PRIBIT

Technology

Introduction to Products and Technologies Focused on ZTA Implementation

Young Rang Kim
PRIBIT Technology CEO/CTO

benjamin@pribit.com

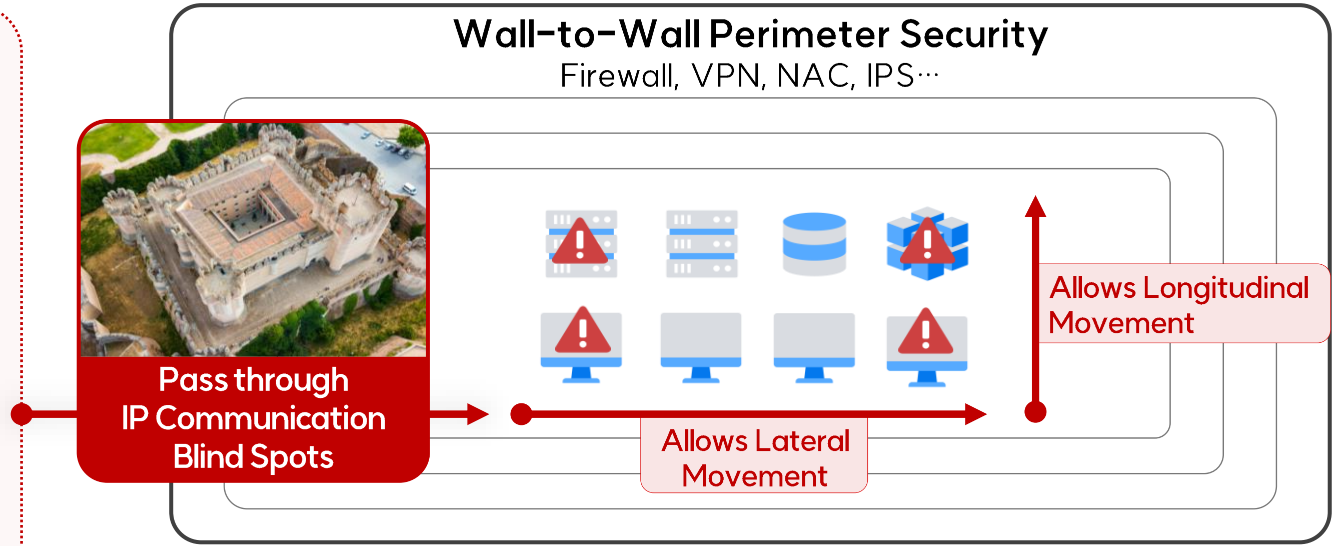
01 Problem Statement

Vulnerable to Hijacking due to Blind Spots in the Perimeter Security Model

Untrusted Networks (Over 288 trillion communicable destinations based on IPv4)

- Unauthorized Users
- Non-authenticated Users
- DDoS Attack
- S/W with Inherent Vulnerabilities
- S/W not available for work
- Malware-infected Terminal
- Terminals without Antivirus
- Hijacked Users
- Ransomware
- Counterfeit S/W
- Antivirus-bypassing Malware
- Terminals via Rogue Proxy and Router

Protected Networks (Cloud, Workspace, Wireless Networks …)



Wall-to-Wall Perimeter Security
Firewall, VPN, NAC, IPS…

Pass through IP Communication Blind Spots

Allows Lateral Movement

Allows Longitudinal Movement

IP Technology Suffers from a Lack of Actual Communication Terminal Identification
"Blind Spots in Communication Control"

IP Data Packet Structures

MAC	IP Header	Protocol Header	Payload
(Layer 2)	(Layer 3)	(Layer 4)	(Layer 7)

Struggle with Identifying Actual Terminals, Resulting in Surpassed Technical Improvement Limits and Thresholds

DDoS, Ransomware, Zero Day Attack, Session Hijacking, MITM, Information leakage…Many Security Incidents Involve "The Network"

