



# 시큐어 SD-WAN과 SASE 솔루션을 통해 On-premise + Cloud 보안을 완성

박현희 이사

포티넷 코리아

# Fortinet Security Fabric Enables Digital Innovation



### Zero-trust Network Access

NAC

Identity

Fabric Agent

### Security-driven Networking

Network Firewall

SD-WAN (WAN edge)

SD-Branch (LAN Edge)

FortiSASE (Cloud Edge)

### Dynamic Cloud Security

Public Cloud

Application Security

Data Center

### AI-driven Security Operations

AI / ML

SOAR

SIEM

### Fabric Management Center

Single Pane

Automation

API

# 기업의 환경이 빠르게 변화하고 있습니다.

- 비즈니스 민첩성과 운영 효율성 필수
- 보안, 클라우드 연결성, 비용 절감 및 가시성 확보를 통한 경쟁력 강화

## 디지털 트랜스포메이션



## 멀티 클라우드 & SaaS

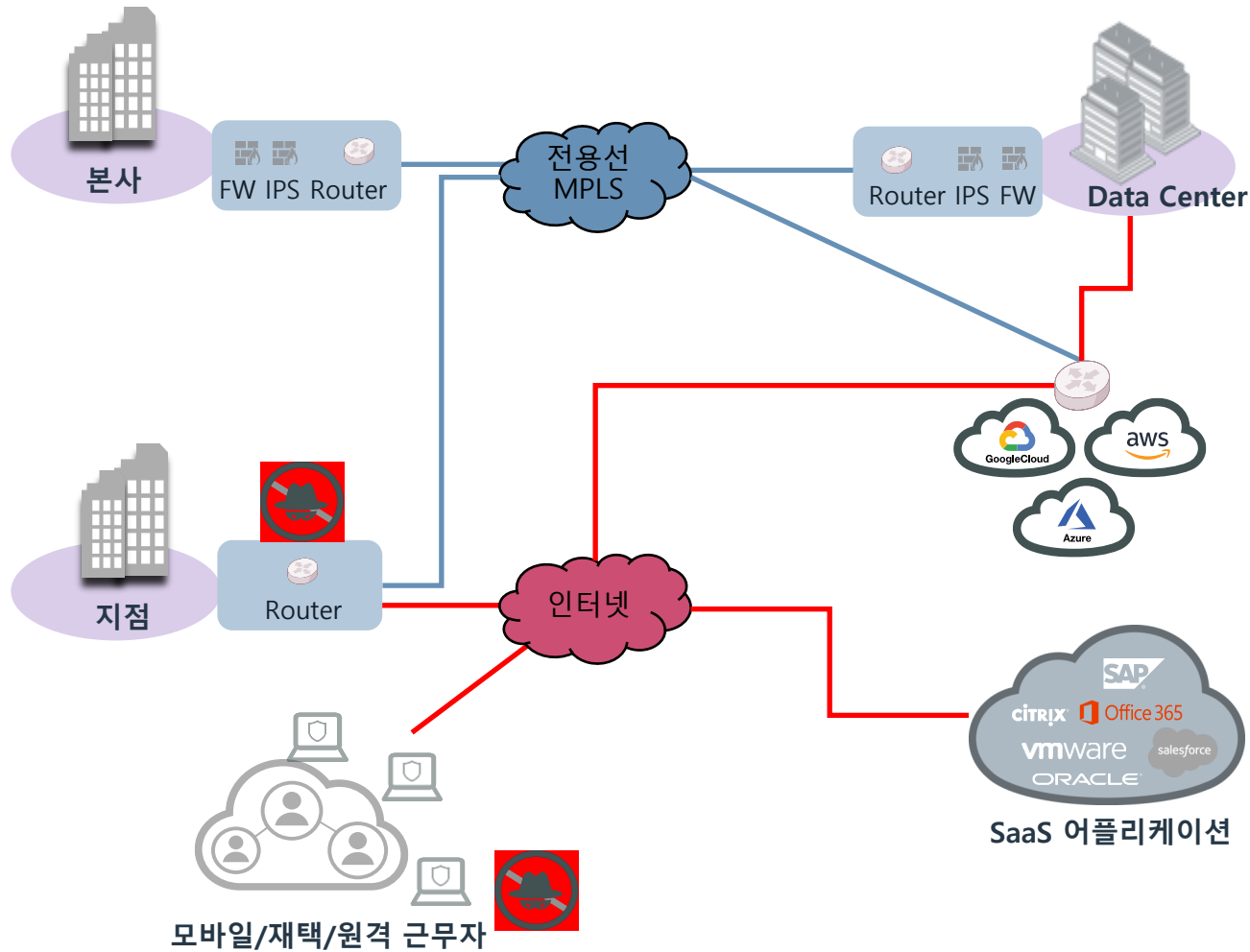


Multi-Cloud



Internet / SaaS

# 기업 환경 변화에 따라 증가하는 고민



## 고정형 지점, 본사, 데이터센터

- 지점 회선 비용 효율화와 통합 관리
- 멀티 클라우드 및 SAAS 어플리케이션 도입
- 보안과 사용자 경험을 모두 만족

## 모바일 오피스, 재택 및 원격 근무자

- 사용자의 위치와 관계없이 기업 본사와 동일한 수준의 보안 필요
- 일관된 Deployment & Manage 의 어려움

# 포티넷 시큐어 SD-WAN

# 변화하는 비즈니스 환경에서 기존 WAN의 한계

기존 WAN은  
복잡하고  
유연성이  
부족합니다

디지털 혁신을 위한 개선 필요



## 매뉴얼 운영 방식

Router CLI 사용으로 중앙 집중 관리의 어려움



## User Experience (사용자 만족도) 부족

멀티 클라우드와 SaaS에 대한 사용자 만족도 부족



## 보안 취약성

직접 인터넷 액세스 관련 보안에 취약



## 높은 구축 및 운영 비용

전용회선 사용과 포인트 솔루션 구매로 높은 구축 및 운영 비용

# SD-WAN 이란?

## □ SD-WAN (Software-defined WAN)

- 기존 WAN 회선 (MPLS, 4G, 5G, ADSL 등) 위에 Software적으로 Overlay 네트워크를 구성하여 사용
- 비즈니스 어플리케이션에 대해 빠르고 쉽게 접근할 수 있도록 다양한 회선을 통한 최적의 경로 제공
- 통합관리를 통한 운영 효율성 제공

