Appgate SDP

소프트웨어 정의 경계 기반의

제로 트러스트 네트워크 액세스 솔루션

appgate

제로 트러스트,

실질적 구축 방법을 찾아야 할 때 입니다.

목차

제로 트러스트

Zero Trust란 무엇인가?

appgate

[제로 트러스트] 개념 정의

- **“누구도 믿지 말고, 계속 검증하라”는 새로운 보안 개념**
- **물리적 위치, 네트워크 위치, 접속장치에 따라 사용자와 단말에 부여된 암묵적인 신뢰는 없다는 전제로 보안 정책 수립**

  - ➢ 모든 액세스 요청자(사람,기기,리소스등)의 Identity에 대한 철저한 사전 검증 요구
  - ➢ 액세스 허용 뒤에도 지속적인 상태 모니터링
  - ➢ 모니터링 결과 정책 위반 행위 발견 시 실시간 통제

[제로트러스트] 급격한 IT 환경 변화

- **레거시 보안 모델로는 IT 환경 변화에 효과적 대응에 한계**

  - ➢ 개인용 디바이스 업무 활용 확대 : 기업 관리자가 통제하기 어려움
  - ➢ 원격 근무의 보편화 : 어디에서나 기업망에 액세스 가능한 환경 요구
  - ➢ 기업 데이터 분산 가속화 : Data Center, Private & Public Cloud로 분산
  - ➢ 공격 방식의 정교화 : 공격 방식의 진화
  - ➢ 내부자에 의한 공격 증가 추세 : 내부 네트워크에 대한 암묵적 신뢰 불가

[제로트러스트] 필요성

- **네트워크 경계 중심의 기존 보안 패러다임에 대한 한계 인식**
  - 네트워크 경계선 방어 ➔ 사용자 / 자산/ 자원 중심의 방어 필요
- **'신뢰할 수 있는 네트워크'라는 개념이 없어짐**
  - 기업망 내부는 신뢰할 수 있다는 가정이 무너짐
  - 접속하는 네트워크 위치에 따라 보안 상태를 결정 할 수 없음
- **모든 사용자, 기기 및 네트워크 트래픽에 대한 암묵적 신뢰 불가**
  - 모든 사용자와 기기의 액세스는 반드시 철저한 사전 인증 필요

[제로트러스트] 핵심 원칙

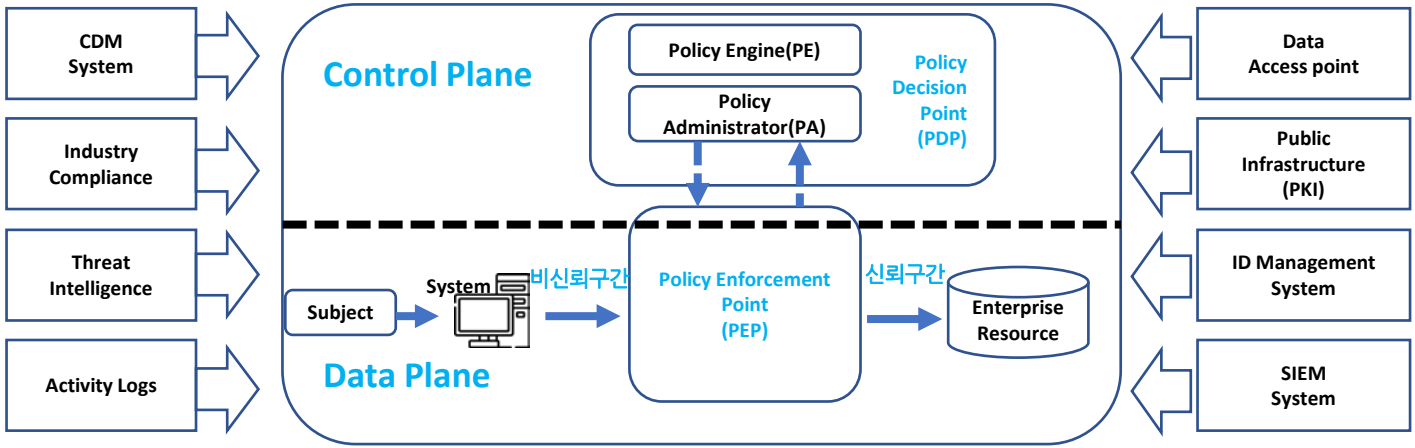
제로 트러스트 보안 철학을 구현하기 위한 3가지 핵심 원칙

- **인증 강화**
  - ID/PW 이외의 추가 인증 수단 요구 : 다중 요소 인증, 디바이스 인증
- **마이크로 세그먼테이션**
  - 서버, 컴퓨팅 서비스 등을 작은 단위로 분리하여 액세스 통제
- **소프트웨어 정의 경계**
  - 소프트웨어기반으로 보호 대상을 분리.보호할 수 있는 경계 생성

[제로트러스트] 기대 효과

- **사용자 자격 증명 도용 대응**
  - 사용자 자격 증명(UID/Password) 뿐만 아니라 기기에 대한 강력한 인증 요구
  - 자격 증명 이후에도 지속적인 모니터링, 정책위반시 적절한 통제
- **원격 공격 혹은 내부자 위협 대응**
  - 사용자 및 기기 자격증명, 마이크로 세그멘테이션을 통해 횡적 이동 차단
  - 보안정책, 사용자 역할, 기기의 속성에 따라 데이터 접근 통제
  - 사용자 단말에 대한 지속적 모니터링, 비정상 활동 시 추가 인증 요구 또는 접근 권한 회수
- **공급망 침투 대응**
  - 모든 사용자와 기기를 기본적으로 신뢰하지 않는다는 가정에서 출발
  - 데이터에 대한 엄격한 접근 제어, 액세스 허용 시 최소 권한 원칙 적용
  - 네트워크 세분화, 사용자 단말 보안 상태 지속적 모니터링, 비정상 활동에 대한 적절한 대응

[제로트러스트] 아키텍처



Core Zero Trust Logical Components – NIST SP 800-207

Control Plane과 Data Plane 분리

- Control Plane : PDP(Policy Decision Point) : PE, PA
- Data Plane : PEP(Policy Enforcement Point)

appgate

[제로트러스트] 아키텍처 구성 요소

- 정책 결정지점(PDP, Policy Decision Point)
  - 정책엔진(PE, Policy Engine)
    - 액세스 주체(User,Device등)가 리소스에 액세스할 수 있을지를 결정하는 역할
  - 정책 관리자(PA, Policy Administrator)
    - 액세스 요청자와 리소스간 세션의 생성.폐쇄를 PEP에 지시하는 역할

- 정책 시행지점(PEP, Policy Enforcement Point)
  - 액세스 주체와 리소스 사이의 세션 연결 및 종료를 담당
  - 결정된 정책을 실행하는 역할

SDP & ZTNA

제로 트러스트 구축, 시작은 ZTNA에서 부터

appgate

[SDP & ZTNA] 개념 정의

- **SDP : Software Defined Perimeter**
  - CSA(Cloud Security Alliance)의 제로 트러스트 원칙을 구현한 보안 아키텍처
  - 보호 대상 리소스 주변에 소프트웨어 기반 가상 경계(Perimeter) 구현
  - ID(Identity) 중심의 액세스 제어
  - 정책 결정지점(PDP)과 정책 실행지점(PEP)의 분리
  - 사용자와 액세스 대상 리소스간의 일대일 연결을 동적으로 생성

