aws re/start

예방: 보안 아키텍처

Security Fundamentals

보안 수명 주기: 예방 - 보안 아키텍처를 시작하겠습니다.

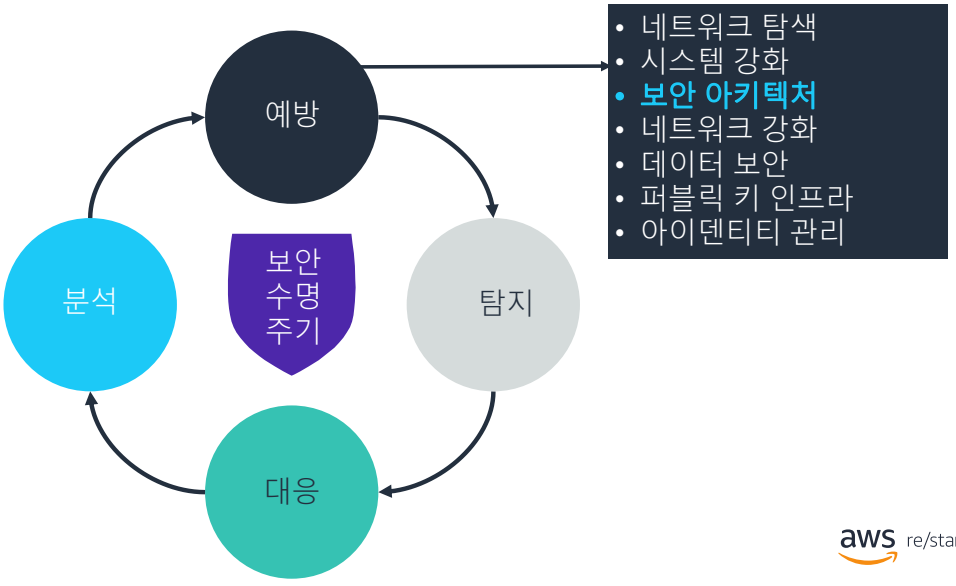
교육 내용

이 강의의 핵심

배울 내용은 다음과 같습니다.

- 네트워킹 디바이스와 네트워킹 디바이스의 보안 용례를 파악합니다.
- 네트워크 영역의 작동 원리를 설명합니다.
- 네트워크 수준의 보안 가능성을 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 문제를 탐지했을 때 어떤 조치를 취할지 설명합니다.
- **분석** - 향후에 문제가 다시 발생하지 않도록 예방하는 새로운 예방 조치를 구현하면서 수명 주기가 완료됩니다.

이 강의에서는 **보안 아키텍처**에 관한 의사결정이 네트워크 리소스를 보호하고 보안 위협을 예방하는 데 어떻게 도움이 되는지 알아봅니다.

보안 아키텍처

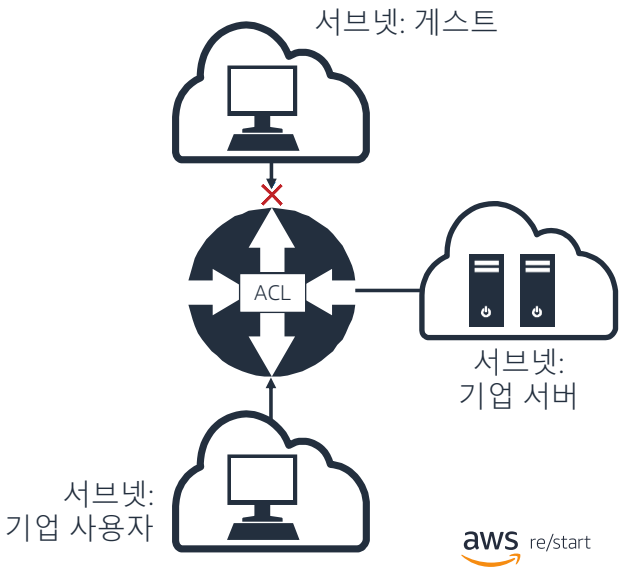
- 개방형 시스템 간 상호 접속(OSI) 모델 전체에서 보안을 강화하는 기술의 집합입니다.
- 올바른 보안 아키텍처에서는 다음을 사용합니다.
  - 관리적 제어
  - 기술적 제어
  - 물리적 제어

보안 아키텍처는 네트워크 계층에서 보안을 강화하는 기술의 집합입니다. 솔루션마다 각기 다른 역할을 수행하여 네트워크를 안전하게 보호함으로써 침입 시도를 어렵게 하고 트래픽이 올바른 방향으로 흐르도록 합니다.