How to Improve the Perimeter Security Model

Untrusted Networks

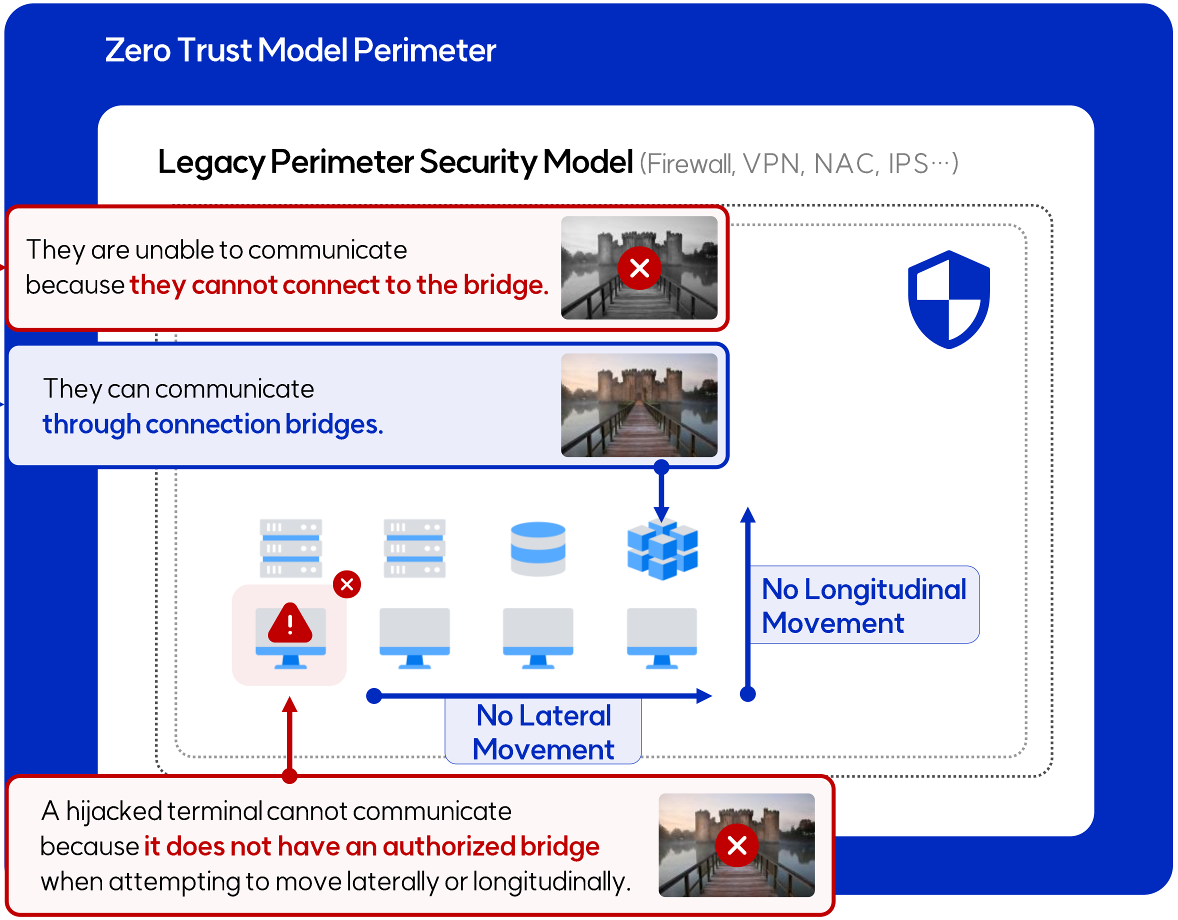
Unauthorized Communication Terminal

- Unauthorized Users
- Ransomware
- DDoS Attack
- S/W with Inherent Vulnerabilities
- S/W not available for work
- Without Antivirus
- Terminals via Rogue Proxy and Router
- Hijacked Users
- Counterfeit S/W
- Malware-infected
- Antivirus-bypassing Malware
- Non-authenticated Users

Authorized Communication Terminal (Logical separation)

- Authenticated Terminal (User, S/W, Terminal)
- Secure Terminal (Security Compliance, S/W)
- Permitted Terminal (User, Terminal, S/W, Service)

Protected Networks (Cloud, Workspace, Wireless Networks ···)



Zero Trust Model Perimeter
Legacy Perimeter Security Model (Firewall, VPN, NAC, IPS···)
No Longitudinal Movement
No Lateral Movement

They are unable to communicate because **they cannot connect to the bridge.**

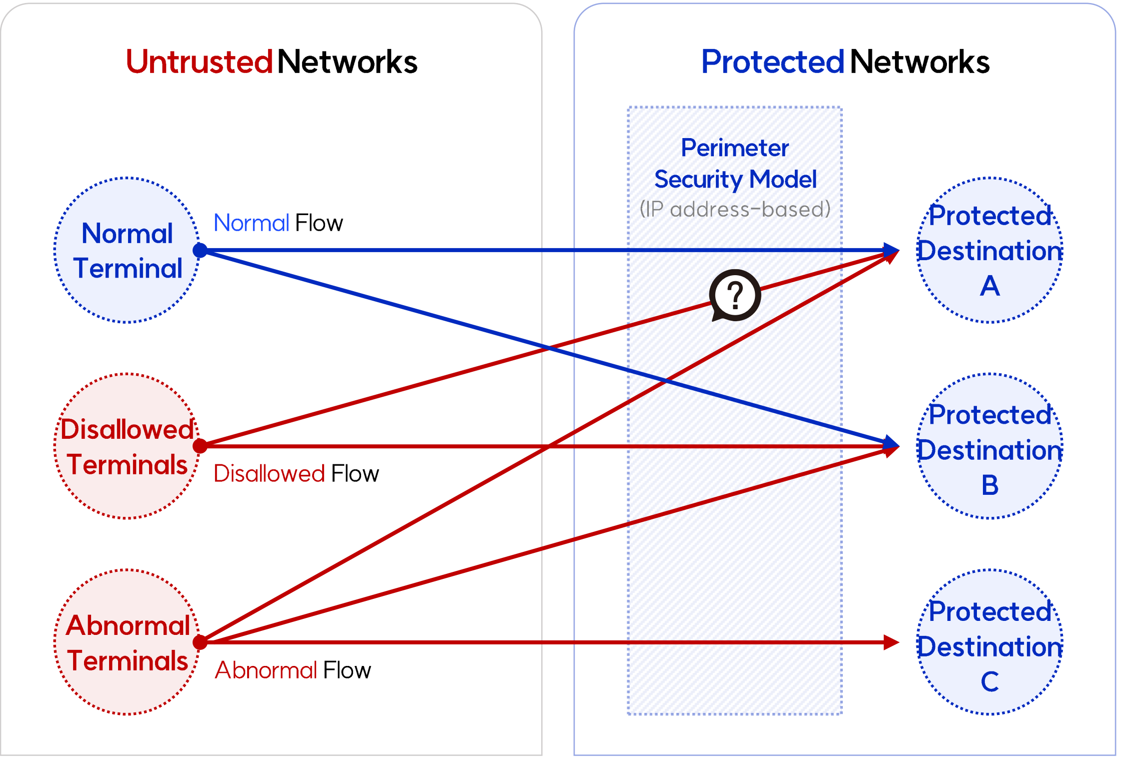
They can communicate **through connection bridges.**

A hijacked terminal cannot communicate because **it does not have an authorized bridge** when attempting to move laterally or longitudinally.

