

Mar, 2021

# 뉴노멀시대의 엔터프라이즈 네트워크 SD-WAN 전략

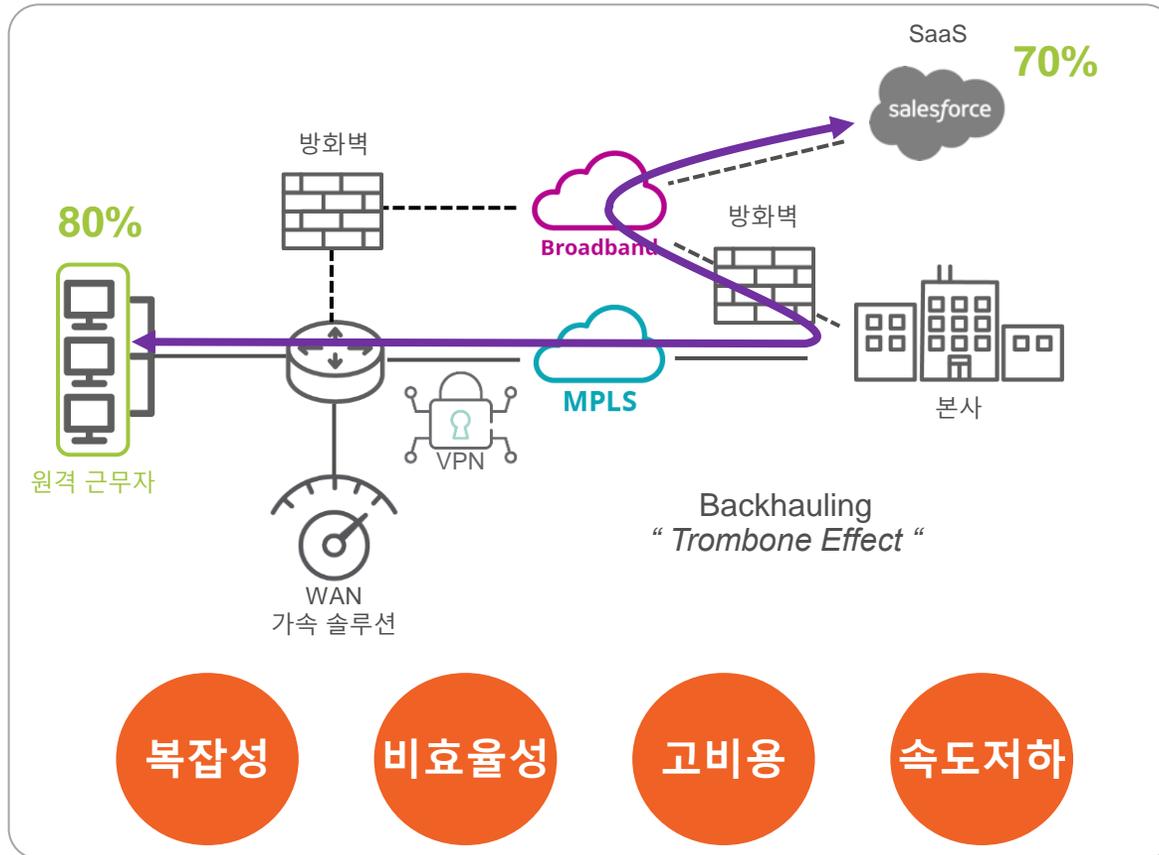
HPE Aruba 이한민 차장

aruba

a Hewlett Packard  
Enterprise company



# Legacy WAN 엔터프라이즈 네트워크의 현실



# IT 환경의 다변화에 따른 Legacy WAN의 한계



## 기존 Legacy 환경에서의 클라우드 어플리케이션 성능 이슈

지속성이 부족한 어플리케이션 성능, 백홀에 따른 회선 비용 낭비



## 복잡한 WAN 구간 솔루션 구성

Active-standby 전송 방식, 다중 라우팅 프로토콜 환경



## 지사 인프라의 지속적인 확장

라우터, 방화벽, WAN가속, 다양한 운영체제



## 운영 전반적인 자동화 기능 부족

각 장비마다 개별 설정 및 수작업 필요



## 고가의 인프라 구축 및 회선 비용

인프라, 기술지원, 인력, 회선 속도 증설

# SD-WAN을 통한 디지털 트랜스포메이션

## 변화하는 IT 환경에 최적화

### LEGACY 인프라에서 탈피

기존 라우터, 방화벽, VPN 장비와 고비용의 MPLS 및 전용선을 대체

