

SECURE DATA BRIDGE

IEUMv2.0

Network Data Transfer System

Secure and Efficient Cross-Network Data Transfer & System Integration Solution



Robust Security

National Intelligence Service (NIS) Certified Technology Ensures Secure and Trusted Data Transmission



User-Centric Design

National Intelligence Service (NIS) Certified Technology Ensures Secure and Trusted Data Transmission



Flexible Scalability

Supports Integration with Various Systems Expandable Architecture for Future Growth



JN JENER SYSTEM

JENER SYSTEM Co., Ltd.

01 Company Introduction

- Company Overview
- Company History
- Certifications
- Maintenance Customers

03 Product Competitiveness

- Security
- User Convenience
- Operational Convenience
- Scalability

05 Data Transfer System

- Data Transfer Communication Method
- Data Transfer Process
- File Transfer Approval Workflow
- Data Import & Export Management

07 Integration Services

- System Integration Service
- Email Integration Service
- Smart Work Service
- CCTV Integration Service

02 Product Overview

- Product Specifications
- Registered Procurement Products
- IEUM v2.0 Overview
- IEUMNet Product Family

04 Network Interconnection Technology

- Network Interconnection Overview
- Data Transfer Method
- Streaming Method
- Technology Comparison Analysis

06 Streaming System

- Streaming Gateway System
- Streaming Communication Method
- Session Connection Method
- Packet Filtering Method

08 Implementation Cases

- Three-Network Segmentation Deployment
- Remote Meter Reading System
- Enforcement Data Relay System
- Smart City Integration

01

COMPANY INTRODUCTION

Company Overview and Corporate History

1. Company Introduction (General Overview)



1997

2012

2016

- Established JENER SYSTEM Co., Ltd.
- Built and maintained security equipment for administrative IT networks
- Built and maintained resident information networks
- Supplied and maintained network equipment for military units
- Supplied and maintained public network and IT equipment

- Launched financial solution development business
- Awarded integrated maintenance projects for the Office of Waterworks, Dobong-gu, and Seoul Medical Center
- Awarded Seongbuk-gu website development project and registered copyright for maintenance PMS
- Awarded maintenance project for Seoul Seonam Hospital
- Surpassed 100 employees, including subsidiary Jaeger Co., Ltd.
- Established JENER SYSTEM R&D Center

- Deployed network separation and interconnection systems for Cheongju, Daemyung, Star, and Namyang Savings Banks
- Deployed network interconnection for the Defense Acquisition Program Administration security monitoring system
- Deployed network separation and interconnection systems for NICE Information & Telecommunication and Free Telecom
- Deployed network separation and interconnection systems for defense companies Hanwha CAS, Dawin Friction, and Vitzro Miltech
- Expanded and relocated JENER SYSTEM Co., Ltd. to a new 5-story headquarters
- Deployed network interconnection solution for Korea Inclusive Finance Agency
- Awarded Korea Childcare Promotion Institute network separation project, including network interconnection solution deployment
- Deployed network interconnection solution for Songpa-gu Office Mayor's Smart Vision System project
- Deployed network interconnection solution for five linked systems in Yangju U-City
- Deployed network interconnection solution for Yangju U-City CCTV video export system

We propose an integrated secure gateway solution to protect your valuable information assets.

1. Company Introduction (General Overview)



- Awarded Phase 2 network separation project for Korea Childcare Promotion Institute
- Deployed network interconnection solution for Gangdong-gu Office web server integration
- Deployed network separation for Hyundai Motor Miso Finance
- Deployed network interconnection solution for Gangdong-gu Office Digital Mayor's Office
- Deployed network separation for LG Miso Finance

- Supplied Network Interconnection Solutions to Yangju Smart City, Dobong Smart City, and Gimje Smart City
- Supplied Network Interconnection Solutions to Gangnam-gu Smart Mayor's Office, Asan City Hall, Inje Waterworks Office, and Gyeongbuk Fire Headquarters
- Supplied Network Interconnection Solutions to Uljin Clean Water Office, Jung-gu Office (Seoul), Gokseong County, Boseong County, and Audi Volkswagen Korea
- Supplied Network Interconnection Solutions to Gangjin County, Hongcheon County, Hapcheon County, Yeongdong County, Dongjak-gu Office, Gimpo Urban Railway, Iksan City, and Gyeryong City
- Supplied Network Interconnection Solutions to UDID Co., Ltd., Space Solution, Chungju City, the National Police Agency, and Dongdaemun-gu Office

- Supplied Network Interconnection Solutions to the Republic of Korea Marine Corps Headquarters, Gangbuk-gu Office, Daeyang Electric, and Songpa-gu Office
- Supplied Network Interconnection Solutions to Yangju ITS, Yeosu City, and Jecheon City
- Supplied Network Interconnection Solutions to Free Telecom, Hansung S&I, and Sunchang County
- Supplied Network Interconnection Solutions to Osung Savings Bank, Anyang City, and Eunpyeong-gu Office
- Implemented Network Interconnection Systems for the National Police Agency, Gimje City Hall, and MOTIE R&D Programs
- Obtained the Security Function Verification Certificate for IEUM V2.0
- Obtained Direct Production Certification for IEUM NAS
- Built IEUM NAS 312 for the Armed Forces Medical School
- Built IEUM NAS 308 for the Daegu Metropolitan Council Secretariat
- Built IEUM NAS 312 for G& Technology
- Built IEUM NAS 308 for the Gwacheon City Council
- Implemented a Network Interconnection Streaming System for the Chungju Environmental & Water Resources Headquarters
- Upgraded the IEUM V2.0 Network Interconnection System for NeoTrans

We propose an integrated secure gateway solution to protect your valuable information assets.