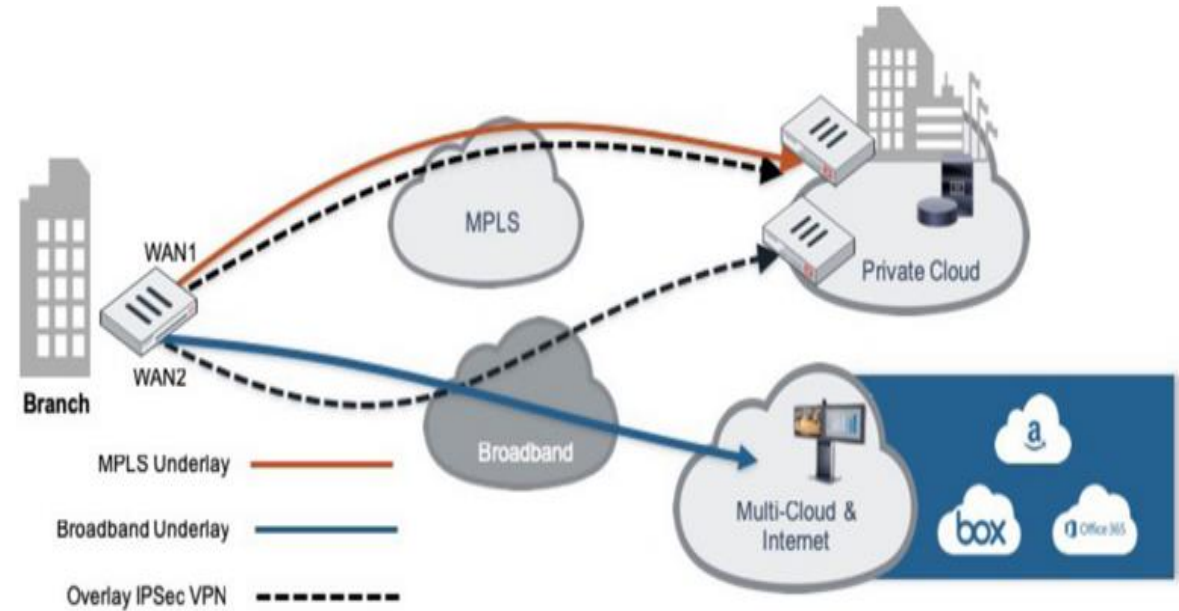


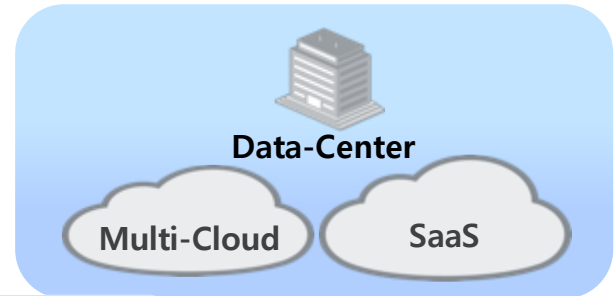
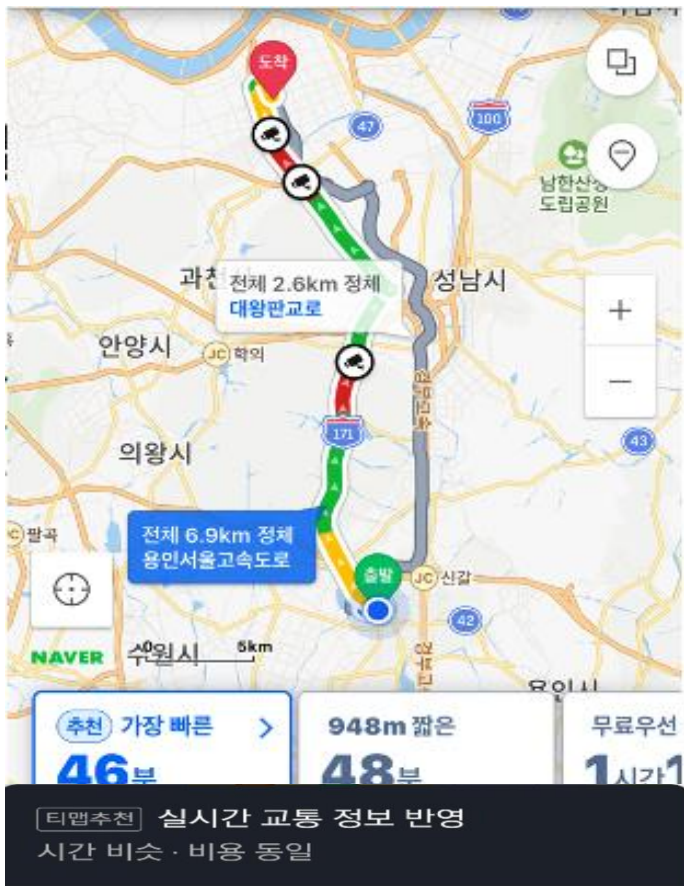
Figure 11: SD-WAN interface members (underlay and overlay).

실시간으로

보다 덜 막히는  
길을 찾고

사고 구간을  
회피하며

보다 빠르고  
효율적이고  
안전하게



| Latency                         |         |
|---------------------------------|---------|
| KT via Actela (port17):         | 42.97ms |
| SK BB (port18):                 | 57.43ms |
| KT via Actela (port17): 10.26ms |         |
| SK BB (port18): 3.95ms          |         |

| Packet Loss                   |       |
|-------------------------------|-------|
| KT via Actela (port17):       | 0.00% |
| SK BB (port18):               | 0.00% |
| KT via Actela (port17): 0.00% |       |
| SK BB (port18): 0.00%         |       |





# SD-WAN 도입시 가장 큰 고려 사항은 바로, “보안”

- 외부에 공개되어 공격에 무방비로 노출되어 있는 WAN

## 공인 IP로 지속되는 공격들

The image displays two screenshots from a network analysis tool. The top screenshot shows a traffic flow with a source IP of 80.49 and a destination IP of 202.12.137.11. The bottom screenshot shows a log of incoming connections to a local host, including details like source IP, port, and the user 'root'.

## 국내 보안에 취약한 POS 5,000여개

This block contains two screenshots. The left screenshot shows Shodan search results for 'POS' in South Korea, listing 5,478 results with a map of South Korea and a list of top cities like Seoul, Busan, and Daegu. The right screenshot shows a Windows Embedded login screen with the text 'Windows Embedded PCReady' and a login field.

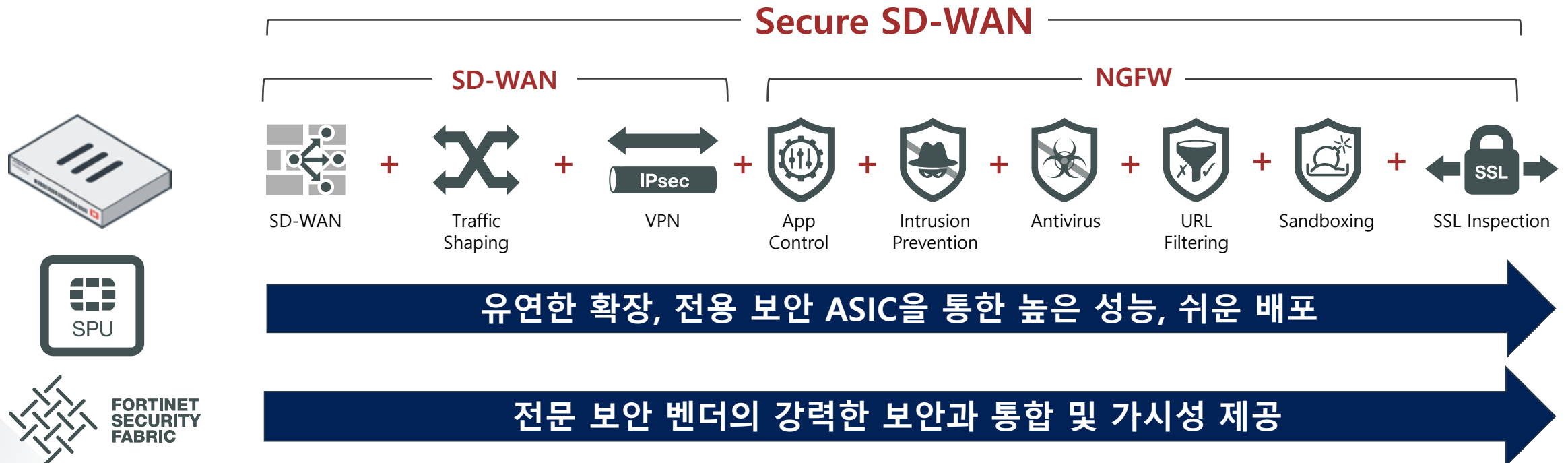
## 노출되어 있는 공장 시스템

The image shows a complex industrial control system interface. It features a central control panel with various buttons and indicators, surrounded by multiple data displays, including numerical values and small charts, representing different parts of a factory system.

