원격 접속의 변화
SSL VPN에서 ZTNA을 넘어 SASE로

방화벽/SSE 솔루션 벤더 지사장이 말아주는 ZTNA와 SASE

김 용 / Country Manager

SonicWall Korea

SONICWALL

AGENDA

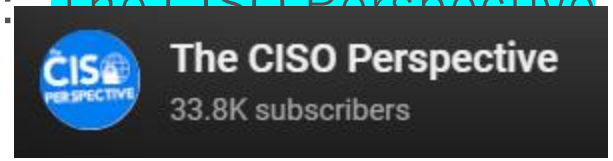
1. 발표자 및 SonicWall소개

2. 최신 보안 용어로 보는 트렌드

3. 기존 SSL VPN의 한계점 및 SSE로의 변화와 필요성

4. 솔루션 예제로 보는 SSE 특장점

>> 자료 참조
- SonicWall Resources
- Youtube Channel : "The CISO Perspective"



SONICWALL OVERVIEW

Boundless Cybersecurity for the Hyper-Distributed Era

FOUNDED 1991 **HEADQUARTERS** Milpitas, California **EMPLOYEES** 1,600+ **WWW.SONICWALL.COM**

~500,000
기업 및 조직을 보호

215+
개 국가 및 테리토리에서

3 백만개+
방화벽을 제공

33+
년 이상 보안에 집중

~300
특허수

17,000+
글로벌 정보보안 파트너수

SONICWALL

2. 최신 용어로 확인하는 보안 트렌드 변화

최신 보안 용어 BINGO

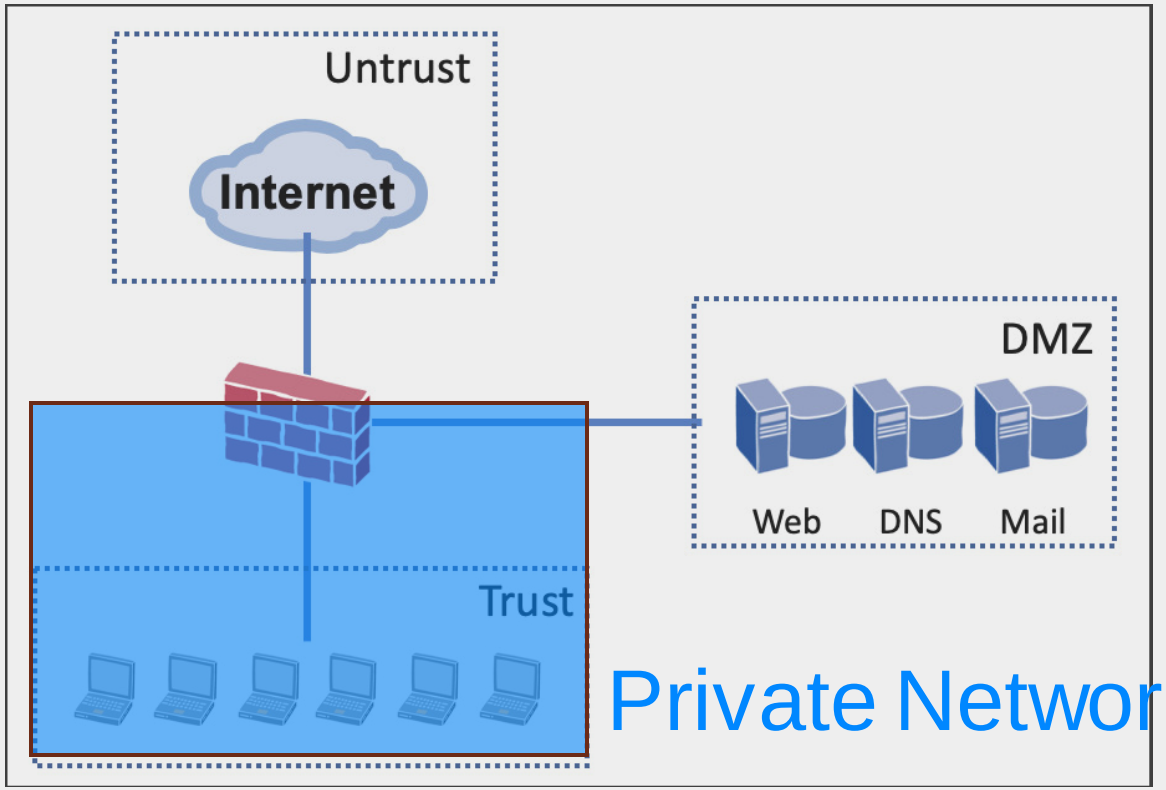
ZT	RBAC	BYOD	NIST	UEBA
VPN	**ZTNA**	SDP	PAM	NAC
SWG	CASB	**SSE**	DLP	RBI
BW	DNS	FWaaS	**SD-WAN**	QoS
POP	CDN	WAF	WIFI	**SASE**

최신 보안 용어 BINGO

ZT	Zero Trust	• 제품이 아니라 보안 모델 • “아무것도 신뢰하지 말고, 항상 검증할 것”
ZTNA	Zero Trust Network Access	• 아이덴티티 중심의 정책 기반 사내 리소스 접근 • 전통적인 VPN 장비를 대체
SSE	Security Service Edge	• 인터넷, SaaS, 사설 리소스에 대한 안전한 접근을 보장 • 클라우드 서비스로 제공됨
SD-WAN	Software Defined Wide Area Networking	• 일반 인터넷과 프라이빗 링크를 통해 엔터프라이즈 네트워크를 연결하고 확장하는 솔루션 • 네트워크 관리를 가상화하여 제공됨
SASE	Secure Access Service Edge	• SSE 보안 및 SD-WAN 네트워킹 기능을 모두 제공하는 솔루션

신뢰형(TRUST) 보안 – "이불 밖은 위험해"

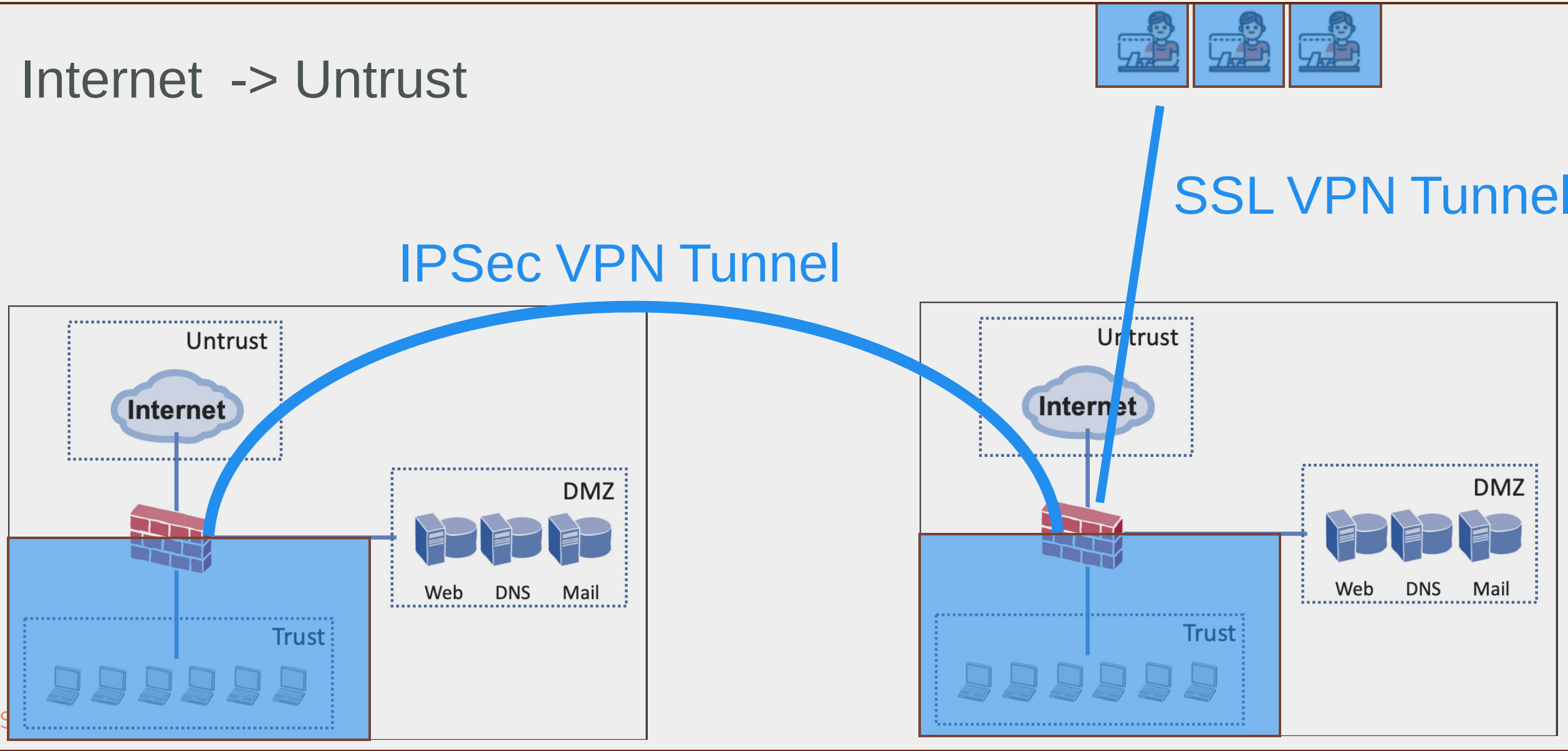
Internet -> Untrust



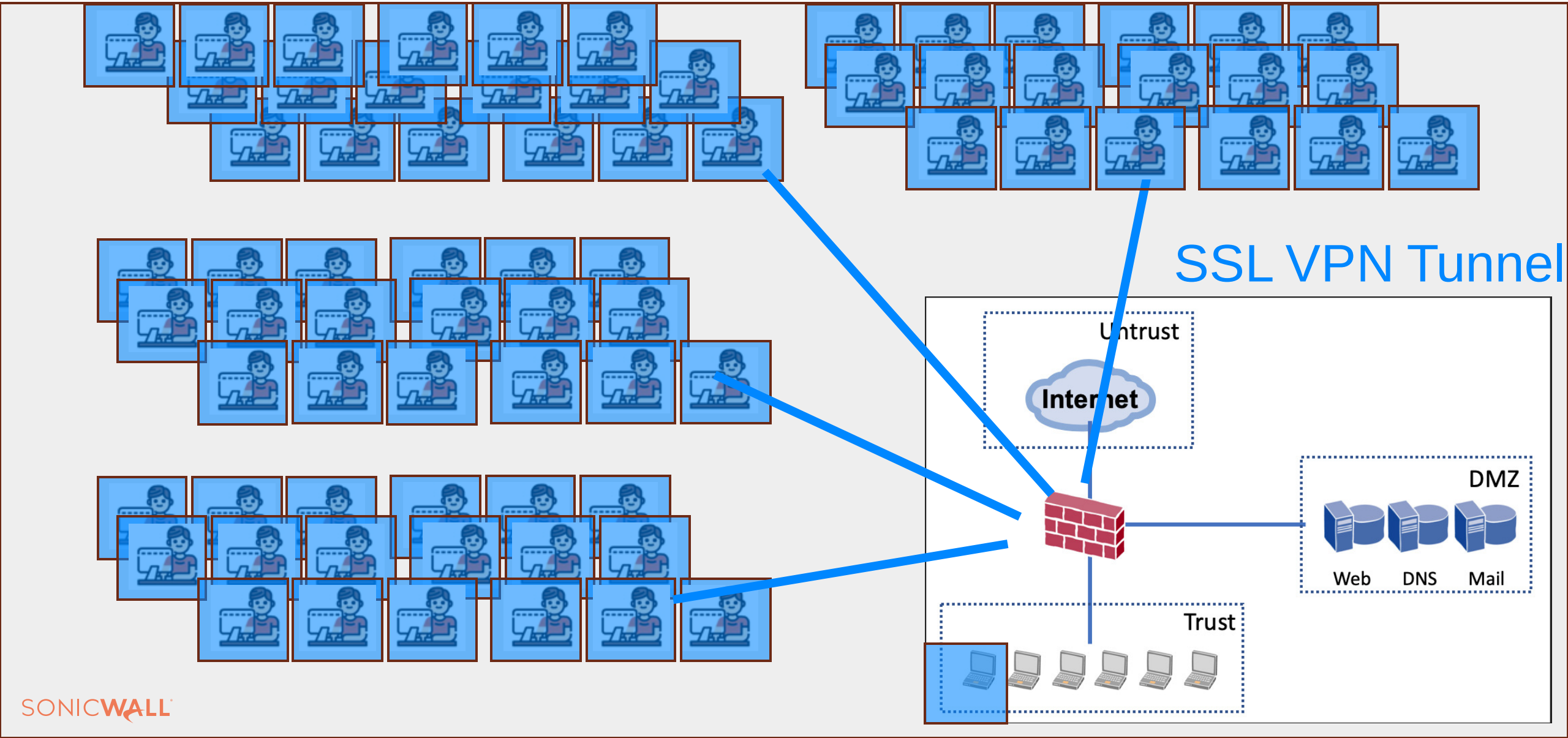
Private Network -> Trust

신뢰형(TRUST) 보안 – "VPN으로 TRUST 확장"

Internet -> Untrust

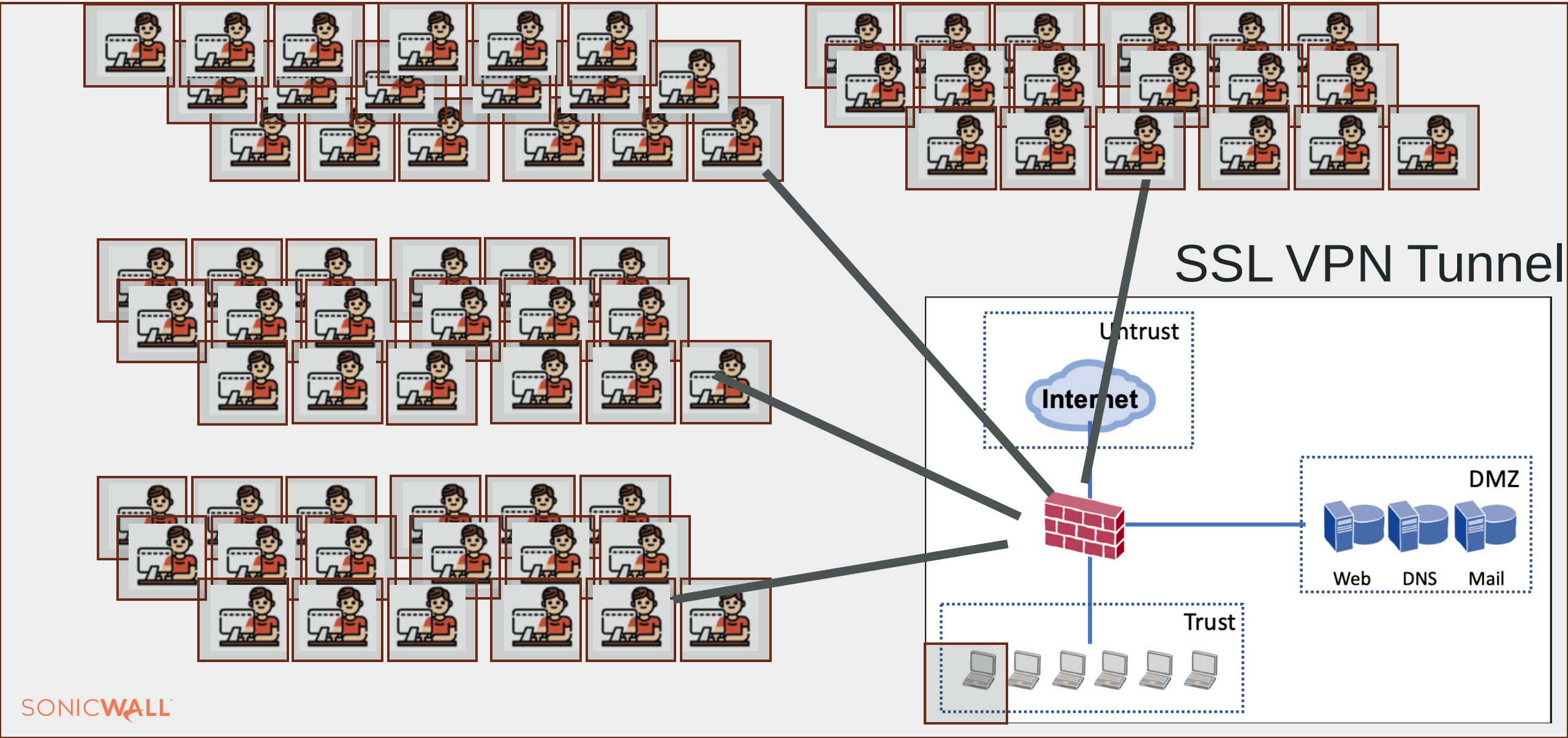


팬데믹- ZERO TRUST의 촉발



SONICWALL

팬데믹- ZERO TRUST의 촉발 : 관리 불가



SONICWALL

기존의 VPN 사용

20년전부터 사용해온 Remote Access VPN (SSL VPN) 접근
모든 업무용 어플리케이션은 전산실 혹은 IDC내 서버에 상주

이 뿐만 아니라, 고려할 많은 보안 이슈

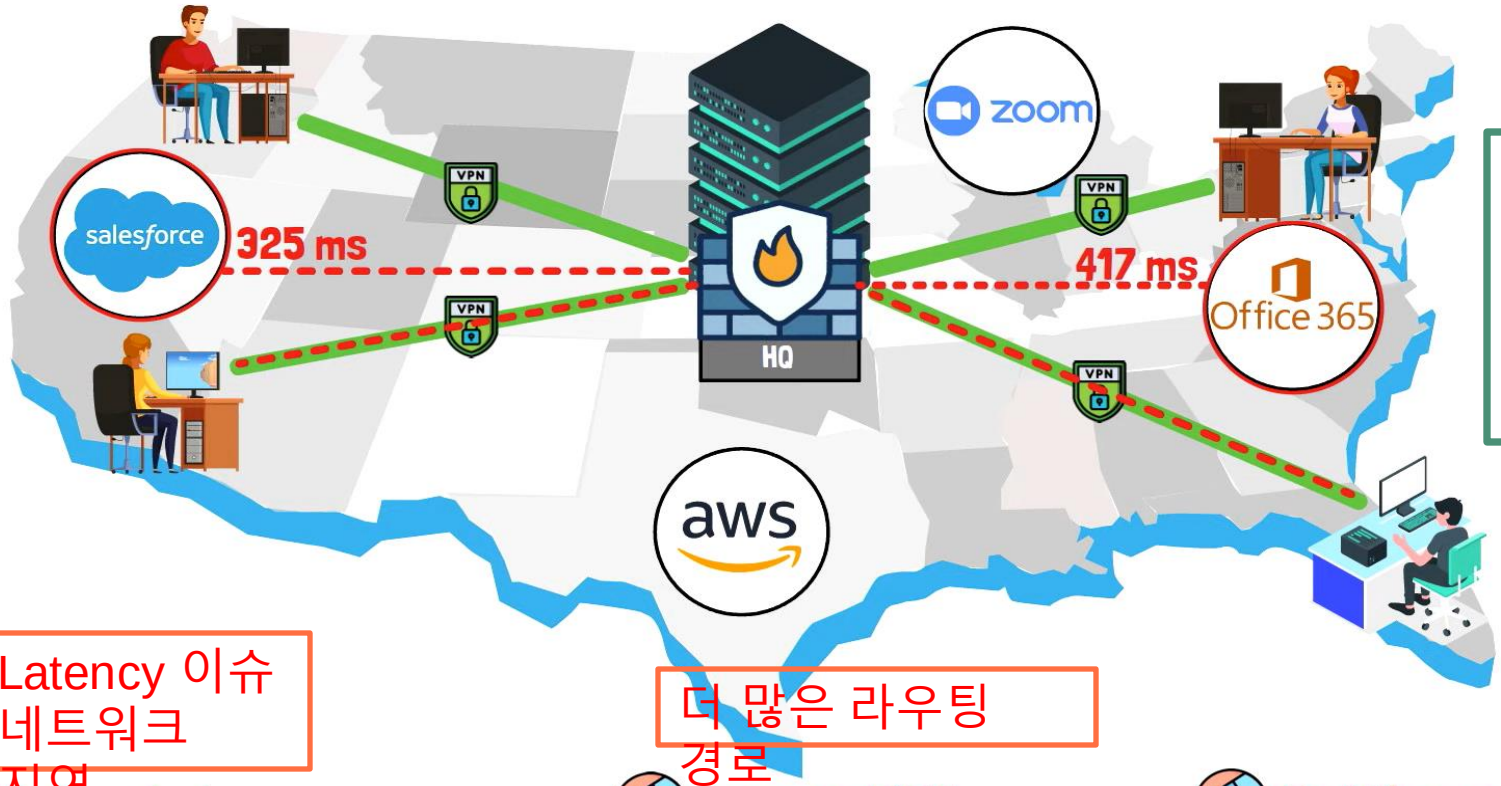
기존의 VPN 사용 문제점

- 접속하고 있는 사용자가 정상 사용자인지 확인 가능?
- 접속하는 PC의 안전성 확보 ?
- 각 접근에 대한 관리?