2. Network Interconnection Solution Maintenance Customers

Public Institutions & Research Organizations



Local Governments



Financial Institutions & Others



We propose an integrated secure gateway solution to protect your valuable information assets.

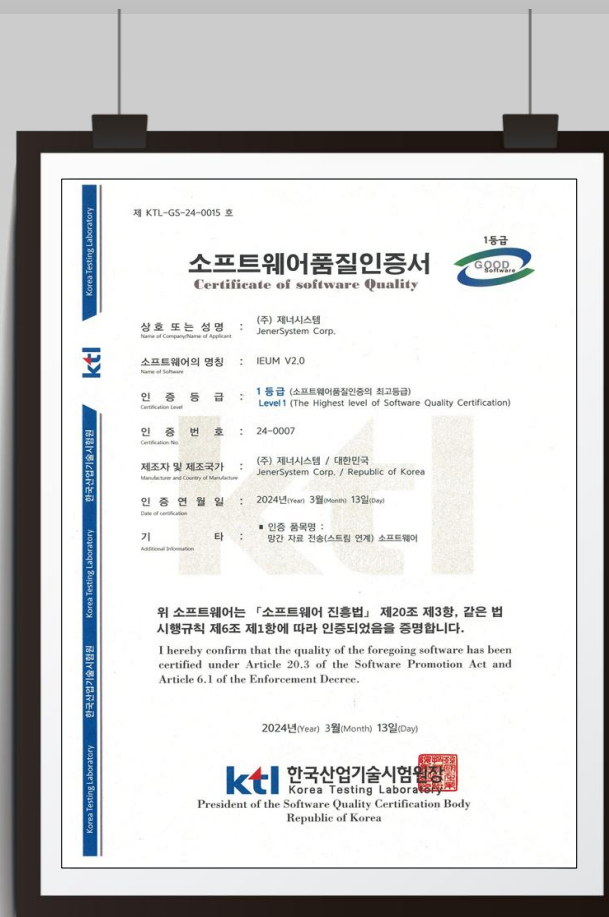
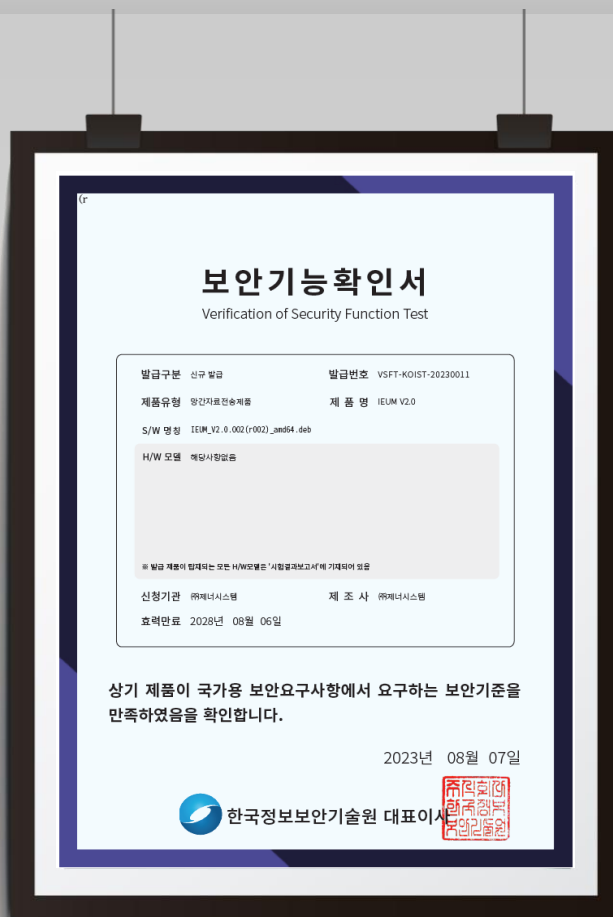
3. Network Interconnection Solution Certifications

Korea's First Product Certified under the National Intelligence Service (NIS) Security Requirements Version 3.0

Korea's First Data Transfer Product Certified with the NIS Security Function Verification Certificate



IEUM V2.0



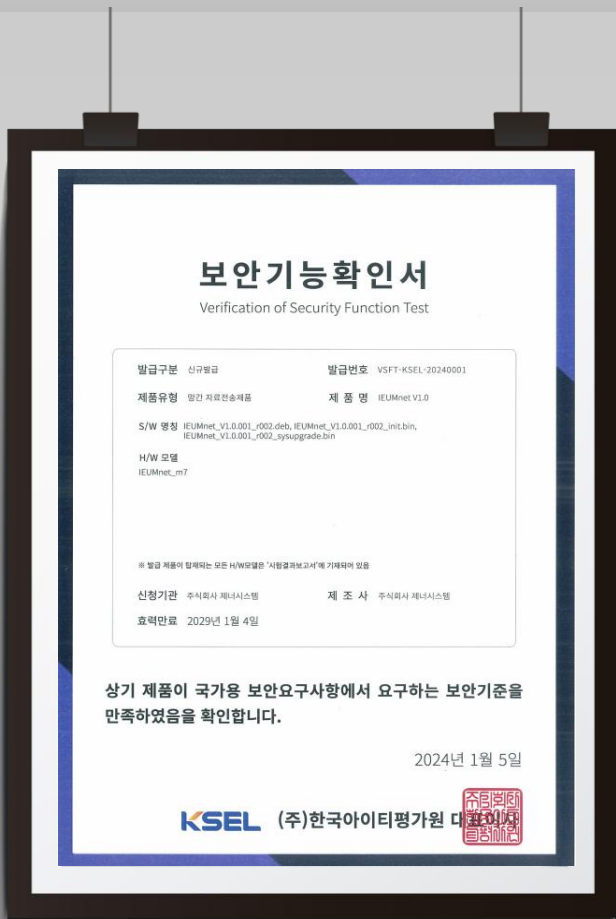
We propose an integrated secure gateway solution to protect your valuable information assets.