# SD-WAN의 진화, 포티넷 Secure SD-WAN

- SD-WAN과 NGFW 기능을 통합하여 WAN의 보안을 강화

90%의 SD-WAN 벤더에서 제공하는 보안기능은  
WAN을 보호하기에 충분하지 않습니다.



# 포티넷 시큐어 SD-WAN을 적용하면?

01

업무 가용성 향상 및  
보안 강화



- 기업 회선의 효율적으로 사용으로 **업무 가용성 향상**
- NGFW와 통합으로 트래픽 **가시성 향상 및 WAN 보안 강화**

02

운영 효율성 향상  
투자/회선비용절감



- 통합 관리 및 모니터링을 통해 **운영 효율성 향상**
- 지점 포인트 솔루션 통합으로 **투자 비용 절감**
- 전용회선을 인터넷 회선으로 대체하여 **회선 비용 절감**

03

사용자 만족도 향상



- 실시간 회선 품질 모니터링을 통한 동적 경로 선택 및 Business Critical application에 우선 순위 부여를 통해 **사용자 만족도 향상**

04

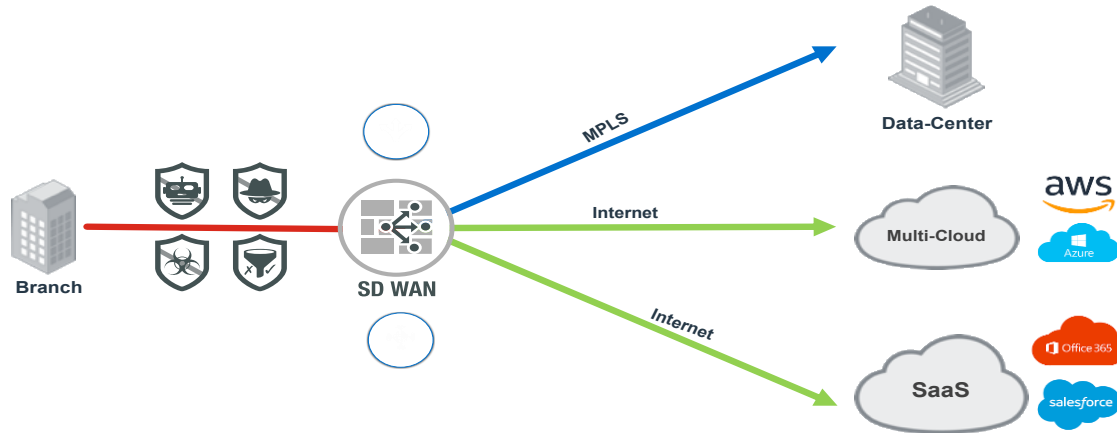
유연한 확장성



- **Secure SD-Branch로 확장**
- **SASE로 확장**

# 업무 가용성 향상 및 WAN 보안 강화

## 업무 가용성 향상



- 전용선, 인터넷 등 회선에 대한 품질 모니터링 수행을 통해 최적의 경로 선택 및 전용회선 사용률 최적화
- 주요 어플리케이션별 우선 순위를 부여하여 사용자 만족도 향상
- 중앙에서 각 Branch별 상태 모니터링

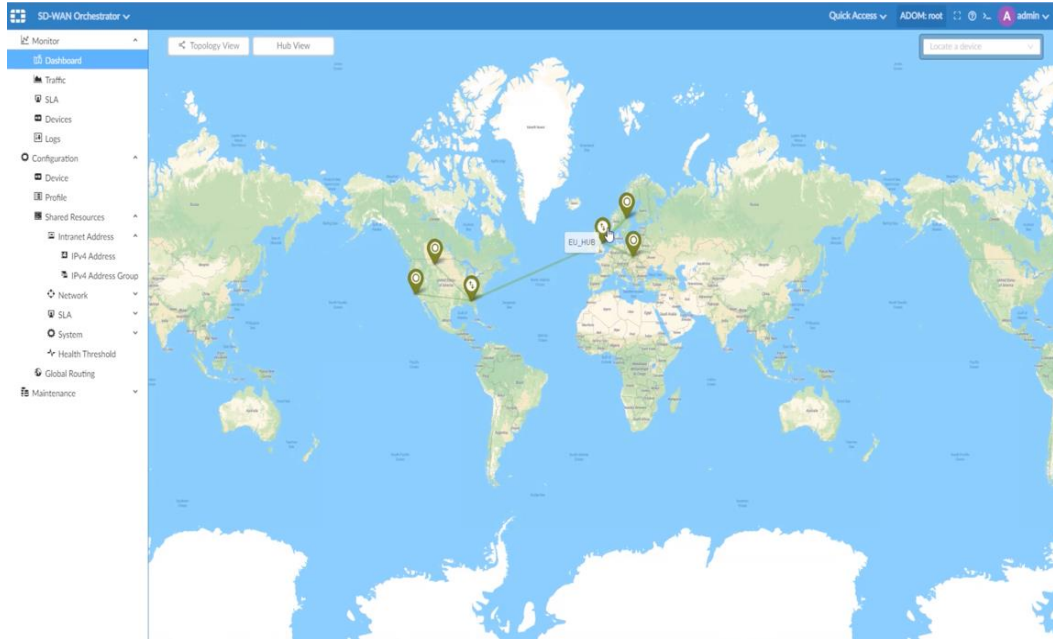
## WAN 보안 강화



- SSL 암호/복호화 기능으로 모든 트래픽 (HTTP, HTTPS)에 대한 애플리케이션 가시성 및 제어
- Anti-Virus, 웹 필터링, IPS를 이용하여 외부로부터의 공격을 최전선에서 차단
- Sandbox와 연동하여 Zero-day 공격 차단