시대의 변화로 ”1.SaaS 및 IaaS가 보편화”로 중앙 집중식 접근의 문제 발생
더불어 “2. 원격지 사용자 폭발”로 인한 접근 방식에 대한 문제점 확대

연결의 안정성을 확보하지 못하면, 수백/수천개의 백도어?

Traditional VPN



SaaS App의 보편화(1000+)

클라우드에 있는 앱을
본사를 통해 접속하면
속도 등 다양한 이슈 발생

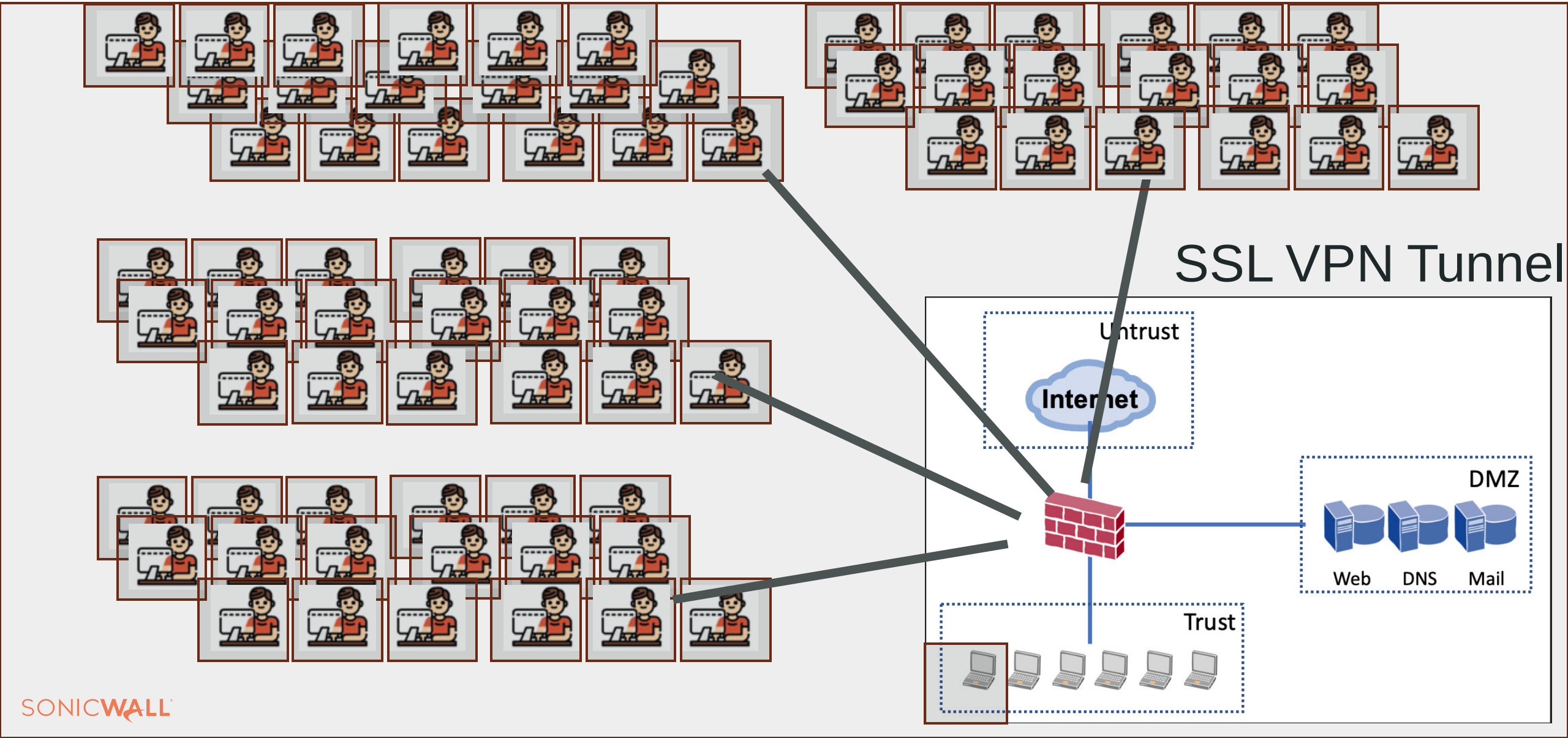
Latency 이슈
네트워크
지연

더 많은 라우팅
경로

병목현상
라우터 / 보안 장비
Capacity
높아지는 회선 비용

Higher Latency **Longer RTT** **Bottlenecks**

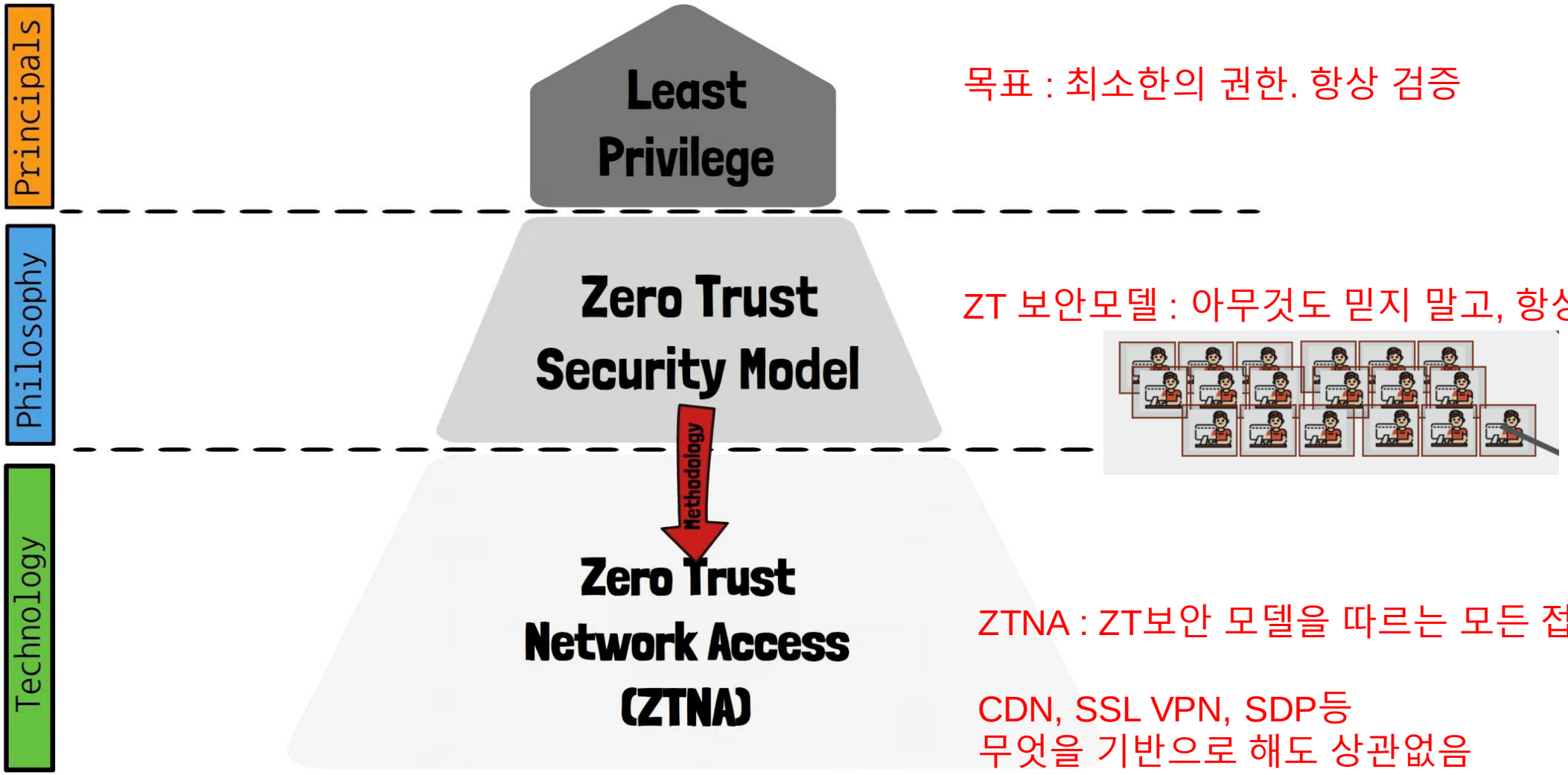
팬데믹- ZERO TRUST의 촉발 : 관리 불가



SONICWALL

ZERO TRUST VS ZERO TRUST NETWORK ACCESS

제로트러스트 컨셉의 재기



목표 : 최소한의 권한. 항상 검증

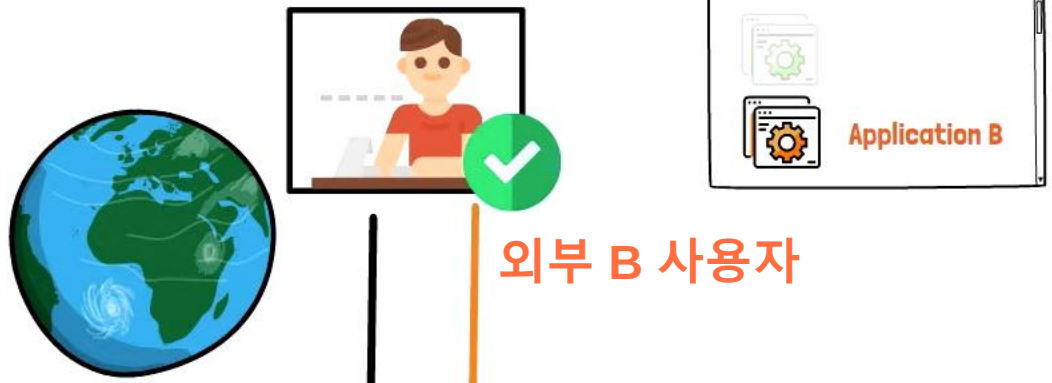
ZT 보안모델 : 아무것도 믿지 말고, 항상 확인 할

ZTNA : ZT보안 모델을 따르는 모든 접근 기술 총

CDN, SSL VPN, SDP등
무엇을 기반으로 해도 상관없음

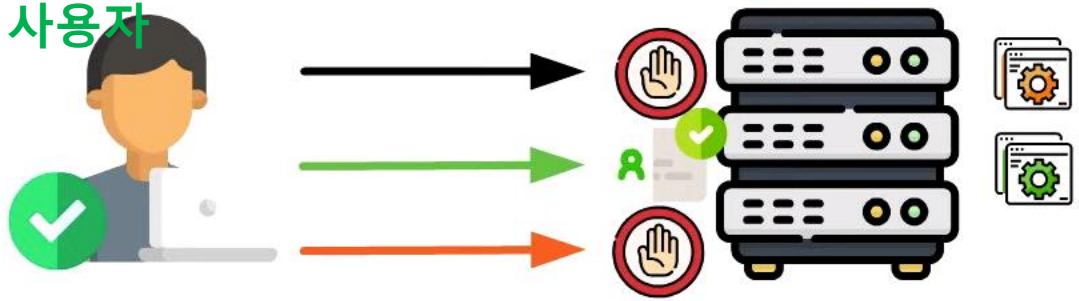
ZTNA

External Network



외부 B 사용자

내부 A
사용자



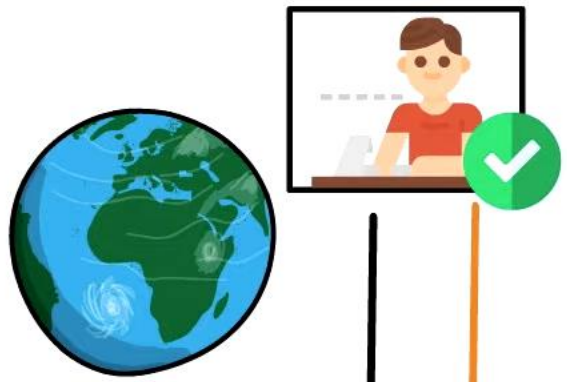
Never Trust; Always Verify

1. Identify
   - ✓ Identification + Authe
2. Context
   - ✓ Least Privilege
3. Security
   - ✓ Machine Secure?

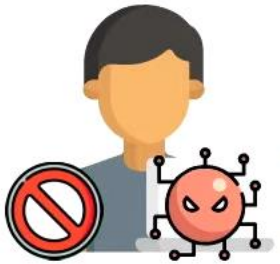
Internal Network

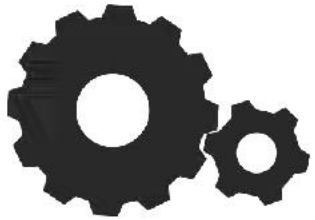
ZTNA

External Network



Internal Network





Never Trust; Always Verify

1. Identify
   - ✓ Identification + Authe
2. Context
   - ✓ Least Privilege
3. Security
   - ✓ Machine Secure?

SSE 출현

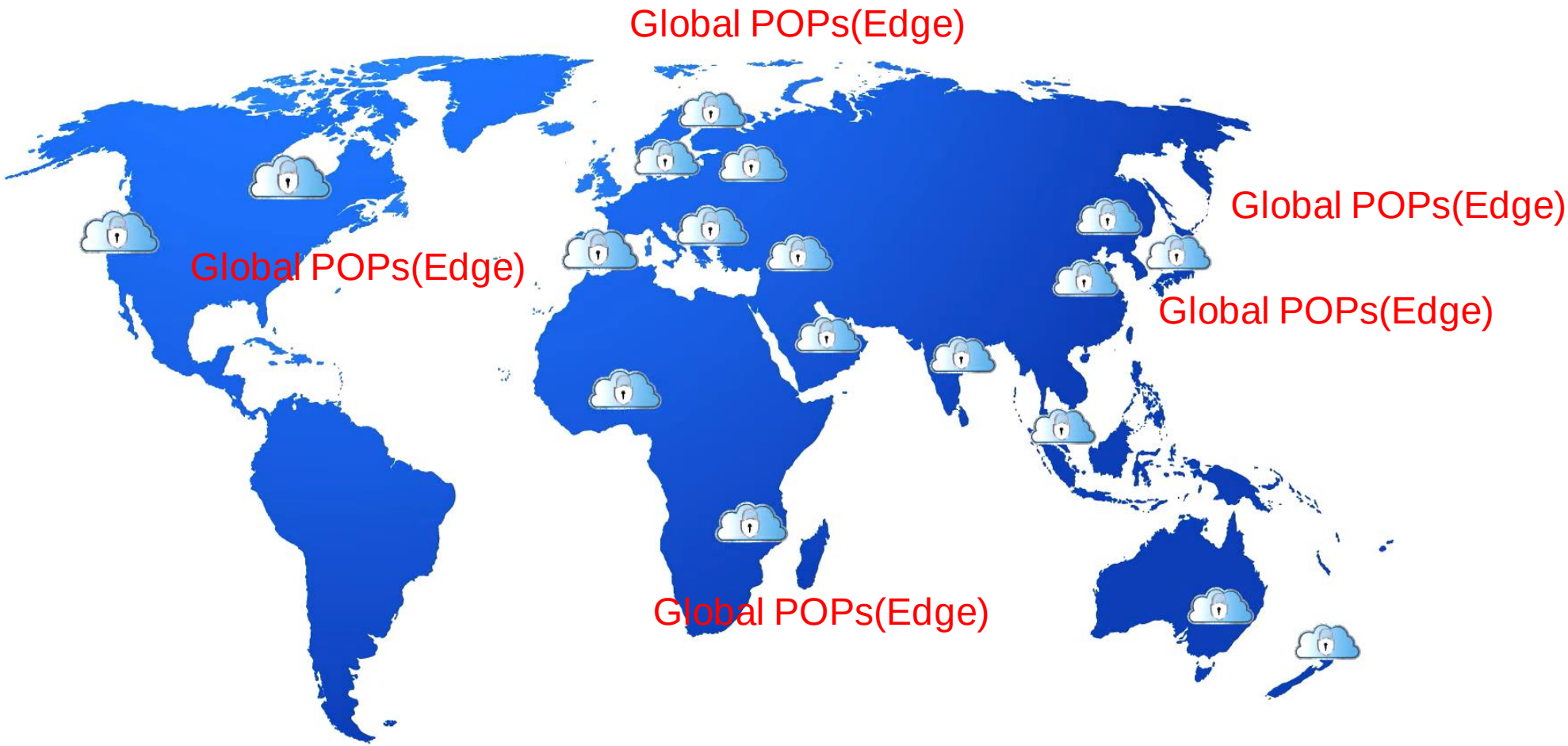
SSE

Security
Service Edge

- 인터넷, SaaS, 사설 리소스에 대한 안전한 접근을 보장
- 클라우드 서비스로 제공됨

SSE 출현 – CDN에서 모티브?

CDN(Contents Delivery Network)의 Edge 네트워크 아키텍쳐 예시
자체 망 생성으로 인한 퀄리티 보장. 기존 네트워크(Underlayer) 위에 자기만의 네트워크 생성(OverLayer)하는 대표적인 서비스



SSE 출현

SSE는 “CDN의 Edge 네트워크” + “Security”?

본사가 아닌,
가장 가까운 Cloud POP(Edge) 접속

SSE 출현

SSE는 “CDN의 Edge 네트워크” + “Security”?

