

May 26, 2020

언택트 시대 변화하는 IT 인프라

Aruba Remote Solution with Central

aruba

a Hewlett Packard
Enterprise company



COVID-19

BCP
PLAN





단일 솔루션으로 모든 문제를 해결하세요!



전용선은 복잡하고
비쌉니다.



SaaS
애플리케이션은
다시 데이터센터를
통해 통신합니다.

WAN
Challenges



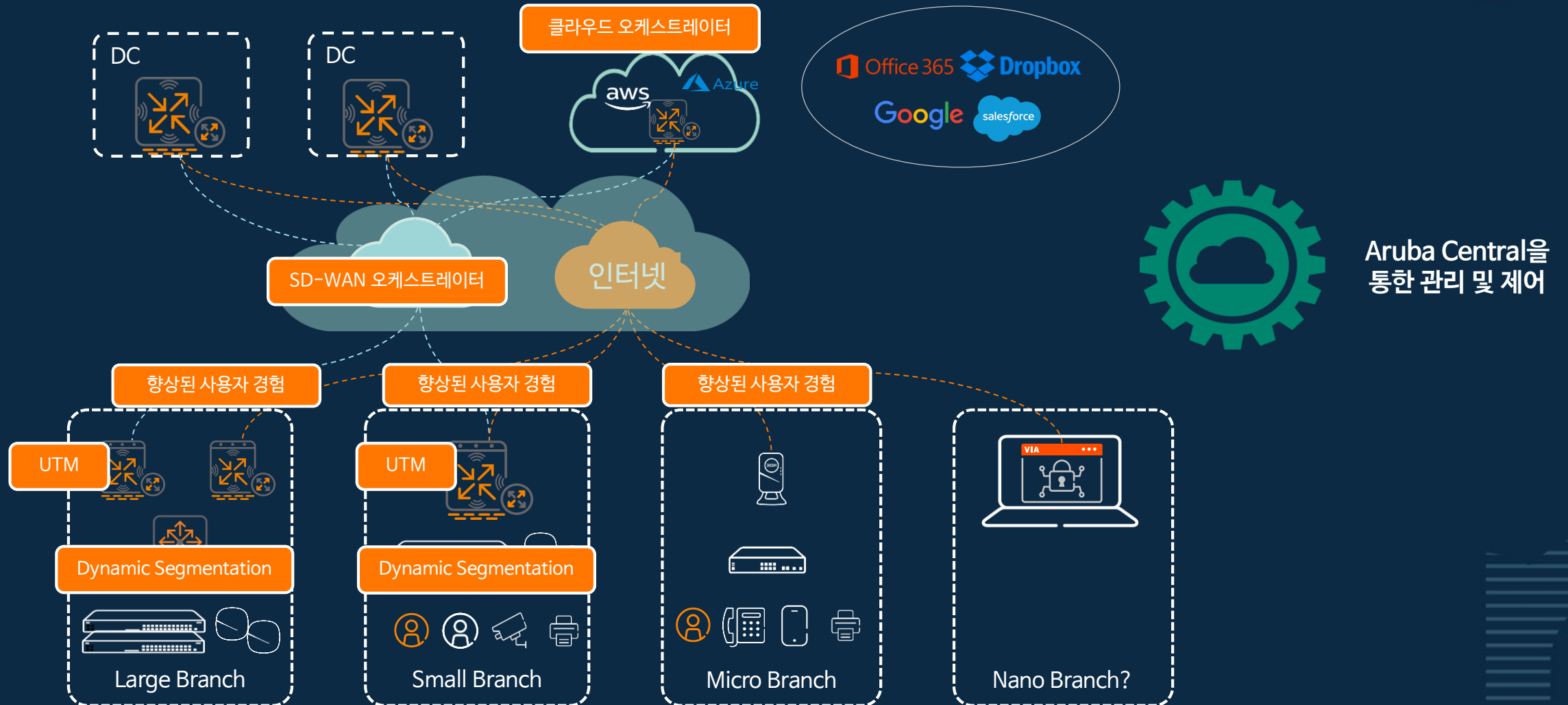
IoT 단말의 증가로
보안팀의 위협
부담이 높아집니다.



장치가
무분별하게
확장되고
수동으로 구성

BRANCH
Challenges

Cloud-First Architecture



안전하게 네트워크를 확장하는 USECASE 예시 - Aruba RAP

- ARUBA 엔지니어는 유선 연결을 요구합니다.
 - Aruba 엔지니어에게 각각 RAP를 제공
 - 집에서 ARUBA 본사까지 IPSec 연결
 - 별도의 VPN / Token 불 필요
 - 사무실에 있는 것과 동일한 환경 제공
- 원격 콜 센터
 - 노트북 연결을 위한 무선 환경
 - 전화기 연결을 위한 PoE 유선 포트



RAP MODELS



AP-203R (P)

- 전원 어댑터 내장
- 2개의 이더넷 포트
- 추가 PoE Out (옵션)
- BLE
- TPM



AP-203H

- PoE로만 연결
- 1개의 이더넷 포트
- No BLE
- NO TPM



AP-303H

- PoE 또는 외부 전원 연결
- 3개의 이더넷 포트 (1개 PoE 포트)
- 100Mb Wired Crypto
- Passthru port
- BLE
- TPM



AP-505H

- 2.5G 업링크
- PoE 또는 외부 전원 연결
- 4개의 이더넷 포트 (2개의 PoE 포트)
- 500Mbps Wired crypto
- BLE / ZIGBEE
- TPM
- WIFI6



SOLUTION OVERVIEW



모빌리티 컨트롤러 / 게이트웨이



BRANCH GW



IAP-VPN



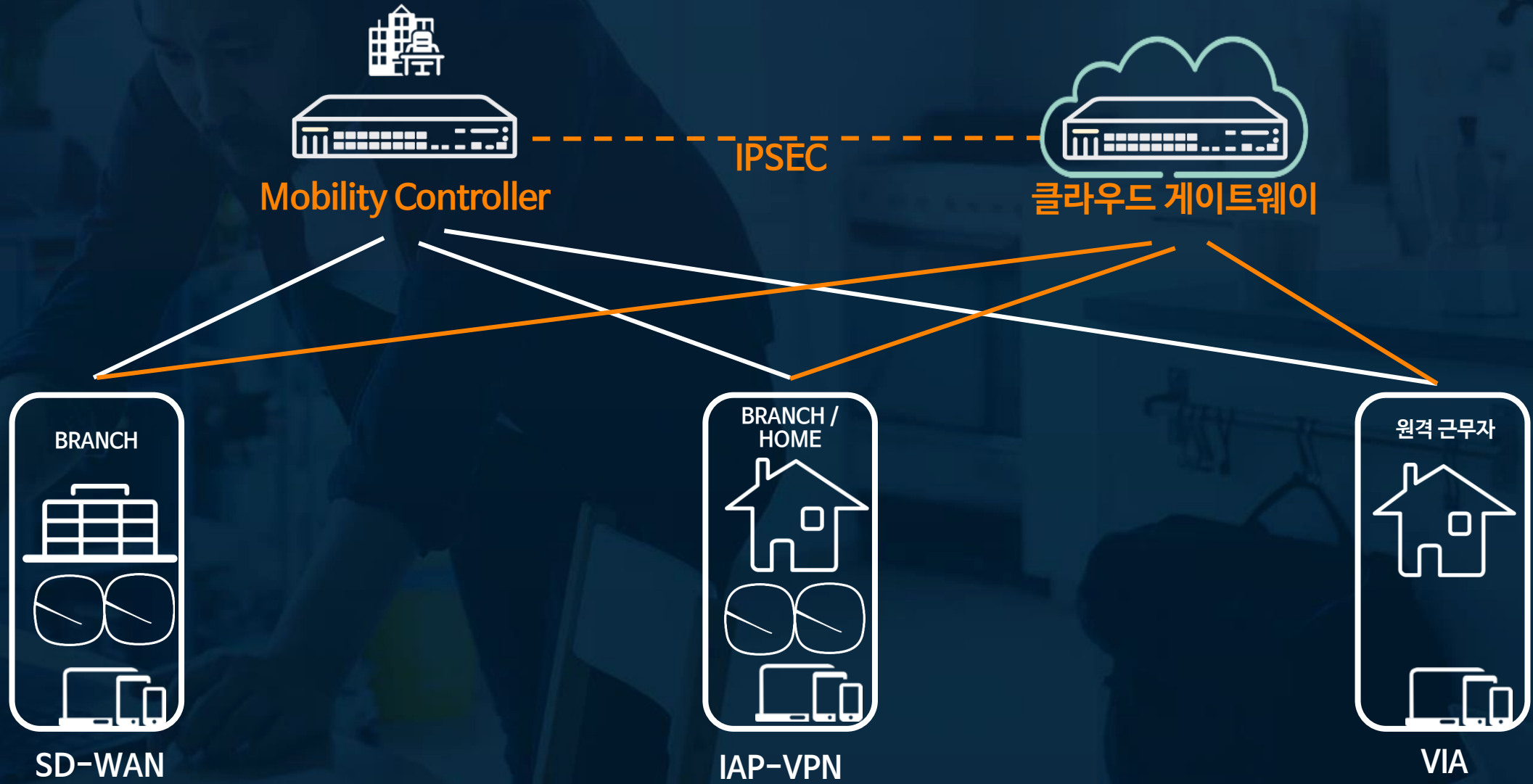
RAP



VIA



SOLUTION OVERVIEW - 클라우드 관리형



그럼 무엇을 사용해야 할까요?