The Zero Trust Model logically Separates Unauthorized and Authorized Communication Terminal

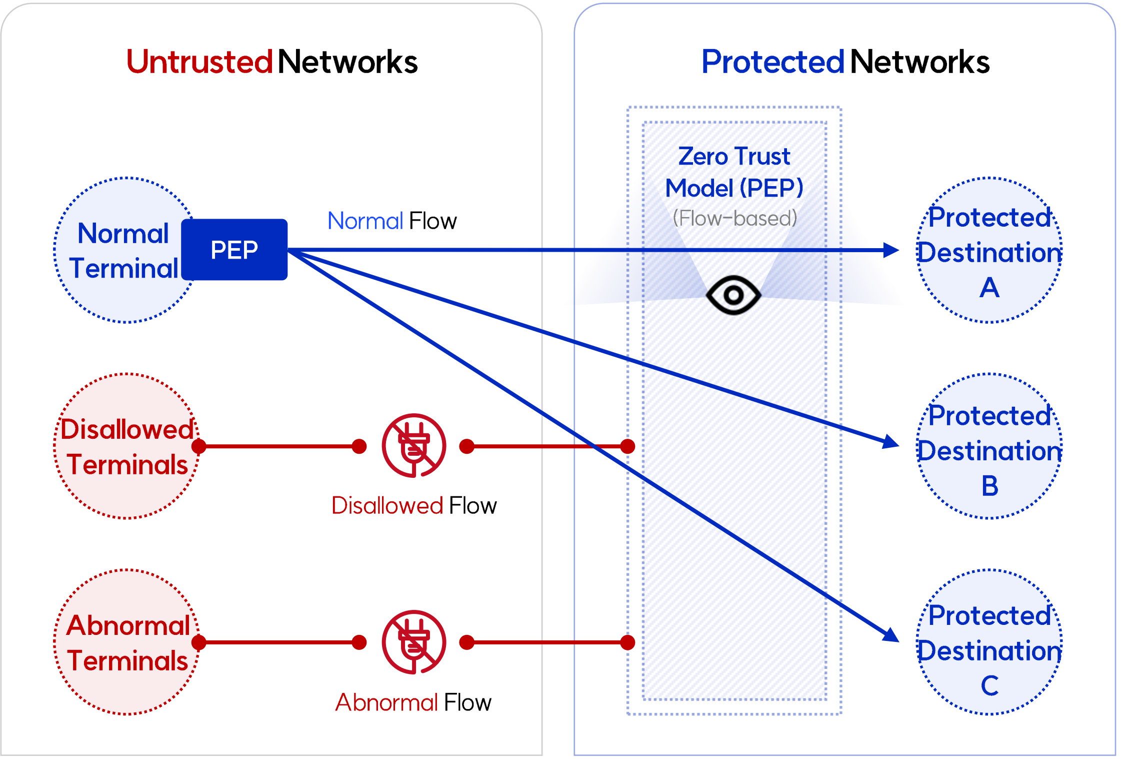
The Power of a Zero Trust Model to Control Telecommunication

In the Perimeter Security Model (AS-IS)



- **Inability to Identify and Control Flows between Terminal and Destination**
  - Identify Terminal and Destination by IP Address
  - Set Policies and Control based on IP Address
  - Requiring Massive Amounts of Log Recording and Analysis

In the Zero Trust Model (TO-BE)



- **Identify and Control Flows between Terminal and Destination**
  - Identify as Terminal, Users, S/W, IP Addresses, and Logical Units
  - Set Policies and Control based on Flow
  - Intuitive Flow-Driven Log Recording and Analysis Scheme

02 Introduction to Technologies around the Zero Trust Model

Zero Trust Mechanisms

In the Perimeter Security Model | A Paradigm Shift in the Perimeter Security Model | **In the Zero Trust Model**

Untrusted
Unidentified Terminal

All Communication Terminal are Untrusted

Beware of unidentified devices, users, and malware or ransomware infections.

Minimal Trust
Terminal and User

User authentication and basic verification

Verify security compliance, including device and user authentication and anti-virus software installation.

Partial Trust
S/W

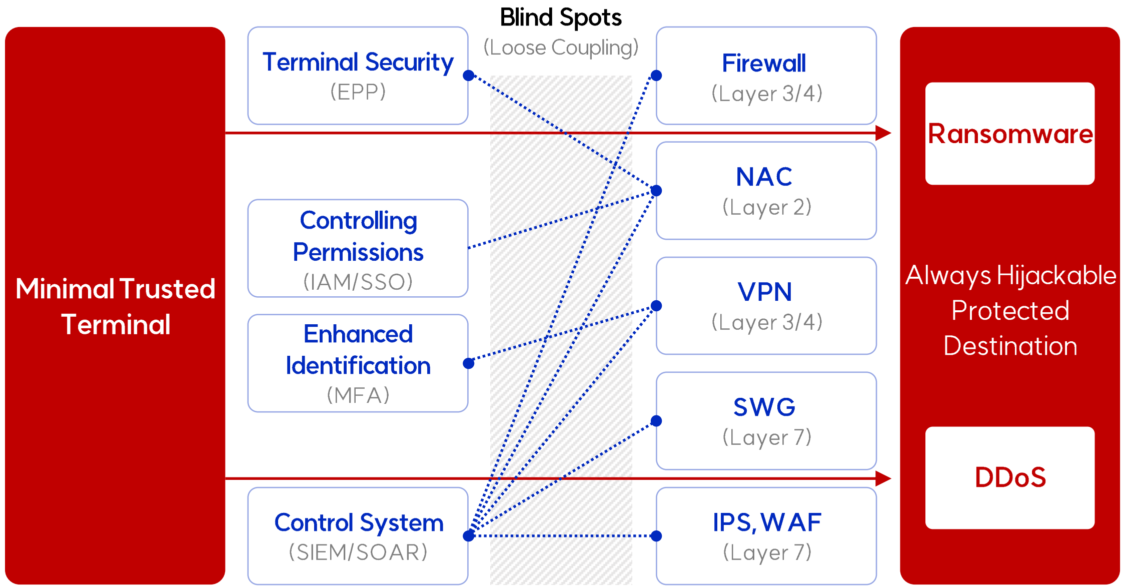
Detection of network access Inspection of S/W