### 어떤 전송 방식으로든 동작

비디오와 음성 데이터를 포함한 전체 업무 데이터를 다양한 회선을 통해 전송

### SLA 보장

수천 개의 클라우드 기반 어플리케이션 서비스를 위한 성능, 품질, 보안 기능 제공

### 자동화

수많은 위치와 다수의 장비에 병목현상 없이 설정과 정책을 배포하는 오케스트레이션

### 진보한 보안 기능

각 지점에 설치된 하드웨어 보안 솔루션이 아닌 클라우드 기반 보안으로 전환

### 자유로운 선택

업계 최고의 솔루션들과 손쉬운 통합 작업을 통해 최고 수준의 경험을 제공

# SD-WAN 구성 요소

**Control Plane: Controller / Manager / Orchestrator**

**Data Plane: Underlay Tunnel**

- 물리적인 네트워크 전송 구간
- MPLS, Internet, LTE 등
- 각 사이트를 IPsec 터널로 연결

**Overlay Tunnel**

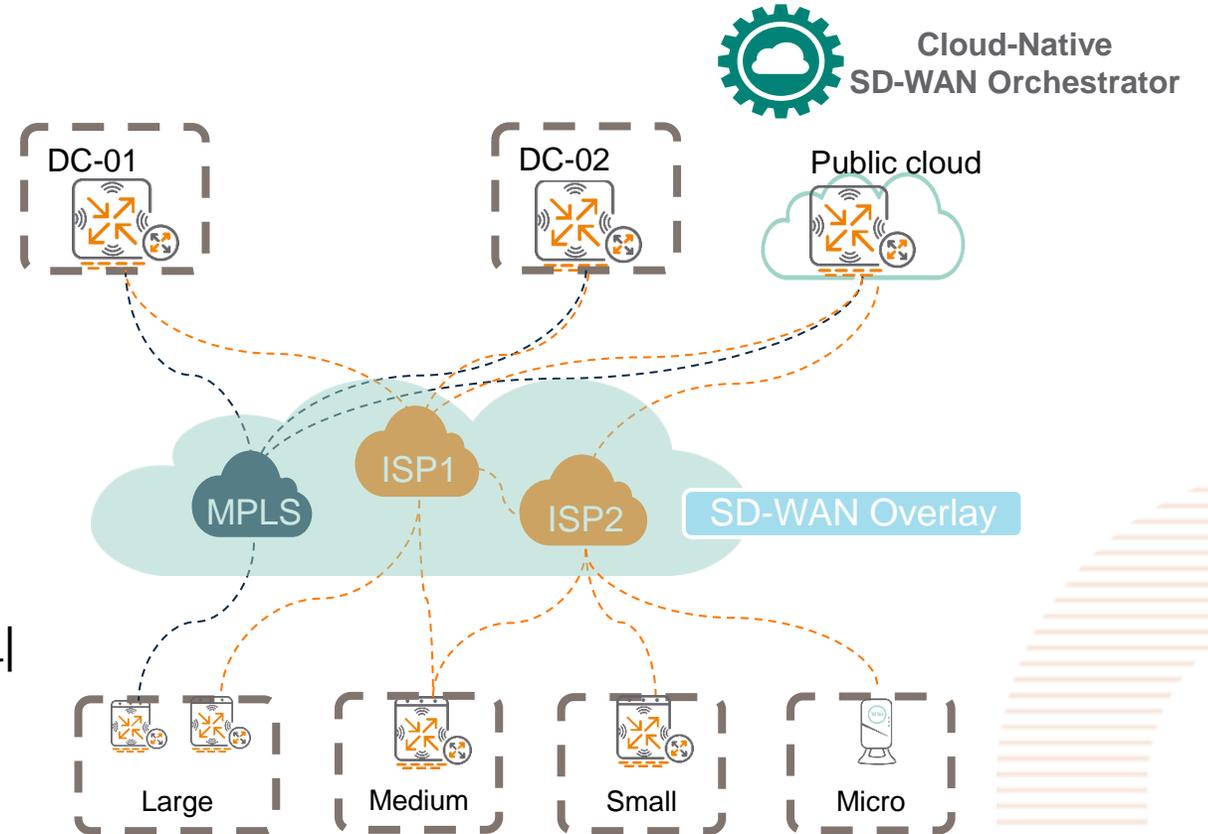
- 논리적인 연결 경로
- Control Plane 설정에 따라 하나 또는 다수의 언더레이 터널 사용 가능



