 3 – 시퀀스 번호 예측
  - Step 4 - 공격대상 컴퓨터 격리(offline)
  - Step 5 - 세션 가로채기 및 유지

  세션 하이재킹에 대한 대응으로는 안전한 세션을 위해 SSH나 VPN을 이용하여 트래픽을 공격자로부터 보호하고 서버의 공개키를 변경하라는 등의 공격자의 위조 경고 메시지 등에 유의해야 한다.

- **무선 네트워크 보안**

  스마트기기의 확산에 따라 유선 네트워크보다는 무선 네트워크에 접속하여 다양한 서비스를 사용하는 추세이다. 하지만 무선 네트워크와 이를 이용하는 무선 디바이스에서는 유선 네트워크에서 발견되는 것과는 다른 유형의 보안 문제가 발생한다. 무선 네트워크에서 보안 위협을 초래하는 주요 요소를 유선 네트워크에 비교하여 검토하면 다음과 같다.

- **채널**

  . 무선 네트워크는 브로드캐스팅 형태의 통신으로 유선보다는 도청이나 재밍에 취약

  . 무선 네트워크는 통신 프로토콜의 취약점을 악용하는 공격에 더욱 취약

- **이동성(mobility)**

  . 유선 디바이스에 비해 휴대와 이동이 간편

  . 이동성으로 인한 많은 리스크 유발

- **자원(resource)**

  . 스마트폰이나 태블릿 등의 무선 디바이스는 정교한 운영 체제를 내장

  메모리와 프로세싱 자원이 제한적 서비스 거부 공격, 말웨어 위협 대처가 어려움

- **접근성(accessibility)**

  . 센서/로봇 같은 무선 디바이스는 사람이 관리하기 어려운 원격이나 적대적 장소에 위치

  . 물리적 공격에 매우 취약

- 즉, 무선 네트워크은 아래 그림13과 같이 무선 클라이언트(endpoint), 무선매체(wireless medium) 그리고 무선 접속점(access point: AP)으로 구성되는데 3가지 모두 위협에 취약하다. 무선 클라이언트에는 스마트폰, 와이파이 기능을 가진 랩톱이나 태블릿, 무선 센서 블루투스 장치 등이 포함된다. 무선 접속점은 네트워크나 서비스로의 연결을 제공하는 기능을 수행한다. 무선 전파를 반송하는 무선매체도 외부 위협에 매우 취약하다.

- **무선 네트워크 위협**

  무선 네트워크에서 발생할 수 있는 위협은 아래와 같다.

  - 우연한 연관성: 기업의 무선 LAN이나 AP는 전송 영역이 중첩될 수 있기 때문에 하나의 LAN에 연결하려는 이용자는 의도하지 않게 이웃 네트워크의 무선 AP에도 연결될 가능성이 존재. 이로 인한 의도하지 않은 연결로 위협에 노출

  - 악성 연관성: 무선 디바이스가 합법적인 AP로 인식하도록 설정하여 AP 운영자는 합법적인 이용자의 패스워드 갈취한 후 무선 AP를 통해 유선 네트워크에 침투를 시도

  - 애드 혹 네트워크(Ad hoc networks): AP가 없는 무선 시스템 간의 P2P 네트워크가 구성될 수 있는데 이 경우 중앙 통제가 없어 그로 인한 보안 위협에 노출 가능

  전통적 방식이 아닌 네트워크(Nontraditional networks): 개인 네트워크 블루투스 장치, 바코드리더, 휴대용 PDA 같은 비 전통적 방식의 네트워크와의 링크는 도청이나 스푸핑과 같은 보안 위협에 취약

  - 신원 도용(Identity theft): 공격자가 네트워크 트래픽을 도청하여 네트워크 권한을 가진 컴퓨터의 MAC 주소를 식별해낼 수 있는 경우를 신원도용으로 인한 위협 발생

- **무선 네트워크 위협**

  - 신원 도용(Identity theft) : 공격자가 네트워크 트래픽을 도청하여 네트워크 권한을 가진 컴퓨터의 MAC 주소를 식별해낼 수 있는 경우를 신원도용으로 인한 위협 발생

