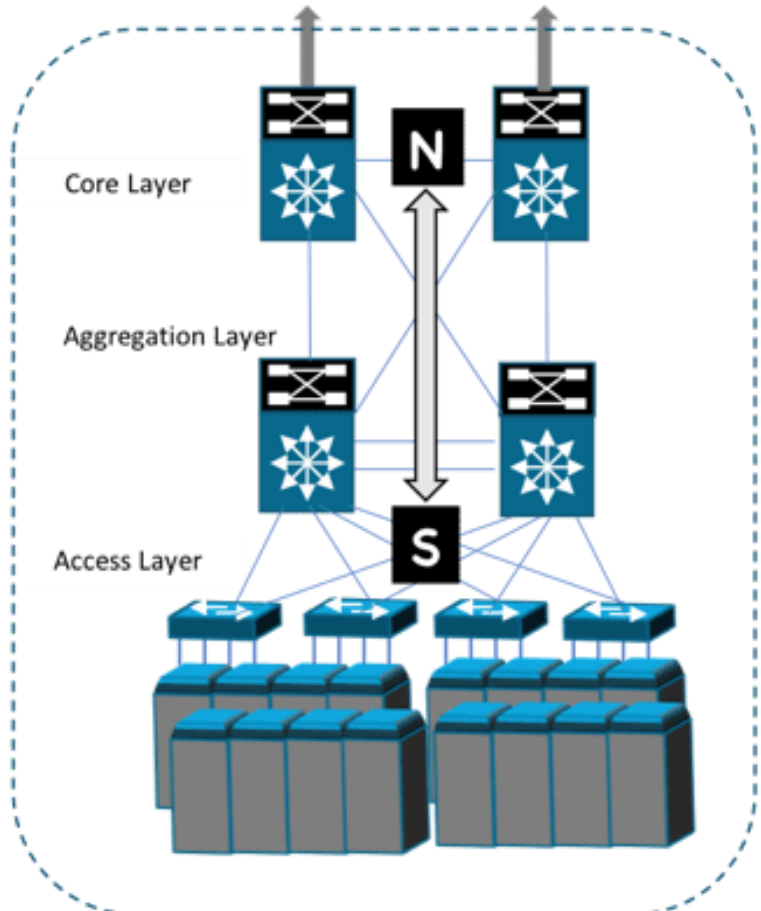


“

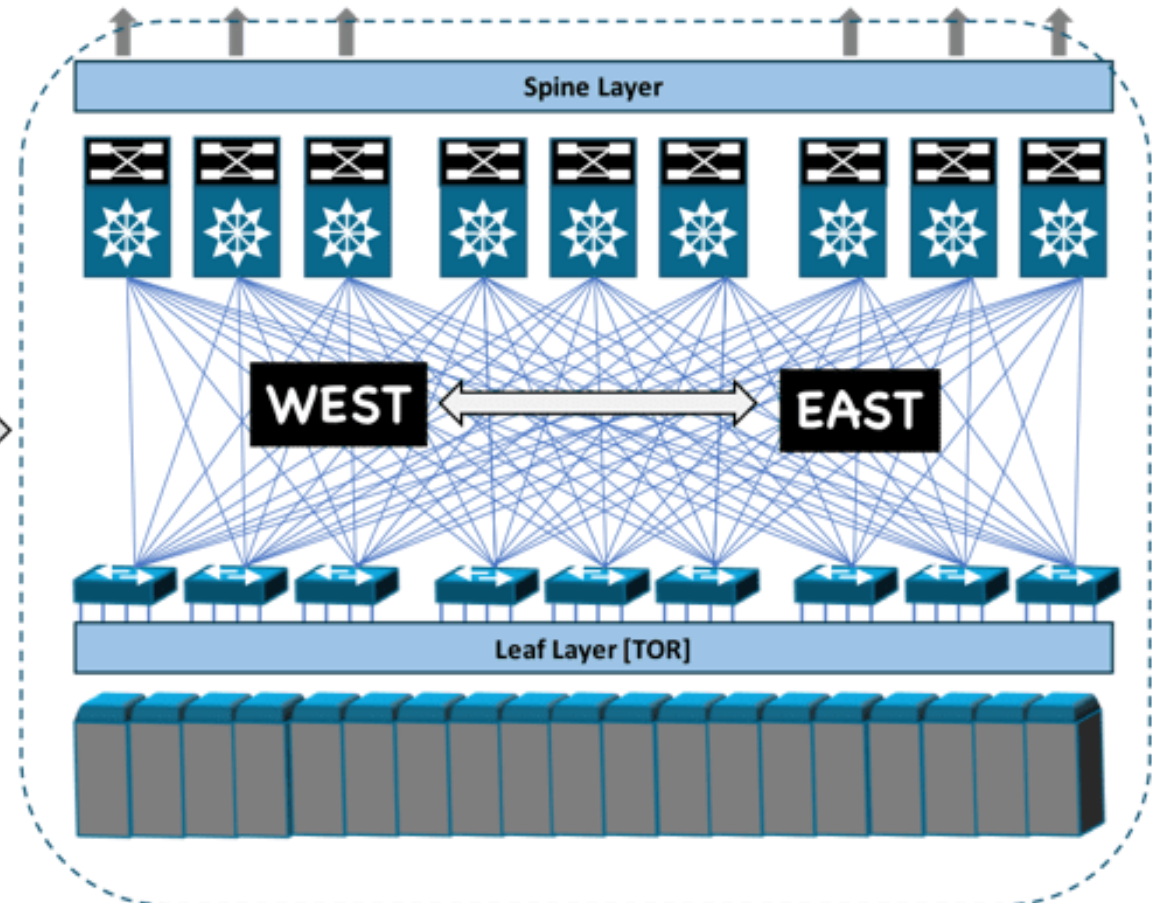
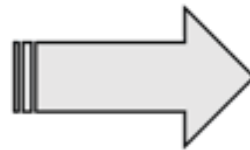
# Flow Microsegmentation



