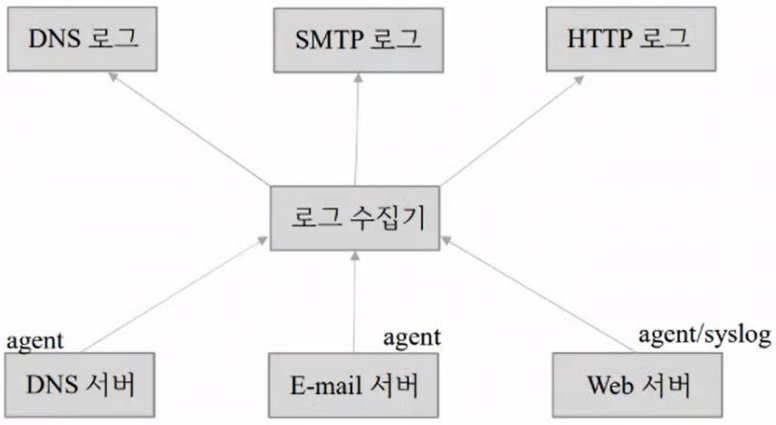
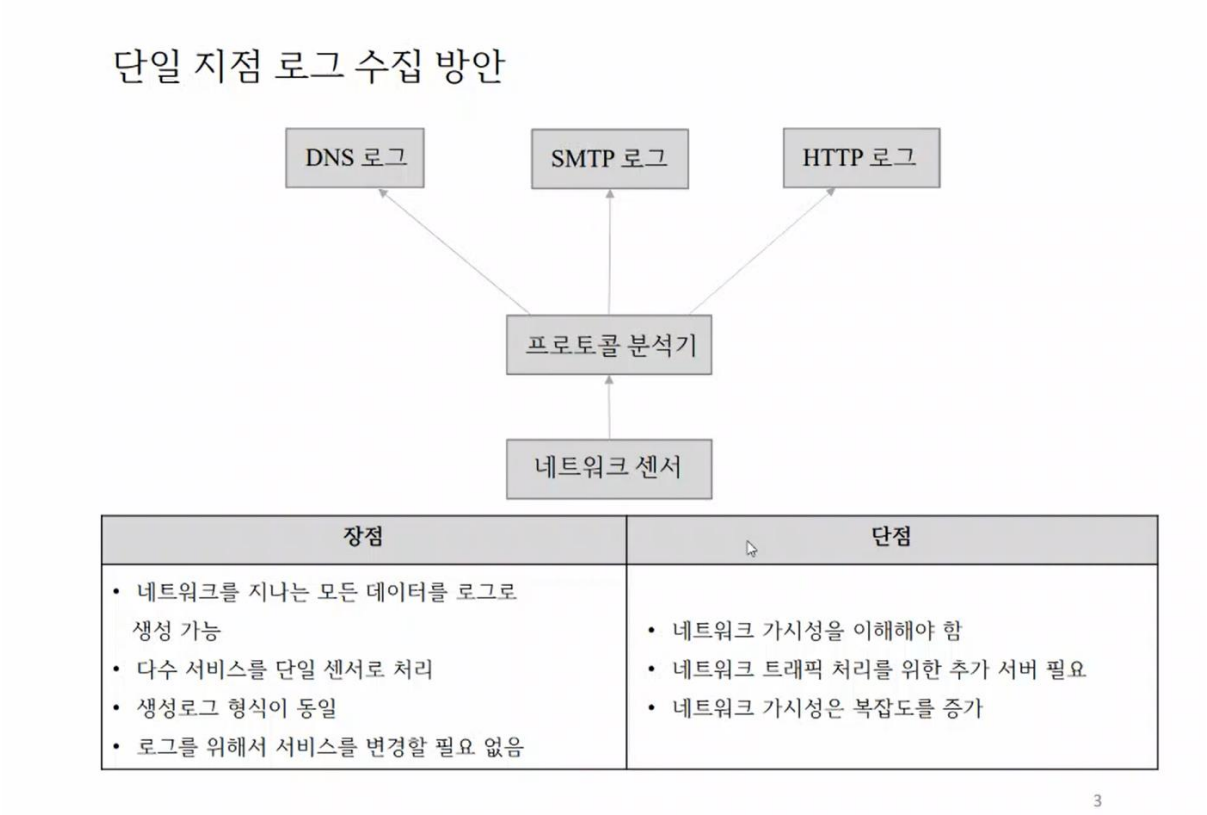
로그 수집 전략

- 다중 지점 로그 수집 방안
  - 내부에서 운영하는 애플케이션이 개별적으로 로그를 전송
  - 개별 수집 프로그램이나 syslog를 이용해서 로그 전송
- 단일 지점 로그 수집 방안
  - 네트워크 센서에서 트래픽을 직접 입력받아 로그 생성하고 이를 색인 시스템으로 전송
  - 네트워크 센서는 프로토콜 분석까지 수행하고 서비스별 로그를 생성
  - Zeek프로그램 하나만 갖고도 DNS, SMTP, HTTP를 모두 분석 가능

다중 지점 로그 수집 방안



장점	단점
• 이해하기 쉬움 • 단순한 구축이 가능 • 네트워크 구조에 비의존적	• 시스템 관리가 어려움 • 관리자가 아는 항목만 수집 • 별도 서비스마다 수집해야 함 • 서비스 별 로그 형식이 다름



-zeek 이란 애를 쓸것임

다중지점과 단일지점의 가장 큰 차이 : 다중지점이 수집하는 로그는 로그 데이터, 단일지점은 일반 데이터를 로그로 만들어서 저장

일반 데이터 수집 ➔ 정규화 ➔ 로그데이터 변환 ➔ 로그별로 그룹핑

일반데이터

로그 데이터

서로 다르다.

TCP 헤더 / UDP 헤더 / IP 헤더

+데이터 / + 데이터 / + 데이터

Ethernet Header + IP header + TCP header + DATA => 일반데이터

2023-0726-1034 localhost 1234 ..... -> 로그데이터

수집 로그 종류

- Network log

  - 라우터, 스위치, 방화벽 등과 같이 네트워크 계층에서 수집한 로그

- Endpoint log

  - 하위 연결이 더 이상 없는 PC와 서버에서 수집한 로그

Network log	Endpoint log
비교적 소수의 장비 관리가 용이	많은 수의 장비 관리가 어려움
데이터 접점이 적음	데이터 접점이 많음
암호화 패킷을 분석 할 수 없음	Endpoint에서는 암호화 해재