  - 중간자 공격(Man-in-the-middle attacks) : 사용자와 접속점(AP)을 속여서 그들이 상호 통신하고 있다고 믿도록 만드는 유형의 공격을 의미하는데 무선 네트워크의 경우 이런 유형의 공격에 매우 취약

  - Denial of service (DoS) : 공격자가 지속적으로 대량의 트래픽을 무선AP나 다른 접속 가능한 무선 포트를 공격하여 시스템 자원을 소모시키는 공격 유형인데, 무선 환경은 공격자가 쉽게 다수의 무선 메시지를 목표물로 전송하는데 가능하여 서비스 거부 공격에 적합

  - 네트워크 인젝션(Network injection) : 이 공격은 라우팅 프로토콜 메시지나 네트워크 관리 메시지와 같은 유형의 필터링 하지 않은 네트워크 트래픽에 노출된 무선 AP를 대상으로 하는공격. 이를 통해 라우터나 스위치의 성능을 저하시키려는 의도 실행함.

- **무선 네트워크 보안 방안**

  무선 전송에 대한 위협으로는 도청, 메시지 변조 및 삽입 그리고 통신 방해 등이다. 도청에 대한 대응으로는 신호 은닉 기술과 암호화 기술을 사용한다. 암호화와 인증 프로토콜을 사용하여 변조 및 삽입을 시도하는 위협을 막을 수 있다. 통신 방해를 유발하는 의도하지 않은 DoS 공격의 위험을 줄이기 위해서 동일한 주파수를 사용하는 다른 장치의 존재를 감지하는 사이트 조사를 실시하여 AP의 위치를 결정한다. 주변의 전송으로부터 무선 환경을 격리시키기 위해 신호 강도를 조정하고 차폐를 할 수 있다.

- **무선 접속점(AP) 보안**

  무선 액세스와 관련된 주요 위협 포인트는 네트워크에 대한 무단 액세스이다. 예방을 위한 주요 방법으로는 포트 기반 네트워크 액세스 제어에 대한 내용을 포함하고 있는 IEEE 802.1X 표준에 따르는 것이다. 표준에서는 LAN 또는 무선 네트워크에 연결하려는 디바이스에 대한 인증 메커니즘을 제공한다. 802.1X를 사용하여 불법 AP 및 다른 비인가 디바이스가 안전하지 않은 백도어가 되는 것을 방지 할 수 있다.

  * 802.1x: 802.1x 기술은 포트 기반의 인증을 구현한 기술로 표준화된 프로토콜. 네트워크단의 최종 말단 스위치(End Point와 접속되는) 및 무선 AP에서 사용자 인증을 통해 접근을 제어하는 기술로 안전성과 함께 물리적인 통제가 강한 장점을 지님.

- **무선 전송구간 보안**

  무선 네트워크의 보안을 위해서 아래의 사항을 추천한다.

  - 암호를 사용: 일반적으로 무선 라우터에는 라우터와 라우터 간의 통신을 위한 암호 메카니즘이 내장되어 있음.

  - 안티 바이러스, 안티 스파이웨어 및 방화벽을 사용: 모두 무선 네트워크 최종단에 설치

  - 식별자(SSID) 브로드캐스팅 모드 끄기: 일반적으로 식별자 브로드캐스팅 모드를 온 상태로 두어 신호범위 안에 있는 모든 장치가 라우터의 위치를 인식하도 하는데 이것을 비활성화하여 공격 시도를 차단할 수 있음.

- **무선 전송구간 보안**

  - 디폴트로 설정된 라우터의 식별자(identifier)를 변경

  - 관리용으로 라우터에 미리 설정된 패스워드를 변경

  - 무선 네트워크에 접속 가능한 컴퓨터 제한: 허가된 MAC주소를 가진 경우만 접속 허용

- **모바일 디바이스 보안**

  모바일 디바이스는 전체적인 네트워크 인프라의 한 부분으로 조직의 필수 요소이다. 스마트 폰의 확산 이전에 네트워크 보안은 내부 네트워크와 신뢰하지 않는 인터넷을 분리하는 명확하게 정의된 경계에 기반하여 조직이 주도적으로 통제하였다. 하지만 모바일 환경의 확산으로 조직의 네트워크은 새로운 환경에 대응을 해야 하는 상황에 직면한다.