# Network Traffic Trend 변화



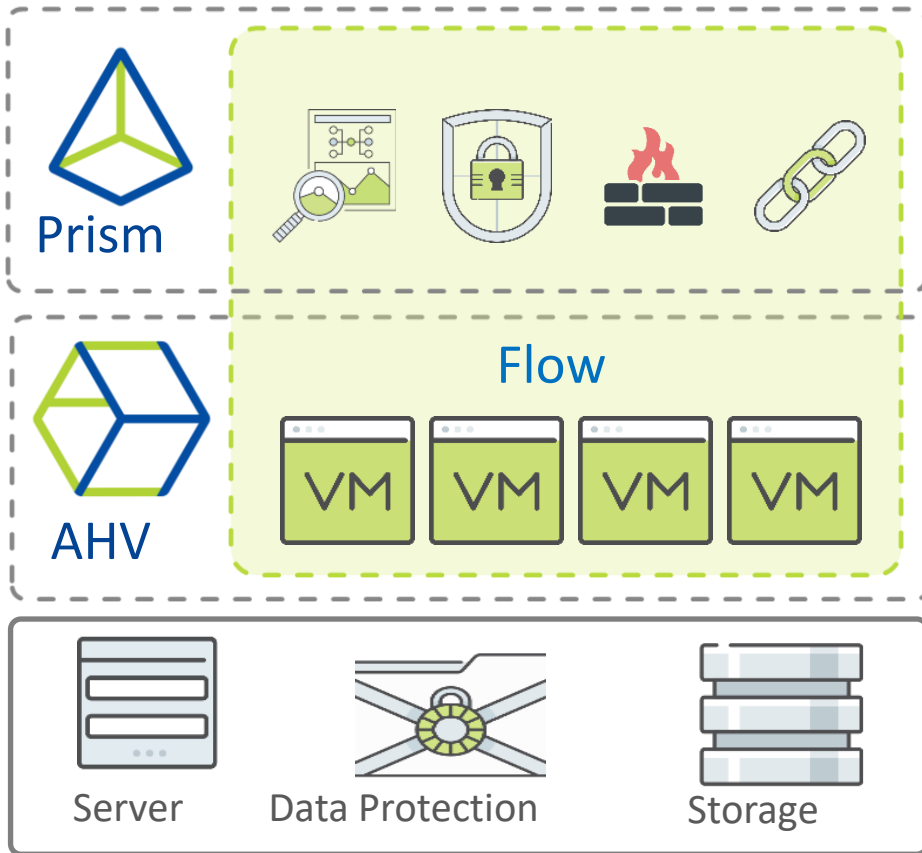
Traditional Datacenter: 3-Tier Topology



Cloud Datacenter: Leaf-Spine Topology



# Flow: 엔터프라이즈 클라우드의 네트워킹



- Nutanix Enterprise Cloud 포함
- 강력한 시각화, 정책, 마이크로세그멘테이션 및 네트워크 자동화 기능
- 별도의 도구가 필요 없는 직관적이고 확장 가능한 솔루션
- 원-클릭의 단순성