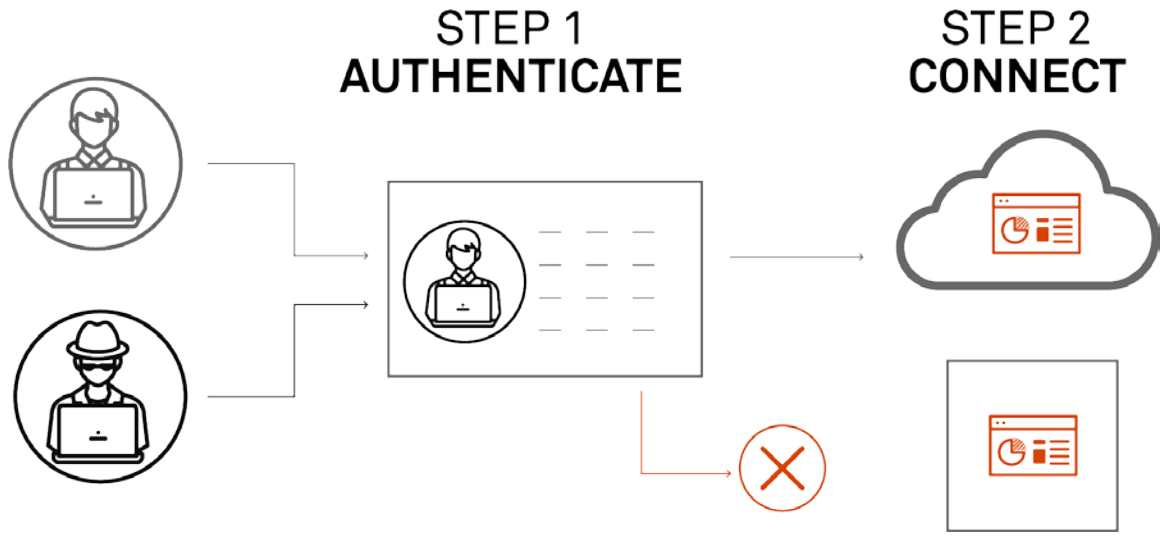
- **ZTNA : Zero Trust Network Access**
  - SDP 기술을 사용한 네트워크 액세스 아키텍처
  - SDP와 같은 의미로 호환

[SDP & ZTNA] 핵심 원칙 3가지

- Identity 중심
  - 사용자 Identity를 중심으로 한 보안 설계
  - 네트워크 액세스 권한을 부여하기 전에 사용자/디바이스 인증이 필수
- 제로 트러스트 원칙 적용
  - 네트워크 액세스 허용 시 최소 권한 원칙 적용
  - 권한 없는 사용자에게 리소스 노출 차단
  - 마이크로 세그멘테이션
- 클라우드 중심
  - 클라우드(Public, Private, Hybrid) 아키텍처에 작동하고, 클라우드처럼 확장성 있도록 설계

[SDP & ZTNA] 동작 방식

- 선 인증, 후 연결 : 사전 인증없이 액세스 불가
  - ➢ 사용자 신원 확인, 디바이스 상태 평가



[SDP & ZTNA] 제로 트러스트 실제 구축은 어디서 부터?

- **제로 트러스트 구축 이니셔티브 2가지**
  - **ZTNA(제로 트러스트 네트워크 액세스)**
    - Front-end 애플리케이션 세분화
    - 사용자와 애플리케이션(User-to-Application)간 연결 세분화 역할
    - 견고한 Identity 기반이 필수적으로 요구됨
  - **Micro-segmentation(마이크로 세그멘테이션)**
    - Back-end 네트워크 세분화
    - 워크로드간 통신(Workload-to-Workload) 세분화 역할
    - 견고한 Identity 기반이 필수적으로 요구됨

[SDP & ZTNA] 적용 시 장점

- 접근 통제 강화 및 단순화
- 공격 표면 노출 감소
- 정책관리 복잡성 제거
- 최종 사용자 경험 개선
- 통합 및 자동화를 통한 원활한 운영

Appgate SDP

ZTNA 솔루션 분야의 글로벌 리더

appgate

[Appgate SDP] ZTNA 분야의 글로벌 리더

- **Appgate(www.appgate.com)** 사의 **ZTNA** 솔루션
- **CC** 인증을 받은 유일한 **SDP** 기반 **ZTNA** 솔루션
- 미 국방성 산하 기관을 비롯한 정부기관 및 글로벌 기업 채택

Forrester New Wave:
Zero Trust Network Access, Q3 2021

COMMON CRITERIA CERTIFICATION

Secure critical infrastructure with Common Criteria-certified Appgate SDP.

COMMON CRITERIA

Gartner

REPRESENTATIVE VENDOR - ZTNA MARKET GUIDE
GARTNER PEER INSIGHTS: 4.8 OF 5 STARS*

NIST

ZERO TRUST ARCHITECTURE
SP800-207
SELECTED TO COLLABORATE WITH NCCoE

appgate

[Appgate SDP] SDP 원칙 모두 수용

- **소프트웨어 정의 경계(SDP) 기반의 ZTNA 솔루션**
- **CSA(Cloud Security Alliance)의 SDP 3가지 핵심 원칙 준수**
  - ➢ **신원중심(Identity-Centric)**
    - 사용자 또는 장치별로 다차원 프로필 구축, 액세스 권한 부여전에 사용자 인증
  - ➢ **제로 트러스트 모델**
    - 네트워크 액세스시 최소권한 원칙 적용
    - 공격 표면을 완전히 줄여 줌
  - ➢ **클라우드 중심(Cloud-Centric)**
    - 클라우드 환경(Public, Private, Hybrid)을 완벽하게 지원하고
    - 클라우드처럼 완전한 분산 운영 및 확장성을 제공하는 아키텍처

[Appgate SDP] 하이브리드 인프라 환경에 적합

- 온-프레미스 및 멀티 클라우드 환경 동시 지원
- Identity 중심의 Micro-Perimeter - 리소스에 대한 세밀한 액세스 제어
- 단일패킷인증(SPA)기술 - 보호 대상 리소스의 외부 노출 차단
- 강력한 API 제공 - 주변 보안 시스템과 보안 생태계 구축
- 멀티 사이트/리소스 동시 액세스 - 특허기반의 Multi-tunnel 기술
- 액세스 디바이스 보안 상태 확인 - 위험한 장치의 액세스 제한

[Appgate SDP] 핵심 기술(1/2)

- **단일 패킷 인증(SPA, Single Packet Authorization)**
  - SPA 보안 기술을 통해 검증된 사용자만 시스템과 통신 허용
  - 검증되지 않은 사용자에게 내부 인프라 노출 차단 및 공격 표면 감소
  - Controller와 Gateway는 외부 공격자가 탐색, 스캔 또는 공격 불가
- **실시간 권한 부여(Live Entitlement)**
  - 사용자와 디바이스 상황을 반영한 동적 액세스제어
  - 정적(Static) 액세스 규칙 ➔ 실시간 사용권한(Live Entitlement) 방식
  - 사용자가 언제, 어디에서 무엇을 하는지에 따라 보안 정책의 동적 변경 적용

[Appgate SDP] 핵심 기술(2/2)