# SD-WAN Orchestration

## 안정적인 연결성을 보장하는 경로 및 터널 정책 운영

- 클라우드 기반의 중앙 집중형 관리
  - 터널 상태 및 키 관리의 편의성
  - 손쉬운 설정과 확장
- 정책 기반 SD-WAN 오버레이 운영
  - WAN 연결 장비 및 회선 자동 검색
  - 설정된 토폴로지를 기반으로 한 터널 관리
  - SD-WAN 네트워크 전체 경로 조정



# SD-WAN 솔루션 핵심 기능

## 정책 기반 운영: 트래픽 관리

### 어플리케이션 트래픽 스티어링

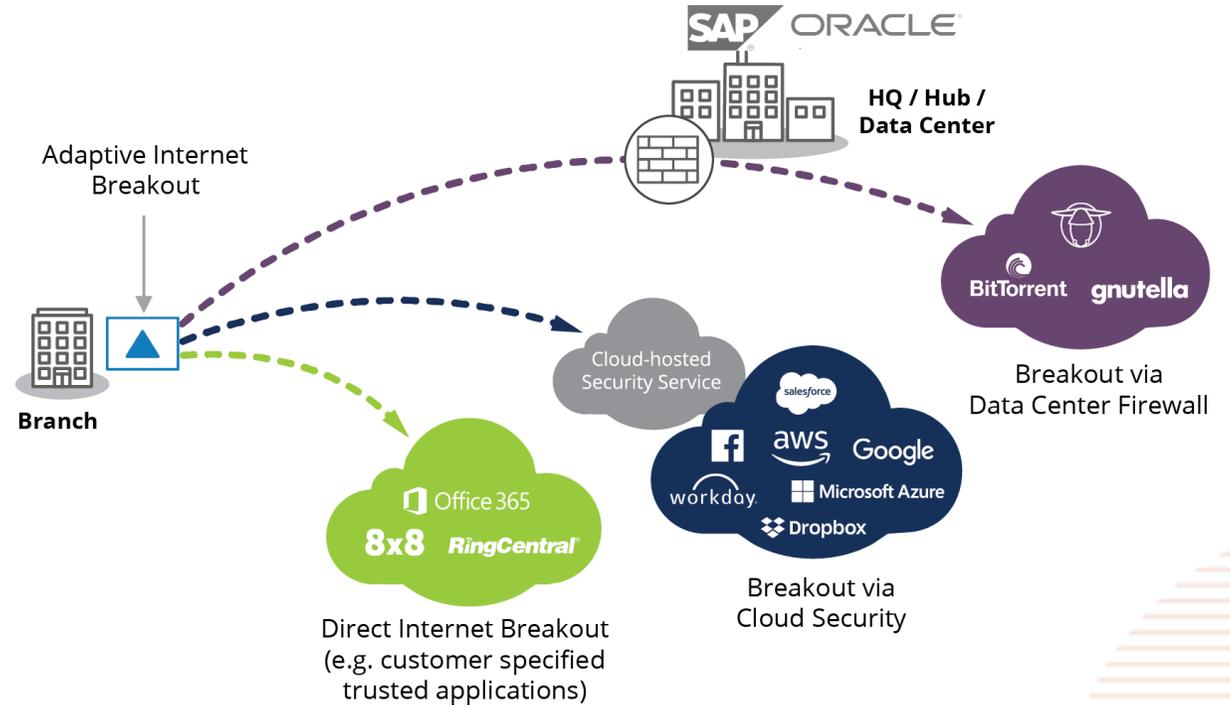
- SaaS 또는 인터넷 트래픽을 식별하여 각 지점에서 분기

### 보안 모델 재정의

- 어플리케이션 중심으로 보안 정책 변환

### 네트워크 보안 정책의 일관성 유지

- 네트워크 전반에 걸쳐 어플리케이션 보안성 및 성능 저하요인을 제거



### 어플리케이션 응답 속도 향상

- 어플리케이션 트래픽을 직접 관리하여 시간 지연을 방지

### 백홀 트래픽 감소

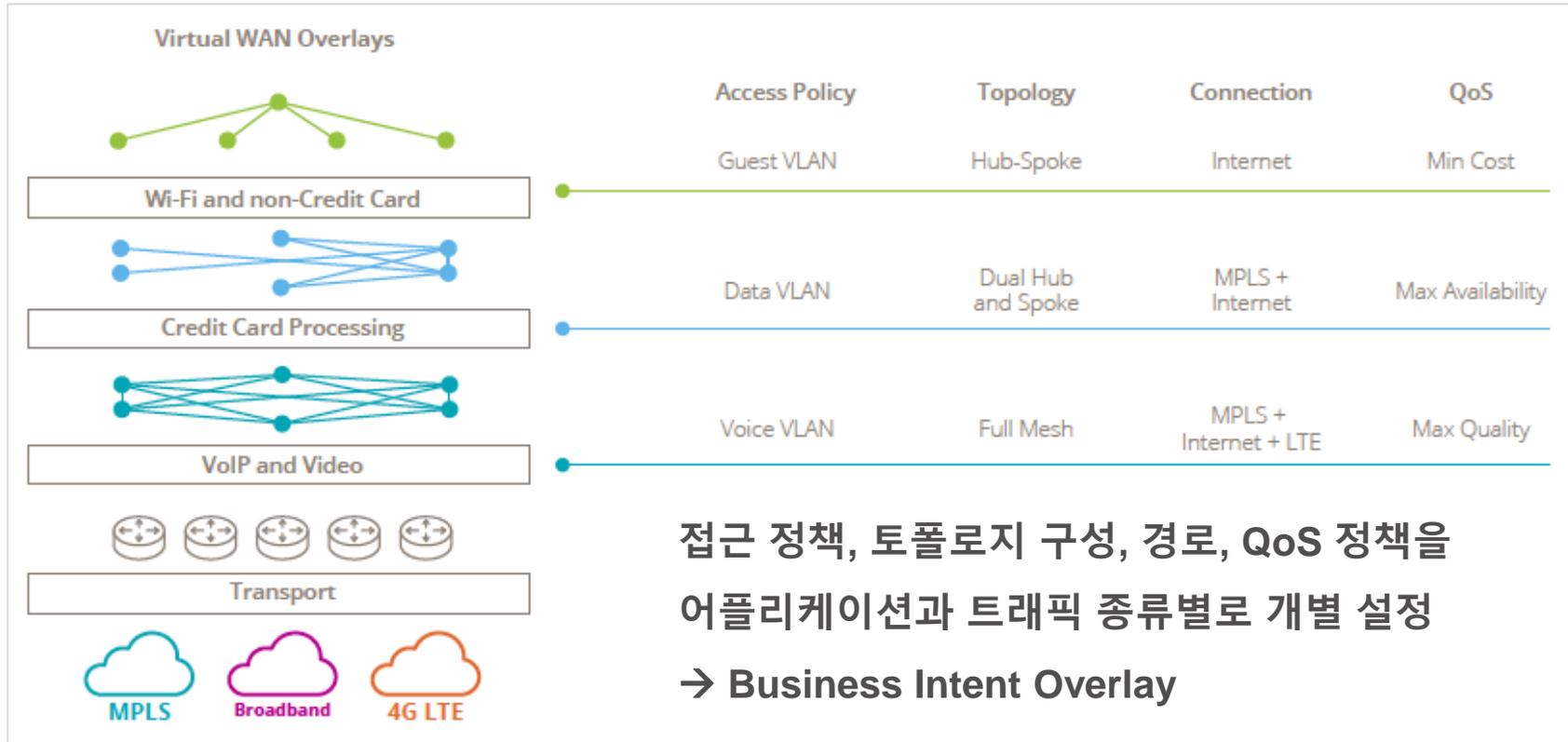
