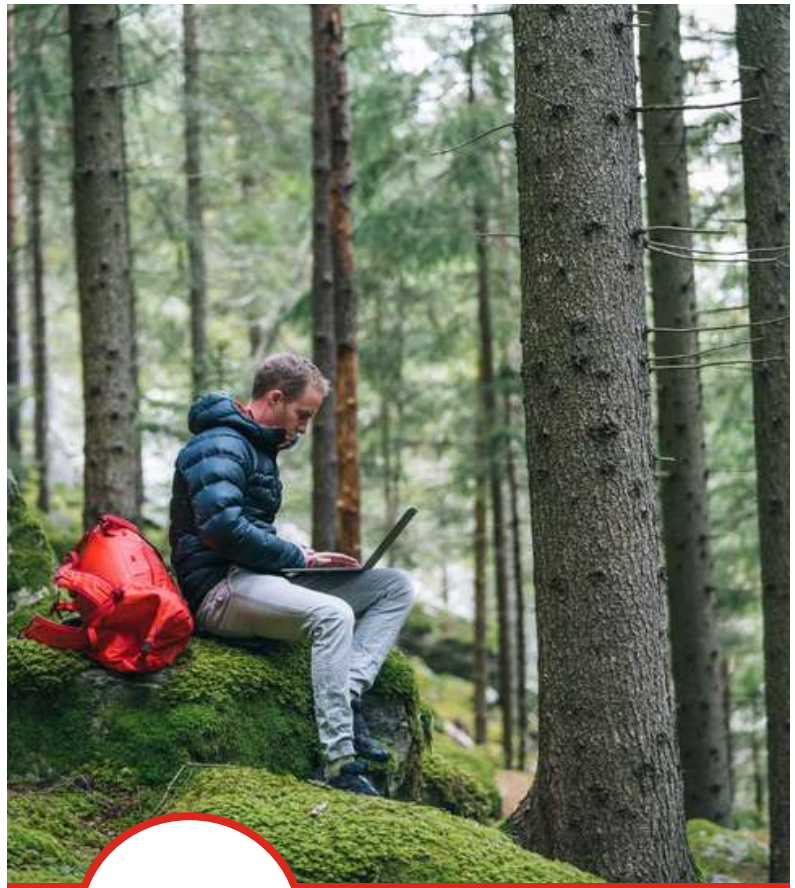
포티넷 SASE 솔루션으로 인프라 환경에 제약없이 유연한 보안 구축

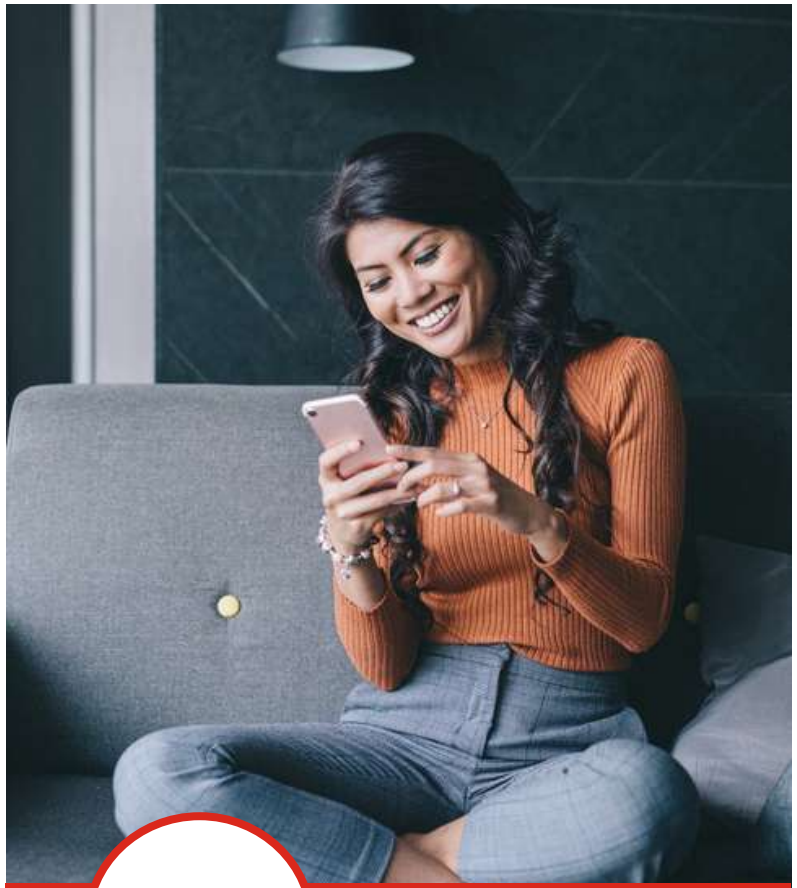
: WAN Edge 및 Security Service Edge 환경에 맞게 구축하기

포티넷 코리아 이창운

어디에서나 일하는 새로운 세계



72% Hybrid Workforce



70% Use Any Device

93% Access Cloud Apps

오늘날의 트렌드에 대한 제로 트러스트 사고방식

코로나 이후 원격 근무 고착화

"재택근무로의 전환은 팬데믹 이후에도 지속될 것으로 예상됩니다. **CIO의 52%는 2021년에 재택 근무가 증가할 것으로 예상합니다"**

Gartner – Top Priorities for IT: Leadership Vision for 2021

디지털 전환 가속에 동반되는 보안 요건

"이사회의 69%는 디지털 전환 가속화로 COVID-19에 대응했으며, 60%는 디지털 비즈니스를 통해 운영 우수성을 개선하였습니다"

Gartner – Top Priorities for IT: Leadership Vision for 2021

끊임없는 랜섬웨어/악성코드와의 창과 방패 싸움 증가

36%의 조직은 랜섬웨어 공격을 방지하는데 가장 큰 걸림돌은 **점점 정교해지는 공격 기술이라고 말합니다.**

Fortinet – Ransomware survey 2021

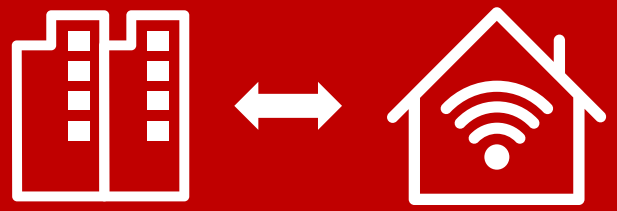
만성적인 사이버 보안 전문 인력 부족

73%의 조직이 작년 최소 1회 이상의 사이버 보안 기술 격차로 인해 발생한 **보안 침해 사고를 경험하였습니다**

Fortinet – Cybersecurity Skills Survey 2,500 US and Canadian companies 2021

오늘날의 트렌드에 대한 제로 트러스트 사고방식

하이브리드 업무 형태는 여전히 지속되고 있음



"재택근무로의 전환은 팬데믹 이후에도 지속될 것으로 예상됩니다. CIO의 52%는 2021년에 재택 근무가 증가할 것으로 예상합니다."

Top Priorities for IT: Leadership Vision for 2021
Gartner®

공격 표면의 확장 및 다양화

"응답자의 거의 절반이 직원의 재택 근무나 원격 근무 환경에 대해 보안을 효과적으로 적용할 수 없다고 말했습니다.."

Cybersecurity Survey: April 2020
Dimensional Research

새도우 IT의 지속적인 존재

"최근 설문조사에서 응답자의 37%는 임직원이 IT부서의 직접적인 승인없이 모바일 전용 애플리케이션을 구매했다고 말했습니다."

2021 Digital Readiness Survey
ManageEngine

해결해야 할 사이버 보안 챌린지의 지속적인 증가

사용자, 디바이스 보안

출장, 외근자

WFH
재택/원격 근무

사무실 근무자

스마트
팩토리 공장

네트워크 보안

Wi-Fi

스위치

SD-WAN

5G

클라우드-온-
램프

애플리케이션 보안

클라우드

데이터 센터

SaaS

엣지 컴퓨팅

SecOps (섹옵스, 보안팀)

격리된 사일로
제품들과 독자 기술
제품 존재

관리 불가능할
정도의 시스템
경고량

사이버 보안 전문
인력 부족

공격자 : 대용량
자동화된 사이버
보안 공격

다중 단계별 기획된
사이버 보안 공격

머신러닝을 이용한
공격 우회 전술 출현

보안 침해 사고로 인해 증가되는 경제
손실과 인사(HR) 충격

장치 유형 및 사용자 접속 위치에 관계없이 일관된 엔터프라이즈급 보안 보장

디지털 전환 가속에 따라, 다양한 신생 네트워크 엣지 도입으로 인해서, 현존 보안 경계(Perimeter) 기반의 보안 정책의 한계 극복이 시급히 필요함

애플리케이션과 데이터의 지속적인 마이그레이션과 멀티 클라우드로 분산됨으로 인한 복잡한 운영 오버헤드 생성과 보안 문제 야기

수 많은 보안 제품과 이벤트 정보의 양은 만성적인 인력 부족에 시달리는 보안팀을 압도하여 신속한 보안 사고 탐지 및 대응 능력을 저하시킴

공격자는, 기업 인프라 공격 대상 표면 및 주기에 걸쳐서 인공지능 기반의 통찰력과 대규모 공격 자동 실행을 활용하여 지속적으로 혁신할 것임

IT 환경 변화를 이용한 공격 사례

재택근무로 늘어난 '빈틈' 노린다…전세계 10초당 1건 랜섬웨어 피해

무차별 유포는 옛말, 마약 조직처럼 분업화·전문화

직원들 이메일·원격 업무망등
보안 취약한 침투경로 많아져
전세계서 10초당 한 번꼴 피해

작년 의료기관 공격 45% 쑥
환자 데이터 빼내 공개 협박
몸값 협상 전문가까지 등장

◆ 랜섬웨어 주의보 ◆

재택근무의 역습, 누군가 우리집 PC를 노린다

안경애 기자 | 입력: 2021-02-23 10:11

서울 송파구 삼성SDS 사옥 전경

삼성SDS(사장 황성우)는 지난해 국내외에서 발생한 보안 이슈와 현장 사례를 분석해 '2021년 사이버보안 7대 트렌드'를 선정해 발표했다.

7대 트렌드로는 △비대면 환경을 노린 위협 증가 △랜섬웨어 고도화 △AI를 활용한 해킹 지능화 △산업설비에 대한 위협 본격화 △개인정보 등 민감 데이터 보호 중요성 증대 △클라우드 대상 공격 증가 △의료분야 집중 공격이 꼽혔다.

IT 환경 변화를 이용한 공격 사례

VPN 취약점 악용 공격 증가

VPN (Virtual Private Network)

주로 서버에 대한 원격 접속 용도로 사용되며, 공용 네트워

COVID-19로 인한 재택근무가 증가하고, 이에 대한 보안 대

VPN 제품 취약점을 이용한 공격이 성공한다면, 해당 제품

알려진 VPN 취약점은 패치가 신속히 제공되지만, 일부 사

2021년 6월, 한국원자력연구원, KAI (한국항공우주산업)가

한국원자력연구원 해킹 내용

21.05.14.금	해킹 발생
21.05.29.토	한국과학기술정보연구원 -> 한국원자력
21.05.31.월	보안 조치

- VPN 취약점을 통해 외부인이 일부 시스템에 접속한 이력
- 13개 외부 IP주소에서 VPN 시스템 비인가 접속
- 피해 IP주소: VPN, 메일 시스템, KMS 인증 서버 (Windows, Unix)

한국원자력연구원과 같은 VPN 제품을 사용하고 있던 KAI 역시 해킹당해 중요 정보가 유출됐다.

게다가 해당 VPN 제품은 국내 VPN 1위 업체로 공공기관, 기업, 학교 등 400여 곳에서 사용하고 있다.

해커는 발견한 취약점으로 여러 기관을 동시다발적으로 손쉽게 해킹할 수 있게 됐다.

국정원도 이미 지난 4월부터 해당 제품이 해커에게 뚫렸다는 사실을 파악하고 보안 조치를 요구했다.

하지만, 보안 업데이트 등 대처가 늦어지며 해킹을 막지 못했다. [3]

해킹에 뻥뚫린 재택근무필수 VPN, 킹 북한 해커소행

2021년 7월 8일 pitchone 0

KISA 2 sslvpn 1 VPN보안 1 과기정통부 33 국정원 4 이반티코리아 1 한국인터넷진흥원 4

코로나시대로 재택근무가 일반화하면서 가상사설망(VPN)을 통한 해킹 및 악성코드
련 보안대책이 시급한 것으로 지적된다.

원자력연구원의 해킹 통로 전락한 VPN, 공공기관 취약점 점검 나섰다

cfpa 0건 277회 21-06-30 11:55

출처 : 보안뉴스

https://www.boannews.com/media/view.asp?idx=98570

보안뉴스 원병철 기자] 한국원자력연구원의 해킹 사건이 공개된 이후, 조사가 급물살을 타고 있다. 현재 과학기술정보통신부(이하 과기정통부)와 국가정보원이 한국원자력연구원 해킹사건으로 현장조사를 실시하고 VPN을 통한 전산망 침투를 확인한 것으로 알려졌다. 이와 관련 정부부처 및 공공기관을 중심으로 VPN 점검에 나선 것으로 확인됐으며, 공공기관에 많이 공급된 국내 특정 VPN 솔루션이 중점 점검대상이 되고 있는 것으로 본지 취재 결과 드러났다.

특히, 국가정보원은 원자력연구원에 취약한 VPN 운영을 중단하도록 조치했고, 연구원 보안장비를 통해 해킹 경유지를 차단하도록 하는 등 긴급 대응했다고 밝혔다. 아울러 관계부처와 합동으로 피해규모와 공격 배후에 대해서도 확인하고 있다고 덧붙였다. 또한 국가/공공기관을 대상으로 취약점이 확인된 VPN 제품에 대해 장비제조사와 협조해 보안패치를 설치토록 하는 등 추가 피해예방을 위해 노력하고 있다고 밝혔다.

과기정통부 역시 국가정보원과 함께 이번 사건을 조사하고 있으며, 한국인터넷진흥원(KISA)은 이번 사건의 핵심인 VPN의 취약점을 확인하고 제조사에 대책을 촉구한 것으로 알려졌다.

IT 환경 변화를 이용한 공격 사례

Gang teases Samsung data leak

In a note posted earlier to
extortion gang teased abo
Samsung data with a snap
C/C++ directives in Samsu

NVIDIA는 최근 사이버 공격에서 데이터가 도난당했음을 확

칩 제조업체의 거인 Nvidia는 지난 주 사이버 공격으로 네트워크가 침해되어 침입자가 독점 정
세스할 수 있게 되었음을 확인했습니다.

LAPSUS$ 해커들, 마이크로소프트와 인증 회사인 Okta 해킹했다고 밝혀

LAPSUS$ Hackers Claim to Have Breached Microsoft and Authentication F

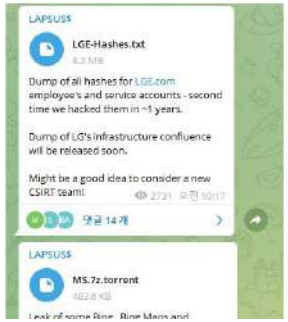
LAPSUS$가 마이크로소프트 및 인증 서비스 제공업체인 Okta를 해킹했다고 밝히 회사에
하고 있다고 밝혔습니다.

이 사고는 Vice 및 Reuters가 처음으로 보도했으며, 해당 사이버 범죄 그룹이 회사의 내부
스텔의 스크린샷과 소스코드를 공개한 후 이루어졌습니다.

데일리시큐 [긴급] 삼성전자 해킹한 LAPSUS$ 그룹, 오늘 LG전자 해킹 주장하며 관련 정보 공개해

[긴급] 삼성전자 해킹한 LAPSUS$ 그룹, 오늘 LG전자 해킹 주장하며 관련 정보 공개해

3월 22일 오전 10시 17분, LG전자 해킹한 계정 정보 공개...MS 정보도 공개



아주경제 | 해커 그룹 랩서스, 삼성 이어 LG도 해킹…'임직원 메일 주소' 유출

해커 그룹 랩서스, 삼성 이어 LG도 해킹…'임직원 메일 주소' 유출

김수지 기자 | 입력 2022-03-22 17:39

비디아, 삼성전자 해킹했던 '랩서스'…MS 해킹도 주장

커 그룹 랩서스(LAPSUS$)가 이번에는 LG전자를 해킹했다.

계에 따르면 랩서스는 이날 텔레그램에 'LG전자 홈페이지의 직원 및 서비스 계정 해시값'이라고 주장하는 파
다. LG전자는 정보 유출 사실을 확인하고, 보안 강화에 들어갔다.

객 정보 유출은 없었던 것으로 알려졌다. LG전자 관계자는 "임직원 이메일 주소 일부만 유출된 것으로 보인
했다.

사스는 지난 1일 미국 반도체기업 엔비디아, 삼성전자 등을 대상으로 사이버 공격을 벌여 해킹했다고 주장한
실제 랩서스는 엔비디아의 서버에서 그래픽처리장치(GPU) 회로도 등을 빼냈다.

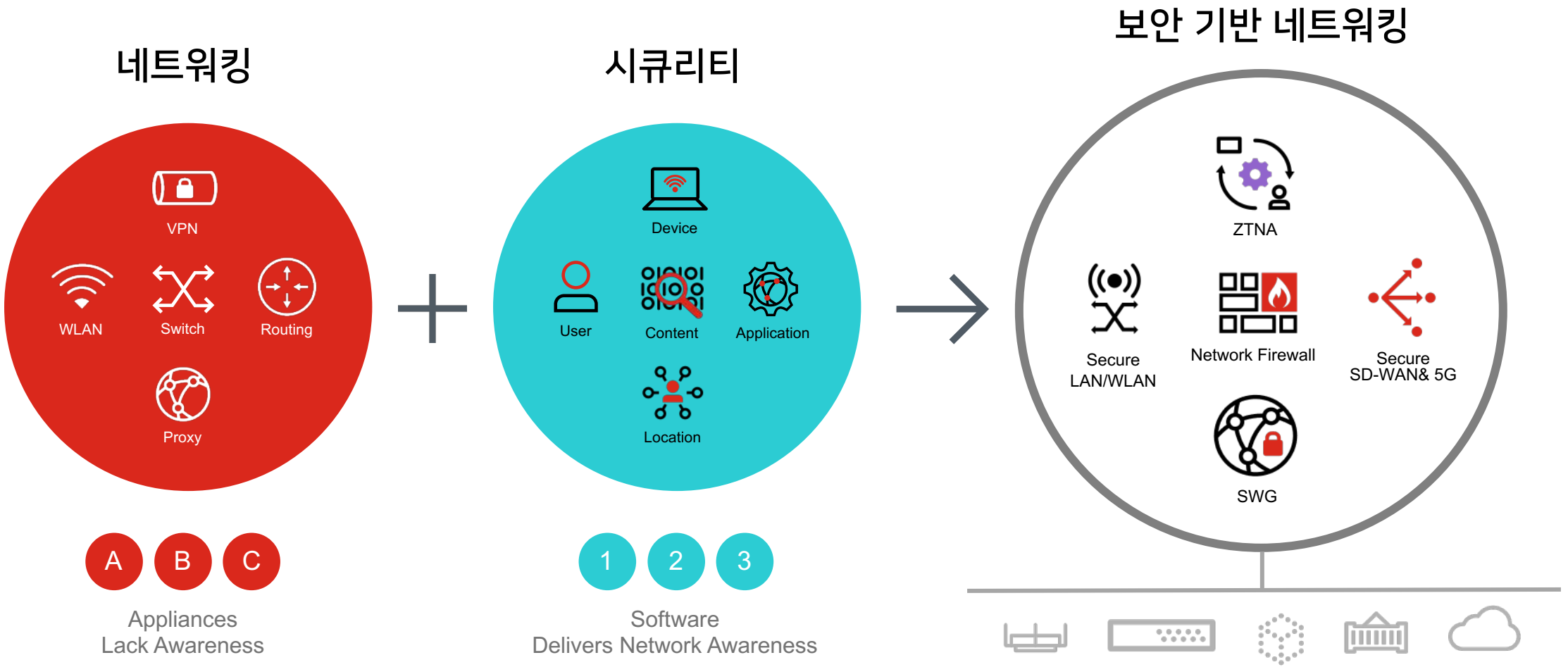
실시간 인기

종합 | 경제 | 정치 | 사회 | 모바일

1 文 46.7%-尹 46.0%...尹 측 "낮은 자세로...
2 쌍용차, 에디슨모터스 계약 해지 등...
3 현대차, '보이콧'부터 '국유화'까지 사면초...
4 尹당선인, 취임 전 '양대 노총' 안 만난다…'...
5 임원 4명 중 1명이 女... '유리천장' 깬 LG제...
6 "죽쒀 곧 품린다"…서울 아파트 매매 '지지...
7 "배민1 배달 안 받아요"… 뿔난 자영업자들...

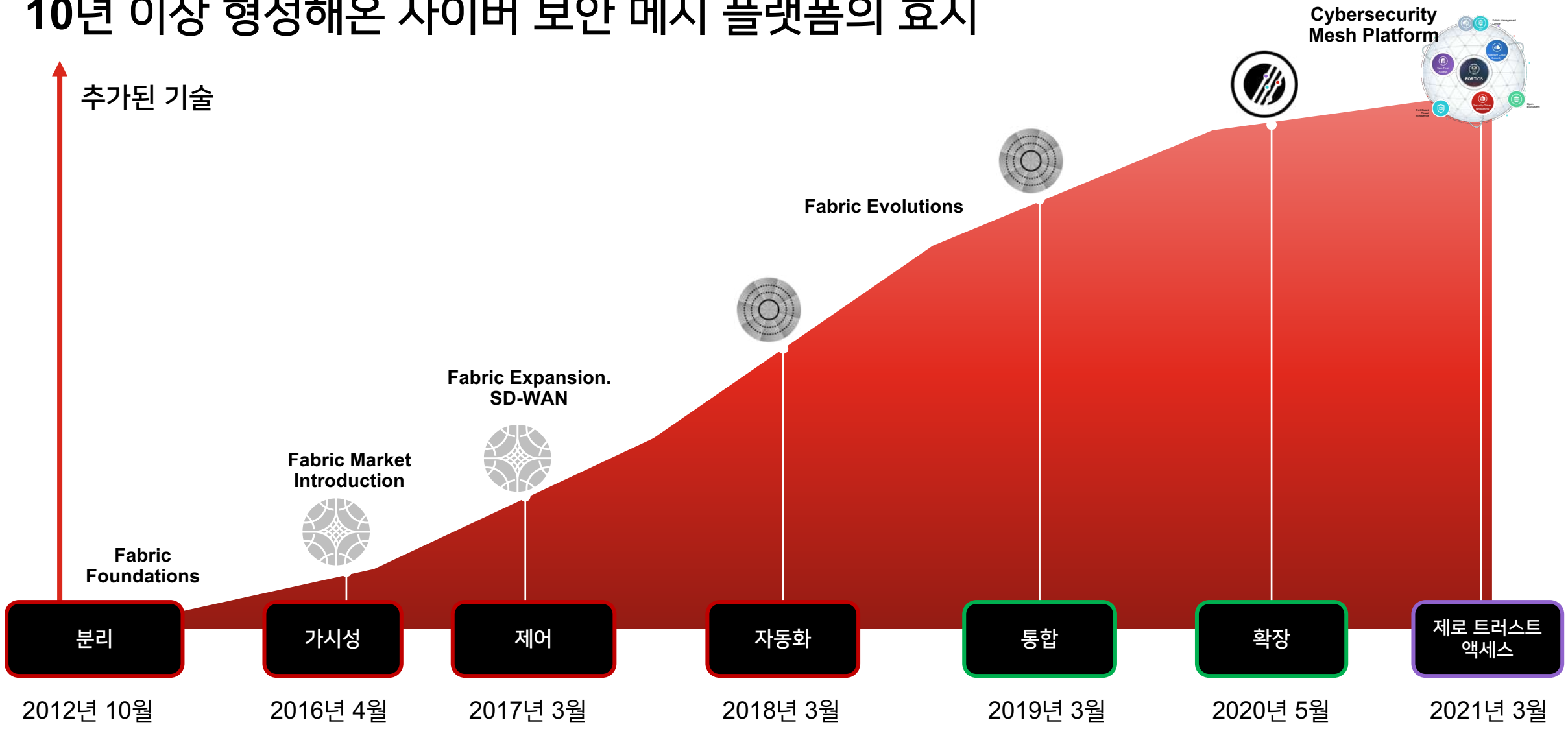
포티넷의 컨버전스 접근방식

보안 기반 네트워킹으로 일관된 컨버전스 가능



포티넷 시큐리티 패브릭

10년 이상 형성해온 사이버 보안 메시 플랫폼의 효시



글로벌 고객사들의 트렌드

Top Strategic Technology Trends for 2022: Cybersecurity Mesh

Accelerating Growth	Sculpting Change	Engineering Trust
• Generative AI	• AI Engineering	• Cloud-Native Platforms
• Autonomic Systems	• Hyperautomation	• Privacy-Enhancing Computation
• Total Experience	• Decision Intelligence	• **Cybersecurity Mesh**
• Distributed Enterprise	• Composable Applications	• Data Fabric

Source: Gartner

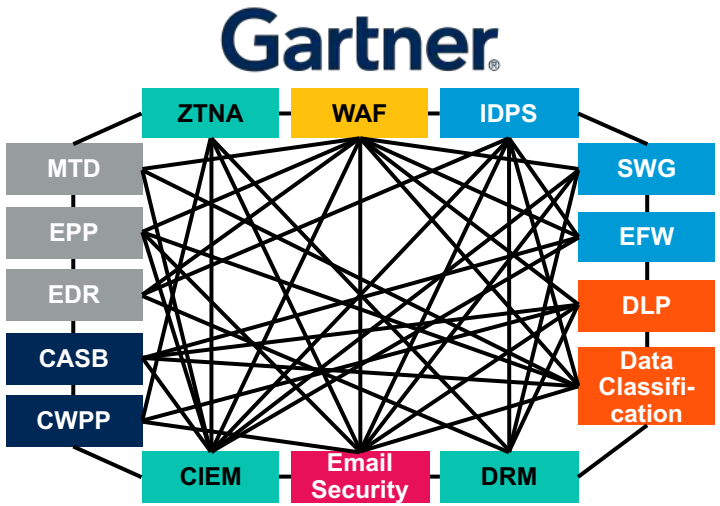
매년 IT 동향에 대한 연례 보고서를 발표하는 **가트너**는 **2022년**의 **[전략 기술 트렌드 Top 12]**를 소개 했습니다.

가트너는 전략적 IT 동향에 대한 연례 보고서를 통해 **AI와 클라우드, 보안** 또는 **엔지니어링에 대한 디지털 투자** 등 12개의 사항이 오는 **2022년 최고의 기술 추진 요인**이 될 것으로 전망했습니다.

그 중에서 **사이버 보안 메쉬**에 대해 언급하며 이는 새로운 트랜드이며, 2022년 및 가까운 미래에 대한 가트너의 **최고 전략 기술 동향**이 될 것으로 이야기했습니다. **사이버 보안 메쉬**는 기업이 분산된, 가장 필요한 인프라 등에 보안을 배포 및 확장할 수 있도록 하는 보안 아키텍처에 대한 **현대적인 접근 방식**으로, 더 큰 확장성, 유연성 및 안정적인 사이버 보안 제어를 가능하게 합니다.

가트너는 증가하는 사이버 보안 위협은 보안 기술의 혁신을 불러일으키고 있으며 **2024년까지 CSMA를 채택하는 조직이 개별 보안 침해 사고로 인한 발생할 수 있는 재정적 피해를 평균 90% 감소시킬 수 있다고 이야기 하였습니다.**

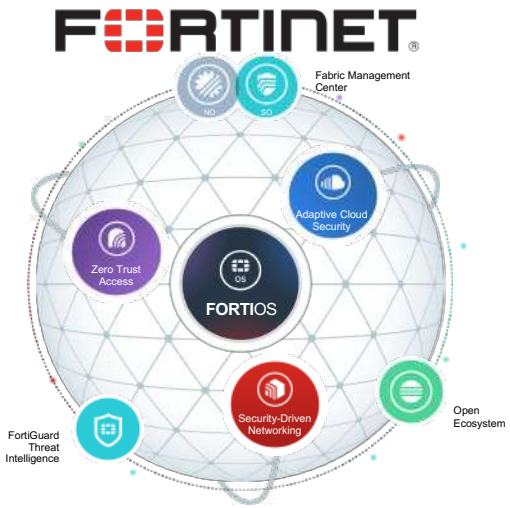
가트너가 말하는 아키텍처에 부합하는 포티넷 시큐리티 패브릭



Gartner는 "2024년까지, 사이버 보안 메시 아키텍처를 채택하여 여러 보안 도구를 통합해 협업 에코시스템 형태로 운영하는 기업은 개별적인 보안 침해사고가 미치는 경제적 손실을 평균 90%까지 줄일 수 있을 것"이라고 전망합니다.