포괄적인 가시성, 보안 및 자동화



# Flow: Overview

5

중앙 관리, 운영, 거버넌스

4

웹, 애플리케이션 및 DB에 대한 정책 정의 그룹의 모든 기존 VM 과 새 VM 에 자동 적용되는 정책은 각 노드의 로컬 적용을 위해 Push됨

3

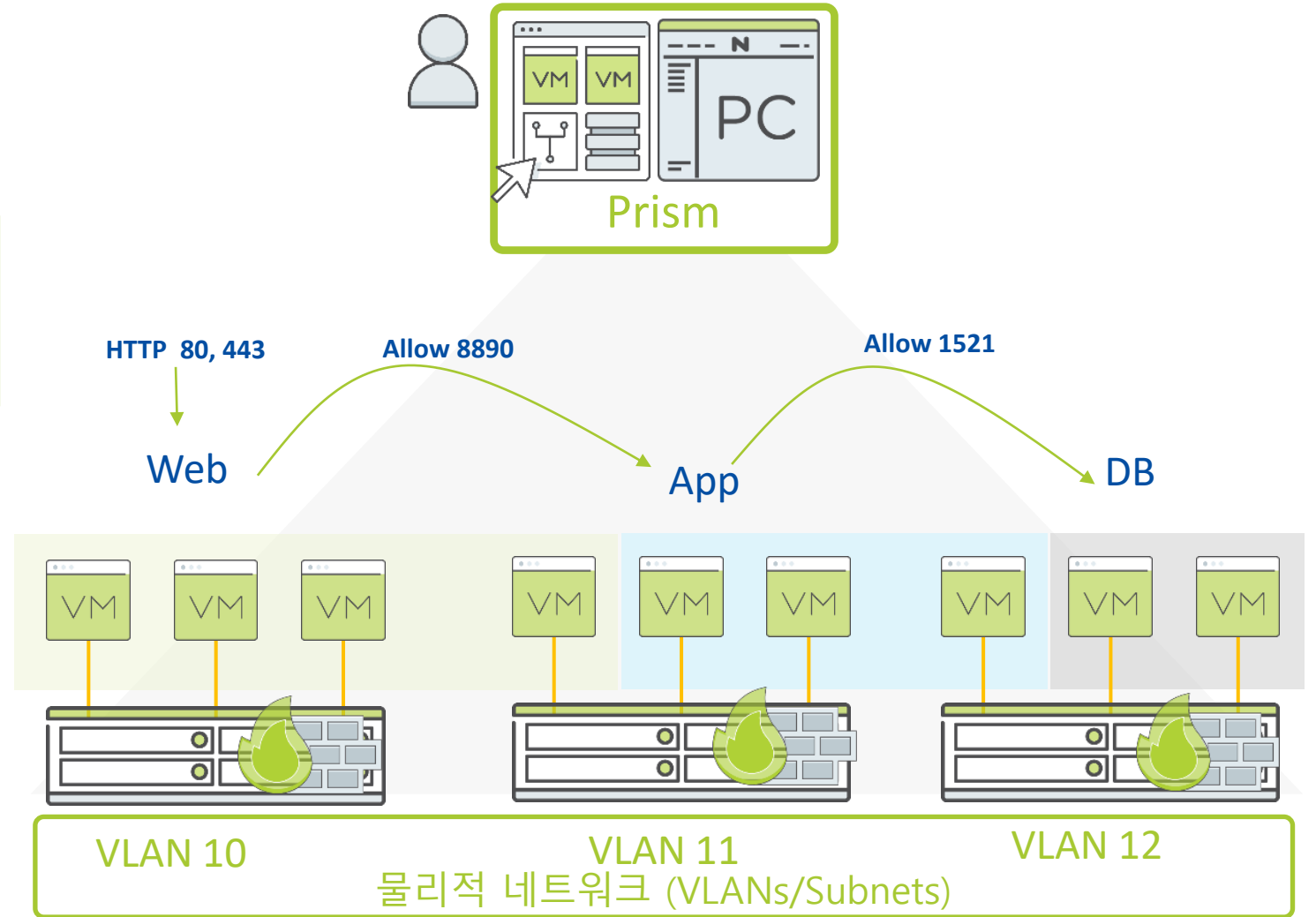
애플리케이션 토폴로지 기반의 VM 그룹화 (물리적 인프라, VLAN, 서브넷과 독립적)