# 중앙 관리 및 모니터링을 통한 운영 효율성 향상

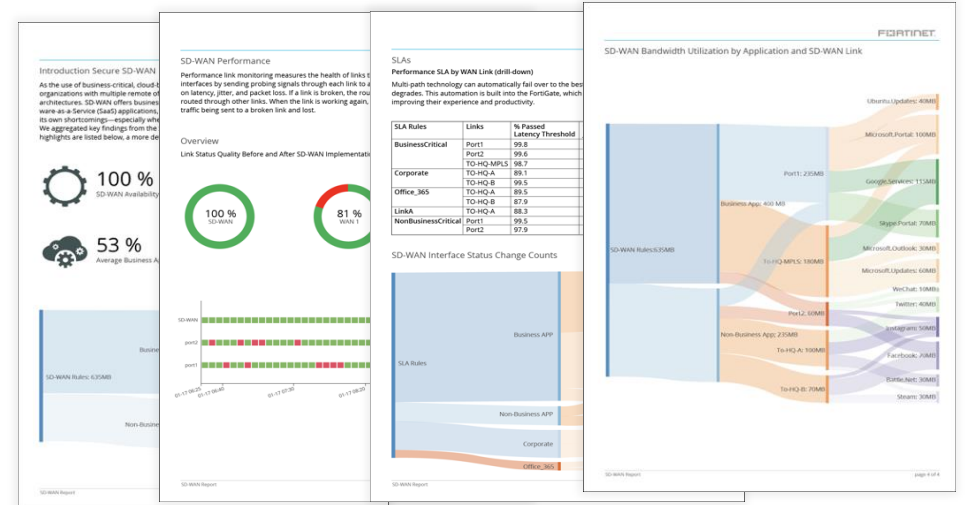
여러 장비에 대한 중앙 관리 및 정책 관리



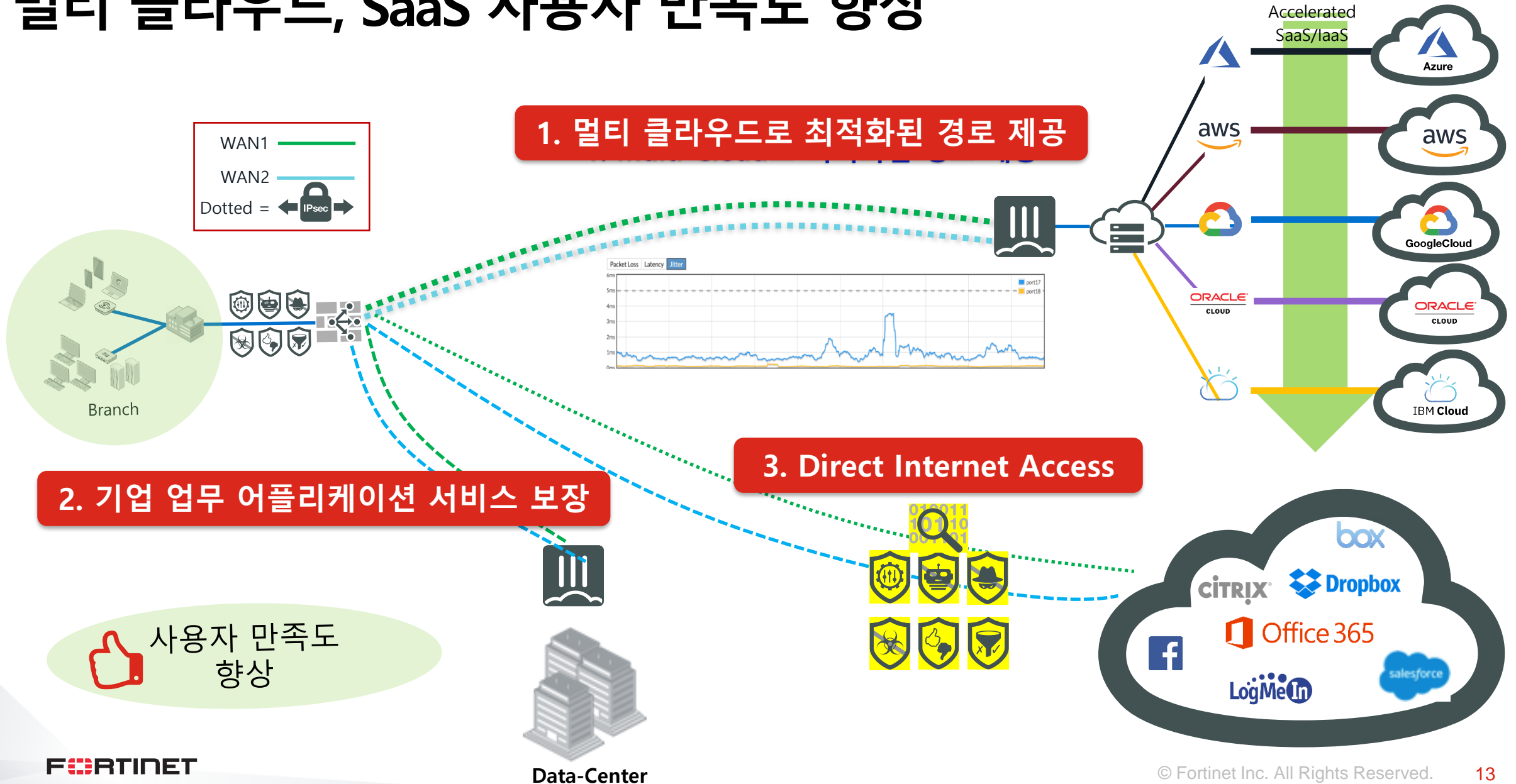
SD-WAN Rules

| ID | Name                  | Source | Destination                                   | Criteria                    | Members   |
|----|-----------------------|--------|---|-----------------------------|-----------|
| 1  | ip                    | all    | 172.16.14.30                                  | Latency                     | wan1      |
| 2  | FQDN_Best-Quality     | all    | gmail.com                                     | Custom-profile-1 (Default_G | wan1 wan2 |
| 3  | APP_lowest-Cost       | all    | Facebook, Twitter, KakaoTalk, Twitch, YouTube | Default_Google Search#1     | wan1 wan2 |
| 4  | any_Maximiz-Bandwidth | all    | all   | Main_SW_SLA#1               | wan1 wan2 |
|    | sd-wan                | ALL    | ALL   | Usage Based                 | ALL       |

통합 로깅 및 리포트



# 멀티 클라우드, SaaS 사용자 만족도 향상



# 시큐어 SD-Branch로 확장

- WAN과 LAN (유무선) 통합하여 관리/운영



**SD-WAN, NGFW, Switch, AP  
모두 통합 관리**



Connector



APIs



DevOps



Extended Ecosystem



Legacy WAN

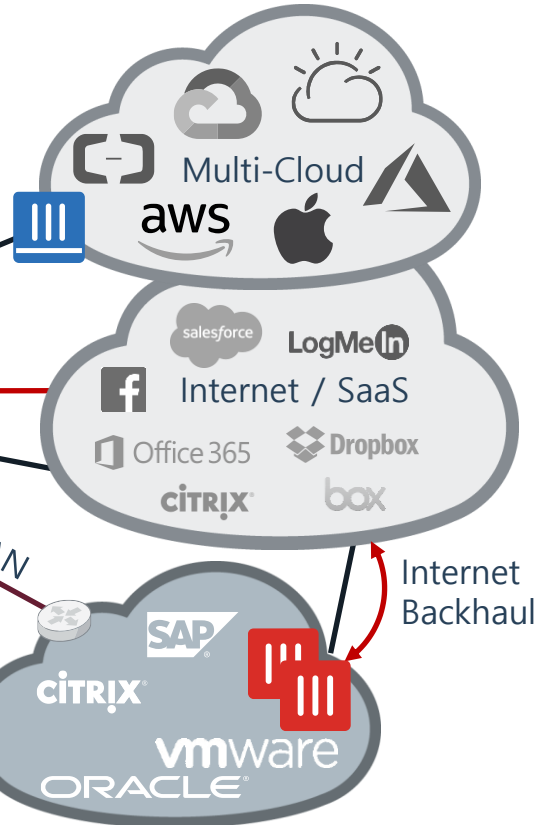
SD WAN

SD-WAN

Secure SD-WAN

SD-Branch

Secure SD-Branch



# 포티넷 시큐어 SD-WAN ROI Calculator

## SD-WAN 도입 시 ROI 절감 효과 확인

### 시큐어 SD-WAN ROI Calculator

포티넷 시큐어 SD-WAN은 고급 보안 기능을 통합하는 동시에 고가의 MPLS 브로드밴드 마이그레이션하여 애플리케이션 경험을 개선하고 WAN 운영을 단순화하며 비용을 절감합니다.

포티넷 시큐어 SD-WAN을 통해 얼마나 비용 절감을 할 수 있는지 궁금하시다면, 지금 바로 시큐어 SD-WAN Calculator를 사용해보십시오.

사이트 수  
사무실 수 입력.

허브 수  
데이터 센터 수 입력.

사이트당 월간 MPLS 비용  
각 지점 사무실의 MPLS WAN 링크에 대한 월평균 비용 입력.

사이트당 MPLS 대역폭 요구 사항  
각 지점 사무실의 MPLS WAN 링크에 대한 월평균 대역폭 용량(Mbps) 입력.  Mbps

MPLS 감소 비율(%)  
인터넷 연결로 교체할 MPLS 링크의 비율 입력.  %

사이트당 월간 인터넷 비용  
모든 지점 및 허브에 대한 월평균 비용 입력.

