



제로 트러스트 접속 제어

PacketGo ZTNA

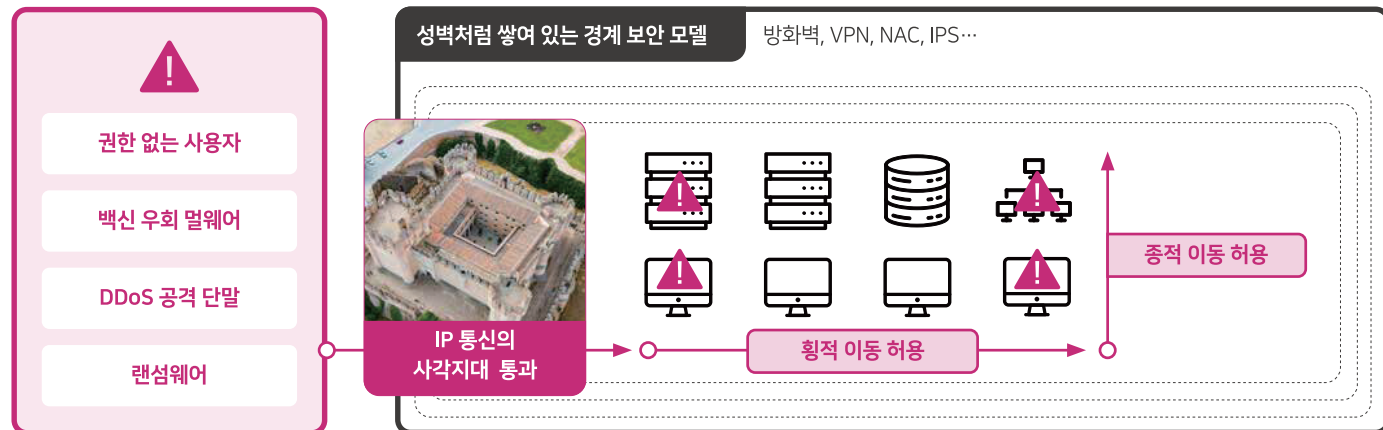


PacketGo ZTNA

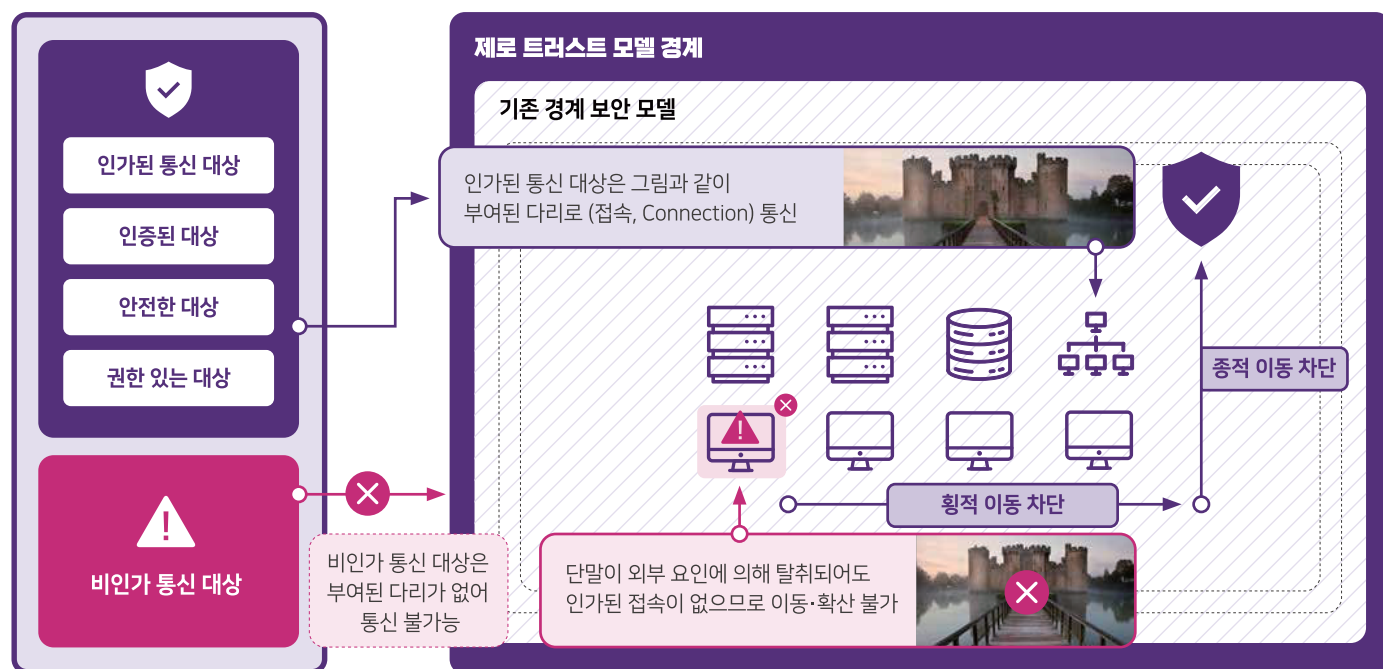
제로트러스트 네트워크 접속 제어(ZTNA) 솔루션

프라이빗네트웍스(株)는 차세대 보안 기술로 주목받고 있는 제로 트러스트 모델 기반 소프트웨어 정의 경계 프레임워크를 적용하여 비즈니스 환경에 최적화된 보안과 안전한 대상만 네트워크 접속을 허용하는 제로 트러스트 통신 서비스를 제공합니다.

☑ 실질적 통신 대상 식별이 불가능한 **경계 보안** 모델



☑ 비인가 통신 대상과 인가된 통신 대상을 논리적으로 분리하는 **제로 트러스트** 모델



ZTNA (Zero Trust Network Access)