3. Network Interconnection Solution Certifications

Korea's First Product Certified under the National Intelligence Service (NIS) Security Requirements Version 3.0
Korea's First Data Transfer Product Certified with the NIS Security Function Verification Certificate



IEUMnet



We propose an integrated secure gateway solution to protect your valuable information assets.

JN JENER SYSTEM

02

PRODUCT DESCRIPTIONS

Network Interconnection Security Solution

1. Product Specifications

Korea's First Product Certified under the National Intelligence Service (NIS) Security Requirements Version 3.0
Korea's First Data Transfer Product Certified with the NIS Security Function Verification Certificate

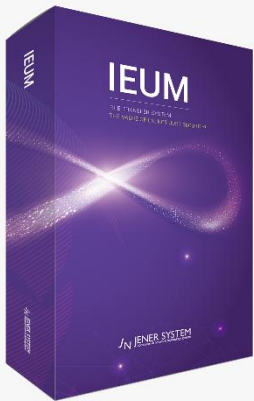
Product Features



Product Type	Network Interconnection Solution (Network Segmentation) / Korea's First Product Certified under NIS Security Requirements Version 3.0 / Korea's First Product Certified with the NIS Security Function Verification Certificate
Relay Method	Socket Device Method
NIC	1G * 8port(SFP), 10/100/1000BASE-TX * 8port 10G 2Port 추가 옵션
CPU	Intel 4 Core 3.2GHz
HDD	HDD 500GB * 2ea
Memory	8GB RAM
Power Supply	Redundant Power Supply

We propose an integrated secure gateway solution to protect your valuable information assets.

2. Network Interconnection Solution Procurement Registration

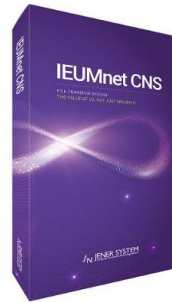


IEUM V2.0

Product Name : IEUMV20
Detailed Product Category : Security Software
Product ID : 25106380

Manufacturer	JENERSYSTEM Co., Ltd.
Contract Method	Third-Party Unit Price Contract
Commodity Classification Number	43233205
Product ID	25106380
Specification	Security Software, JENER SYSTEM, IEUM V2.0, Business Document Security Solution, 1 Package
Delivery Condition	On-Site Installation Included
Supply Region	Nationwide
Certifications	Security Function Verification Certificate, GS Certification Grade 1

Optional Products



IEUMnet CNS (Server)

Product Name : IEUMnetCNS
Detailed Product Category : Security Software
Product ID : 25342306



IEUMnet ONS (Client)