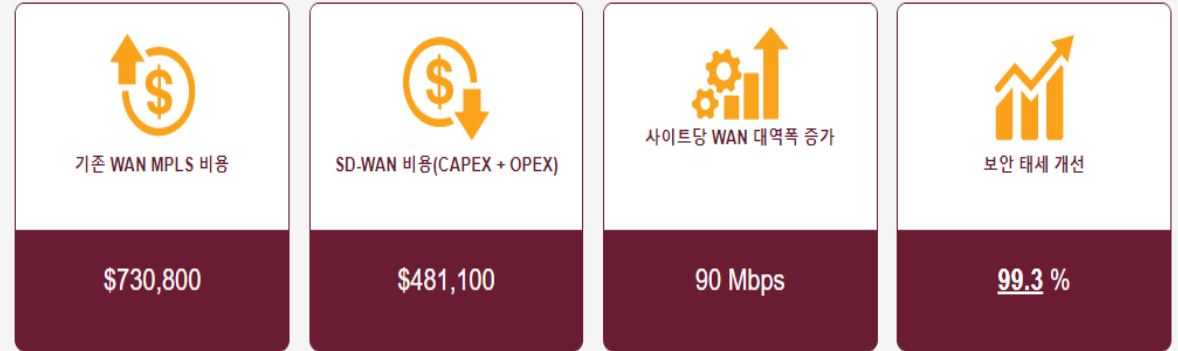
사이트당 이용 가능한 인터넷 대역폭  
인터넷에서 지점 및 허브에 제공하는 평균 대역폭 용량 입력.  Mbps

기간(년)  
ROI를 계산할 기간(년) 입력.  Year(s)

시큐어 SD-WAN  
NGFW 보안이 요구 사항인지 선택.

**계산**

총 34%의 금액을 3년동안 절약 가능



<https://www.fortinet.com/kr/products/sd-wan#secure-sdwan-roi-calculator>

<포티넷 SD-WAN ROI Calculator 바로가기 >



# 포티넷 시큐어 SD-WAN, Secure SD-Branch는

Gartner 에서 인정 받은  
Fortinet Secure SD-WAN

Magic Quadrant Network Firewall “Leader”  
WAN Edge “Leader”

2020 Magic Quadrant for Network Firewalls “Leader”

Figure 1. Magic Quadrant for Network Firewalls



Source: Gartner (November 2020)

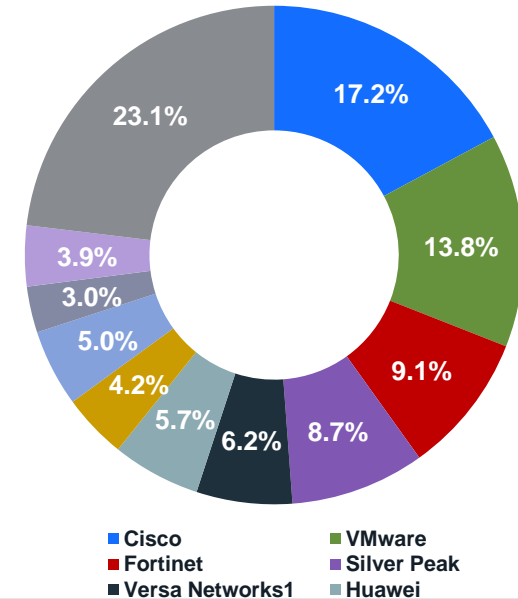
2020 Magic Quadrant for WAN Edge Infrastructure “Leader”

Figure 1. Magic Quadrant for WAN Edge Infrastructure



Source: Gartner (September 2020)

Global Top 3 시장 점유율



Global Top3 시장 점유율

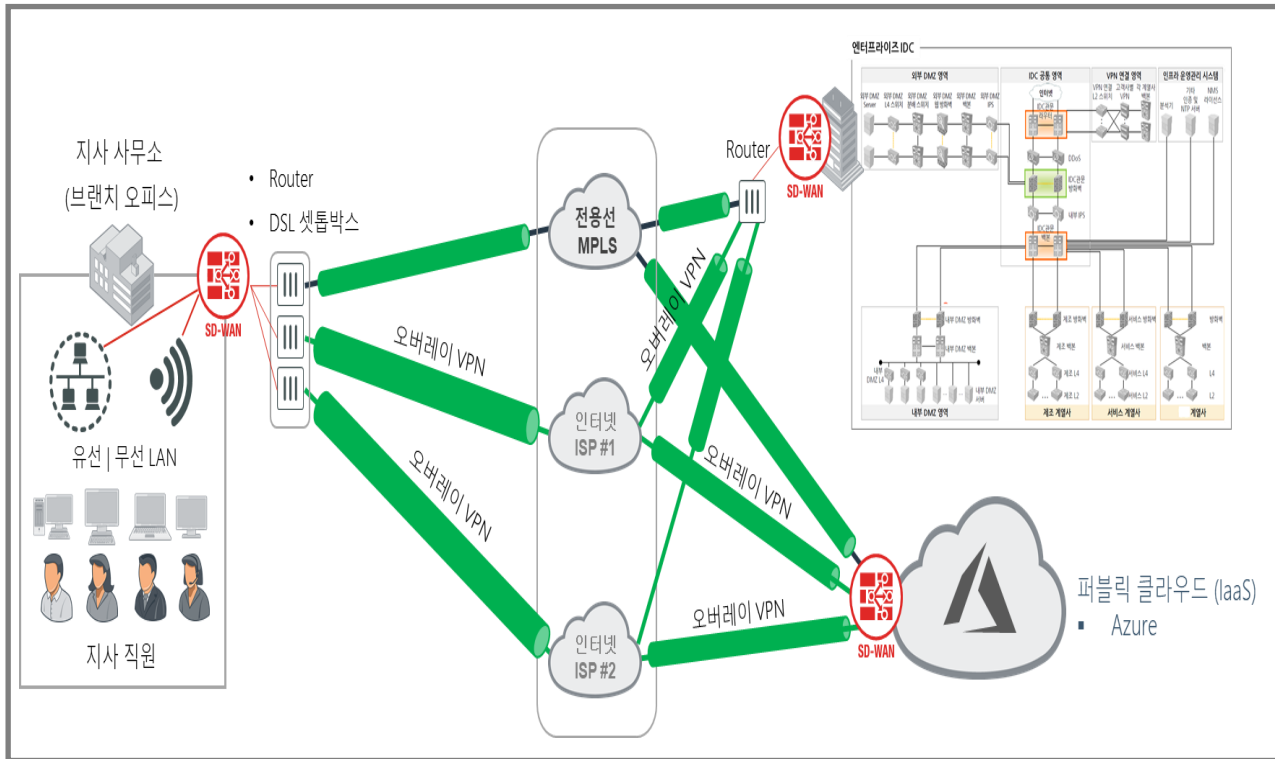
SD-WAN 글로벌 Market 점유율 Top3  
(2019년)