"Top Strategic Technology Trends for 2022: Cybersecurity Mesh, Felix Gaehtgens, James Hoover, Henrique Teixeira, Claudio Neiva, Michael Kelley, Mary Ruddy, Patrick Hevesi, 18 October 2021"

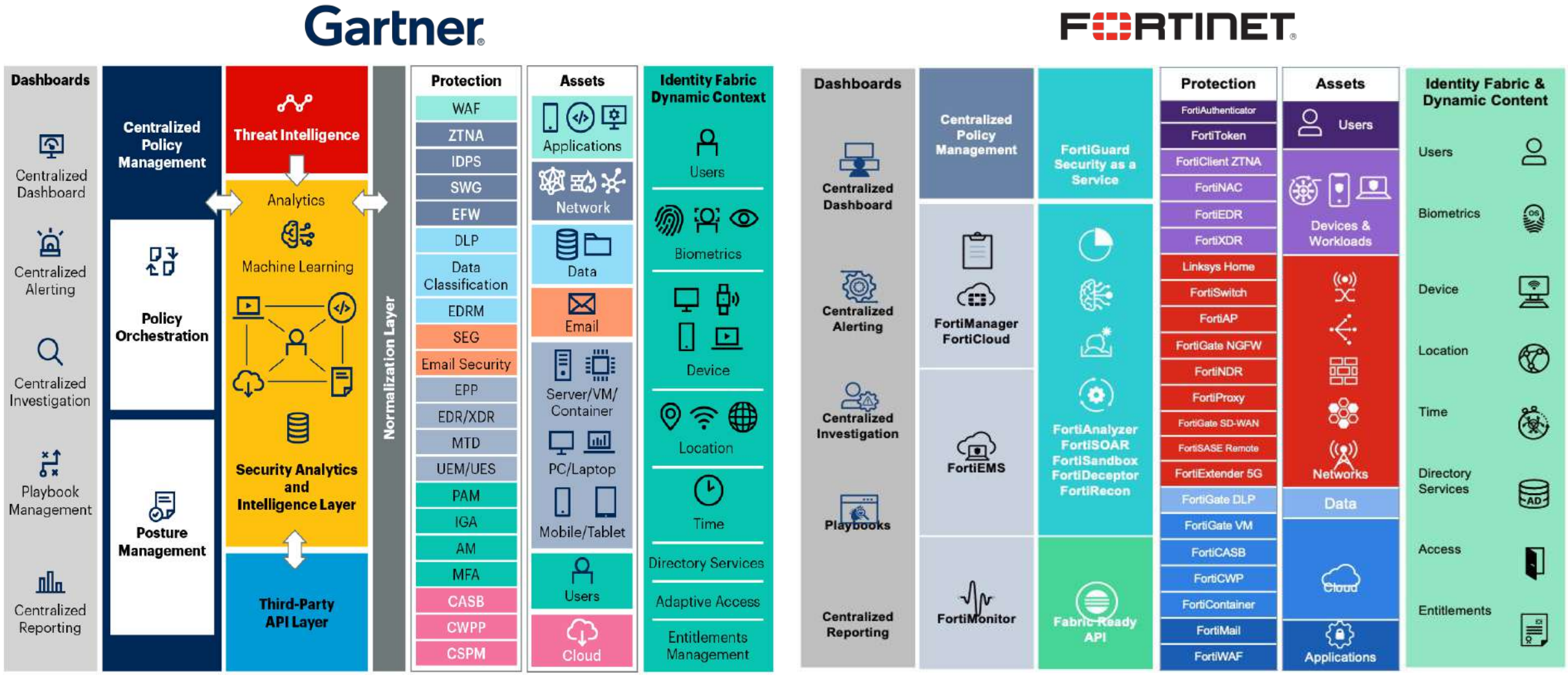
Felix Gaehtgens, James Hoover, Henrique Teixeira, Claudio Neiva, Michael Kelley, Mary Ruddy, Patrick Hevesi. As of October 2021



사이버 시큐리티 메쉬 아키텍처 (CSMA) 구축 목표에 부합하는 포티넷 시큐리티 패브릭 기술

- 모든 엣지를 커버하는 높은 **가시성** 제공
- 분산된 보안 솔루션을 **중앙 원격 관리** 지원
- 하이브리드 환경에서 **일관된 보안 정책 적용** 지원
- 포티넷 시큐리티 패브릭 솔루션의 실시간 글로벌 **위협 인텔리전스** 정보 연동 지원
- 보안 조치 대응 **자동화** 툴 & **API** 지원
- 광범위한 대상 장비 지원, 최적화된 연동 기능 지원하는 **오픈 에코 파트너** 환경 지원

가트너 아키텍처에 부합하는 포티넷 시큐리티 패브릭

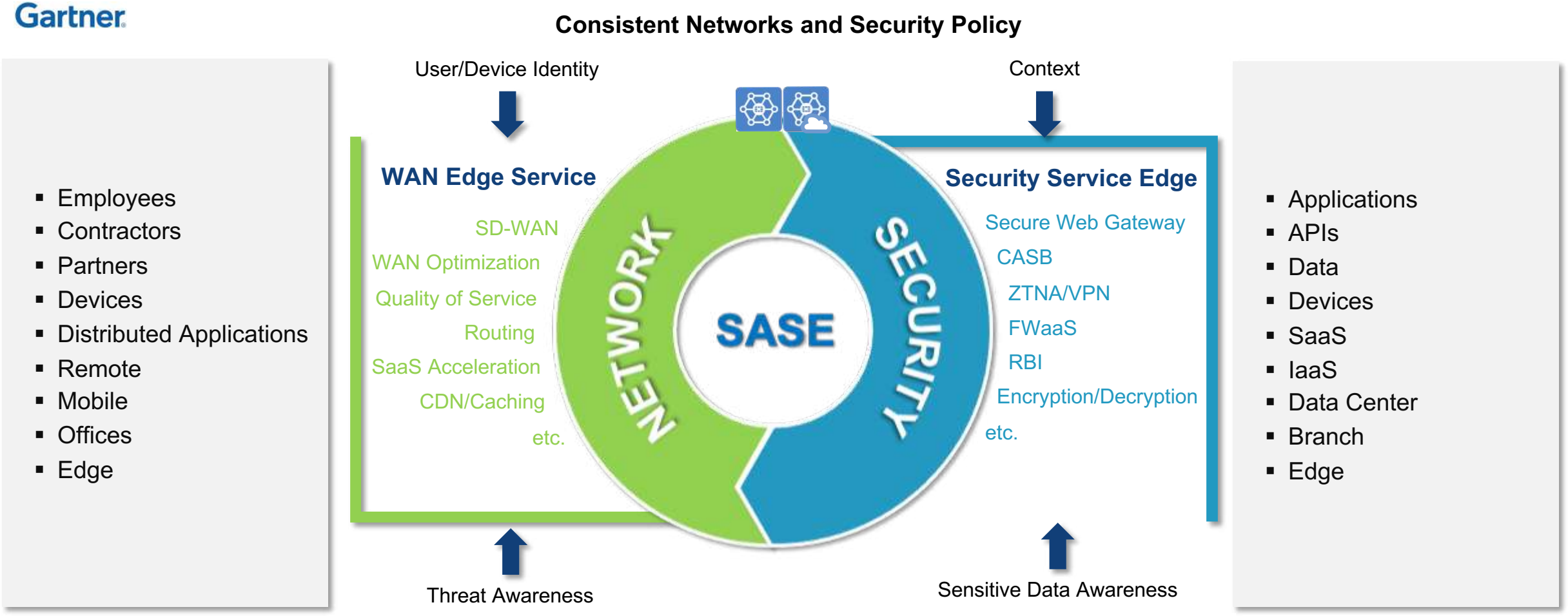


Source: Gartner

Source: *Gartner "Guide to Cloud Security Concepts"*, Patrick Hevesi, Richard Bartley, Dennis Xu. 21 September, 2021

SASE 자세히 보기 : SaaS 구독형 서비스와 자가 구축형 서비스

Gartner

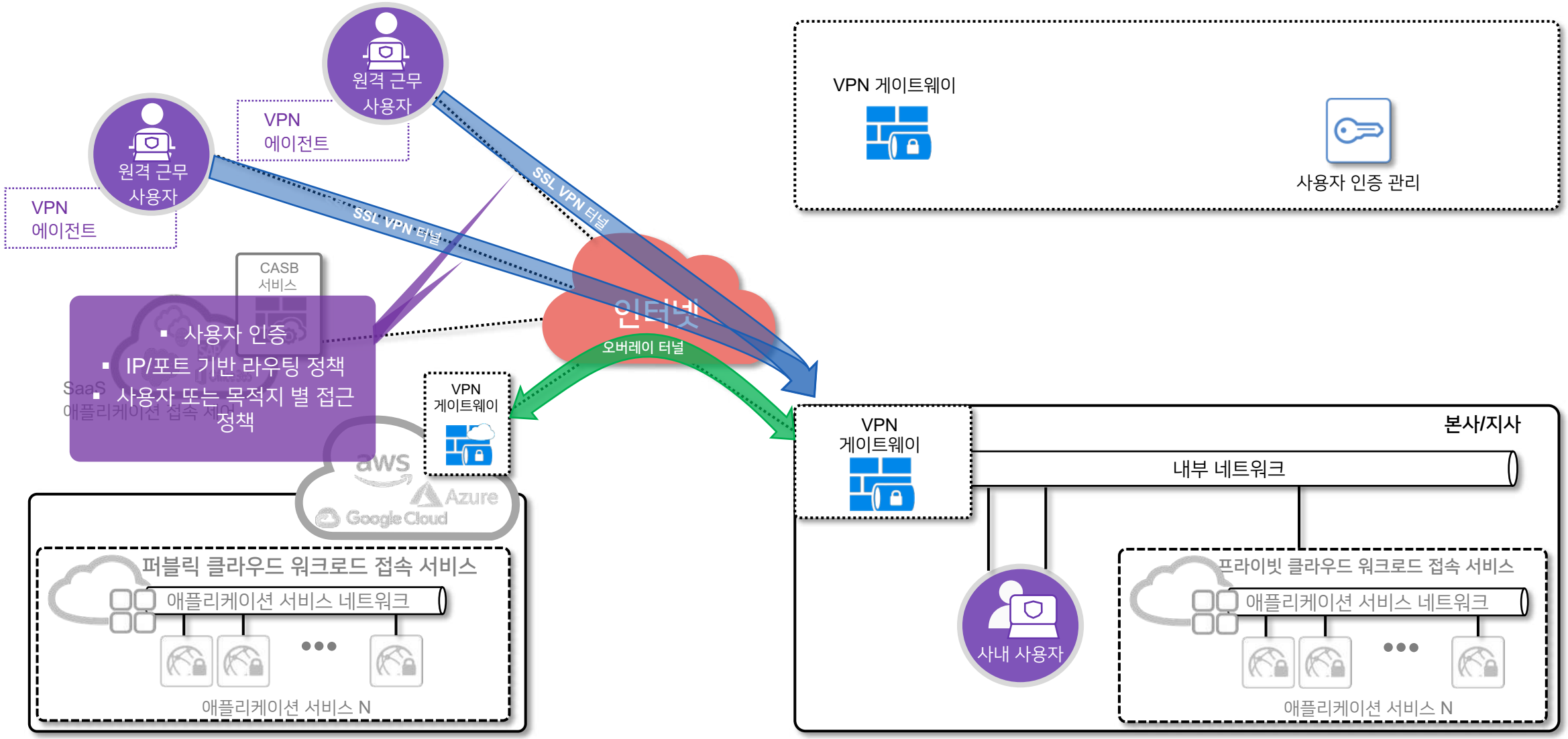


Source : Gartner

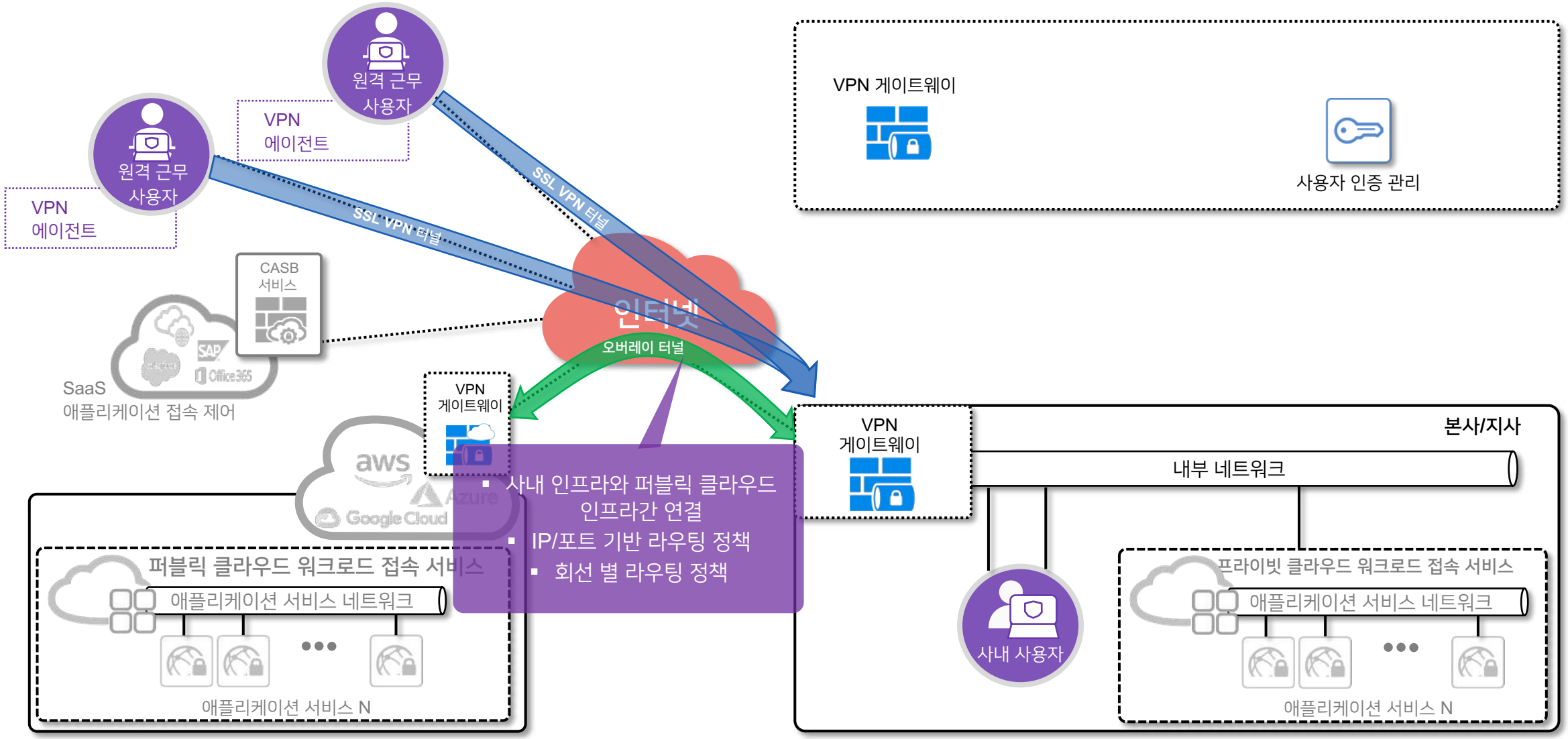
유즈케이스

:온프레미스

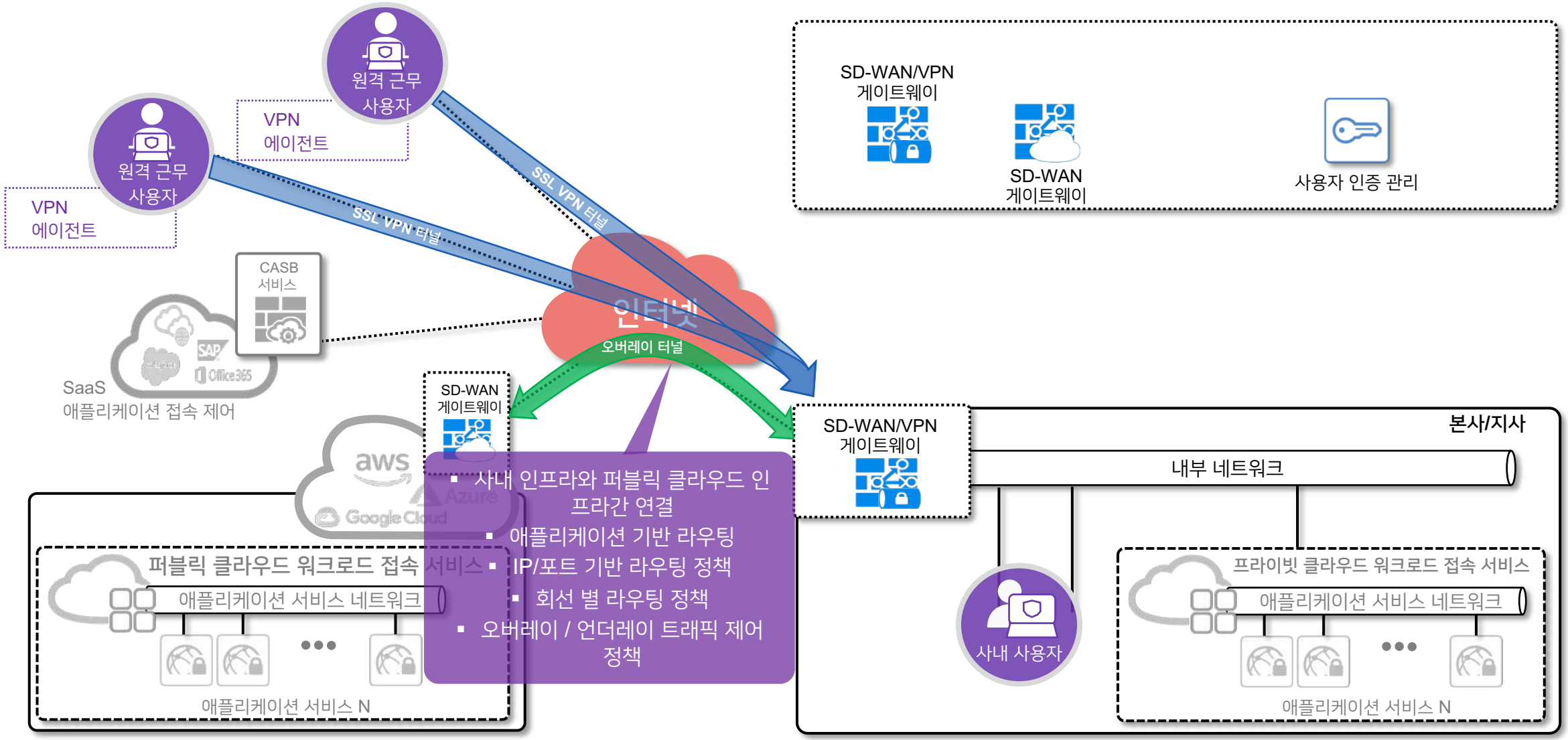
일반 VPN 서비스의 제한 (1)



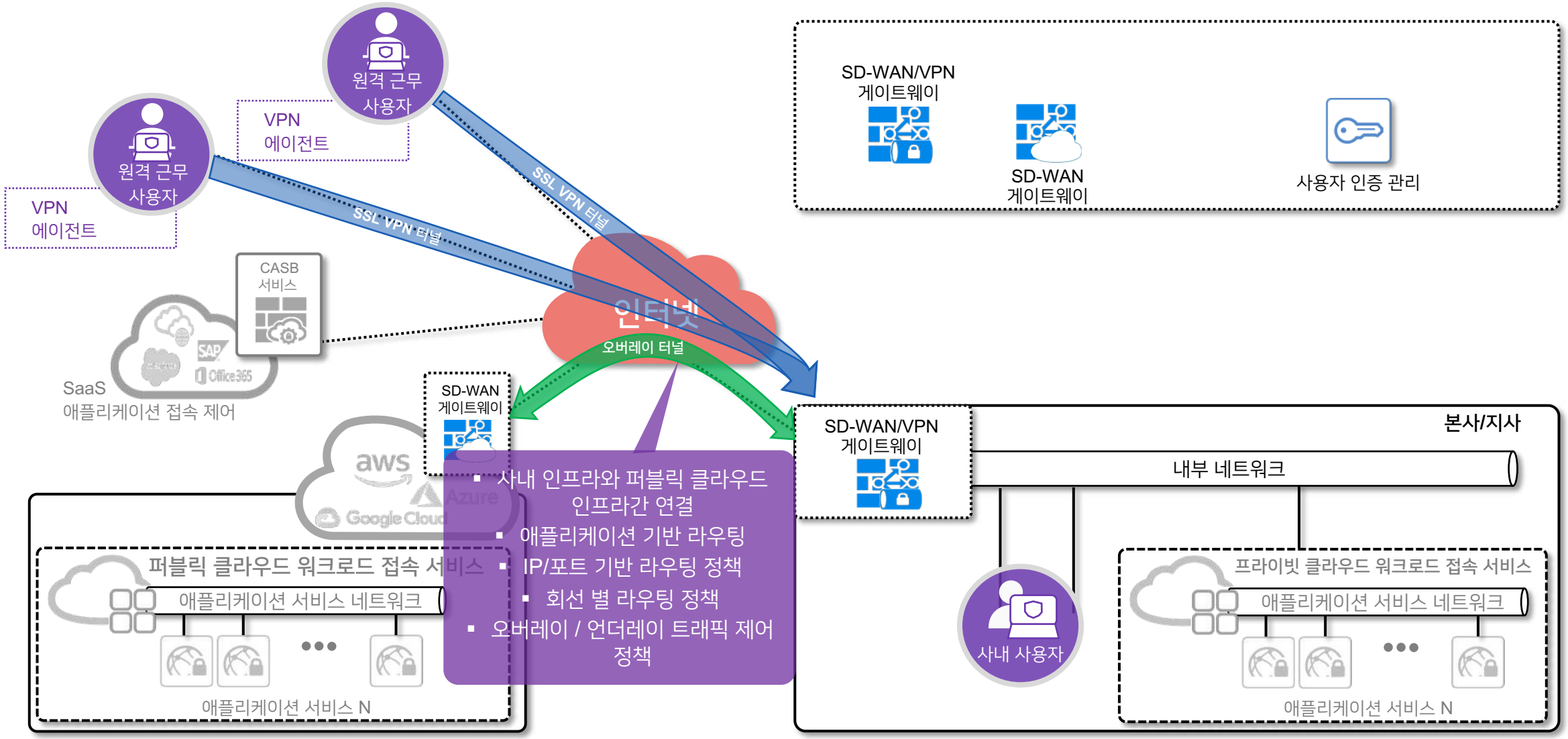
일반 VPN 서비스의 제한 (2)



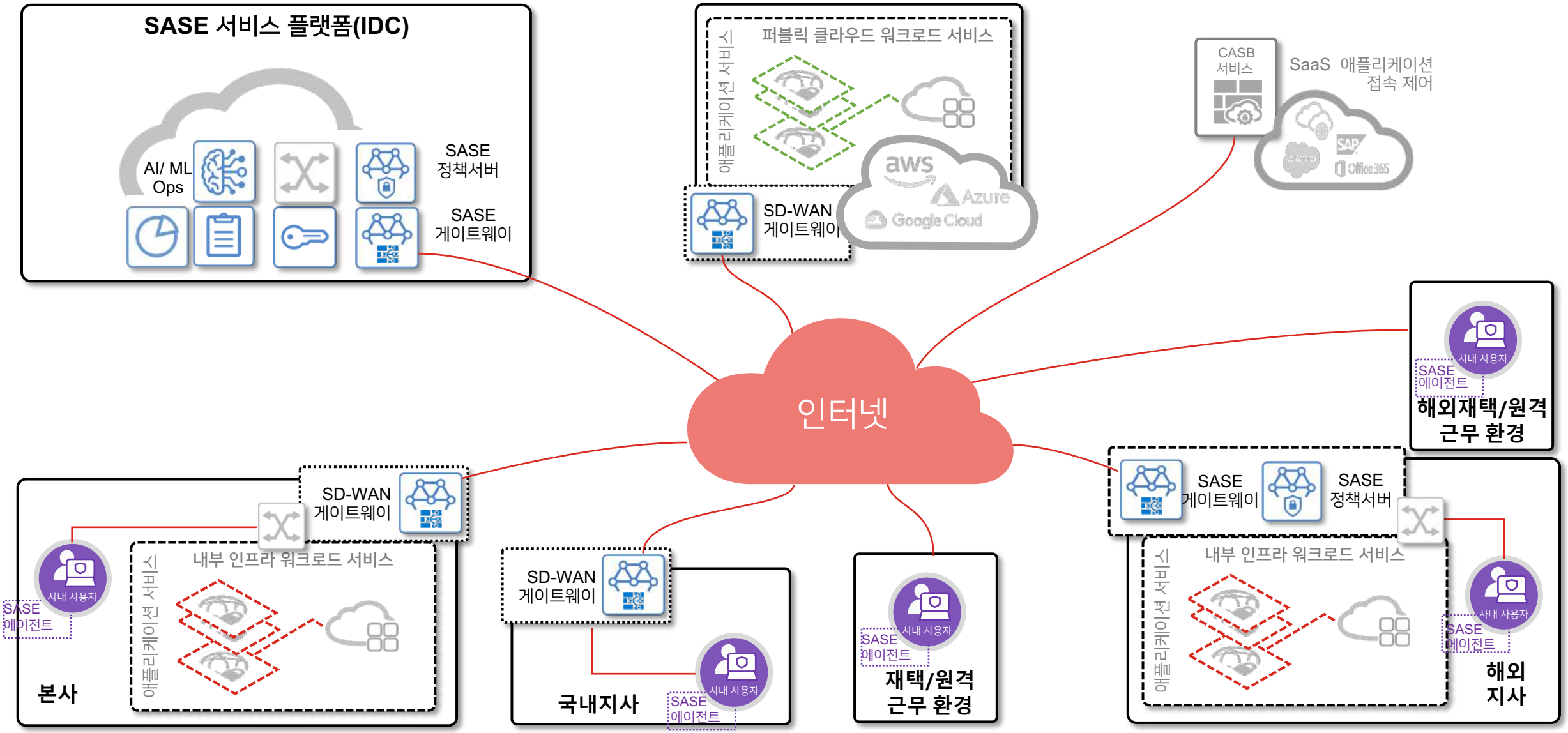
일반 SD-WAN 서비스의 제한 (1)