하드웨어 또는 소프트웨어 방식의 VPN

클라우드 또는 On-Prem 방식



게이트웨이 / SD-WAN

다수 AP 로밍

ZTP

Failover를 위한 다수 업링크

집과 회사간 프로파일 분리

안전한 유선 포트



IAP-VPN

다수 AP로밍

ZTP

VRRP 이중화

집과 회사간 프로파일 분리

안전한 유선 포트



REMOTE AP

단일 AP

ZTP

집과 회사간
프로파일/SSID 분리

클러스터간 Stateful L2
failover

안전한 유선 포트



VIA

클라우드 관리형 또는 On-Prem

별도의 하드웨어 불필요

사용자가 VIA 클라이언트
다운로드

대부분의 OS에서 동작 가능



ARUBA RAP를 활용하여 네트워크를 안전하게 확장



병원



리테일/상점



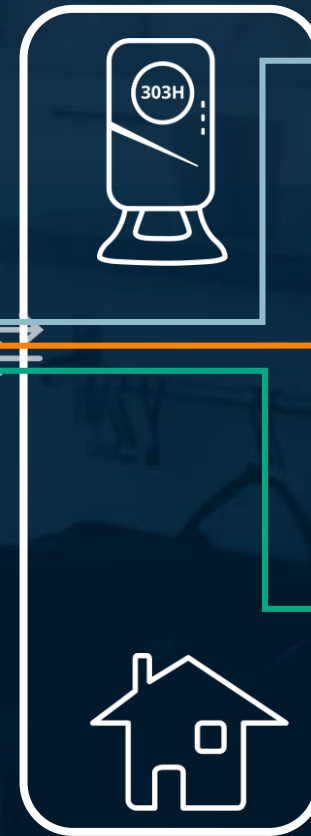
회사/사무실



학교



Aruba 모빌리티 컨트롤러



재택 근무 환경

GUEST / HOME



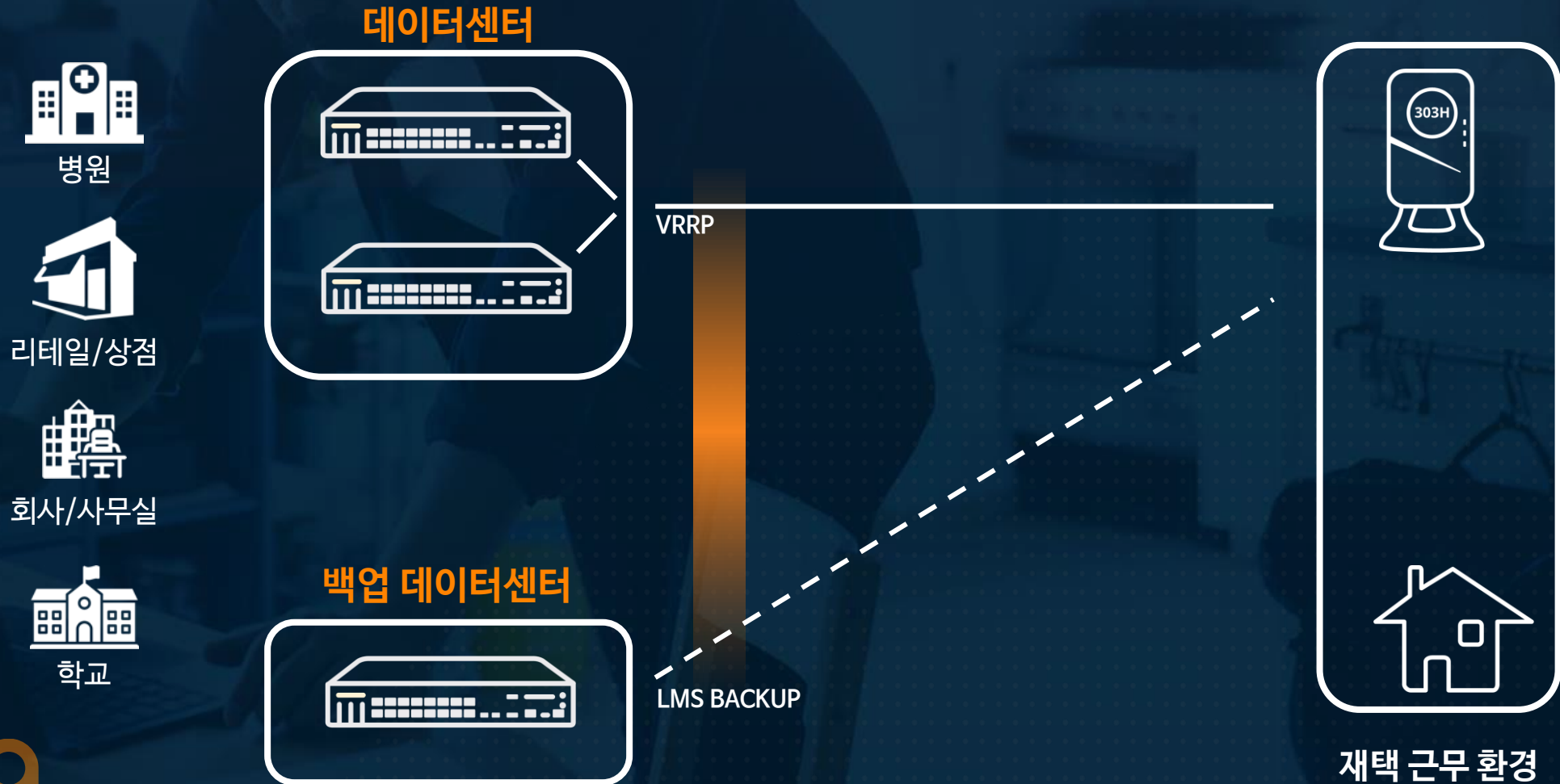
유선 / 무선 음성 통화



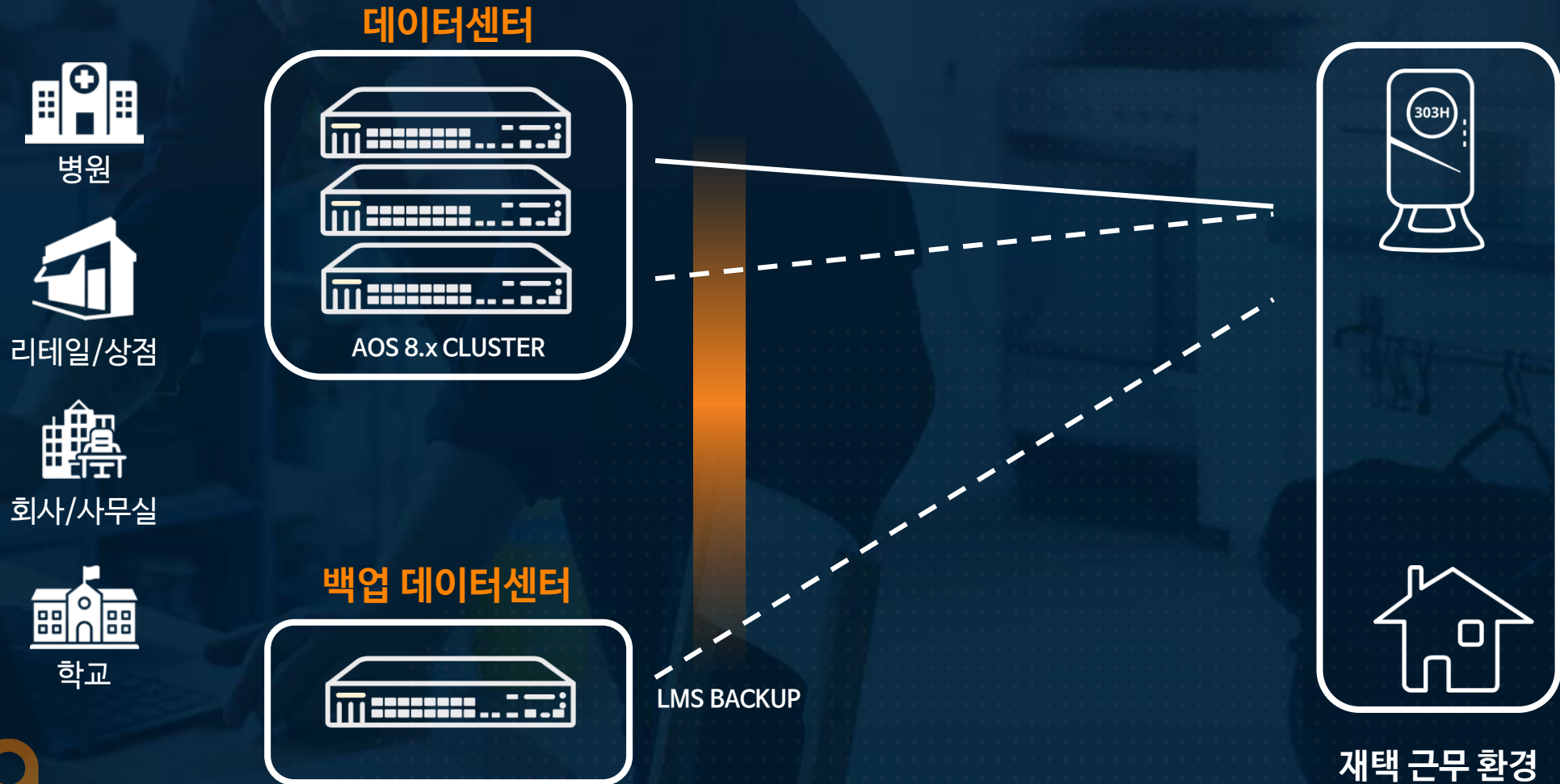
업무용 회사 SSID



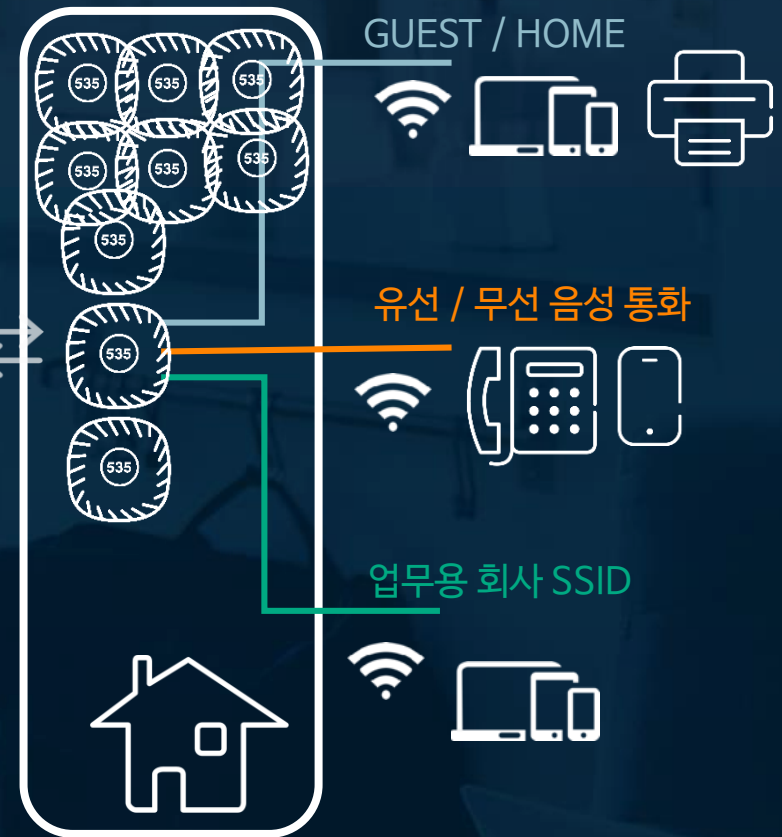
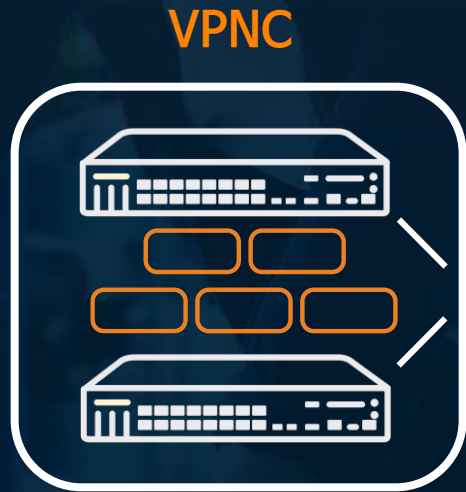
RAP 이중화로 네트워크를 안전하게 확장



모빌리티 마스터와 함께RAP 이중화로 네트워크를 안전하게 확장



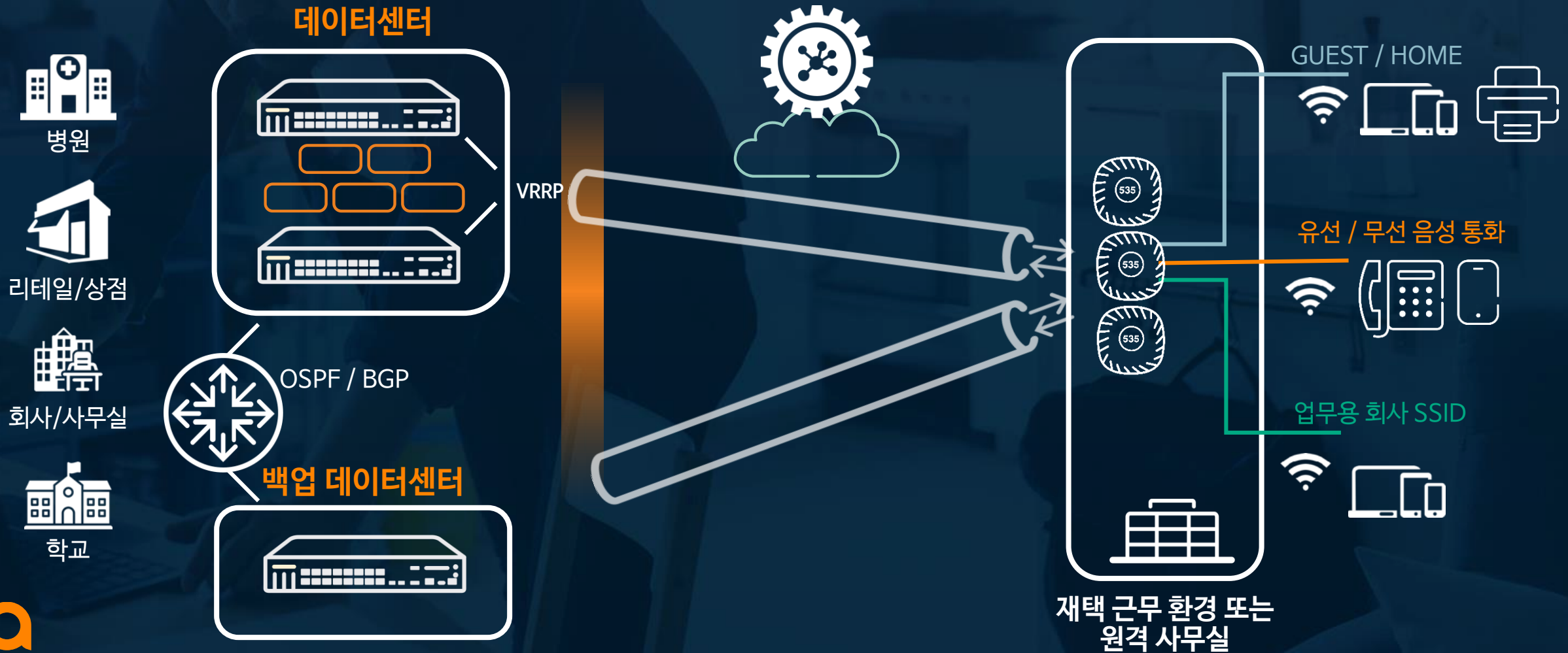
IAP-VPN로 네트워크를 안전하게 확장



재택 근무 환경



IAP-VPN로 네트워크를 안전하게 확장

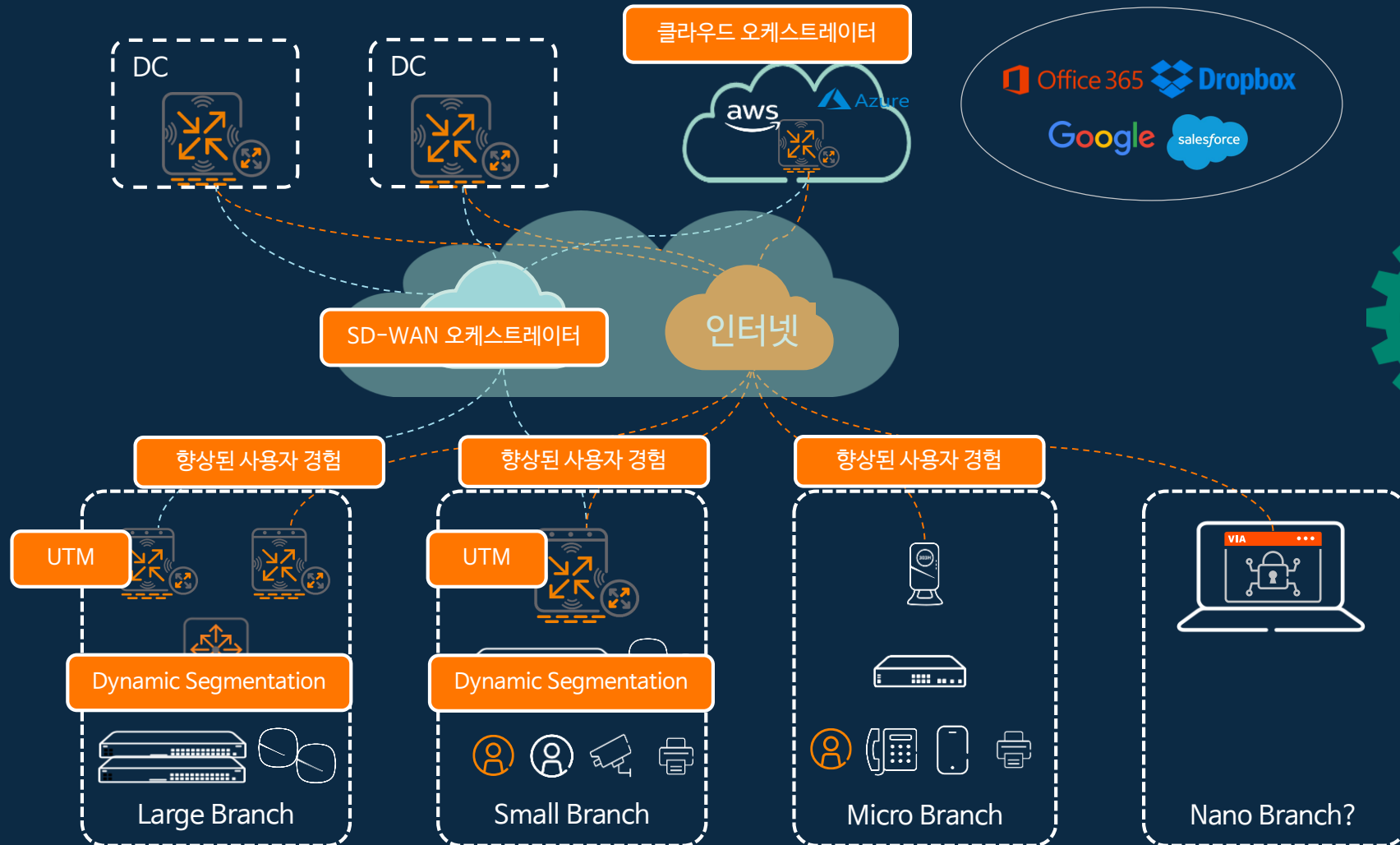


RAP 설치 방식에 따라 네트워크를 안전하게 확장

- 사무실에서 준비 및 프로비저닝
 - AP가 컨트롤러와 연결
 - RAP 역할로 수동 프로비저닝
- Zero Touch Provisioning (ZTP) (수동)
 - AP를 수동으로 추가
 - AP를 위한 그룹 설정 및 Booting 룰 설정
 - AP는 설정한 Profile에 따라 자동 프로비저닝
- Zero Touch Provisioning (ZTP) (자동)
 - AP가 배송될 때 인증서버에 자동 등록
 - AP Whitelist가 인증서버에서 MM으로 동기화
 - AP는 설정한 Profile에 따라 자동 프로비저닝



Cloud-First Architecture



Aruba Central을 통한 관리 및 제어



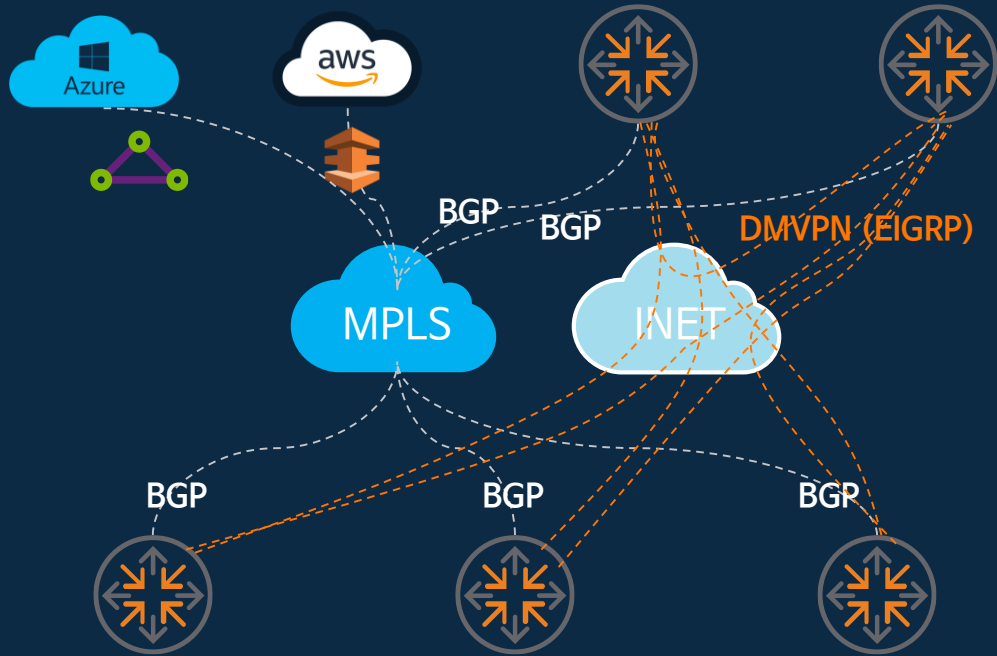
SD-WAN 오버레이

전송 독립적 연결 보장

SD-WAN 오케스트레이션

왜 중요할까요??

예전에는 어떻게 연결했었나요?