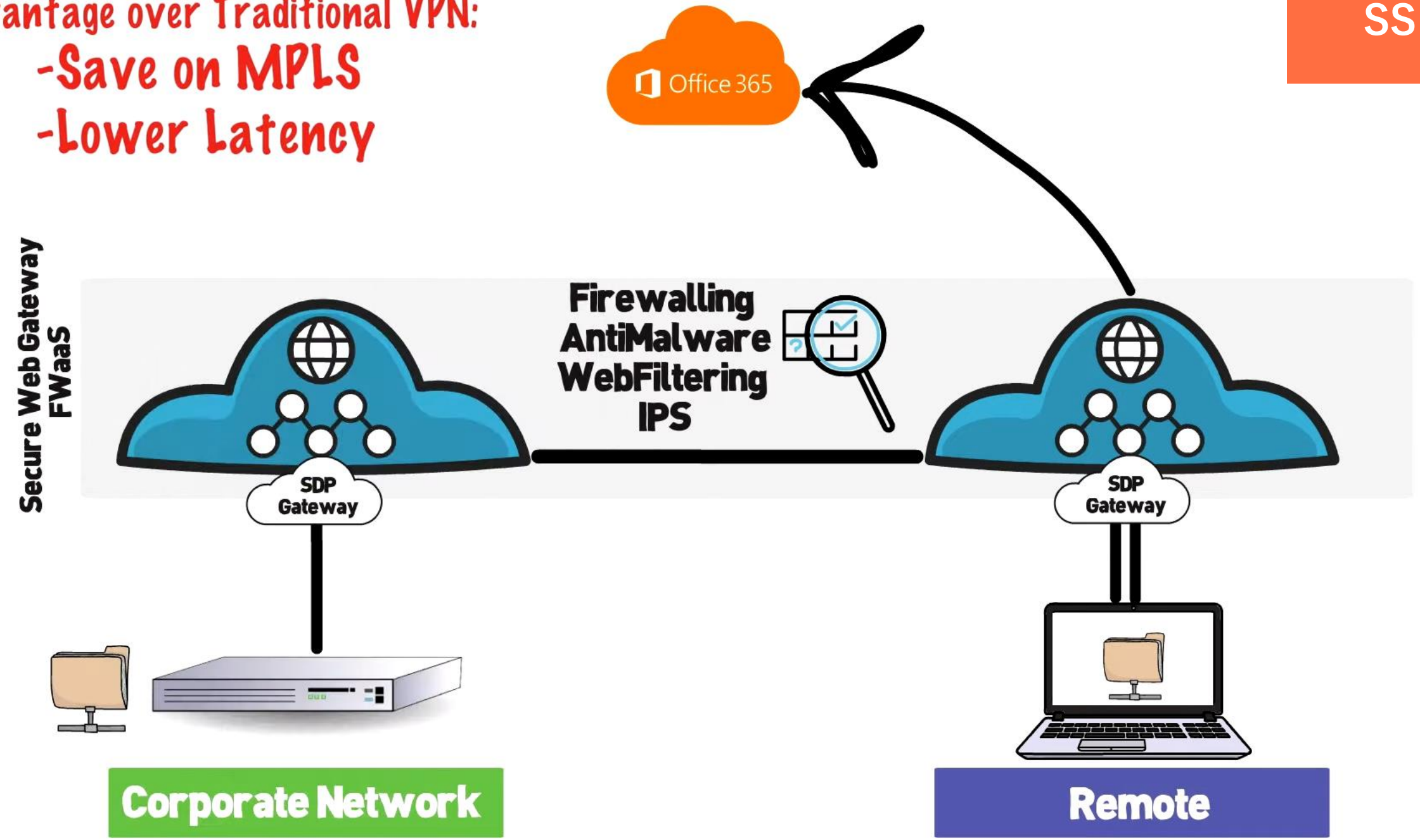
가장 가까운 Cloud POP(Edge)

- 해당 POP이 직접 라우팅
- 해당 POP에서 보안 필터링

SSE

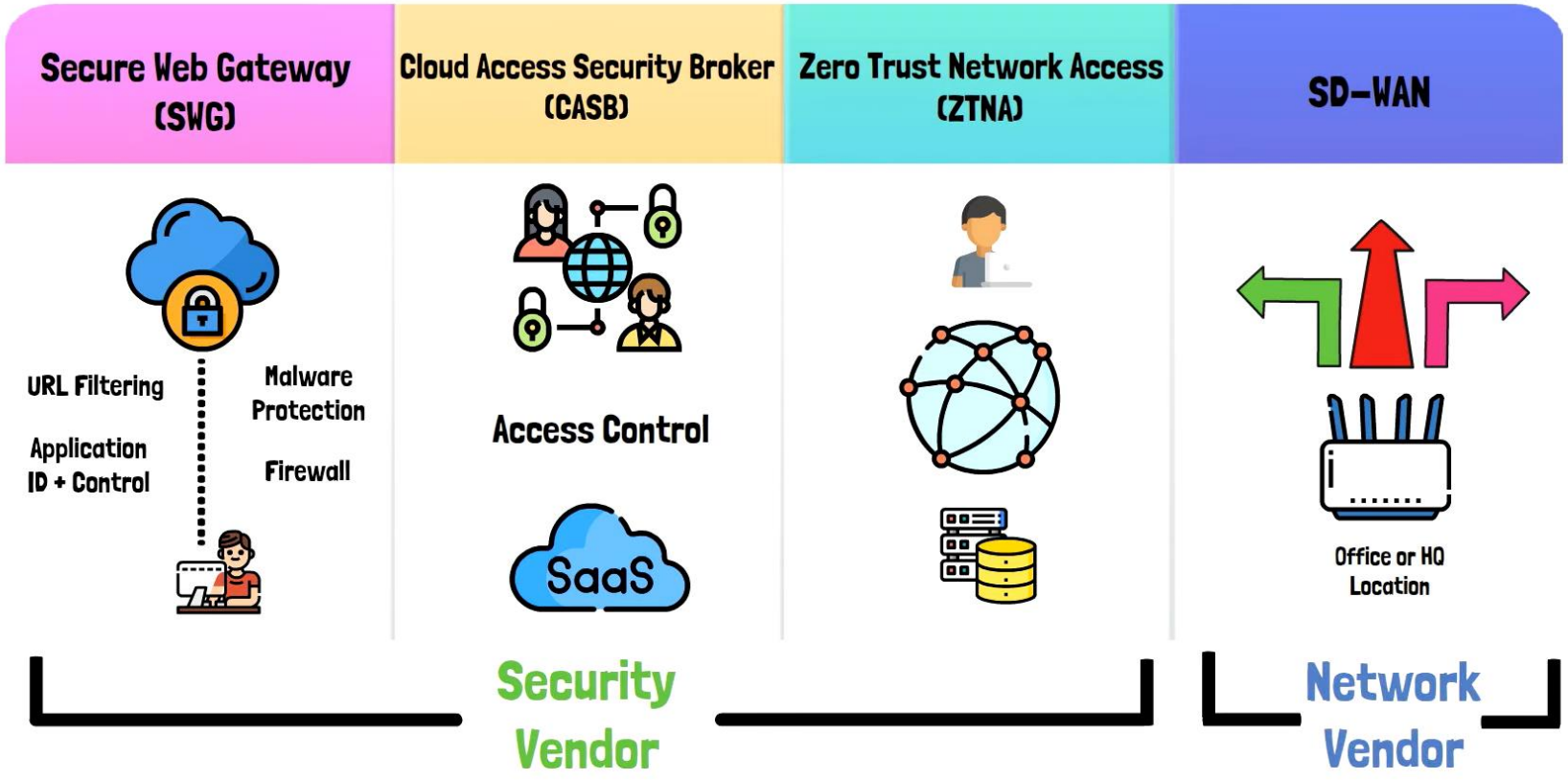
Advantage over Traditional VPN:

- Save on MPLS
- Lower Latency



SASE

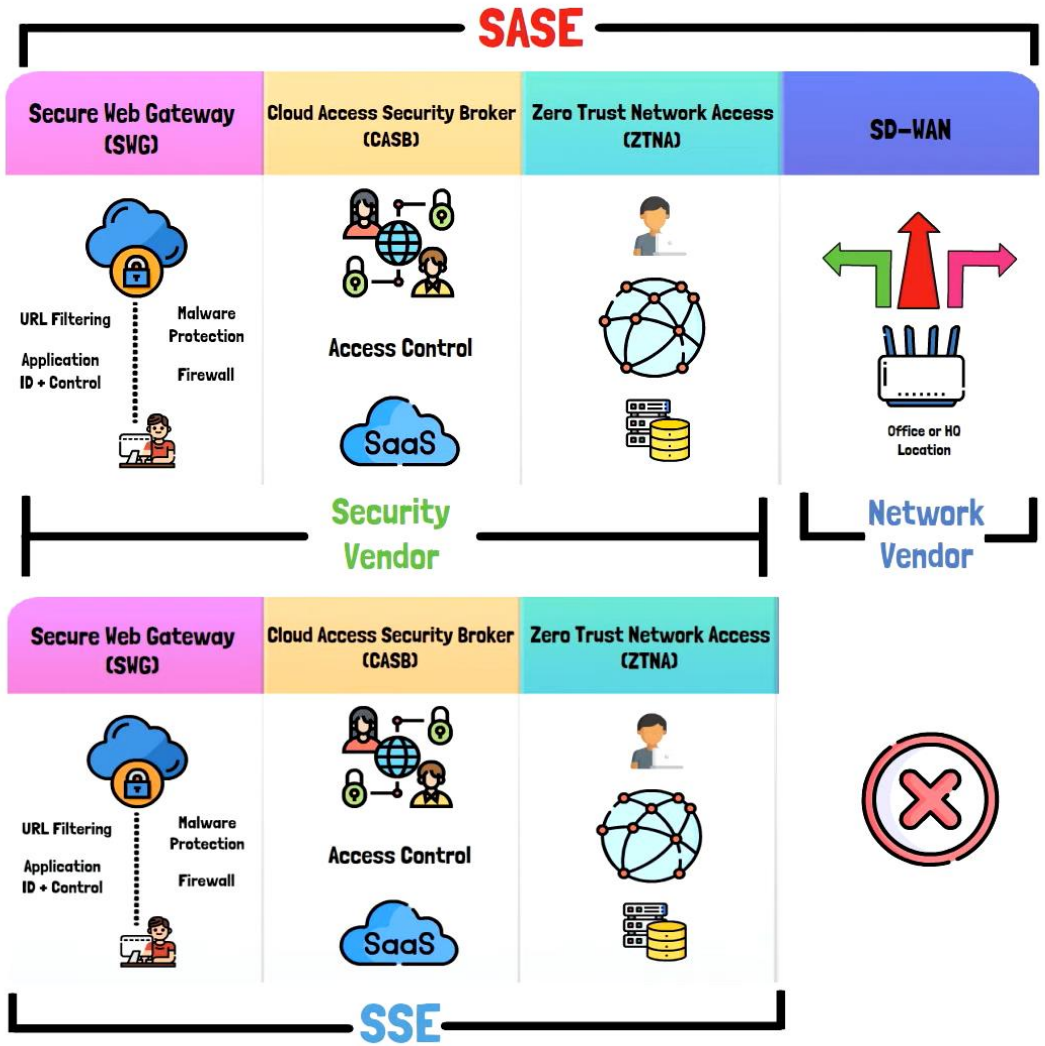
SASE의 구성 요소 - SWG / CASB / ZTNA / SD-WAN



SSE
SASE

SSE / SASE 차이 및 공통사항

SSE = SWG + CASB + ZTNA **SASE** = SSE + SD-WAN



Secure Access Service Edge (SASE)

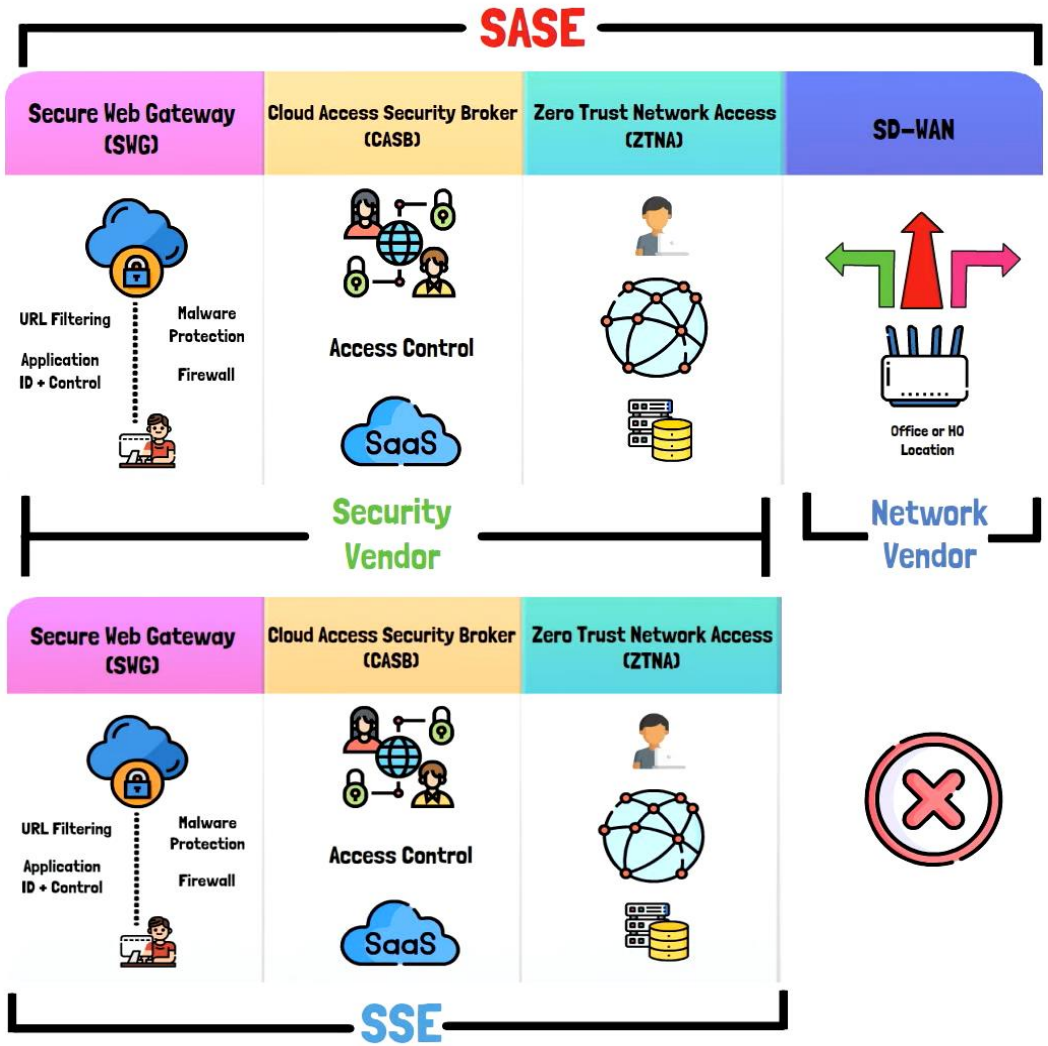
Security Service Edge (SSE)