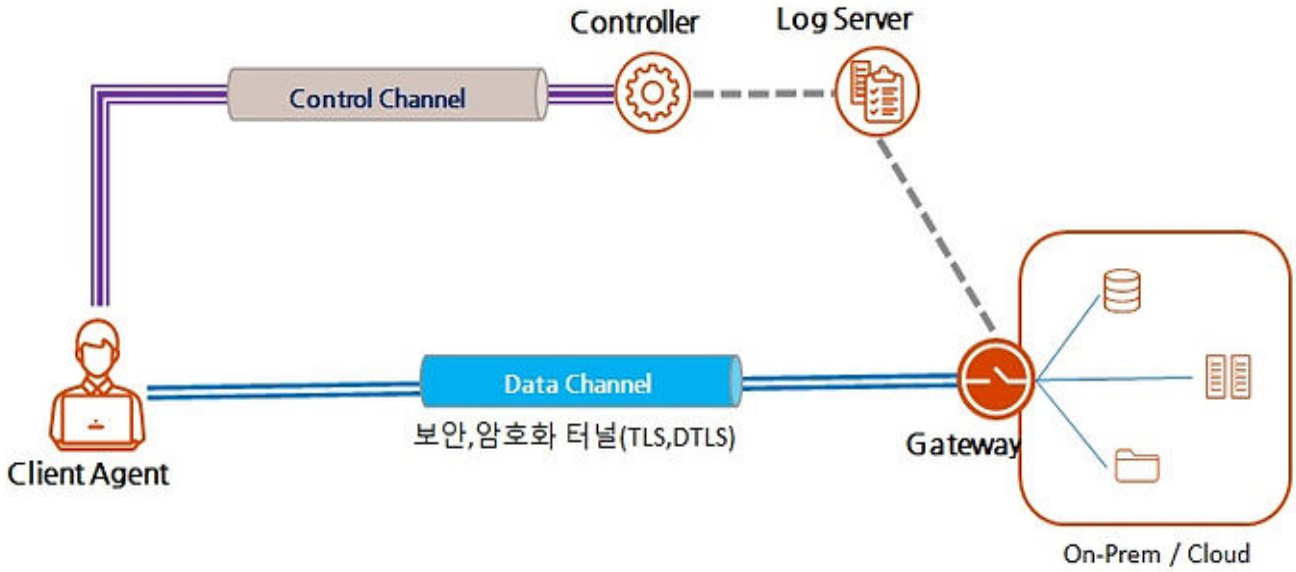
- **마이크로 세그먼트(Micro-Segment)**
  - 세분화되고 개별화 된 액세스 제어
  - 정책에 대한 실시간 이해를 바탕으로 각 사용자별 개별화 된 경계 생성
  - 권한이 부여되면 암호화된 터널(하나의 세그먼트)을 통해 특정 리소스로만 트래픽이 흐르도록 통제
- **횡간 이동 차단(Ringfence)**
  - 무단 액세스로 부터 사용자 디바이스 보호
  - 보호된 리소스와 사용자 장치에 대한 모든 Inbound 연결 차단
  - 로컬 네트워크의 악의적인 사용자에 대한 우려없이 내부 리소스에 대한 액세스 권한 부여
- **멀티 터널링(Multi-tunneling)**
  - Client Agent와 복수의 Gateway 동시 세션 연결 지원
  - 특허 기술 기반의 멀티 사이트 동시 연결

[Appgate SDP] 구축 방식

- **고객 자체 구축형**
  - ➢ 고객이 관장하는 Cloud 또는 On-Premise에 Appgate SDP 설치 및 운영
  - ➢ Controller, Gateway등이 모두 고객사의 시스템에 구축되고 운영

- **서비스형**
  - ➢ Appgate사에 제공하는 SDP 플랫폼 서비스를 이용하는 방식
  - ➢ Controller는 Appgate사에서 운영하는 클라우드 플랫폼에서 운영
  - ➢ Gateway는 고객사의 보호 대상 리소스가 있는 Site에 설치되고 운영

[Appgate SDP] 핵심 구성 요소

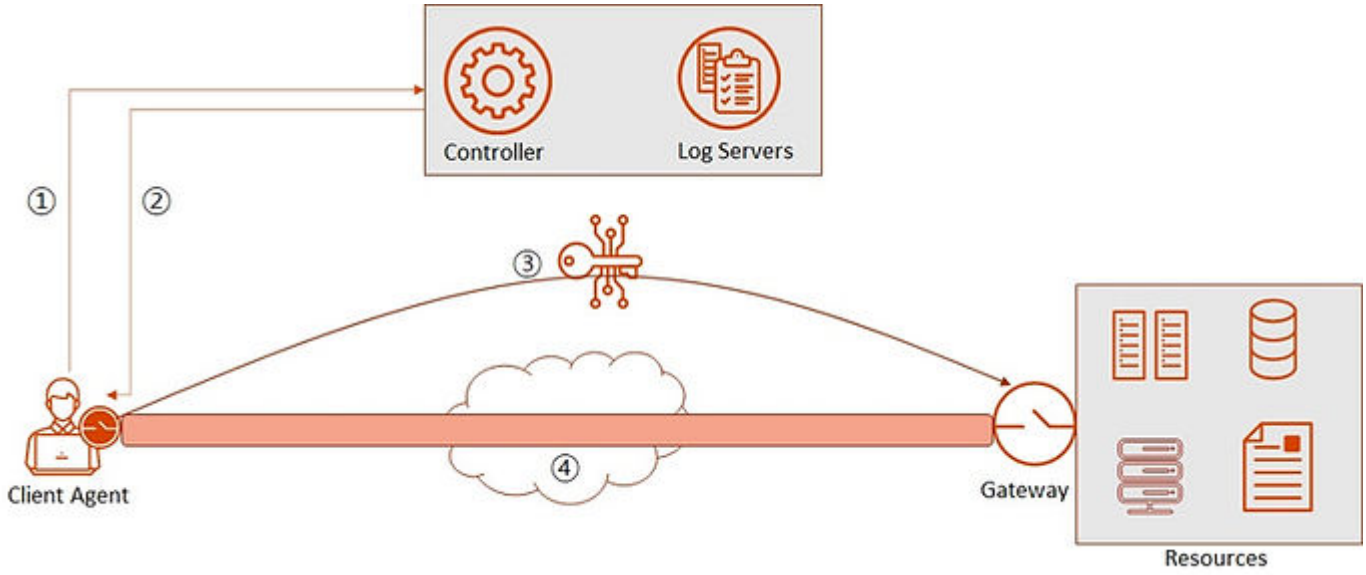


구성 요소 : **Client, Controller, Gateway, LogServer**

[Appgate SDP] 구성 요소별 역할

- **Client Agent**
  - 사용자 디바이스에 설치되는 Agent 소프트웨어
  - 디바이스 Context 수집, 인증 및 액세스 요청
- **Controller**
  - ➢ 정책 결정 지점(PDP), 정책 엔진(Policy Engine) 역할
  - ➢ 사용자, 장치, 워크로드에 대한 액세스 권한 부여,인증, 정책,조건 및 권한 관리 담당
- **Gateway**
  - ➢ 정책 실행 지점(PEP)
  - ➢ 부여된 권한을 기반으로 세션별 마이크로 방화벽 또는 마이크로 경계 동적 구축
- **Log Server**
  - Controller 및 Gateway 감사 로그 저장

[Appgate SDP] 동작 순서



[Appgate SDP] 동작 순서

① **Client** : **SPA(단일패킷인증)** 기술을 사용하여 Controller에 액세스 요청

② **Controller** : 인증 후 Client에 적합한 **자격 증명 토큰(Entitlement Token)**제공

③ **Client** : Controller로부터 받은 자격 증명 토큰을 Gateway에 전달

④ **Gateway** : 자격 증명에 따라 사용자에게 적합한 정책을 적용,

사용자(Client)와 리소스간 1:1 마이크로 세그먼트 세션 생성

⑤ **Controller** : 세션 형성 후에도 사용자 환경 **지속적 모니터링,**

환경 변화 시 변화된 환경에 따라 동적으로 정책 적용

SPA 패킷이 없는 클라이언트는 Appgate SDP에 접속 불가

appgate

[Appgate SDP] 단일패킷 인증(SPA) 기술

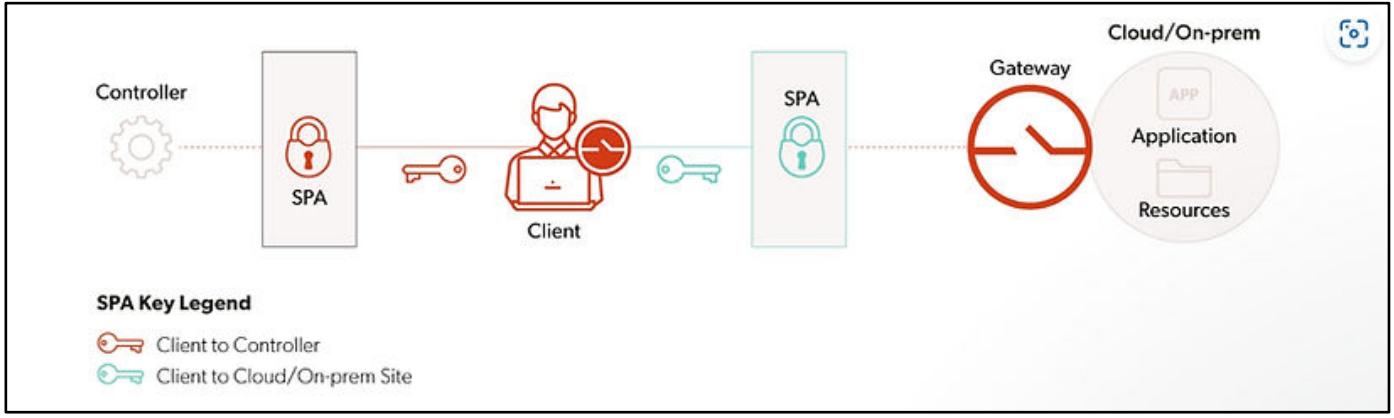
- SPA(Single Packet Authorization, 단일패킷인증)
- 하나의 암호화된 데이터 패킷(Single Packet)에 사용자와 디바이스에 관한 정보를 전달하고 액세스를 요청하는 인증 프로토콜
- 유효한 SPA 패킷이 전달되지 않으면 액세스에 필요한 네트워크 포트는 외부에 노출되지 않고, 따라서 서비스가 외부에 노출되지 않음
- Appgate SDP의 핵심 차별화 요소 중 하나
- 표준 SPA 기술에 Appgate 자체의 보안 기술 추가 적용