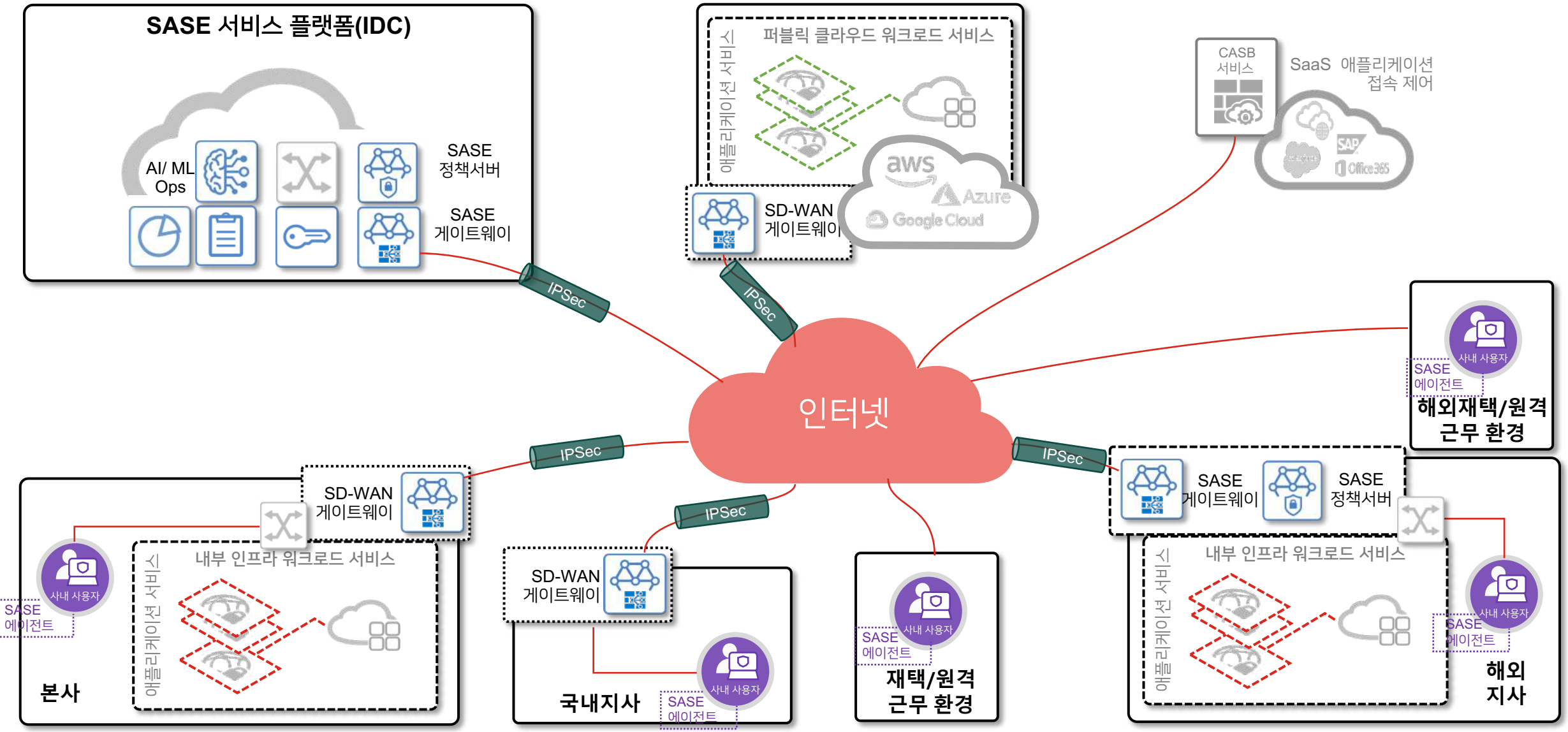
일반 SD-WAN 서비스의 제한 (2)