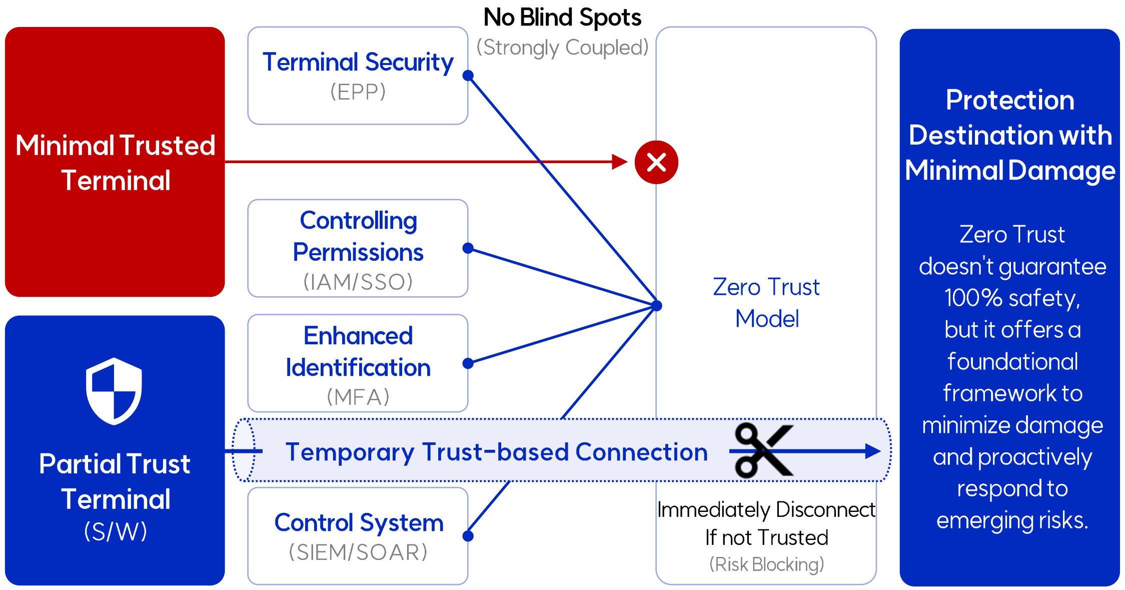
Identifying and inspecting substantial communications and verify access permissions