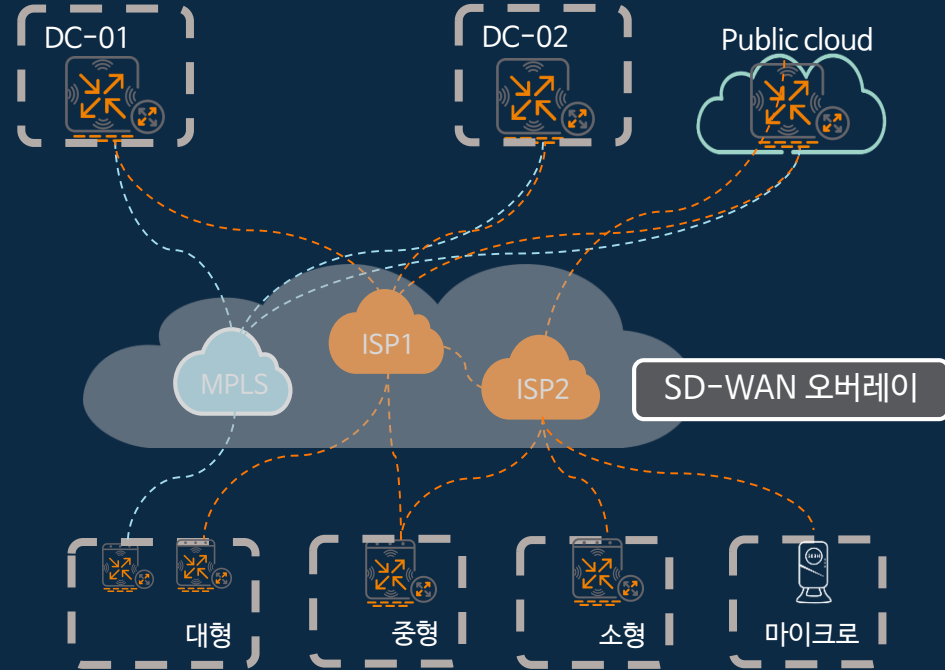
Boss: 새로운 App이 출시될 예정이야.
"\$%^#*!" 변경사항이 있을거야



SD-WAN 오케스트레이션 사용



클라우드 네이티브
SD-WAN 오케스트레이터



Boss: 새로운 App이 출시될 예정이야.
"\$%^#*!" 변경사항이 있을거야



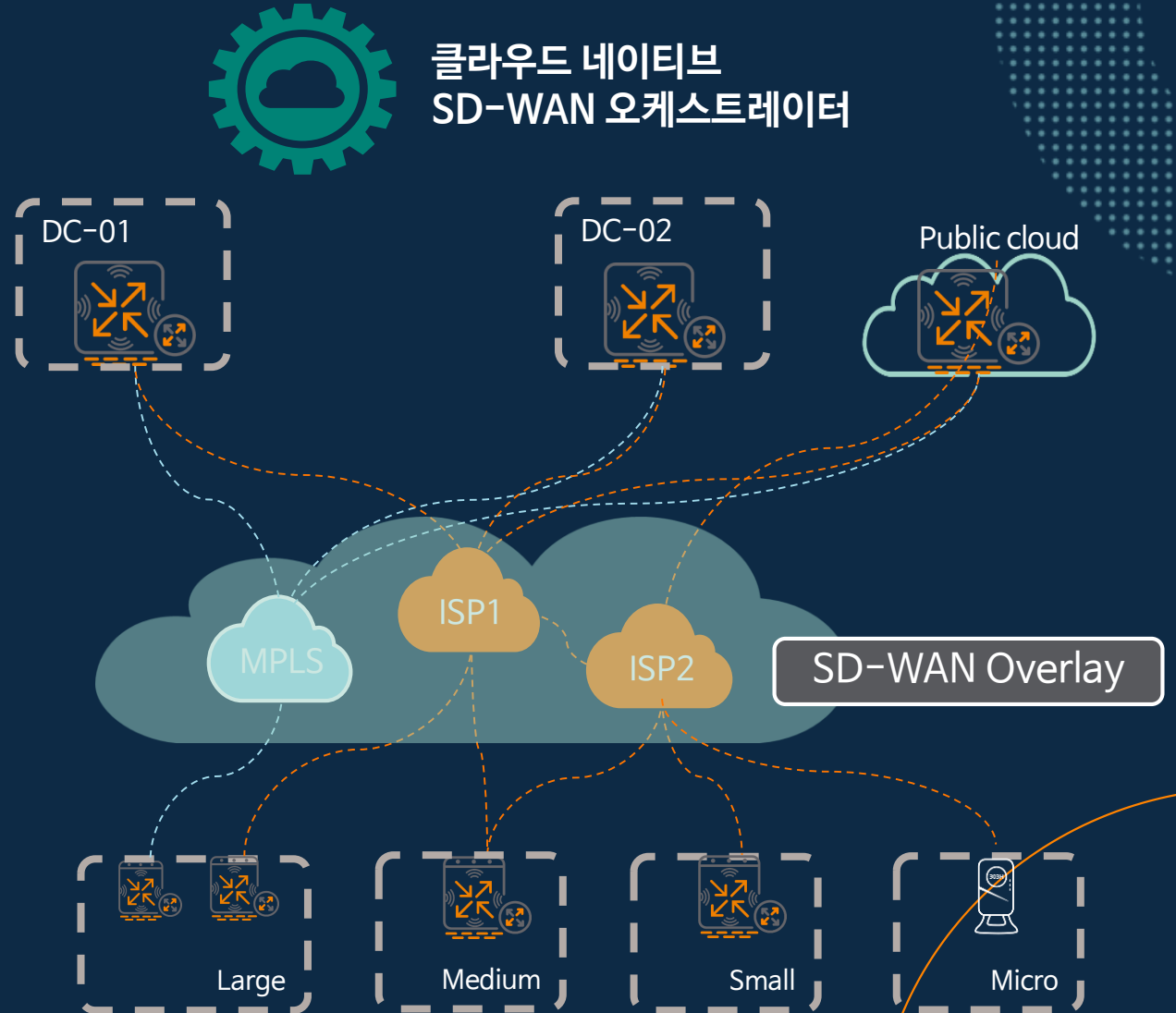
완료!



SD-WAN 오케스트레이션

어떻게 동작하나요?

- 중앙 클라우드 네이티브 방식의 제어부
 - 중앙화된 키 관리
 - 수평적 확장성
- 정책 중심의 SD-WAN 오버레이
 - 네트워크간 WAN 링크 자동 탐색
 - 토폴로지 요구사항에 따라 라우팅 및 터널링 오케스트레이션



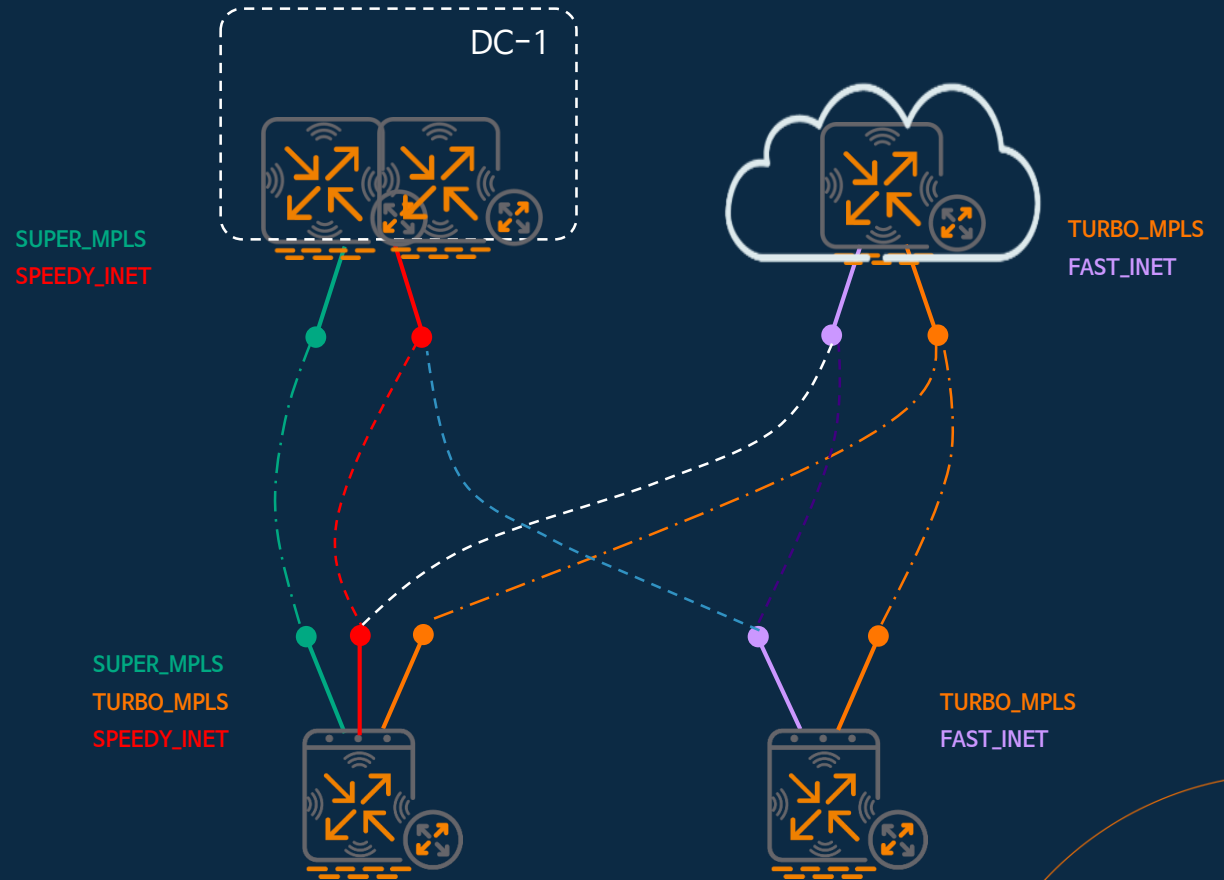
SD-WAN 오케스트레이터

터널링 오케스트레이션



SD-WAN 오케스트레이터

출발지	목적지	방식	태그	Cost
BG-1	DC-1-VPNC-1	MPLS	SUPER	10
BG-1	DC-1-VPNC-2	MPLS	SUPER	20
BG-1	DC-1-VPNC-1	INET	SPEEDY	20
BG-1	DC-1-VPNC-2	INET	SPEEDY	10
BG-1	DC-2-VPNC-1	MPLS	TURBO	30
...



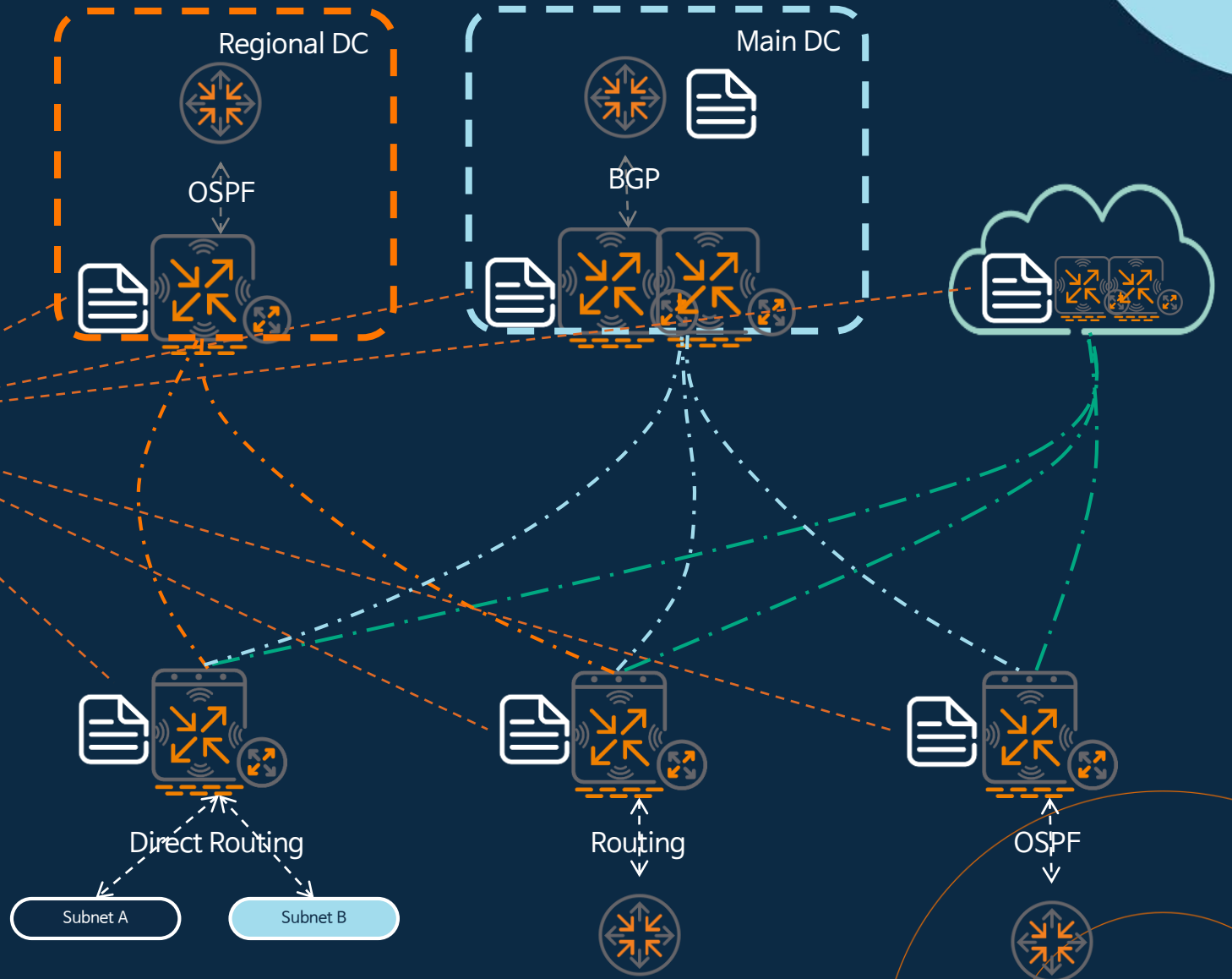
오버레이 오케스트레이션

라우팅 오케스트레이션

SD-WAN
오케스트레이터



게이트웨이	네트워크	NextHop
BGW-01	10.96.0.0/16 (branches)	R-DC
BGW-01	10.0.0.0/8 172.16.0.0/12 (summary-global)	Main-DC
BGW-01	10.127.0.0/16 (AWS-VPC)	Cloud
...