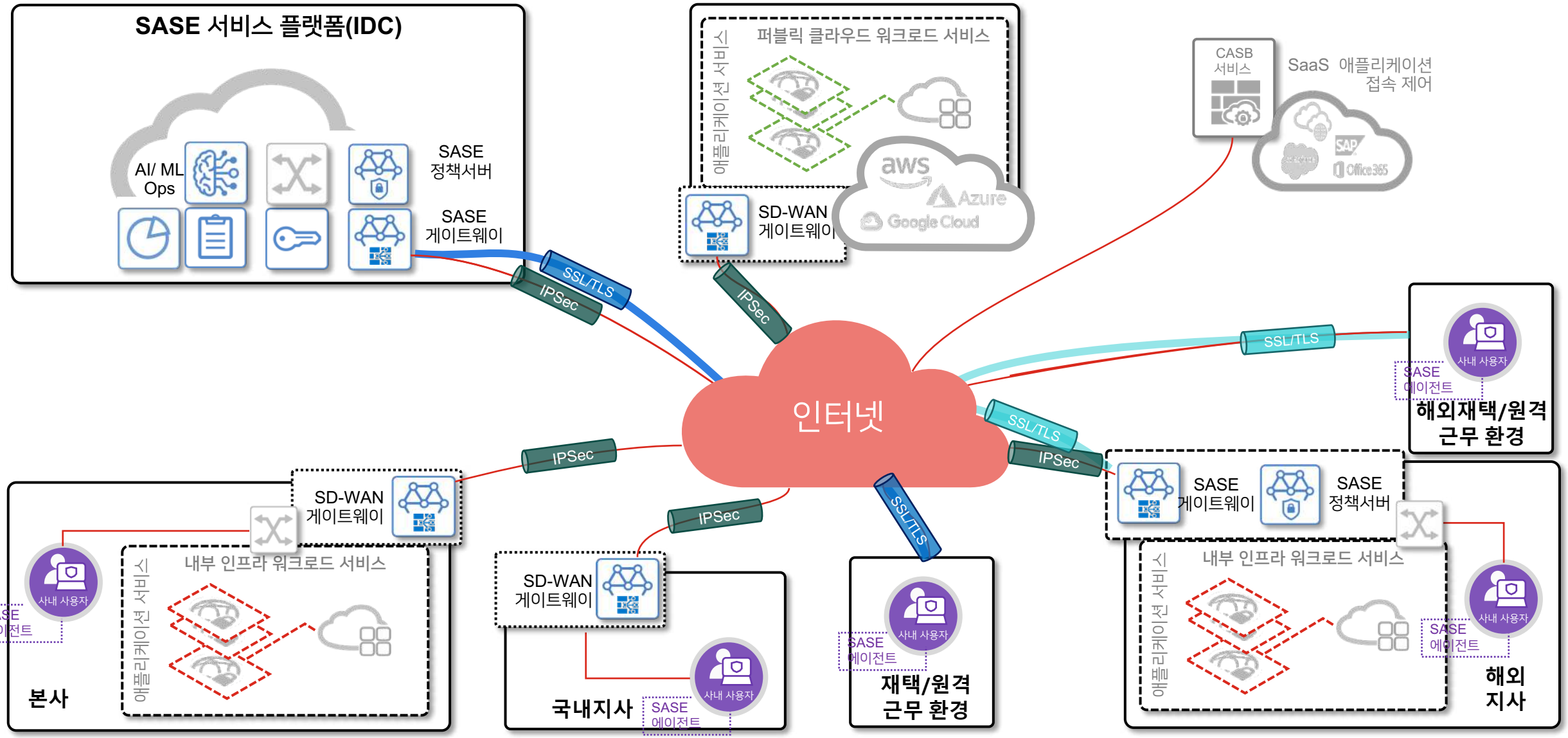
유즈케이스 : 온프레미스



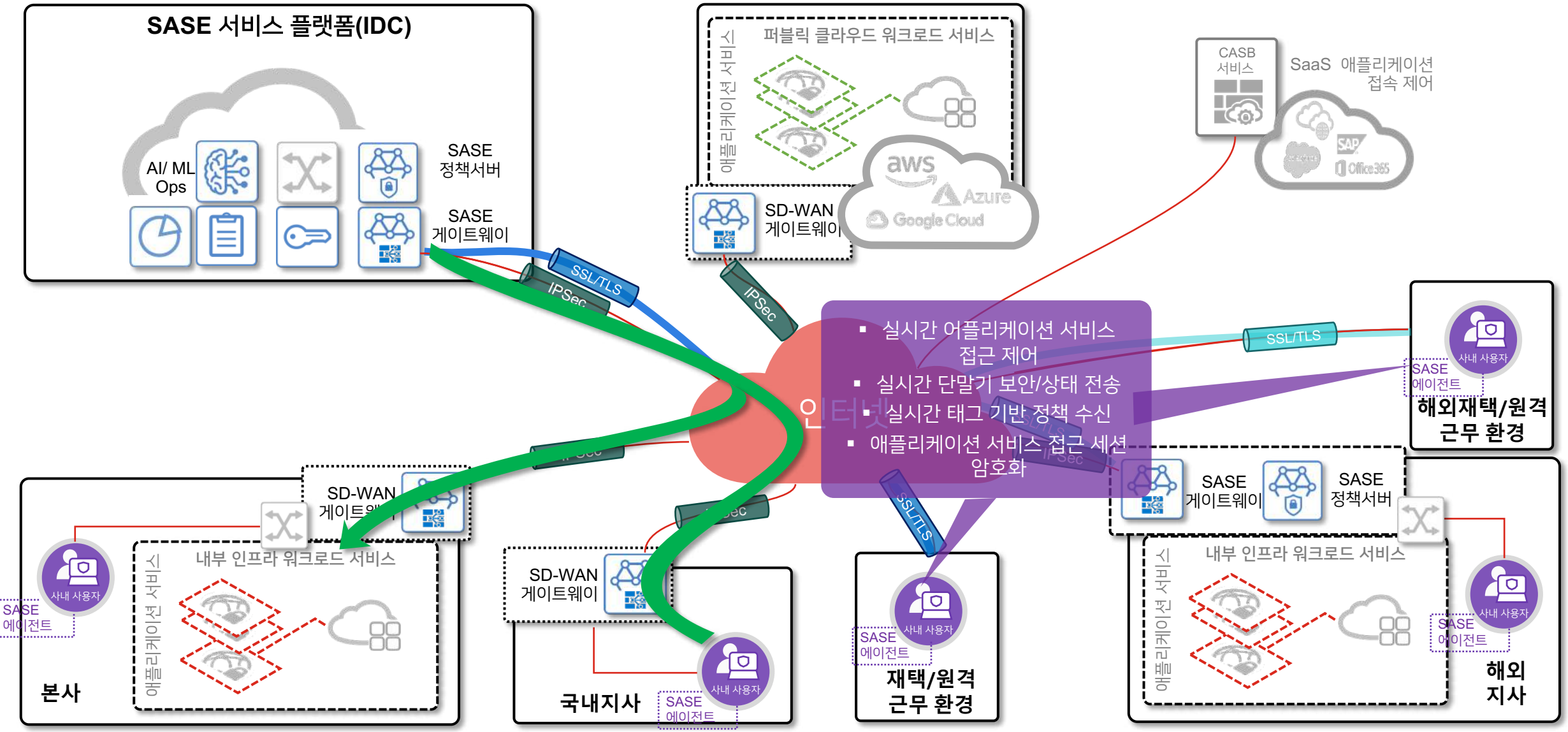
유즈케이스 : 온프레미스



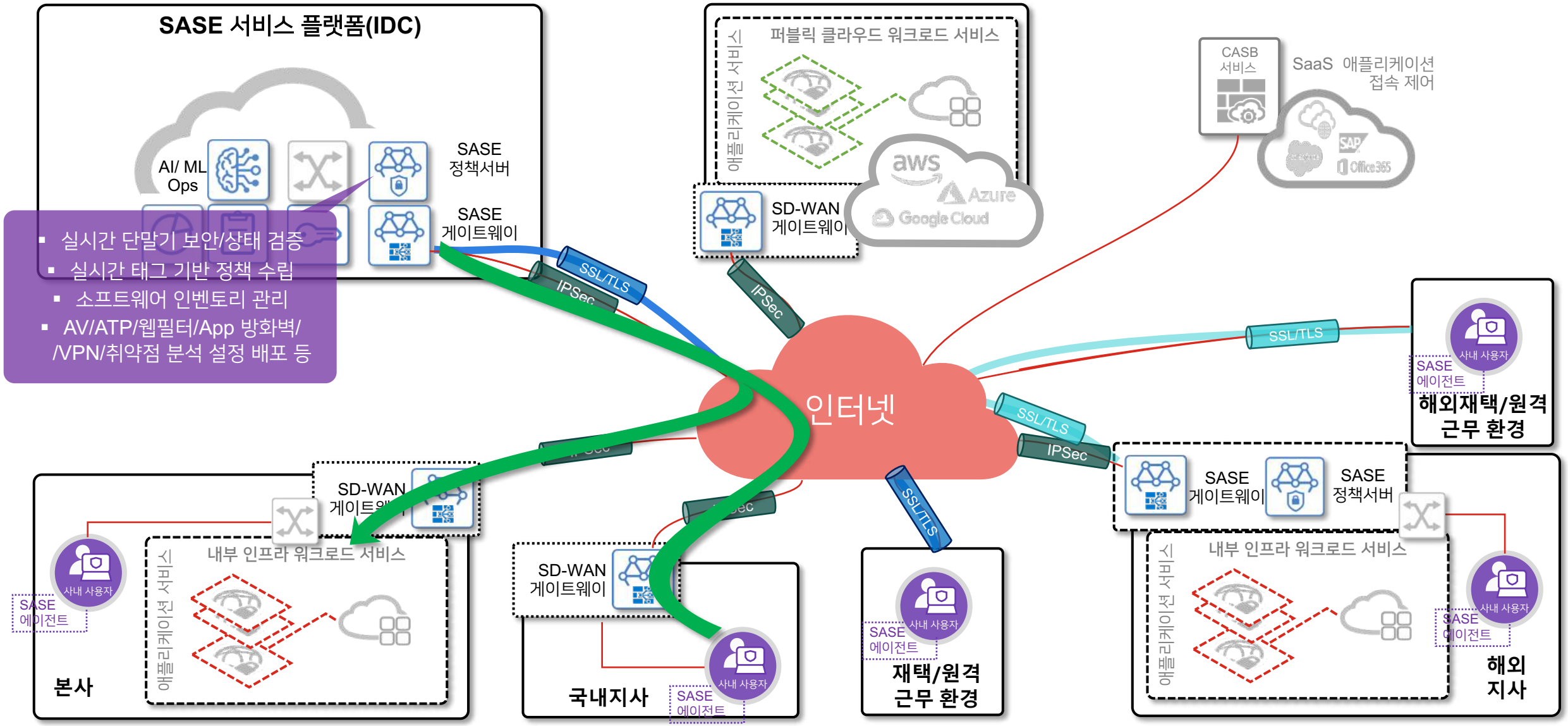
유즈케이스 : 온프레미스



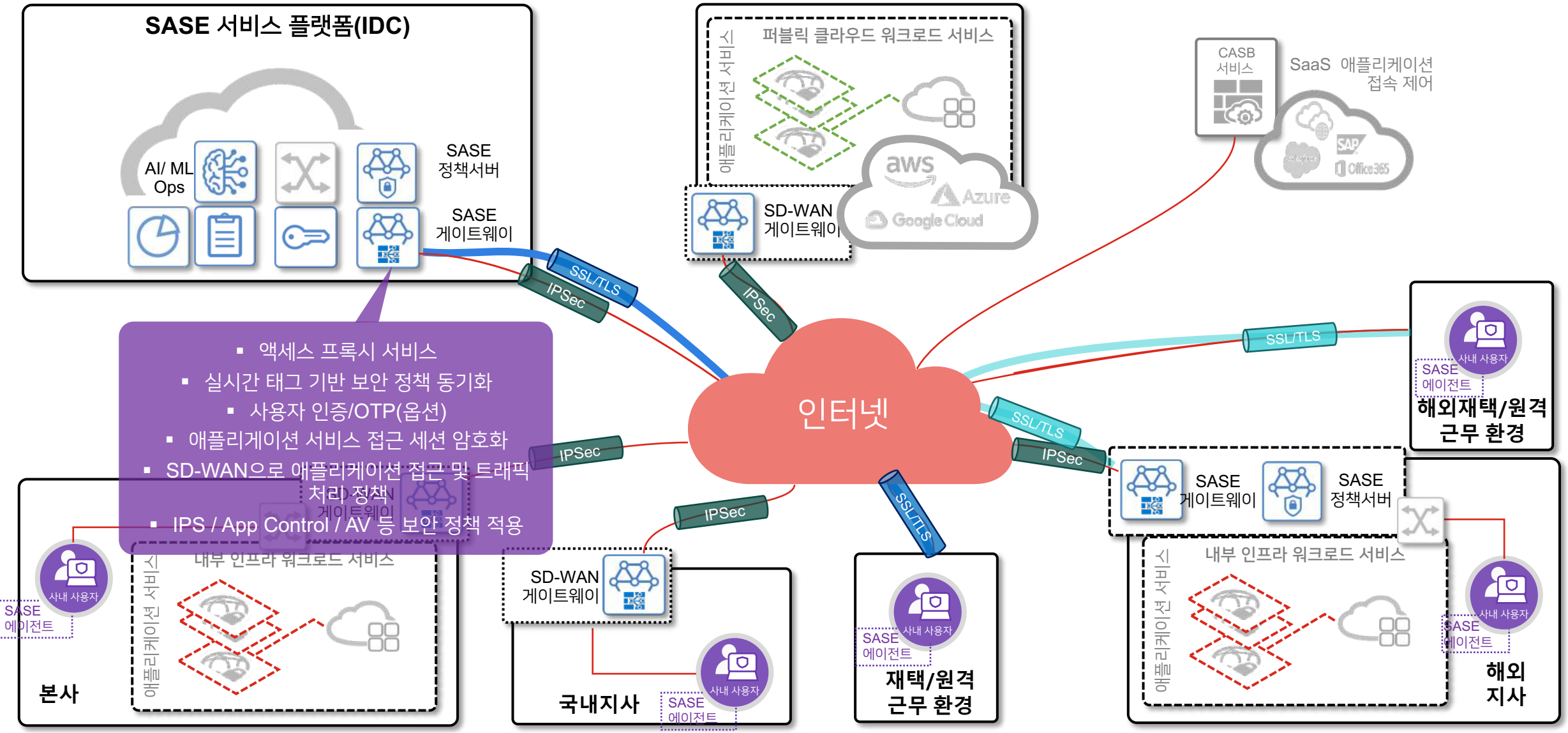
유즈케이스 : 온프레미스



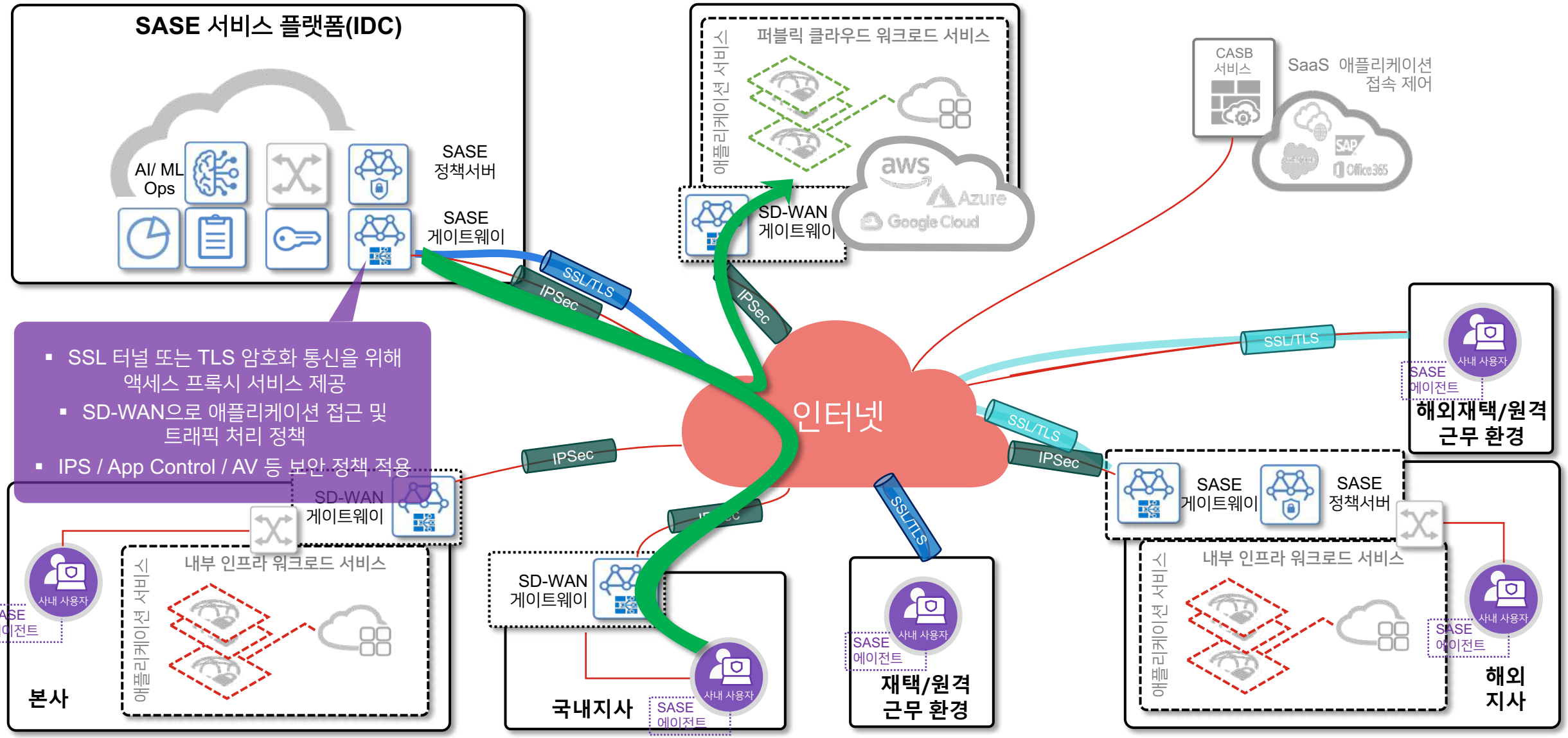
유즈케이스 : 온프레미스



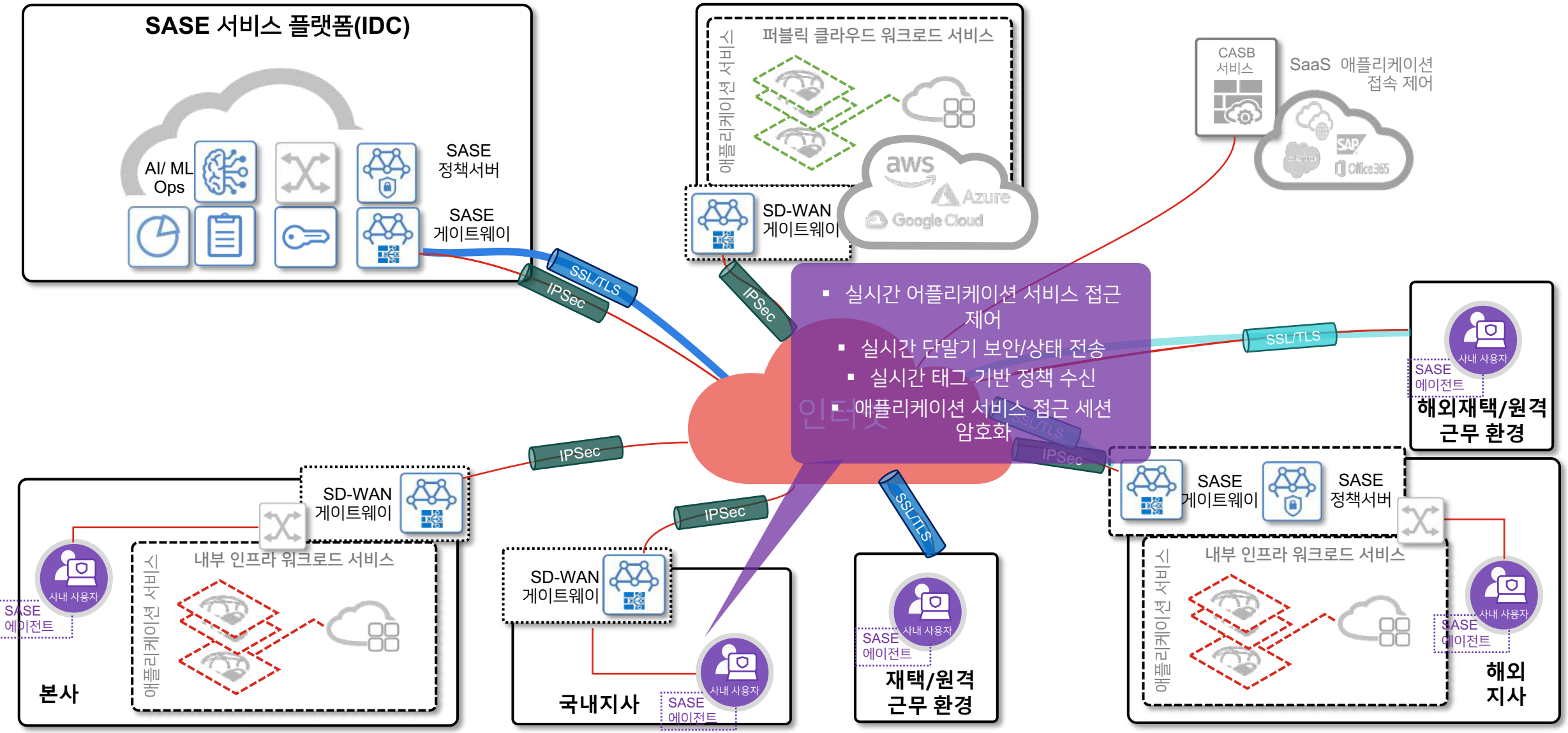
유즈케이스 : 온프레미스



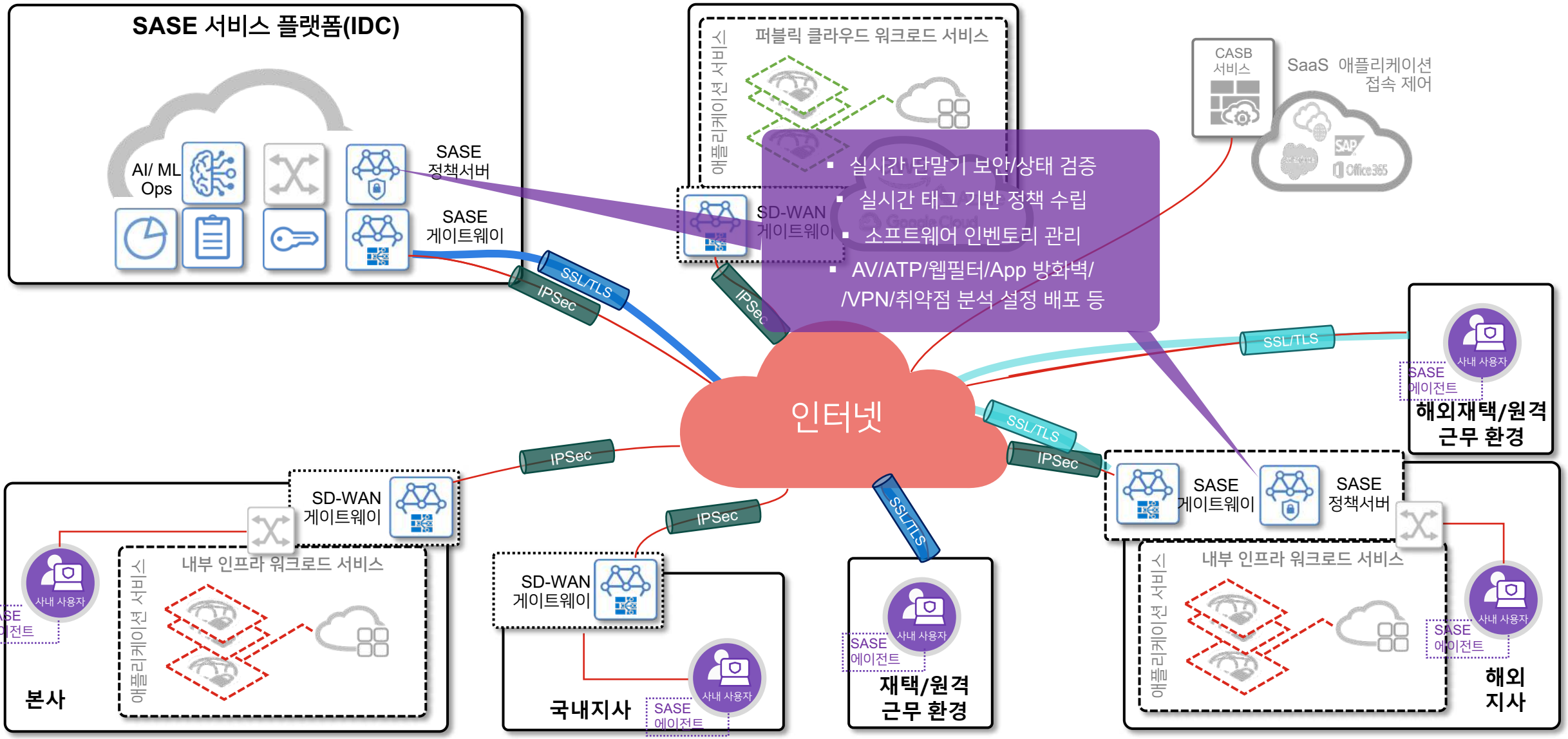
유즈케이스 : 온프레미스



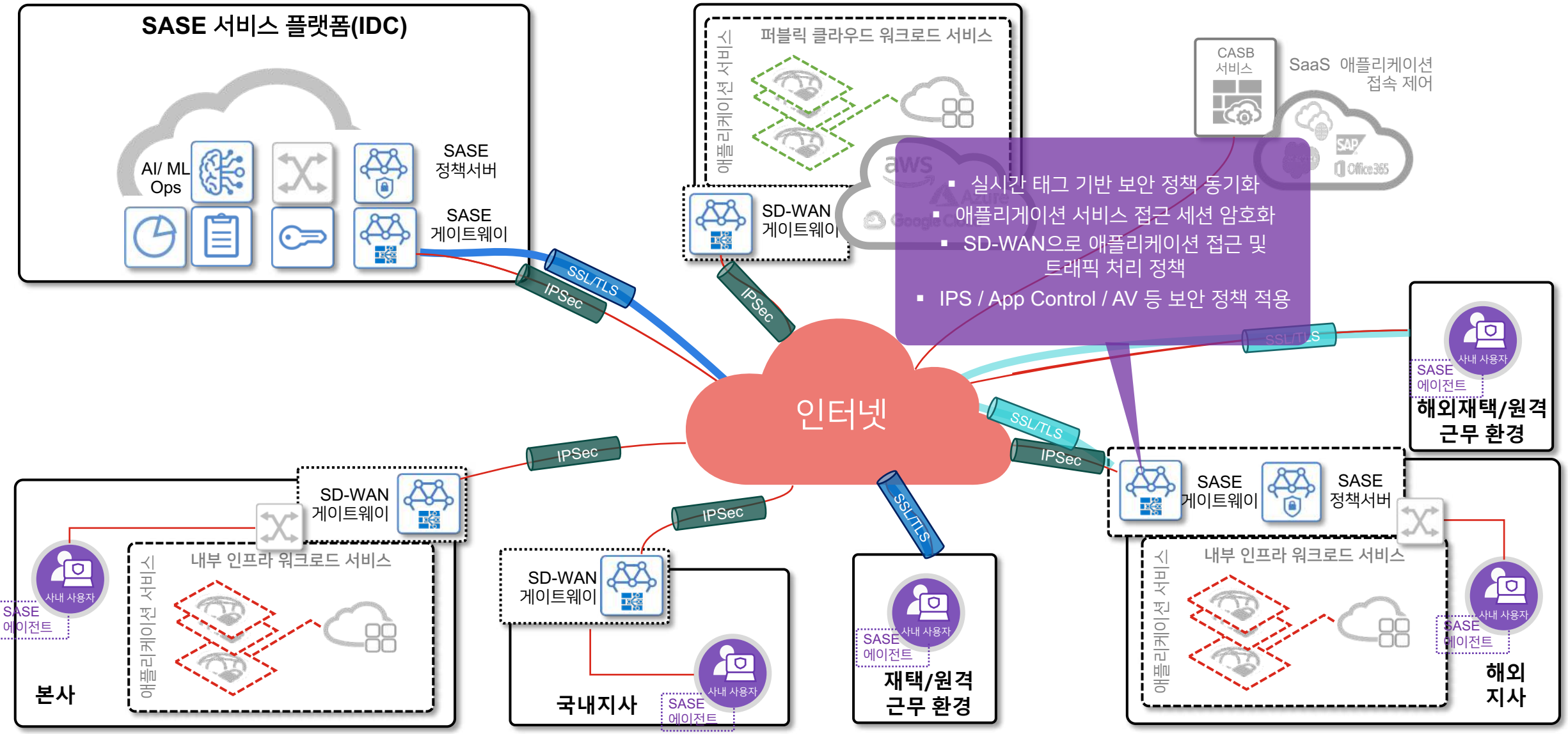
유즈케이스 : 온프레미스



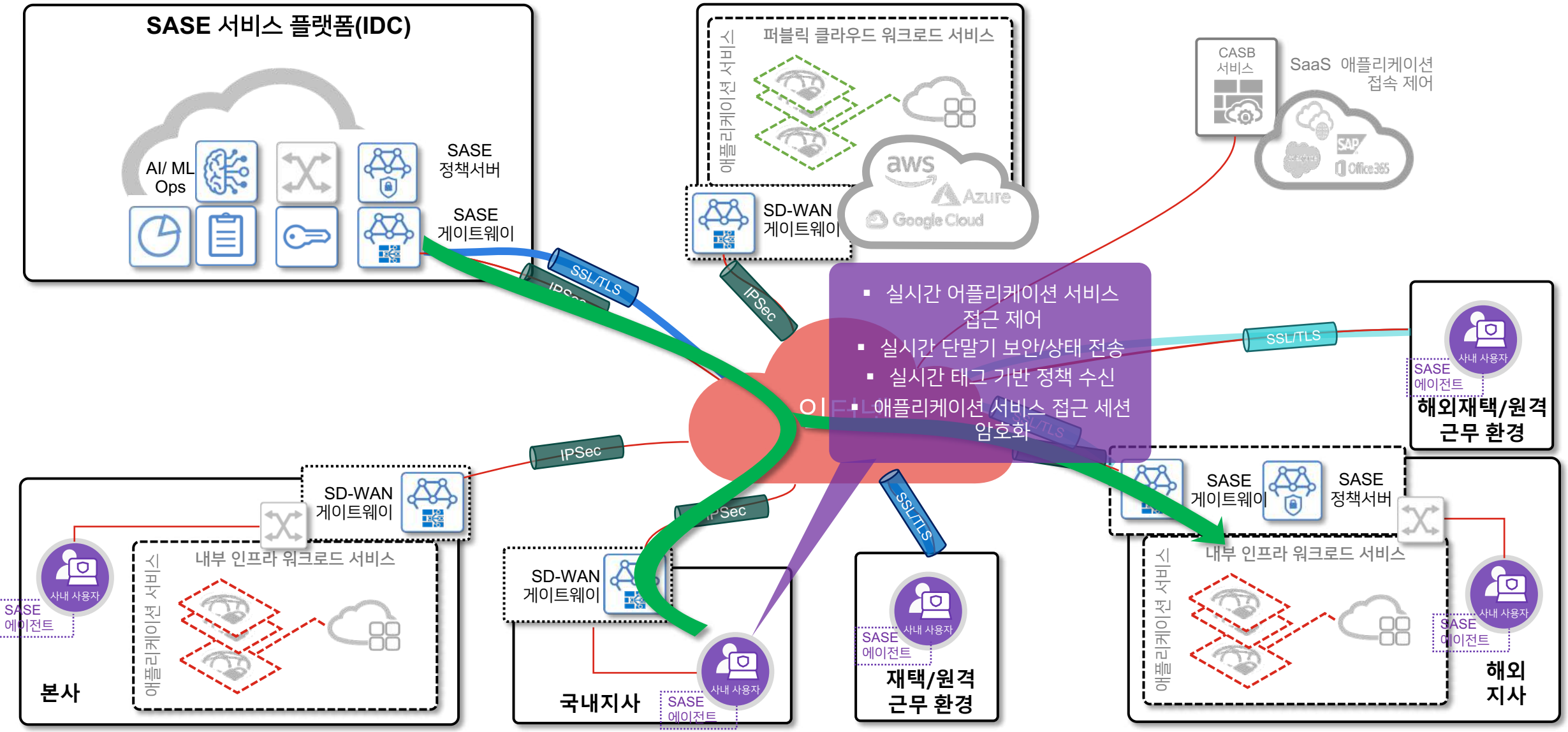
유즈케이스 : 온프레미스



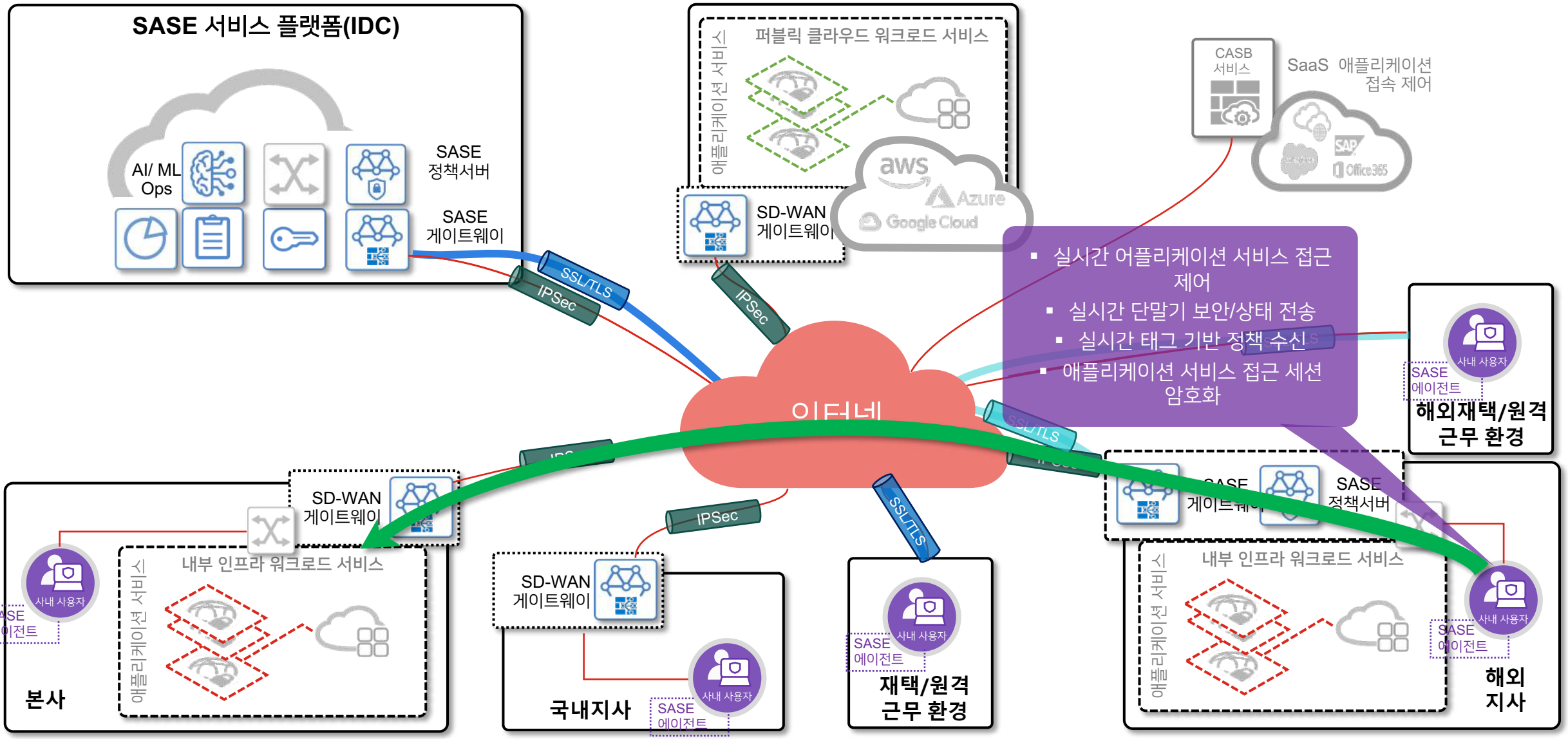
유즈케이스 : 온프레미스



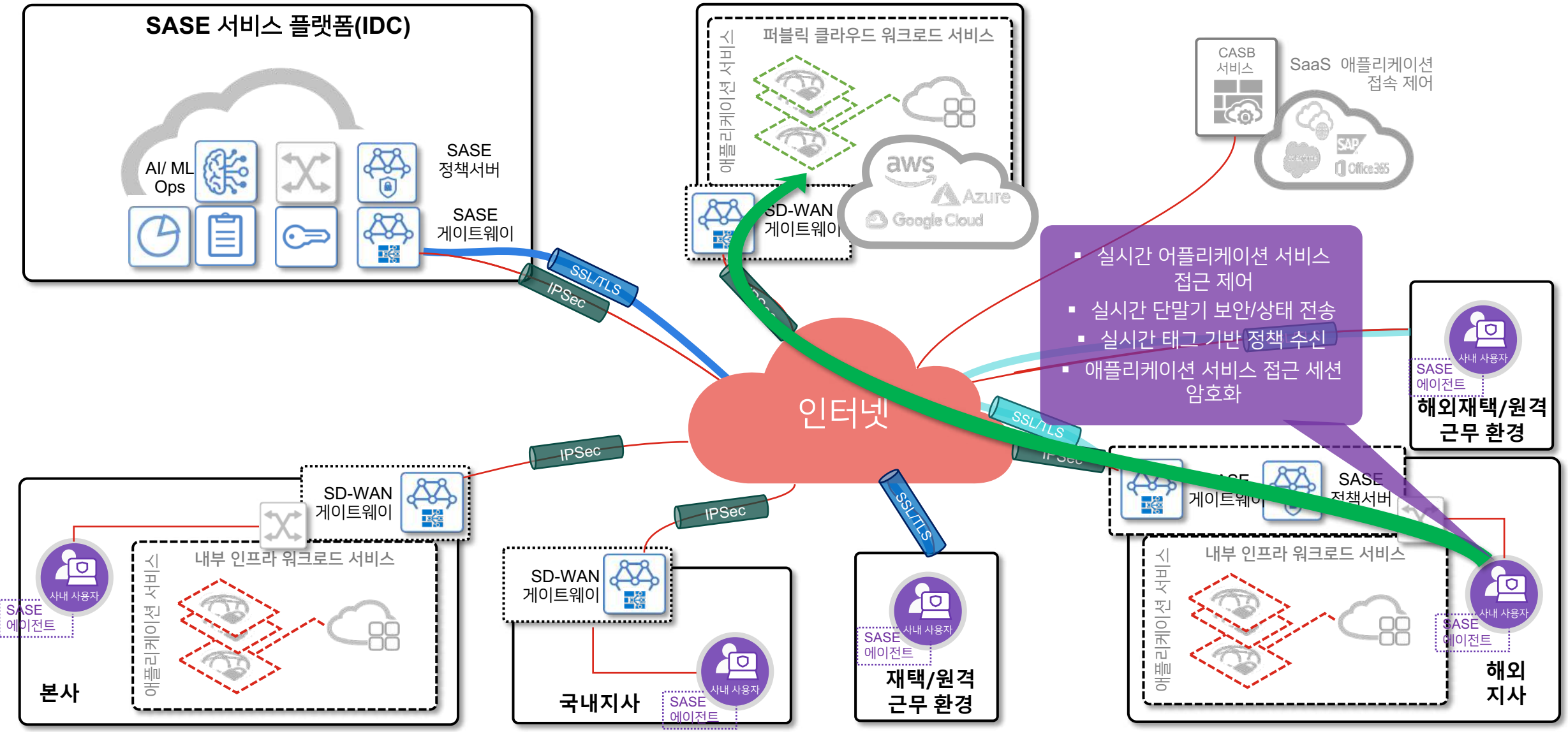
유즈케이스 : 온프레미스



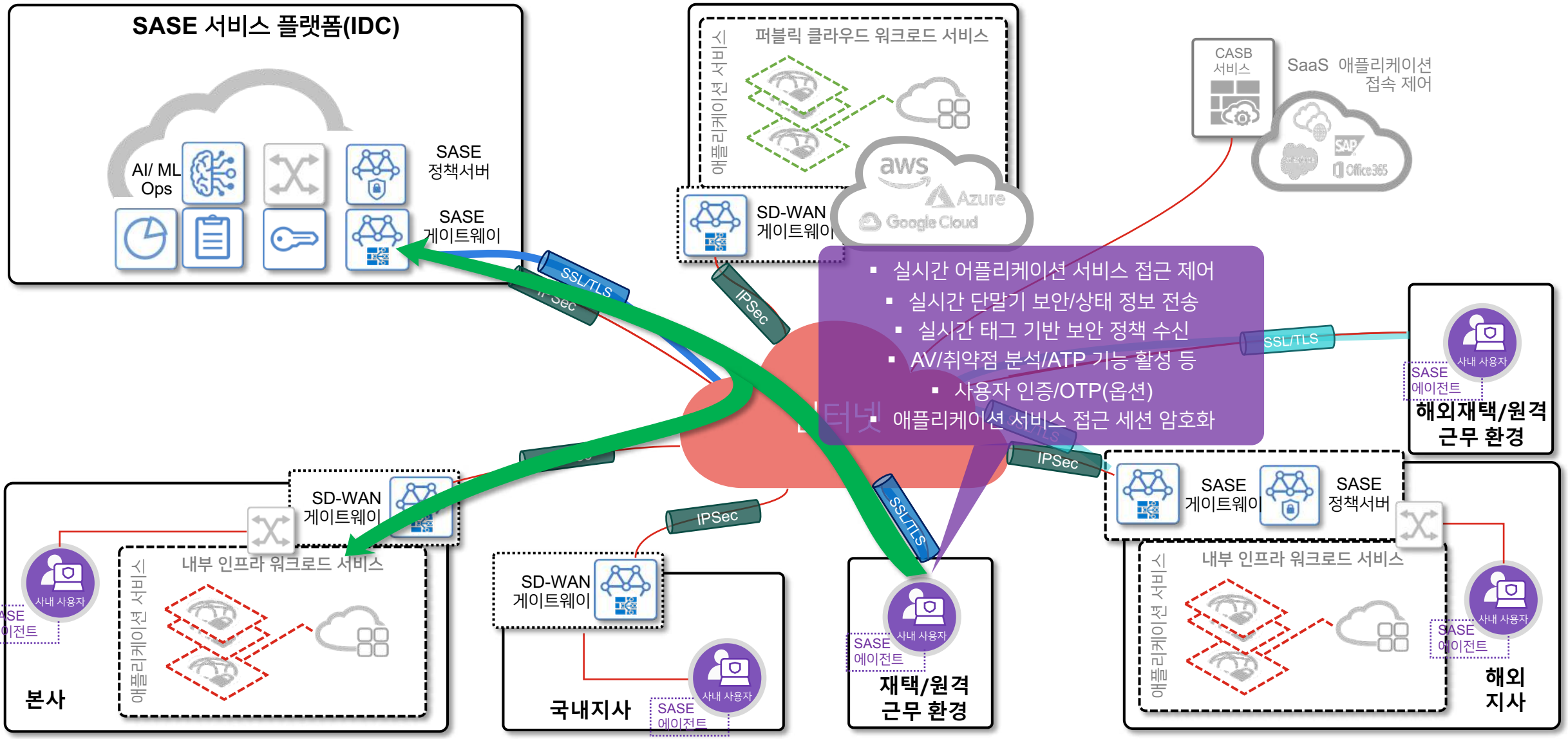