Temporary Trust
S/W ↔ Service Access

Allow communication after minimal authorization Always-on inspection

Allowed terminal can communicate temporarily with granted connection

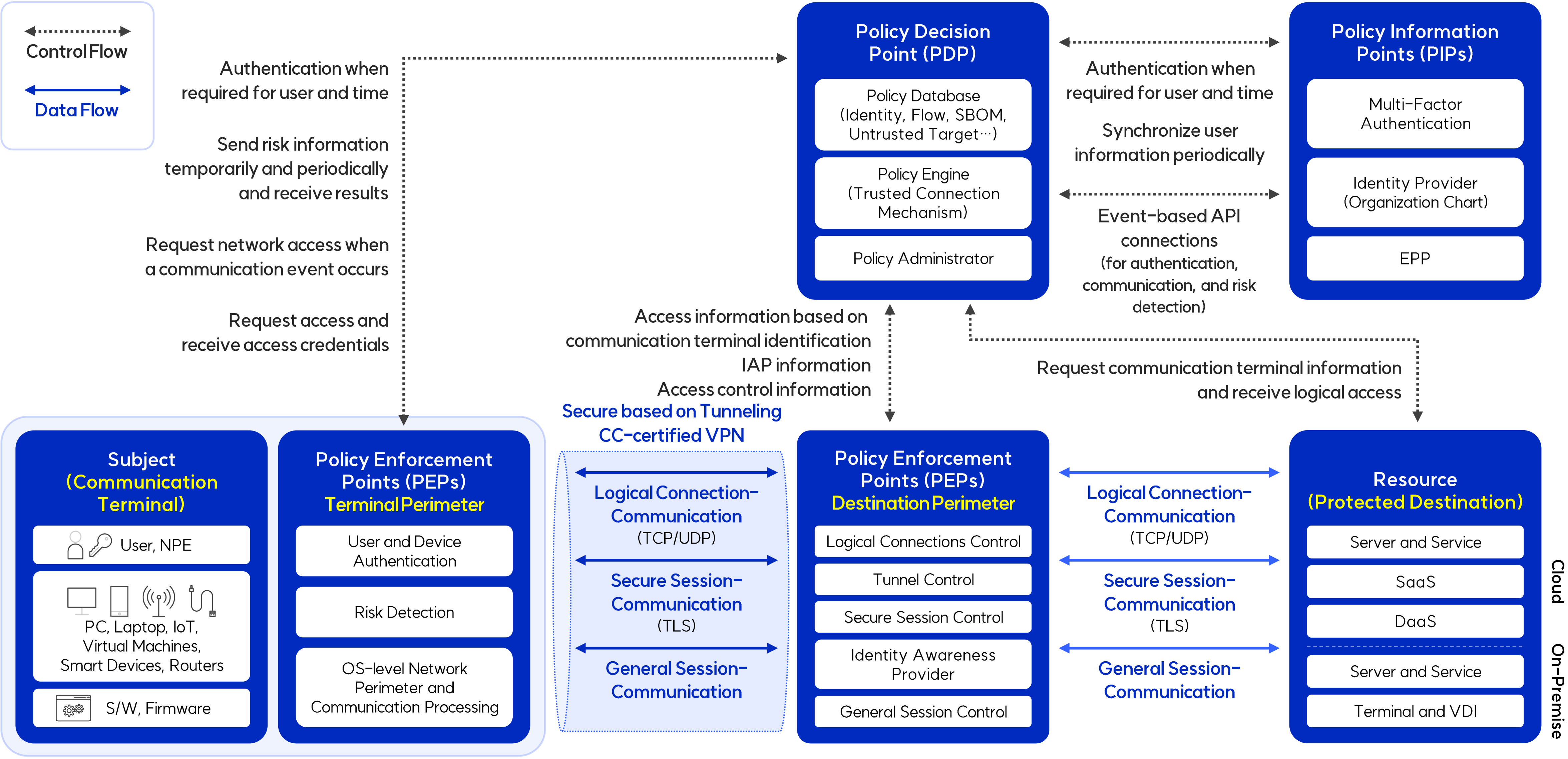




Zero Trust doesn't guarantee 100% safety, but it offers a foundational framework to minimize damage and proactively respond to emerging risks.

Zero Trust Architecture Implementation Elements

(Based on the Zero Trust Demonstration Model 'NIST SP 1800-35', Component Flowchart)



Control Flow

Data Flow

Authentication when required for user and time

Send risk information temporarily and periodically and receive results

Request network access when a communication event occurs

Request access and receive access credentials

Policy Decision Point (PDP)

- Policy Database (Identity, Flow, SBOM, Untrusted Target…)
- Policy Engine (Trusted Connection Mechanism)
- Policy Administrator

Authentication when required for user and time

Synchronize user information periodically

Event-based API connections (for authentication, communication, and risk detection)

Policy Information Points (PIPs)

- Multi-Factor Authentication
- Identity Provider (Organization Chart)
- EPP

Access information based on communication terminal identification

IAP information

Access control information

Request communication terminal information and receive logical access

Subject (Communication Terminal)

- User, NPE
- PC, Laptop, IoT, Virtual Machines, Smart Devices, Routers
- S/W, Firmware

Policy Enforcement Points (PEPs) Terminal Perimeter

- User and Device Authentication
- Risk Detection
- OS-level Network Perimeter and Communication Processing

Secure based on Tunneling CC-certified VPN

Logical Connection-Communication (TCP/UDP)

Secure Session-Communication (TLS)

General Session-Communication

Policy Enforcement Points (PEPs) Destination Perimeter

- Logical Connections Control
- Tunnel Control
- Secure Session Control
- Identity Awareness Provider
- General Session Control

Logical Connection-Communication (TCP/UDP)

Secure Session-Communication (TLS)

General Session-Communication

Resource (Protected Destination)