01

인가된, 안전한 애플리케이션 전용 터널 기반 통신 체계

02

중앙화 제어 기반 네트워크 접속 수명 주기 관리와 지속적 위협 탐지를 통한 접속 격리 체계

03

인가된 터널의 최적화된 흐름 제어를 통한 네트워크 경계 관리 체계

04

경계의 통제를 받으며 어디든 안전하게 갈 수 있는 터널 라우팅

05

진화 가능한 지능형 네트워크 통제 체계

✓ 구성요소

Controller

신원 인증, 정책
단말 제어 및 접속 경로 지정

- 사용자 인증
- 앱 단위의 정책 세분화를 통한 최소 권한 정책
- 접속 요청에 대한 가장 접속 경로 부여
- 게이트웨이와 연결 지정

Gateway

보안 연결(VPN) 및
접속 경로 목적지 경로 전송

- Multi Tunnel 제로 트러스트 기술
- 인증 받은 암호화 모듈
- 사용자의 요청 목적지에 대한 전송 경로 지정

Agent

단말 OS 검증
정책에 의한 통신 연결

- 권한 부여된 애플리케이션에 대한 무결성 검사 및 실행
- 단말 PC의 OS 무결성 검증
- PC 보안 기능 일부 제공

Appliance Server

Controller Server

PCC 100/500/1000/3000/5000



Gateway Server

PCG 100/500/1000/3000/5000



Virtual Server