2

별도 추가 설치 없이 라이선스 활성화를 통해 사용

1

기존 물리적 인프라와 함께 작동

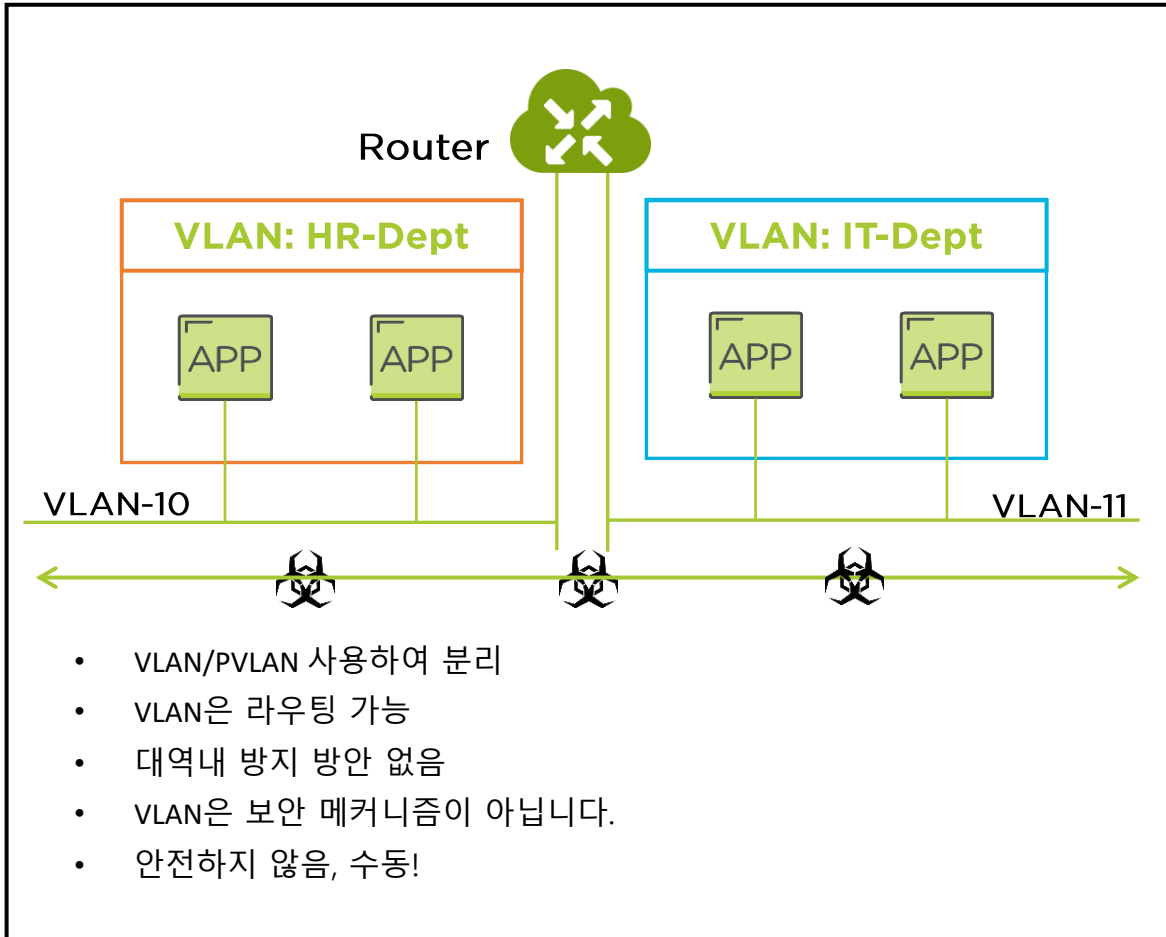


# Use Cases and Scenarios

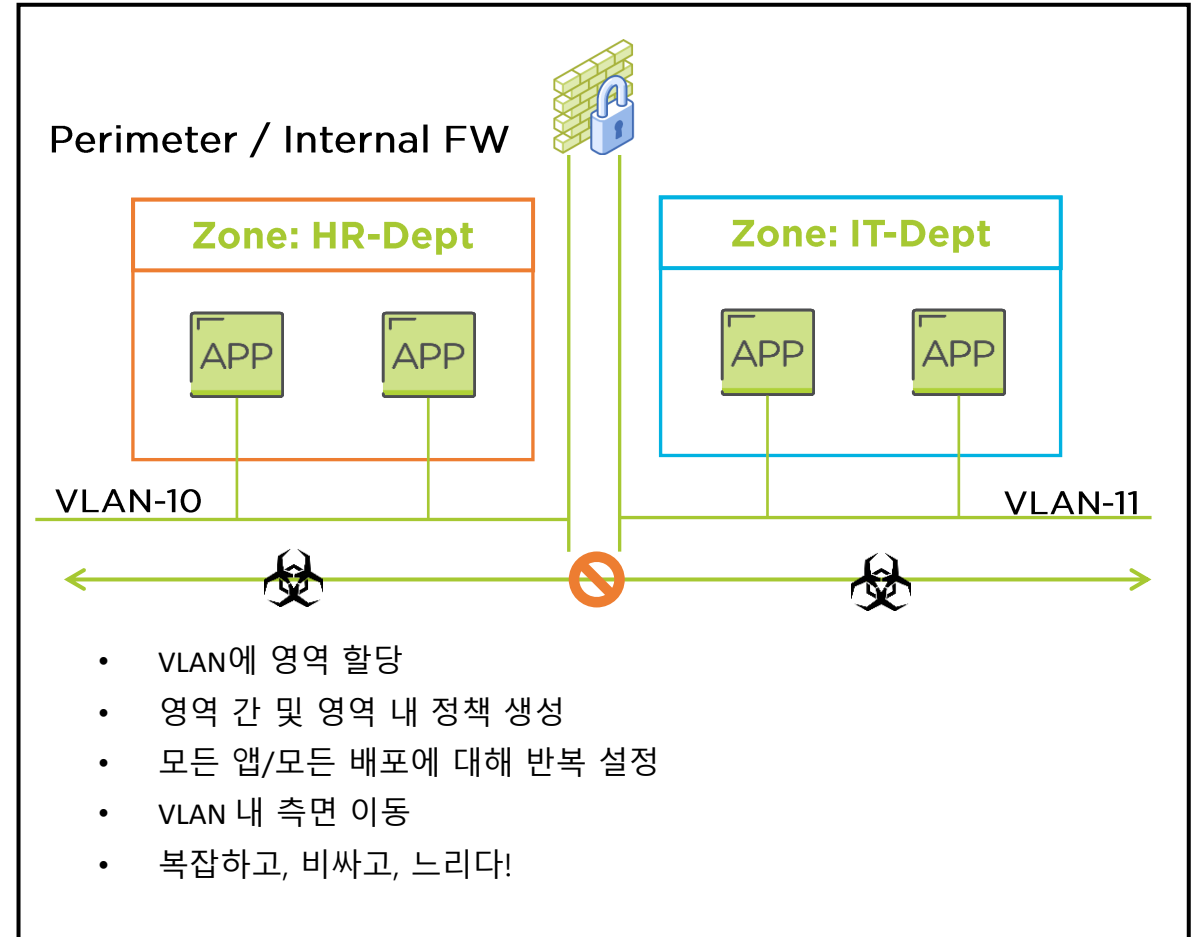


# 전통적인 격리 환경 구성

## VLAN 기반의 Isolation



## Firewall