Cloud

- Server and Service
- SaaS
- DaaS

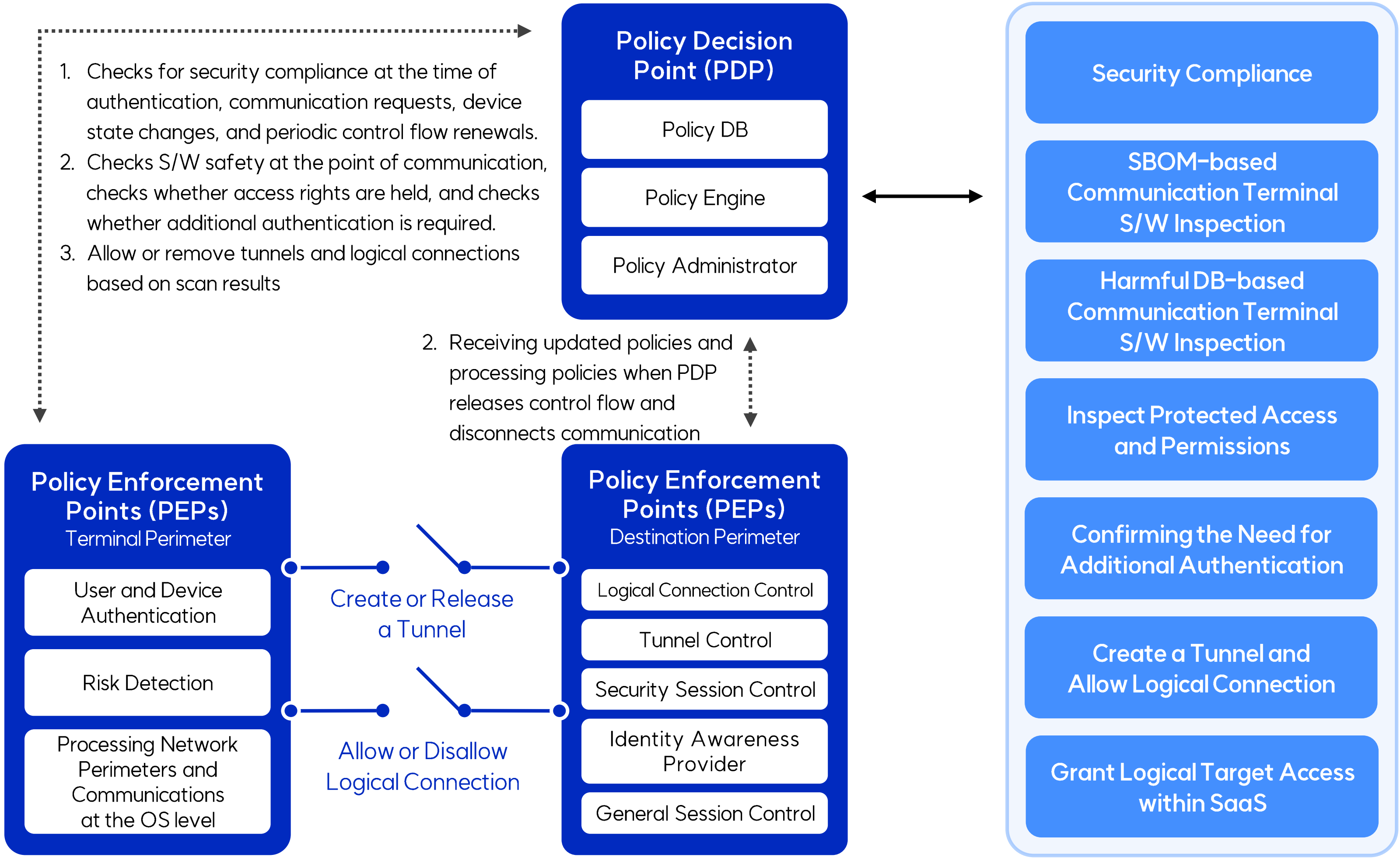
On-Premise

- Server and Service
- Terminal and VDI

PRIBIT

Elements of implementing the 7 Tenets of Zero Trust

6. All Resource Authentication and Authorization are Dynamic and Strictly Enforced before Access is Allowed



1. Checks for security compliance at the time of authentication, communication requests, device state changes, and periodic control flow renewals.
2. Checks S/W safety at the point of communication, checks whether access rights are held, and checks whether additional authentication is required.
3. Allow or remove tunnels and logical connections based on scan results

Policy Decision Point (PDP)

- Policy DB
- Policy Engine
- Policy Administrator

2. Receiving updated policies and processing policies when PDP releases control flow and disconnects communication

Policy Enforcement Points (PEPs)
Terminal Perimeter

- User and Device Authentication
- Risk Detection
- Processing Network Perimeters and Communications at the OS level

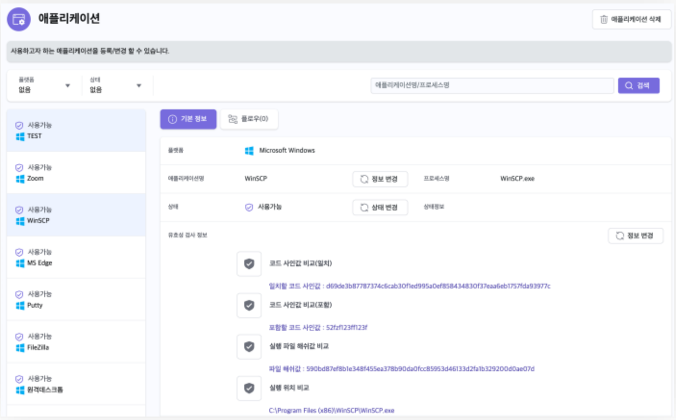
Create or Release a Tunnel

Allow or Disallow Logical Connection

Policy Enforcement Points (PEPs)
Destination Perimeter

- Logical Connection Control
- Tunnel Control
- Security Session Control
- Identity Awareness Provider
- General Session Control

- Security Compliance
- SBOM-based Communication Terminal S/W Inspection
- Harmful DB-based Communication Terminal S/W Inspection
- Inspect Protected Access and Permissions
- Confirming the Need for Additional Authentication
- Create a Tunnel and Allow Logical Connection
- Grant Logical Target Access within SaaS



애플리케이션

사용하고자 하는 애플리케이션을 등록/변경 할 수 있습니다.

플랫폼: 없음 | 상태: 없음

플랫폼: Microsoft Windows

애플리케이션명: WinSCP | 프로세스명: WinSCP.exe

상태: 사용가능 | 상세정보

유효성 검사 정보

코드 사인값 비교(일치)

일치할 코드 사인값 : d69de3b87787374c6cab30f1ed995a0ef858434830f37eaa6eb1757fda93977c

코드 사인값 비교(포함)

포함할 코드 사인값 : 52fzf123ff123f

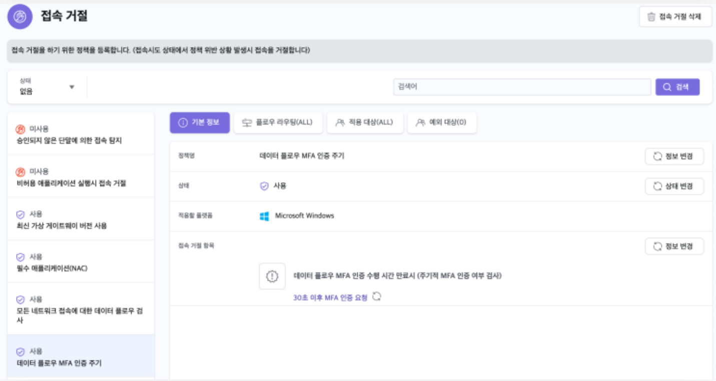
실행 파일 해쉬값 비교

파일 해쉬값 : 590bd87ef8b1e348f455ea378b90da0fcc85953d46133d2fa1b329200d0ae07d

실행 위치 비교

C:\Program Files (x86)\WinSCP\WinSCP.exe

S/W Management



접속 거절

접속 거절을 하기 위한 정책을 등록합니다. (접속시도 상태에서 정책 위반 상황 발생시 접속을 거절합니다)