appgate

[Appgate SDP] 표준 SPA 대비 높은 보안성

1. Unique Key 활용 (통신 상대 별로 각기 다른 KEY 사용)

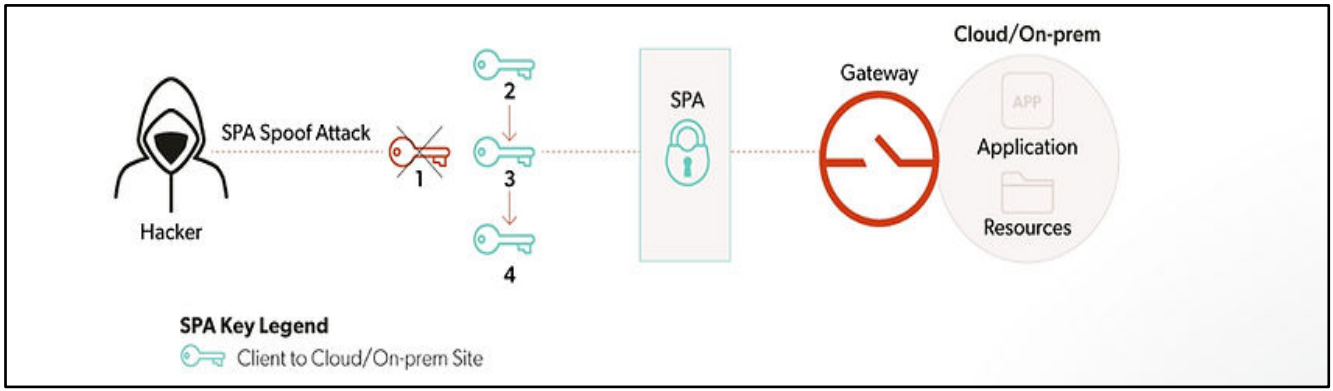
- 통신 상대 별로 각기 고유의 KEY를 사용하는 보호 키 시스템 채택
- 즉, Client<-->Controller, Client<-->Gateway 및 Controller-Gateway간 각기 다른 Key 사용



[Appgate SDP] 표준 SPA 대비 높은 보안성

2. Revolving Key 할당(Spoofing 방지)

- 일반적인 SPA와 달리 고정 Key를 사용하지 않고, 수 초 간격으로 새로운 Key 할당
- 스푸핑 된 SPA 패킷은 더 이상 유효하지 않기 때문에 액세스가 거부됨

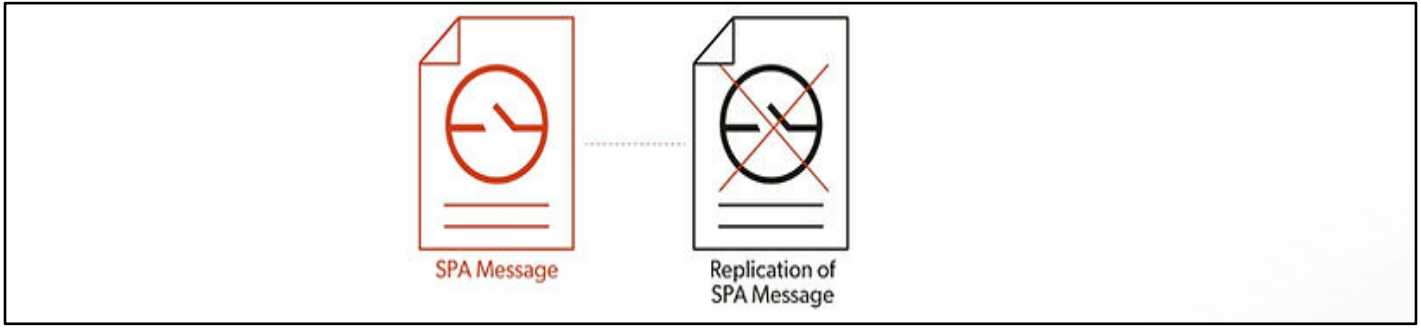


appgate

[Appgate SDP] 표준 SPA 대비 높은 보안성

3. 복제 방지

- Appgate SDP의 SPA 메시지는 독자 기술로 특수한 방식으로 제작됨
- 악의적 사용자가 복제하거나 재생성 할 수 없음

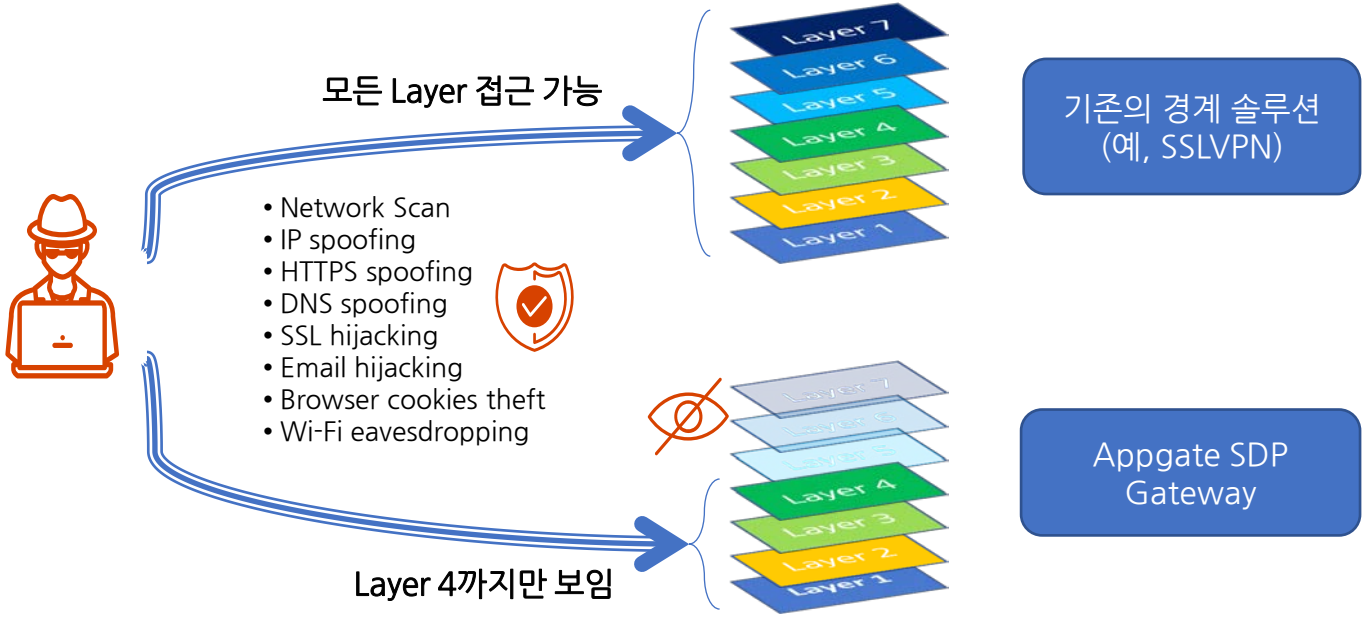


[Appgate SDP] 특장점

- **접속 게이트웨이 은폐 (선 인증, 후 연결)**
  - ➢ 보이지 않는 것은 공격할 수 없다는 원칙 활용
  - ➢ SPA(싱글패킷인증)을 통한 게이트웨이등의 Network Access Port 노출 방지
  - ➢ Port Scan에 노출되지 않으며, SPA 메시지는 암호학적 해시를 통해 추가로 보호 됨
  - ➢ Gateway와 Controller는 완전히 은폐되어 탐색, 스캔 또는 공격을 받지 않음
  - ➢ 네트워크 정찰을 방지하고 네트워크내 측면 이동을 제한하여 네트워크 공격 표면을 크게 줄여 줌