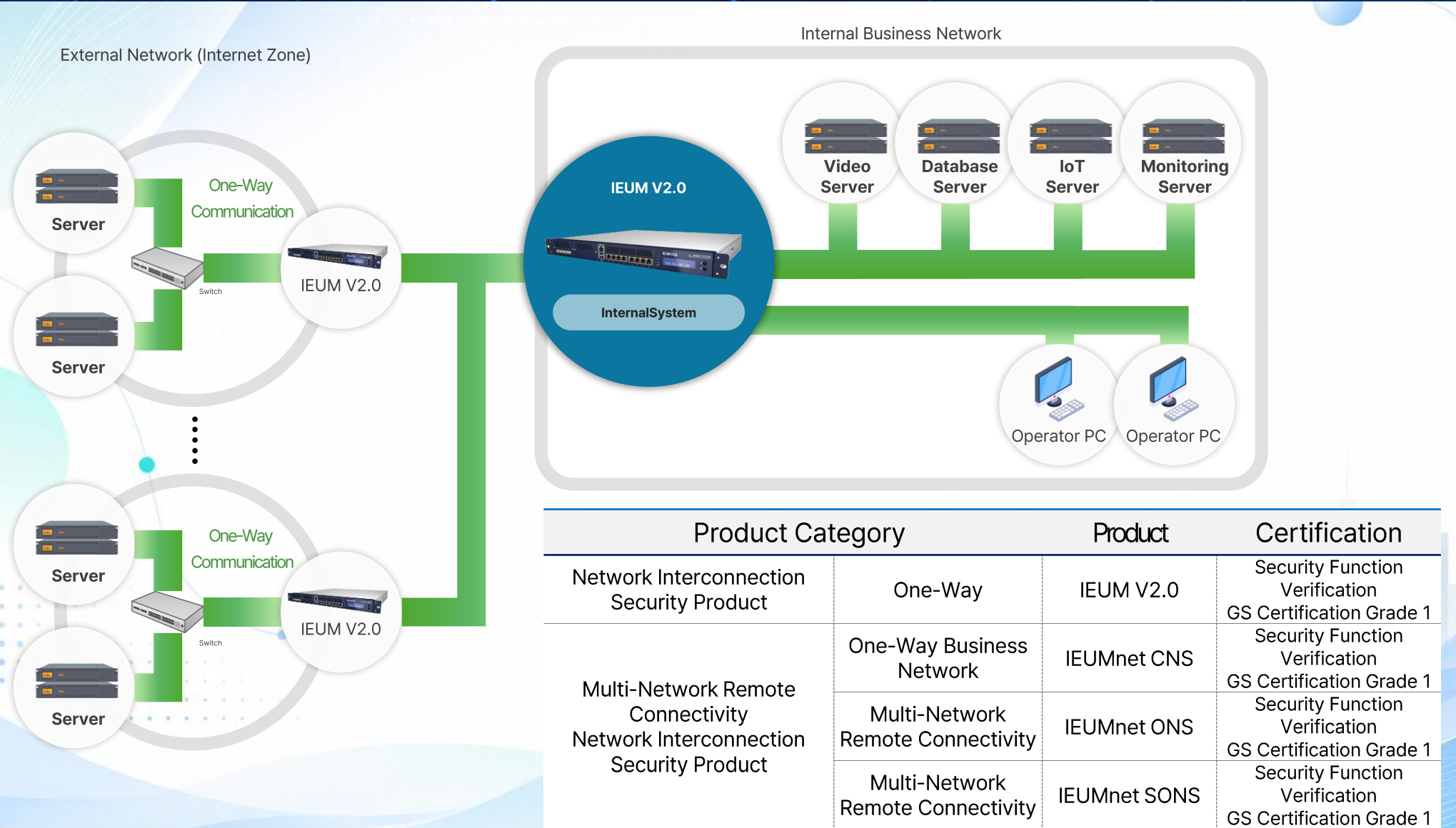
Product Name : IEUMnetONS
Detailed Product Category : Security Software
Product ID : 26050514



IEUMnet SONS (Client)

Product Name : IEUMnetSONS
Detailed Product Category : Security Software
Product ID : 25342307

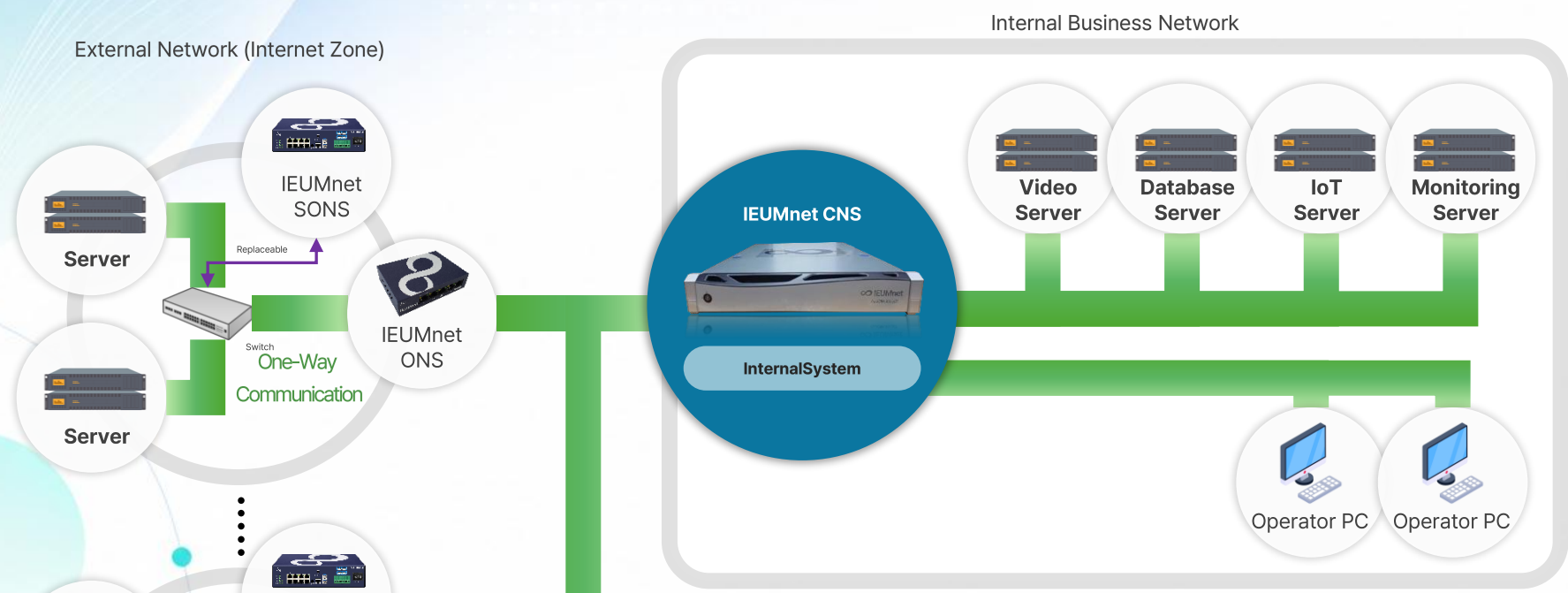
3. IEUM V2.0 Overview



Product Category		Product	Certification
Network Interconnection Security Product	One-Way	IEUM V2.0	Security Function Verification GS Certification Grade 1
	One-Way Business Network	IEUMnet CNS	Security Function Verification GS Certification Grade 1
	Multi-Network Remote Connectivity	IEUMnet ONS	Security Function Verification GS Certification Grade 1
	Multi-Network Remote Connectivity	IEUMnet SONS	Security Function Verification GS Certification Grade 1

We propose an integrated secure gateway solution to protect your valuable information assets.