# 포티넷 시큐어 SD-WAN, 시큐어 SD-Branch는

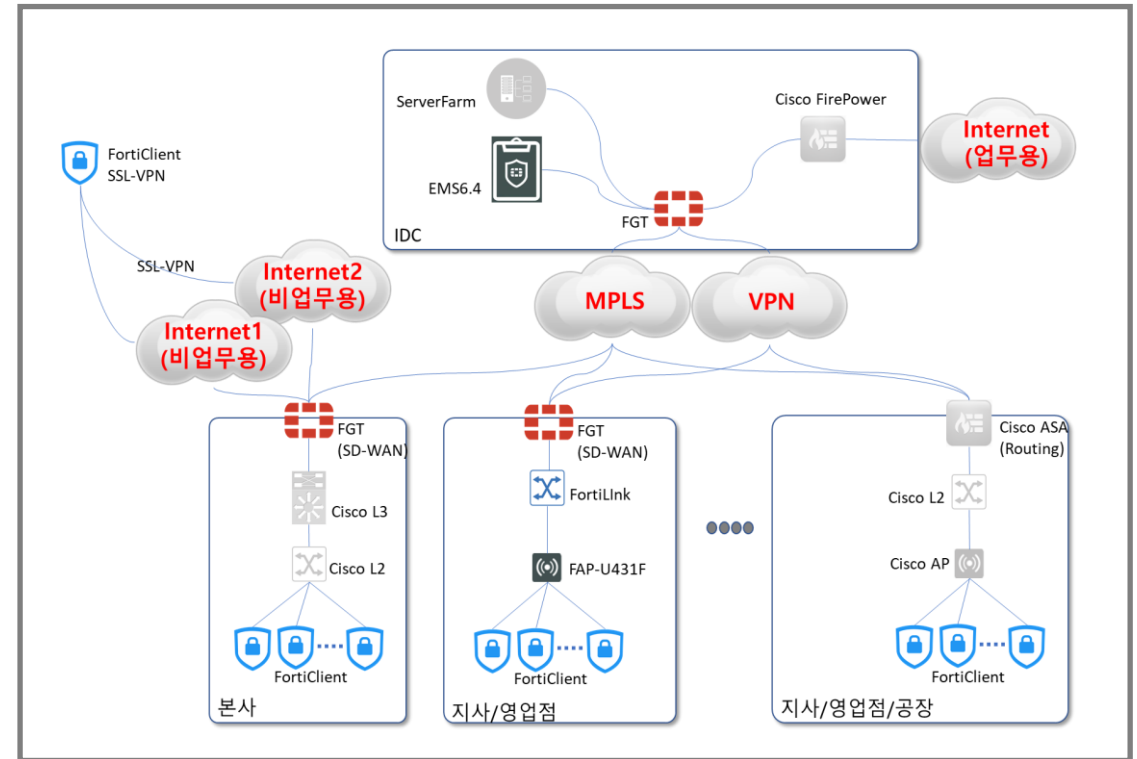
국/내외에서 검증된  
우수한 솔루션

시큐어 SD-WAN : 국내 대기업 사업장  
시큐어 SD-Branch : 국내 제약 그룹사

## Secure SD-WAN



## Secure SD-Branch

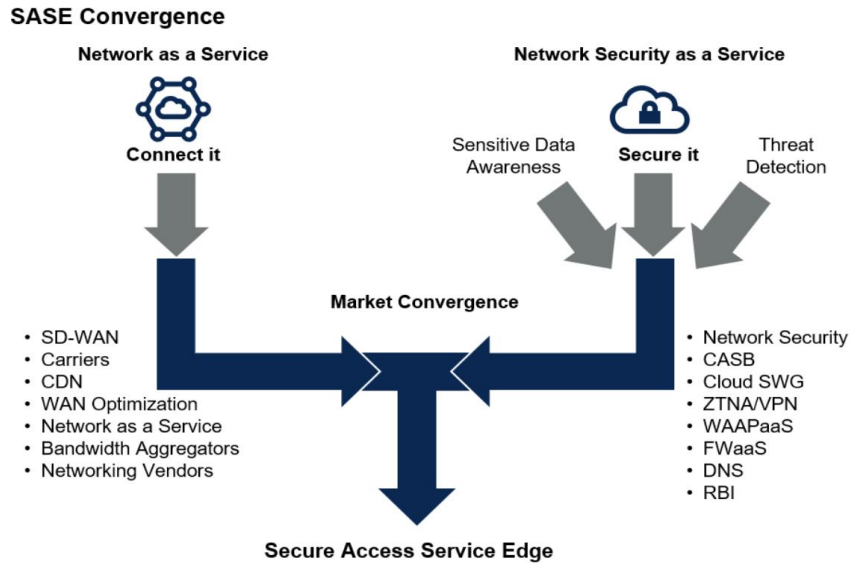


# 포티넷 SASE 솔루션

SASE(새시), Secure Access Service Edge

# SASE (Secure Access Service Edge)

가트너는 SD-WAN, SWG, CASB, DNS 보호, 클라우드 기반 방화벽이 포함된 네트워크 및 보안 서비스를 융합하는 기술 범주를 설명하기 위해 SASE('새시'로 읽음)라는 개념을 소개



CDN: content delivery network; RBI: remote browser isolation; WAAPaaS: web application and API protection as a service.  
Source: Gartner ID: 441737

시큐리티월드 보안뉴스

Home > 전체기사  
떠오르고 있는 보안 전략 새시(SASE), 도입할까 말까?

안택트 시대, 차세대 네트워크 보안 관심 'UP'  
내년까지 기업 60% SDP 도입 예상...프라이빗테크놀로지 등 사업 확장

[아이뉴스24 최은정 기자] '언택트(비대면)' 시대를 맞아 기업 고객들이 강화된 네트워크 기술을 찾으면서 소프트웨어정의 경계(SDP) 등 차세대 네트워크 보안 시장이 주목받고 있다.

14일 업계에 따르면 최근 기업 사이에서 재택근무 등 새로운 업무환경을 더욱 안전하게 보호하기 위한 기술 수요가 늘고 있다.

대표적인 분야가 SDP다. SDP는 가상사설망(VPN)을 대체할 수 있는 기술로, 제로트러스트 개념을 기반으로 허가된 사용자에게만 접근을 허용한다. VPN이 서버 접속 후 인증을 거쳐 내망에 접속한다면 SDP는 인증