X86 기반 Server H/W

Windows Hyper-V

VMWare ESX

OpenStack

Linux Ubuntu 20.04

위 VM 기반 Cloud Platform

Software

설치 환경

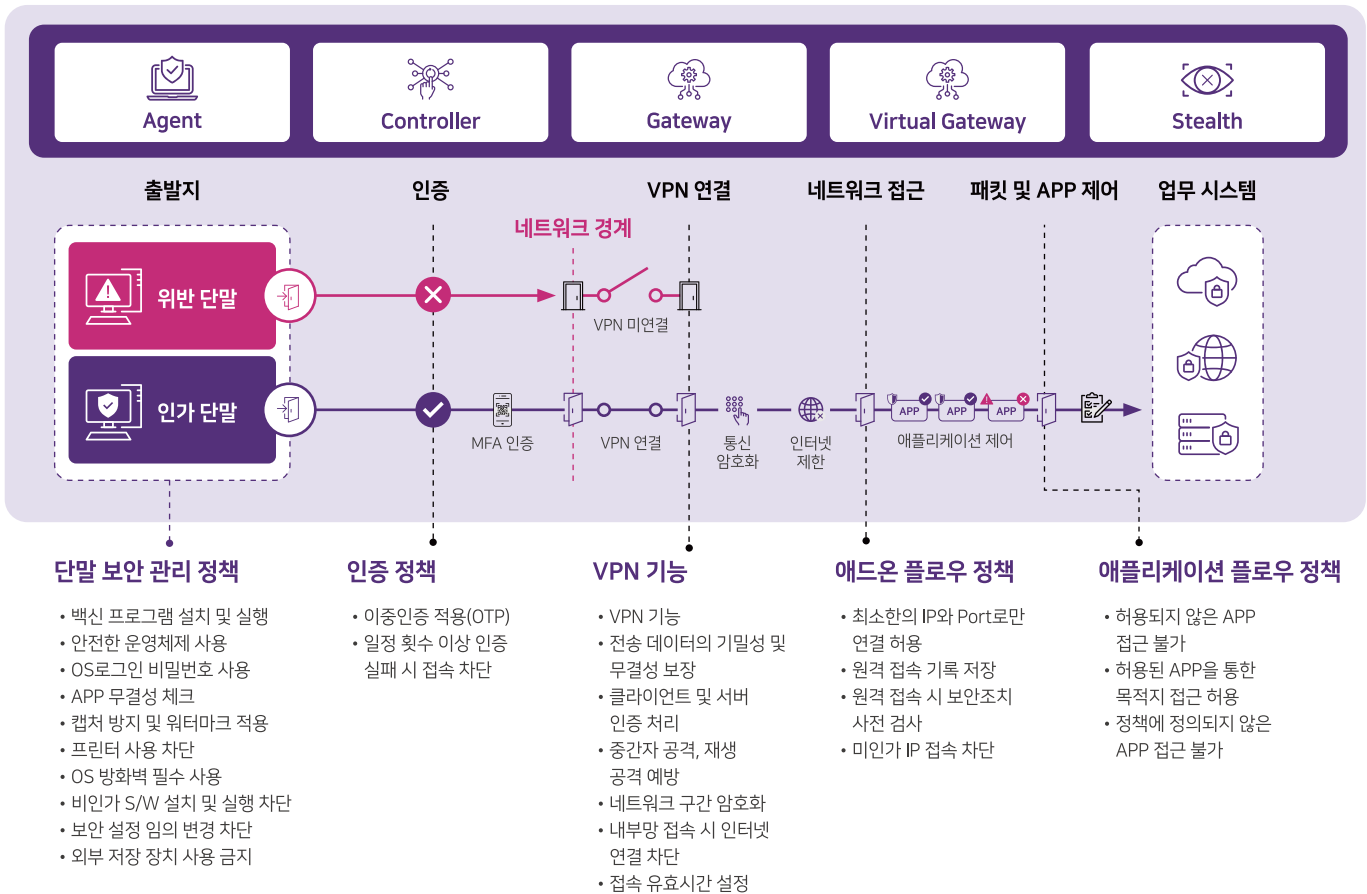
Windows 8 이상

Mac OS

Android

iOS

✓ 프로세스



✓ Micro-Segmentation 정책 예시

접속위치	보안정책	플랫폼	Role	서비스	접속 가능 앱	접속 가능한 서비스
업무용 네트워크	업무용정책	Windows, Android	일반 직원	그룹웨어	msedge.exe, chrome.exe	172.168.1.10: 443
				ERP	sapbo.exe	172.168.1.21: 443
				파일서버	explorer.exe	172.168.1.55: 445
원격업무 네트워크	원격근무 보안정책	Windows	서비스개발	형상 관리서버	git.exe	172.168.1.10: 443
				개발 DBMS	heidisql.exe	172.168.1.55: 3360
관제 네트워크	관제망 보안정책	Windows	시스템 운영	원격 접속	mstsc.exe	172.168.1.1: 3389
				텔넷기반 접속	putty.exe	172.168.1.10: 22

