aws re/start

예방: 네트워크 강화

Security Fundamentals

보안 수명 주기: 예방 - 네트워크 강화를 시작하겠습니다.

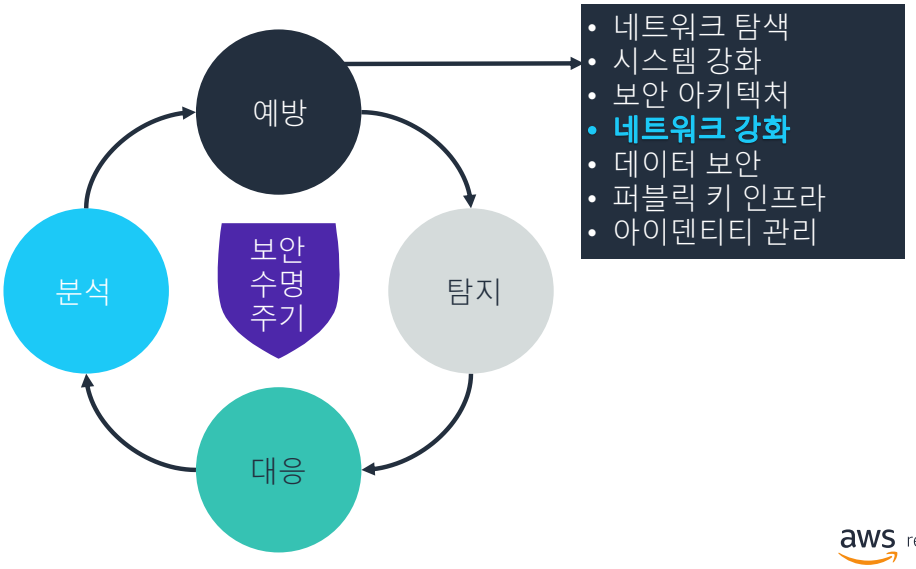
교육 내용

이 강의의 핵심

배울 내용은 다음과 같습니다.

- 네트워크 디바이스 보호 메커니즘을 나열합니다.
- 트래픽 필터링을 위한 모범 실무를 설명합니다.

보안 수명 주기: 예방



aws re/start

복습하자면 보안 수명 주기는 이렇게 구성됩니다.

- **예방** - 첫 번째 방어선입니다.
- **탐지** - 예방이 실패했을 때 수행됩니다.
- **대응** - 보안 위협이 탐지되었을 때 취해야 할 조치를 설명합니다.
- **분석** - 향후에 문제가 다시 발생하지 않도록 예방하는 새로운 조치를 구현하면서 주기가 완료됩니다.

이 강의에서는 예방 단계에서 사용할 수 있는 **네트워크 강화** 기법을 배웁니다.

원격 관리자 액세스 제어

- 네트워크 디바이스가 불법적으로 이용되면 네트워크에 심각한 영향을 미칠 수 있습니다.
  - 네트워크 디바이스에 액세스할 수 있는 사람을 제한하기 위해 AAA 솔루션을 구현합니다.
    - 엔지니어
    - 관리
    - 루트 수준 액세스
  - 원격 관리에 사용되는 프로토콜을 제한합니다.
  - 원격 관리를 수행할 수 있는 위치를 제한합니다.