다음 주제에서는 안전한 네트워크 아키텍처를 만드는 데 사용할 수 있는 도구와 기법을 살펴보겠습니다.

라우터

- 라우터:
  - 기본 라우팅과 필터링 함수를 실행함
  - 액세스 제어 목록(ACL)을 사용하여 트래픽을 필터링함
  - 서브넷을 통해 네트워크 세그먼트화를 지원함
  - 정보를 빠르게 처리하지만 고급 필터링 기술을 사용하지 않음

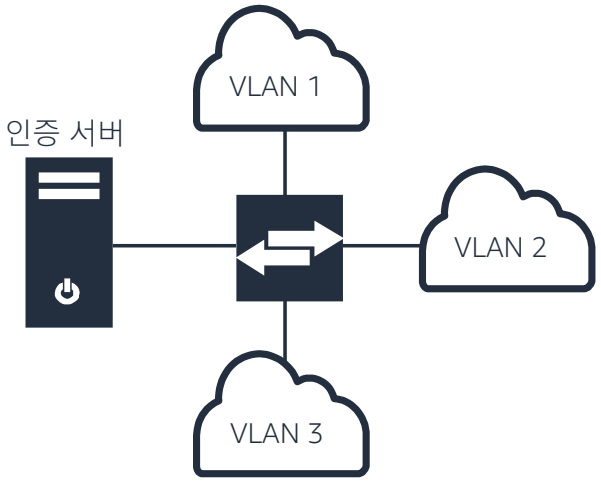


네트워크를 보호하려면 라우터의 기본적인 필터링 함수를 사용하십시오. 네트워크에서 허용된 트래픽을 제한하기 위해 액세스 제어 목록(ACL)을 사용할 수 있습니다. 구체적으로 ACL은 네트워크에 대한 액세스를 허용하거나 거부하는 규칙을 정의합니다.

서브넷은 네트워크에서 식별 가능한 부분입니다. 네트워크를 개별 서브넷으로 세그먼트화하면 네트워크의 일부를 격리하는 아키텍처를 설계할 수 있습니다. 이 아키텍처에서 서브넷에 서로 다른 보안 액세스 수준을 할당할 수 있습니다.

스위치

- 스위치:
  - 네트워크에 대한 물리적 액세스를 세그먼트화 및 제어함
  - 컴퓨터를 그룹화하여 가상 광역 네트워크(VLAN)를 만듦
  - 디바이스 인증을 지원함
  - 네트워크 플러딩을 예방함
- 계층 3(네트워크 계층) 스위치는 라우팅과 스위칭 함수를 모두 실행합니다.

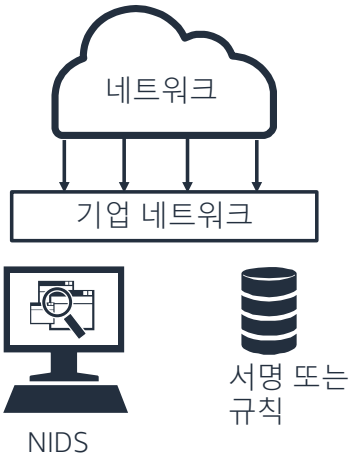


aws re/start

라우터와 마찬가지로 스위치를 사용하여 네트워크를 세그먼트화하고 가상 광역 네트워크(VLAN)를 만들 수 있습니다. VLAN을 사용하면 같은 물리적 네트워크에 연결된 디바이스가 별도의 네트워크에 있는 것처럼 보이게 할 수 있습니다. 이 기능을 사용하여 서로 다른 액세스 요구 사항을 기반으로 네트워크의 각 부분을 보호하는 네트워크 아키텍처를 설계할 수 있습니다.