- 불필요한 터널 트래픽 유입 방지

### WAN 트래픽 효율화

- MPLS, 전용선 효율화를 통해 회선 사용량 및 비용 절감

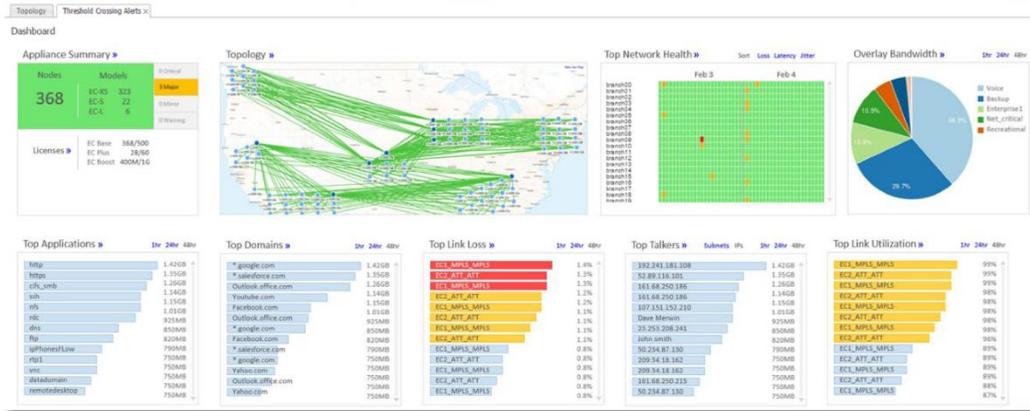
# SD-WAN 솔루션 핵심 기능

## 정책 기반 운영: Overlay 설정

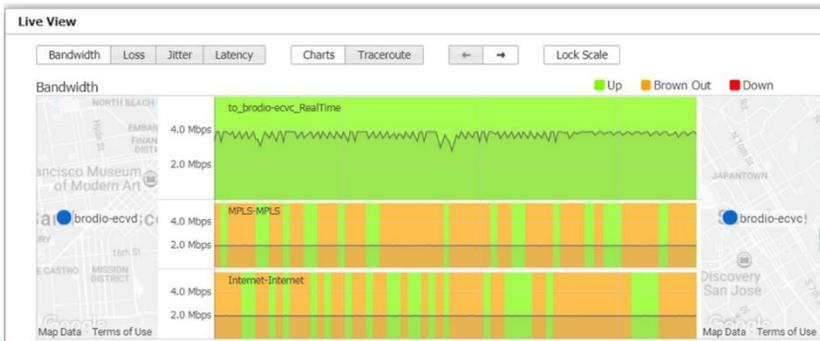
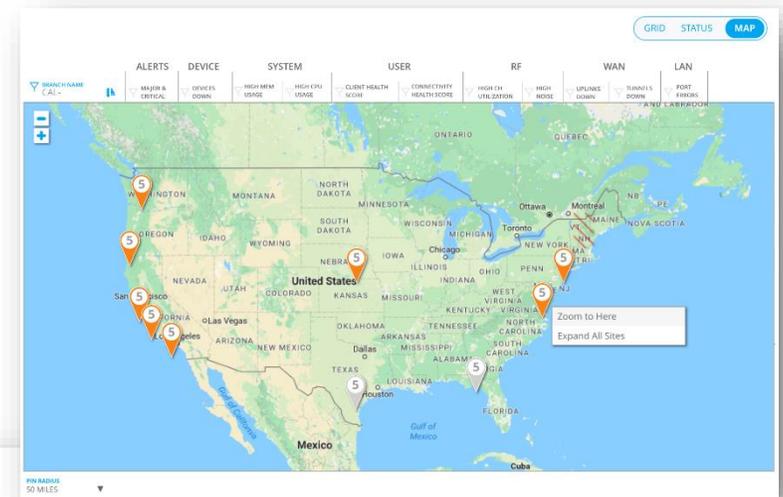