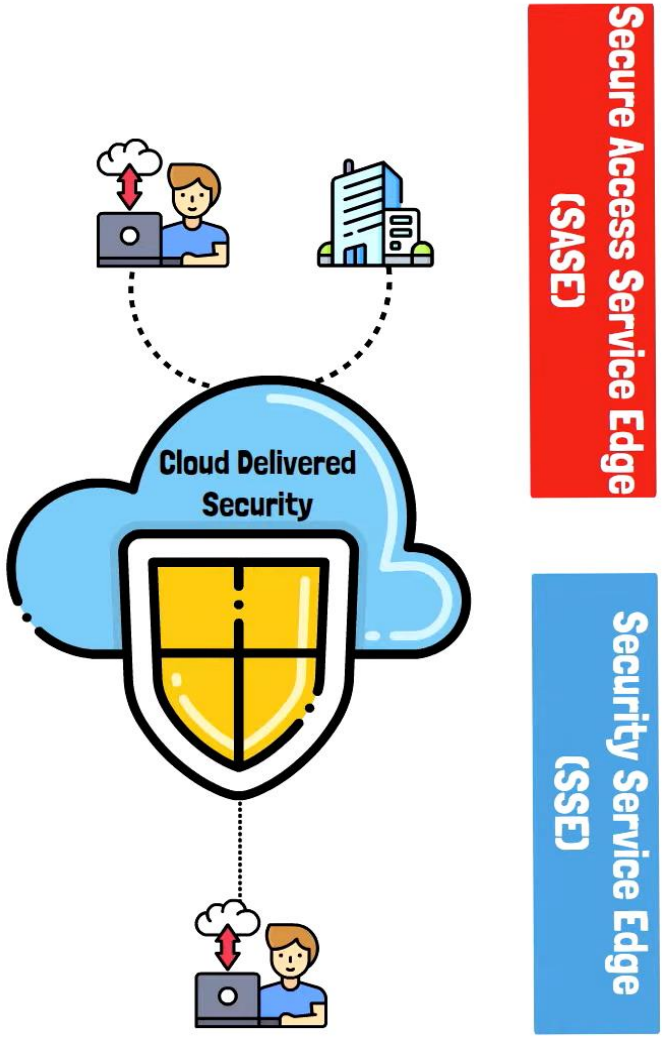
SONICWALL

SSE
SASE

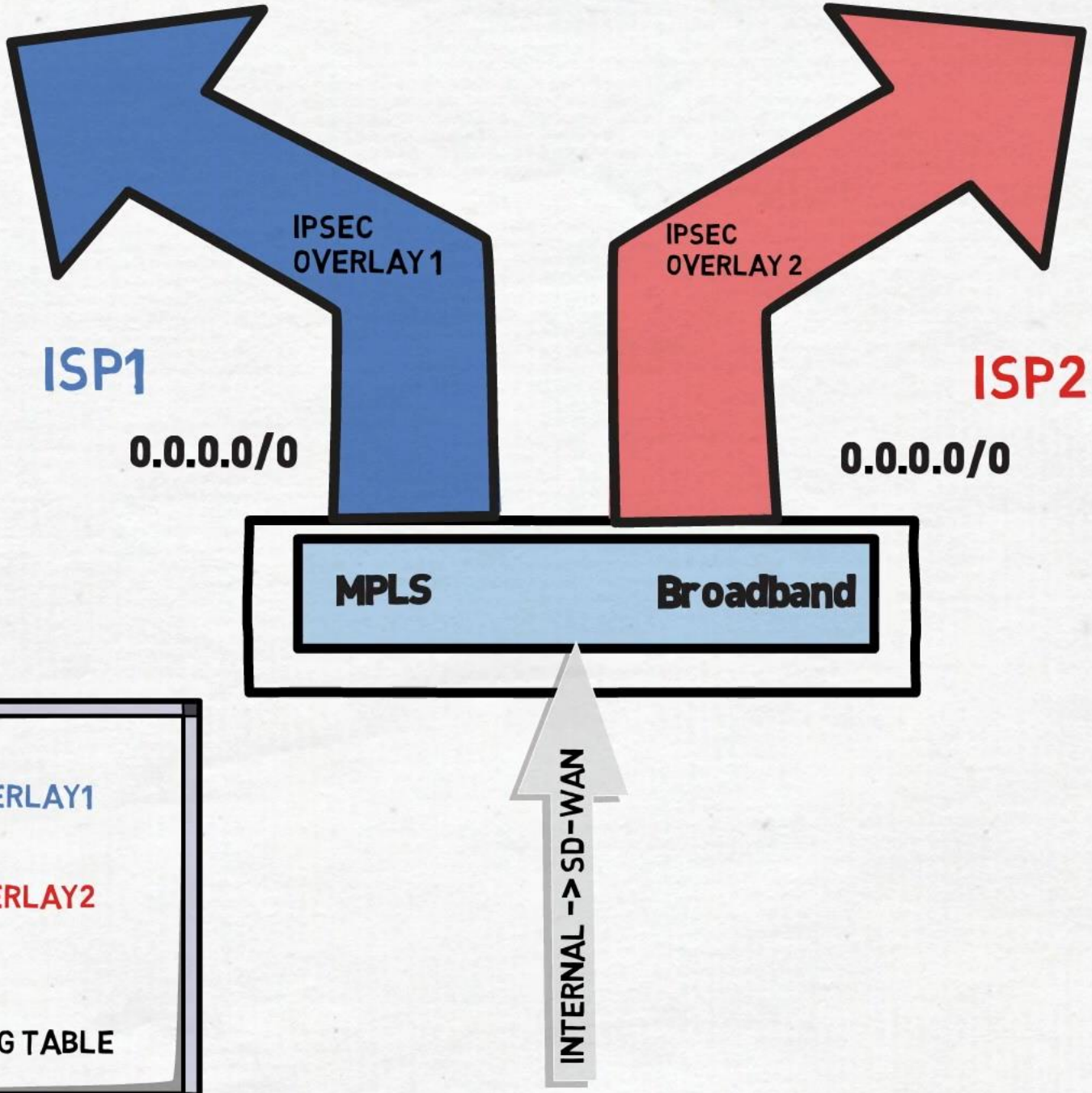
SSE / SASE 차이 및 공통사항

SSE = SWG + CASB + ZTNA **SASE** = SSE + SD-WAN





SD-WAN

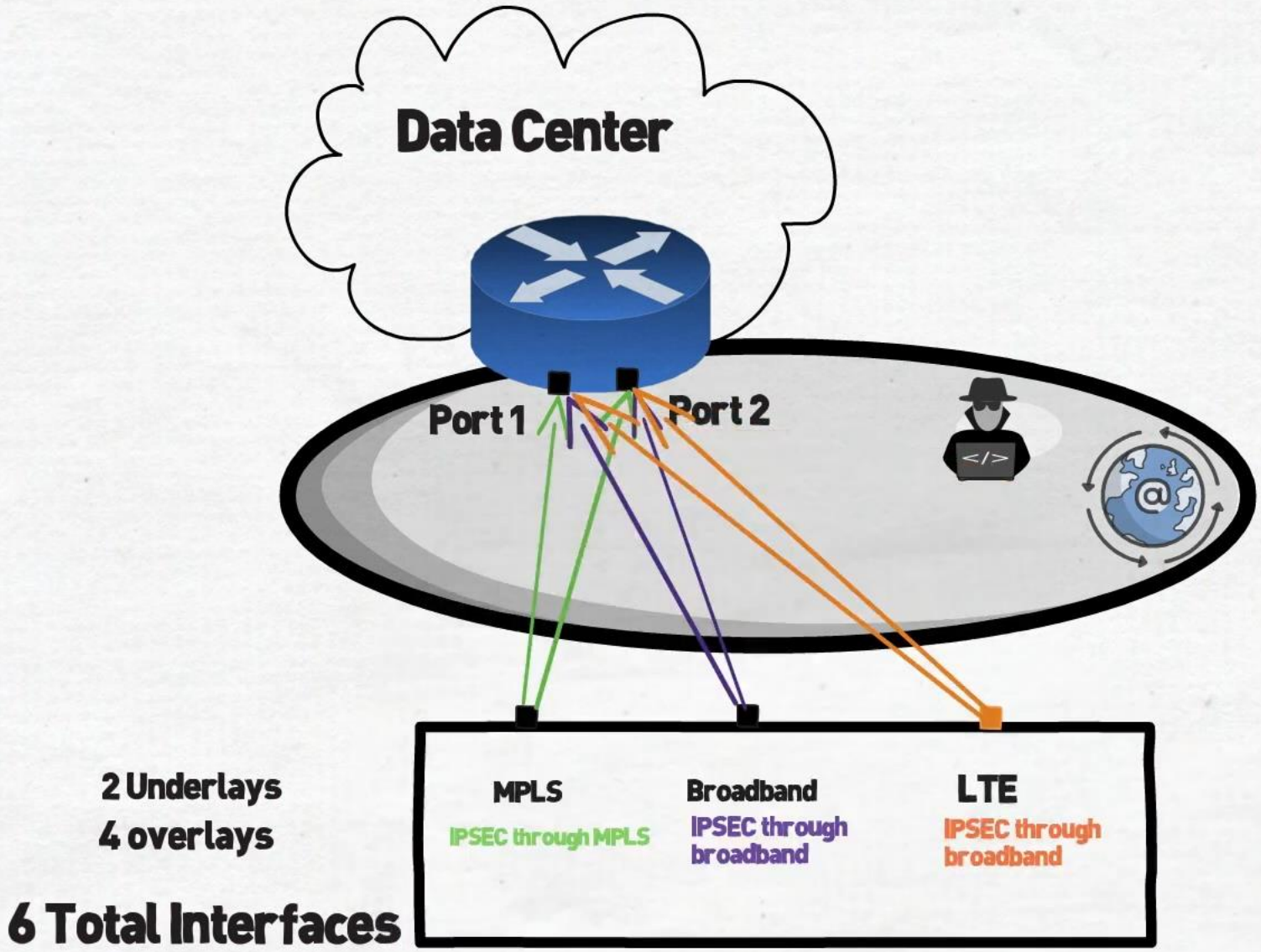


INTERNAL -> IPSEC_OVERLAY1
SLA1

INTERNAL -> IPSEC_OVERLAY2
SLA2

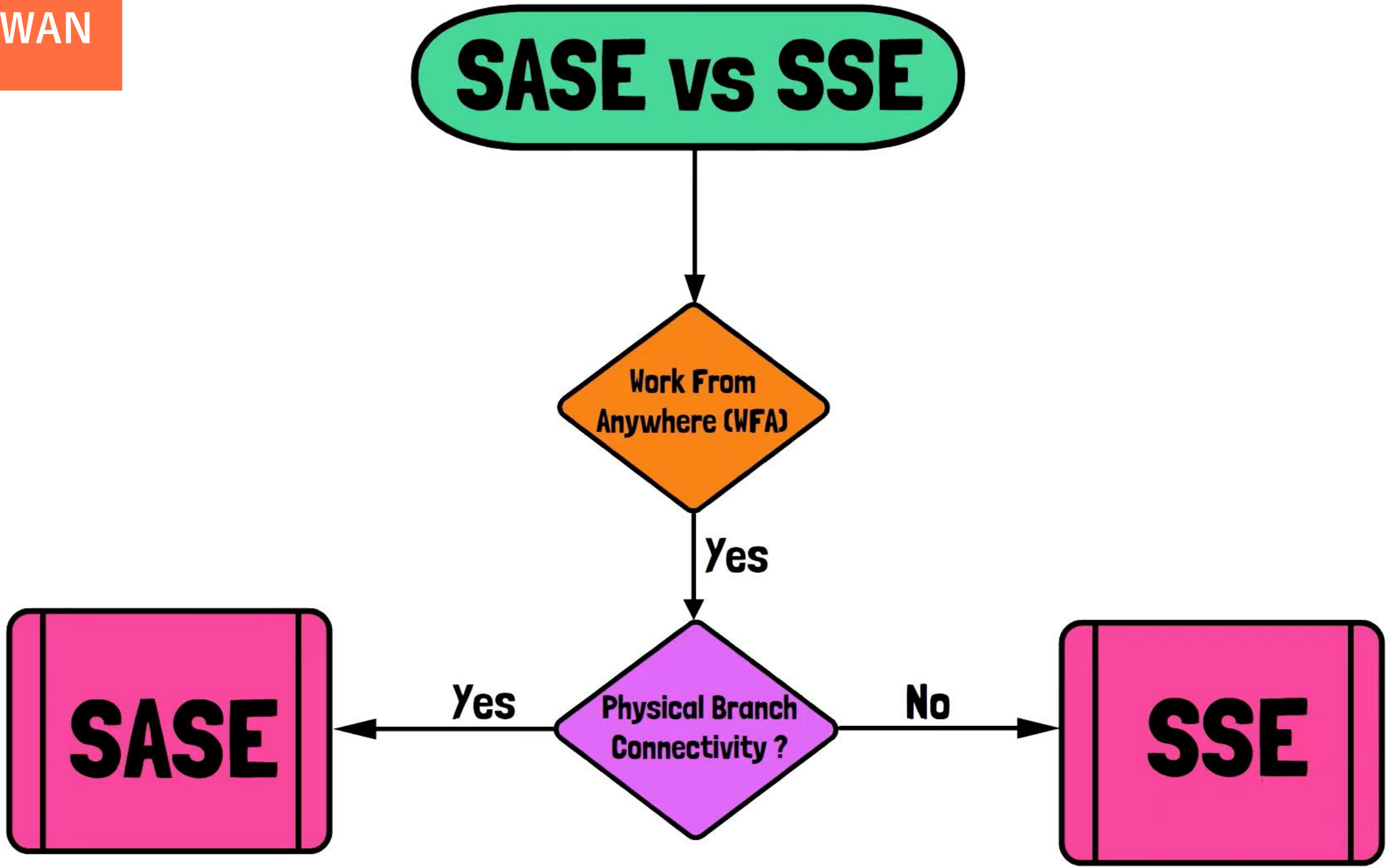
CATCH ALL: USE ROUTING TABLE

SD-WAN



- **Core 요구사항**
  - **Software**
    - Routing
    - App 인지
    - Path 선택
    - VPN 과 L4 FW
  - **Form Factor**
    - Virtual / Physical
    - Edge / Headend
  - **Orchestration**
    - Config
    - Management
    - Visibility
- **Optional 요구사항**
  - Native Advanced Security
  - Cloud Gateway
  - App performance 최적화

SD-WAN


SASE vs SSE
Work From Anywhere (WFA)
Yes
Physical Branch Connectivity ?
Yes
No
SASE
SSE

3. 원격접속이 변화하고 있는 이유

기존 SSL VPN vs SSE/SASE

무심히 해오던 나의 IT, 네트워크, 보안 업무 돌아보기

LEGACY VPN

관리성

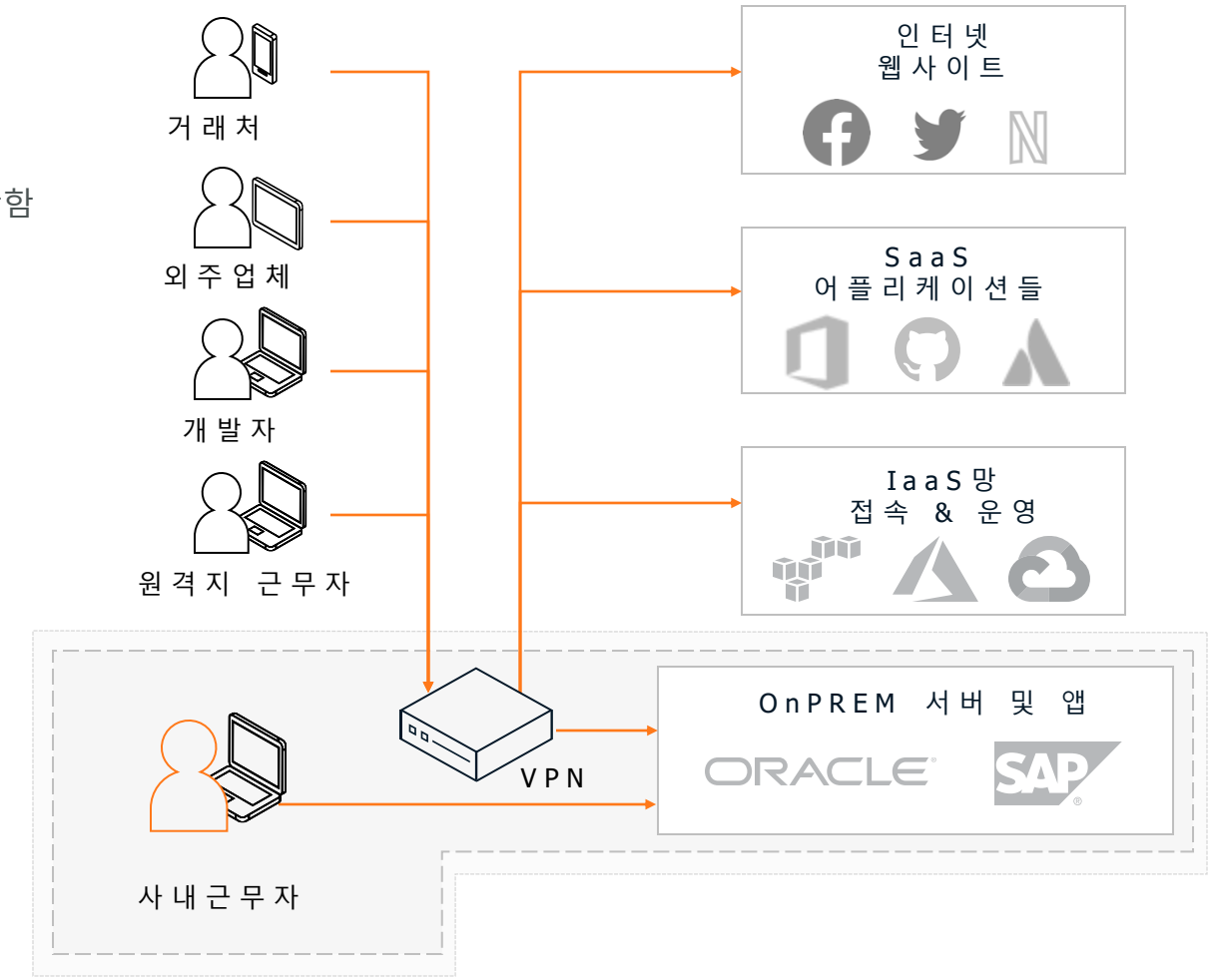
- ✕ HW 및 네트워크 정책 관리가 복잡함 or 지나치게 간단함
- ✕ 실시간 패치 관리의 어려움

사용성

- ✕ 열악하고 신뢰할 수 없는 사용자 경험
- ✕ 느리고 연결이 자주 끊어짐

보안

- ✕ 광범위한 네트워크 접근 및 측면 이동 공격
- ✕ 일회성 인증



SONICWALL

SSE의 시장 요구

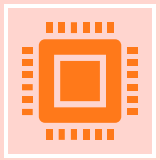
ZTNA를 통해 “기존의 방화벽/VPN을 현대화”하는 경우

외부망 접속 필요시 “인터넷 위협 및 자격 증명 유출 보호”

“고위험도 사용자를 보호”할 경우 - 3rd Parties / BYOD / M&A

SONICWALL

SSE 이점 : 쉽고, 빠르고, 안전한 연결



매우 쉬운 관리

다중 테넌트 관리를 위한 간단한 클라우드 기반 정책

원클릭 배포 및 실시간 업그레이드

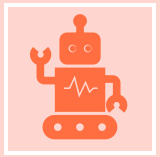
기존 툴과의 쉬운 통합(IDP, EDR, MDM, SIEM)

빠르고, 신뢰성 높은 연결성

더 이상 느리거나 끊어지는 연결 없음

클라우드 처리량과 함께 유연한 확장 가능; 동시 사용자 제한 없음

고가용성의 글로벌 인프라



제로 트러스트 보안

세밀한 접근 제어

지능형 기기 상태 관리

실시간 연속적 정책 시행

SONICWALL

4. 솔루션 예제로 보는 SSE 특장점

SONICWALL CLOUD SECURE EDGE (CSE)

ZTNA

SSE

사용자가 어떤 기기에서도 안전하게 모든 리소스에 접근할 수 있도록 지원합니다.

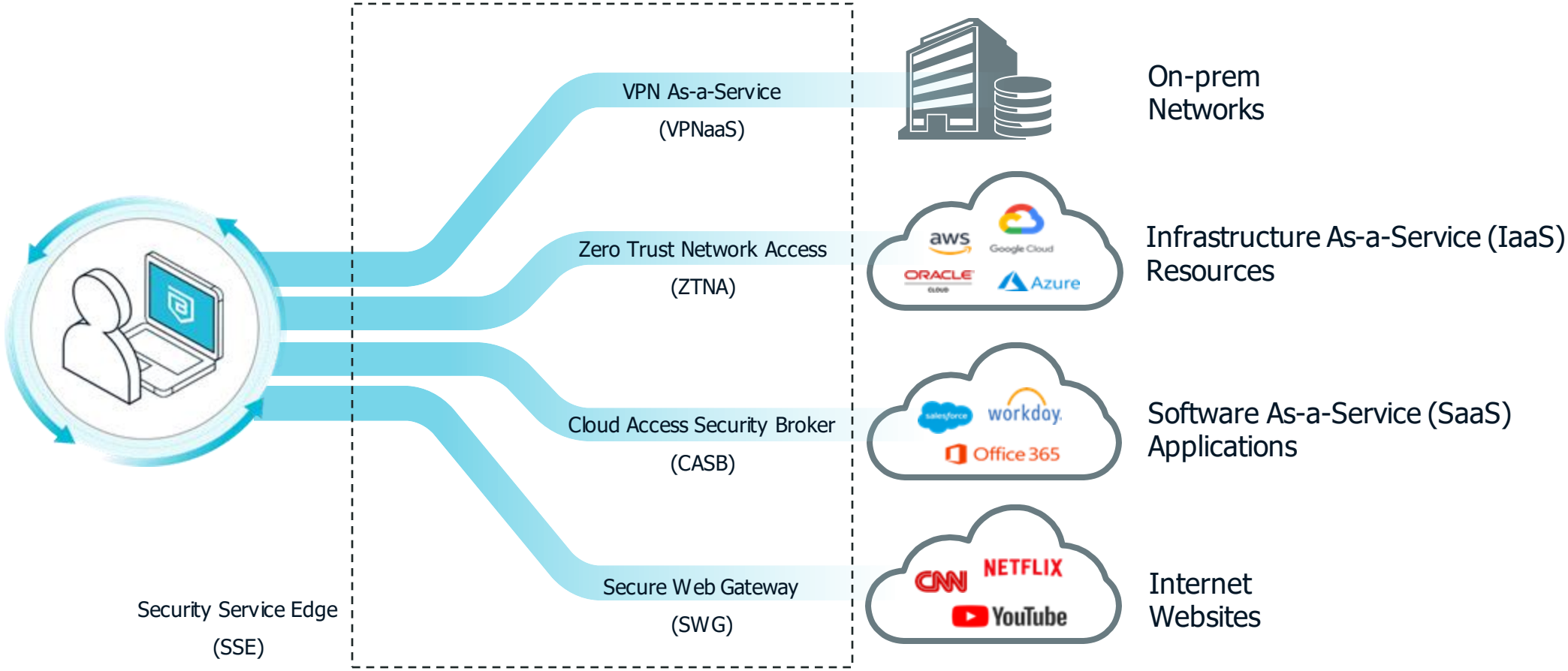
회사의 인적자원의 가장 앞선에서, 차세대 위협의 80%를 우선 예방합니다.