  - 새로운 디바이스 증가

  - 클라우드 기반의 응용 서비스: 클라우드를 통하여 조직의 목적의 응용서비스와 개인 용도의 응용서비스를 개인 스마트폰으로 처리하면서 보안의 새로운 어려움이 발생

  - 네트워크 경계의 붕괴: 디바이스, 응용 서비스, 사용자 그리고 데이터가 다른 네트워크를 사용하기 때문에 네트워크의 경계를 기반으로 하는 과거의 보안 메카니즘은 한계에 직면

  - 외부 비즈니스 요구: 조직은 고객, 제3자 계약자, 비즈니스 파트너가 항상 네트워크 접속이 가능하도록 허용해야 하는 상황에서 새로운 보안 문제 발생

  모바일 환경의 급격한 변화로 인한 무선 디바이스는 아래와 같은 다양한 위협에 노출된다.

  물리적 보안 통제 부재: 모바일 디바이스에 대한 보안 정책은 모바일 디바이스 분실, 악성 집단에 의해 접속 등을 고려하여 수립

  신뢰할 수 없는 모바일 기기 사용: 조직의 모든 디바이스를 신뢰 할 수 없음을 전제

  신뢰할 수 없는 네트워크 사용: 보안 정책은 모바일 디바이스와 조직 사이의 네트워크는 신뢰할 수 없다는 가정을 전제

  다른 시스템과 상호 교환: 조직이 모든 디바이스를 동기화시켜 통제하지 않는 한, 조직의 데이터가 안전하지 않은 장소 저장되거나 말웨어가 유입되는 상당한 위험이 존재

  신뢰할 수 없는 콘텐츠 사용: 모바일 디바이스는 다른 컴퓨팅 디바이스가 접하지 않는 컨텐츠에 접속 및 사용

  위치 서비스 사용: 공격자는 디바이스와 사용자의 위치 정보를 이용

  - 출처 불분명한 응용 프로그램 사용: 3자가 만든 응용 프로그램을 통해서 말웨어가 설치될 가능성 존재

  모바일 디바이스에 대한 다양한 위협에 대응하기 위해서 디바이스 자체에 대한 보안, 클라이언트-서버 간의 트래픽 보안 그리고 경계(barrier) 보안을 고려한다.

- **디바이스 보안**

  직원용으로 모바일 디바이스를 지급하고 조직의 보안 정책에 따라 디바이스를 사전에 설정하도록 한 경우에는 보안통제가 크게 문제되지 않는다.

- **디바이스 보안**

  하지만 많은 조직에서는 직원의 개인 디바이스로 기업의 자원에 접속하도록 하는 BYOD(Bring Your Own Device) 정책을 적용한다. 이 경우 IT 관리자는 기업 네트워크를 허용하기 이전에 각 디바이스를 조살 능력이 있어야 한다. 즉 운영체제와 응용 프로그램에 대한 설정 가이드라이니을 제시해야 한다. 예를 들어 탈옥(jail-broken) 다바이스는 네트워크 접속을 허용하지 않으며 모바일 디바이스의 로컬 저장영역에 회사 접촉과 관련된 정보를 저장하지 않도록 해야 한다.

- **트래픽 보안**

  트래픽 보안은 일반적으로 암호와 인증 메카니즘을 토대로 실시한다. 즉, 모든 트래픽은 SSL이나 IPv6와 같이 암호화하여 안전한 상태로 전송되도록 해야 한다. 또한 가상 사설망을 통하여 모바일 디바이스와 조직의 네트워크 간에 모든 트래픽이 통과하도록 설정해야 한다.

  강력한 인증 프로토콜을 사용하여 디바이스에서 조직의 자원에 접속을 제한하도록 해야 한다. 모바일 디바이스의 경우에는 디바이스 사용자가 거의 한 사람밖에 없기 때문에 단일 인증 메카니즘을 사용한다. 경우에 따라서는 디바이스 인증 후에 사용자를 한 번 더 인증한다.

- **경계 보안**

  허가받지 않은 접근으로부터 네트워크를 보호하기 위해서 보안 전략에 모바일 디바이스 트래픽에 대한 침입차단시스템 정책을 포함해야 한다. 즉 모바일 디바이스로부터의 데이터와 응용 프로그램 접근 범위를 엄격하게 제한하도록 해야 한다.