# SD-WAN 솔루션 핵심 기능

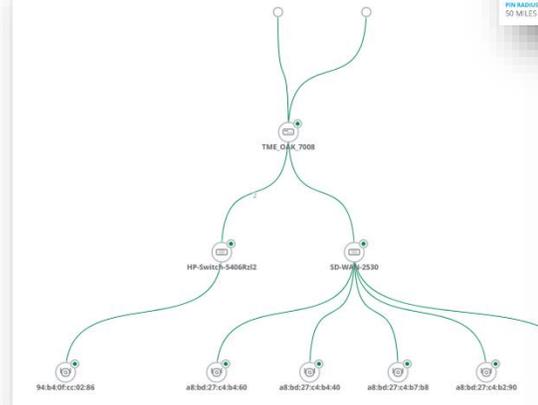
## 가시성



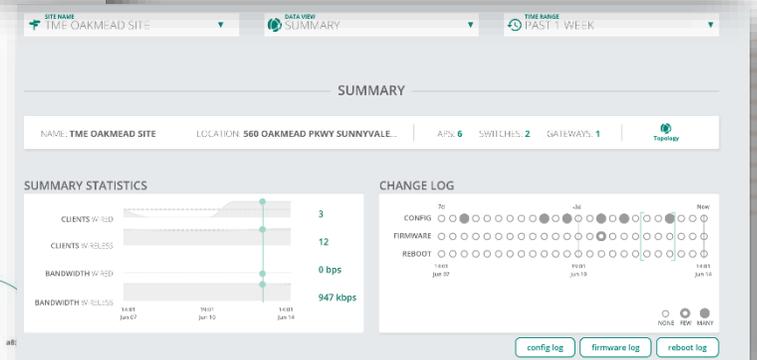
Dashboard



실시간 트래픽 모니터링



토폴로지 자동 구성

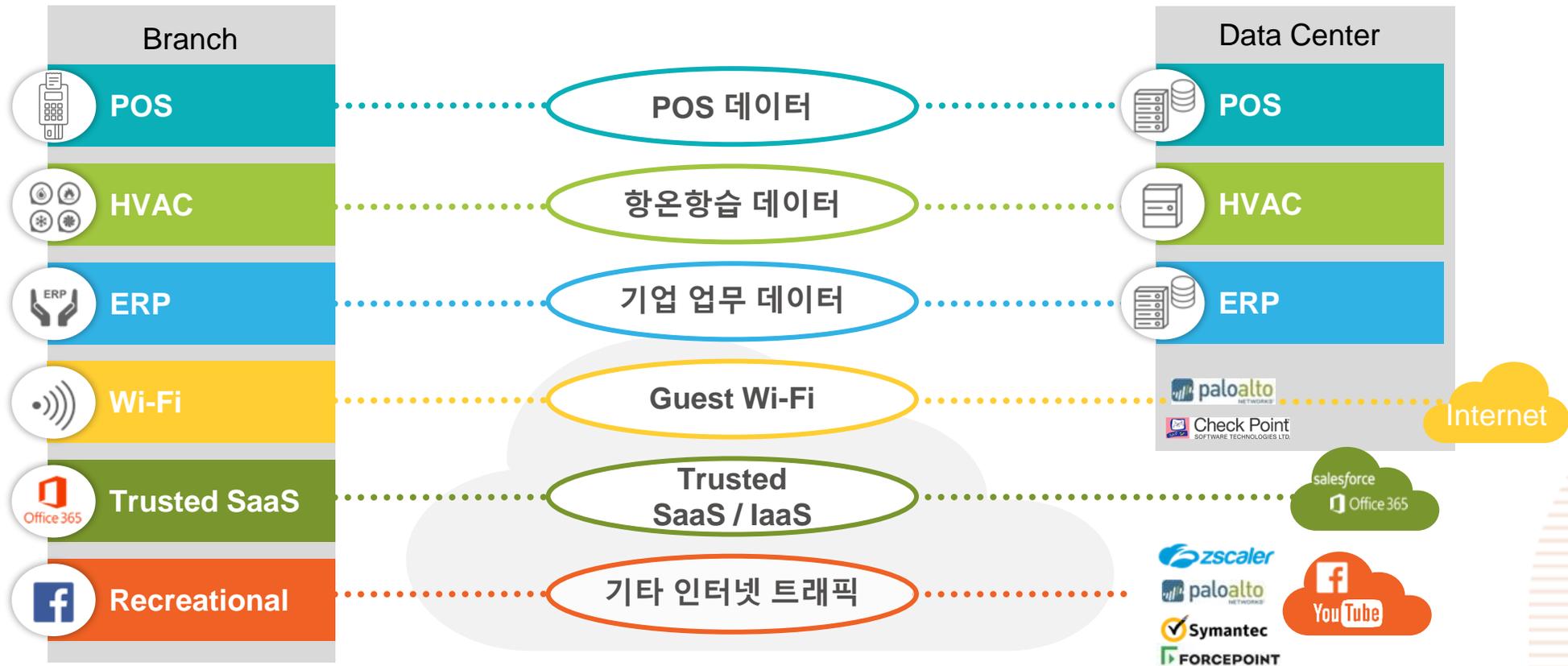


작업 이력 확인



# SD-WAN 솔루션 핵심 기능

## 보안: End-to-End Segmentation



# SD-WAN 솔루션 핵심 기능

## 보안: Zone Based Firewall

- 트래픽을 영역(Zone)으로 구분하여 고유한 보안 정책을 정의하고 적용
- 트래픽의 특성에 따른 각 영역별 토폴로지 구성과 Failover 정책 정의
- 분할된 영역에 어플리케이션을 할당하여 안전한 사용자 접근 제공
- LAN 영역과 WAN 세그먼트를 매핑

### Security Policies ?

Matrix View Table View

Merge Replace

| To Zones ⇄            | To Default                                      | To CorporateBranch                              | To GuestWifi | To BusinessCritical                             | To CorporateWAN                          |
|-----------------------|-------------------------------------------------|-------------------------------------------------|--------------|-------------------------------------------------|------------------------------------------|
| From Zones            |                                                 |                                                 |              |                                                 |                                          |
| From Default          | Allow All                                       | Deny All                                        | Deny All     | Deny All                                        | Deny All                                 |
| From CorporateBranch  | Allow: ACL Internet_Traffic<br>Deny: Everything | Allow All                                       | Deny All     | Allow: ACL BusinessCritical<br>Deny: Everything | Allow: ACL Corporate<br>Deny: Everything |
| From GuestWifi        | Allow: ACL Internet_Traffic<br>Deny: Everything | Deny All                                        | Allow All    | Deny All                                        | Deny All                                 |
| From BusinessCritical | Deny All                                        | Allow: ACL BusinessCritical<br>Deny: Everything | Deny All     | Allow All                                       | Deny All                                 |
| From CorporateWAN     | Deny All                                        | Allow: ACL Corporate<br>Deny: Everything        | Deny All     | Deny All                                        | Allow All                                |