네트워크 기반 침입 탐지 시스템

- NIDS라고도 합니다.
- NIDS의 특징은 다음과 같습니다.
  - 네트워크 활동을 모니터링함
  - 서명과 규칙을 사용하여 악의적인 패턴을 탐지함
  - 로컬 데이터베이스를 사용하여 실시간 이벤트를 식별함
  - 거짓 경고를 최소화하도록 구성해야 함
  - 네트워크 어플라이언스 또는 애플리케이션으로 설치할 수 있음



aws re/start

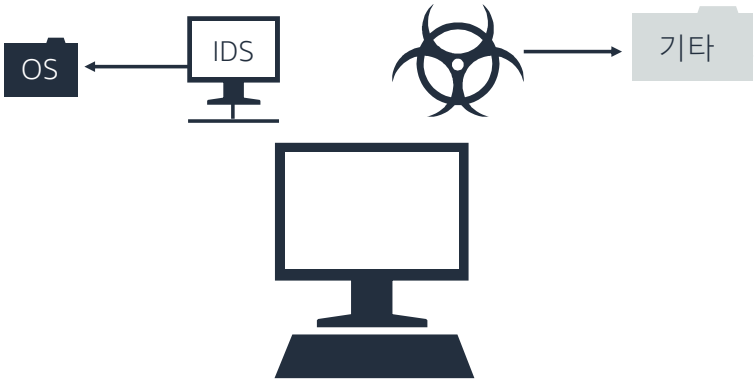
네트워크 기반 침입 탐지 시스템(NIDS)은 트래픽과 프로토콜의 이상 현상을 식별하고 보고하기 위해 실시간 네트워크 트래픽을 스캔합니다. NIDS는 **서명 기반** 탐지와 **행동 기반** 탐지를 조합하여 사용합니다.

서명 기반 탐지는 네트워크 트래픽을 알려진 악의적 패턴의 데이터베이스와 비교하여 일치하는 경우 알립니다. 알려지지 않은 이벤트에 대해서는 효과적이지 않다는 점이 단점입니다.

알려지지 않은 이벤트에 대한 보호를 위해 **이상 현상 기반** 탐지라고도 하는 **행동 기**반 탐지를 사용할 수 있습니다. 이 탐지 유형은 **규칙** 세트 또는 알려진 기준을 사용하여 이상 현상, 즉 일반적이지 않은 현상을 탐지합니다.

호스트 기반 침입 감지 시스템(HIDS)

- 중요한 파일을 보호합니다.
- 조작된 컴퓨터 상태로 인한 행동 변화를 예방합니다.
- 악성 소프트웨어를 식별합니다.
- 바이러스 백신 소프트웨어를 보완합니다.



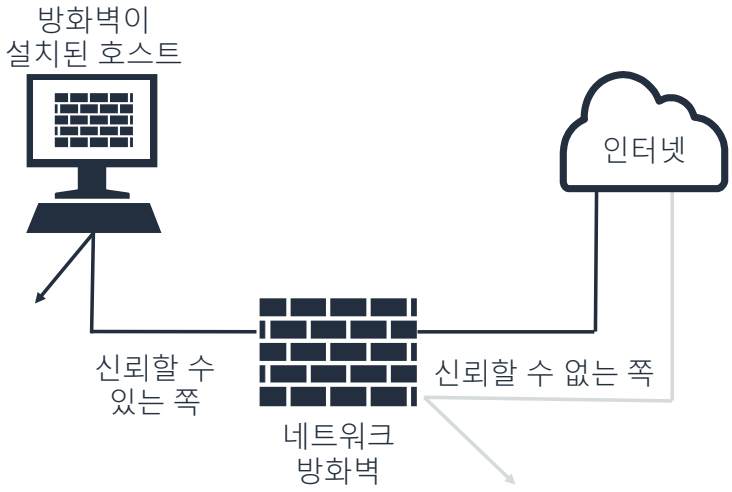
aws re/start

호스트 기반 침입 탐지 시스템은 바이러스 백신 솔루션을 보완합니다. 보완하는 방법은 다음과 같은 특수한 위협을 탐지하기 위해 핵심적인 시스템 파일을 추가로 스캔하는 것입니다.