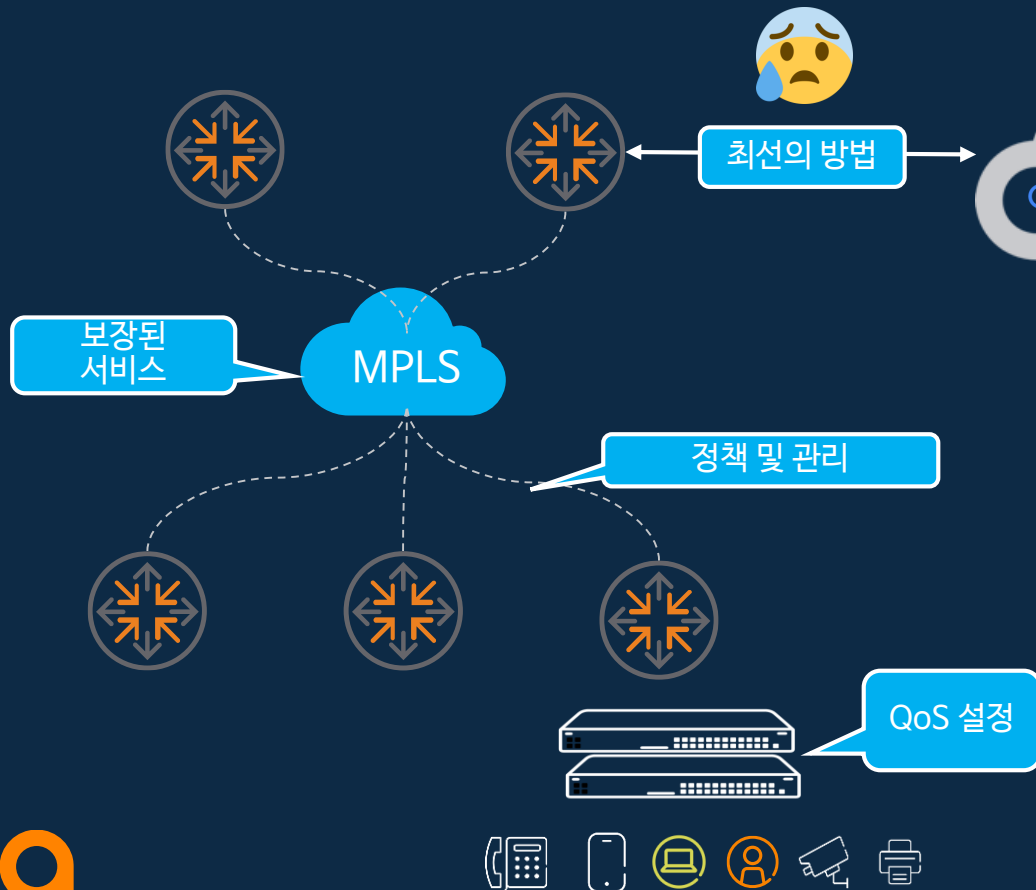
비즈니스 정책

사용자 경험 향상

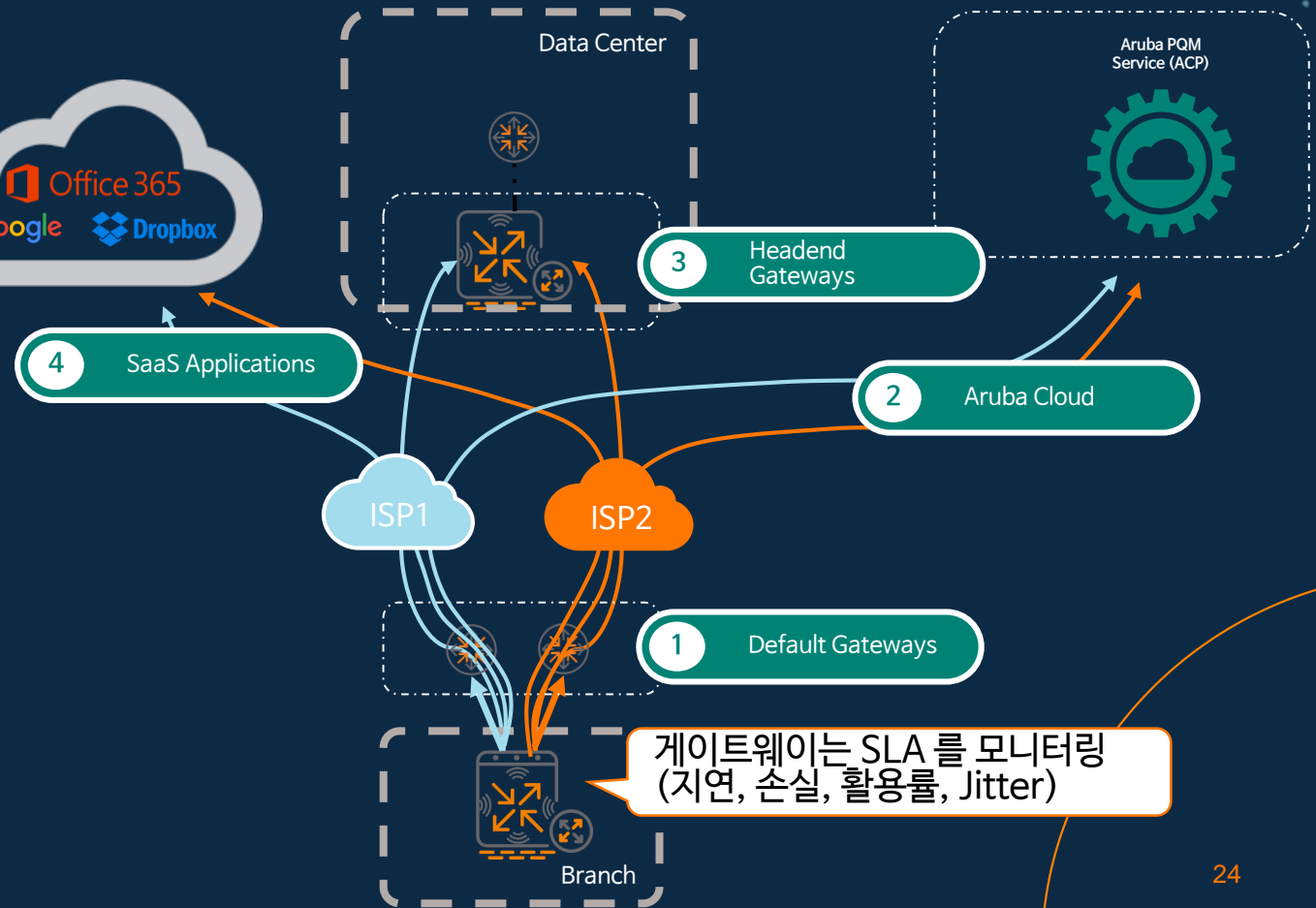
사용자 경험의 퀄리티

왜 중요할까요?

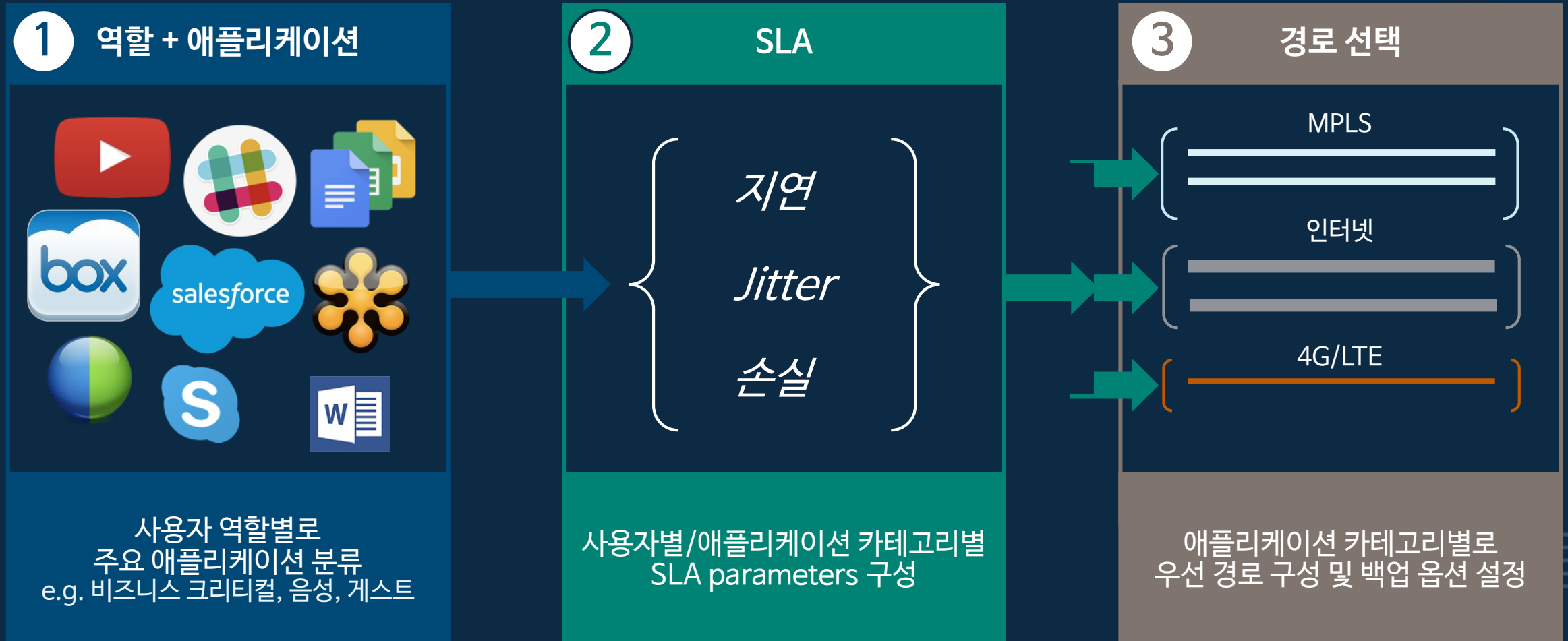
이전에는 어떻게 퀄리티를 높였나요?



어떻게 SD-WAN으로 퀄리티를 높이나요?



Dynamic Path Selection/Steering



Dynamic Path Steering

WAN 링크가 애플리케이션 SLA를 준수하는지?

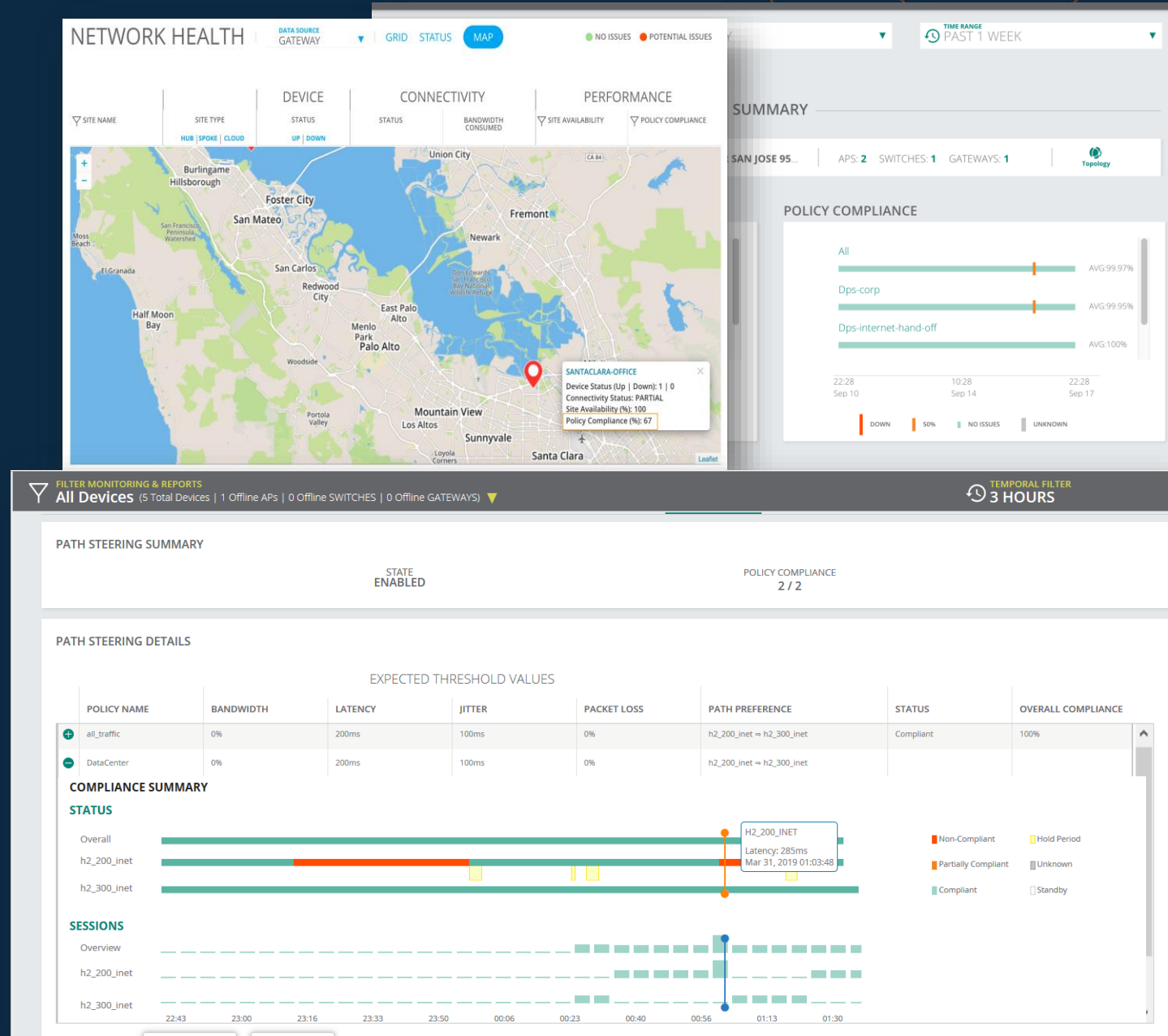
- WAN 링크별 컴플라이언스 확인
- 특정 사유로 인한 위반 항목 강조

정책이 경로 기본설정을 준수하는지?

- 활성 링크간 세션 분배 확인

WAN 링크 SLA 위반시 DPS 수행?

- WAN 링크간 세션 이동을 신속하게 식별



Dynamic Path Steering

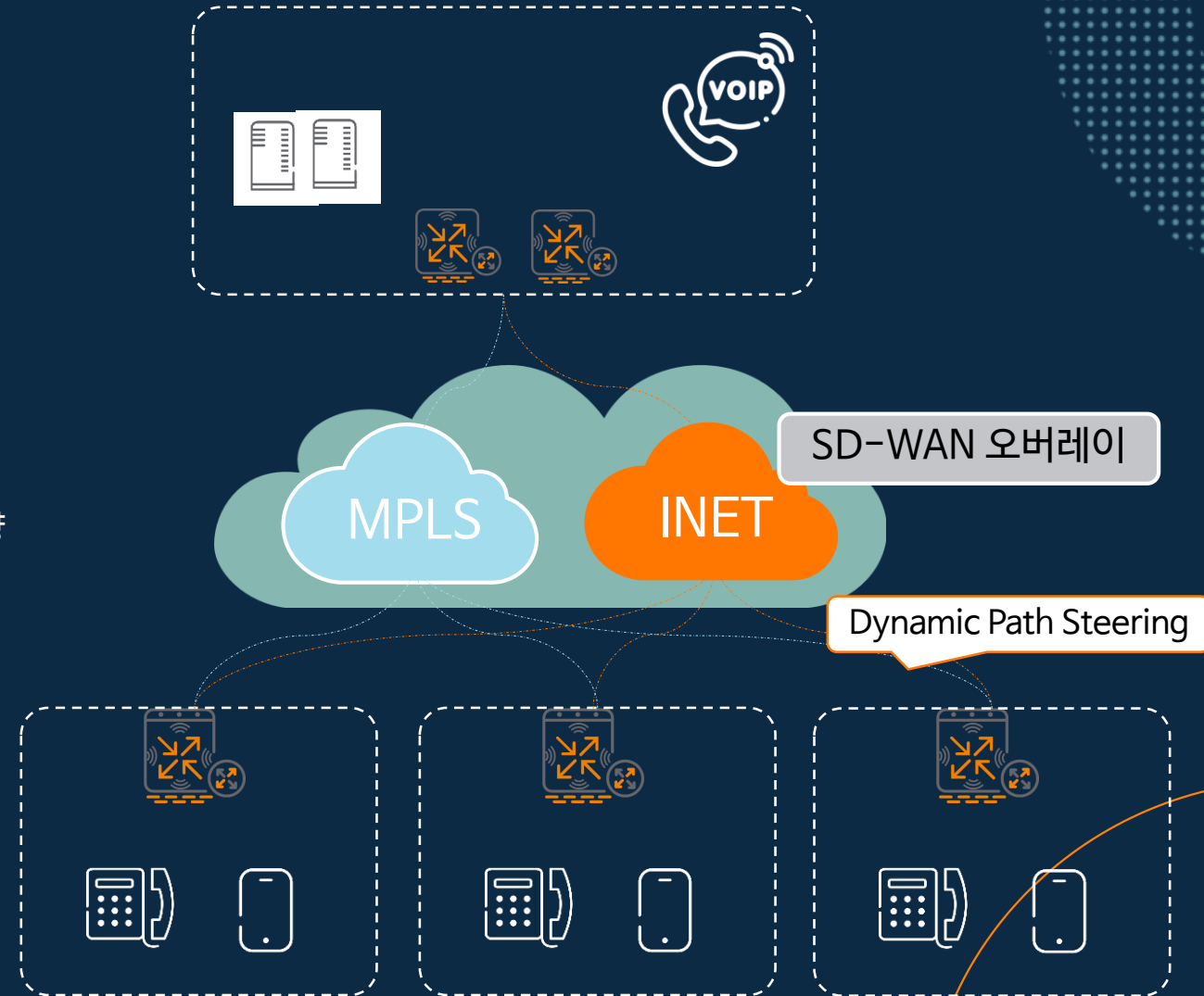
어떻게 도와줄 수 있나요?

- 무엇이 문제인가요?

- VoIP 서비스는 매우 중요하기 때문에, 지연 시간이 짧아야 하고 Jitter 값이 작은 MPLS 경로가 적합합니다.
- 반면 MPLS는 새로운 애플리케이션의 대역폭 요구사항을 처리할 수 없음

- 어떻게 대응하나요?