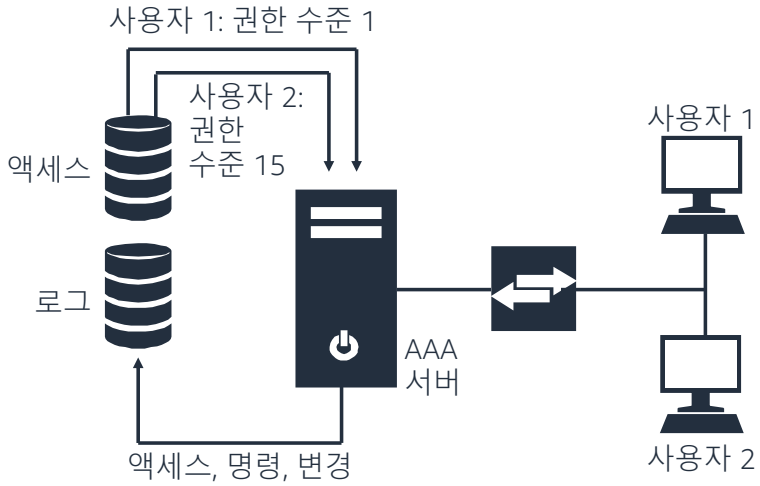
네트워크 디바이스가 불법적으로 이용되거나 비활성화되면 네트워크의 많은 부분에 영향을 미칠 수 있습니다. 따라서 잘 설계된 인증, 권한 부여, 계정 관리(AAA) 솔루션을 모든 엔지니어 및 네트워크 디바이스에 대한 관리 액세스와 루트 수준 액세스에 구현해야 합니다. 이 AAA 솔루션은 특히 네트워크 디바이스를 원격 관리하는 경우 필요합니다.

액세스 제한 방법:

- 관리 액세스가 허용된 **사람**을 제한합니다.
- 디바이스가 액세스되는 **방법**(예: 사용할 수 있는 프로토콜)을 제한합니다.
- 디바이스가 액세스되는 **위치**를 제한(예: 인터넷을 통한 원격 관리는 엄격하게 금지됨)합니다.

AAA 구현: 관리 액세스

- 네트워크 디바이스에 대한 액세스 제어에 기존 AAA 솔루션을 사용합니다.
  - 세분화된 권한 제어
  - 액세스, 명령, 디바이스 변경 사항 로깅
  - 변경 제어 프로세스 시행



aws re/start

네트워크 디바이스에 대한 액세스 제어에 AAA 솔루션을 사용하십시오. AAA 솔루션은 다음과 같은 일을 합니다.

- 액세스, 명령, 디바이스 변경 사항 로깅
- 변경 요청 관리를 위한 프로세스 시행(변경 제어)

토론: 방화벽

- 네트워크에 방화벽이 몇 개 있어야 합니까?
- 네트워크 방화벽을 어디에 배치해야 합니까?

aws re/start

방화벽의 목적을 다시 떠올려 보고 네트워크 보안 강화에 어떻게 사용할 수 있을지 생각해 보십시오.

다음 질문에 답하십시오.

1. 네트워크에 방화벽이 몇 개 있어야 합니까?

2. 네트워크 방화벽을 어디에 배치해야 합니까?

정답

1. 포괄적인 답변은 '가능한 한 많이'입니다. 구체적으로 말하자면, 네트워크 토폴로지와 보안 요구 사항에 따라 정답이 다릅니다. 디바이스의 수, 디바이스의 유형, 액세스 요구 사항, 취약성 위험과 같은 요인에 따라 달라집니다.

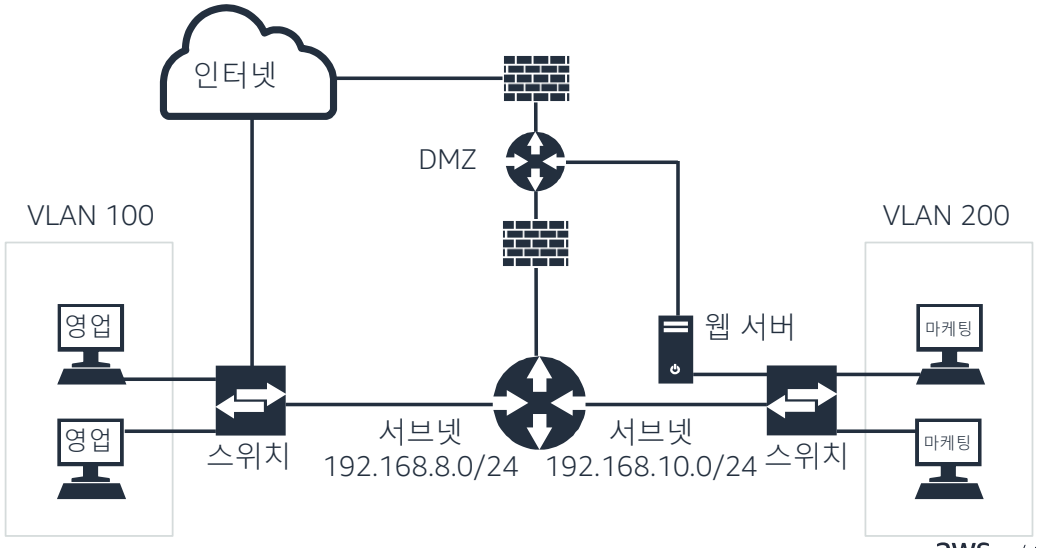
2. 악성 트래픽을 파악하거나 중단하거나 둘 다 하려면 소스와 최대한 가까운 네트워크의 교차 지점에 방화벽을 배치합니다.