4. IEUMNet Overview



Product Category		Product	Certification
Network Interconnection Security Product	One-Way	IEUM V2.0	Security Function Verification GS Certification Grade 1
	One-Way Business Network	IEUMnet CNS	Security Function Verification GS Certification Grade 1
Multi-Network Remote Connectivity Network Interconnection Security Product	Multi-Network Remote Connectivity	IEUMnet ONS	Security Function Verification GS Certification Grade 1
	Multi-Network Remote Connectivity	IEUMnet SONS	Security Function Verification GS Certification Grade 1

We propose an integrated secure gateway solution to protect your valuable information assets.

03

PRODUCT COMPETITIVENESS

Key Security Features and Solution Usability

1. Memory Vulnerability Issues in C and C++

JENER SYSTEM has completed the development of its products using Rust, a memory-safe programming language designed to address security vulnerabilities commonly found in C and C++.

Programming Language Security Vulnerabilities

White House Urges Transition Away from C and C++; Experts Call It a Timely Recommendation

2024.02.28 | Grant Gross | InfoWorld

The Biden Administration has urged software developers to move away from programming languages that are prone to buffer overflows and other memory access vulnerabilities.



In a blog post released on February 9, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) encouraged developers to adopt memory-safe programming languages. CISA, the Federal Bureau of Investigation (FBI), the National Security Agency (NSA), and allied government agencies also published a report titled "Memory Safe Roadmaps" in December of the previous year.

The 19-page report identified C and C++ as representative examples of programming languages vulnerable to memory safety issues and highlighted Rust as an example of a memory-safe language. In addition, an NSA Cybersecurity Information Sheet released in November 2022 listed Rust, C#, Go, Java, Ruby, and Swift as programming languages designed with memory safety considerations.

The Biden Administration's recommendation encourages software developers to discontinue the use of vulnerable programming languages such as C and C++ and instead adopt memory-safe programming languages.

2. Key Product Competitiveness

Korea's First Product Certified under NIS Security Requirements Version 3.0

Korea's First Data Transfer Product Certified with the NIS Security Function Verification Certificate

Security

- Secure system operation based on user authentication and access control
- Enhanced information protection through data encryption and access control
- Stable security architecture optimized for public-sector environments

The IEUM Series applies role-based access control and authentication mechanisms to prevent unauthorized access and ensure the secure management of critical data.

In addition, data encryption and audit logging capabilities enhance the protection of personal information and operational data. The solution provides a security architecture optimized for public institutions and administrative systems.

Operational history management and access tracking functions enable efficient incident response and security auditing.

User Convenience

- Provides an intuitive UI/UX for fast and easy operation
- User-centric design optimized for both mobile and PC environments
- Enables effective use with minimal training

The IEUM Series features a user-friendly and intuitive interface designed for ease of use.

A simplified menu structure and improved accessibility to key functions help increase operational efficiency, while providing a consistent user experience across both mobile and desktop environments.

In addition, automation features and reduced repetitive tasks help minimize user workload and maximize productivity.

Operational Convenience

- Provides centralized administration and monitoring functions
- Designed for easy maintenance and data management
- Supports real-time status monitoring and statistical reporting

The IEUM Series provides an integrated management platform that allows administrators to centrally manage users, permissions, data, and statistics.

Real-time monitoring and log management functions enable immediate visibility into system status and support rapid troubleshooting and maintenance.

Excel export, data backup, and administrative management functions further reduce operational burden.

Scalability

- Supports integration with various systems and external solutions
- Flexible architecture for feature expansion and customization
- Scalable platform designed for future service expansion

The IEUM Series is built on a modular architecture that enables easy feature expansion and system scalability.

Support for external APIs and third-party solutions ensures compatibility with existing systems while allowing customization based on organizational requirements.

The platform is also designed to flexibly accommodate emerging technologies such as AI, Big Data, and IoT in future deployments.

3. Core Features



Core Features

Provides essential features for efficient business operations while supporting integrated data management and system administration.



Threat Prevention

Effectively blocks external threats and unauthorized access through robust security controls and access management.



Reliability

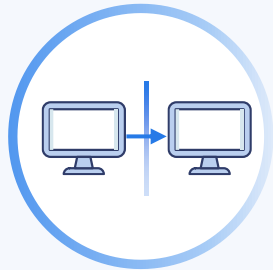
Provides failure prevention and data protection capabilities based on a stable operating environment.



Usability

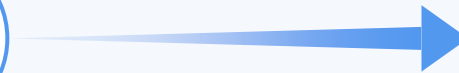
Enables users to operate the system quickly and easily through an intuitive user interface.

4. Security Features



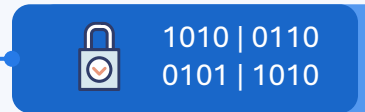
1. Unidirectional Communication

Enhances internal system protection by allowing data transmission only to external networks.



2. Dedicated Protocol

Ensures secure and reliable communication through the use of a dedicated protocol.