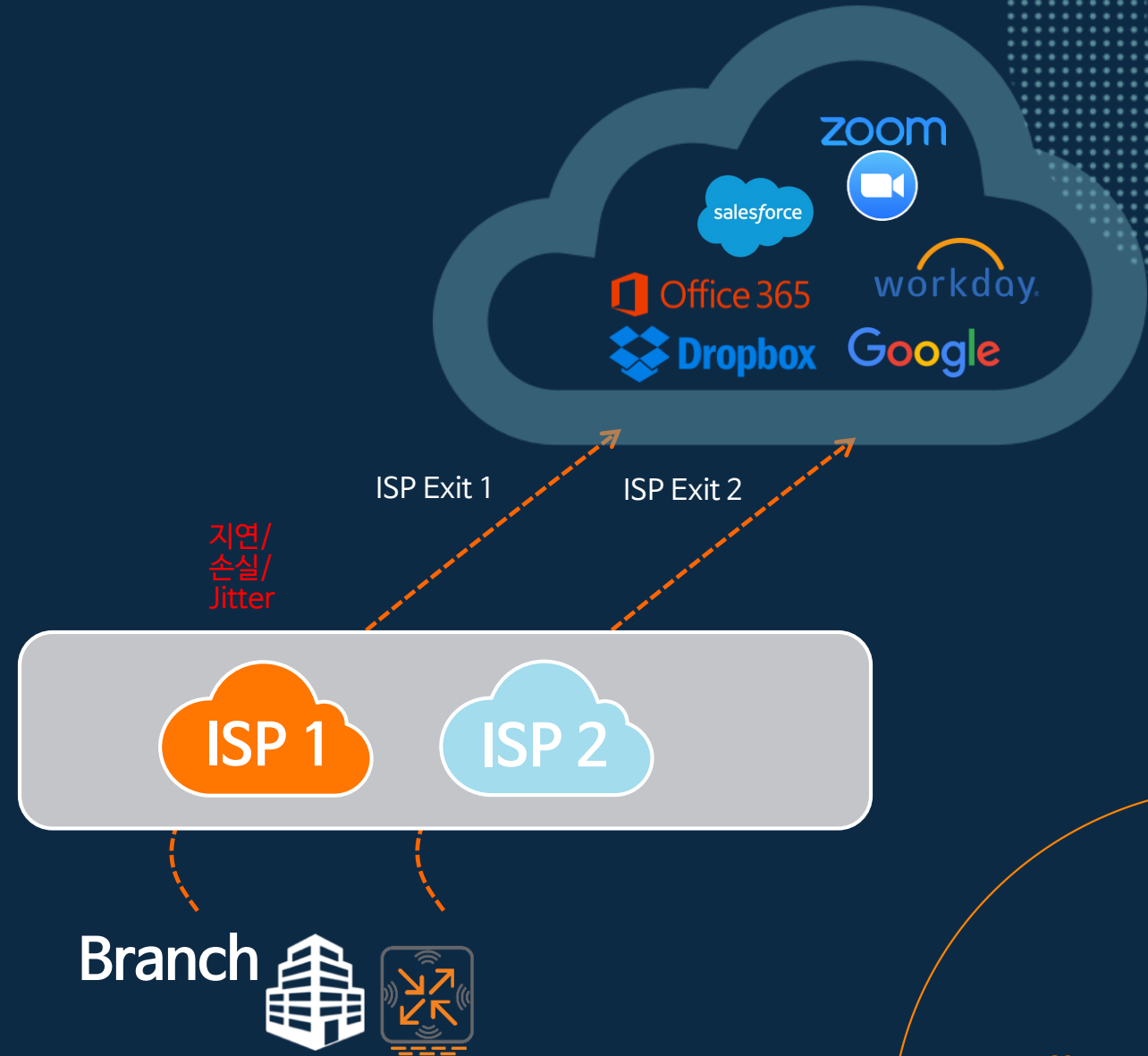
- Aruba SD-WAN은 모든 WAN 회선에 대해서 지연, 손실, Jitter, 사용량 등 상태 값을 모니터링 합니다.
- Aruba SD-WAN은 MPLS 회선에 대해서 이중 QoS 태깅을 적용하고, 인터넷 회선에 대해 애플리케이션 기반의 QoS 스케줄링을 적용합니다.
- Dynamic Path Steering은 가장 이상적인 회선으로 트래픽이 흐르도록 선택적으로 조절합니다.
 - 지연과 Jitter에 민감한 트래픽은 MPLS
 - 대역폭을 많이 사용하는 애플리케이션은 인터넷 회선
 - SLA를 만족 못하는 경우 실시간으로 트래픽 이동



SaaS 최적화

어떻게 동작하나요?

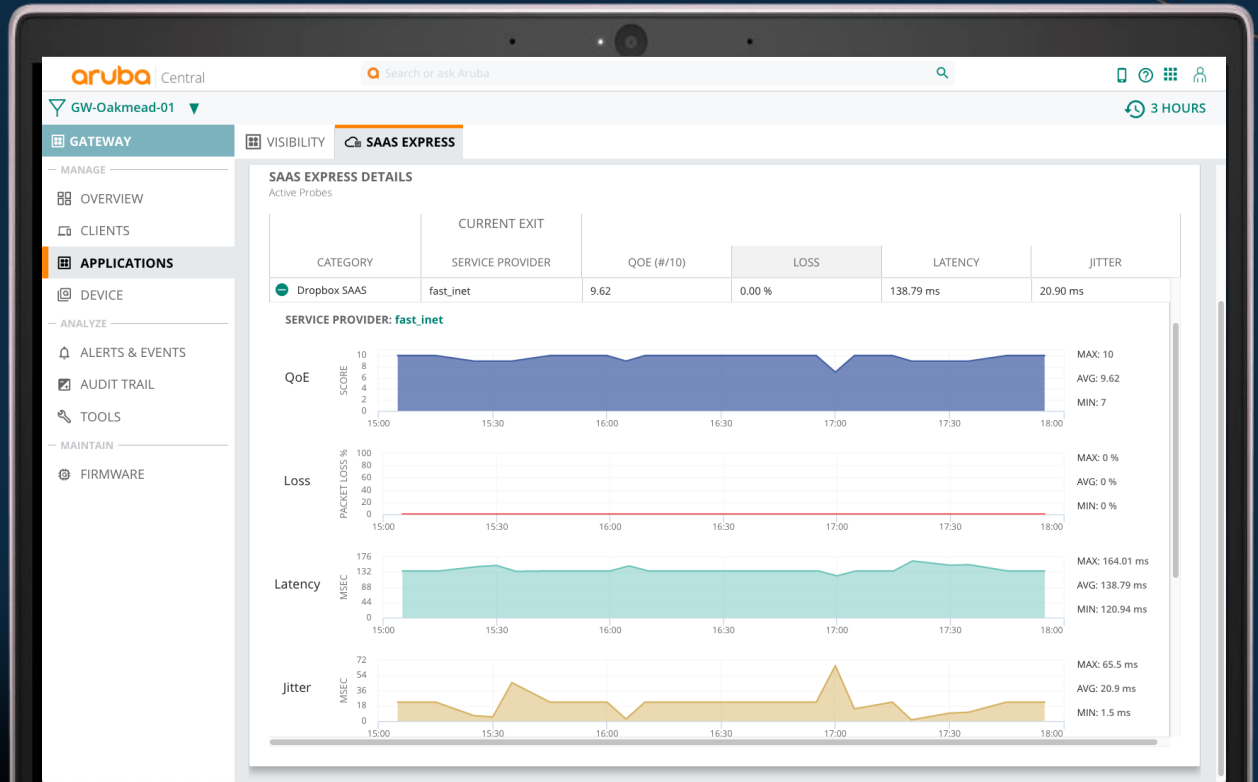
- Office 365와 같은 높은 업무 우선 순위 SaaS 솔루션에 대해 자동으로 최적화된 라우팅을 정의
- 각 지점의 엔드-투-엔드간 사용자 경험의 품질을 측정하기 위해 SaaS 서버로 HTTP 연결 시도
- 선택된 ISP를 통해 DNS Request 리다이렉트
- 최초 패킷 분류



중요 SaaS 성능 지표 시각화

1 모든 TCP 애플리케이션의 사용자 경험 시각화
(패시브 측정방식 기반)

2 중요 SaaS 애플리케이션에 대한 선택 경로와
사용자 경험에 대한 시각화
(액티브 프로브 기반)



SaaS 최적화

어떤 도움을 주나요?

- 무엇이 문제인가요?

- 전국적인 배포, 의존도가 높은 SaaS 서비스에 대해 전국 단위로 구축
- 기업 내 모든 단말들이 기업 데이터센터에 위치한 DNS 서버를 사용
- 기본 타이머를 사용하여 최대 30초 이내 Failover 수행 (2-3초 내로 줄일 수 있지만, 그것은 overkill이 될 것임)

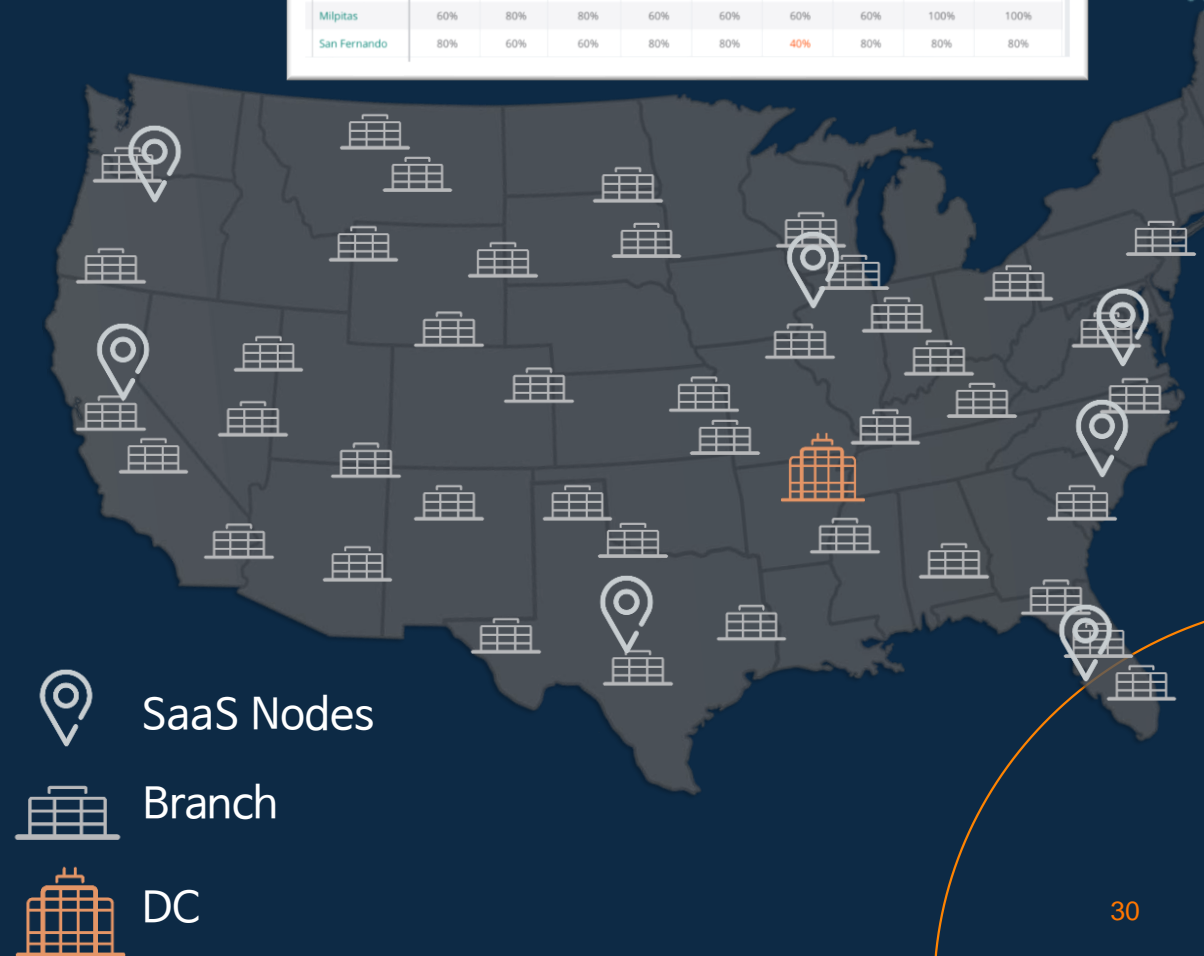
- 어떻게 해결해야 할까요?

- SaaS Express
 - 각 지점의 엔드-투-엔드간 사용자 경험의 품질을 측정하기 위해 SaaS 서버로 HTTP 연결 시도
 - 선택된 ISP를 통해 DNS Request 리다이렉트
 - 최초 패킷 분류

NETWORK HEALTH | DATA SOURCE SAAS EXPRESS | Grid | Status | Map

● NO ISSUES ● POTENTIAL ISSUES

SITE	DC1	DC2	DROPBOX	YOUTUBE	GMAIL	CITRIX	0365	GOOGLE	SALESFORCE
100 Unique Sites	80%	84%	82%	84%	94%	90%	80%	95%	95%
Mountain View	80%	90%	80%	90%	90%	90%	90%	100%	100%
Los Angeles	50%	50%	50%	50%	85%	35%	50%	100%	100%
Santa Clara	90%	90%	80%	80%	80%	31%	80%	80%	80%
San Jose	90%	45%	45%	80%	80%	80%	80%	80%	80%
San Francisco	60%	90%	80%	90%	90%	90%	90%	90%	90%
Santa Monica	80%	90%	80%	80%	80%	80%	80%	100%	100%
Sunnyvale	60%	80%	80%	60%	60%	60%	60%	100%	100%
Long Beach	80%	60%	60%	80%	80%	40%	80%	80%	80%
Milpitas	60%	80%	80%	60%	60%	60%	60%	100%	100%
San Fernando	80%	60%	60%	80%	80%	40%	80%	80%	80%