보안 / 클라우드 ©2020.06.01

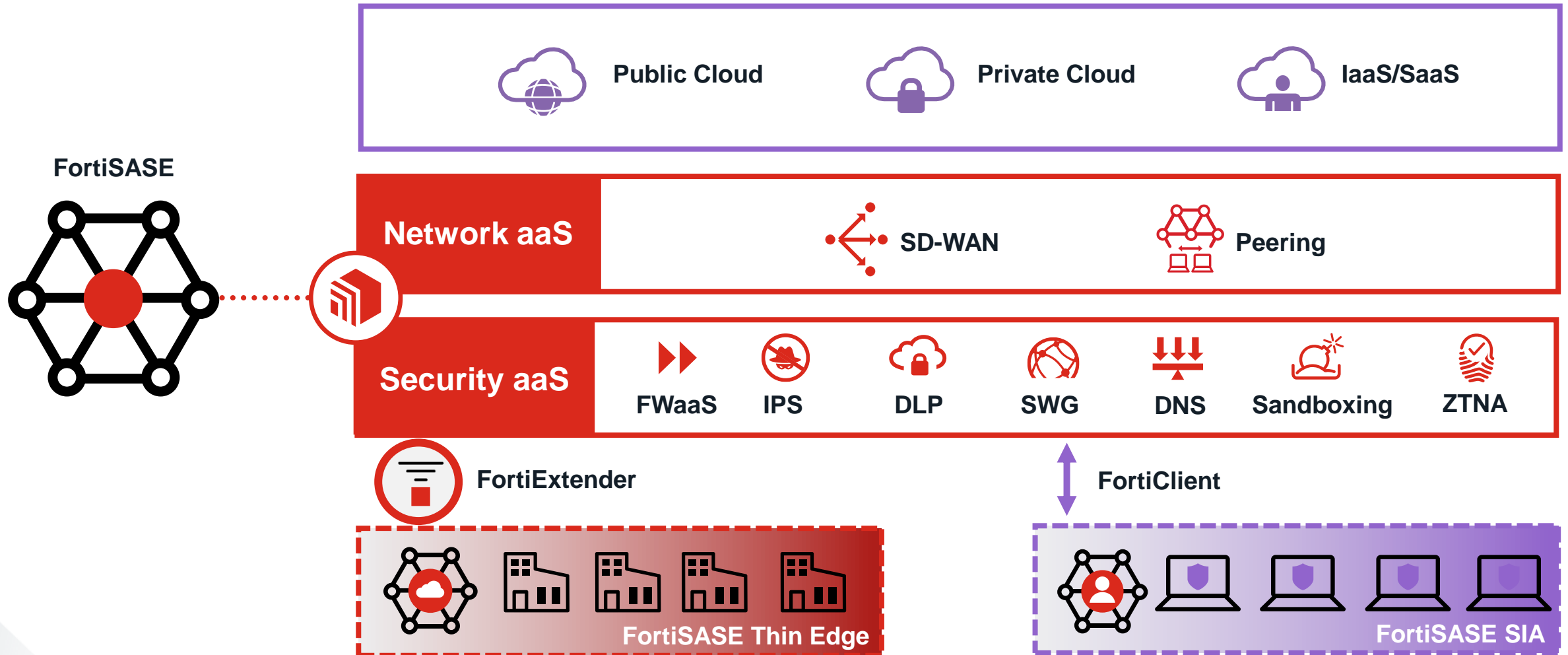
**재택근무를 위한 보안 강화 대책으로 주목받는 SASE**

Maria Korolov | CSO

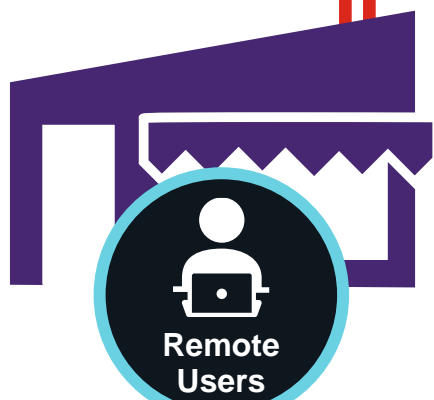
코로나19 팬데믹으로 SASE(Secure Access Service Edge)를 원래 계획보다 조기에 도입하는 기업이 늘고 있다.

가트너는 지난 여름 기업의 SASE 도입 비율을 1% 미만으로 추산하면서 SASE 기술이 주류가 되기까지는 5~10년이 걸릴 것으로 예측했다. 그러나 가트너 애널리스트 존 윌러에 따르면, 현재 SASE는 가장 많은 관심을 끄는 분야 중 하나다.

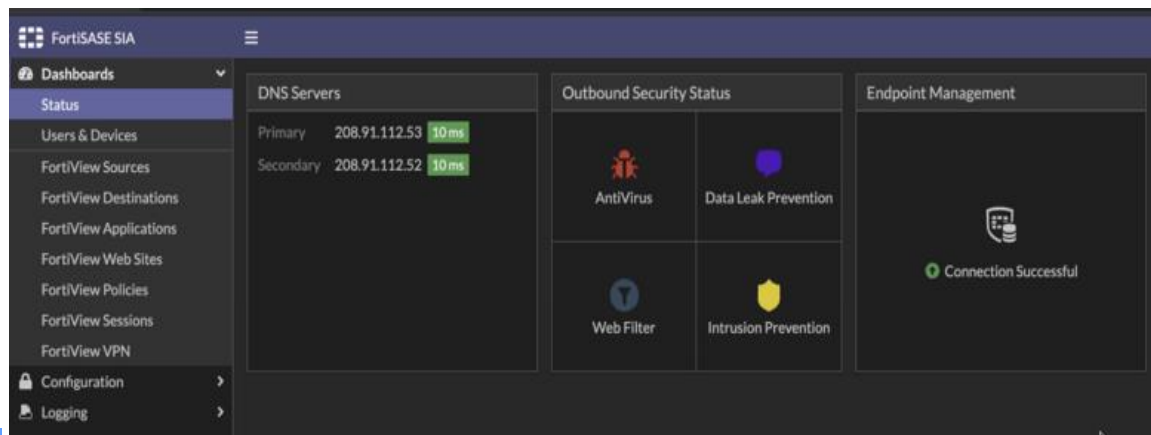
# FortiSASE Thin Edge and SIA



# FortiSASE Secure Internet Access (SIA)



Windows, Mac, Linux



## Zero Trust Security

- Zero Trust Agent
- Central Management vis EMS
- Dynamic Security Fabric Connector
- Vulnerability Agent & Remediation
- SSL / IPSEC VPN with MFA
- USB Device Control
- Automated Endpoint Quarantine
- Application Inventory

## Cloud Based Endpoint Security (SASE)

- SSL Inspection
- Inline AV & Anti-Malware
- Intrusion Prevention (IPS)
- FortiGuard Web Filtering
- Application Firewall
- Data Leak Prevention

## Additional Services

- 24 x 7 Support
- SASE Cloud Management
- SASE Cloud Logging
- Best Practice Onboarding Service