클라우드에서 제공
Cloud Delivered

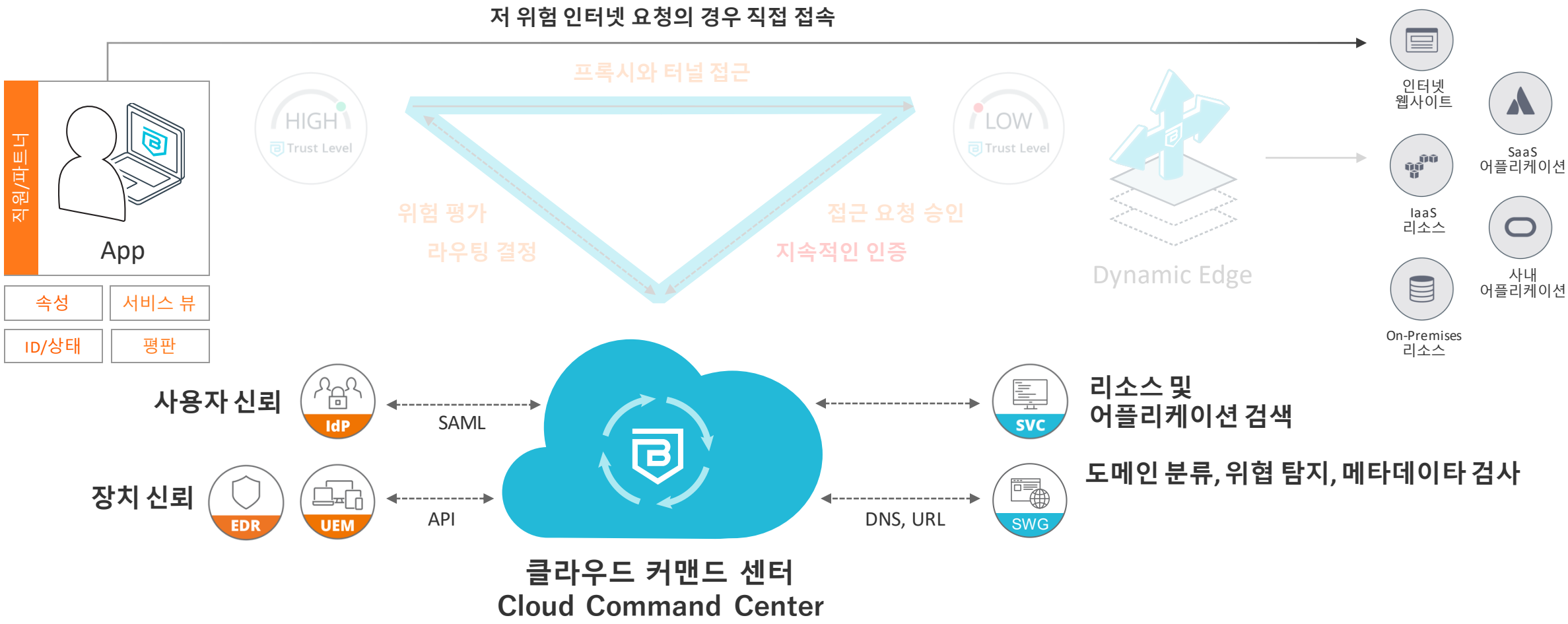
지능형 라우팅
Intelligent Routing

제로트러스트 보안
Zero Trust Security

솔루션: SonicWall Cloud Secure Edge
업계 선도하는 Security Service Edge (SSE)

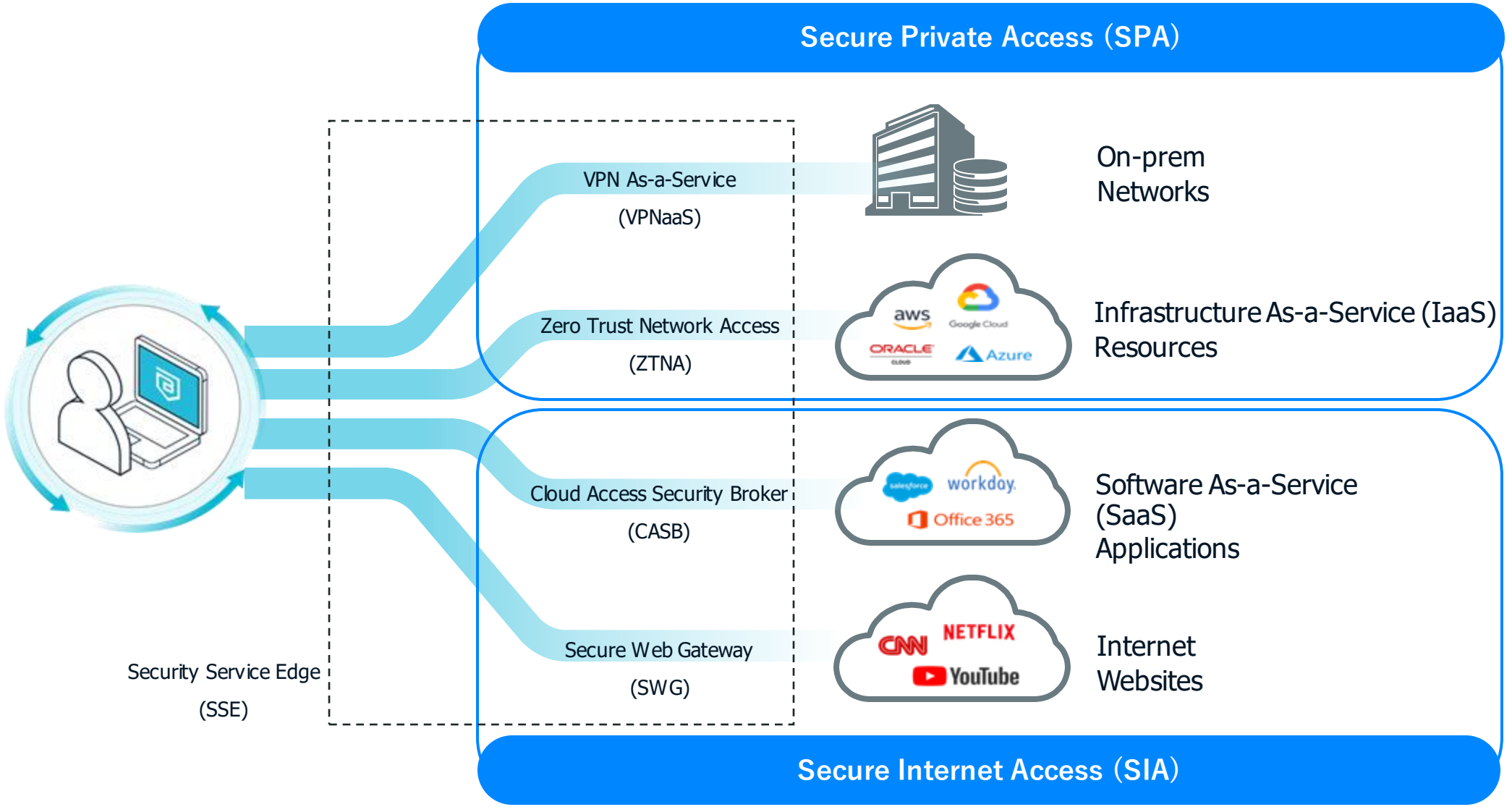


작동 방법 (HOW TO WORK)



SIA와 SPA의 수량을 상이 하게 구매 및 적용 가능
SPA / SIA 를 믹스하여 사용 가능.

접속 방법별 분류



CSE 접속방법별 분류 – 사내 접속 OR 인터넷 접속 보호

SPA
Secure Private Access

SPA Basic
- ZTNA 터널 (VPNaaS)은 우리의 글로벌 엣지를 통해 제공

SPA Advanced
- 개인 엣지, ZTNA 프록시, 통합 또는 비밀번호 없는/클라이언트 없는 접근이 필요한 경우

SIA
Secure Internet Access

SIA Basic
- 모든 운영 체제에서 어디서나 디바이스를 보호하는 엔드포인트 기반 DNS 필터링

SIA Advanced
- 클라우드 액세스 보안 브로커, 고급 보안 웹 게이트웨이, EDR/MDM/SIEM 통합이 필요한 경우.

SPA Basic: Dunder Mifflin

SPA Adv: Chic-fil-a

SIA Basic: Remote Work / K-12 CIPA

SIA Adv: A Corporate Bank

CSE 최고수준의 ZTNA를 제공하며, 대규모 배포를 지원합니다.

사용자 편리성

- 클라우드 중심 솔루션 대비 우수한 성능
- Low latency, Always-on, 지능형 라우팅

보안성

- 유저/ 디바이스/ 리소스 기반
  리스크 모델링 통한 지속적인 권한검증
- 기존 보안 솔루션 데이타를
  실시간 평가에 반영 (e.g., EDR)

데이터 보안

- Data Plane을 풀 컨트롤 할수 있는
  Dynamic Edge 기능 제공
- Self-hosted 또는 Vendor-managed

편리한 구성 및 TCO

- 손쉬운 구매 , 배포, 관리 및 사용
- IT Helpdesk 티켓의 감소
- 빠른 사용자/디바이스 온보딩 / 오프보딩

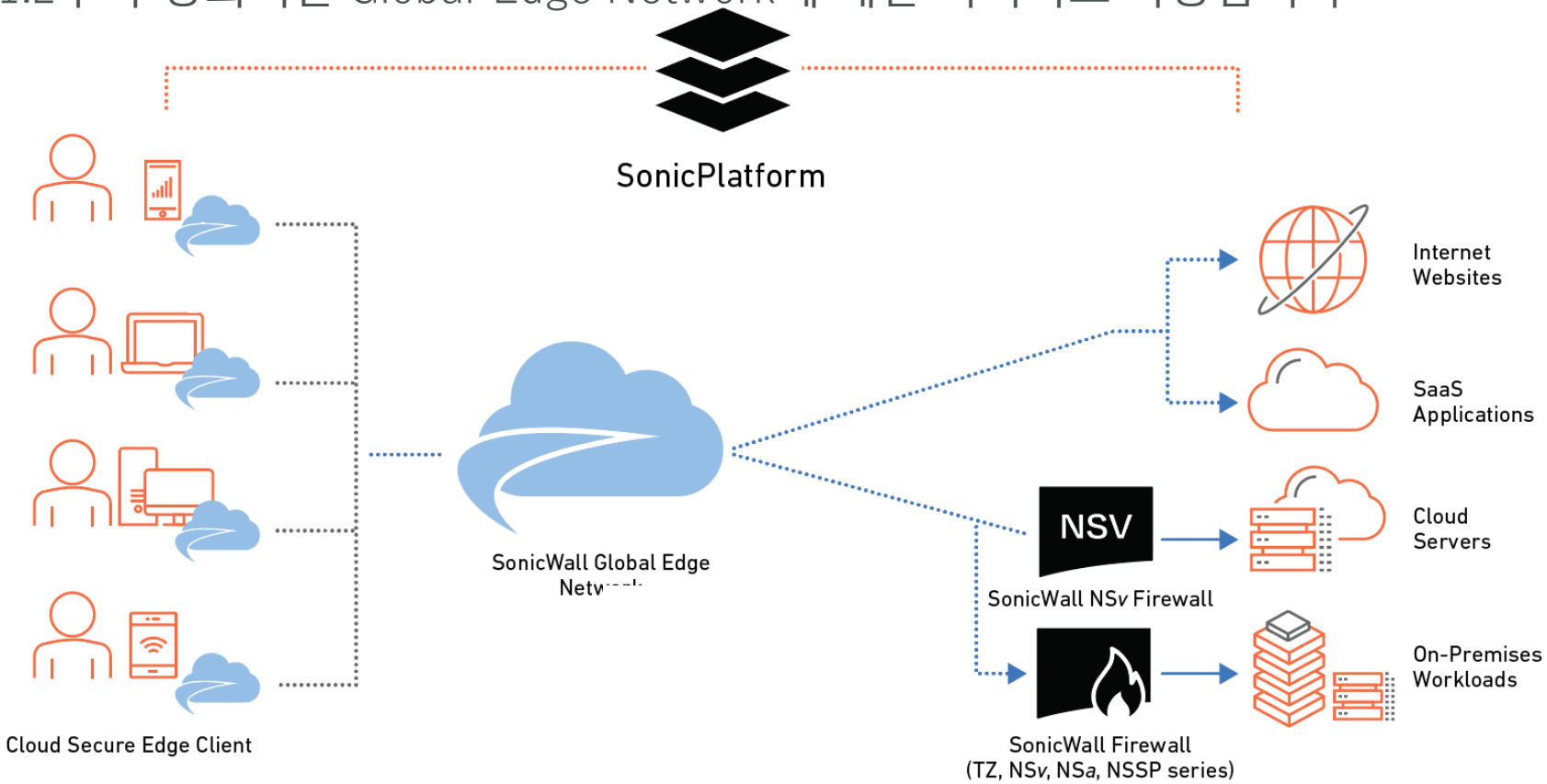
대규모 배포 레퍼런스

Adobe
Lemonade
ORACLE NETSUITE
Chick-fil-A
carta
SAP
STRIKING DISTANCE STUDIOS
COMPASS
talend

소닉월 SSE 특장점

Cloud Secure Edge (CSE)는 조직의 개인 리소스에 접근하기 위한 두 가지 엣지 배포 모델인 **“Self-Hosted Private Edge”(고객사 자체 POP)**와 **“Global Edge”(소닉월 POP) 네트워크**를 제공합니다.

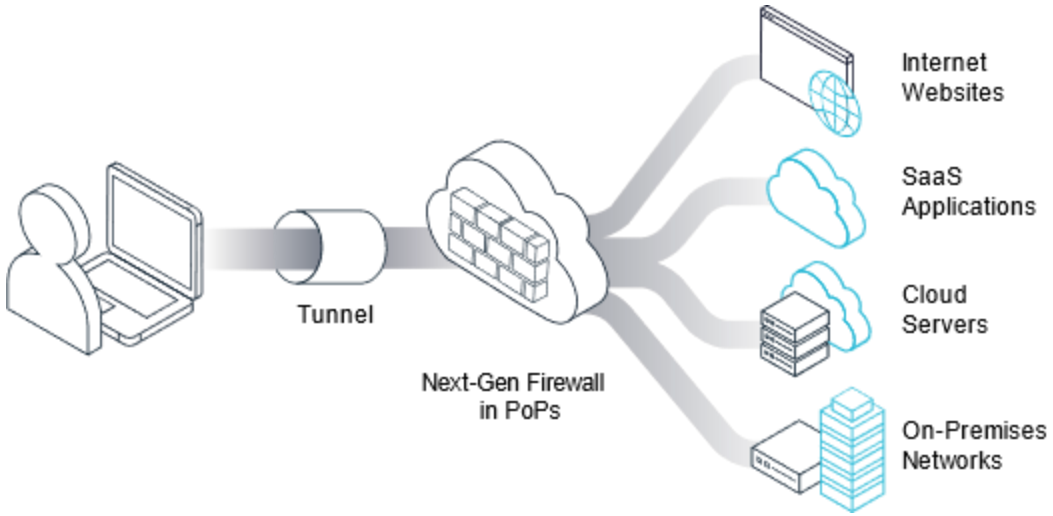
SonicOS 7.1.2부터 방화벽은 Global Edge Network에 대한 커넥터로 작동합니다



소닉월 SSE 특장점

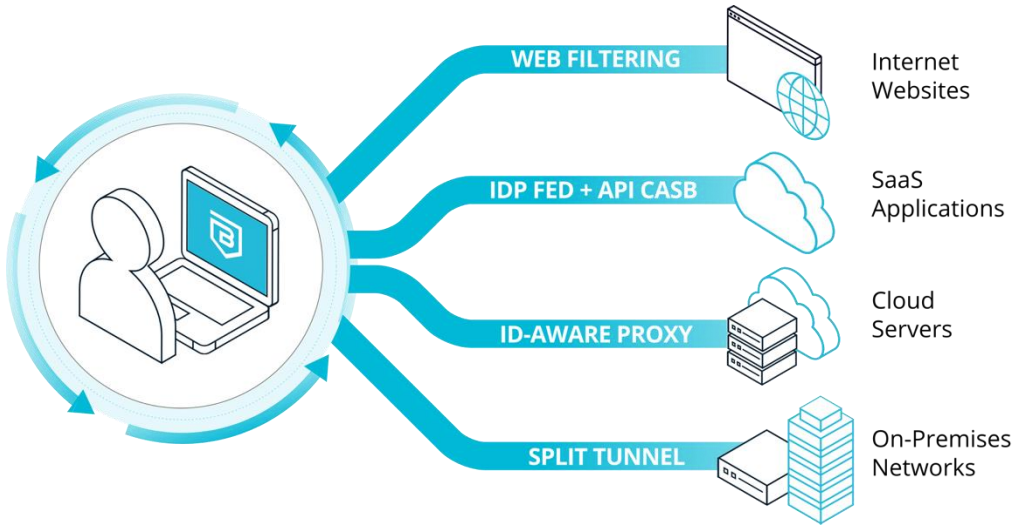
Other Vendors

Tunnel 기반 | 항시 패킷 감지
낮은 퍼포먼스 및 사용자 경험(UX)



Cloud Secure Edge

인텔리전트 라우팅 | 항시 보호, 단 항시 인라인 X
좋은 퍼포먼스 및 사용자 경험 (UX)



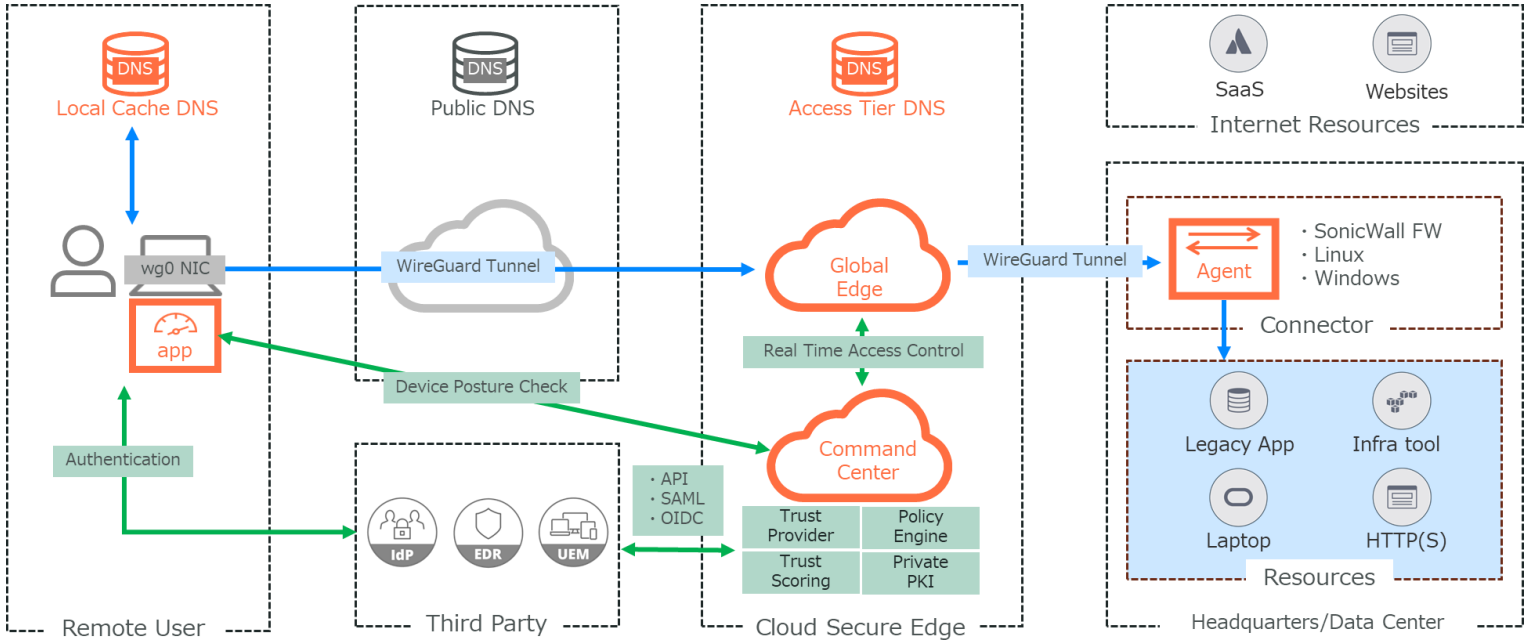
사설 네트워크 접근을 위한 Connector 구성

커넥터는 글로벌 엣지 네트워크와 안전한 터널을 설정하는 다이얼 아웃 커넥터입니다.
커넥터는 내부 서비스에 연결할 수 있는 위치에 배포할 수 있습니다. 각 커넥터는 아웃바운드로만 연결되며, 올바르게 작동하기 위해 어떤 인바운드 포트도 열 필요가 없습니다. 커넥터가 사용될 때, 인터넷의 엔티티에서 액세스 계층으로 트래픽이 흐르고, 그 다음 커넥터를 통해 내부 서비스로 전달됩니다.

참고: 커넥터는 아웃바운드로 인터넷에 연결할 수 있어야 하며, 올바르게 작동하기 위해 인바운드로 열려 있는 포트는 필요하지 않습니다.