Security

각 지점을 위한 통합 보안



애플리케이션/사용자 인지 방화벽



Deep Packet Inspection



웹 콘텐츠 & URL 필터링



App & URL 평판 조회 및 차단



클라우드 보안 연동



침입 탐지 및 차단 시스템

NEW



위협 시각화

- 시간 외 근무시 발생할 위협 가능성
- 사용자 및 애플리케이션 시작과 함께 네트워크 방향으로 오버레이
- 위협 소스 및 임팩트

정책 중심 수행

- 즉시 사용 가능한 IDS / IPS 정책
- 사용자 정의 화이트리스트 (Whitelist)
- 오탐 관리 플로우

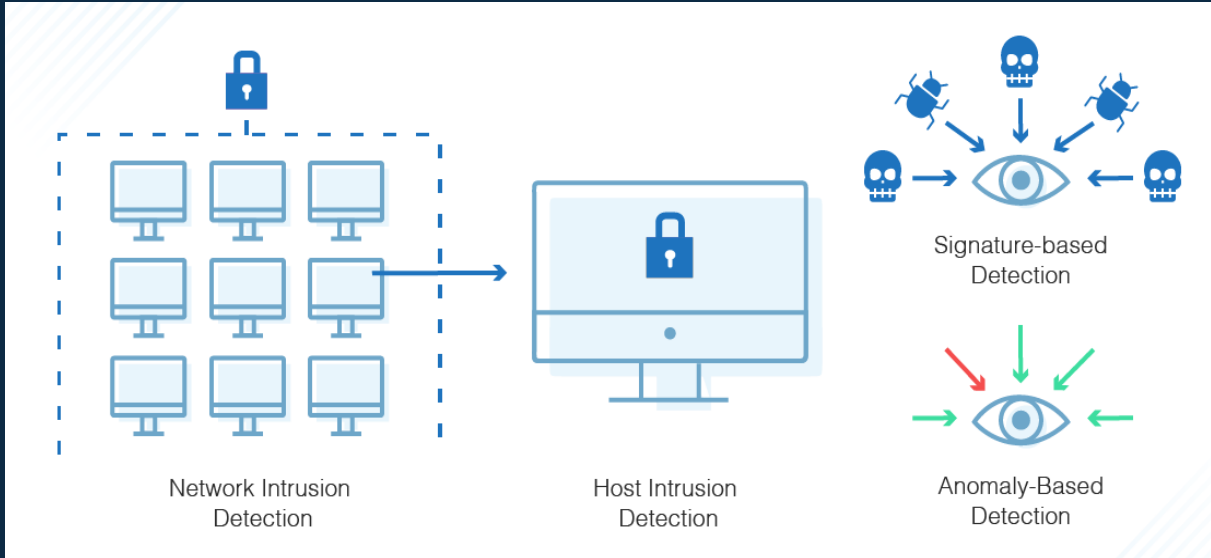


인시던트 관리와 상관관계 분석

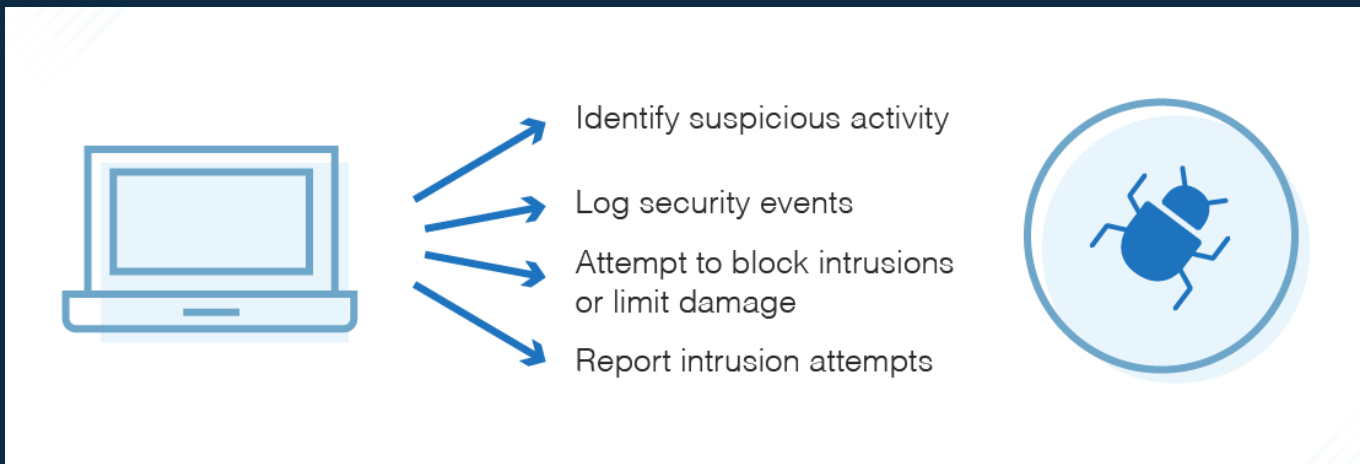
- 외부 연동 가능한 이벤트로 SoC로 스트리밍
- 비즈니스 영향도에 따른 알람과 알림
- REST 엔드포인트로 이벤트 스트리밍

IDS/IPS가 무엇인가요?

IDS



IPS



- 네트워크 IDS/IPS
- 룰셋 중심의 보안
 - 시그니처 기반
 - 패턴 기반
- 침입에 대한 대응
 - CVE 기반
 - 회피 공격
 - 사용한 시퀀스 추론 방식
- 전형적인 위협요소 포함
 - 스캐닝 공격
 - 비대칭 라우팅
 - 버퍼 오버플로우 공격
 - 특정 프로토콜 공격
 - 악성 코드
 - Traffic Flooding

보안 대시보드



- 시간 흐름에 따른 위협 시각화
 - 사용자/애플리케이션 시작 및 네트워크 트래픽 vs 위협
 - 위협 트렌드
- 위협 요소
 - 카테고리별, 유형별, 위험도별
 - 위협 확산
 - 영향 받은 사용자 및 장치
 - 소스 및 영향도 레벨
- 드릴 다운
- SIEM 연동 (Splunk가 첫번째 사례가 될 예정)



Dynamic Segmentation

역할 부여가
“Dynamic”

사용자 및 단말

- 임직원
- BYOD
- IOT
- 방문객



같은 VLAN 내에서도
“Segmentation”

애플리케이션 및 사용자

- Office 365 (Green checkmark)
- Network Camera (Red X)
- n0tma1ware .biz (Red X)
- AirGroup (Green checkmark)

역할 기반의 방화벽!!



역할 기반 보안으로 Micro-Segmentation

어떤 도움을 주나요?

– 무엇이 문제인가요?

- IoT로 인해 VLAN이 폭발적으로 증가 (20+)
- 개별적으로 구성된 VLAN 포트는 규모에 맞게 관리하기 어려움
- 대규모 NAC 프로젝트 (100개 이상의 병원/클리닉 등)에서는 증가하는 VLAN을 관리하기 어려움
모든 장치가 CoA에 따른 연결 해제에 반응하는 것은 아님

– 어떻게 해결해야 할까요?

- 인프라 관리를 위한 언더레이 VLAN
- 각 지점 서비스를 위한 오버레이 VLANs for branch services (VLAN 1개 정도)
- 역할 기반의 보안 정책



클라우드 보안 시스템 연동

고급 보안이 가장 적절한 곳은 어디인가요?

수동적인 연동 방식



클라우드
보안으로 PBR

역할 기반의
접근 정책

오케스트레이션을 통한 연동



1. API를 통한 "site" 생성
2. 가장 가까운 클라우드 위치 찾기
3. 터널링 구성



PBR to Cloud
Security

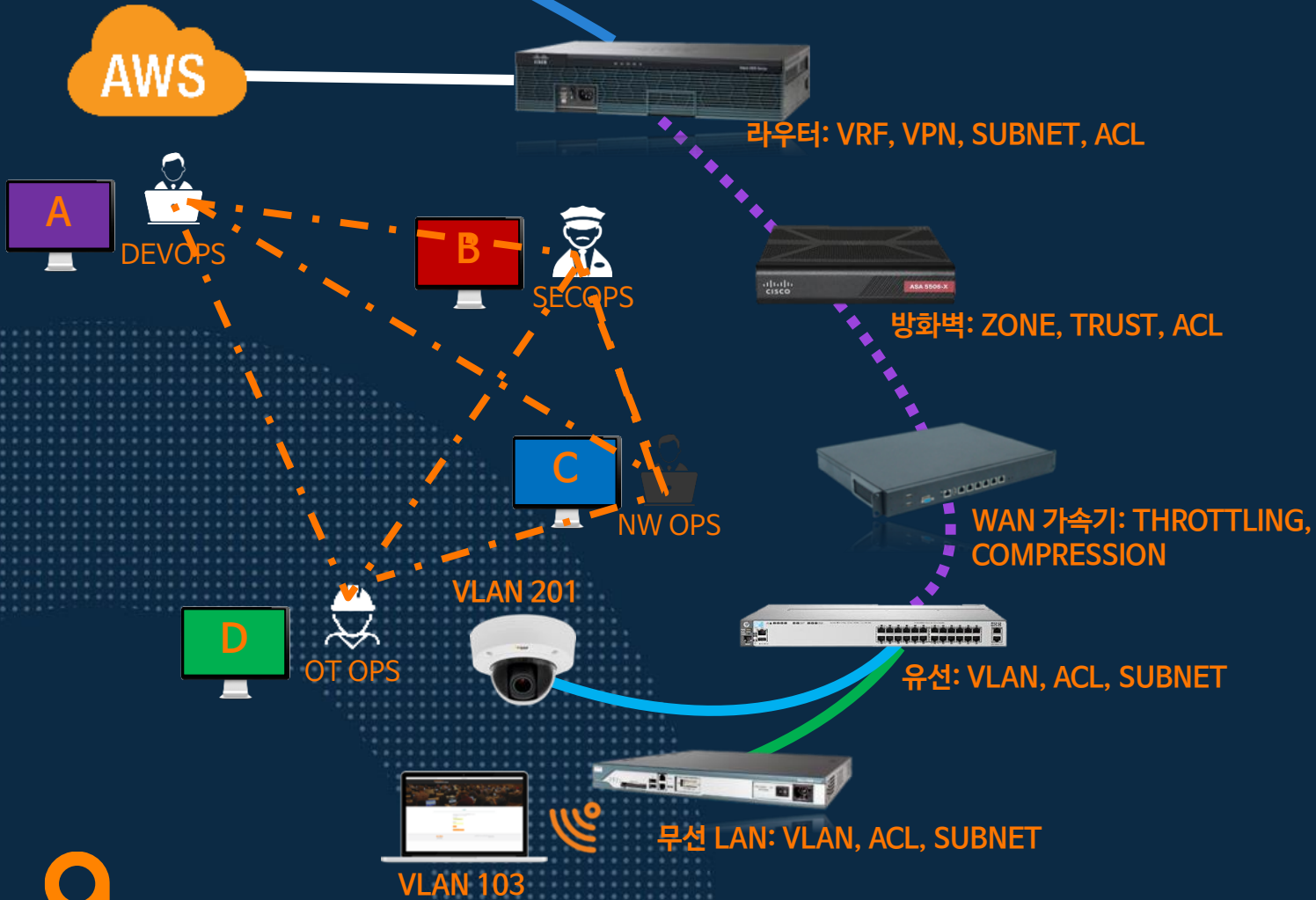
역할 기반의
접근 정책



Operation

엔드-투-엔드 SD-Branch 솔루션

왜 중요한가요?



COMPLEXITY BEFORE



엔드-투-엔드 SD-Branch 솔루션

왜 중요한가요?

SIMPLICITY AFTER

통합 DYNAMIC
SEGMENTATION:
유선, 무선, WAN, 보안



NETWORK
MANAGEMENT



SECURITY



LOCATION
SERVICES



ANALYTICS
& ASSURANCE

정책 중앙화



AWS



모든 트래픽이
보호됨



Aruba 클라우드 플랫폼 - 엔드-투-엔드 네트워크 서비스

경험 중심의
매니지먼트

LAN / WAN / WLAN



Aruba-OS
스위치



보안
게이트웨이



독립형
액세스 포인트

부가 서비스 (옵션)

게스트
Wi-Fi



방문객
분석



인공지능
인사이트



SD-WAN



보안



REST API를 통한 확장성
(구성, 모니터링, 알람 및 안전한 접속)

간소화된 프로비저닝
& 워크플로우 기반의 운영 모델

포괄적인 관리 및 지능형 자동 인사이트

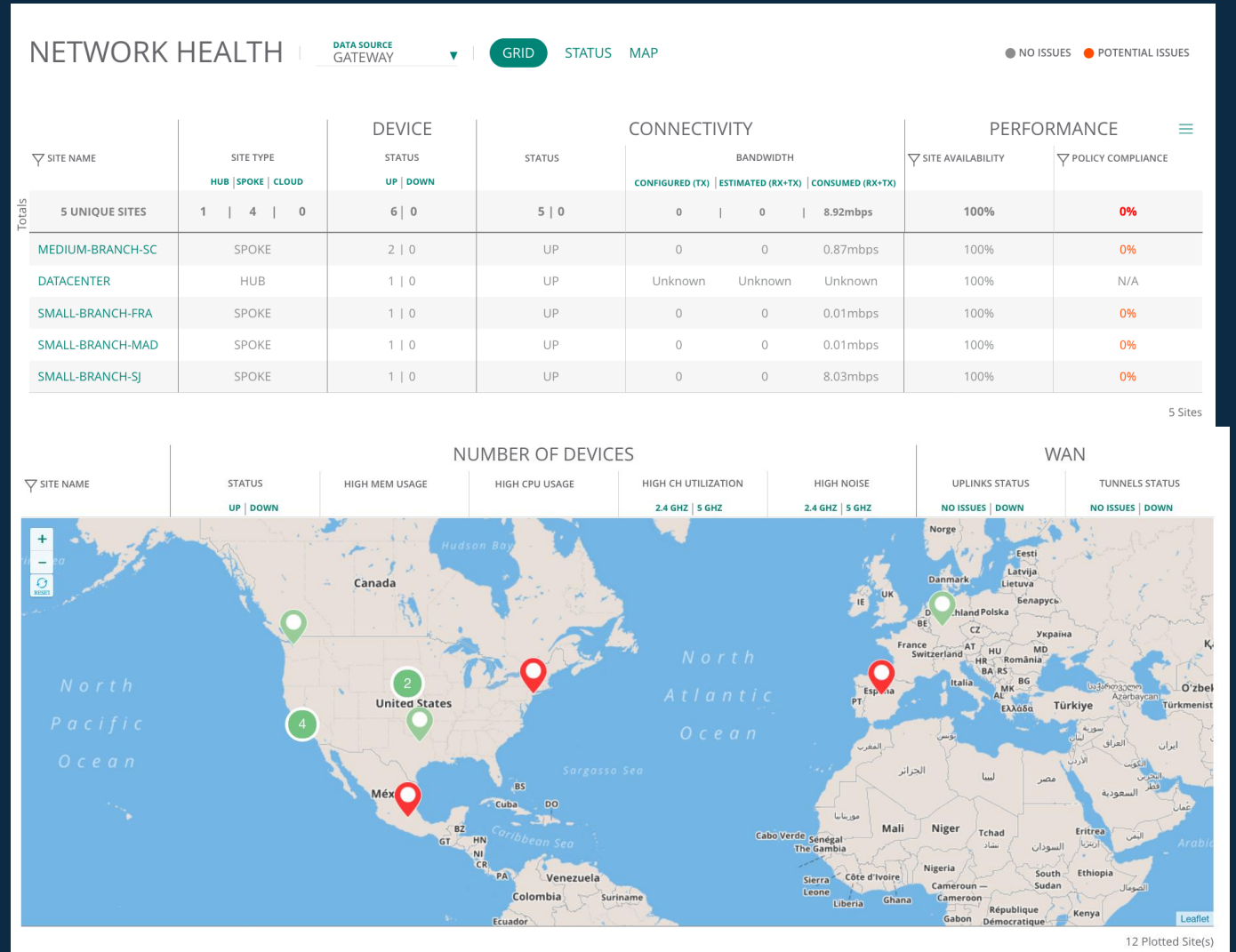
모바일과 IoT 단말 프로파일링이
통합된 플랫폼

3rd party 소프트웨어 솔루션과
연동을 위한 API 내장



상태 대시보드

- 두 가지 접근 방식에 따른 모니터링
 - 패시브하게 수집되는 매트릭 값 및 통계
 - 통합 트랜잭션으로부터 액티브하게 수집되는 매트릭 값과 통계
- 세 가지 방식으로 결과 제공
 - API를 통해서 또는 API 기반의 알림
 - 추출 가능한 리포트를 통한 방식
 - Central 대시보드를 통한 방식