유즈케이스 : 온프레미스



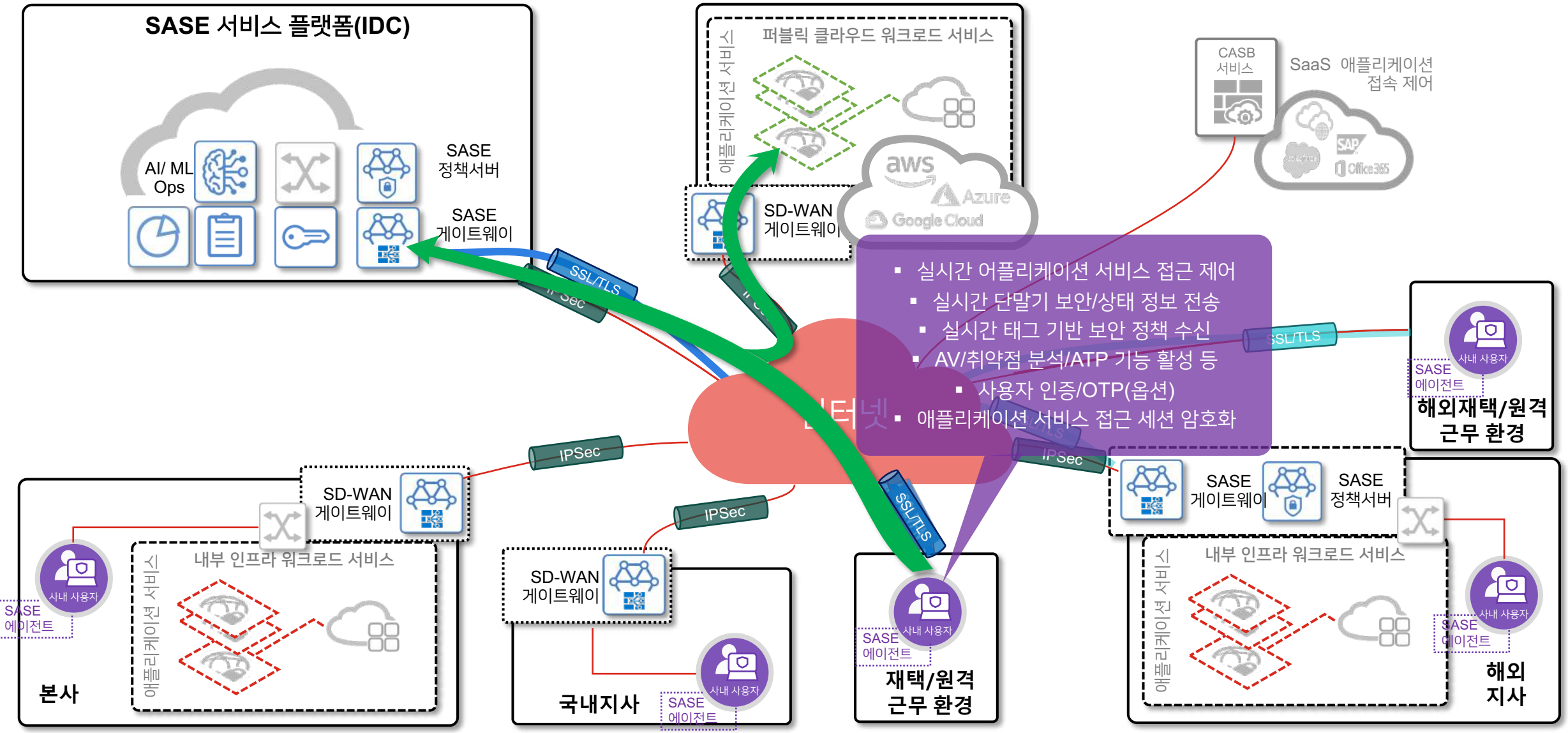
유즈케이스 : 온프레미스



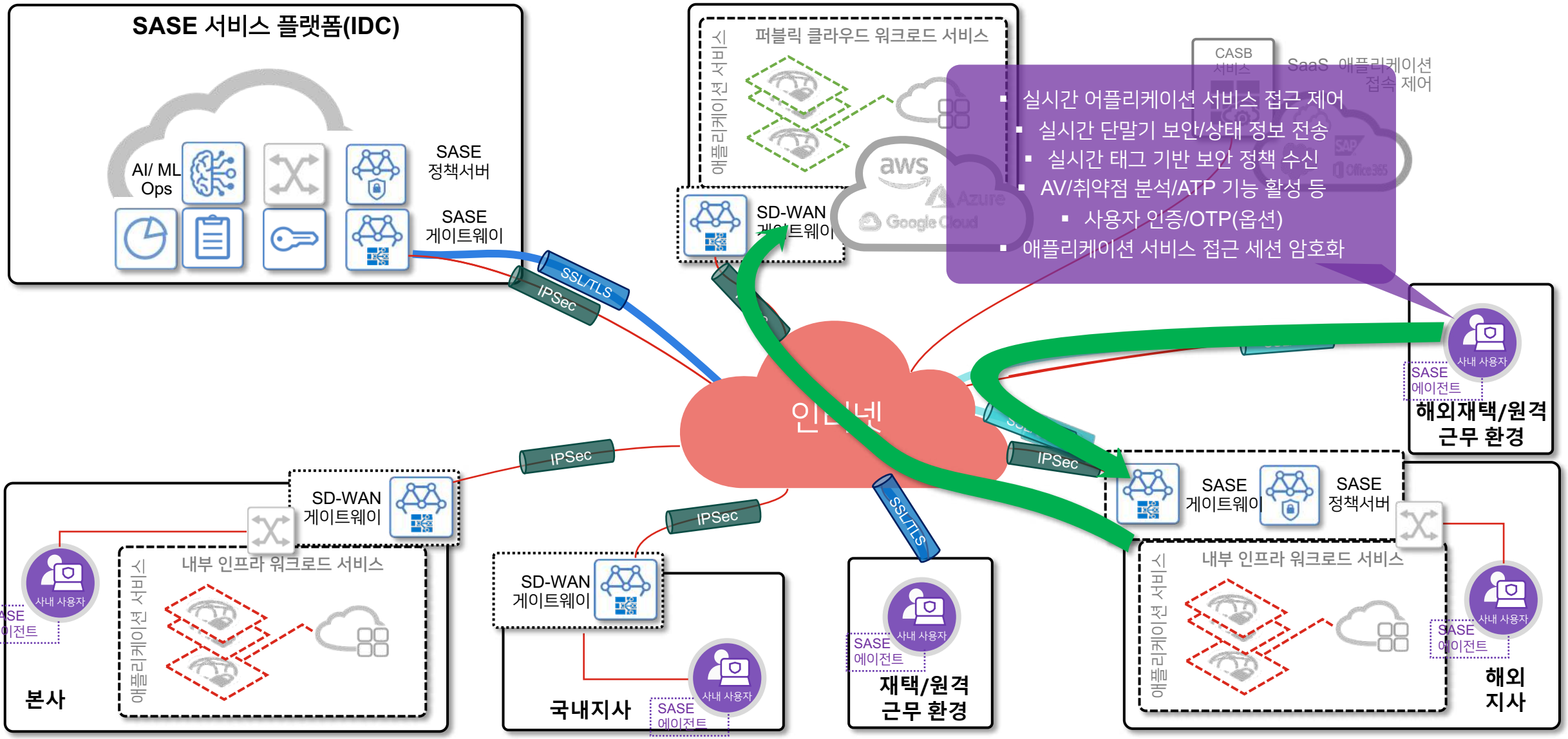
유즈케이스 : 온프레미스



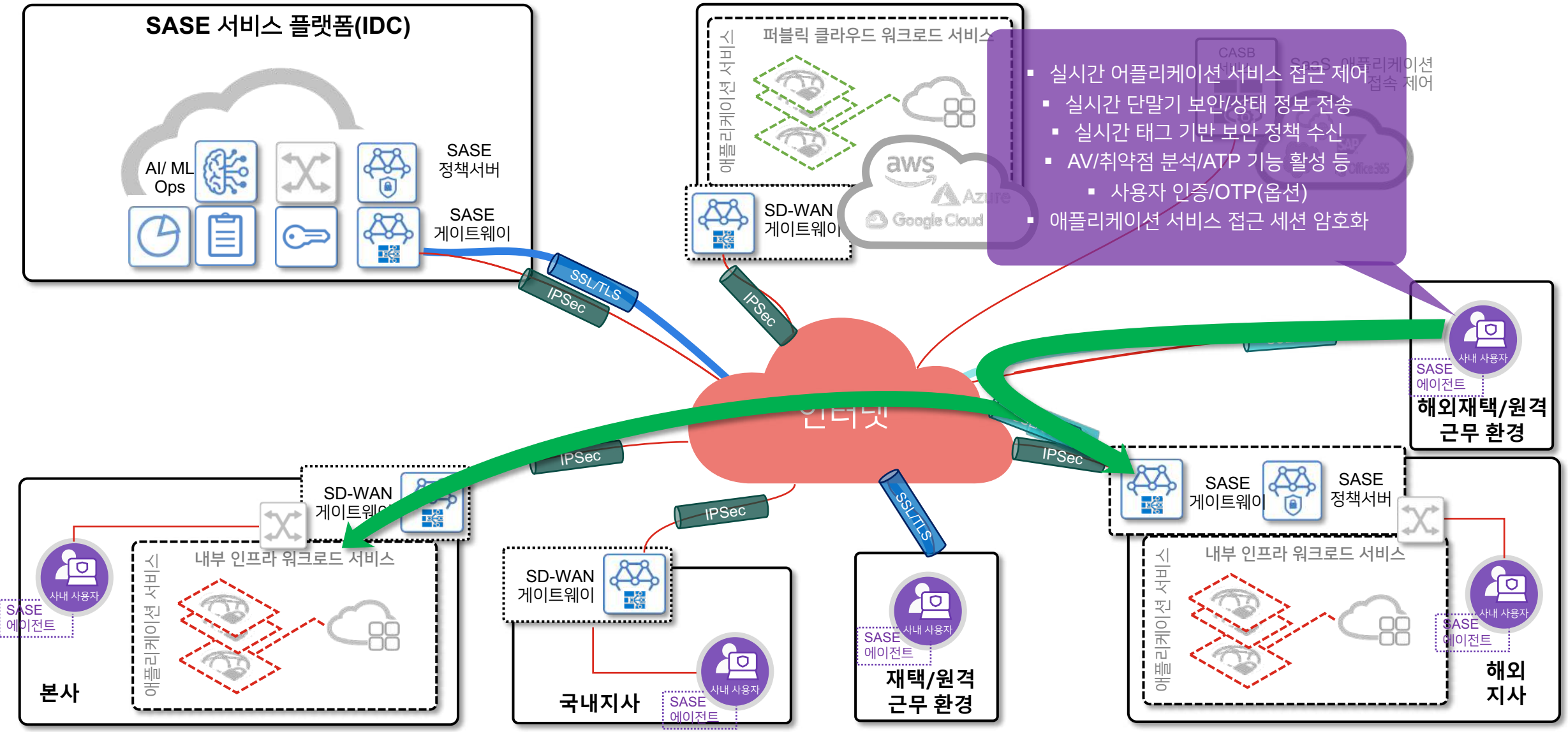
유즈케이스 : 온프레미스



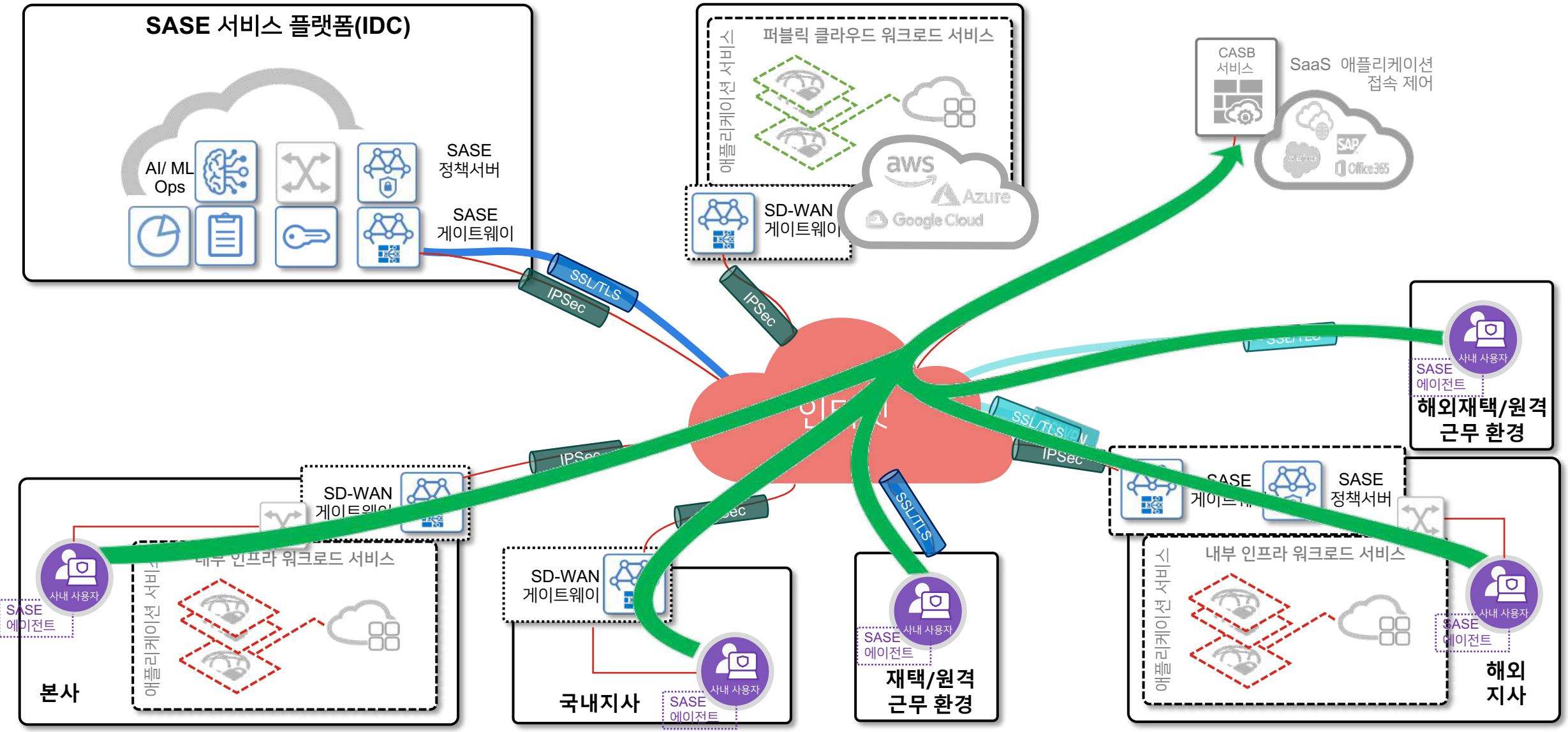
유즈케이스 : 온프레미스



유즈케이스 : 온프레미스



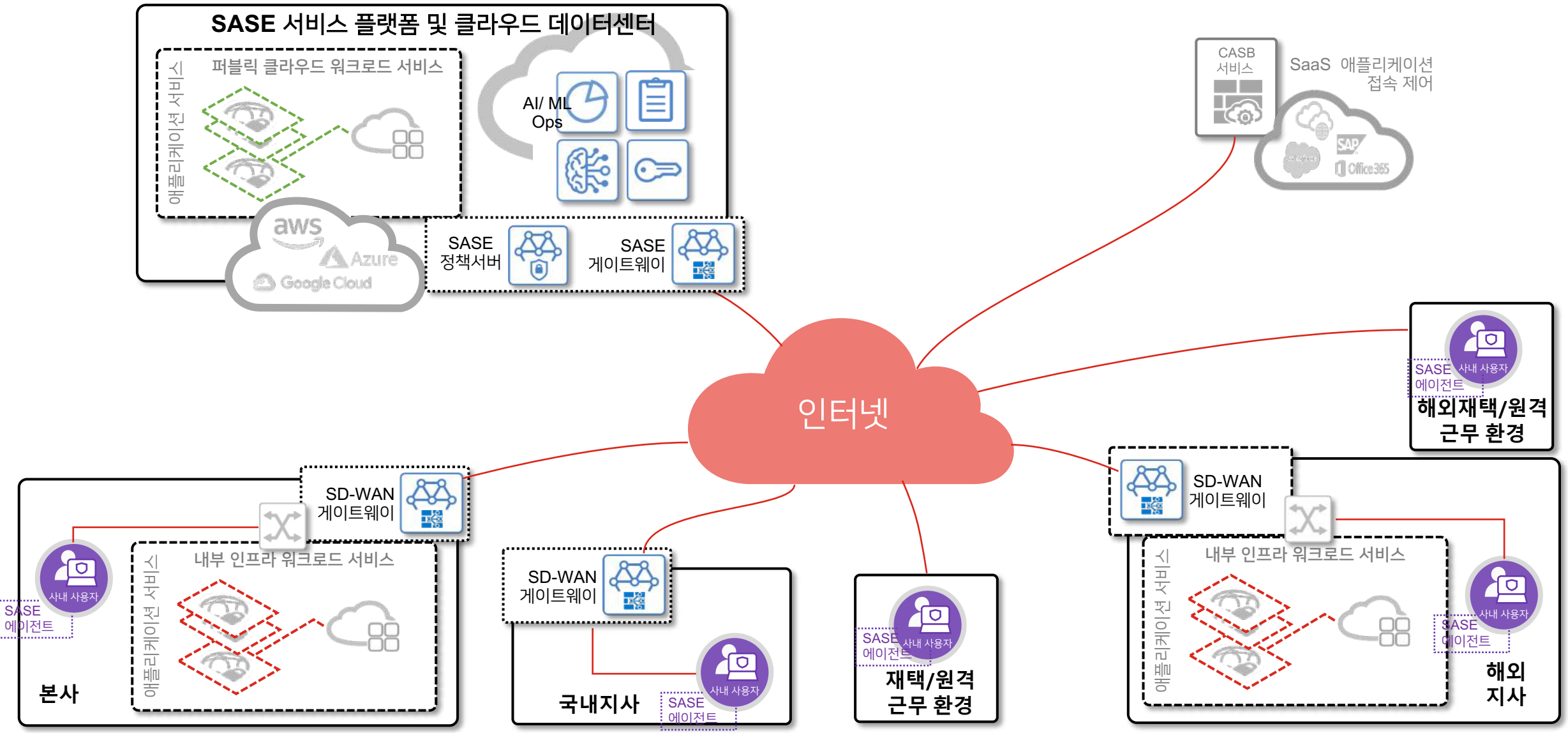
유즈케이스 : 온프레미스



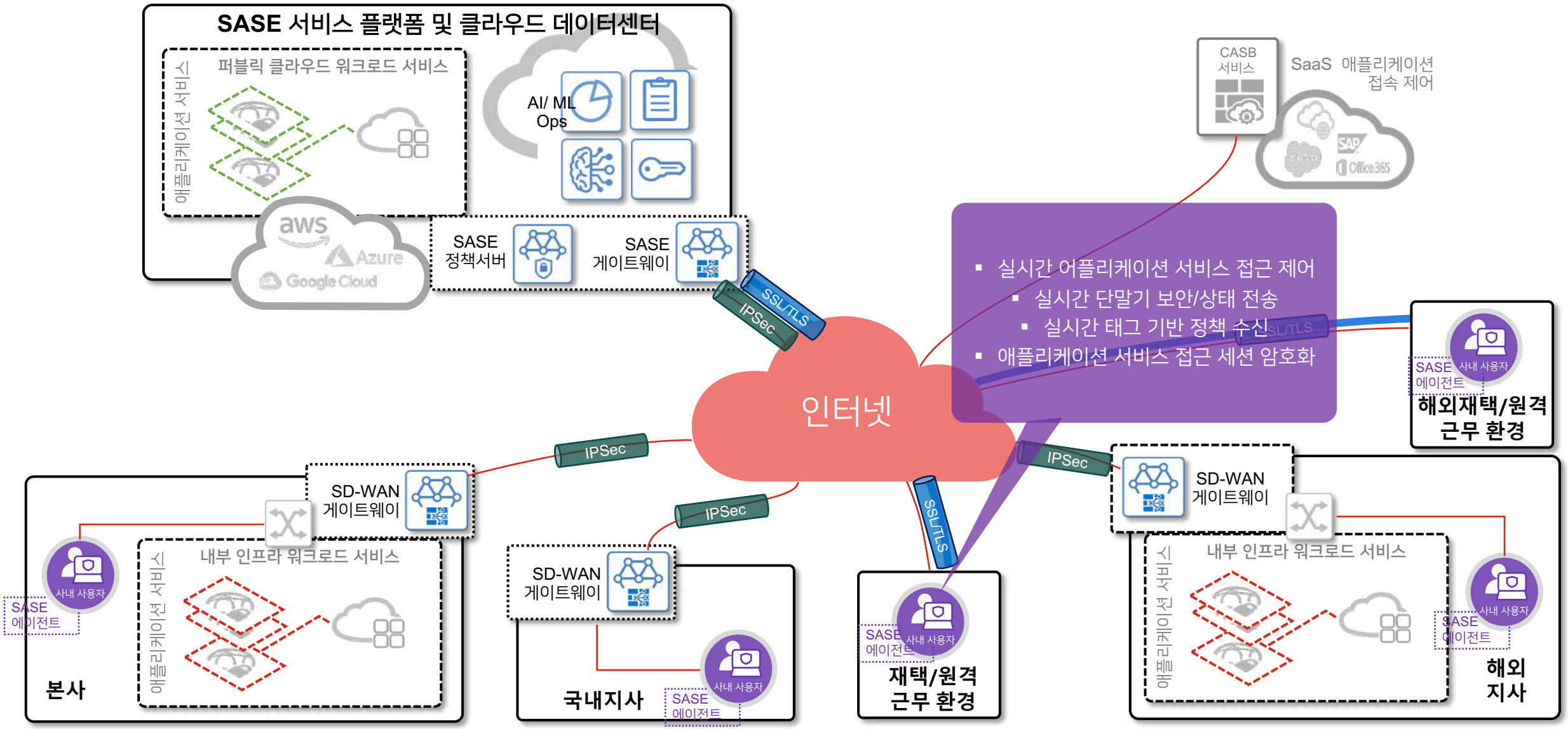
유즈케이스

클라우드

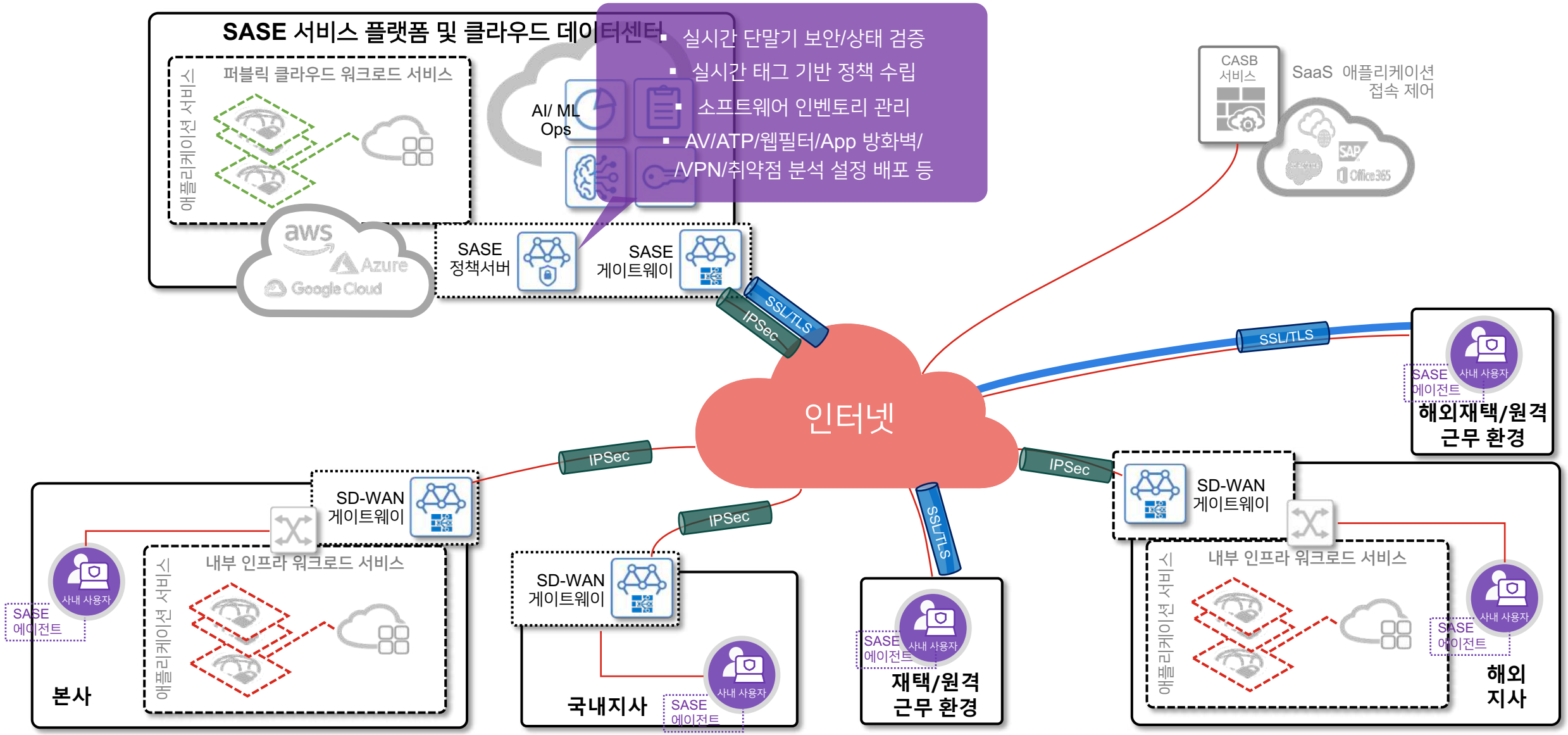
유즈케이스 : 클라우드



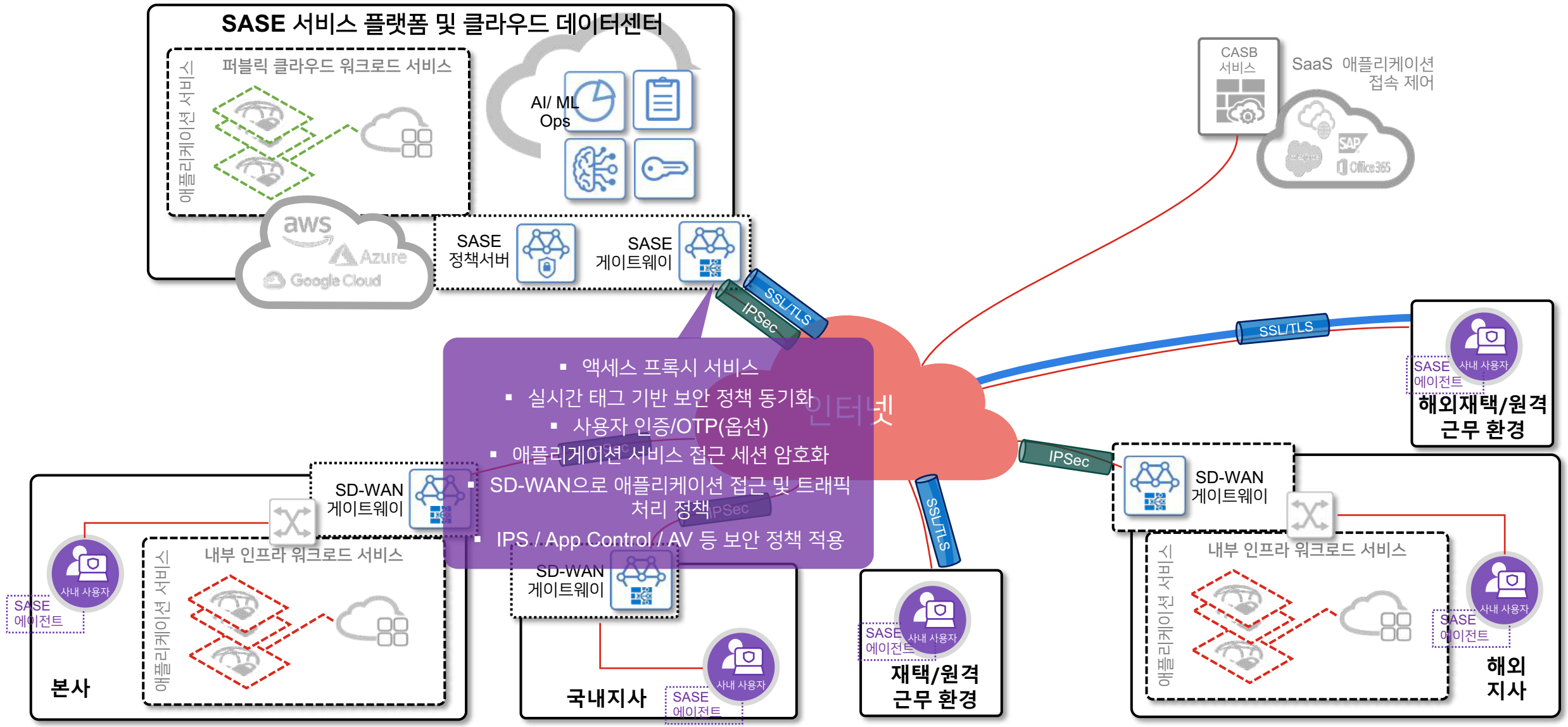
유즈케이스 : 클라우드



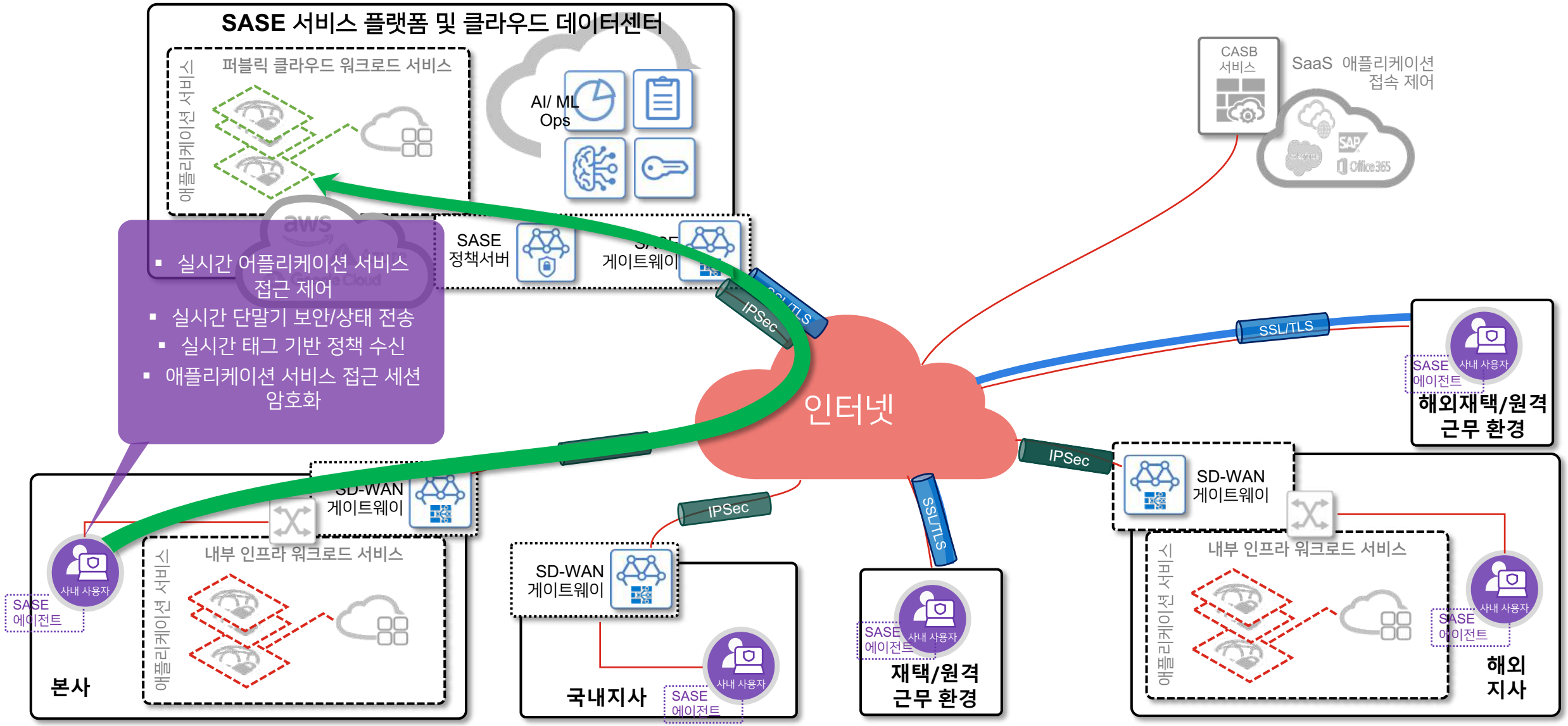
유즈케이스 : 클라우드



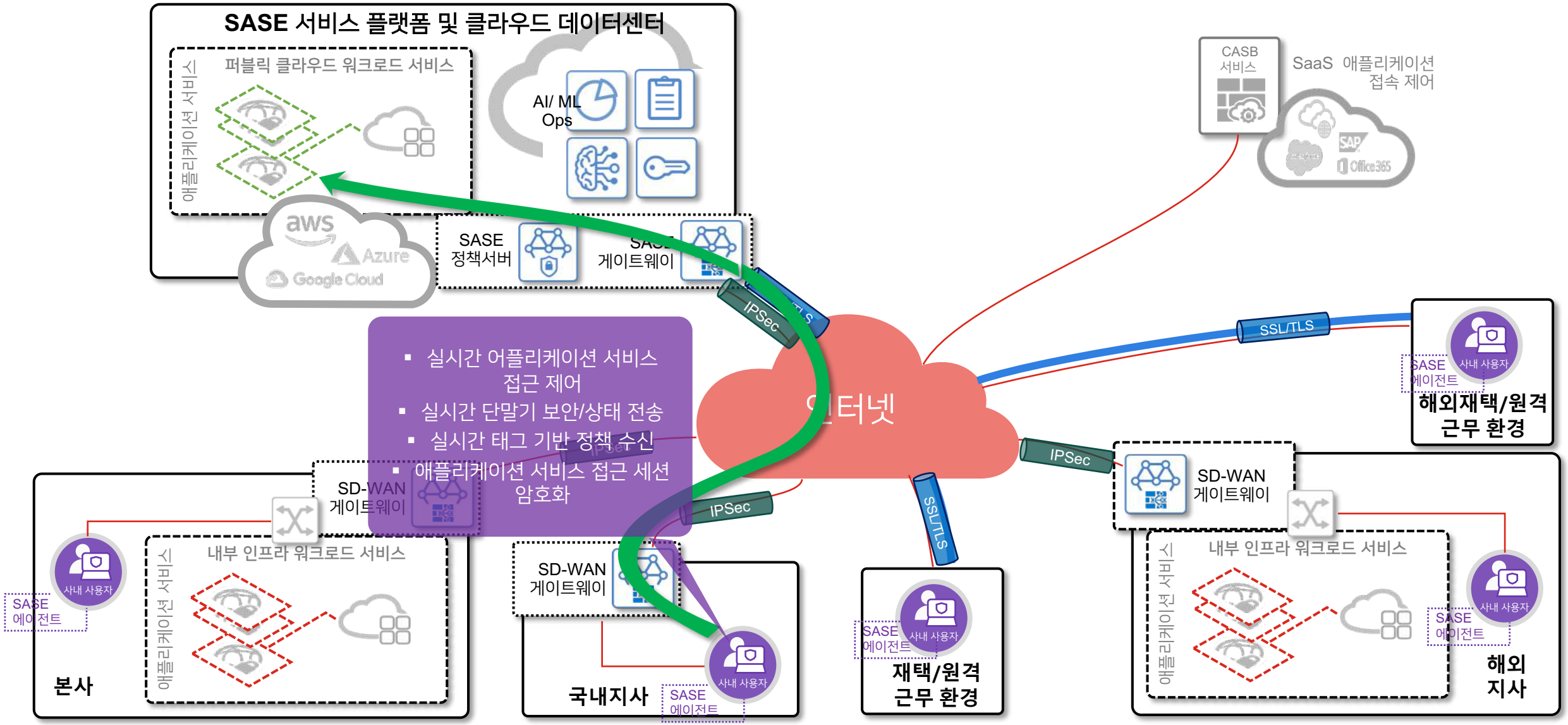
유즈케이스 : 클라우드



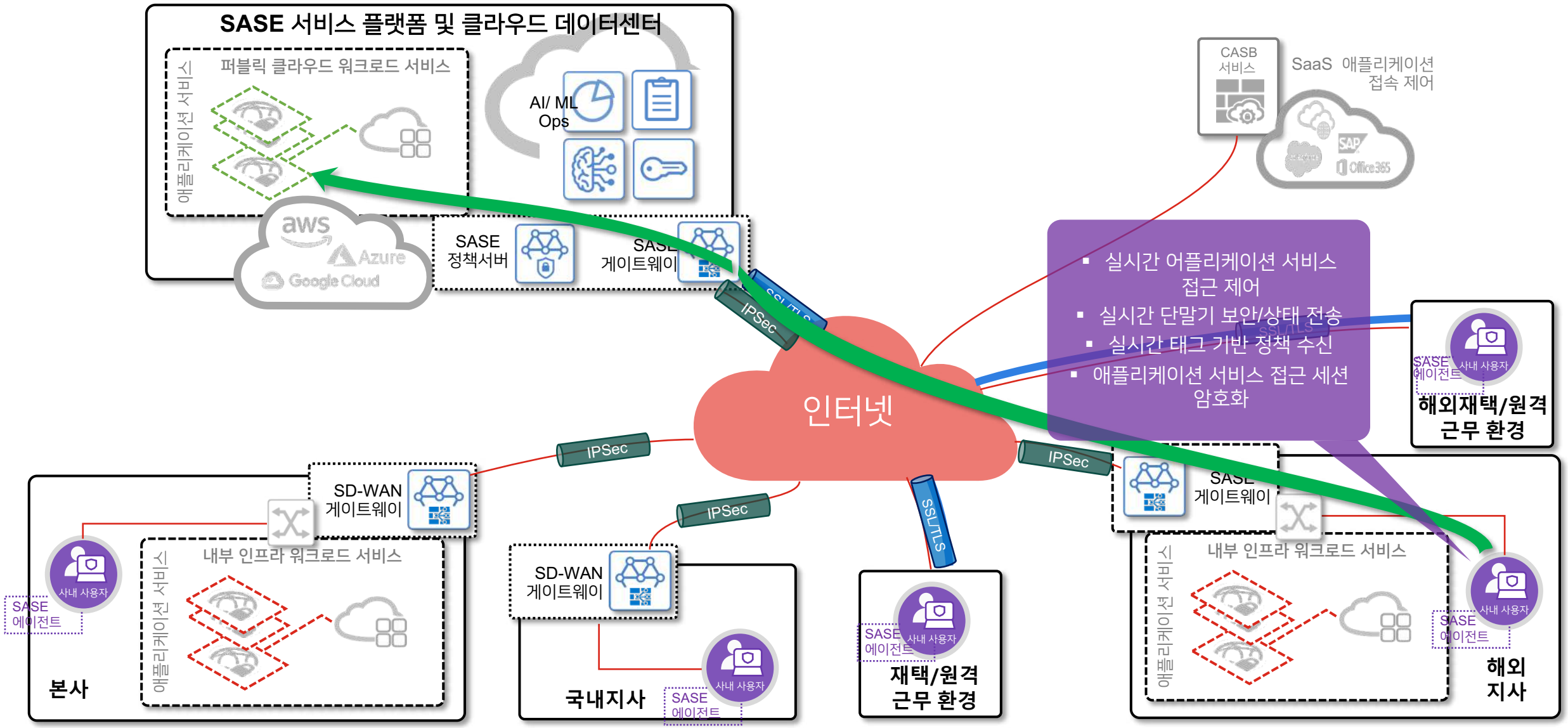
유즈케이스 : 클라우드