### Edit Rules: Guest\_Wifi to InternetBreakout

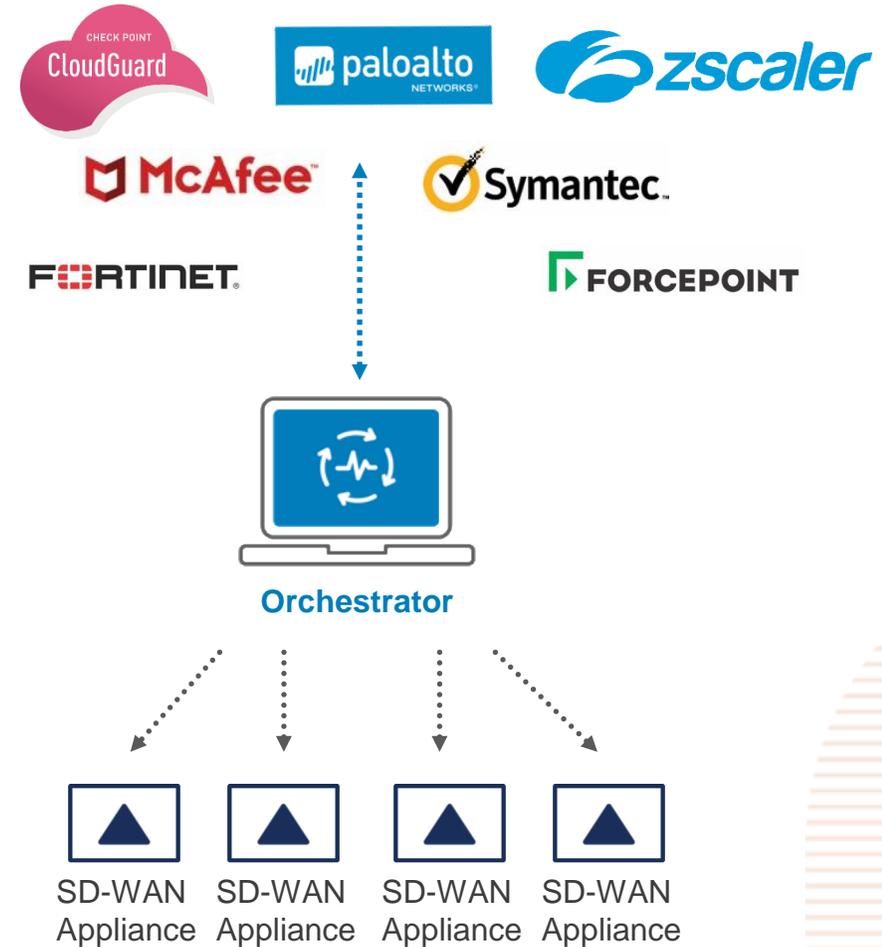
Add Rule

| Priority | Match Criteria                   | Action | Enabled                             | Tag | Comment |
|----------|----------------------------------|--------|-------------------------------------|-----|---------|
| 1001     | Application group Social_Network | deny   | <input checked="" type="checkbox"/> |     |         |
| 1002     | Application group Games          | deny   | <input checked="" type="checkbox"/> |     |         |
| 1004     | ACL Internet_Traffic             | allow  | <input checked="" type="checkbox"/> |     |         |
| 65535    | Match Everything                 | deny   | <input checked="" type="checkbox"/> |     |         |

# SD-WAN 솔루션 핵심 기능

## 보안: 클라우드 보안 솔루션과의 통합

- 다양한 클라우드 보안 서비스를 지원
- 오버레이 설정에서 Drag&Drop 방식으로 손쉽게 클라우드 보안 서비스 연계 가능
- 빠르게 성장하는 글로벌 에코시스템과 다양한 연결 및 연동 방식으로 통합



# SD-WAN 솔루션 핵심 기능

## 보안: SASE(Secure Access Service Edge)

The ideal complement for delivering a SASE architecture



- SD-WAN
- Routing
- Advanced Segmentation
- ZB FW
- WAN Opt



- SWG
- FWaaS
- IDS/IPS
- A/V
- ZTNA
- DLP
- Sandbox
- CASB
- DDoS

*“The secure access service edge (SASE) is an emerging offering combining comprehensive WAN capabilities with comprehensive network security functions (such as SWG, CASB, FWaaS, and ZTNA) to support the dynamic secure access needs of digital enterprises.” \**