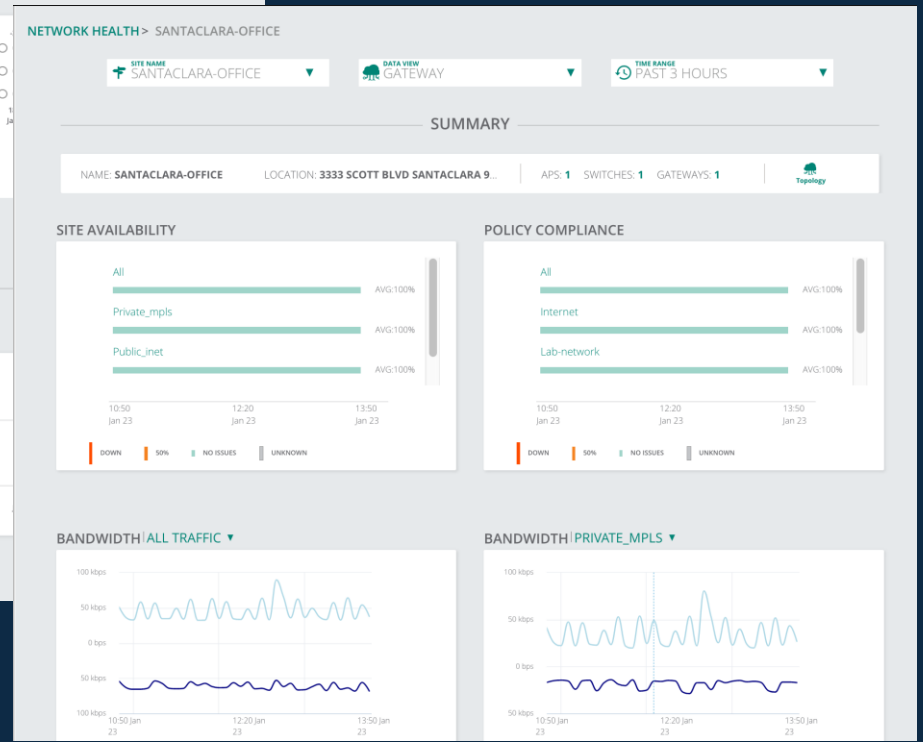
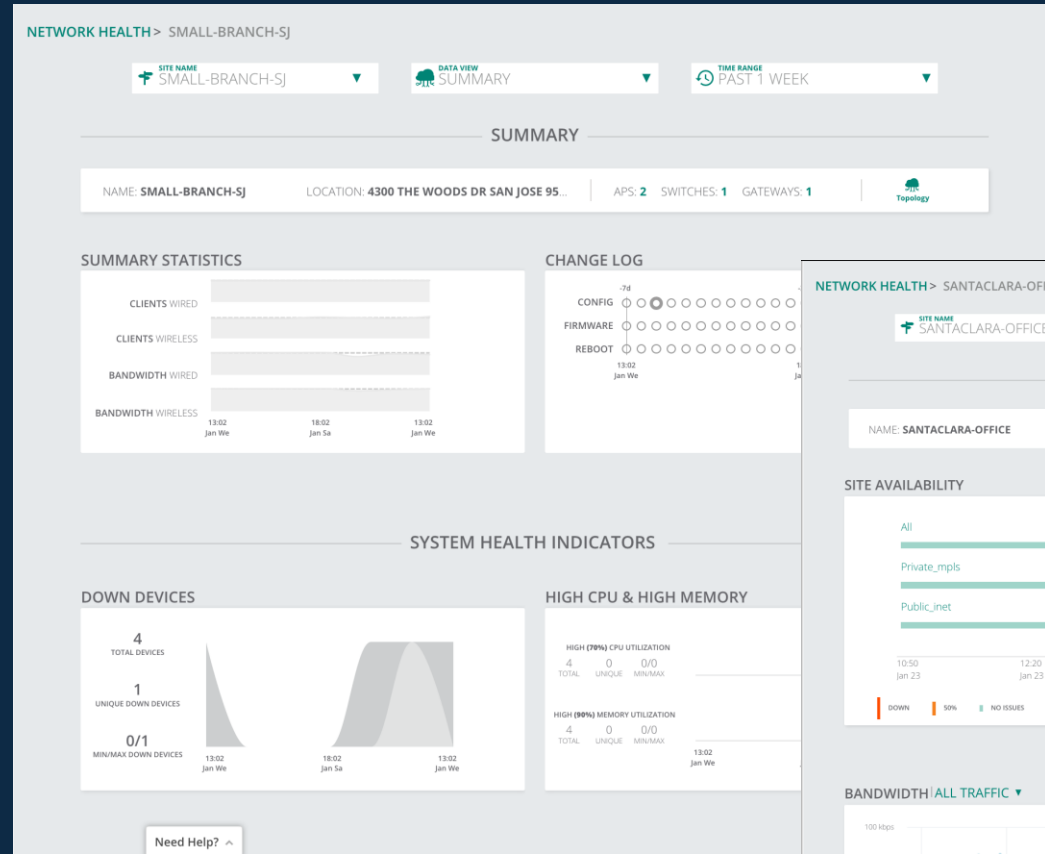
사이트 상태 대시보드

- 시스템 상태 표시
 - 장치 연결 끊김
 - CPU 사용량
 - Memory 사용량

- 무선 상태 표시
 - 채널 사용량 (5/2.4Ghz)
 - 총간 노이즈 (5/2.4Ghz)

- 클라이언트 상태 표시
 - 클라이언트 상태 값 점수화 (Scoring)
 - 연결 상태 값 점수화 (Scoring)

- WAN 상태 표시
 - 정책 준수 여부
 - WAN 사용량



토폴로지 View

- 계층적 또는 방사형 방식
- 상태 현황 확인
- 주변 정보
- VLAN 오버레이

FILTER MONITORING & REPORTS
SMALL-BRANCH-SJ (4 Total Devices | 0 Offline APs | 0 Offline SWITCHES | 0 Offline GATEWAYS)

GW-SanJose-1
SW-SanJose-1
IAP-SanJose-1
IAP-SanJose-2

Details Filter

Name: GW-SanJose-1
Serial: CR0012809
IP: 10.90.120.1
MAC: 20:4C:03:06:F0:B0

Type: BOC
Model: Aruba7030-US
Status: ↑
Health: ●

Tunnels:

● GW-SanJose-1:uplink-1_mp... ^

VLAN: 430
Established Time: 2019-01-23 11:34 AM
Peer MAC: 00:1A:1E:02:3B:58
Port Number: 7
Source IP: 172.16.1.3
Destination IP: 10.67.70.111

● GW-SanJose-1:uplink-2_ine... ▾



사용자 및 애플리케이션 중심의 Branch 시각화

사용자 중심

The user-centric view shows a network diagram of the Sanjose-Office branch. It features two uplink links (uplink-1_mph and uplink-2_inet) connected to a central gateway (GW-Sanjose-1), which is then connected to a switch (SW-Sanjose-1) and two IAPs (IAP-Sanjose-1 and IAP-Sanjose-2).

Details:

- Uplink Type: Internet
- VLAN: 431
- Link Status: ↑
- Description: uplink-2_inet
- WAN Status: ↑
- Public IP: 0.0.0.0
- Device MAC: 20:4C:03:0A:84:60
- Serial: CNCB5P00R
- Port Number: GE 0/0/6

Sanjose-Office Dashboard:

- Filter Monitoring: ZAG3KH40CC
- Device Health: 100%
- SNR: 54dB
- Tx Rate: 144 Mbps
- Rx Rate: 300 Mbps
- Connected to: IAP-Sanjose-1

Data Path: CLIENT (ZAG3KH40CC) → SSID (SD-Branch-Guest-UP) → AP (IAP-Sanjose-1) → SWITCH (SW-Sanjose-1) → GATEWAY (GW-Sanjose-1)

Client Details:

CLIENT	NETWORK	CONNECTION
USERNAME: --	VLAN: 460	CHANNEL: 52 (40 MHz)
HOSTNAME: ZAG3KH40CC	SSID: --	BAND: 5GHz
IP ADDRESS: 192.168.1.7	AP ROLE: SD-Branch-Guest	CLIENT CAPABILITIES: 802.11an
MANUFACTURER: Aruba Networks	AP DERIVATION: Radius	CLIENT MAX SPEED: 600 Mbps
CONNECTED SINCE: May 17 2019 15:48:--	GATEWAY ROLE: guest-device-role	
	AUTH SERVER: --	
	DHCP SERVER: 192.168.1.1	

애플리케이션 중심

The application-centric view provides a detailed look at network sessions and application usage. It includes a sessions summary table, a detailed sessions table, and two bar charts showing application and website usage.

SESSIONS SUMMARY:

CURRENT ENTRIES	MAX ENTRIES	HIGH WATER MARK	ALLOCATION FAILURES	DENIED ENTRIES
1853	16383	8203	120	162

SESSIONS (LAST UPDATED: 5:45:01 PM):

APPLICATION	SOURCE IP	DESTINATION IP	APP PORT	ACTION	PACKETS	STATE
RTP	192.168.64.254	192.168.64.194	1820	Permit	3209	Established
YouTube	192.168.64.254	208.65.153.251	443	Permit	243043	Established

APPLICATIONS: A bar chart showing application usage over time. Key applications include Google Play (416.4 MB), YouTube (208 MB), and Facebook (156.3 MB).

WEBSITES: A bar chart showing website usage over time. Key websites include Computer and Internet Info (192.2 MB), Social Networking Web (155.7 MB), and Business and Economy (152.5 MB).

클라이언트 뷰

- 엔드-투-엔드 시각화 완성:
 - 클라이언트 정보
 - 무선 및 상태 정보
 - 위치
 - Clarity
 - UCC
 - ...

The screenshot displays the Aruba Central interface for monitoring clients. It is divided into two main sections: 'site-name-007' and 'site-name-001'.

Site-name-007 Overview:

- Access Points: 12.4k (30) | Switches: 249 (3) | Gateways: 12 (0) | Clients: 8.73k (23)
- Client: sriram.venkiteswaran
- Device Health: Good | Retries: 95% | SNR: -68 dBm | Rate: 54 Mbps
- Connected to: aruba-ap-001

Site-name-001 Overview:

- Access Points: 12.4k (30) | Switches: 249 (3) | Gateways: 12 (0) | Clients: 8.73k (23)
- Client List: site-name0829..
- Summary: 8412 WIRELESS, 1025 WIRED, 9658 BLACKLISTED

Client List Table (Site-name-001):

CLIENT NAME	STATUS	REASON / HEALTH	TIME LAST SINCE	CONNECTED TO		LINK		ROLE	
				AP SWITCH	SSID PORT	IAP	GATEWAY		
Nick's Ipad	Failed	DHCP	Jul 20 23:30	AP-002	HP - Guest	NA	NA	NA	NA
Scott	Failed	Captiveportal	Jul 20 23:30	AP-002	HP - Employee	NA	NA	NA	NA
Jay's Desktop	Failed	DHCP	Jul 20 23:30	SW-001	PORT 0/0/1	NA	NA	NA	NA
FCF8AE010010	Failed	Association	Jul 20 23:30	AP-002	HP - Guest	NA	NA	NA	NA
80001COMMA	Failed	DHCP	Jul 20 23:30	SW-002	PORT 0/0/2	NA	NA	NA	NA
Rocky Jay 22	Failed	Dot 1x	Jul 20 23:30	NA	HP - Employee	NA	NA	NA	NA
SID's PC	Connect...	POOR	Jul 20 23:30	AP-002	NA	Employee	Employee	NA	NA
F1081RAY	Connect...	FAIR	Jul 20 23:30	SW-003	PORT 0/0/3	NA	NA	NA	NA
Senthil's Android	Connect...	GOOD	Jul 20 23:30	AP-002	HP - Guest	Guest	Guest	NA	NA
FCF8AE010010	Offline	NA	Jul 20 23:15	AP-002	HP - Guest	Guest	Guest	NA	NA
Sid - Android	Offline	NA	Jul 20 23:15	AP-002	HP - Employee	Guest	Guest	NA	NA
F5772HEEP	Offline	NA	Jul 20 23:15	AP-002	NA	NA	NA	NA	NA
Senthil's Kali Li...	Blacklist...	NA	Jul 20 23:30						

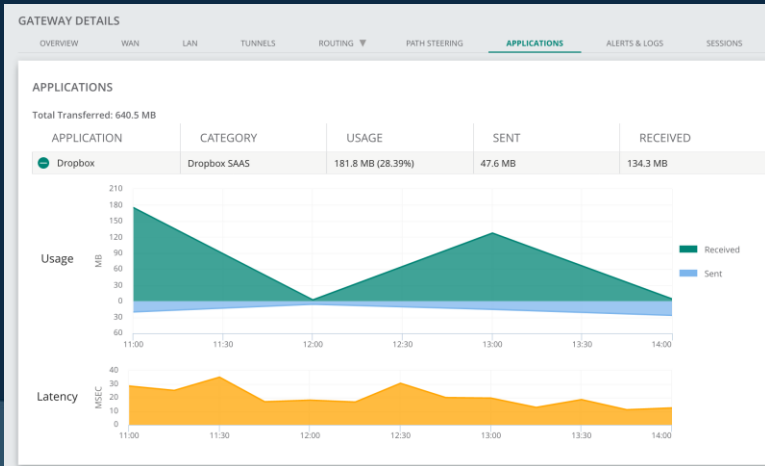


AP/스위치/게이트웨이 모니터링 개선

클라이언트 시각화 페이지에서 클릭으로 확인

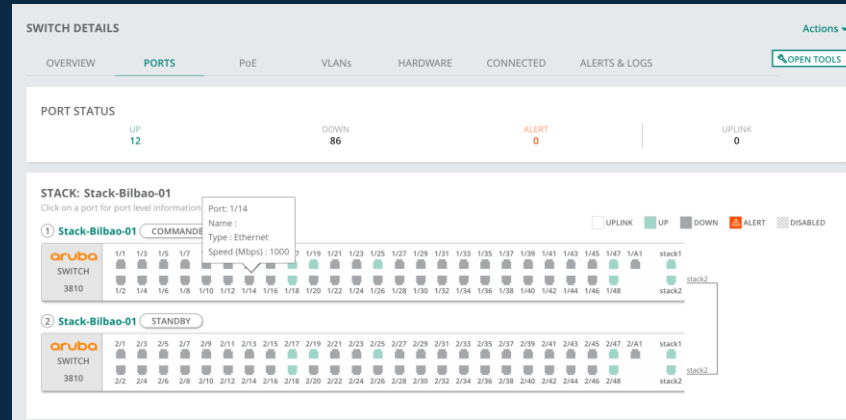
게이트웨이 상세 페이지

- 한 눈에 보여줌



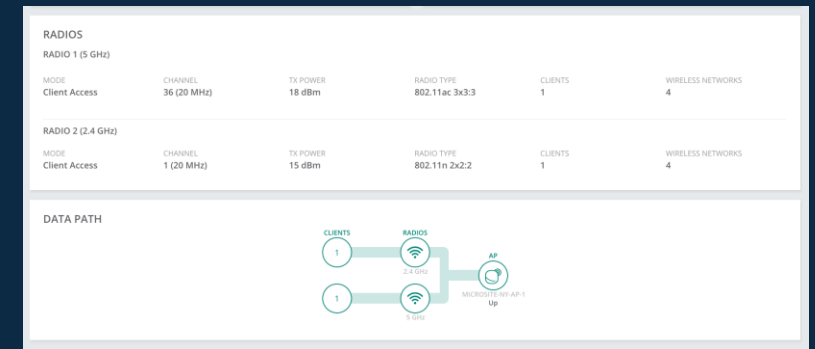
스위치 상세 페이지

- 한 눈에 보여줌



AP 상세 페이지

- 한 눈에 보여줌
- 세그웨이에서 게이트웨이까지



간소화된 운영

어떻게 동작하나요?