커넥터 설치를 지원하는 항목은 아래와 같습니다:

- Tarball (Linux server)
- Docker Container
- Windows Executable
- SonicWall Gen7 Firewall with SonicOS 7.1.2

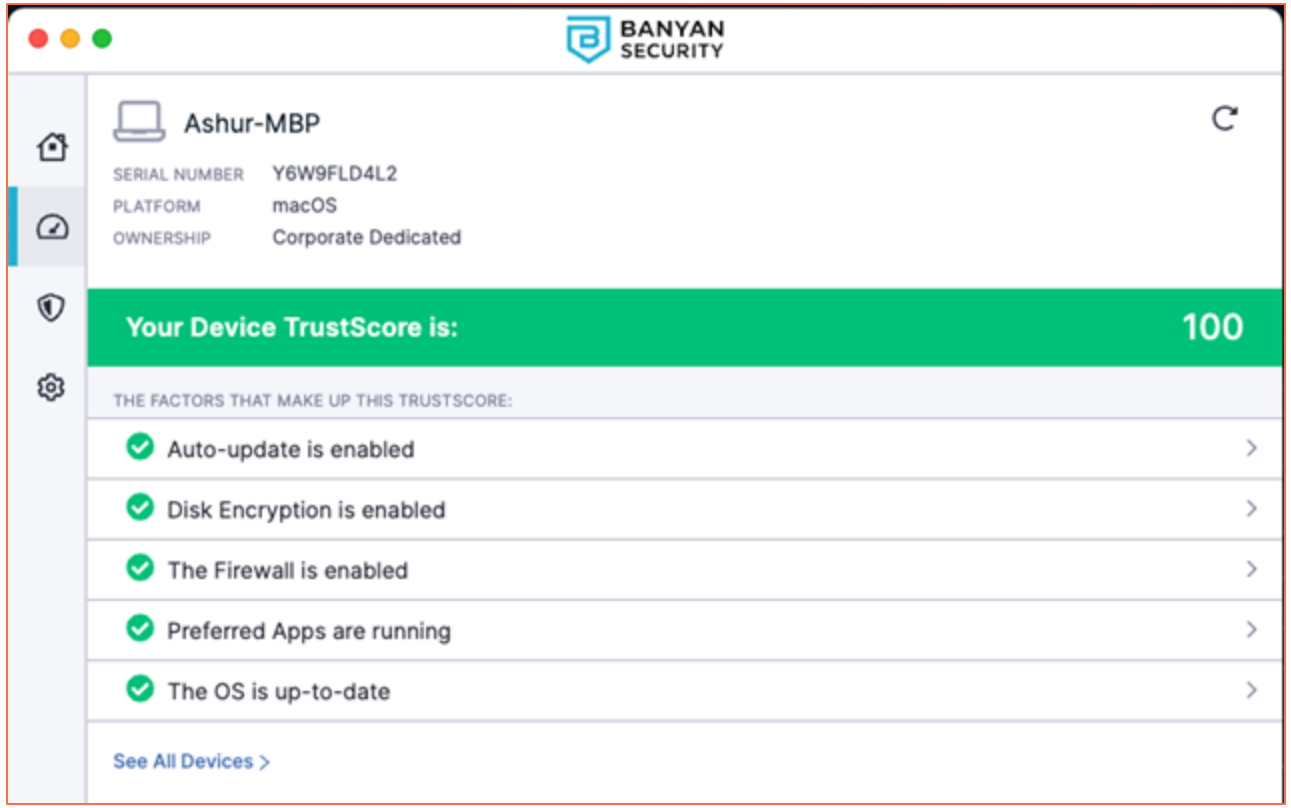


CSE 주요 요소 기능

1. Agent – PC 및 Mobile 용
2. Cloud Command Center
3. Edge – Global 및 Private
4. 그 외 기능 슬라이드

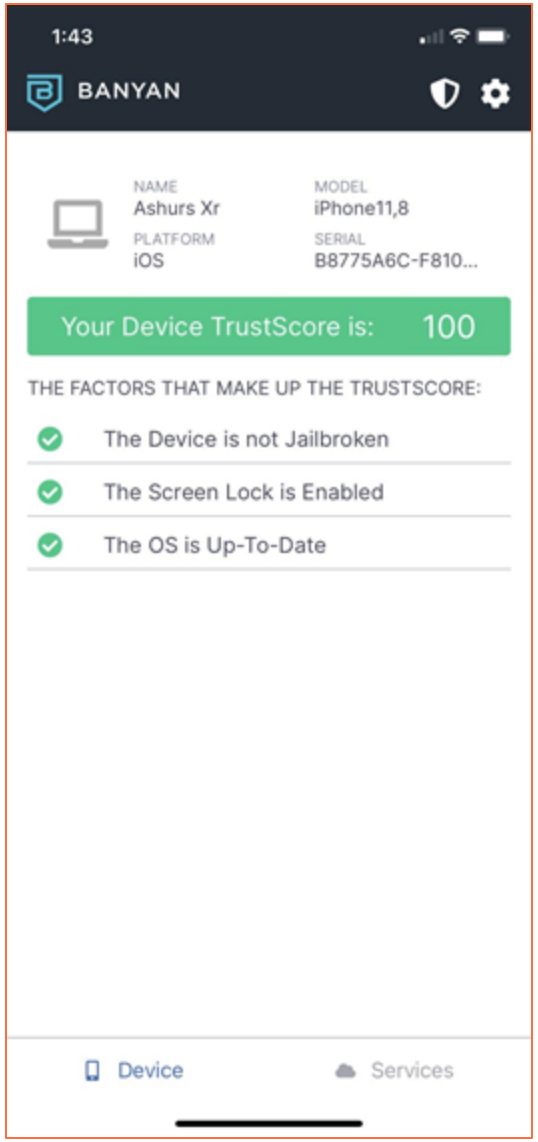
1. CSE APP – PC

› Windows, macOS, Linux 지원
› 다양한 L3/L4 연결 방식 지원
› 다중 조직 지원
› 디바이스 보안 상태 확인 지원



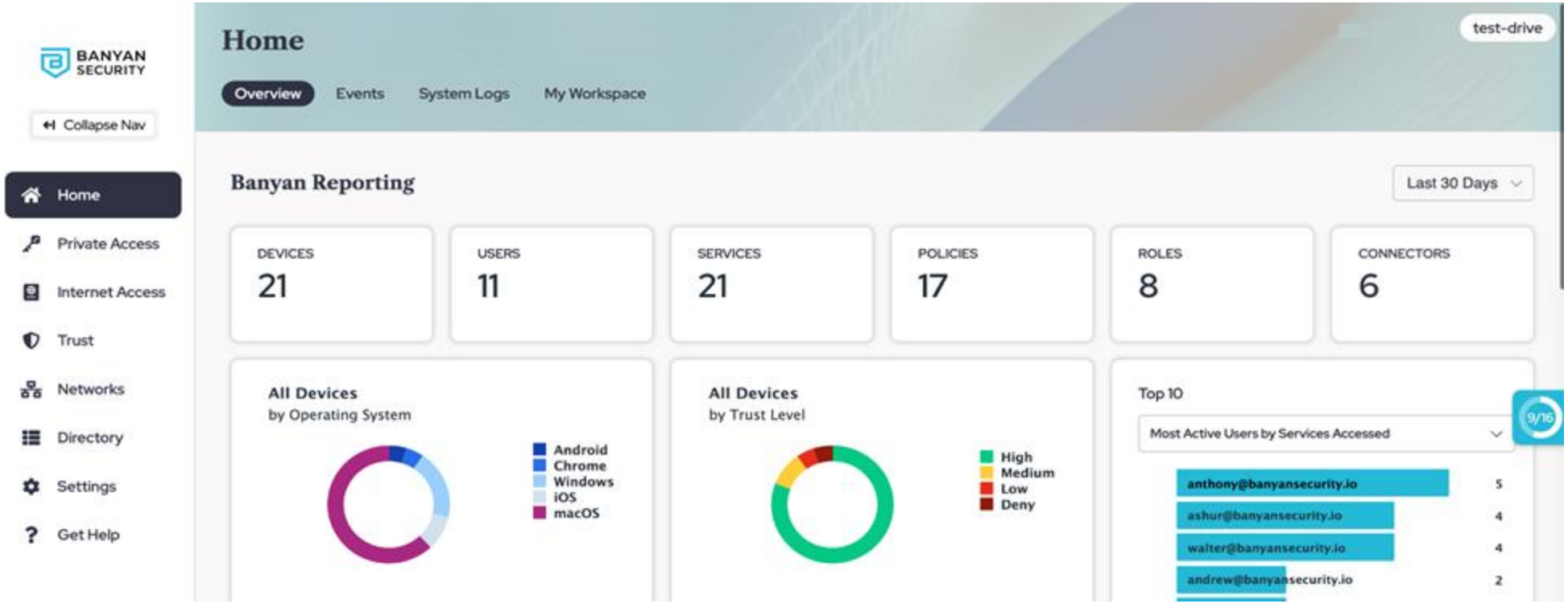
1. CSE APP – MOBILE

- iOS 및 Android 지원
- 직접 Apple App Store 및 Google Play 다운로드 가능
- 루팅 및 탈옥 디바이스 탐지
- 최신 상태 및 보안 상태 유지



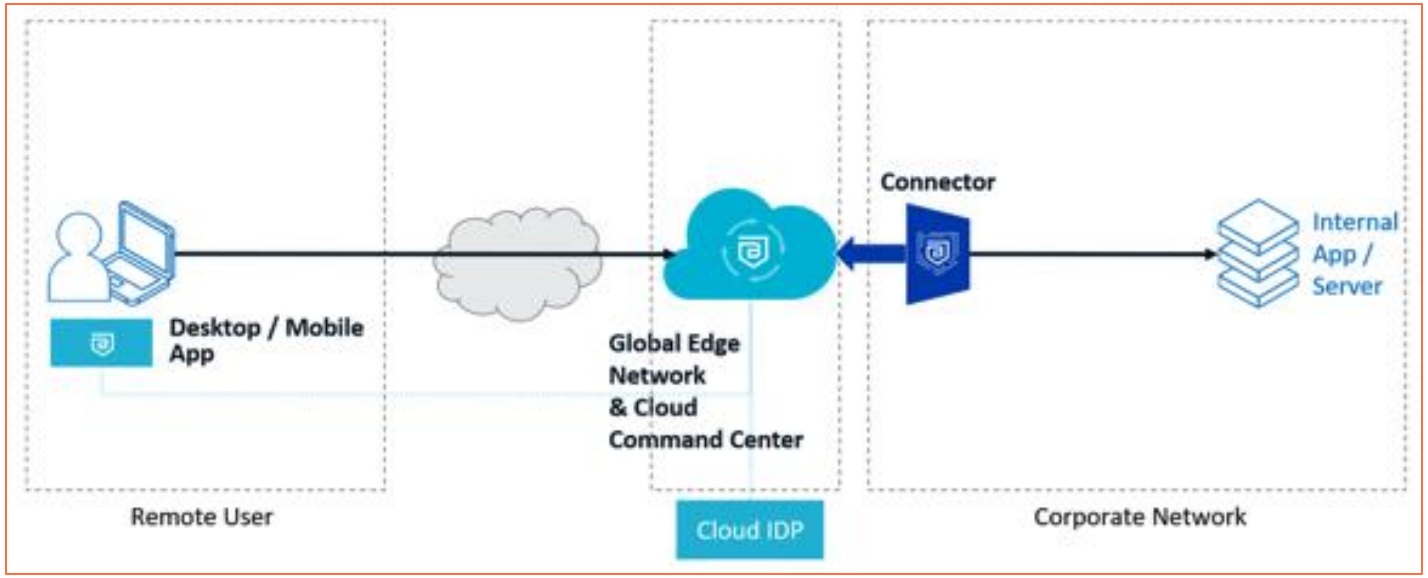
2. CLOUD COMMAND CENTER – 관리 콘솔

› 멀티-테넌트 및 마이크로 서비스 기반 SaaS 플랫폼
› 모든 설정 및 관리자 작업에 대한 가시성 제공
› TOP Cloud Vender 환경에서 운영 중
› SOC 2 Type 2 인증 보유



3. EDGE - GLOBAL EDGE (SONICWALL-HOSTED ACCESS TIER)

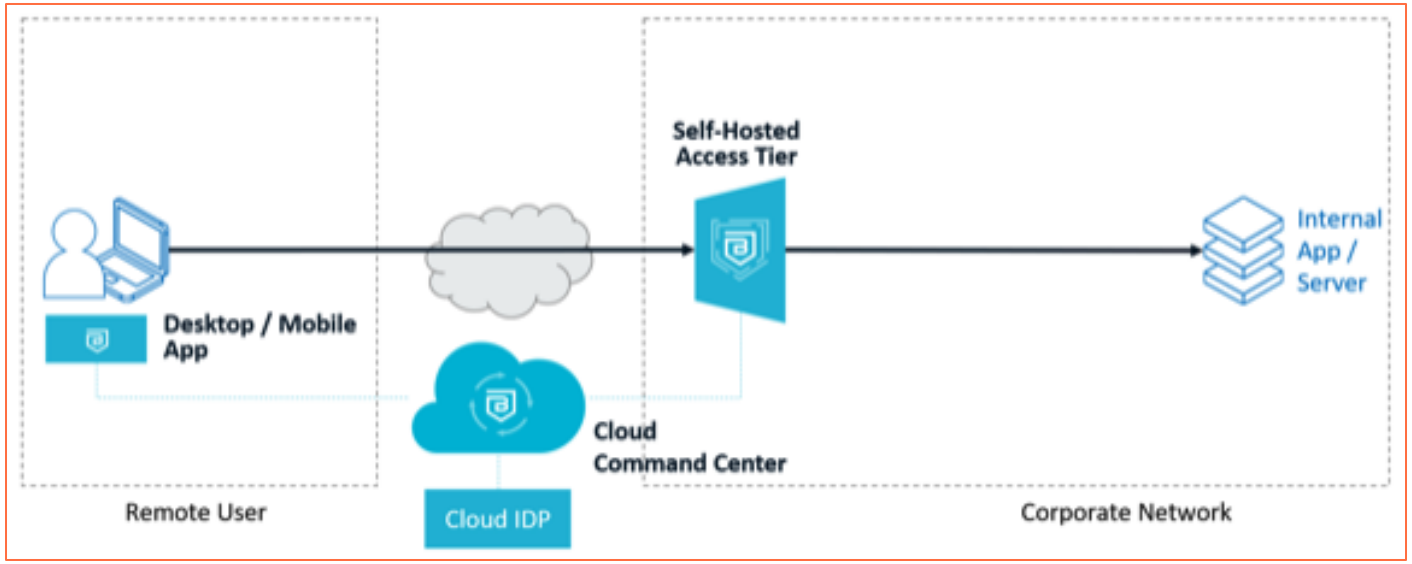
- 동일한 사용자 인증 기반 프록시
- SonicWall 호스팅
- 모든 사용자 트래픽을 (data plane) SonicWall 글로벌 인프라에서 처리
- 사내 접속시 경량 Connector를 고객 인프라에 배포 필요
- Outbound 연결만 필요
  - 방화벽 정책 변경 불필요
  - 443/TCP
  - 40000-44000/UDP
- 빠른 구축(수분내)
- 참고Site:
  - https://docs.banyansecurity.io/docs/banyan-components/connector/



3. EDGE - PRIVATE EDGE (SELF-HOSTED ACCESS TIER)

"분산(*Distributed*)" Access Tier로도 부름

- 사용자 인증 기반 프록시
- 고객이 직접 호스팅 (self-hosting)
- 모든 사용자 트래픽(data plane)을 고객 내부 인프라에서 처리
- 빠른 배포(수분내)
- 요구사항:
  - External IP address
  - Internet Access
  - Inbound Ports:
    - 443 (web services)
    - 8443 (infrastructure services)
    - 51820 (service tunnels)
- 참고Site:
  - https://docs.banyansecurity.io/docs/banyan-components/accesstier/



3. EDGE – EDGE 타입에 대한 결정

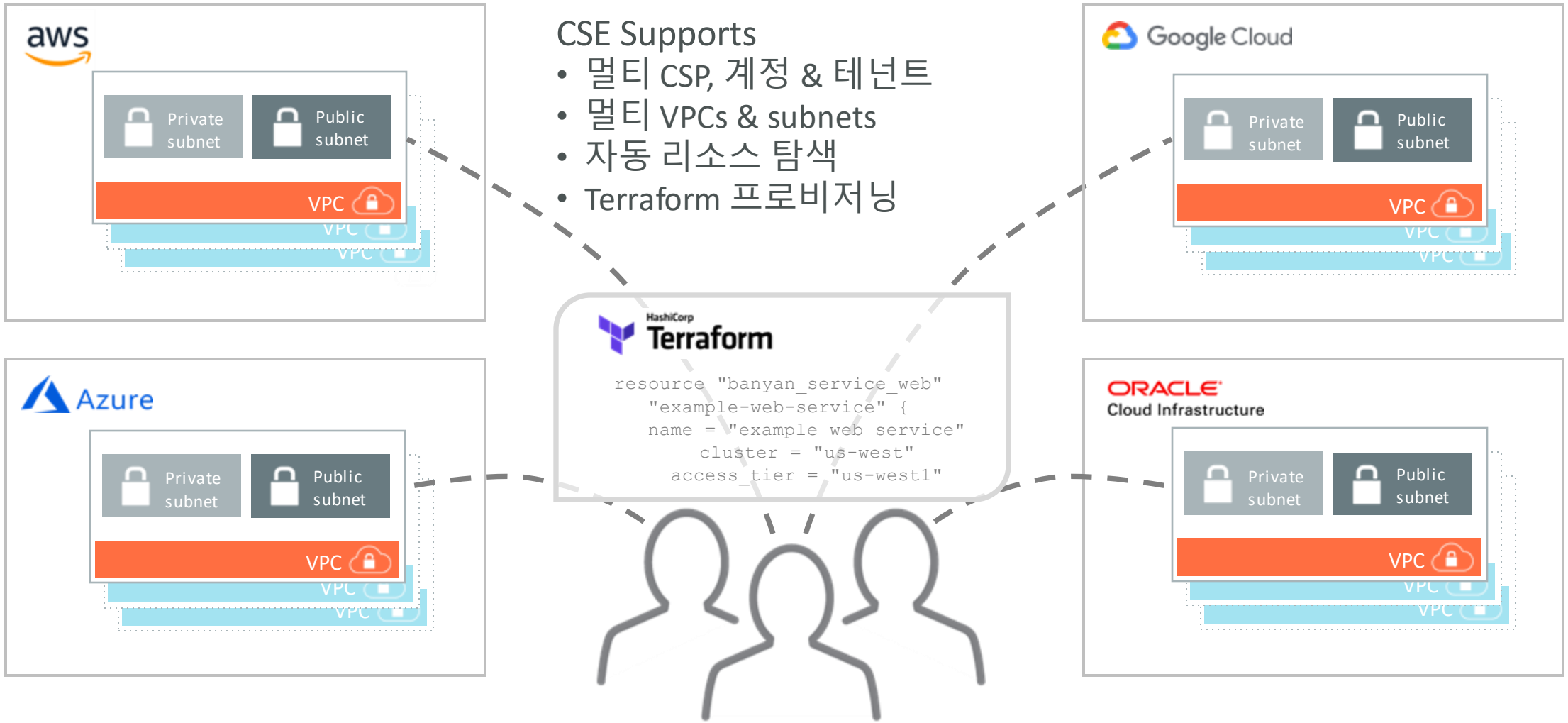
	기업별 적합한 사용 구성
Global Edge	• Iaas/SaaS 등 Cloud 를 우선적으로 사용중인 조직 • 관리 포인트의 간편함을 원하는 조직 • 메인 데이터 센터가 없이 다수 및 소수의 지점을 갖고 있는 조직
Self-hosted Private Edge	• 메인 데이터 센터를 기반으로 다수의 지점을 갖고 있는 조직 • 기존 DevOps 프로세스와의 통합이 필요한 조직 (좀더 많은 제어 기능이 필요한) • 트래픽 감사 및 추적에 컴플라이언스 준수가 필요한 조직 • 모든 사용자 트래픽을 직접 관리하고 싶은 조직
Hybrid	• 인수 합병 등으로 조직이 성정하고 있으며 빠른 시스템 통합이 필요한 조직 • 클라우드 마이그레이션이 천천히 진행되고 있는 조직 • 데이터 및 Application이 데이터 센터에서 Cloud 지속적으로 이동 하고 있는 조직

고가용성 (HIGH AVAILABILITY)

- 클라우드 관리 콘솔(Command Center) 이중화
  - 리전 내 이중화 구성 (Kubernetes & DB)