[Appgate SDP] 특장점

- **VPN과 같은 기존의 솔루션과 달리 L4까지만 외부에 보여짐**

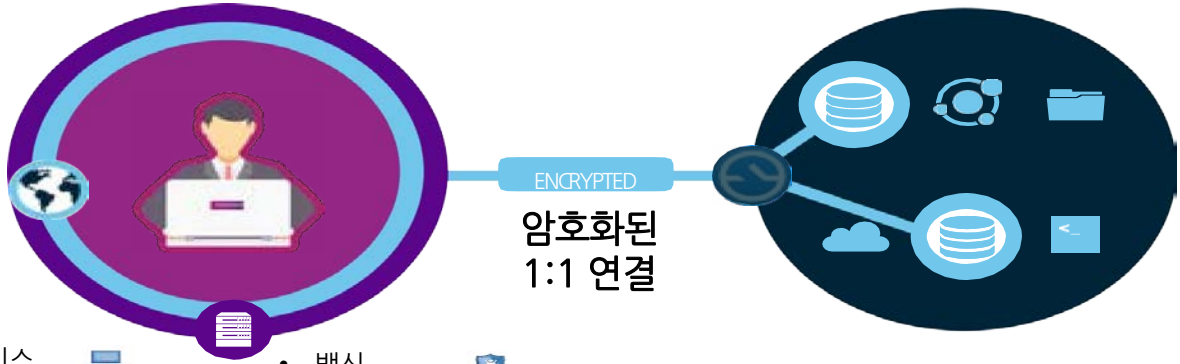


[Appgate SDP] 특장점

- 사용자 중심의 보안 정책
  - Identity 중심의 액세스 권한 설정
  - 디바이스 및 접속 환경에 따라 일회성 정책 권한 부여
  - 접근 대상 자원에 대해 IP, Hostname, Domain , Cloud Service Resource, Script등의 동적 정보에 따른 설정 가능
  - 최소 접근 권한 원칙 적용
  - ID 관리 시스템 및 MFA 연동

[Appgate SDP] 특장점

- 사용자 중심의 보안 정책



- 디바이스
- 인증 방식
- 위치
- 시간

- 백신
- 애플리케이션
- 소속 그룹
- 커스텀 속성

- IP
- Hostname
- HTTP URL 주소
- Cloud 리소스 명 /그룹

- Script 기반 동적 리소스

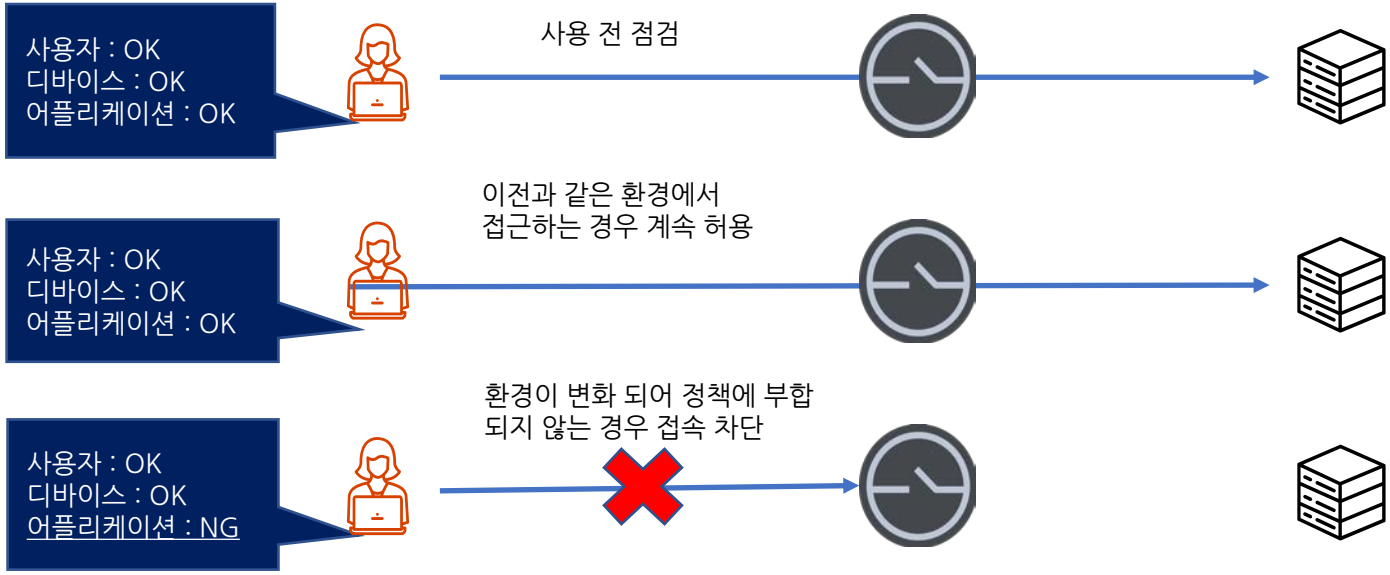
+ 서비스 Port

[Appgate SDP] 특장점

- **지속적 모니터링**
  - ➢ 세션 활성화 후에도 환경 변화 지속적 모니터링
  - ➢ 사용자 Context 변화에 따른 동적 대응
  - ➢ 필요한 액세스 권한을 필요한 시간 동안만 부여
  - ➢ 주요 내부 리소스에 대한 주기적 재 인증 또는 암호 재입력 요청
  - ➢ 접속 환경의 위험도 및 접속 디바이스 정보에 기반하여 적용
  - ➢ 일관성 있는 자동화 정책 수립 가능

[Appgate SDP] 특장점

- 환경 변화에 따른 동적 정책 적용



[Appgate SDP] 주요 용도

- 원격 근무 직원의 액세스 관리
- 복수의 클라우드 플랫폼에 대한 액세스 관리
- 외부 파트너 등의 내부 시스템 액세스 관리
- 온-프레미스 사용자의 내부 리소스 액세스 관리
- 클라우드 마이그레이션시 활용
- MPLS 트래픽 전환
- SD-WAN 필요성 제거
- NAC 대체

appgate

Appgate SDP 구축 모델

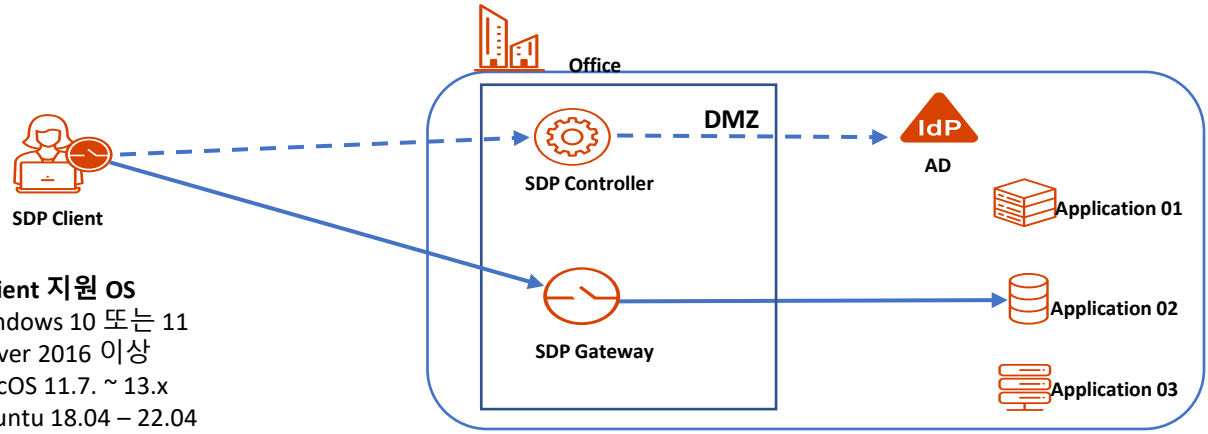
On-Premise / Cloud
Single-Site / Multi-Site

appgate

[구축 모델] 검증을 위한 PoC 환경 구축

다음 절차를 통해 간편하게 PoC 환경 구축 가능

- SDP Appliance 설치 : Hypervisor 또는 Cloud Platform
- IdP연동 및 SDP 구성
- SDP Client를 이용한 액세스