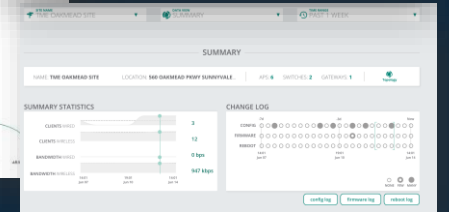
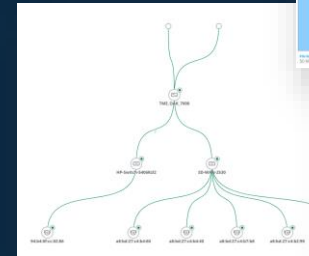
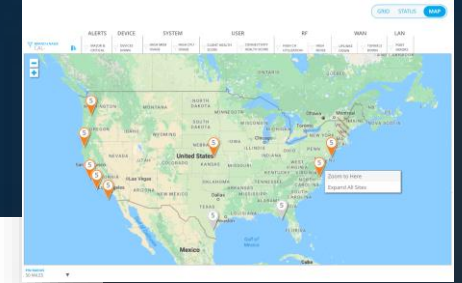
1

작업 생성

SITE NAME	CITY	STATUS	INSTALLED DEVICES	INSTALLATION DATE
6 UNIQUE SITES				
Salzburg	Salzburg	In Progress	0 0 1	Tue May 29 2018
EMEA-ATM-18	Siberik	In Progress	1 0 1	Tue May 29 2018
TME Oakmead Site	Sunnyvale	In Progress	1 0 0	Tue May 15 2018
TME Santa Clara Site	Sunnyvale	Pending		
SEEL-45	Sunnyvale	Pending		
SmallSite	Independence	Pending		

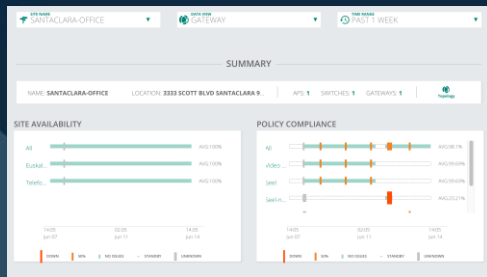
2

설치 기사가 장치 스캐닝



3

지리별 단말 태깅 Branch 뷰 생성



Report

API

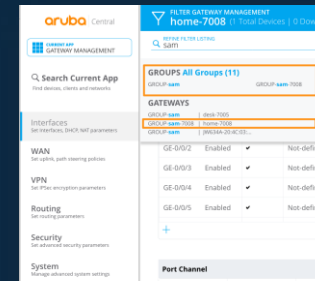


5

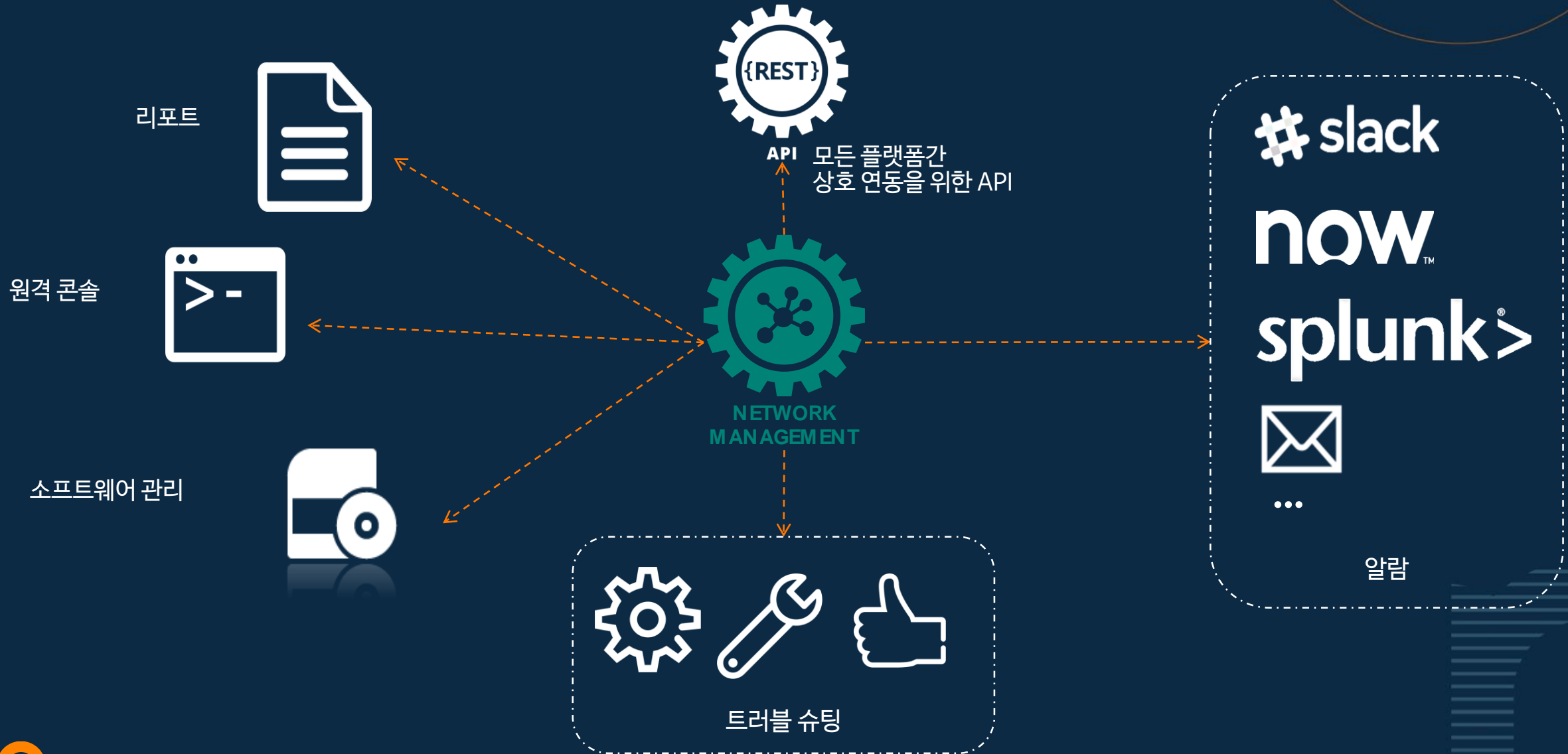
사이트 및 그룹 기반으로 사전 경고 및 리포팅

4

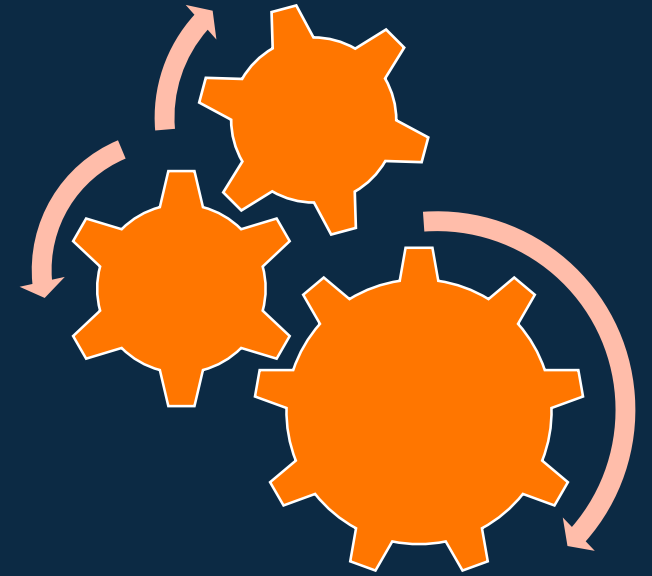
자동 SW 업그레이드 계층적으로 구성 요소 내려 받기



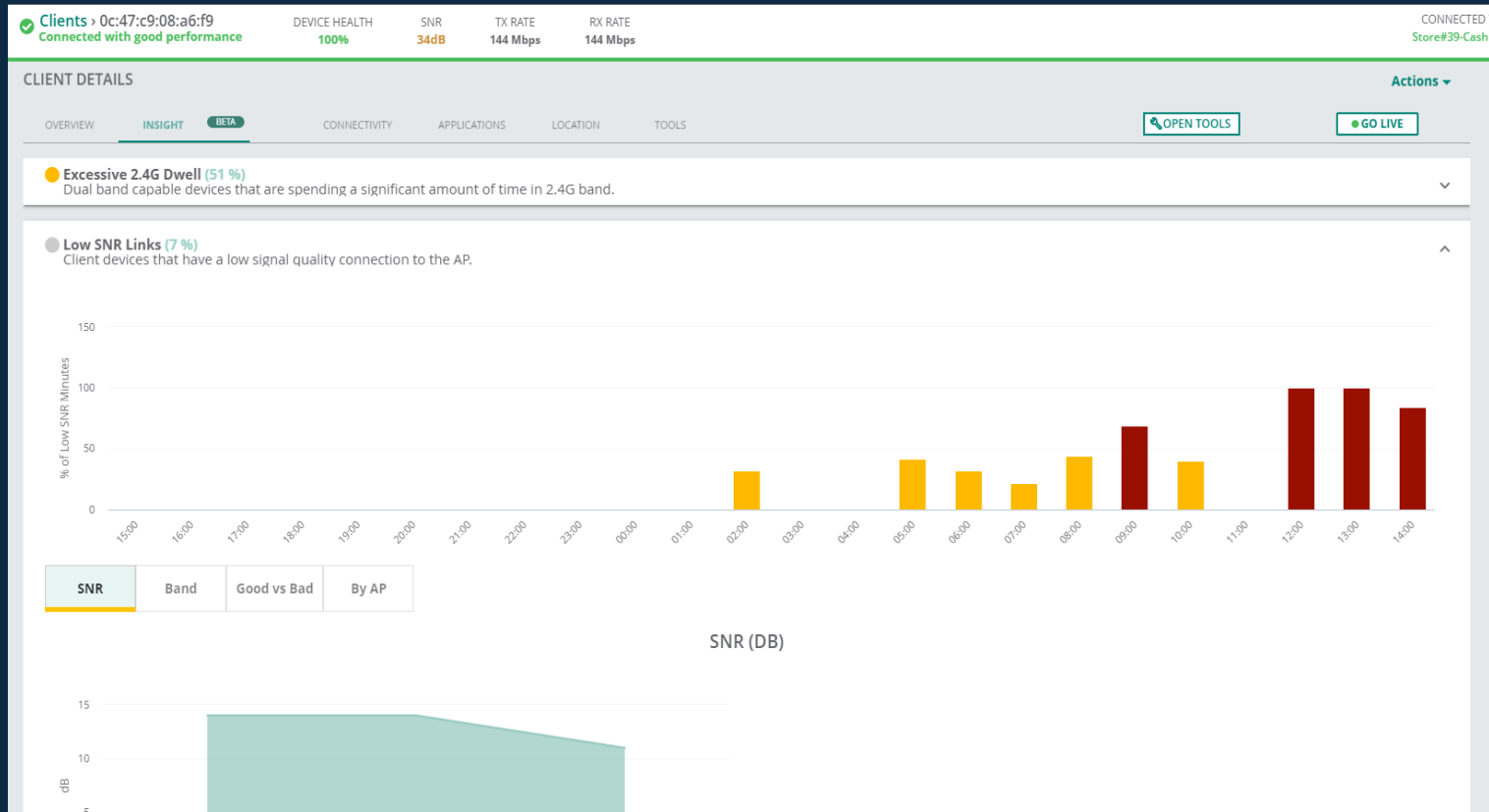
단순 모니터링 이상의 것들을...



Aruba Central로 고급 트러블 슈팅 워크플로우



시인사이트



인사이트를 통해 사전 예방 및
보다 효율적 운영

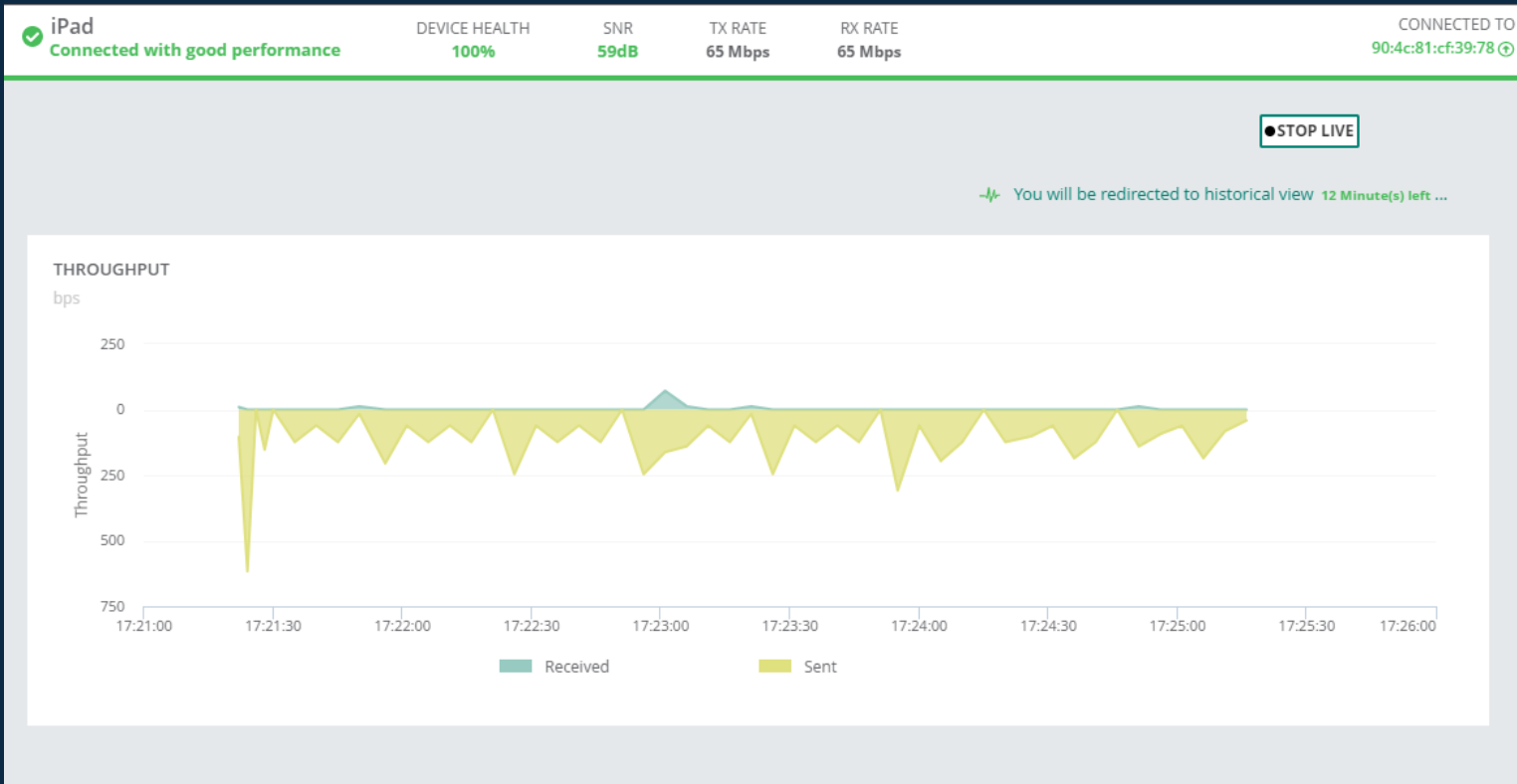
전반적인 성능의 요구사항과
기대치를 충족하도록 보장

규범적 권고사항으로
추측적인 작업을 대체

클라이언트와 IoT 단말의 상태 값
및 트래픽과 사용자 경험의 이해



클라이언트 및 단말 트러블슈팅



한 눈에 상태 및 노이즈,
전송/수신 값 확인

현 상태에 대한 상세 확인을 위한
라이브 모니터링

추가적인 분석과 상세정보를 위한
패킷 캡처 기능

자동으로 표준 모니터링으로 복귀
(~15분)

Summary

사용자 경험 향상





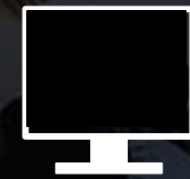
보안 및
컴플라이언스



VPN



클라우드
애플리케이션



VDI Farm에서
원격 데스크톱

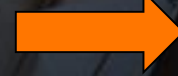
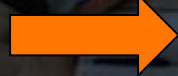
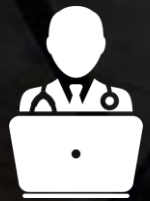


보안 및
컴플라이언스

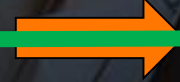
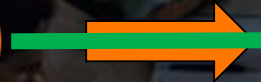


연결 방식

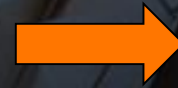
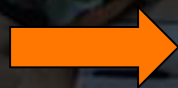




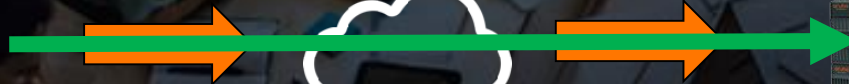
연결 방식



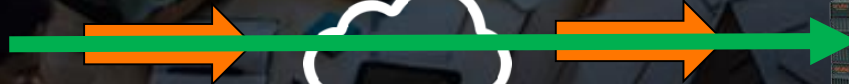
연결 방식



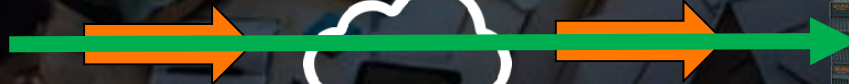
연결 방식



연결 방식



연결 방식

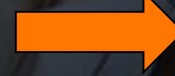
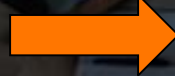


연결 방식



구축 및 설치

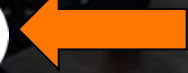


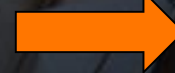
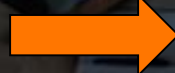


구축 및 설치



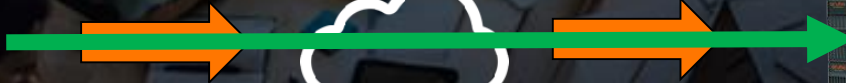
활성화 및 등록





구축 및 설치





구축 및 설치





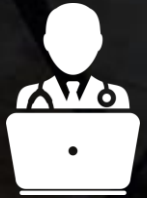
연결 방식



연결 방식



연결 방식



매니지먼트



Aruba Central



매니지먼트

Q&A



STAY SAFE
STAY CONNECTED