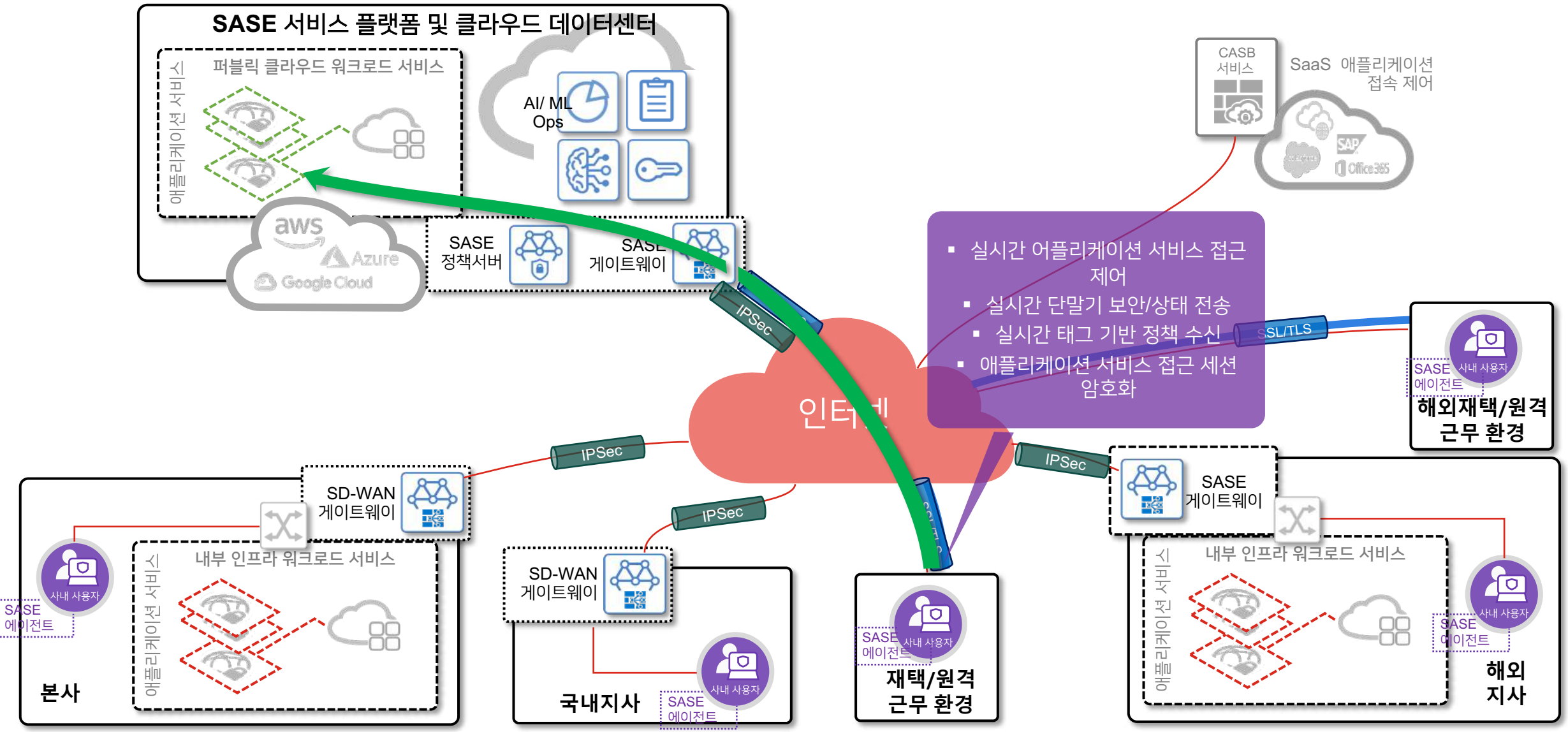
유즈케이스 : 클라우드



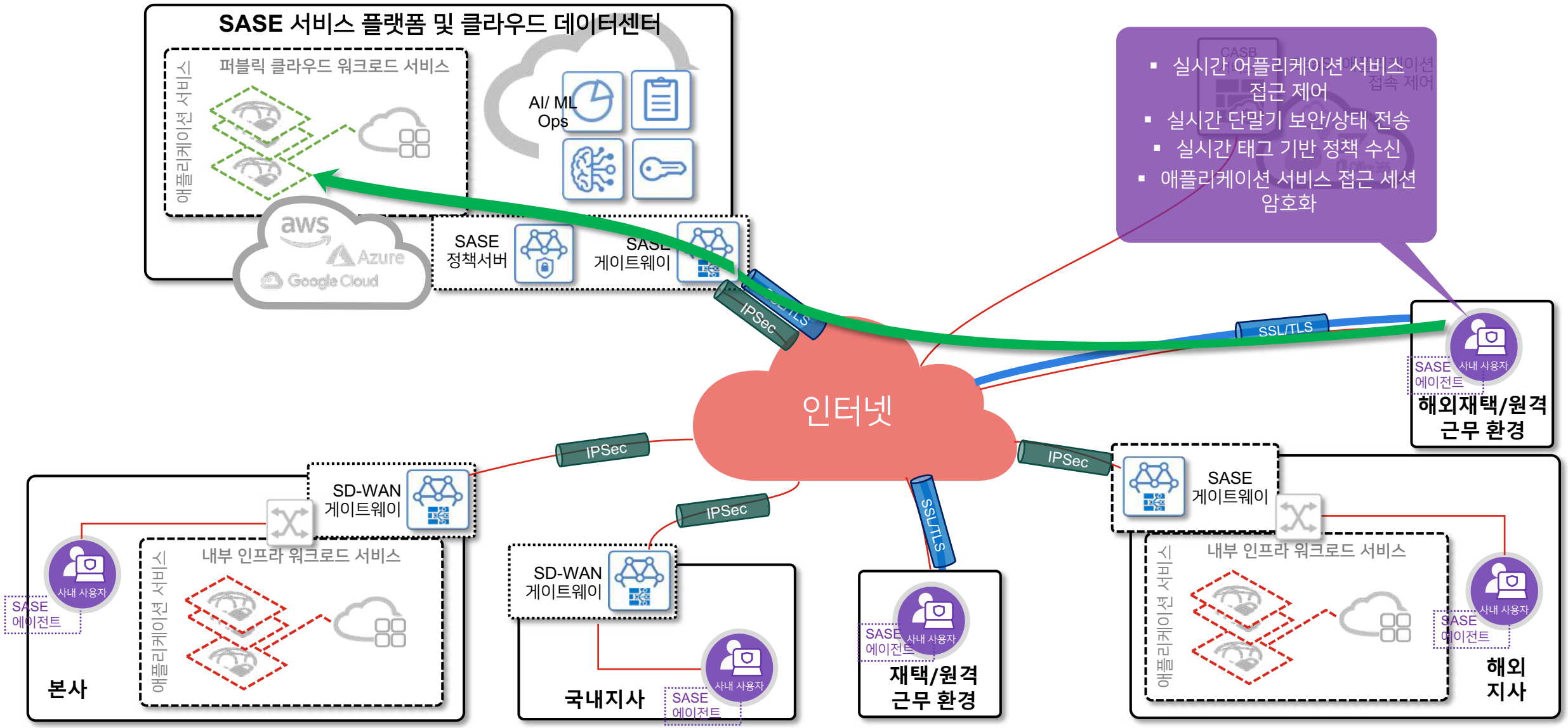
유즈케이스 : 클라우드



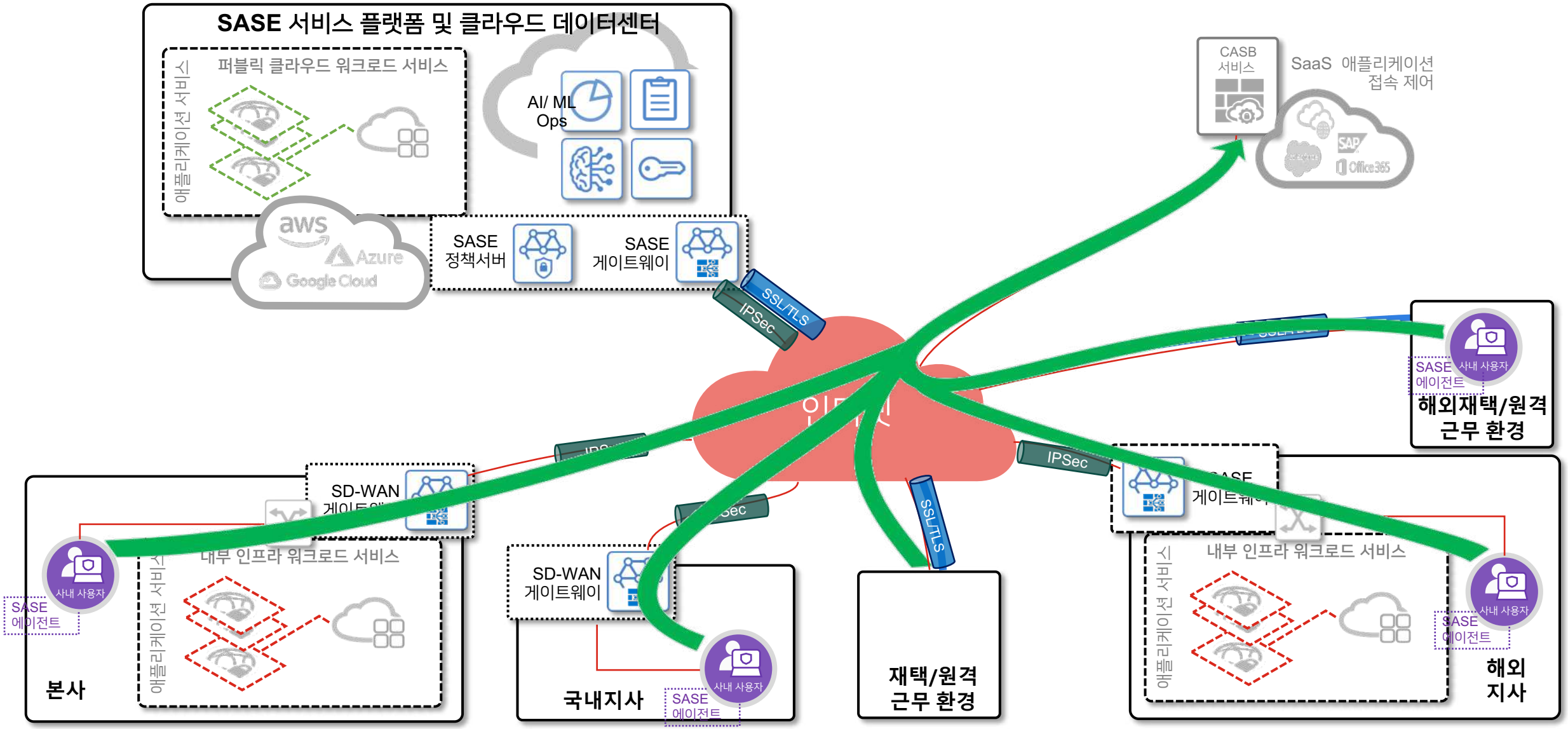
유즈케이스 : 클라우드



유즈케이스 : 클라우드



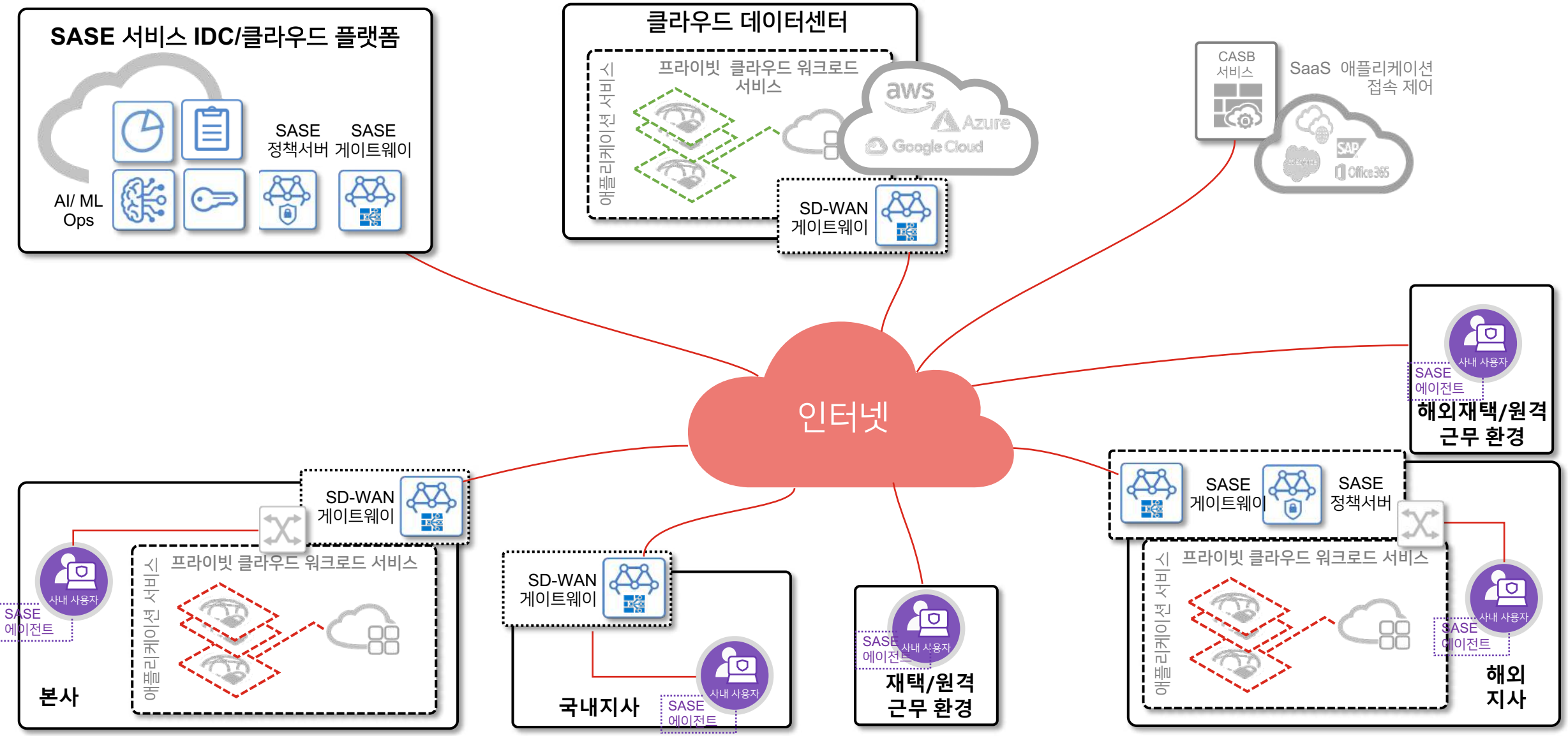
유즈케이스 : 클라우드



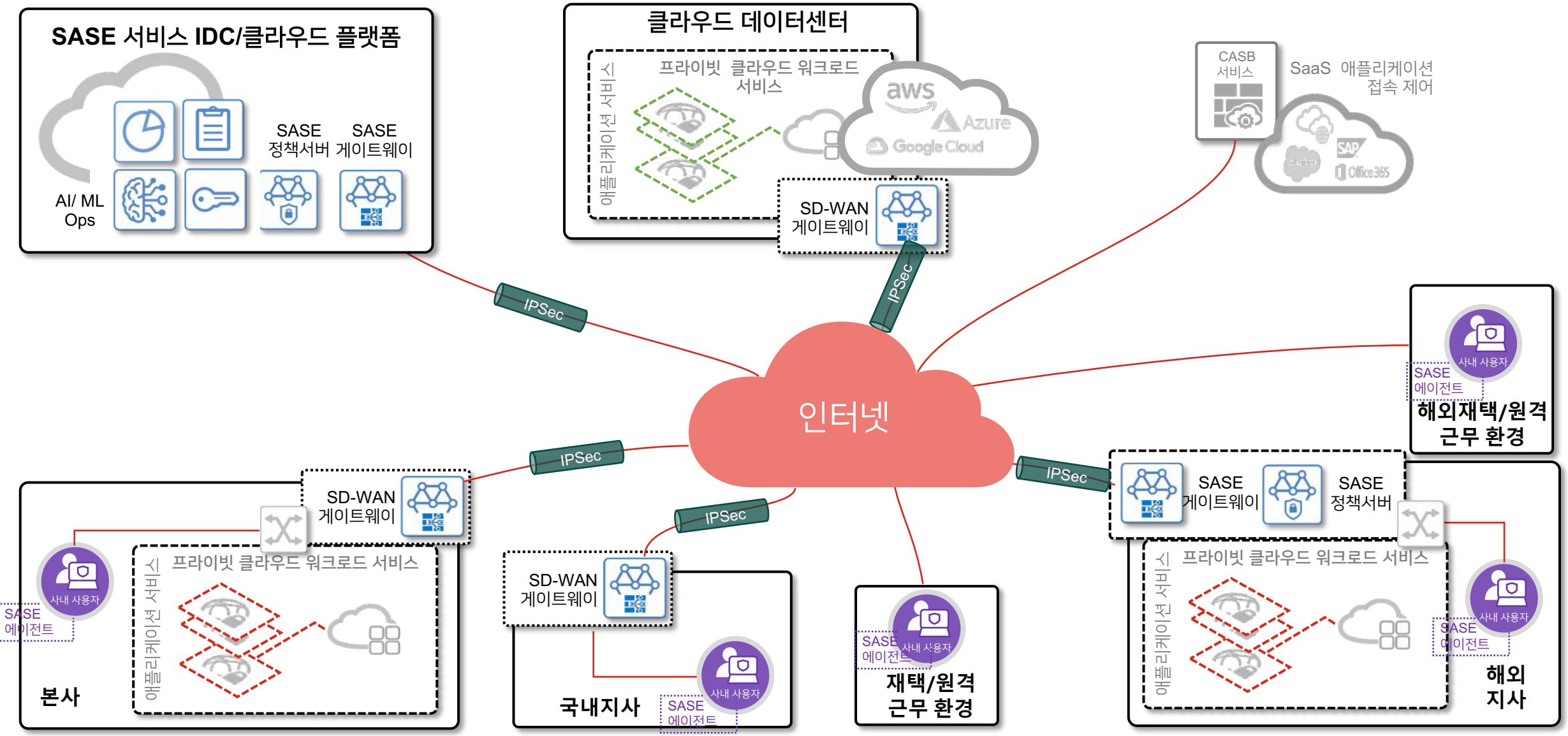
유즈케이스

하이브리드

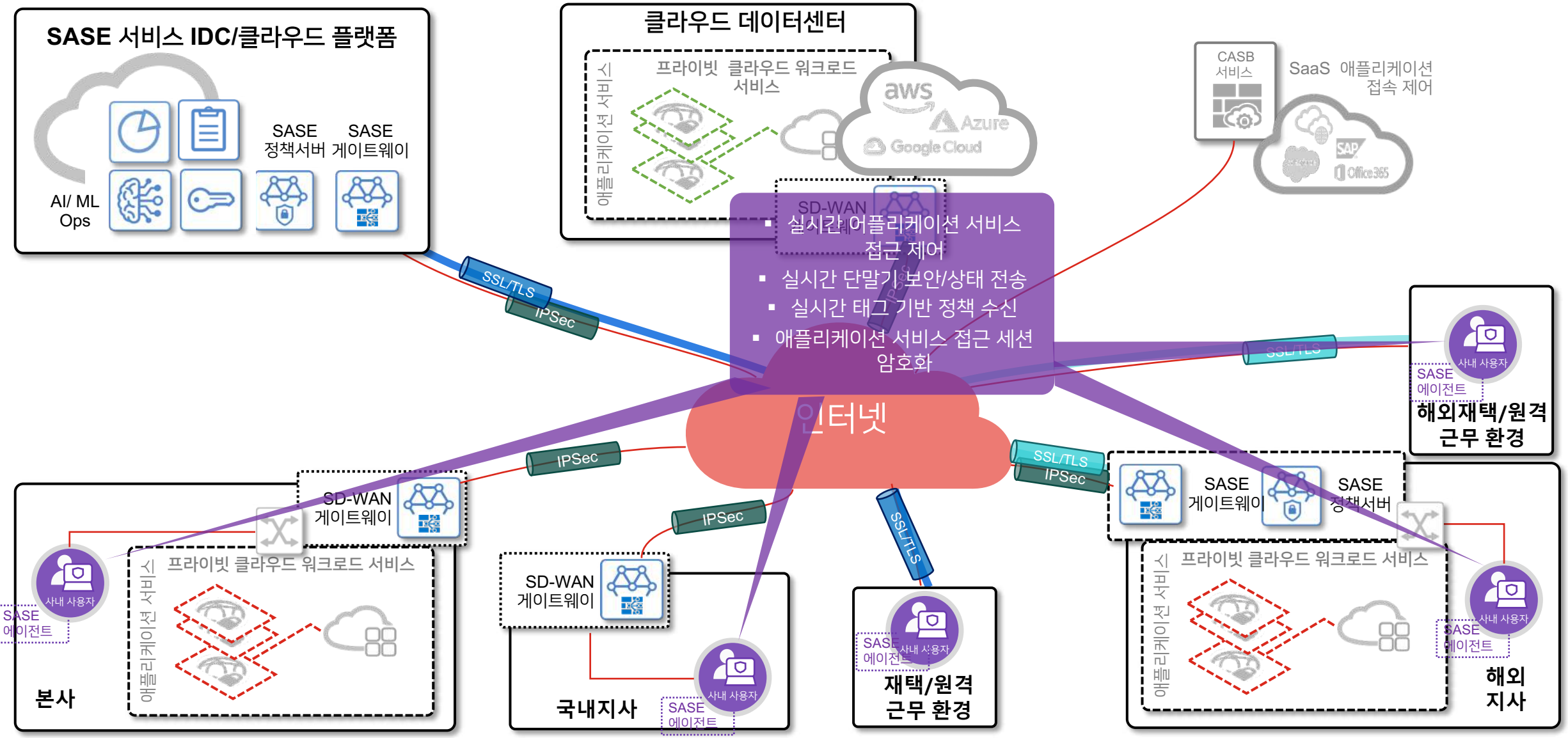
유즈케이스 : 하이브리드



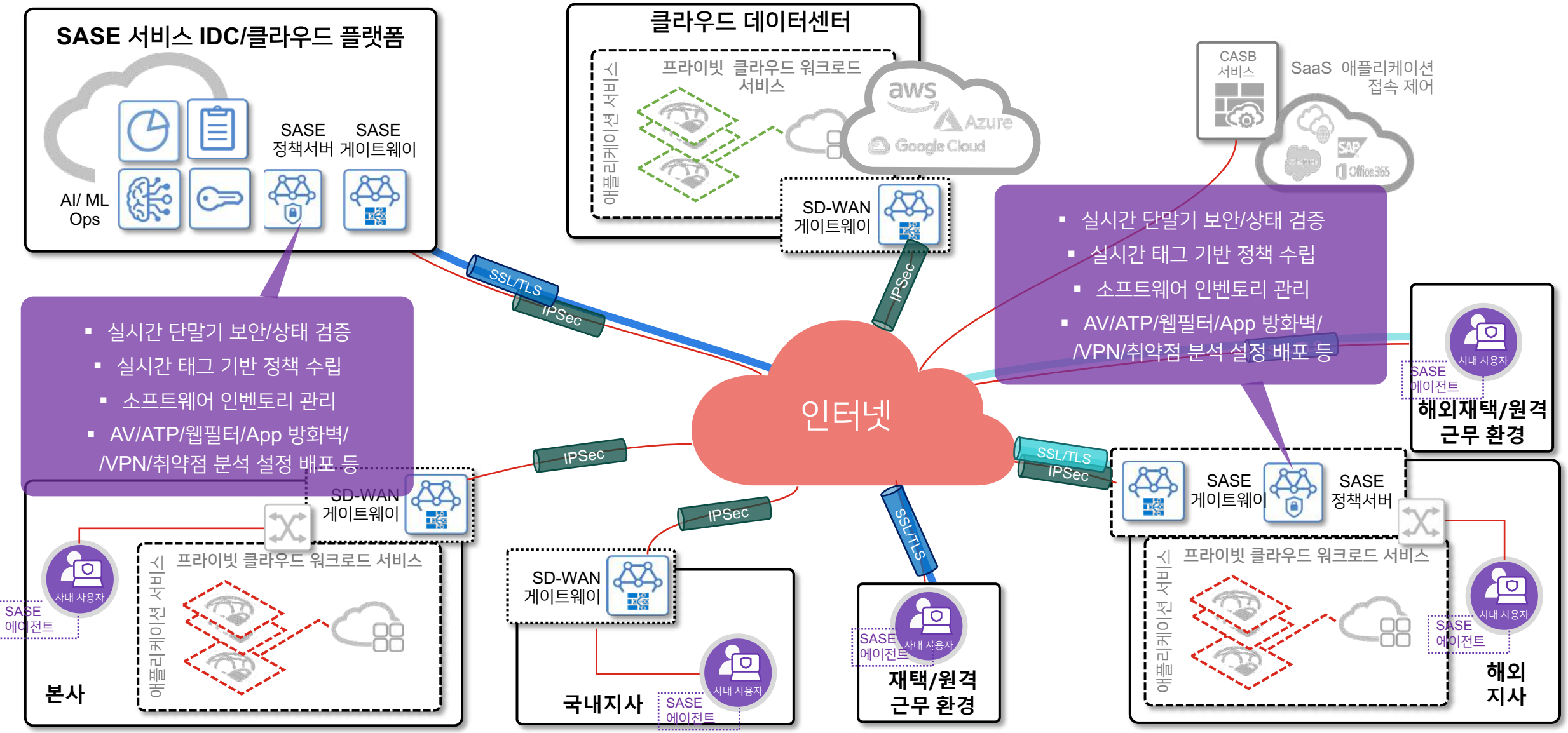
유즈케이스 : 하이브리드



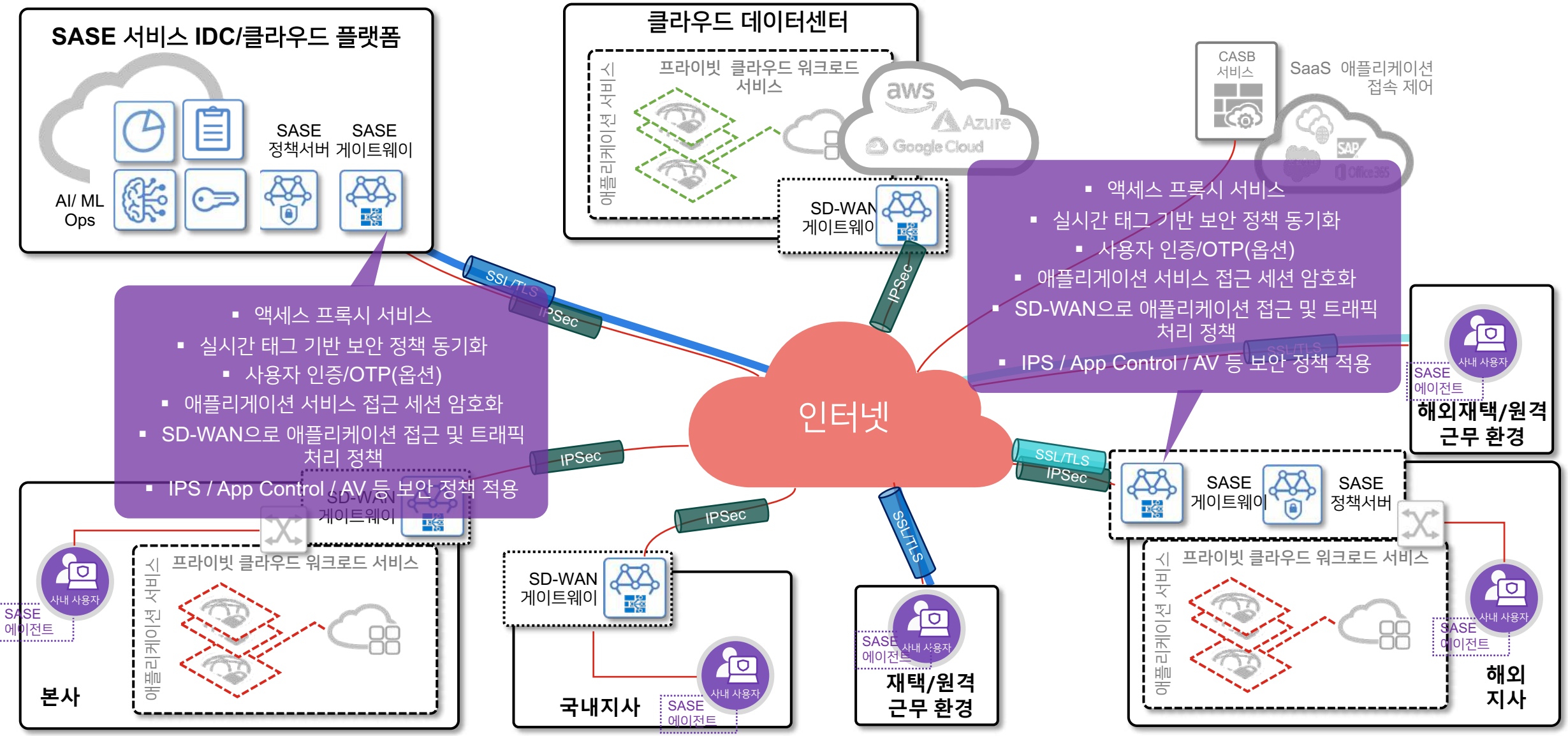
유즈케이스 : 하이브리드



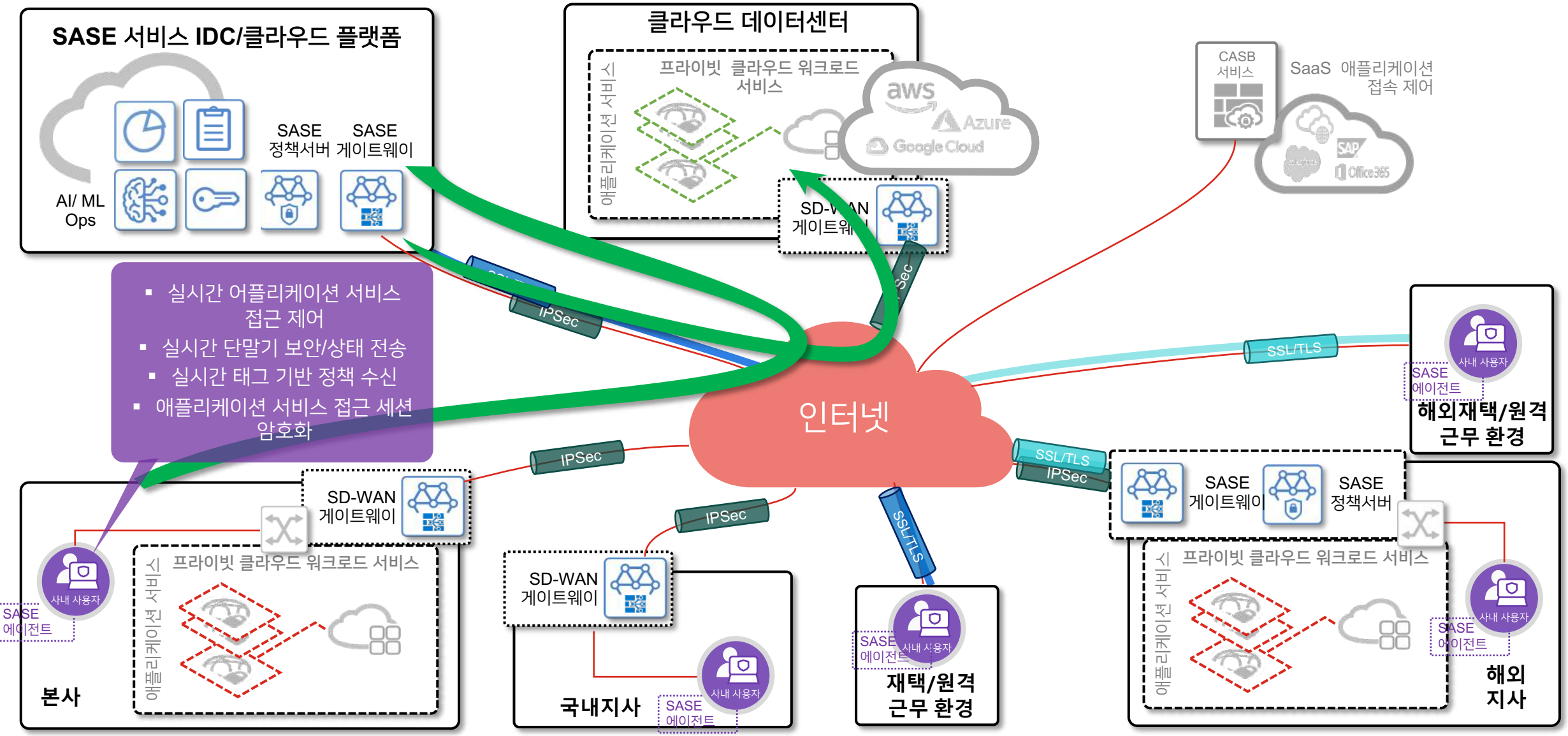
유즈케이스 : 하이브리드



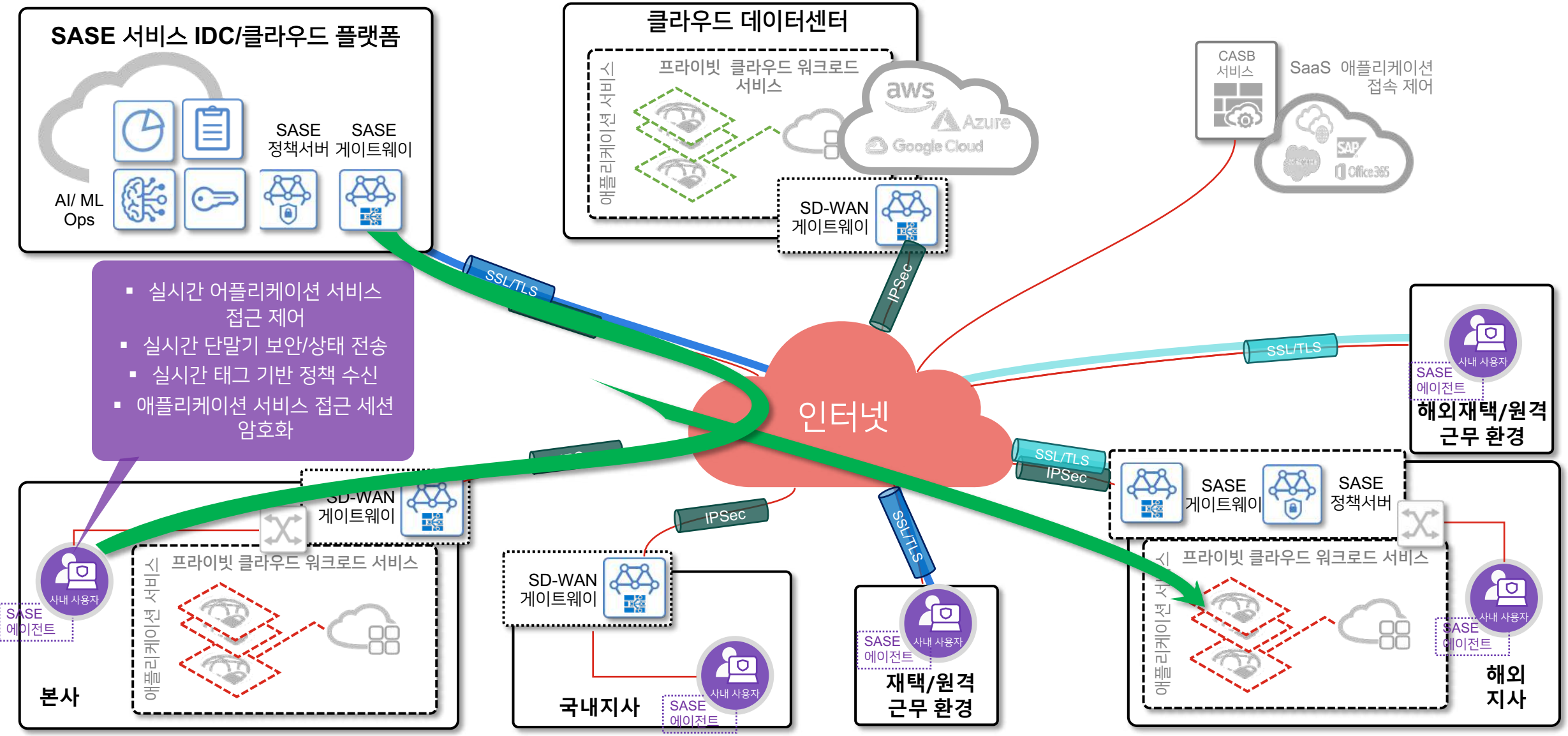
유즈케이스 : 하이브리드



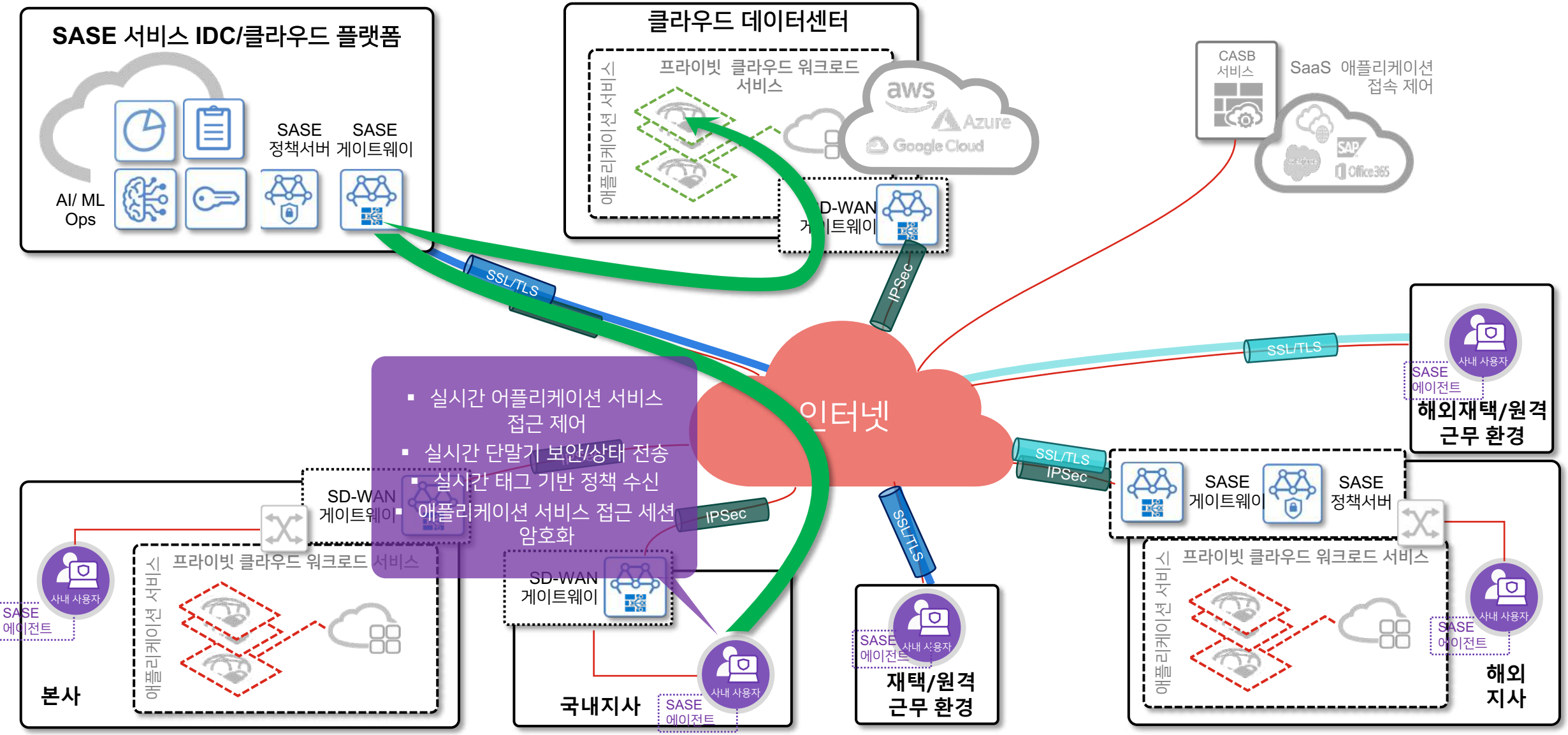
유즈케이스 : 하이브리드



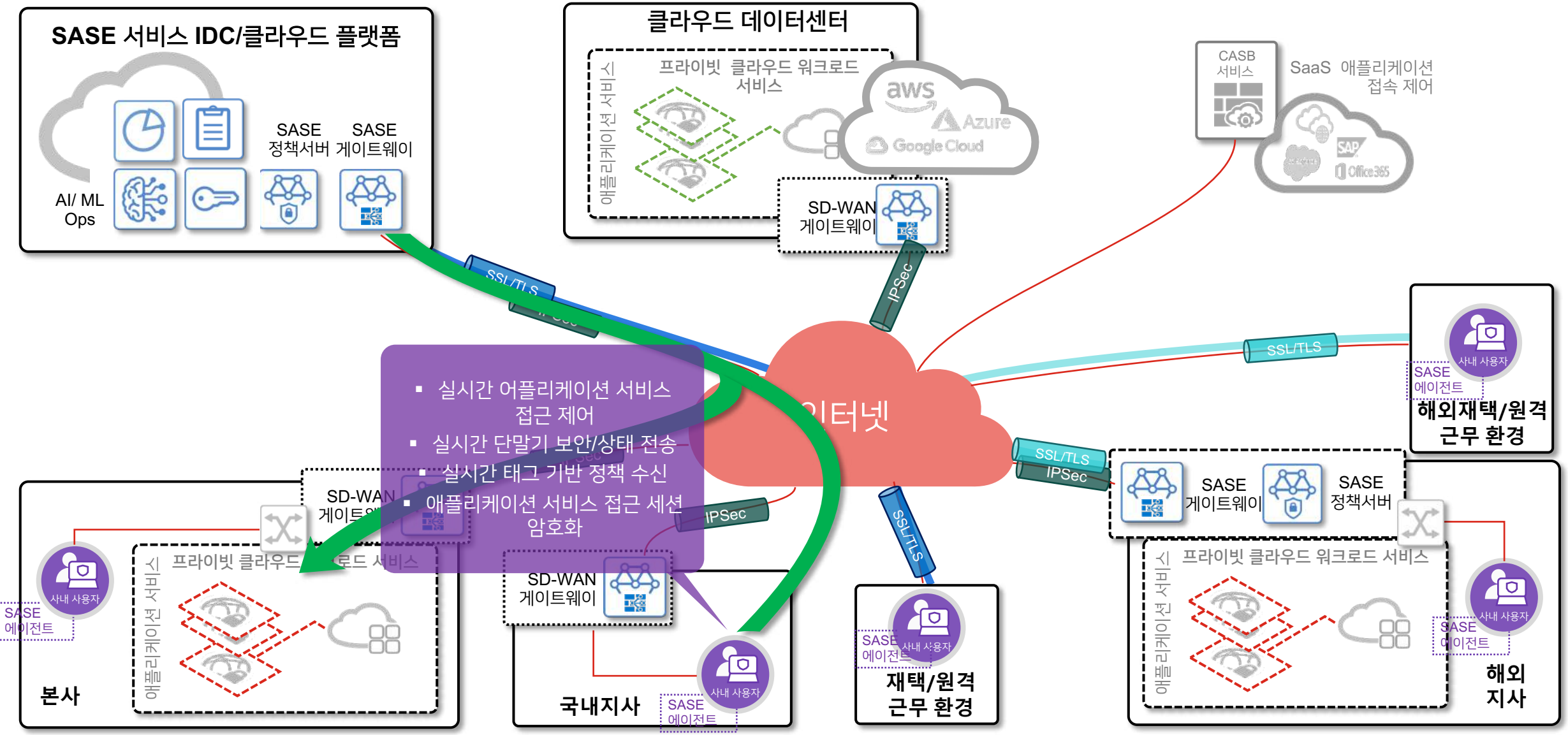