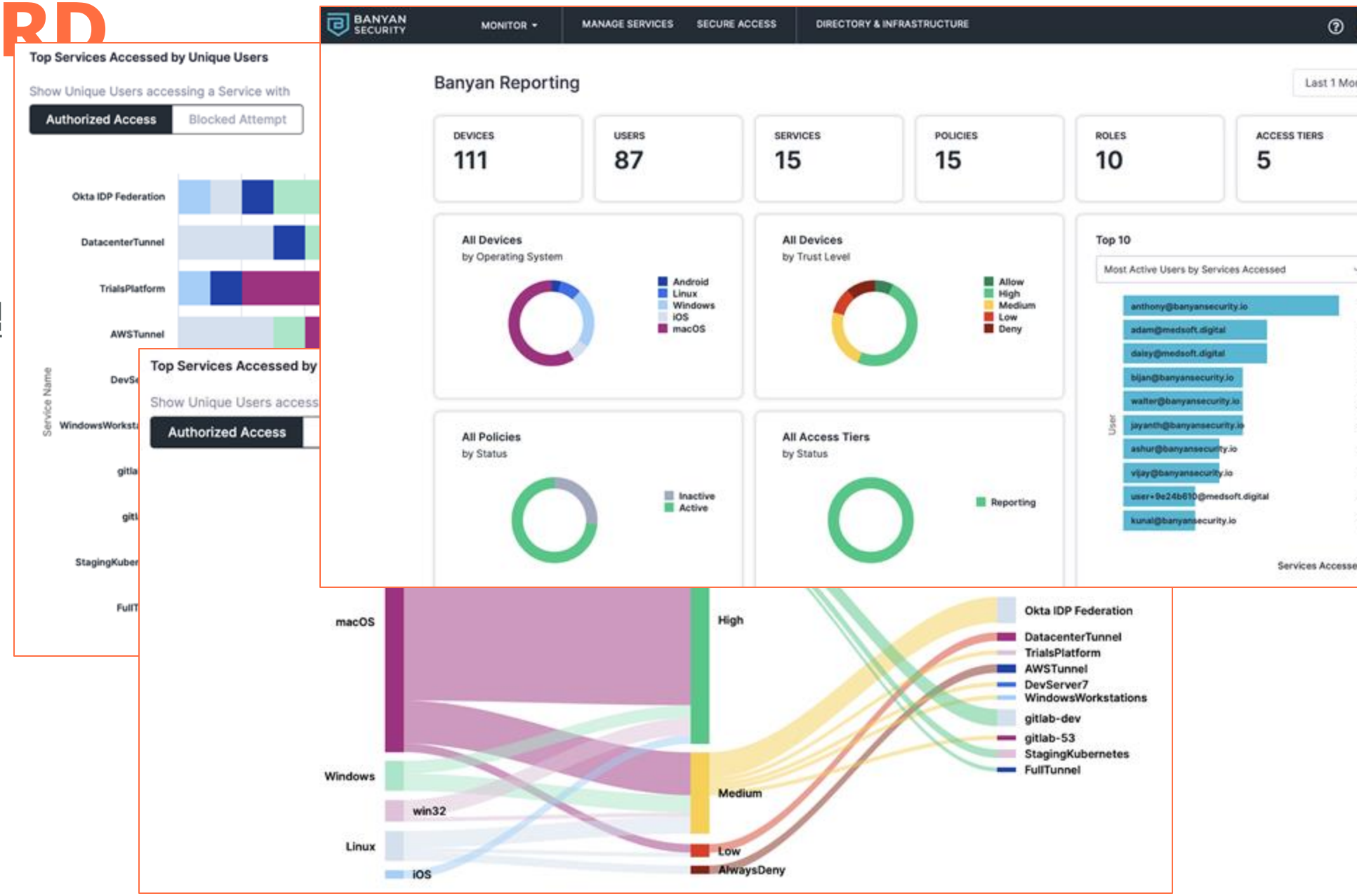
- Access Tier(EDGE) 및 Connector에 대한 이중화
  - 고객에 의해 관리되는 Access Tier(Private Edge)
    - Access Tier(Edge)를 로드 밸런서 하단에 구성하여 다중화 및 고가용성 구성 가능
    - 고객 요청시 다중 리전 Access Tier(Edge) 구성 가능 (사전 협의 필요)
  - 고객에 의해 관리되는 “Connector”
    - 로드밸런서 하단 구성 불가. 단, 다중 배포 가능
  - Global Edge HA
    - 리전 내 자동 HA
    - Global DNS routing & multiple pops 기반 멀티 리전 HA 지원 예정

멀티 클라우드 자동화 및 지원



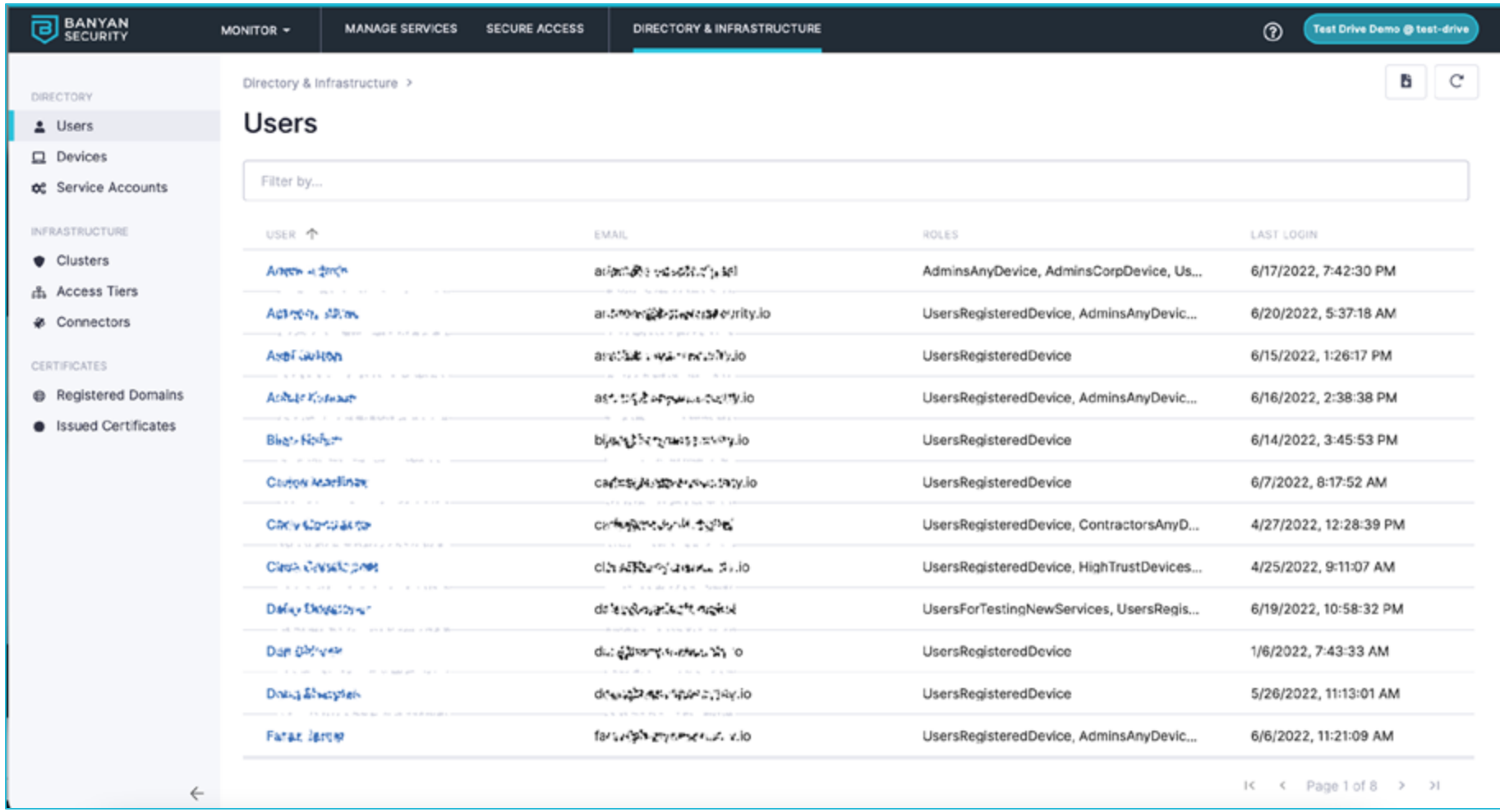
DASHBOARD

- 대쉬보드 및 레포트
- 위젯 기반 정보
- 원클릭 상세정보 연결
- Syslog/SIEM 연동 지원



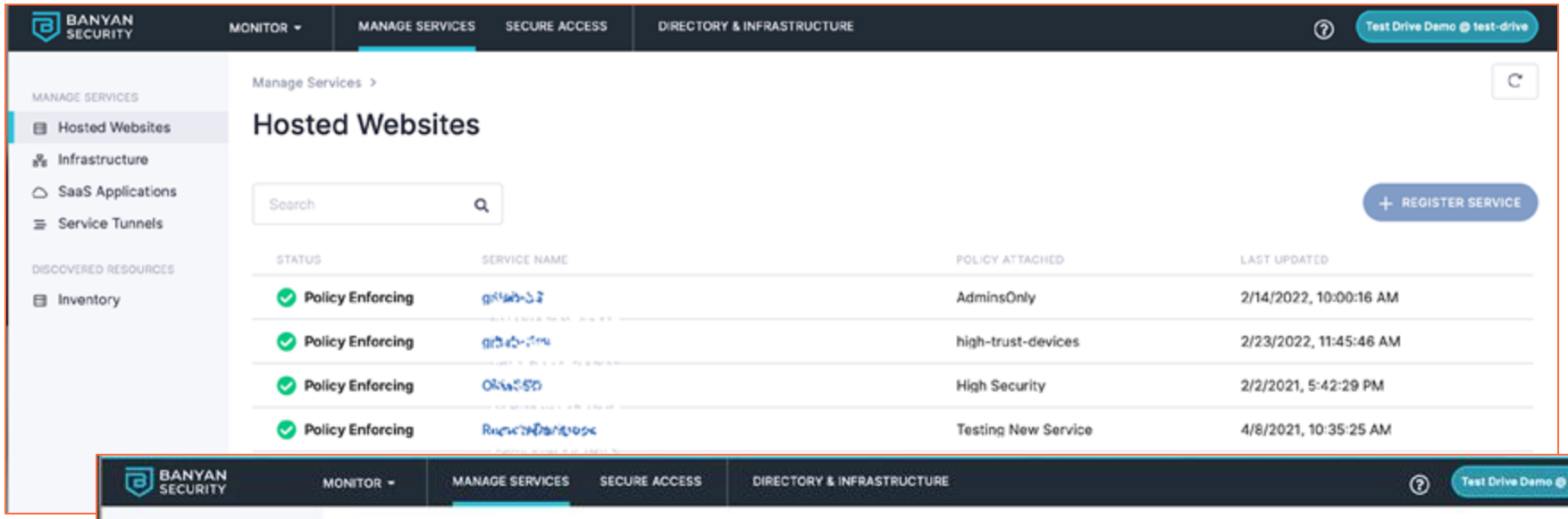
인증(AUTHENTICATION)

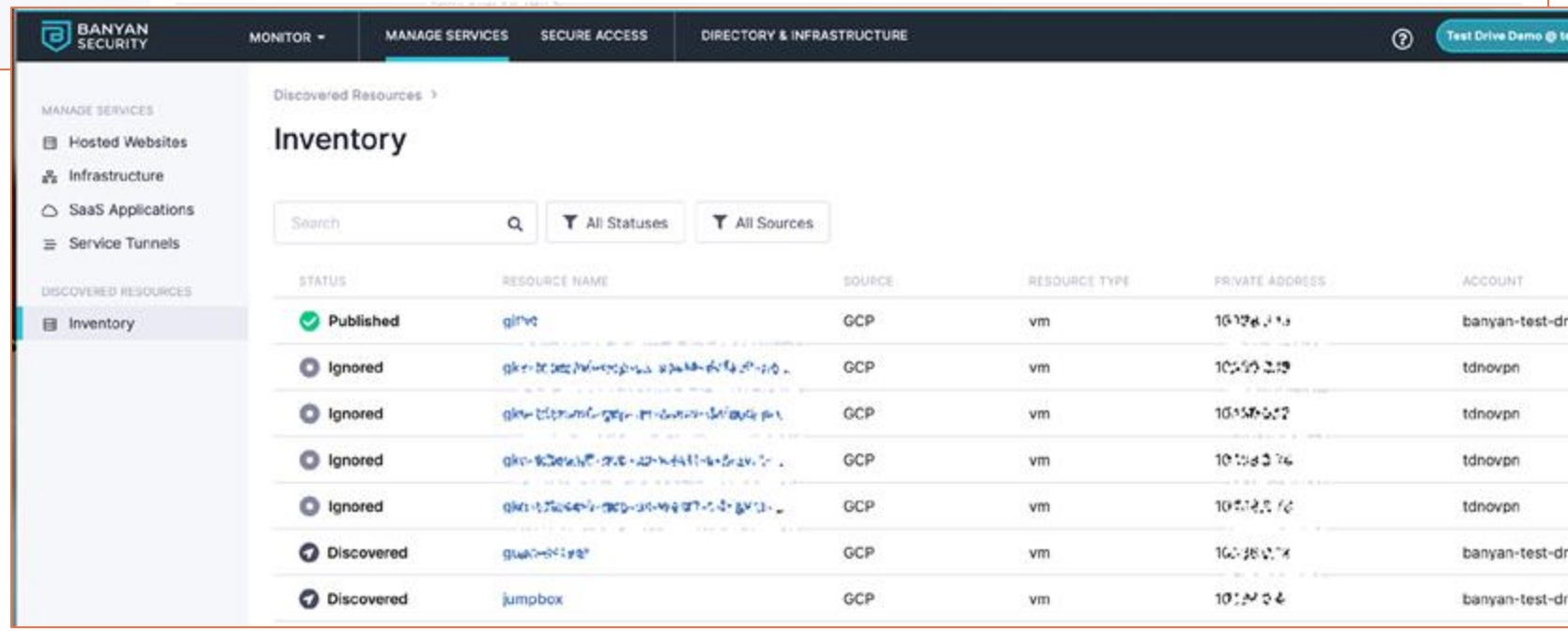
- Local 인증
  (Team Edition only)
- 외부 IDP 연동
  - SAML
  - OIDC
- Passwordless
- Groups and Roles
- MFA



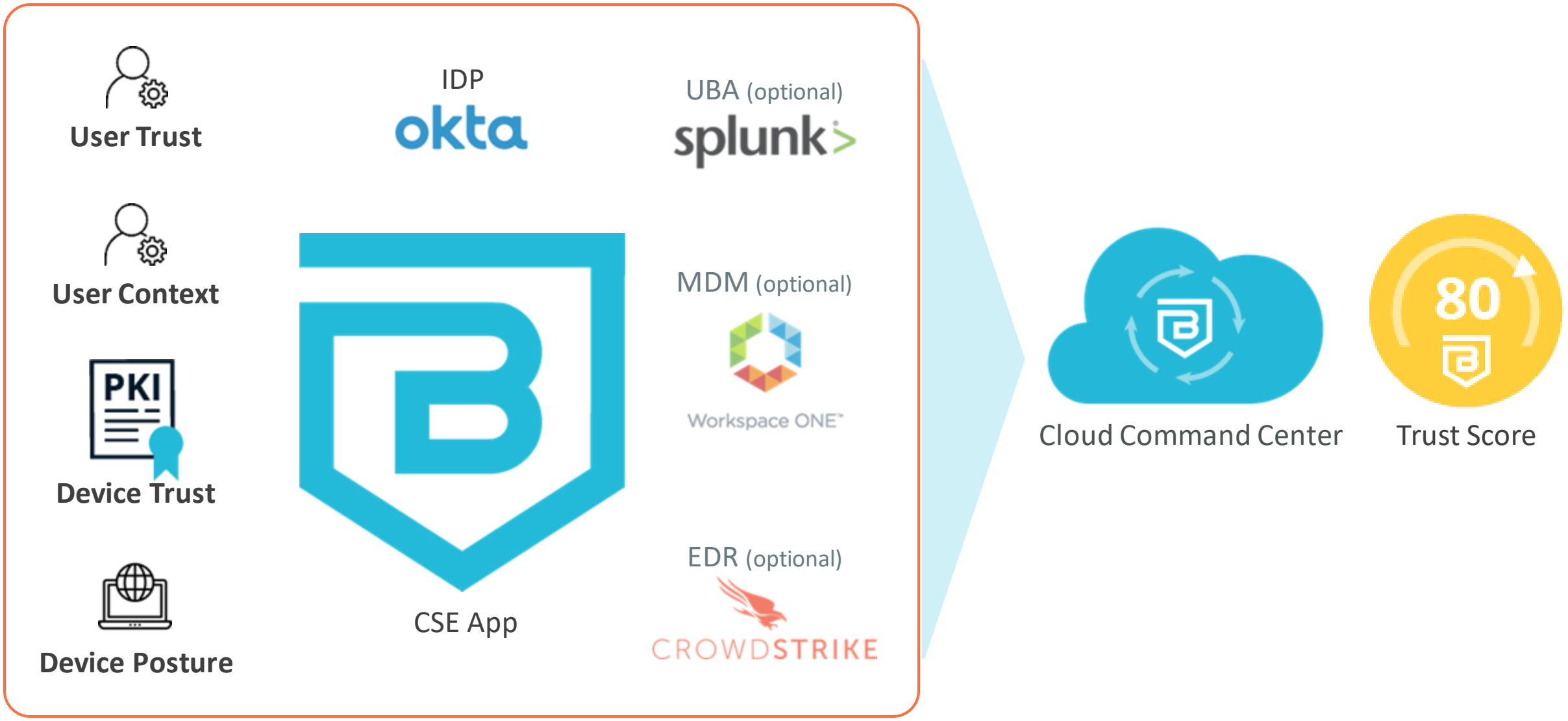
RESOURCES

- 수동 등록
- 자동 탐색 및 등록
- Types:
  - Web Applications (HTTP and HTTPS)
  - SSH
  - RDP
  - Kubernetes
  - 일반적인 TCP services (DBs and VNC 포함)
  - SaaS 어플리케이션
  - Service Tunnels (L3)