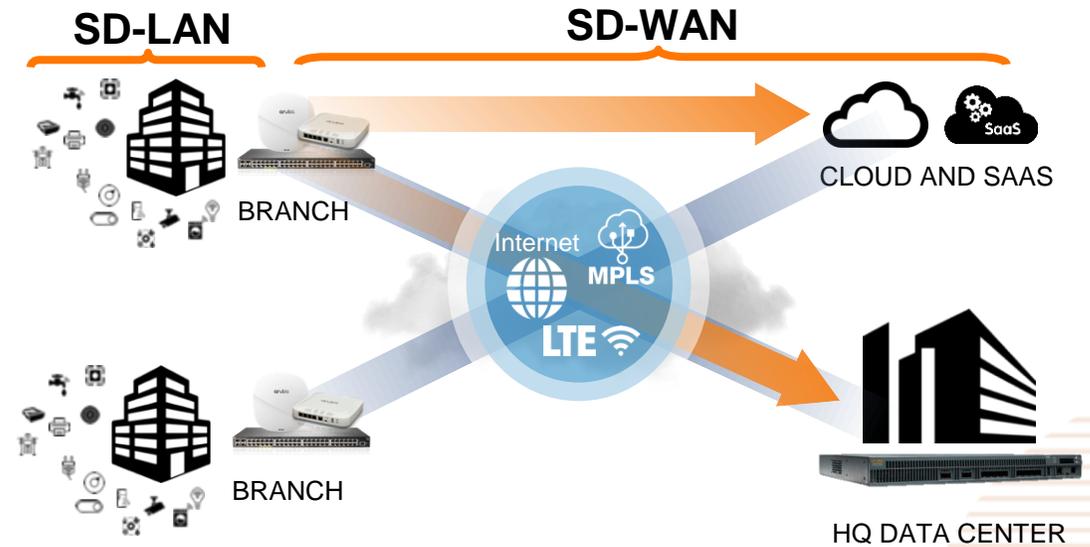
\*Gartner, “The Future of Network Security is in the Cloud,” August 30, 2019

**Gartner**

# SD-WAN을 품은 SD-Branch

SD-Branch = SD-WAN + SD-LAN(Security)

|                   |                                    |                                           |
|-------------------|------------------------------------|-------------------------------------------|
| SD-WAN<br>오케스트레이션 | WAN 어플라이언스의<br>손쉬운 설치 및 관리         | Role/어플리케이션<br>식별<br>동적 경로 설정<br>SaaS 최적화 |
| 클라우드 솔루션<br>통합    | 어플리케이션 방화벽<br>웹 콘텐츠 및 평판 기반<br>필터링 | 유무선 통합 관리<br>Dynamic<br>Segmentation      |



SD-WAN을 포함하여, 지점 및 본사 유무선 네트워크 인프라와 보안 정책을 통합 관리하는 클라우드 기반의 지점간 네트워크 운영 솔루션

# 엔터프라이즈 네트워크 SD-WAN 기대 효과

| 업무 영역          | 이슈 사항                                                          | 기대 효과                                    |
|----------------|----------------------------------------------------------------|------------------------------------------|
| 회선 비용          | MPLS, 전용선 서비스 등 회선 비용 이슈                                       | 기존 회선 또는 서비스를 이용하더라도 SLA를 충족             |
| 아키텍처           | 라우팅, 보안, WAN 가속, VPN 등 복잡한 장비 구성 및 개별 운영                       | 단일 장비와 관리 화면을 통한 솔루션 구성 및 운영 가능          |
| 자동화 & 업무 소요 시간 | 트래픽 이슈 처리에 긴 시간이 소요<br>솔루션 간 통합 분석이 어려움<br>장비 구성과 설정에 반복 작업 필요 | 손쉽고 빠른 분석 및 대응<br>설정 및 배포 자동화            |
| 가시성            | 가시성 및 모니터링 기능 부족으로 선제적 대응이 불가                                  | 실시간 트래픽 및 대역폭, 어플리케이션 성능 모니터링을 통한 운영 효율화 |
| 클라우드           | On-premise와 Legacy 인프라 중심의 네트워크 구성에 따른 클라우드 서비스 속도 지연          | Legacy 인프라와 클라우드 서비스 구분 없이 어플리케이션 성능을 보장 |



aruba

a Hewlett Packard  
Enterprise company

**Thank you**