- 백도어 위협: 공격자가 일반적인 보안 검사를 우회하여 시스템에 액세스할 수 있게 하는 취약성
- 루트킷 위협: 공격자가 탐지되지 않는 방법으로 권한이 있는(루트) 사용자로 시스템에 액세스할 수 있게 하는 취약성

방화벽

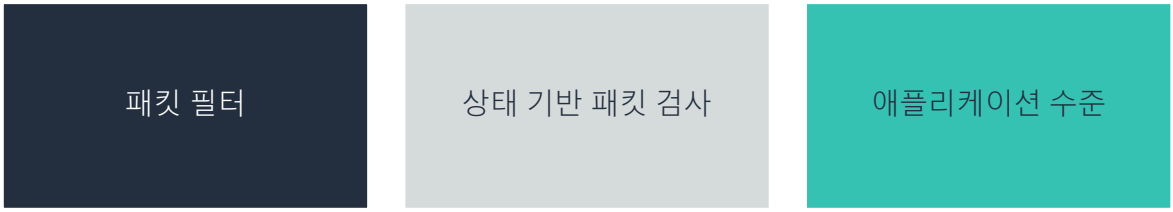
- 네트워크 또는 호스트 간 트래픽을 허용하거나 허용하지 않습니다.
  - 네트워크 방화벽은 두 서브넷 간의 패킷을 필터링함
  - 호스트 방화벽은 호스트로 향하는 패킷을 필터링함
- 어플라이언스일 수도 있고 소프트웨어로 설치될 수도 있습니다.



aws re/start

방화벽은 보안 아키텍처의 필수 요소입니다. 방화벽은 네트워크 트래픽 제어에 도움이 되는 규칙과 예외를 생성할 수 있게 합니다. 아키텍처의 적절한 위치에 방화벽을 배치하고 활성화 상태를 유지하도록 하십시오.

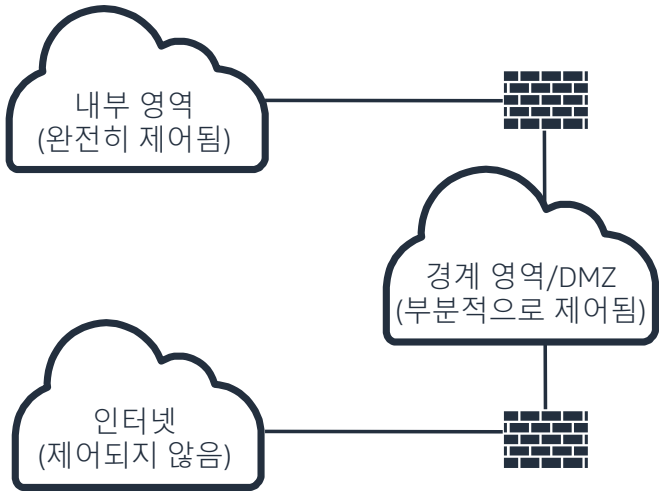
방화벽 범주



방화벽의 다양한 범주가 슬라이드에 나와 있습니다. 패킷 필터는 상대적으로 속도가 빠릅니다. 반면, 상태 기반 검사는 속도가 가장 느리지만 더 정교한 이벤트를 탐지합니다.

네트워크 영역

- 네트워크 영역은 일반적인 보안 속성이 있는 지정된 영역입니다. 영역은 다음과 같을 수 있습니다.
  - 완전히 제어됨
  - 부분적으로 제어됨
  - 제어되지 않음