3. Encrypted Communication

Communication Channel Encryption Based on TLS 1.3
Utilizes International Standard Encryption Algorithms Including AES-256
Encryption Architecture Compliant with Domestic and International Security Requirements

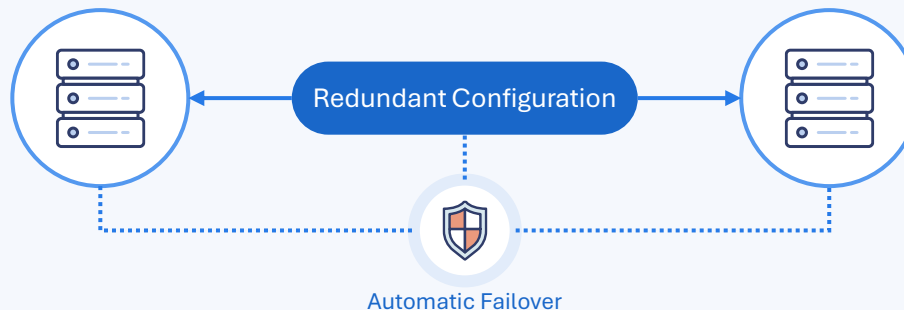


5. Key Features



1. High Availability (Redundancy)

Ensures service continuity by implementing redundancy for critical system components, providing stable operation even in the event of a failure.



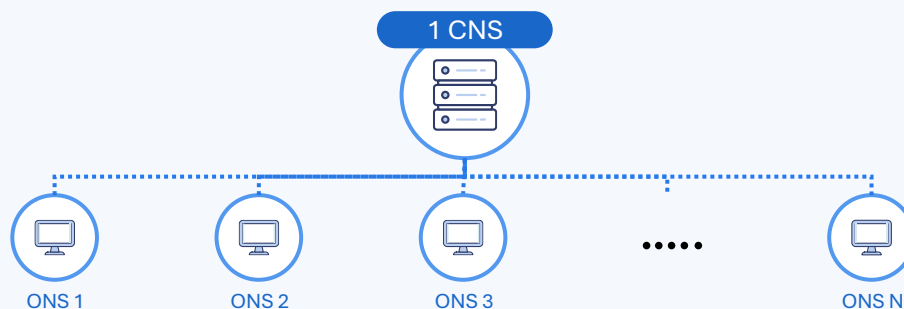
2. Monitoring

Monitors system status and performance in real time, rapidly detecting abnormal conditions to ensure stable operation.



3. Multi-Patch Management

A single IEUM V2.0 system centrally manages multiple IEUM V2.0 systems, enabling efficient patch deployment and administration while providing a scalable operating environment.



6. Ease of Management



1. Monitor system status in real time through an integrated management environment
2. From operational policies and user management to log analysis and statistical reporting
3. All functions can be efficiently managed from a single platform.



Status Monitoring

Provides real-time visibility into system status and resource utilization.



Policy Control

Enables centralized configuration and immediate application of operational policies.



Alert Management

Provides real-time notifications to administrators when abnormal events are detected.



User Management

Supports systematic user registration, modification, and deletion.



Access Control Management

Allows granular management of user roles and access permissions.



Audit Logs

Records all operational activities for security auditing and traceability.



Data Management

Enables efficient storage and management of operational data.



Backup Management

Ensures data reliability through regular backup operations.



Statistical Analysis

Provides operational status and performance metrics through comprehensive statistical reports.



7. Integrated Management Functions



Policy Configuration



Log Management



Dashboard

Statistical
Reports

Policy Configuration

- Provides functions for easily configuring and managing user permissions, security policies, and operational standards.
- Supports the application of policies tailored to organizational and operational environments, enabling stable and efficient system operation through a structured management framework.

Log Management

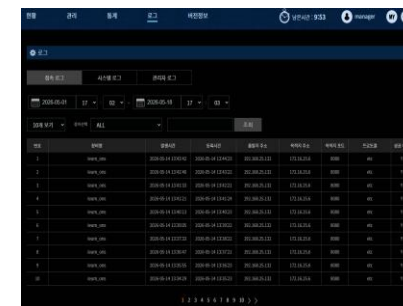
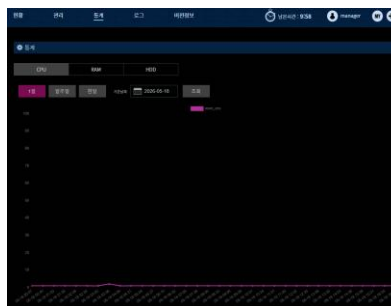
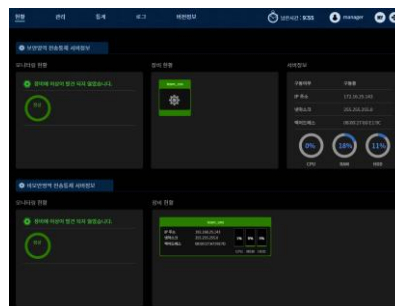
- Records and centrally manages user access logs, operational histories, and system events in real time.
- Enables rapid root-cause analysis during incidents and supports security audits and operational history management.

Dashboard

- Provides an integrated monitoring dashboard that offers a comprehensive view of system operations, device status, traffic, and key data.
- Its intuitive UI enables real-time visibility, improving operational efficiency and response speed.

Statistical Reports

- Provides operational data and system usage information through various statistical reports, supporting efficient data analysis and decision-making.
- Enables systematic performance management through period-based and category-based analysis functions.