유즈케이스 : 하이브리드



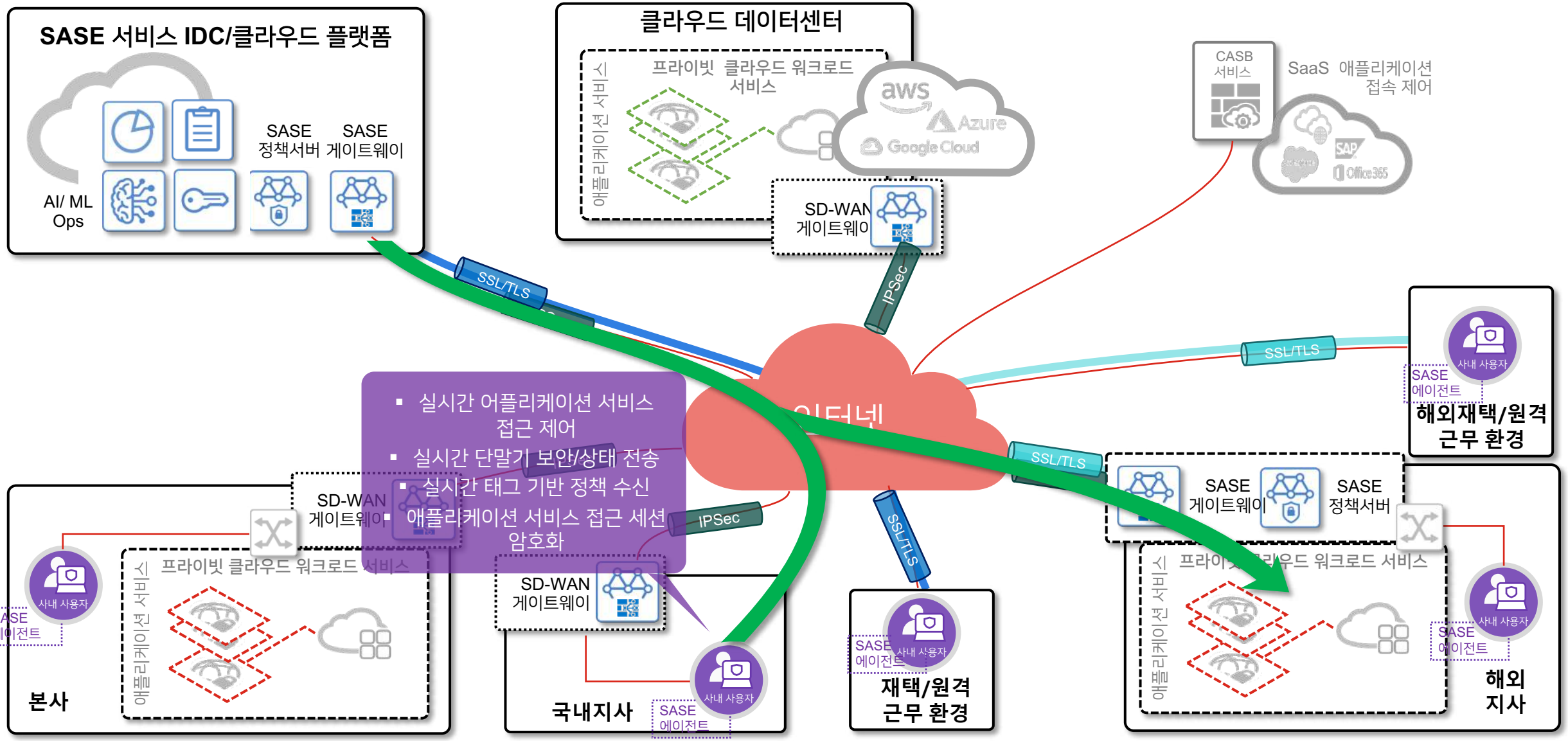
유즈케이스 : 하이브리드



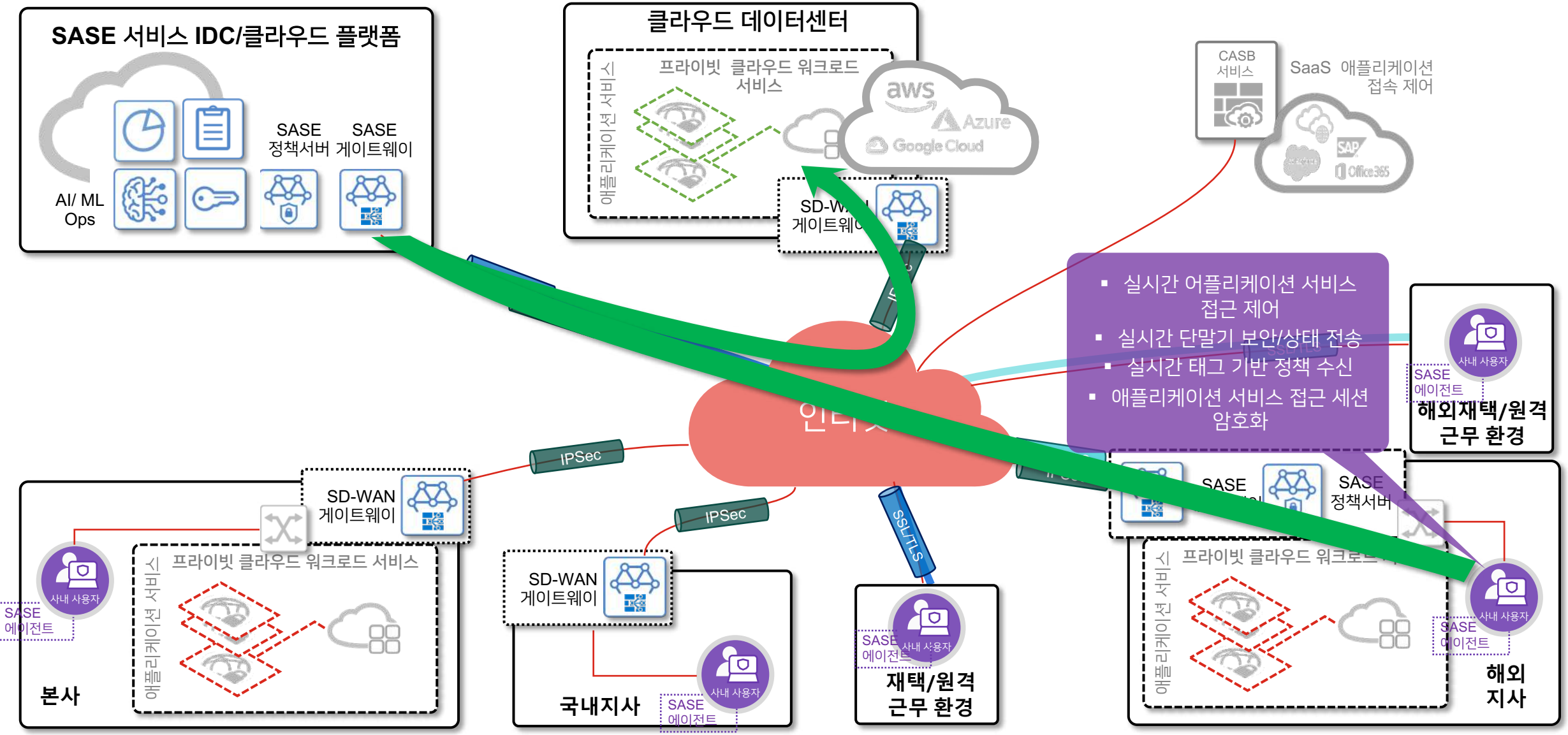
유즈케이스 : 하이브리드



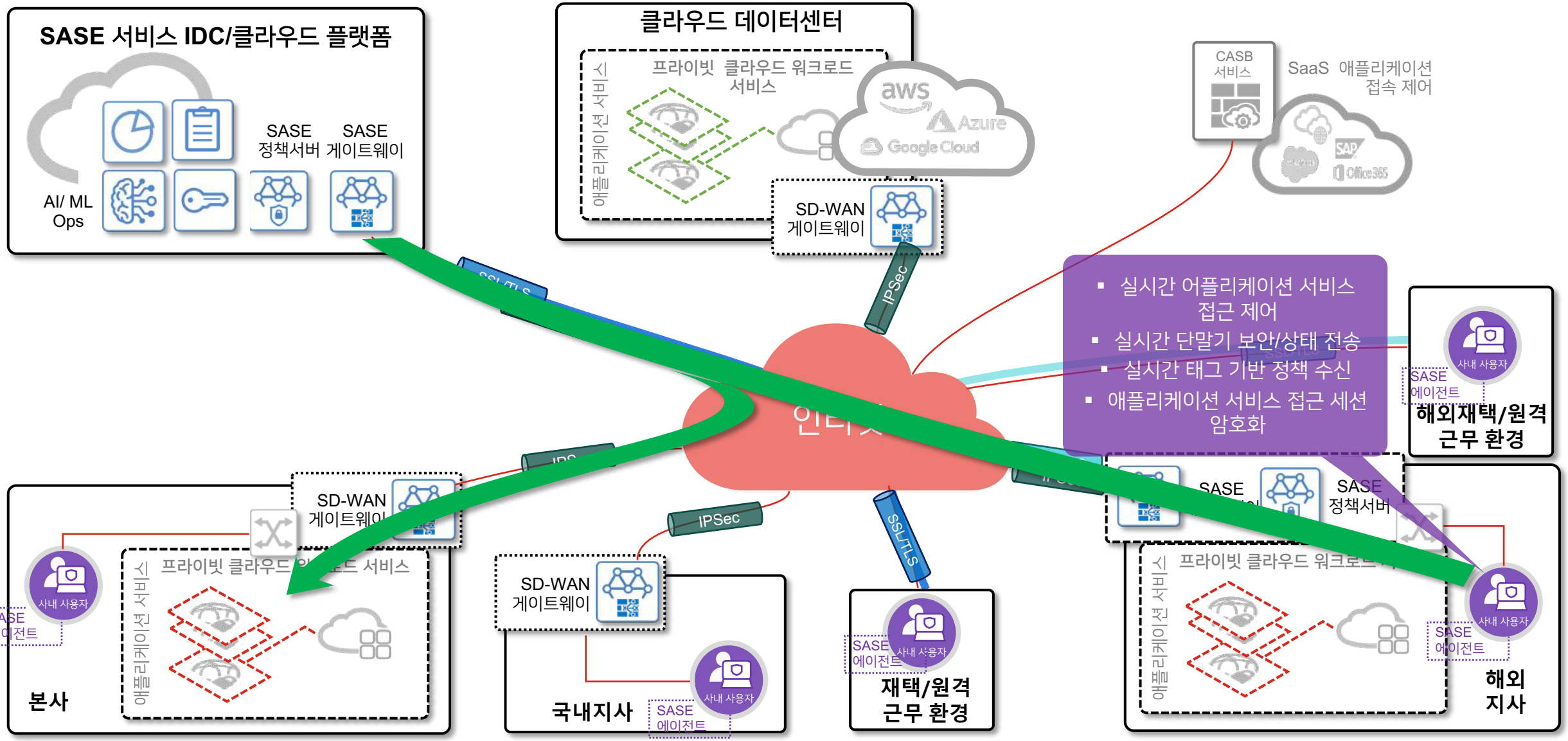
유즈케이스 : 하이브리드



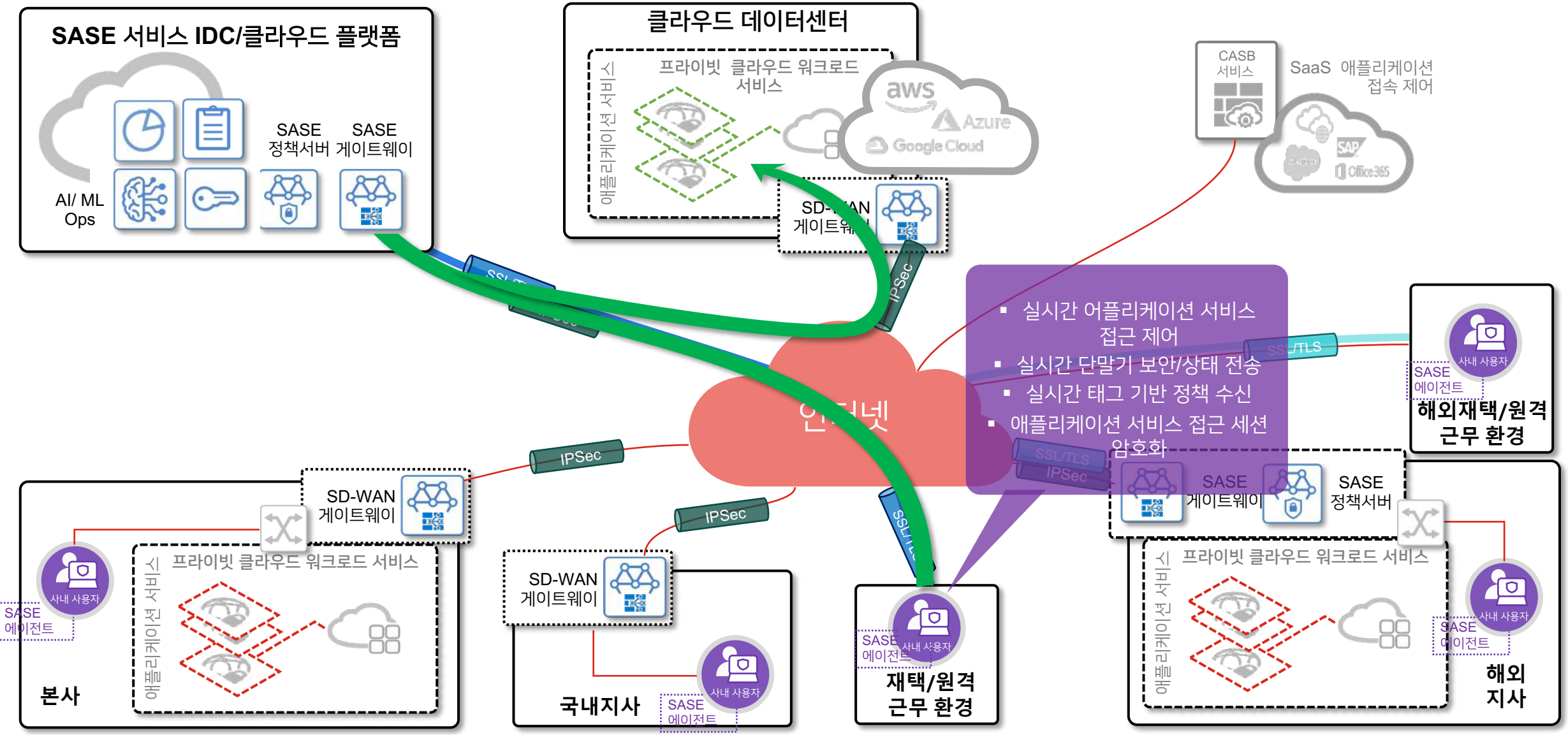
유즈케이스 : 하이브리드



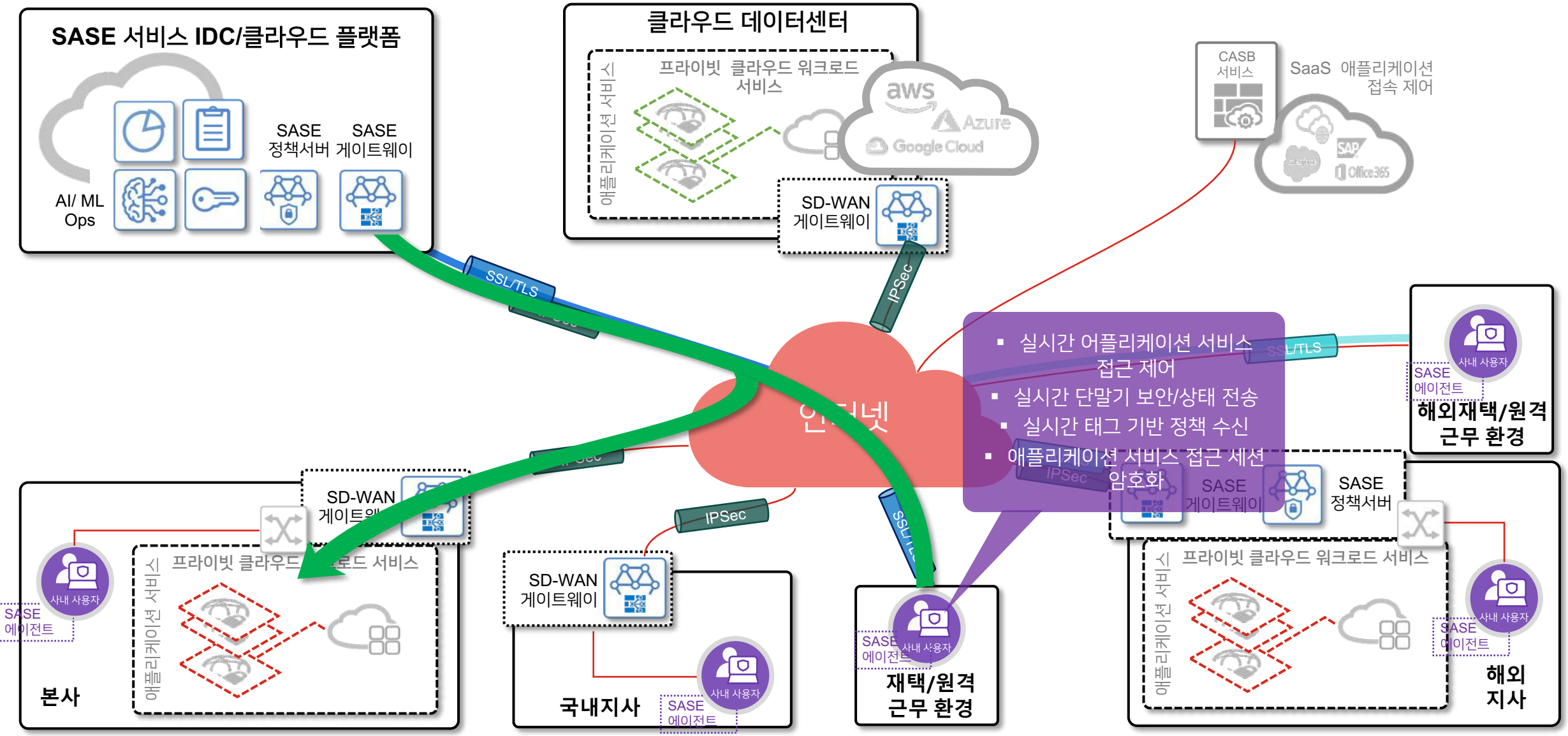
유즈케이스 : 하이브리드



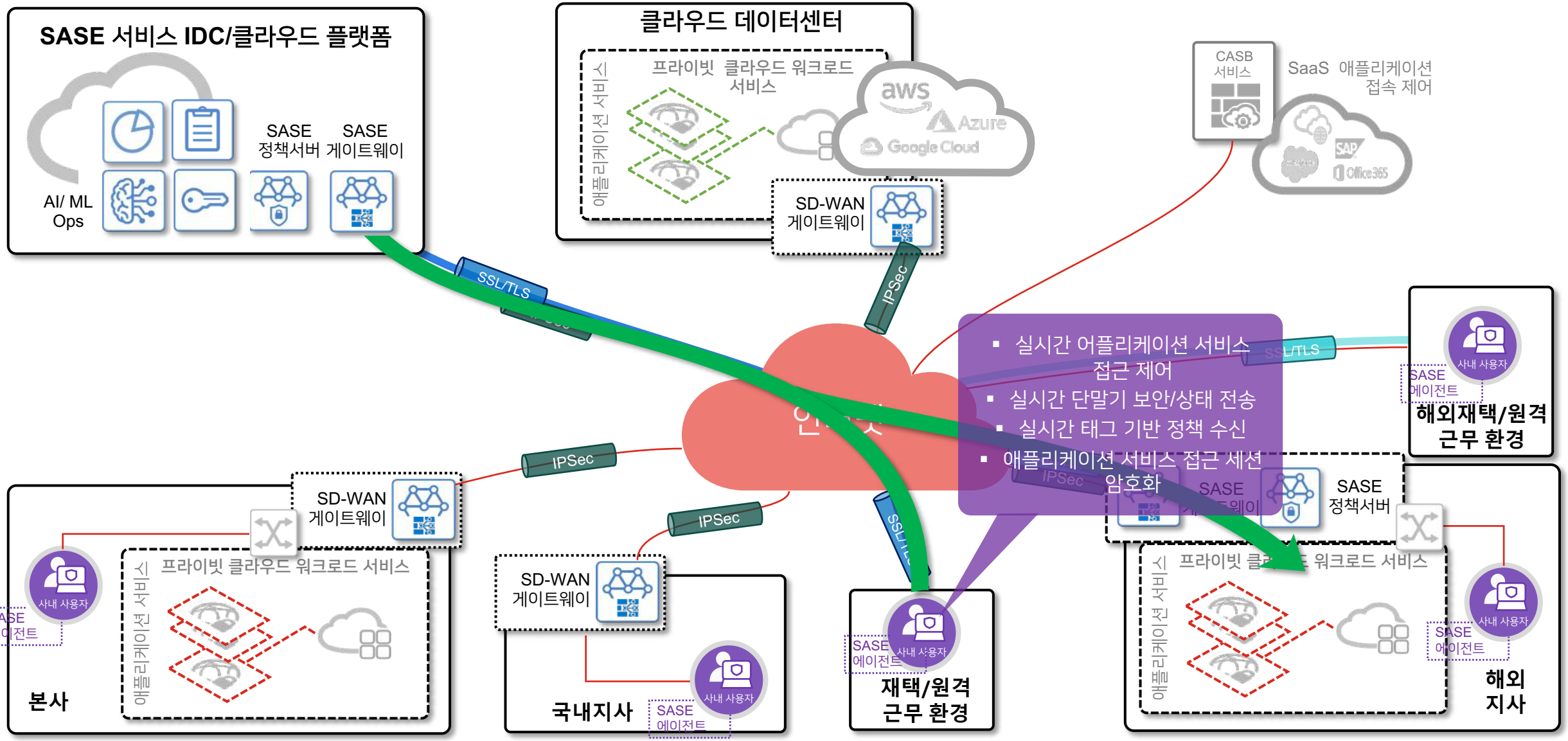
유즈케이스 : 하이브리드



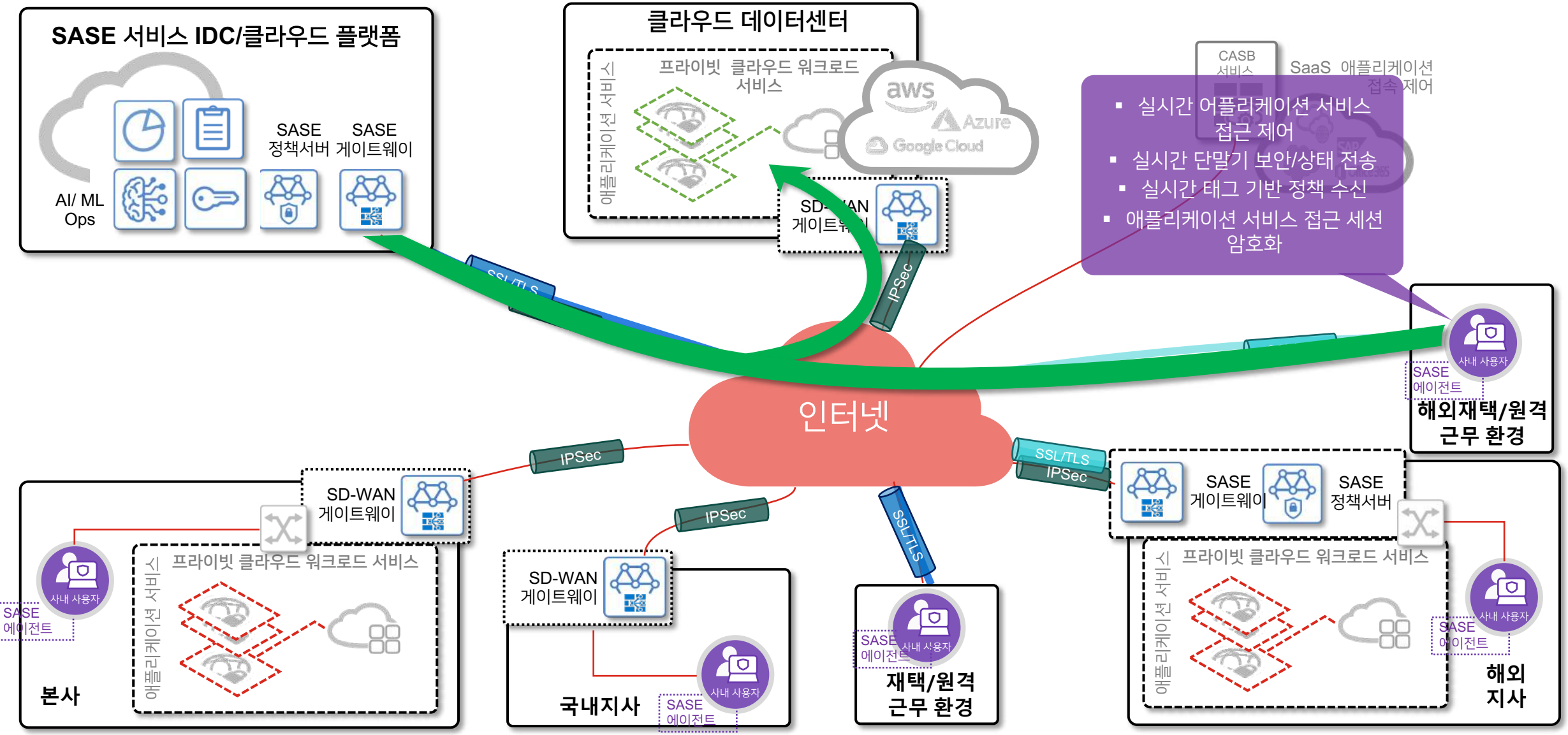
유즈케이스 : 하이브리드



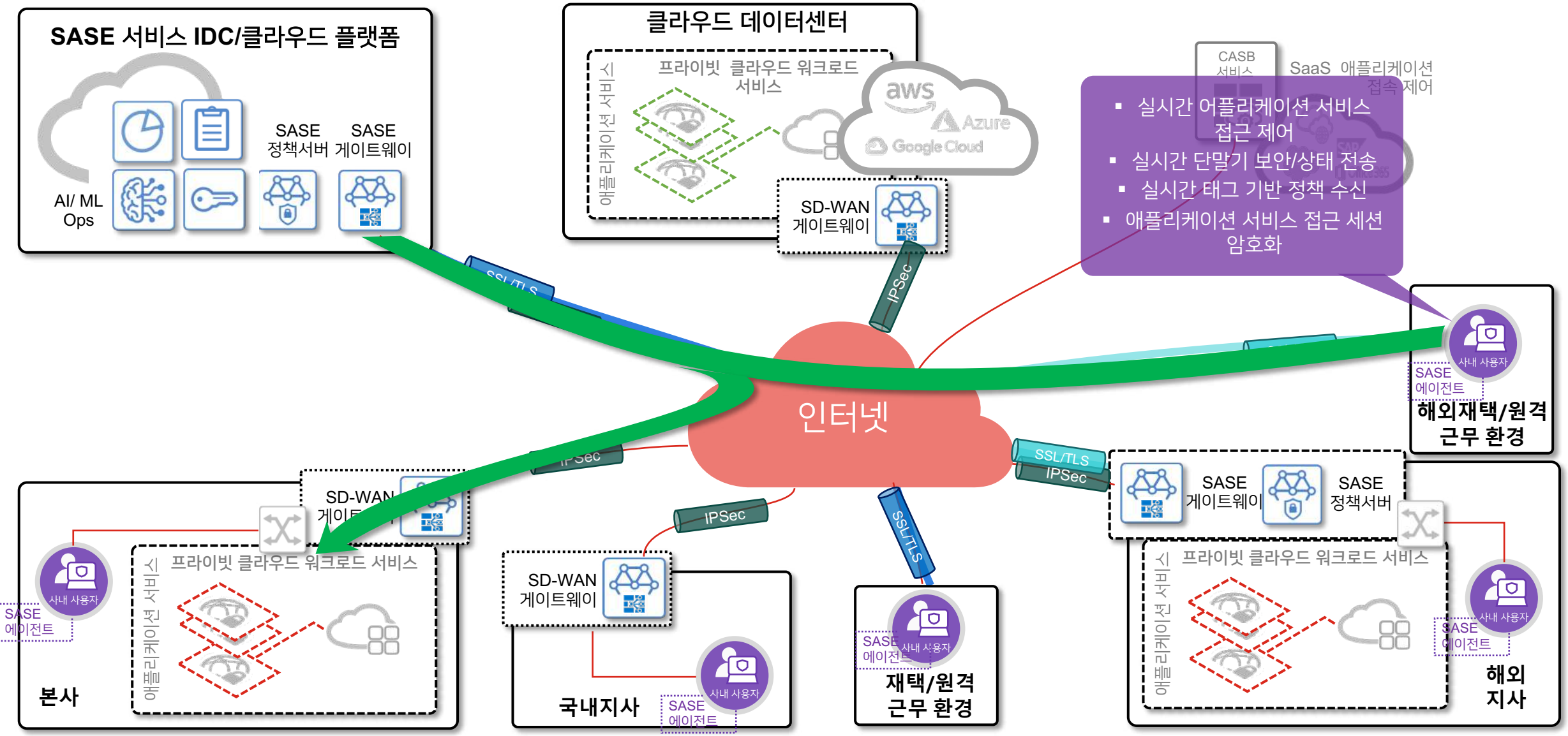
유즈케이스 : 하이브리드



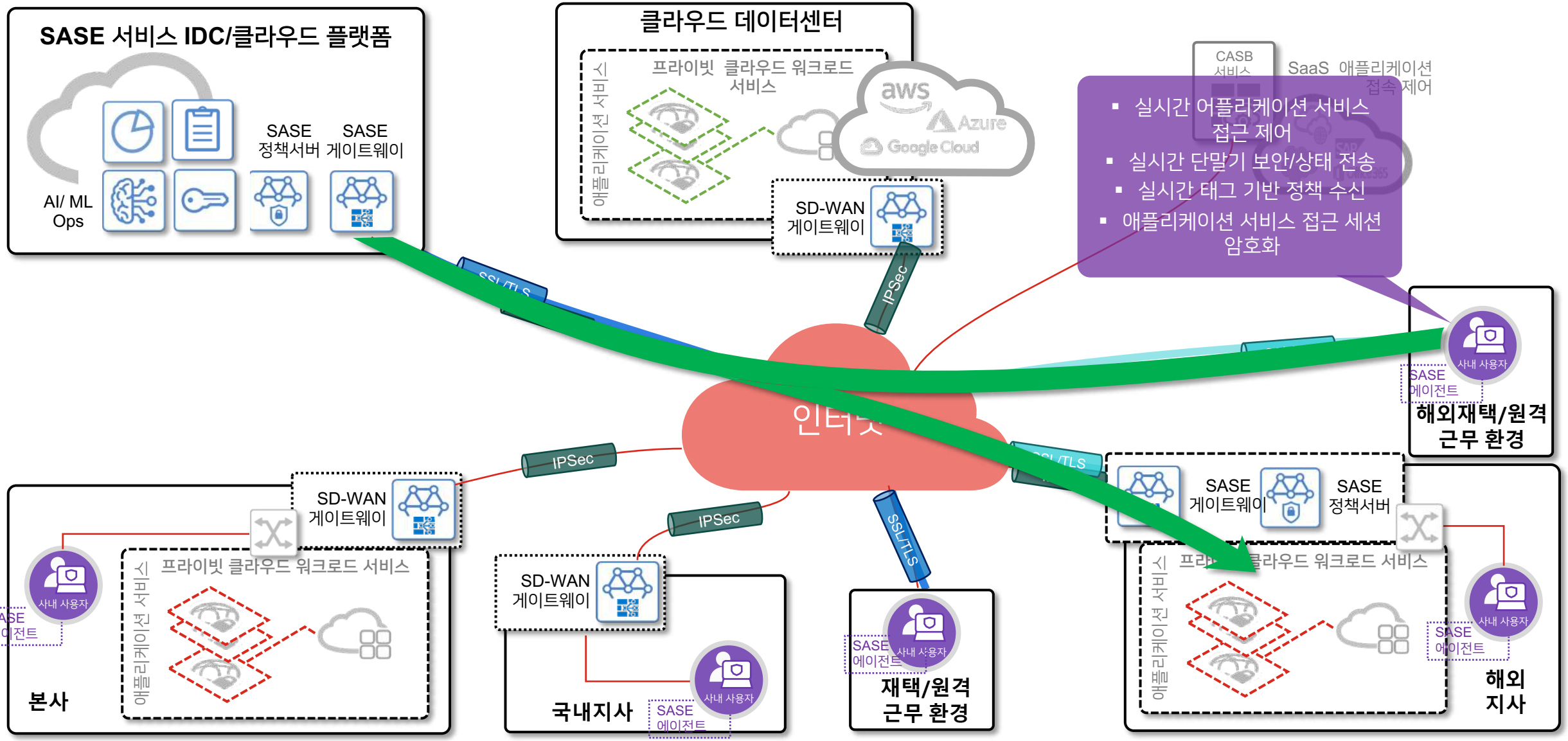
유즈케이스 : 하이브리드



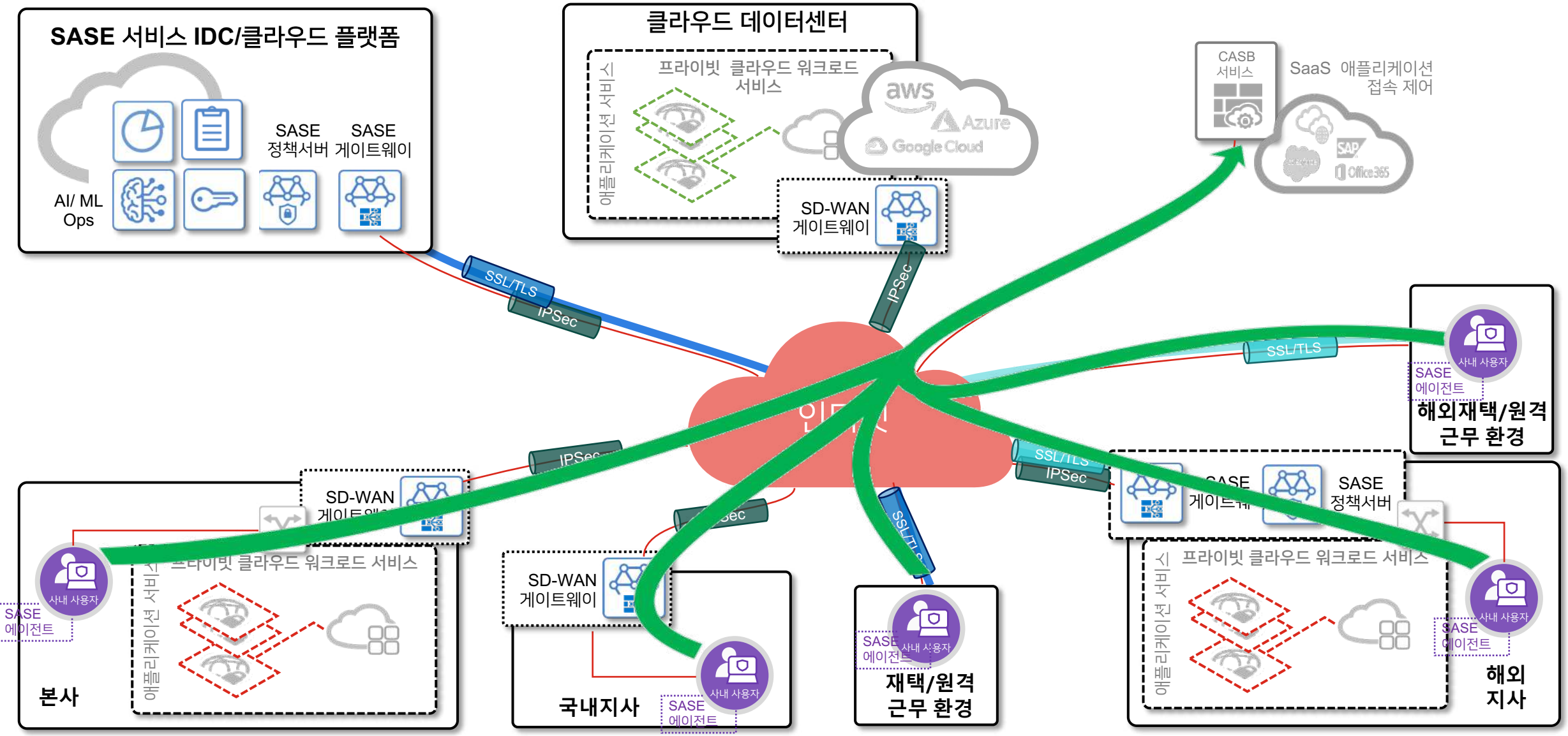
유즈케이스 : 하이브리드



유즈케이스 : 하이브리드



유즈케이스 : 하이브리드



포티넷 자가 SASE 솔루션 주요 기능 요약

구분	항목	포티넷