네트워크 세그먼트화

- 네트워크 세그먼트화는 큰 네트워크를 작은 크기의 논리적 그룹으로 나누는 것입니다.
- 세그먼트화의 이유:
  - 더 쉬운 관리
  - 액세스 제어 세분화
  - 브로드캐스트 축소
  - 보안 향상
  - 논리적 주소의 확장성 증대

네트워크 세그먼트화는 네트워크의 보안을 향상하는 또 다른 기법입니다. 제공하는 서비스의 유형에 따라 리소스가 각기 다른 네트워크에서 호스팅됩니다. 더 작은 크기의 네트워크 수집으로 인해 보안과 확장성이 강화되고 관리가 쉬워집니다.

네트워크 세그먼트화

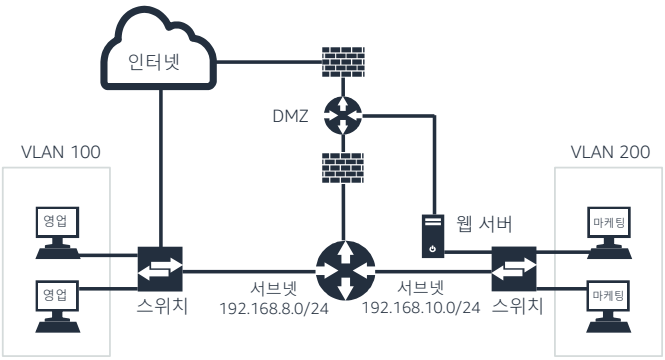


aws re/start

네트워크 세그먼트화는 네트워크의 보안을 향상하는 또 다른 기법입니다. 제공하는 서비스의 유형에 따라 리소스가 각기 다른 네트워크에서 호스팅됩니다. 더 작은 크기의 네트워크 수집으로 인해 보안과 확장성이 강화되고 관리가 쉬워집니다.

예: 네트워크 세그먼트화

- 앞서 예로 들었던 사무실 건물을 다시 예로 들자면 네트워크 세그먼트화는 사무실 건물 내의 보안 영역과 비슷합니다. 이 보안 영역에는 위험한 화학 물질이 있는 실험실, 무균실, 전기실 등이 포함됩니다.
- 각 공간에 들어가려면 스와이프 키와 규칙이 필요합니다. 무균실의 경우 감염 예방을 위해 특수한 옷을 입어야 합니다.
- 사무실 건물에 들어올 수 있는 모든 사람이 이런 보안 영역에 들어올 수 있는 것은 아닙니다.

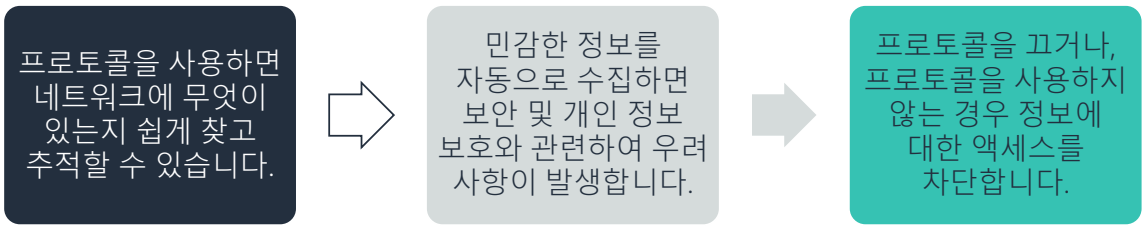


aws re/start

이전 강의에서 예로 들었던 사무실 건물을 다시 예로 들자면 네트워크 세그먼트화는 사무실 건물 내에 보안 영역을 두는 것과 비슷합니다. 이 보안 영역에는 위험한 화학 물질이 있는 실험실, 무균실, 전기실 등이 포함됩니다.