SDP Client 지원 OS

- Windows 10 또는 11
- Server 2016 이상
- macOS 11.7. ~ 13.x
- Ubuntu 18.04 – 22.04
- Fedora 36 이상
- RHEL 8
- iOS
- Android

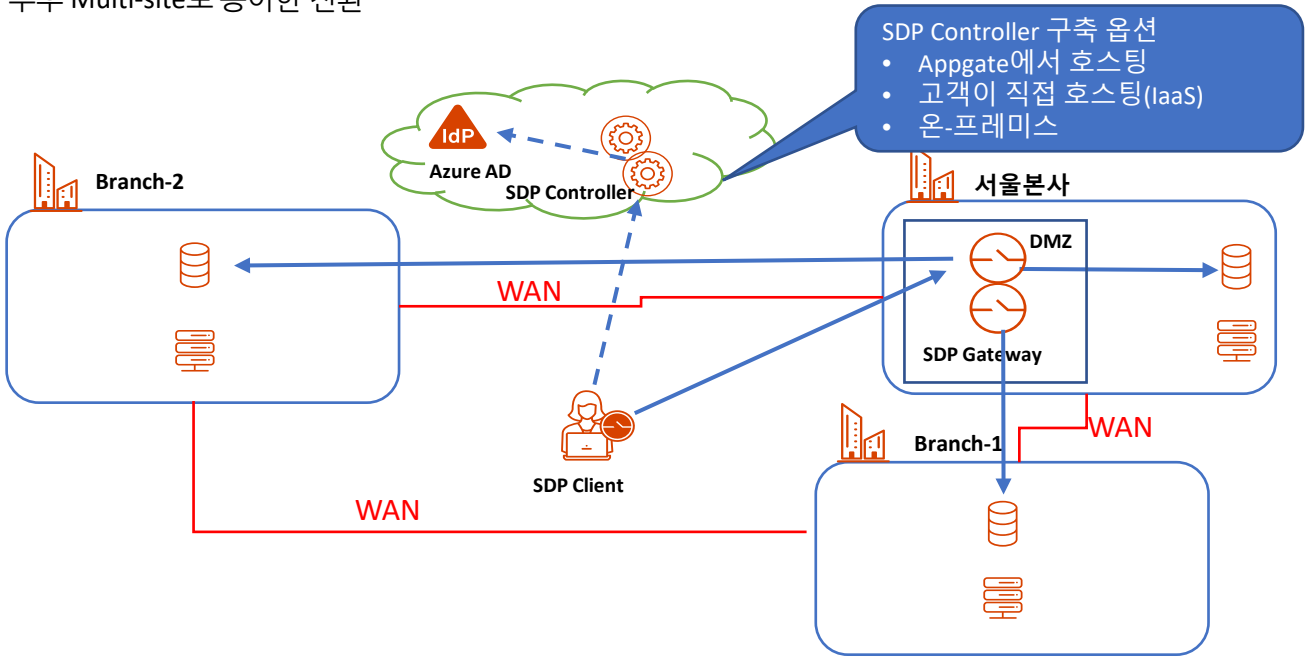
Virtual Machine

VMware ESX v7이상, KVM, MS Hyper-V, Citrix Hypervisor (7.4 or higher), Agent, Nutanix AHV, Oracle VirtualBox, VMware workstation

[구축 모델] VPN 대체 모델

Single-site 구성

- 네트워크 액세스 포인트가 하나로 운영되던 기존 VPN 시스템 대체용으로 적합
- 하나의 Site에만 게이트웨이를 설치하고, 여타 사이트는 WAN을 통해 액세스
- 추후 Multi-site로 용이한 전환