상태: 없음

접속 거절 삭제
검색어
검색
미사용 승인되지 않은 단말에 의한 접속 탐지
미사용 비허용 애플리케이션 실행시 접속 거절
사용 최신 가상 게이트웨이 버전 사용
사용 필수 애플리케이션(NAC)
사용 모든 네트워크 접속에 대한 데이터 플로우 검사
사용 데이터 플로우 MFA 인증 주기
기본 정보
플로우 라우팅(ALL)
적용 대상(ALL)
예외 대상(0)
정보 변경
상태 변경
정보 변경

정책명: 데이터 플로우 MFA 인증 주기

상태: 사용

적용할 플랫폼: Microsoft Windows

접속 거절 항목

데이터 플로우 MFA 인증 수행 시간 만료시 (주기적 MFA 인증 여부 검사)

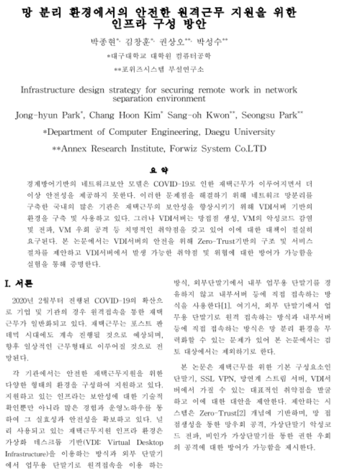
30초 이후 MFA 인증 요청

Security Compliance Management

02 Introduction to Technologies around the Zero Trust Model

Technology verified by a public authority

Demonstrated Improvement by Applying Our Model
(Solving the problems of the perimeter security model)



망 분리 환경에서의 안전한 원격근무 지원을 위한 인프라 구성 방안

박종현*, 김창훈*, 권상오**, 박성수**

*대구대학교 대학원 컴퓨터공학

**포워즈시스템 부설연구소

Infrastructure design strategy for securing remote work in network separation environment

Jong-hyun Park*, Chang Hoon Kim* Sang-oh Kwon**, Seongsu Park**

*Department of Computer Engineering, Daegu University

**Annex Research Institute, Forwiz System Co.LTD

요 약

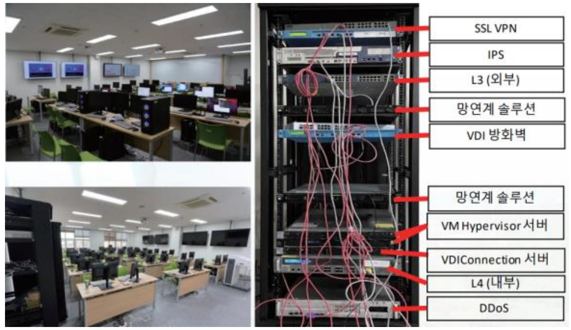
경계방어기반의 네트워크보안 모델은 COVID-19로 인한 재택근무가 이루어지면서 더 이상 안전성을 제공하지 못한다. 이러한 문제점을 해결하기 위해 네트워크 망분리를 구축한 국내의 많은 기관은 재택근무의 보안성을 향상시키기 위해 VDI서버 기반의 환경을 구축 및 사용하고 있다. 그러나 VDI서버는 망접점 생성, VM의 악성코드 감염 및 전파, VM 우회 공격 등 치명적인 취약점을 갖고 있어 이에 대한 대책이 절실히 요구된다. 본 논문에서는 VDI서버의 안전을 위해 Zero-Trust기반의 구조 및 서비스 절차를 제안하고 VDI서버에서 발생 가능한 취약점 및 위협에 대한 방어가 가능함을 실험을 통해 증명한다.

I. 서론

2020년 2월부터 진행된 COVID-19의 확산으로 기업 및 기관의 경우 원격접속을 통한 재택근무가 일반화되고 있다. 재택근무는 포스트 판데믹 시대에도 계속 진행될 것으로 예상되며, 향후 일상적인 근무형태로 이루어질 것으로 전망된다.

각 기관에서는 안전한 재택근무지원을 위한 다양한 형태의 환경을 구성하여 지원하고 있다. 지원하고 있는 인프라는 보안성에 대한 기술적 확인뿐만 아니라 많은 경험과 운영노하우를 통하여 그 실효성과 안전성을 확보하고 있다. 널리 사용되고 있는 재택근무지원 인프라 환경은 가상화 데스크톱 기반(VDI: Virtual Desktop Infrastructure)을 이용하는 방식과 외부 단말기에서 업무용 단말기로 원격접속을 이용 하는 방식, 외부단말기에서 내부 업무용 단말기를 경유하지 않고 내부서버 등에 직접 접속하는 방식을 사용한다[1]. 여기서, 외부 단말기에서 업무용 단말기로 원격 접속하는 방식과 내부서버 등에 직접 접속하는 방식은 망 분리 환경을 무력화할 수 있는 문제가 있어 본 논문에서는 검토 대상에서는 제외하기로 한다.

본 논문은 재택근무를 위한 기본 구성요소인 단말기, SSL VPN, 망연계 스트림 서버, VDI서버에서 가질 수 있는 대표적인 취약점을 발굴하고 이에 대한 대안을 제안한다. 제안하는 시스템은 Zero-Trust[2] 개념에 기반하며, 망 접점생성을 통한 망우회 공격, 가상단말기 악성코드 전파, 비인가 가상단말기를 통한 권한 우회의 공격에 대한 방어가 가능함을 제시한다.