Zones



# Flow: 격리 환경 구성

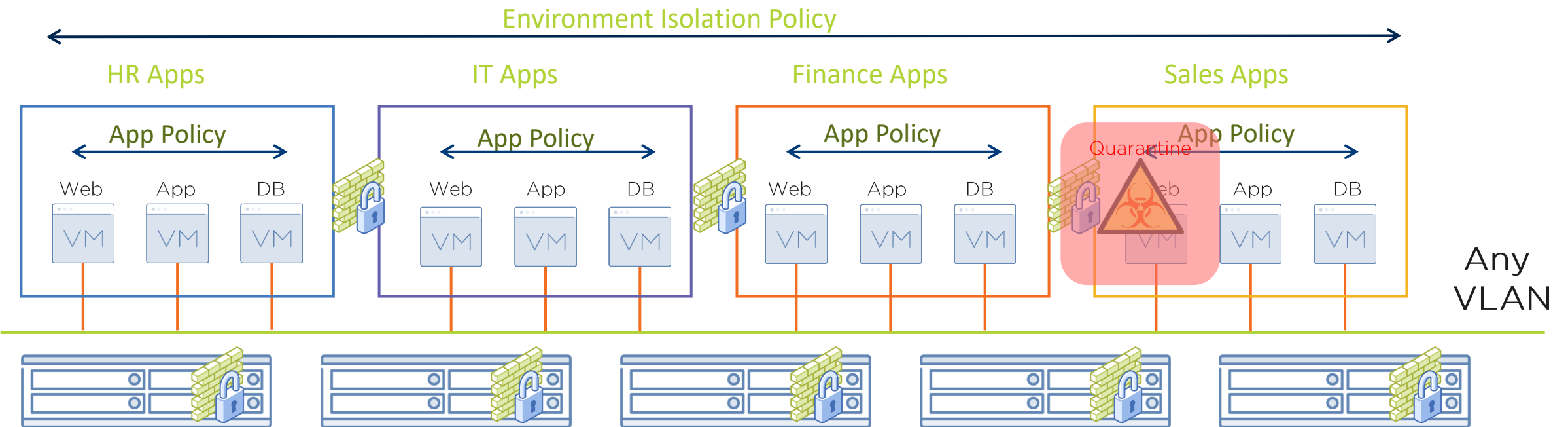


Prism

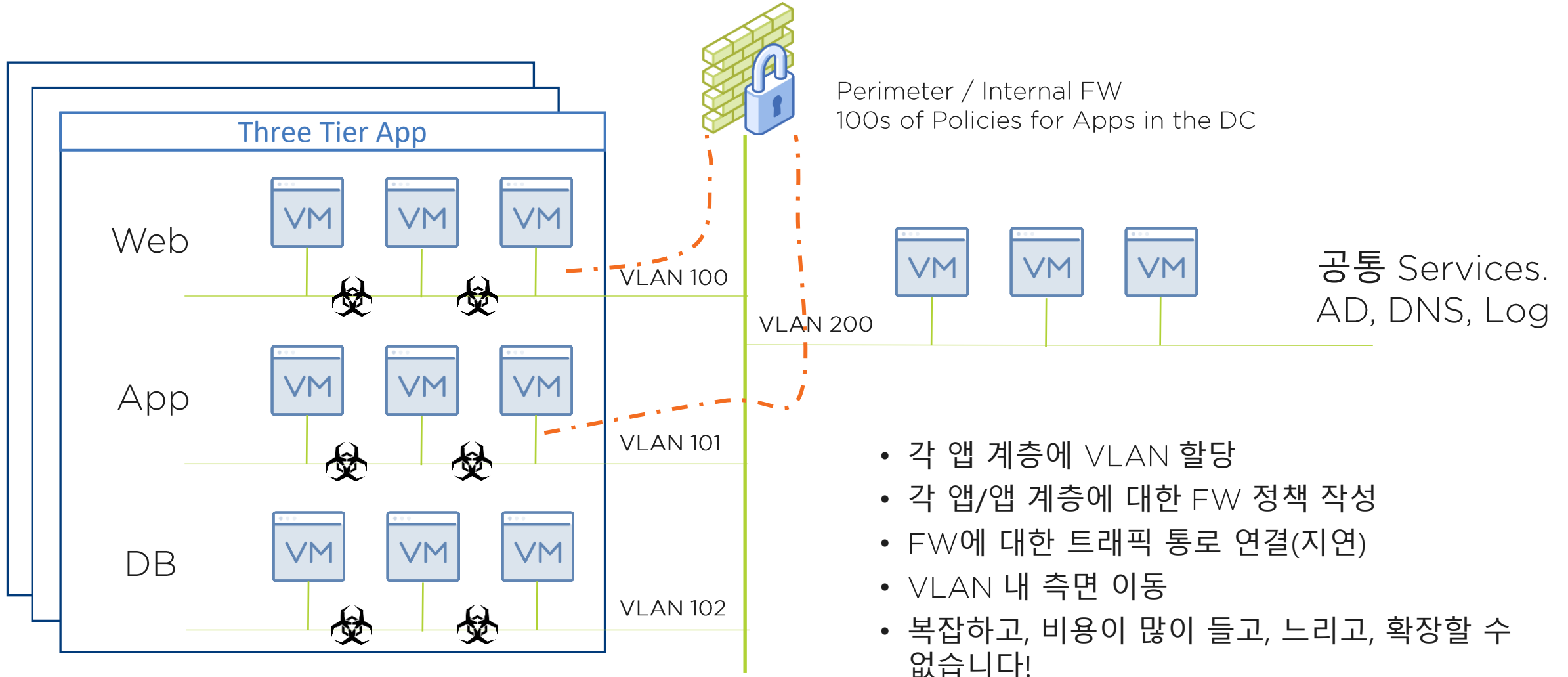


Flow

- 환경에 따른 VM 식별 (IT, HR, Sales..)
- 환경을 위한 격리 정책 정의
  - 인바운드에 대한 최소 권한 (트래픽 허용 안 됨)