각 공간에 들어가려면 스와이프 키와 규칙이 필요합니다. 무균실의 경우 감염 예방을 위해 특수한 옷을 입어야 합니다. 사무실 건물에 들어올 수 있는 모든 사람이 이런 보안 영역에 들어올 수 있는 것은 아닙니다.

탐색 프로토콜 비활성화



aws re/start

네트워크 보안을 강화하기 위해 사용할 수 있는 또 다른 기법은 탐색 프로토콜을 비활성화하는 것입니다. 이 기법은 프로토콜을 면밀하게 모니터링하거나 제어하지 않을 경우 특히 유용합니다.

탐색 프로토콜을 비활성화하면 외부 사용자가 해당 프로토콜을 사용하여 네트워크에 관한 핵심적인 정보를 얻는 것을 예방할 수 있습니다.

탐색 프로토콜의 예는 다음과 같습니다.

- Cisco Discovery Protocol(CDP)
- Link Layer Discovery Protocol(LLDP)

보안 액세스 확립

- 안전하지 않은 프로토콜을 비활성화합니다.
  - Telnet, HTTP, SNMP v1
- 인증, 권한 부여, 계정 관리(AAA)를 사용합니다.
- 관리 트래픽이 시작될 수 있는 위치(서브넷)를 제한합니다.
- 디바이스에 직접 액세스하려고 시도하는 모든 트래픽을 중단합니다.
- AAA의 마지막 A를 기억하고 모든 액세스를 로깅합니다.

지금까지 설명한 네트워크 강화 기법을 간략하게 나열한 목록입니다.

약어
- 간이 망 관리 프로토콜(SNMP)

이 슬라이드에는 기본적인 네트워크 디바이스 보호 조치가 요약되어 있습니다.

트래픽 필터링을 위한 모범 실무

- 먼저 명시적으로 모든 트래픽을 거부한 다음 필요한 트래픽만 허용합니다.
- 신뢰할 수 있는 네트워크에서 시작된 것이 아니라면 네트워크 제어 디바이스로 향하는 트래픽을 중단합니다.
- 소스에 최대한 가깝게 필터링을 구현합니다.
  - 인터넷
  - 내부 네트워크 세그먼트
- 다른 디바이스는 적절한 역할을 수행하도록 하고 필터링이 방화벽을 기본적으로 책임지도록 합니다.
  - 심층 방어
  - 다양성 방어
- 모든 예외를 로깅합니다.

네트워크 트래픽 필터링을 위한 모범 실무를 나열한 목록입니다.

핵심 사항

- 네트워크 강화 기법은 다음과 같습니다.
  - 원격 관리 액세스 제어
  - 인증, 권한 부여, 계정 관리(AAA) 솔루션 구현
  - 방화벽을 사용하여 소스에 가장 가까운 트래픽 필터링
  - 사용하지 않거나 취약한 프로토콜 비활성화
  - 네트워크를 서브넷으로 세그먼트화
- 디바이스에 대한 물리적 액세스와 논리적 액세스를 모두 보호합니다.

aws re/start

다음은 이 강의의 핵심 요점입니다.

- 네트워크 강화 기법은 다음과 같습니다.
  - 원격 관리 액세스 제어
  - 인증, 권한 부여, 계정 관리(AAA) 솔루션 구현
  - 방화벽을 사용하여 소스에 가장 가까운 트래픽 필터링
  - 사용하지 않거나 취약한 프로토콜 비활성화
  - 네트워크를 서브넷으로 세그먼트화
- 디바이스에 대한 물리적 액세스와 논리적 액세스를 모두 보호합니다.