We propose an integrated secure gateway solution to protect your valuable information assets.

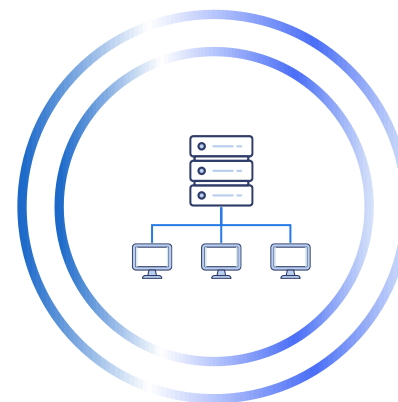
8. Encrypted Communication



Real-Time Data Transfer and Services Between
Secure and Non-Secure Networks

Single IEUM V2.0 Supporting Multiple IEUM V2.0
Connections

Unidirectional Whitelist-Based Access and Encrypted
Communication



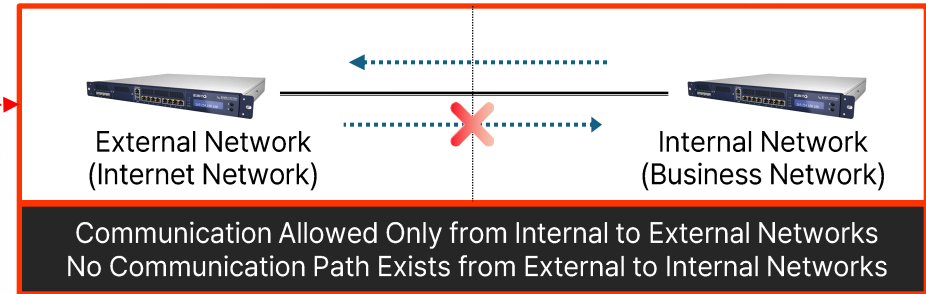
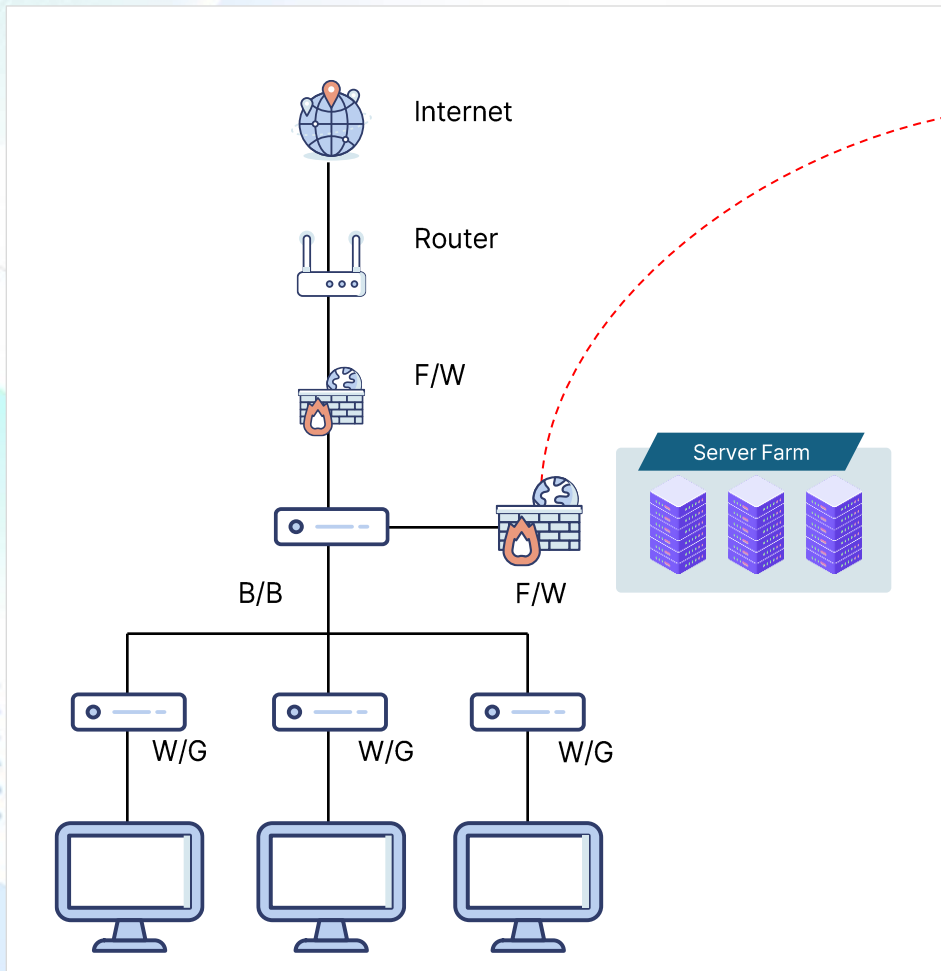
04