# FortiSASE SIA



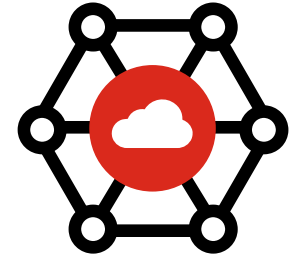
## Security Everywhere

클라우드 NGFW, Web 보안,  
IPS, DLP, SWG, DNS, ZTNA,  
샌드박스 간의 원활한  
오케스트레이션 제공



## Fabric Integrated

포티넷 시큐리티 패브릭의  
일원으로써,  
FortiOS를 통한 엔터프라이즈  
레벨의 보안 장점 극대화

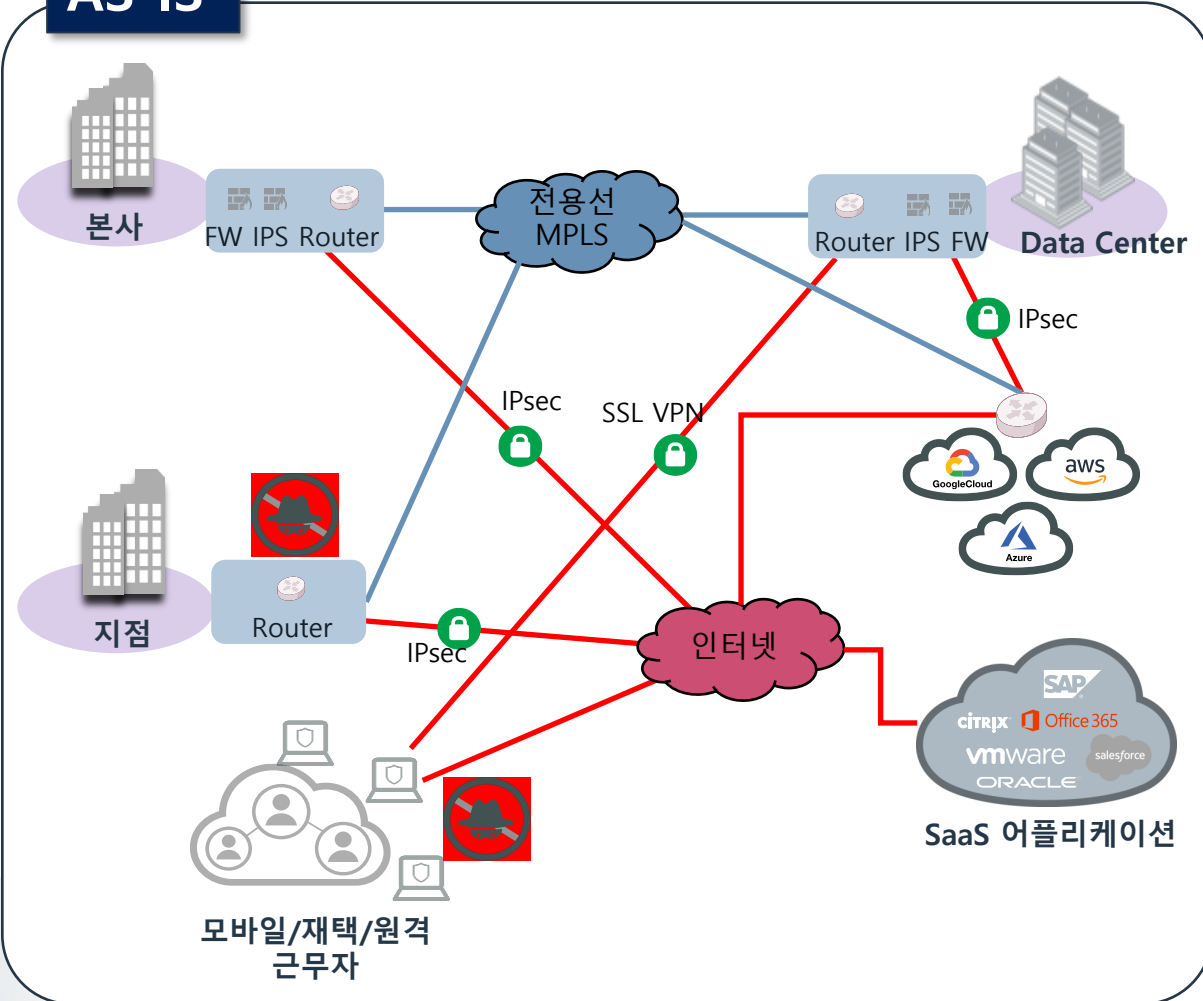


## Work from Anywhere

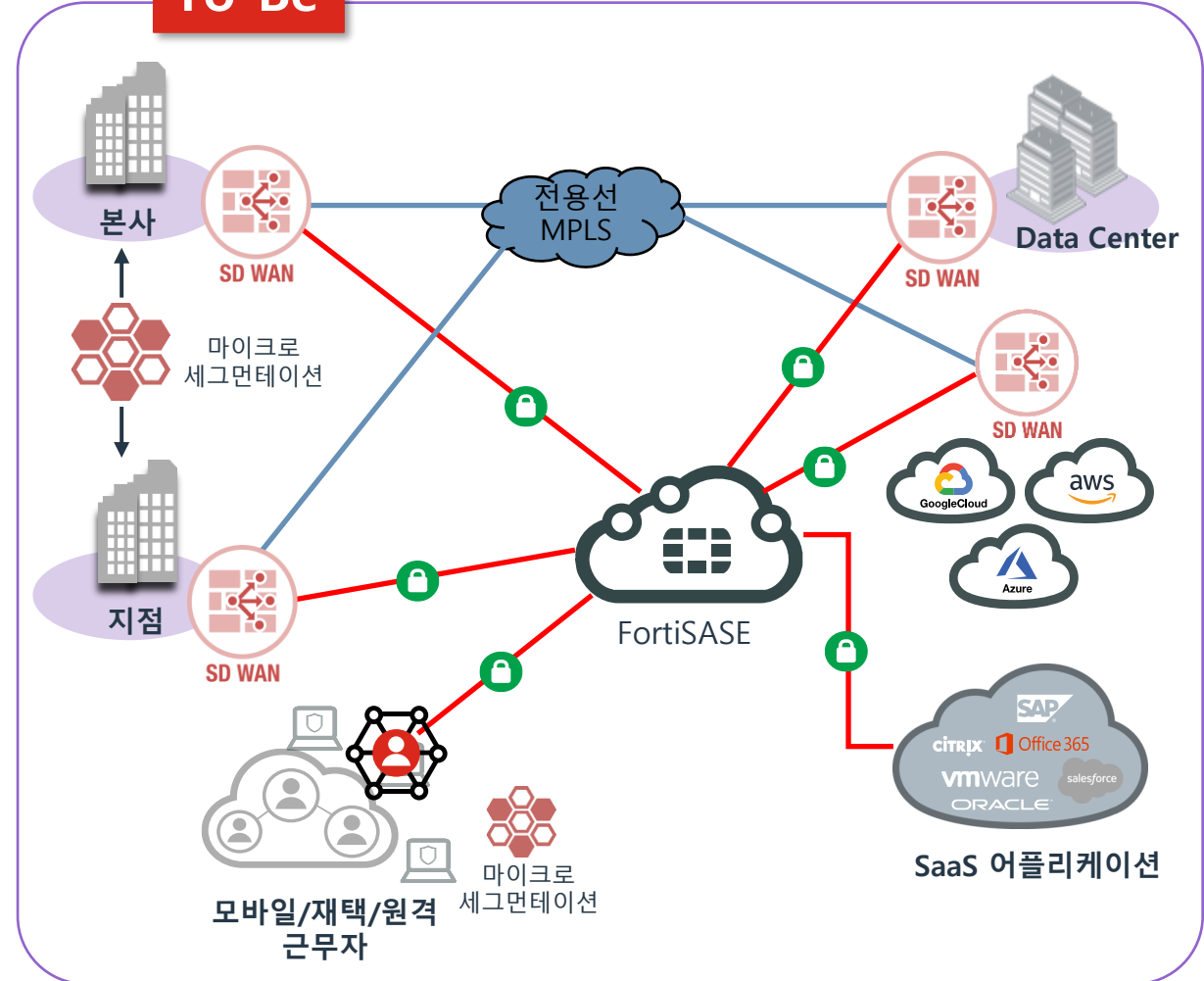
LTE, 5G를 통한 Thin Edge  
및 클라이언트 단위로  
심플한 배포와 관리 등  
유연성 제공

# SD-WAN + SASE (사용자 환경에 따라 최적의 솔루션 제공)

## AS-IS



## To-Be



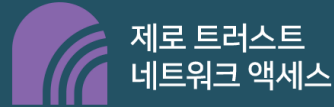


# Summary

- 포티넷은 Secure SD-WAN과 SASE 솔루션을 통하여 최상의 온-프레미스 + 리모트 접근 보안 포트폴리오를 제공합니다.
- 지방/글로벌 지점 보안과, 원격 & 모바일 사용자 보안을 모두 달성
  - 지방/글로벌 Secure SD-WAN 인프라 구축 시간과 비용 절감
  - 일관된 정책 유지관리와 업무 만족도 증가
  - 원격 & 모바일 사용자에게도 Enterprise 레벨의 보안을 편리하고 일관되게 적용

# 포티넷 CBC 고객 솔루션 체험 센터

전세계 TOP3 사이버 보안 벤더인 포티넷에서  
국내 고객 분들을 위해 마련한 솔루션 체험 센터로  
방문하시는 고객 분들의 요구사항에 따라 맞춤형 컨설팅을 제공합니다.



## ❖ 포티넷에 방문해야 하는 이유는 무엇일까요?

- 고객사의 디지털 트랜스포메이션에 필요한 IT보안 요구 사항을 알아보고 최적의 해결 방안을 제시합니다.
- 고객의 비즈니스 목표에 맞추어 당사 기술 전문가와 1:1 맞춤 컨설팅이 가능합니다.
- 축적된 수많은 레퍼런스로 고객의 다양한 상황에 맞는 완벽한 보안 솔루션을 제공합니다.
- 보안 솔루션을 시각적으로 확인할 수 있는 라이브 데모를 직접 체험할 수 있습니다.



CBC 방문 신청하기



CBC 소개 영상 보기

포티넷 CBC는 언제나 여러분께 열려있습니다.  
지금 방문 신청해주세요!



**FORTINET**®