- VM을 "Quarantine"로 설정하면 격리 정책 적용



# 전통적인 App 세그멘테이션

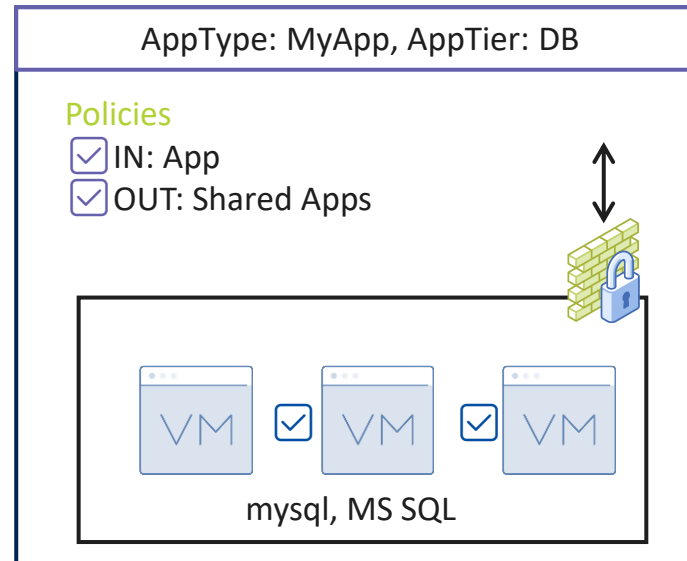
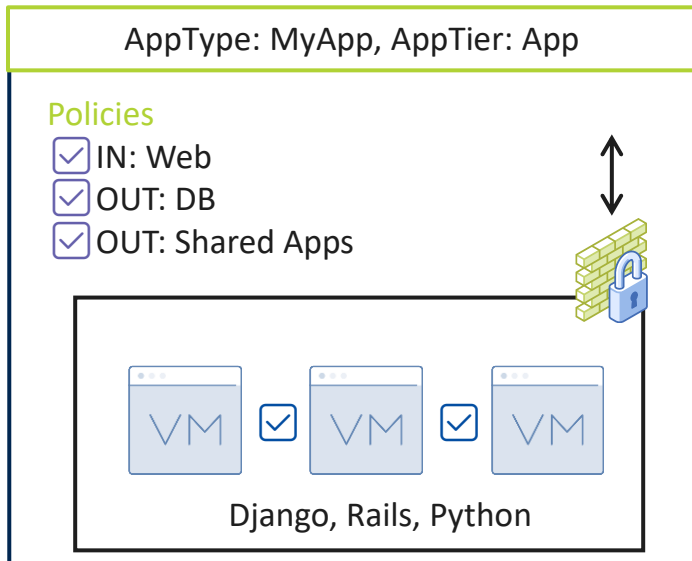
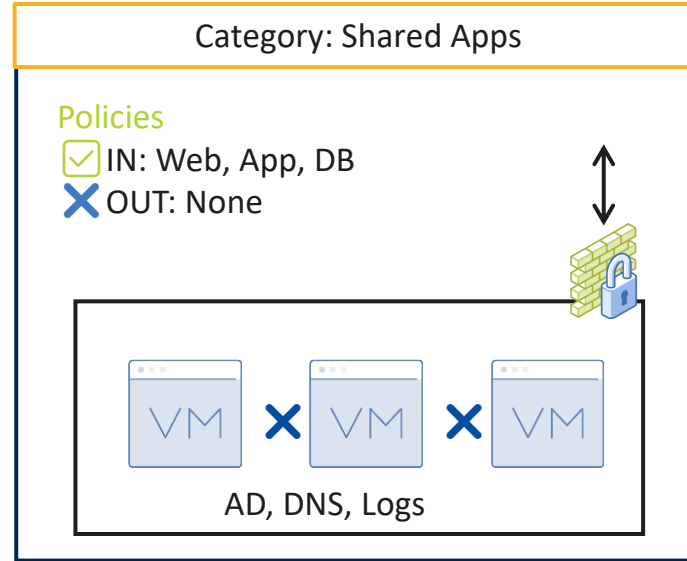
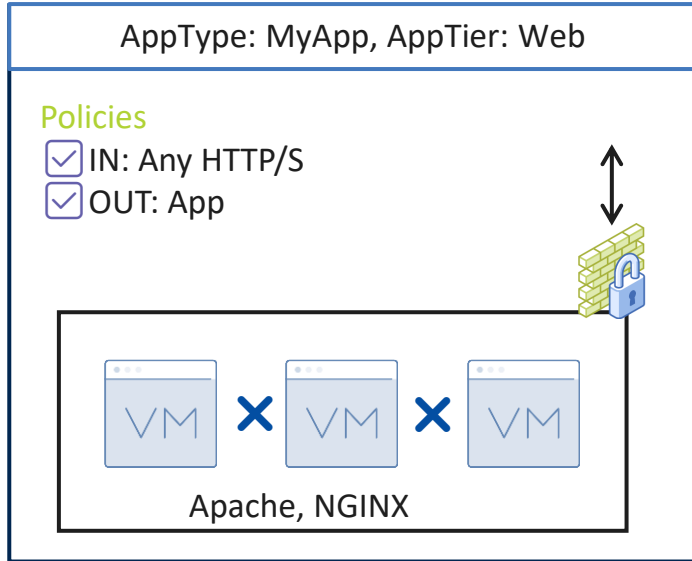