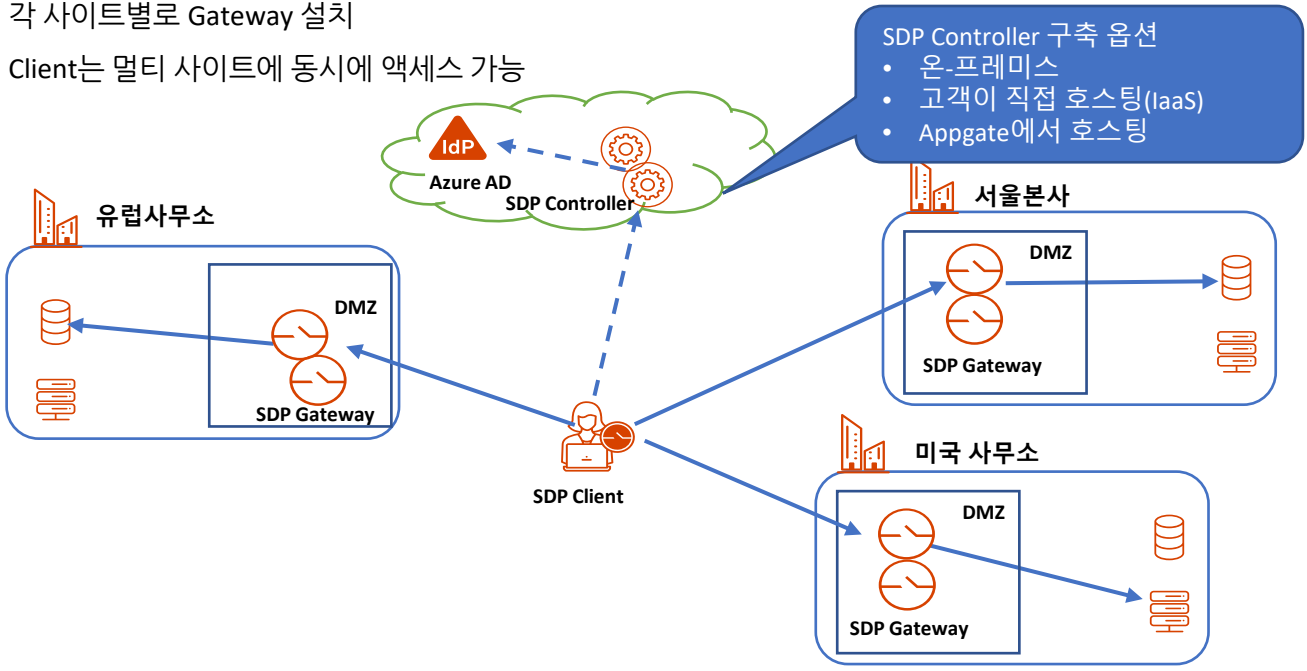


appgate

[구축 모델] Full-Scale 구축

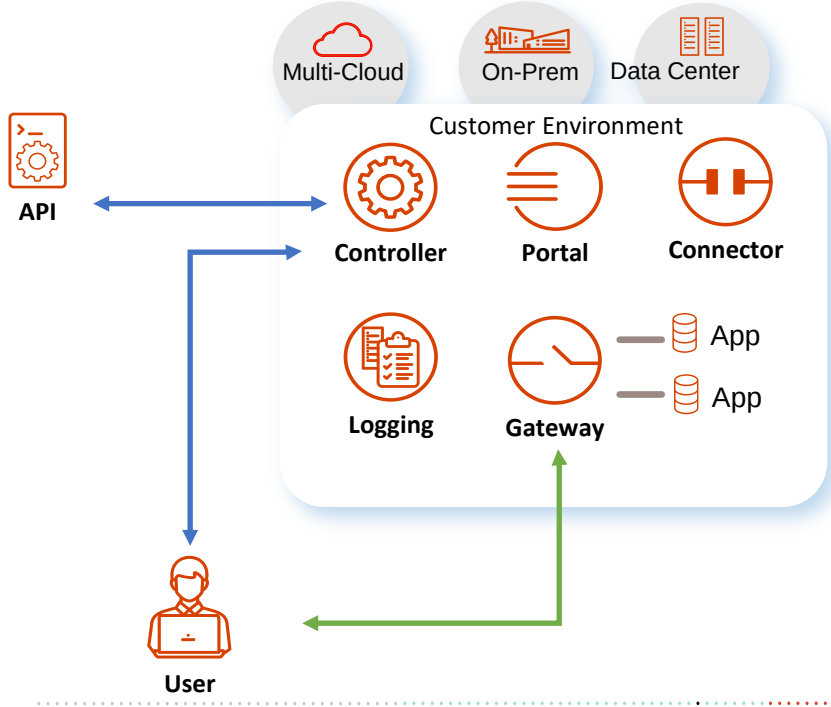
Multi-site 구성

- 지역적으로 분리된 여러 사이트를 운영하는 대규모 조직에 적합
- SDP Controller 및 Gateway 다중화
- 각 사이트별로 Gateway 설치
- Client는 멀티 사이트에 동시에 액세스 가능



[Appgate SDP] 운영 주체에 따른 구축 방식

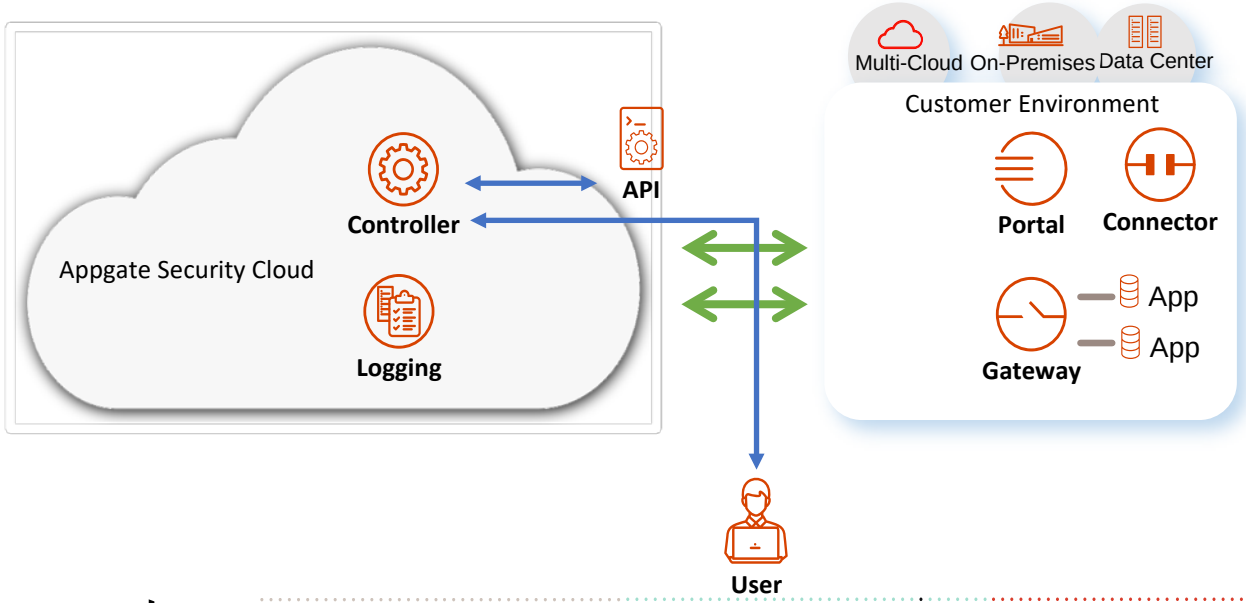
- Self-Hosted
  - ➢ SDP의 모든 구성 요소가 고객사 환경에 구축되고 운영 됨



appgate

[Appgate SDP] 운영 주체에 따른 구축 방식

- As-a-Service 구성
  - Controllers와 LogServers는 Appgate Security Cloud에서 호스팅
  - 고객사에는 Gateways, Connectors 및 Portal appliances 설치 및 운영
  - Data Plane이 Appgate Security Cloud를 절대 통과하지 않음 : Not cloud-routed



Appgate SDP

실질적 구축 방안 제시

VPN 교체 시나리오

appgate

[VPN 교체] VPN은 왜 교체 대상이 되었나?

- **최신 보안 문제 해결에 부적합**
  - 끊임없이 발견되는 보안 취약점 – 공격의 시발점이 됨
  - 원격 사용자 전용으로 개발되어 온-프레미스와 클라우드가 혼재한 상황에 부적합

- **본질적으로 안전하지 않은 아키텍처**
  - Open port 이슈 : 수신 대기 하는 포트를 통해 인터넷과 연결되고, 이 Open Port가 공격의 시작점이 됨
  - 악의적 행위자는 Open Port 스캔 ➔ 취약점 발견 ➔ 침투➔ 내부 시스템간 횡적이동 ➔ 최종 공격 목표 달성
  - IP address 대한 신뢰를 기반으로 한 액세스 허용이 큰 문제점

- **복잡성 요인**
  - 세밀한 액세스 제어가 매우 복잡하고, 관리상의 이슈와 인적 오류 유발 가능성도 매우 높음

- **원격 액세스 전용의 하드웨어기반 사일로형 솔루션**
  - 다른 보안 솔루션들과 통합이 어렵고, 확장이 번거롭고 비용이 많이 듦

[VPN 교체] VPN 교체가 필요한 10가지 이유(1/2)

1. IP 기반 인증 모델의 한계

- Identity 또는 Context에 대한 고려 부족

2. 먼저 연결을 허용한 뒤 인증하는 절차에서 오는 문제점

- Client와 VPN간에 선 TCP 세션 형성, 후 인증 구조의 문제점

3. 네트워크 내에서 횡적이동 차단 불가

- 동일네트워크내 시스템간 이동 통제가 어렵고, 별도의 솔루션 필요

4. 디바이스 상태(Device Posture) 확인 기능이 약함

- Device 상태를 인증에 반영하기 어려움

5. 성능저하와 서비스중단의 원인이 됨

- 보안을 이유로 full-tunneling을 요구 하므로 원격 사용자의 유일한 통로

[VPN 교체] VPN 교체가 필요한 10가지 이유(2/2)

6. 정책관리와 방화벽 관리가 복잡

7. 타 보안 시스템 및 비즈니스 시스템과의 연동성 부족

- 외부 시스템과의 연동에 대한 고려가 부족

8. 하드웨어 어플라이언스 중심으로 확장이 어려움

- 비용과 시간이 많이 소요됨

9. 분산시스템 및 복수의 워크로드에 동시 액세스 불가

- VPN 접속을 끊고 다른 VPN과 재 연결 필요

10. Active/Active 또는 Active/Standby만 지원

- 수평적 확장과 고가용성 구성에 한계

[VPN 교체] 사업추진시 예상되는 장애 요소

- **매몰 비용에 대한 우려**
  - 전면적 교체 지양
  - 시급한 보안 대책이 필요한 영역에 대해 Appgate SDP 우선 적용 검토
  - 점진적 / 단계적 전환 추진 : 기존 VPN 교체 시기 도래 시

- **새로운 시스템에 대한 사용자의 두려움과 불편함**
  - PoC를 통해 사용자 경험 개선을 체험하도록 유도

- **솔루션 추가에 대한 운영자 부담 증가 우려**
  - 중앙집중식 정책엔진으로 관리 포인트 감소
  - 관리해야 할 방화벽 규칙 수 감소
  - 새로운 VPN 솔루션에 대한 투자 억제
  - VPN 집중으로 인한 병목현상 완화