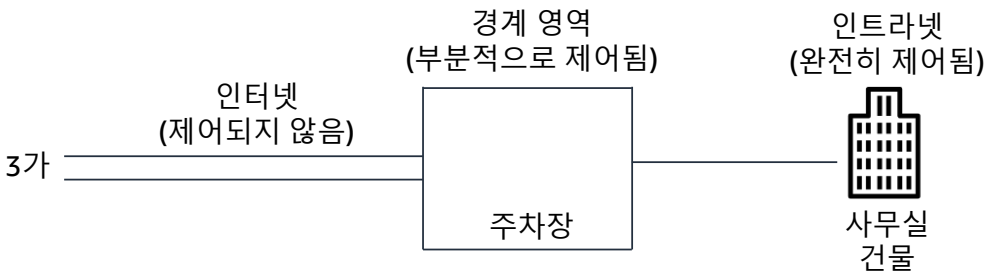
aws re/start

인트라넷은 **완전히 제어되는** 영역의 예입니다.

비무장 지대(DMZ)라고도 하는 **경계 영역**은 **부분적으로 제어되는** 영역의 예입니다.

인터넷은 **제어되지 않는** 영역의 예입니다.

예: 네트워크 영역



aws re/start

사무실 건물을 생각해 보십시오.
- 인터넷은 건물 밖의 거리로 비유할 수 있습니다. 누구나 접근할 수 있는 공동 영역이며, 여기에서 일어나는 일은 건물 안의 회사에서 제어할 수 없습니다.
- 경계 영역은 주차장과 접견실에 비유할 수 있습니다. 여기에 있는 리소스 중 일부에는 대중이 접근할 수 있습니다. 예를 들어, 사람들이 방문자용 주차장에 주차를 하거나 접견실에 들어와 화장실이나 음수대를 이용할 수 있습니다. 그러나 방문자가 할 수 있는 일에는 제한이 있으며, 사람들을 이곳에서 내보낼 권한은 회사에 있습니다.
- 접견실을 지나면 나오는 본 건물은 인트라넷에 비유할 수 있습니다. 이 공간은 완전히 제어됩니다. 권한이 있는 직원만 여기에 들어올 수 있습니다. 직원이 들어오기 위해서는 배지가 필요합니다.

인트라넷 영역

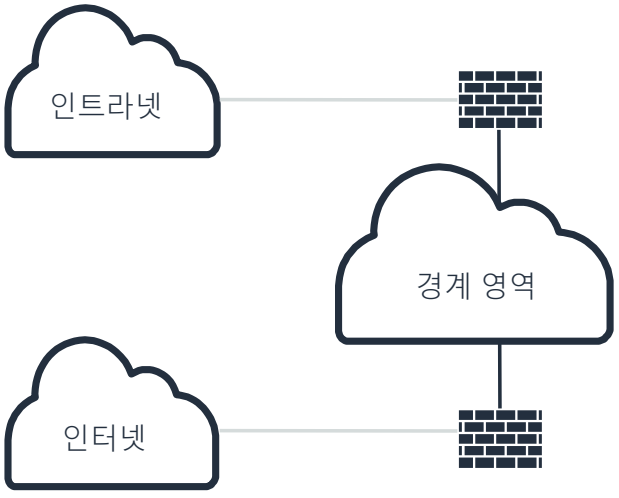
인트라넷에 일반적으로 설치되고 구성되는 자산 또는 서비스 유형:

- 디렉터리 서비스
- 원격 관리 인벤토리
- 동적 호스트 구성 프로토콜(DHCP)
- 도메인 이름 시스템(DNS)
- 모니터링 서버
- 내부적으로 사용되는 애플리케이션을 호스팅하는 웹 서버
- 파일 서버
- 아이덴티티 페더레이션 서버
- 정책 서버
- 관리형 맬웨어 백신
- 소프트웨어 활성화 서버
- 애플리케이션 및 운영 체제 배포 서비스
- 가상화 호스트
- 데이터베이스 서버

클라우드가 아닌 온프레미스 리소스를 사용하는 조직에서 대부분의 인프라는 인트라넷 쪽에 있습니다.

경계 영역

- 경계 영역은 신뢰 수준이 다른 두 영역 사이에서 완충지대 역할을 합니다.
- 경계 영역의 구성 유형:
  - 백투백
  - 삼각



aws re/start

경계 영역의 일반적인 구성 유형은 다음과 같습니다.