- 각 앱 계층에 VLAN 할당
- 각 앱/앱 계층에 대한 FW 정책 작성
- FW에 대한 트래픽 경로 연결(지연)
- VLAN 내 측면 이동
- 복잡하고, 비용이 많이 들고, 느리고, 확장할 수 없습니다!





# Flow: 애플리케이션 세그멘테이션

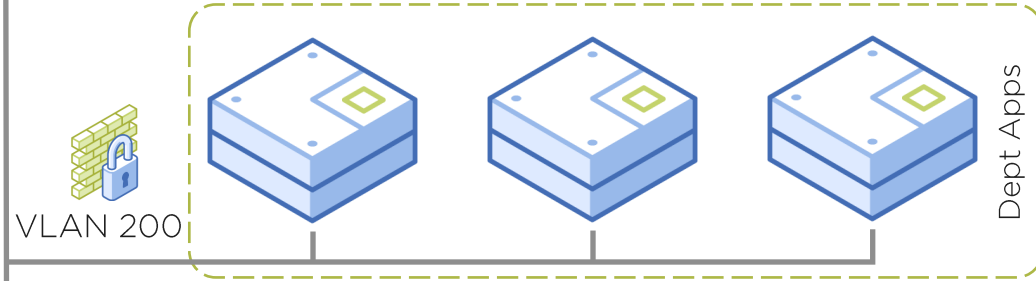
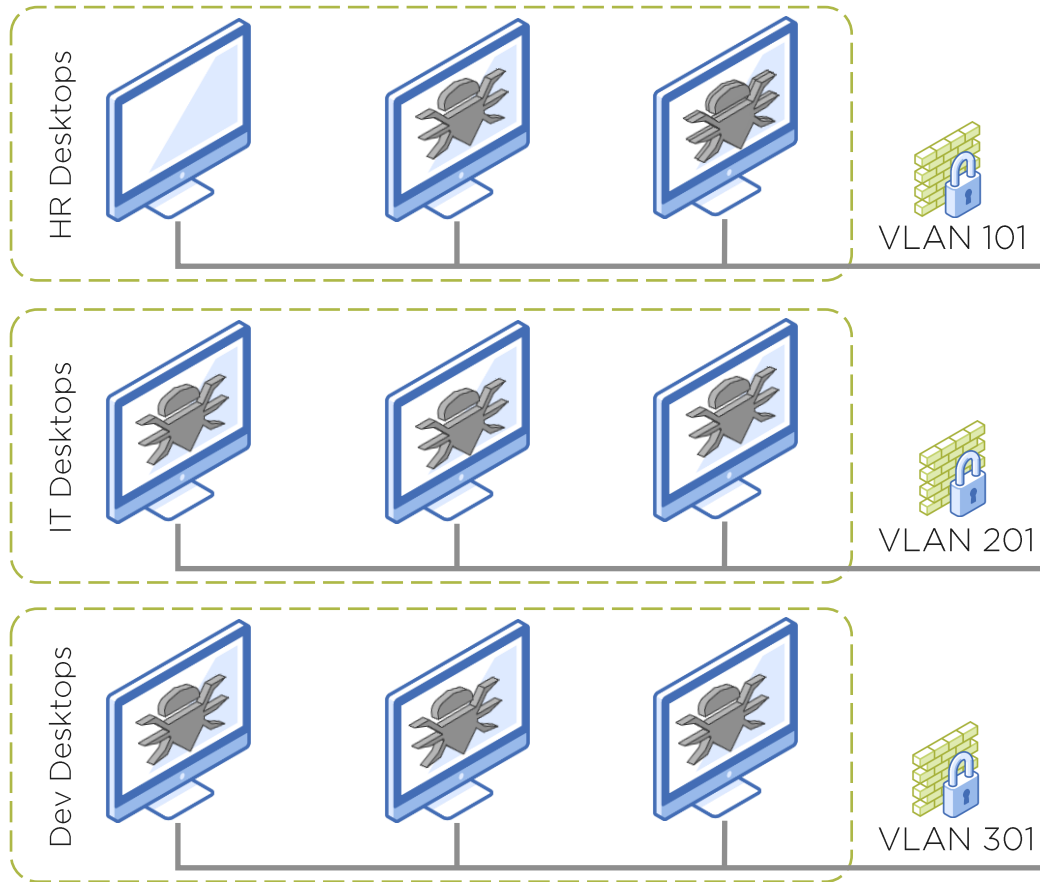