[VPN 교체] 단계적 마이그레이션 절차

1단계 : 기존 VPN 환경 이해

- 기존 VPN 운영 현황 파악 및 개선 사항 도출

2단계 : ZTNA 구축 로드맵 작성

- 향후 확대 적용 대상 및 범위 선정

3단계 : ZTNA 솔루션 선정 및 적용 준비

- 다양한 영역에 활용이 가능한 Universal ZTNA 솔루션 일 것

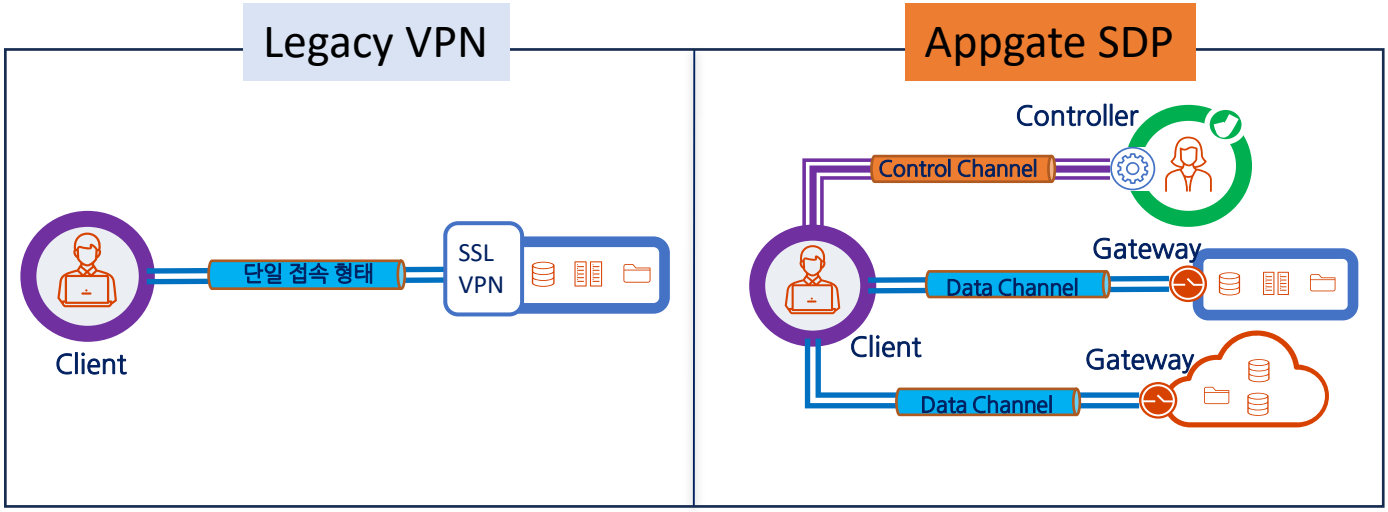
4단계 : 첫번째 Use Case 구축

- VPN Migration

5단계 : 확대 적용

- 수평 확장 : 기존 Use Case의 사용자 확대
- 수직 확장 : 새로운 Use Case 추가

[VPN 교체] 아키텍처 비교



- ✓ 1대의 어플라이언스에서 정책 및 게이트웨이 기능 동시에 제공.
- ✓ 전통적인 방식의 구성으로 외부의 공격에 취약하고 확장이 어려움.

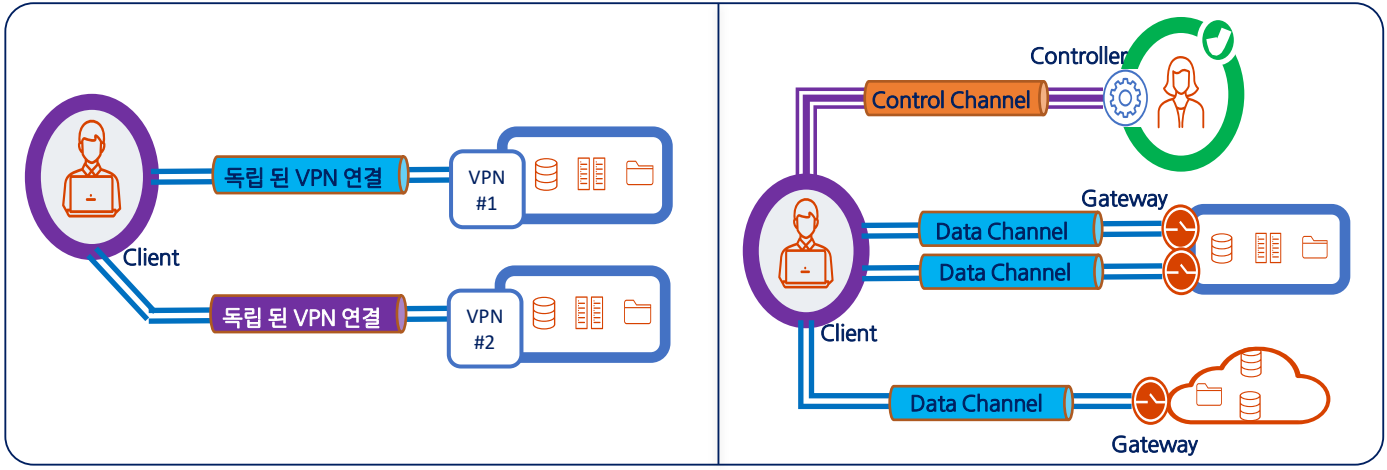
- ✓ 모든 사용자를 신뢰를 하지 않는다는 전제
- ✓ 정책 설정 기능과 게이트웨이 기능 분리로 외부 공격에 매우 강한 구성

appgate

[VPN 교체] 보안 기능 비교

항목	내 용	VPN	Appgate SDP	비 고
Site 침해	인터넷에서 불특정 사용자에 의한 접속 주소 노출 위험 (Scan 등에 의한 Site 탐지)	손쉽게 가능	매우 어려움	SPA
	불특정 사용자에 의한 게이트웨이 웹 접속 시도	손쉽게 가능	매우 어려움	SPA
외부 공격	인터넷으로부터의 웹 공격에 취약점 노출 여부	취약함	매우 안전함	SPA
	중간자 가로 채기 공격(Man in the middle) 등 정교한 공격 취약 여부	취약함	매우 안전함	mTLS
인 증	사용자에게 추가적인 2차 인증 수단 제공 여부	미제공	제공	MFA(OTP), Fido2
	솔루션 관리자의 2차 인증 수단 제공 여부	미제공	제공	MFA(OTP), Fido2
접속 정책	사용자 단말 점검을 통한 정책 적용	제공	제공	Policy
	단말의 환경을 주기적으로 점검하여 자동으로 동적인 정책 적용	미제공	제공	Condition Policy
	동적인 정책 적용을 사용자의 세션 중단 없이 자동 적용	미제공	제공	Condition Policy
사용자 PC 보안	인터넷의 불특정 장치에서, 원격 접속한 사용자 PC로 시도 되는 통신 차단 기능	미제공	제공	Ringfence

[VPN 교체] 구성상 특징 비교



구성 내용	VPN	ZTNA
복수 사이트 운영	• 사이트별 VPN 장비 설치 필요 • 각 장비별로 별도의 정책 관리 부담 • 복수사이트에 동시 접속 불가. 로그아웃 후, 재로그인의 불편함	• 하나의 컨트롤러에서 모든 정책 관리 • 여러 사이트에 게이트웨이 설치 가능 • 사용자는 모든 사이트에 동시 접속 가능
성능/확장성 이슈	• 1대의 성능이 부족한 경우, 고 사양 장비로 새로 교체하여야 함	• 클라우드 방식의 게이트웨이 확장을 통해 아주 적은 비용으로 확장 가능

appgate

감사합니다.

Appgate SDP 마스터리셀러

㈜어레이네트웍스코리아

www.ztsec.co.kr

Appgate SDP

Industry-leading ZTNA solution