- **백투백** - 두 개의 방화벽 사이에 경계 영역이 배치됩니다. 슬라이드의 그림에는 외부 방화벽과 내부 방화벽이 나와 있습니다.
- **삼각** - 경계 영역이 내부 네트워크를 보호하는 같은 방화벽 뒤에 있습니다.

경계 영역 디바이스

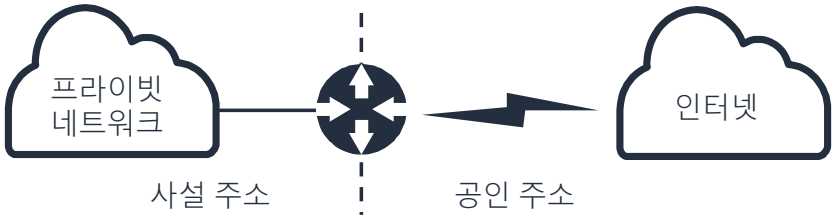
경계 영역 서브넷의 시스템 역할:

- 웹 서버
- 터미널 서비스 게이트웨이
- Remote Authentication Dial-In User Service(RADIUS) 클라이언트
- 파일 전송 프로토콜(FTP) 서버
- 음성 인터넷 프로토콜(VoIP) 게이트웨이
- 원격 액세스 서버
- 이메일 릴레이
- 디렉터리 서버
- 무선 액세스 포인트
- 도메인 이름 시스템(DNS)
- 디렉터리 동기화
- 페더레이션 프록시
- 리버스 프록시
- 인증 서비스

경계 영역에 일반적으로 존재하는 디바이스의 목록입니다.

네트워크 주소 변환

- NAT는 사설 주소를 공인 주소로 변환합니다.
- NAT는 기본적으로 네트워킹 디바이스가 수행합니다.
- PAT는 여러 사설 주소를 하나의 공인 주소와 연결합니다.
- NAT에는 몇 가지 한계가 있습니다. (IPv6에서는 사용되지 않을 가능성이 있음)



네트워크가 퍼블릭 서브넷과 프라이빗 서브넷으로 세그먼트화되는 경우 네트워크 주소 변환(NAT)이 필요합니다. NAT는 내부적으로 공인 IP 주소를 사설 IP 주소로, 사설 IP 주소를 공인 IP 주소로 변환합니다.

약어:

- 포트 주소 변환(PAT)

네트워크 액세스 제어 목록

- 네트워크 액세스 제어 목록(네트워크 ACL)은 보호된 세그먼트에 연결된 시스템을 검사하여 보안 정책을 준수하는지 확인합니다.
- 네트워크 ACL의 역할은 다음과 같습니다.
  - 바이러스 백신을 확인함
  - 방화벽이 활성화되어 있도록 함
  - 스파이웨어 백신을 확인함

잘 설계된 네트워크 보안 아키텍처의 중요한 요소 중 하나는 네트워크 액세스 제어 목록(네트워크 ACL) 솔루션을 제공하는 것입니다. 네트워크 ACL 시스템은 네트워크 리소스의 규정 준수를 검사합니다. 네트워크 ACL은 규정을 준수하지 않는 디바이스를 자동으로 격리하거나 안전하지 않은 노드가 네트워크를 감염시키지 못하도록 합니다.

핵심 사항

- 아키텍처 설계는 네트워크의 보안 태세에 영향을 미치며 위협을 예방하는 데 사용될 수 있습니다.
- 라우터 및 스위치의 필터링과 액세스 제어 기능을 사용하여 네트워크 보안을 구현합니다.
- 방화벽과 네트워크 세그먼트화는 네트워크를 보호하는 데 효과적인 방법입니다.

aws re/start

이 강의에서 다룬 핵심 사항은 다음과 같습니다.

- 아키텍처 설계는 네트워크의 보안 태세에 영향을 미치며 위협을 예방하는 데 사용될 수 있습니다.
- 라우터 및 스위치의 필터링과 액세스 제어 기능을 사용하여 네트워크 보안을 구현합니다.
- 방화벽과 네트워크 세그먼트화는 네트워크를 보호하는 데 효과적인 방법입니다.