- VM 식별 (3 Tier App and Services) – 모든 VLAN/클러스터/호스트
- 카테고리 할당
- 인바운드/아웃바운드 정책 정의
- 인프라 계층 정책 정의
- Flow 를 통한 보안



# EUC 보안 – 전통적인 방식

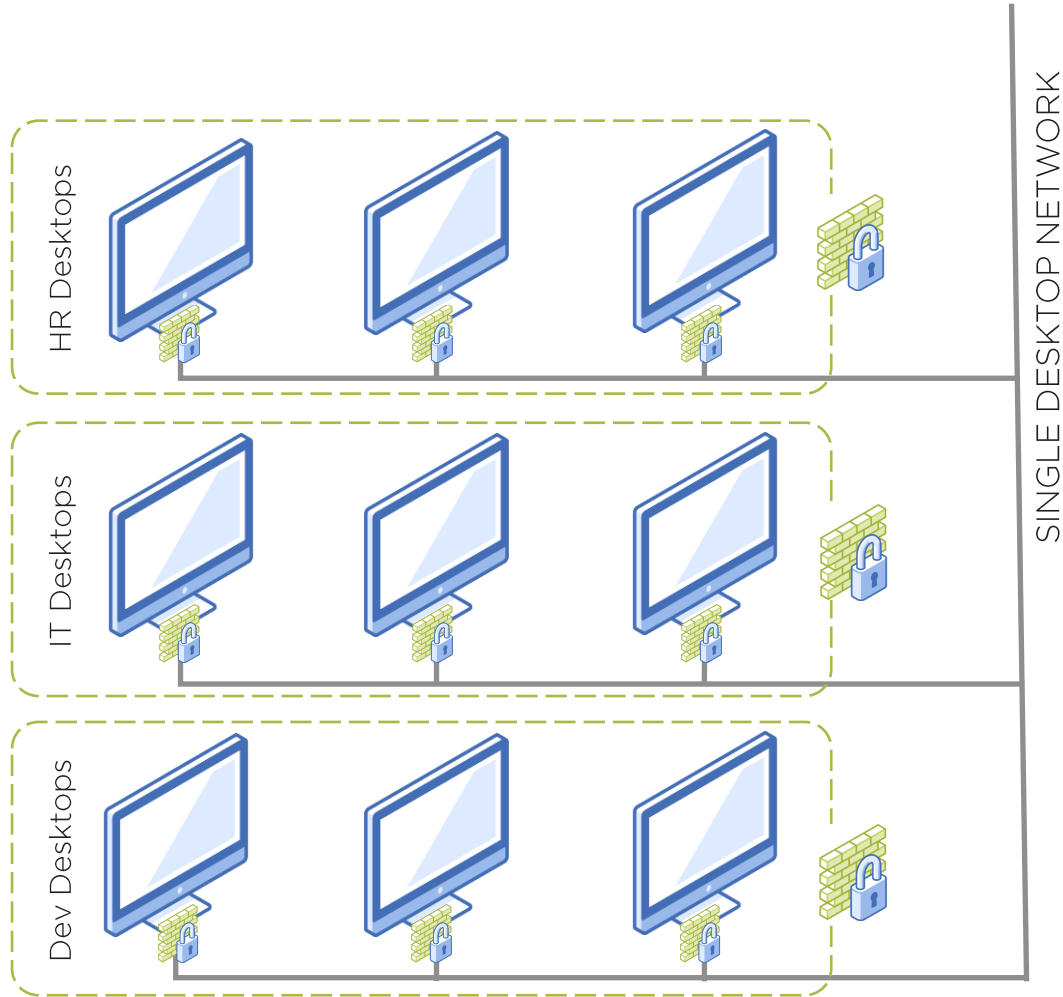
Perimeter/Internal Firewalls  
100s of Policies for Desktop Pools



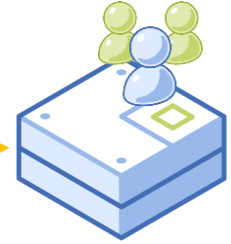
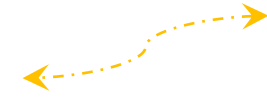
- 각 데스크톱 풀에 VLAN 할당
- 부서별 FW 정책 작성
- 측면 이동 방지 없음
- 복잡하고, 비용이 많이 들고, 느리고, 확장할 수 없습니다!



# Flow: EUC 보안: Identity 기반 방화벽



Flow



디렉토리 서비스

- Flow를 디렉터리 서비스와 통합
- 카테고리에 데스크톱 VM 식별 및 할당
  - 사용자/부서 기반
  - AD 그룹 기반의 자동화
- 인바운드/아웃바운드 정책 정의
  - 인바운드 – Allow HDX, 클라이언트
  - 아웃바운드 – AD, 인터넷
- 계층내 정책 정의
  - Malware 확산 방지