Perimeter Security Model
Experimental Environment

The paper proposes a secure VDI system based on Zero Trust. We have verified through experiments that it can tackle various security threats arising from remote work. By managing access between virtual machines using Local PEP and PDP Controllers, **we were able to prevent malware propagation and permission bypass through virtual machines.** The structure proposed in this paper demonstrates **an alternative for a safer remote work environment.** (Excerpt from the paper)

Prof. Chang Hoon Kim's research team at Daegu University
KIISC, Winning the Best Paper Award in Autumn(2021)

posco INTERNATIONAL

- As a global conglomerate, they need to be able to access our business systems anytime, anywhere – from home, smart offices, and domestic and international business trips.
- **About 5,000 employees of more than 80 corporations around the world worked based on the 24/7 Zero Trust model, and work satisfaction improved.**

Control Blind Spots that Perimeter Security Models Were Unable to Identify

Identify Communication Terminal S/W

137 Cases

Identify Communicable Protected Services

1,350 Cases

Perimeter Security Models Cannot Identify Communication Flows and Block Communication Requests (2020~2021)

Identify Requests from All Users, Devices, and S/W — **2.2 Million Cases**

Block Communication for Potential Risk **(71%)** — **1.56 Million Cases**

Request Acceptance Criteria	Enforce security compliance, Inspect Communication S/W, verify policies for allowing access to protected services, etc.
Blocking Analysis Results	Bypass non-business S/W and antiviruses and check for ransomware and malware blocking port scanning

Based on the Results Applied to the Real Environment, It is the Only One in Korea to Derive Quantitative Effects

PRIBIT

03 Demonstrating a Zero Trust Model In Korea (Ministry of Science and ICT)

Objectives

A Globally-focused Zero Trust Model

Next-Generation Communications Experiences	Secure Wireless Networks and Validate Cloud-based Next-Generation Communications Control Infrastructure	Communications Infrastructure Centered Zero Trust Model
Work From Anywhere	Enable Public Cloud and On-Premises Work Environments that Comply with Korea's Specialized Security Regulations	Build a Cloud-centric Service and Work Environment
National Security Governance	The Security Governance Scheme that Enables Incremental Implementation of the Maturity Model by Integrates SBoM and Existing Security Models	Combine Various Security Models for Flexible Scalability

Demonstration with National Critical Facilities

LG유플러스	Korea's Major Wired and Wireless Service Company	
NIA 한국지능정보사회진흥원	Organizations Working on Digital Platform Government Projects	
HF 한국주택금융공사	FSC-affiliated Organizations that Provide Housing Guarantees and Loans	Serious National Losses Occur due to Cyber Attacks

03 Demonstrating a Zero Trust Model In Korea (Ministry of Science and ICT)

Demonstrate the Next Generation of Zero Trust Telecommunications

Cloud Native NG Core (All IP Network)

Policy Decision Point (PDP)

- Identify and Inspect Terminals
- Decide Whether to Allow within 100 msec
- Unified Relaying of S/W and L2/3/4/7 (Trusted Connection)
- Enable Immediately without Policy Settings (Zero Touch Configuration)
- Communication Information Collection and Real-time Analytics

Policy Information Points (PIPs)

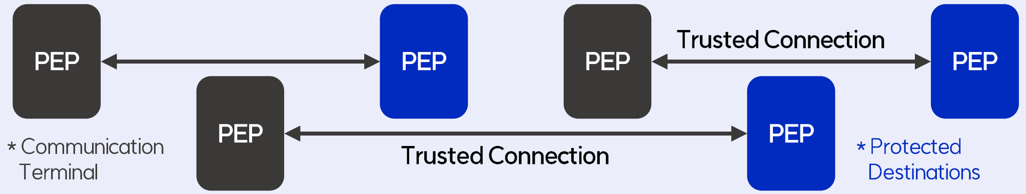
- API-based Extension Scheme
- Connecting the Wired and Wireless Cores

Transcend the Physical boundaries

Wired Network Infrastructure ↔ Wireless Network Infrastructure ↔ Private Network Infrastructure

LG유플러스 NIA 한국지능정보사회진흥원 HF 한국주택금융공사

Secure Connection Relay Even on Untrusted Networks



* Communication Terminal

* Protected Destinations

SDP (Software Defined Perimeter)

- Establishing OS-level Micro-perimeters with S/W Installation
- Support for Multiple OS (Windows, Mac OS, Gooroom OS, Android, iOS, Linux, etc.)
- Pre-Authentication and Post-Access Mechanisms
- Addressing Vulnerabilities in Open Source SDP

Micro-Segmentation (Network Level)

Control communication between:

- Security-compliant Terminals and IoT Devices and Services
- Authorized S/W and Services
- SaaS, DaaS, VDI, and Managed Servers for Privileged Users

Micro-Segmentation (Service Level)

Control Access to:

- Standard Protocol-based Services from Authorized Terminal
- In-service Capabilities of Authorized Terminal
- In-service Data of Authorized Terminal

EIG (Enhanced Identity Governance)

- One ID Authentication with Public Sector User Information Integration
- Establish Access to Centralized Public SaaS, Features, and Data
- Anti Phising FIDO Authentication
- User Authentication with FIDO Before Network Access
- Trusted Connection for Communication Identification
- Troubleshoot Session Hijacking by Not Exposing ID
- Isolate Risky Communication Terminals
- Continuous Authentication with Compliance and Behavioral Analytics

Please question to email below

benjamin@pribit.com

PRIBIT

Thank you