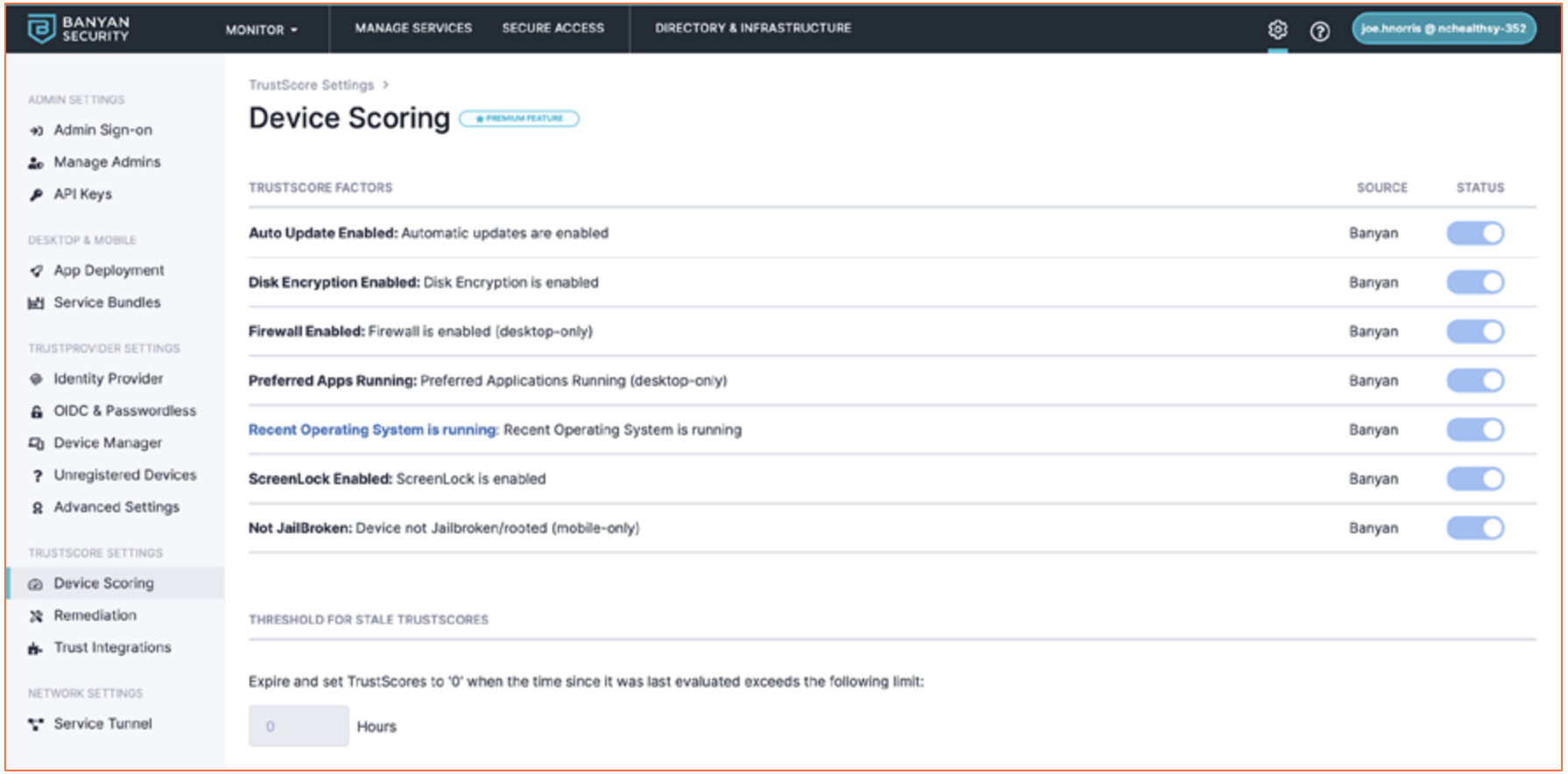
TRUST SCORING 구성요소



디바이스 신뢰도 평가 정책(DEVICE POLICY)

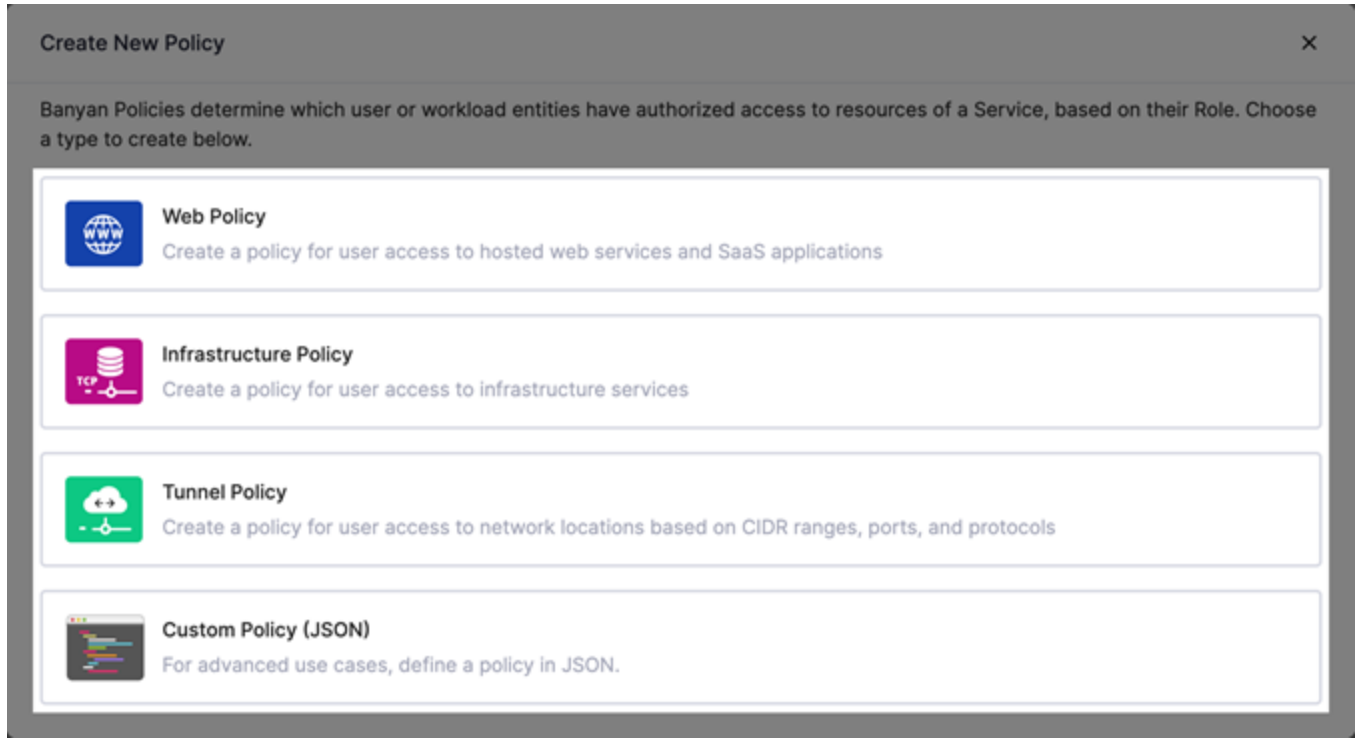
› 다양한 소스를 기반으로 스코어링 가능

› 사용자에게 상태 확인 및 조치 가이드 공유 가능



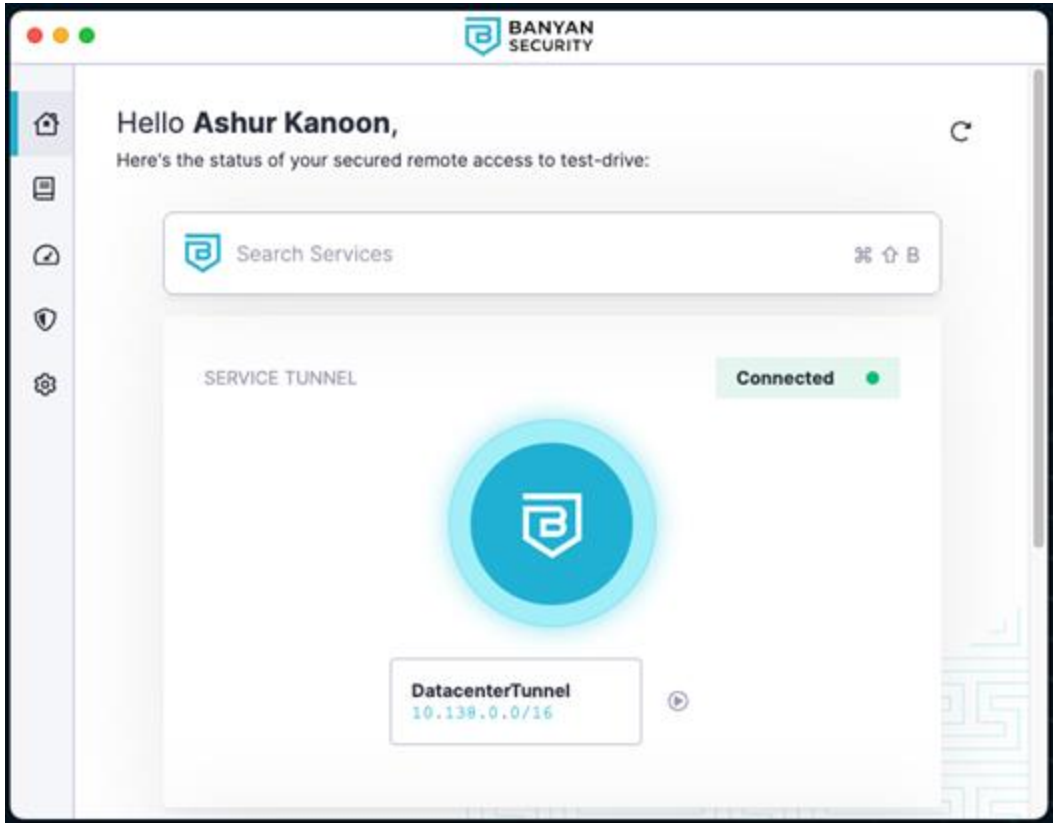
접근제어 정책 (ACCESS POLICY)

- 보호된 서비스 접근 시 사용자에게 적용 되는 정책
- 유연한 정책 구성
- 정책 기반:
  - 사용자/그룹/역할
  - Device 신뢰 레벨
  - 리소스 타입 및 신뢰 레벨
- 다양한 정책 템플릿 제공
- 두가지 모드:
  - Permissive
  - Enforcing
- 특정 대상 정책:
  - 특정 유저,그룹, IP, 및 subnets
  - Whitelist/blacklist



서비스 터널

- VLAN, VPC, Subnet 등 NW 세그먼트에 대한 암호화 된 연결
- Layer 4 기반 접근 제어
  - 프로토콜, 포트, 서브넷 기반 설정
- 전체 연결에 대한 단일 커넥션
- CSE App 필요
- WireGuard 사용



3RD PARTY 연동

- 연동 Type:
  - SAML
  - OIDC
  - APIs (Push or Pull)

- 연동 대상
  - Identity Providers
  - EDR
  - ELK stack
  - SIEM and syslog
  - MDM / UEM

라이선스

- 유저기반 라이선스
  - "Named user license"타입으로 특정 사용자에게 라이선스가 할당 되고 소모 됩니다.
  - "concurrent user license" 및 "Pool license" 타입은 지원하지 않습니다.
- 유저당 디바이스 수량 제한 없음
- 유저 하드 라이선스 제한 없음
- Connectors 및 Access Tier(Edge) 수량 , 트래픽량 제한 없음
- 매분기 라이선스 사용량 정산(Trued up)

- 사용 라이선스 카운트는 ADMIN UI 에 표시 되지 않습니다.
  - 라이선스 소모량은 대시보드 통해 카운트

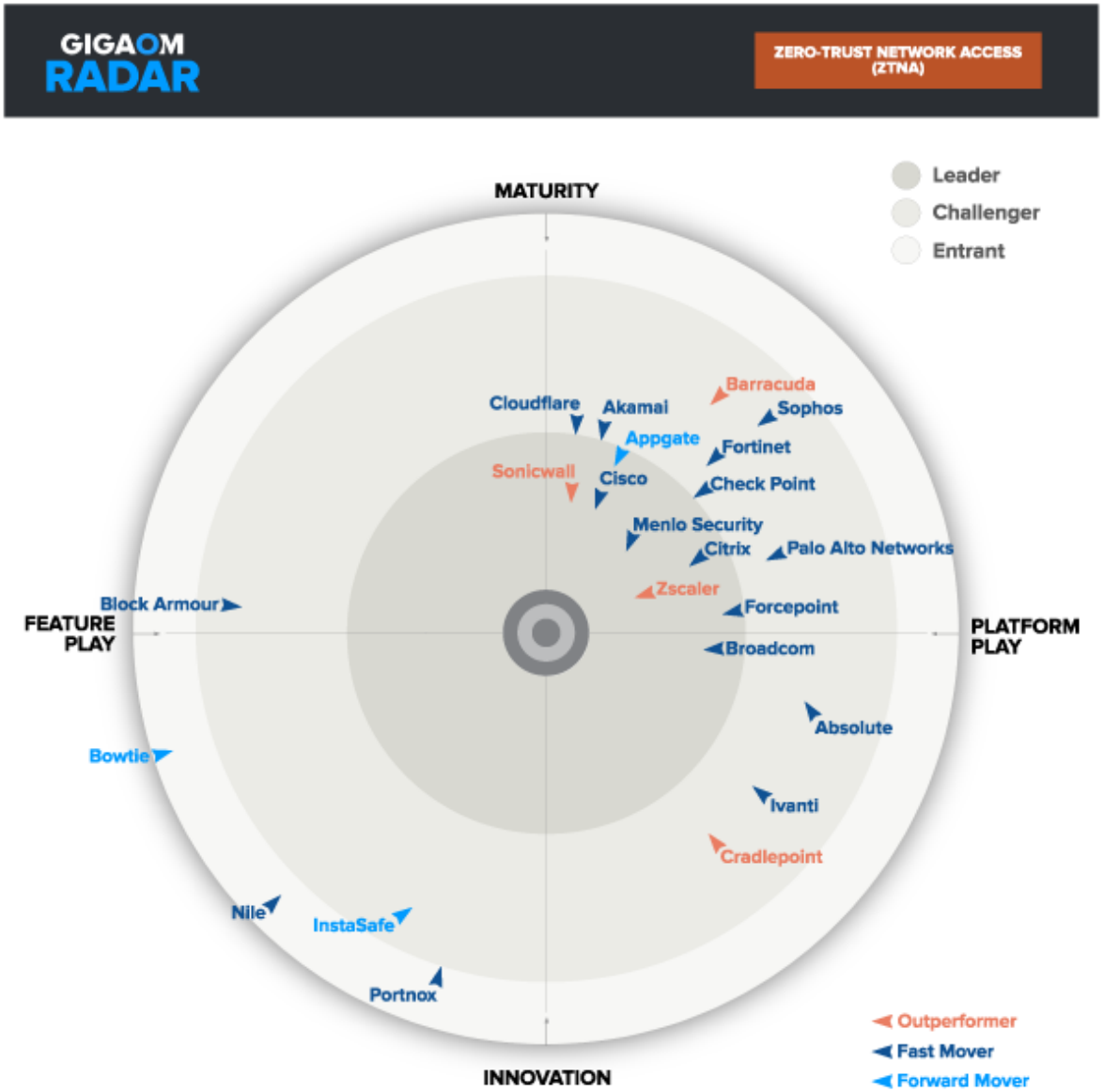
NEW PRICING & PACKAGING

	SPA Basic	SPA Advanced	SIA Basic	SIA Advanced	*SPA Adv + SIA Adv (blended)*
High Performance Data Plane | Cloud Control Plane | Support for all Client Operating Systems | Banyan API	X	X	X	X	*X*
Trust Scoring | Actional Visibility | Continuous Policy Enforcement | Device Posture	X	X	X	X	*X*
Zero Trust Network Access Tunnel (ZTNA)	X	X			*X*
Zero Trust Network Access Proxy (ZTNA) | Private Resource/IaaS Discovery		X			*X*
Unregistered | Clientless | Passwordless Access		X			*X*
EDR | MDM/UEM | SIEM Integration | Service Accounts		X		X	*X*
Private Edge		X			*X*
DNS Filtering (DNS)			X	X	*X*
Cloud Access Security Broker (CASB) | SaaS App Discovery				X	*X*
Preview Secure Web Gateway (SWG)				X	*X*
24x7 Support	X	X	X	X	*X*
RIS/Premier Support	Add-on	Add-on	Add-on	Add-on	*Add-on*
MSRP 1 YR	**$59.99**	**$89.99**	**$35.99**	**$89.99**	***179.98***
MSP Monthly Protect Tier Partner Cost	**$2.99**	**$4.79**	**$1.79**	**$4.79**	***9.58***

**** Not month to month, annually paid***

전문 평가 및 CASE STUDY

외부 평가 : ZTNA 리더 및 아웃퍼포머 선정



GIGAOM RADAR 평가

위험도 기반 인증

Risk 기반 인증에서 높은 점수
실시간 위험 평가에따라 인증 요구 사항을 조정 가능하여, 이는 사용자 행동, 장치 상태, 위치 및 컨텍스트 신호를 고려.
보안을 강화 하고 동적인 ZTNA모델 제공

세션 모니터링 기능

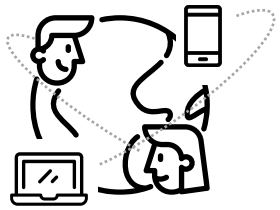
사용자 활동에 대한 실시간 가시성,
로그 기록 및 이상탐지를 제공하여,
각 조직의 보안 및 규정을 효과적으로 유지

높은 사용 편의성

15분 이내 빠른 배포 가능
인프라와 어플리케이션에 대한
원클릭 엑세스 제공
서비스 카탈로그를 통한 관리자 선택 용이

CUSTOMER CASE STUDY: ADOBE

MOBILE WORKFORCE



HYBRID & MULTI-CLOUD

30,000
USERS

120
COUNTRIES

40,000
DEVICES

“CSE는 기존의 보안 및 신원 관리 도구 투자를 활용하여 완벽히 안전한 원격 접근 솔루션을 제공하는 인텔리전스 레이어를 만든 유일한 솔루션이었습니다”

Den Jones
DIRECTOR OF SECURITY

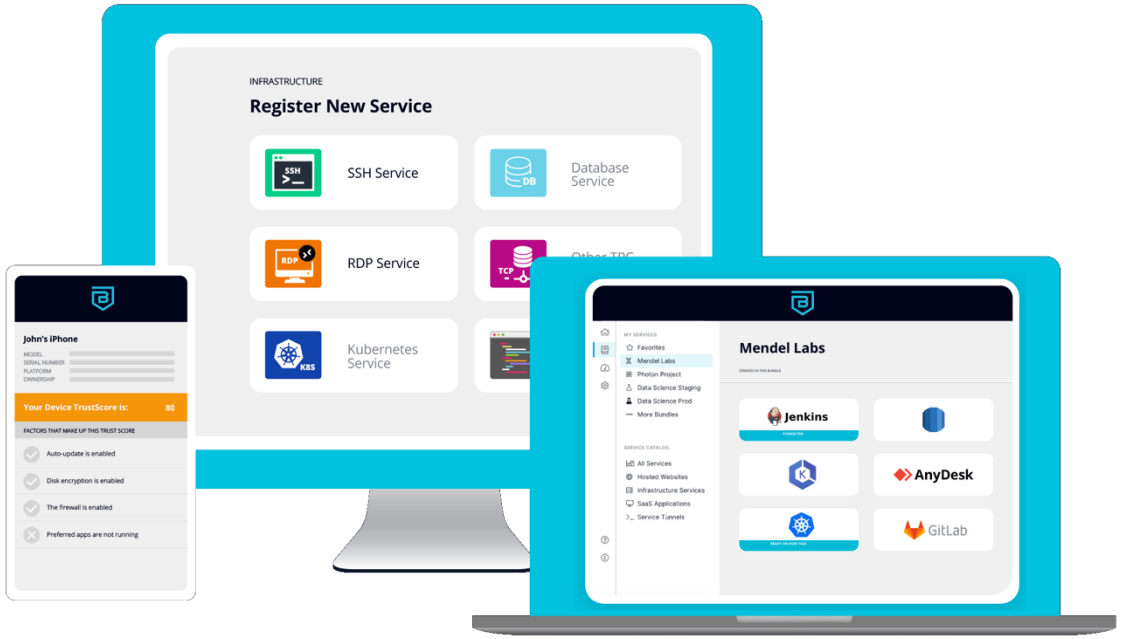
aws

vmware

2,100
APPS & SERVICES

무료 Trial / 정식 라이선스 지원

- Free Trial
  - https://net.banyanops.com/team-edition/create-banyan-account
- Docs
  - https://docs.banyansecurity.io/
- Be up and running in 15 minutes
  - Pick users/groups
  - Create device/resource policy
  - Expand!



SSE 를 고려할때 생각할 부분

필요성	레거시 VPN에서 ZTNA 혹은 SSE솔루션으로 변화가 필요한가
구축방법	클라우드 기반? ZTNA를 통한 Onpremise? Hybrid?
제품성	브랜드, 편의성, 인지도, 레퍼런스, 안정성
확장성/편의성	단일 플랫폼에서 SASE 이외에 무엇을?

THANKS

SONICWALL®