단일 콘솔 관리	네트워크(FWaaS) 및 소프트웨어 정의 경계(SDP) 제어 전반에서 정책 개발 및 시행을 제어	지원
	세분화된 가시성 및 자세한 로깅 옵션	지원
	세션 기반 모니터링	지원
	역할 기반 액세스 제어	지원
안전한 원격 업무 플로우 및 네트워크 보안	애플리케이션 컨트롤	지원, 사용자 기반 애플리케이션 탐지 지원
	대규모 암호화된 트래픽 검사	지원
	위협 방지 (IPS, AV, Virus Outbreak Prevention, APT)	지원
	웹-필터	지원
	DLP (파일 필터 포함)	지원
	단말기 취약점 분석	지원
	시큐어 SD-WAN	지원 (시큐어 SD-WAN)
Zero Trust Network Access*	다양한 OS 지원	Windows, Linux, Mac OS, iOS & Android
	위치에 관계없이 네트워크 전반에 대한 일관된 앤드포인트 정책 적용	지원 : 로컬 네트워크 제로 트러스트 제어 포함
	애플리케이션, 사용자 그룹 기반의 정책	지원
	Thin-Edge 지원	지원
	클라우드 및 온프로미스 기반의 자체 IAM 및 MFA 솔루션	제공 (또는 +3rd-party 통합 가능)
	세션/애플리케이션 자동 보안 터널	지원
	사용자/단말기 기반 컴플라이언스 준수 확인	지원
구축 형태		• SaaS 구독형 서비스(FortiSASE) • 온-프레미스 자가 SASE 구축 솔루션 (포티넷 시큐리티 패브릭 솔루션)