☑ 주요 기능



애플리케이션 제어

프로세스 기반 애플리케이션 접속 통제,
단말의 애플리케이션 무결성 검사 등



암호화 및 터널 라우팅

검증필 암호화 모듈 사용 네트워크 터널링
및 라우팅 IPSec-VPN, SSL-VPN 지원



네트워크 접속 통제

미승인 단말 접속 통제 무선 통제,
위치 기반 통제 등



접속 단말 무결성 검사

단말 OS보안 상태 식별,
필수 프로그램 검증 등



접속 단말 보안

원격 접속 시 파일 복사 제어,
화면 워터마크, 매체제어 등



사용자 인증

인사 DB 연동 사용자 인증,
2차 인증(QR, Mail OTP)

☑ 특징점

강화된 보안

- 제어 및 데이터 채널 분리를 통해 안전한 단말·네트워크·경계 제어 체계 제공
- 암호화된 애플리케이션 레벨 터널 접속 및 라우팅으로 위협 행위 차단
- 단말의 애플리케이션 위반조 방지 및 실행 제어, 비인가 매체 제어를 통한 단말 보호

효율적인 구축 운영 및 확장

- 클라우드, 무선 네트워크, 망분리 등 산재되어 있는 네트워크를 통합하여
일원화된 연결 제공
- All in One 아키텍처 기반으로 핵심 단말·네트워크 보안 기능 및 솔루션 통합 제공
- 화이트박스 기반 스케일 아웃 방식의 지속적 증설 지원, 운영 비용 감소

컴플라이언스 준수

- 보안 심의 기관에서 제공하는 보안 가이드 준수(공공기관, 금융감독원 보안 가이드라인)
- 단말·네트워크 보호를 위한 기술 및 인증 제공
- 상시 시스템 감사 및 평가 체계 제공

제로트러스트 보안 검증 및 글로벌 기술 적용

- 과기정통부 제로트러스트 보안 실증 사업 진행
- TTA 제로트러스트 가이드 준수 시험 결과서 최초 획득
- 미국 NIST 및 FORRESTER사가 정의한 보안 프레임워크 적용

☑ 원격 접속 환경



스마트 워크·재택근무

내부 직원의 외근·재택·공유 오피스 등에서 사내 시스템에 접근하는
모든 행위에 대해 안전한 접속 환경 제공



모바일 업무 환경 보안

Android, iOS 등 모바일 업무 시스템 접근에 대한 사용자 인증 및
애플리케이션 접속 통제, 사내 네트워크 보호



외부 협력사시스템 접근

외주 직원의 시스템 접근에 대한 접속 제어, 보안 강화 및
컴플라이언스 이슈 해결



클라우드접속 보안

클라우드 플랫폼을 이용한 업무 환경에서도 SaaS 환경의
인프라 보안 제공

☑ 사내 보안 환경



공공 업무 PC접속 보안

사내 공유 PC의 애플리케이션 사용 및 네트워크 접근 허용을 최소화
하여 무결성 보장 및 사내 인프라 보호



랜섬웨어·바이러스 확산 차단

비정상 접속 요청에 대한 응답 거부 및 차단으로
주변 인프라에 악성 애플리케이션 및 프로세스 전파를 사전 차단



폐쇄망·인터넷망 결합 구성

라우팅, 사용자 그룹, 접속 목적지 등 정책을 이용해
단일 솔루션으로 망분리 적용 가능



PC 접근·매체·화면 제어

금융감독원 보안 업무 규정 준수를 통해
다양한 기타 PC 보안 기능 제공

☑ 인증 및 레퍼런스



CC 인증 획득



GS 인증 1등급



국정원 보안기능확인서



혁신제품 지정 인증



외교부



정보통신산업진흥원



금산군



여성가족부



한국주택금융공사



기술보증기금



서울교통공사



한국교통안전공단



한국평가데이터



한국노동연구원



서울대 학교



포스코인터내셔널



한화시스템



KT M mobile



LG U+



롯데건설



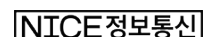
삼양식품



에치와이



E9pay



NICE정보통신



프라이빗테크놀로지

A. 서울시 마포구 양화로8길 32-16 (서교동)
T. 02-859-2560 E. sales@pribit.com

W. www.pribit.com

총판



조달 총판