NETWORK CONNECTION TECHNOLOGY

Network Interconnection Solution Architecture and Technology

1. General Concept of Network Interconnection Solutions

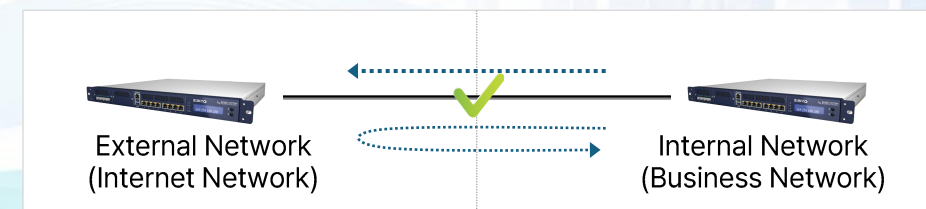
General Network Architecture



Basic Requirements for Network Interconnection

- ① Unidirectional Communication Across the Network Interconnection Section
- ② Encryption Across the Network Interconnection Section
- ③ Malware Inspection Across the Network Interconnection Section
- ④ Only Policy-Registered Devices Are Allowed to Communicate (Whitelist-Based)

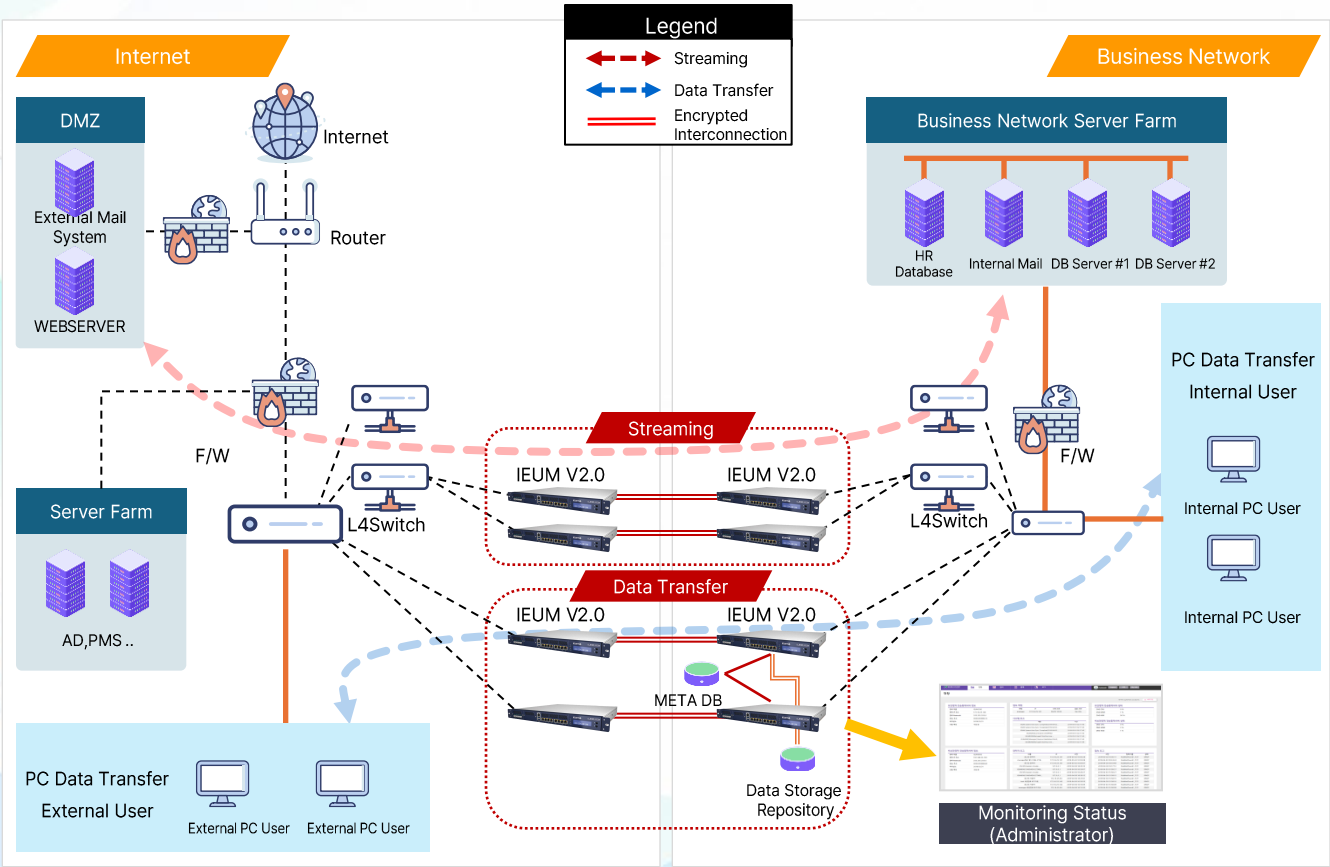
Method for Implementing Bidirectional Communication



2. Network Interconnection Architecture

According to the Security Requirements for National Information Security Products, network interconnection products are classified into Data Transfer Products, which transfer stored data (such as files) between user PCs on separated networks, and Streaming Interconnection Products, which provide service integration between servers located on different networks (such as service connectivity between an external web server and an internal database server).

Example Architecture in a Network Segmentation Environment



Example Required Equipment

Single Configuration	Component	Quantity
Data Transfer	Internal Network Server	1EA
	External Network Server	1EA
Streaming	Internal Network Server	1EA
	External Network Server	1EA

Single Configuration	Component	Quantity
Data Transfer	Internal Network Server	2EA
	External Network Server	2EA
	DB Synchronization Server	1EA
	Storage	1EA
Streaming	Internal Network Server	2EA
	External Network Server	2EA

Data Transfer	PC to PC File Transfer
Streaming	Server to Server service Interconnection

3. Analysis of Network Interconnection Methods

Network interconnection systems can be implemented using various relay media (transmission media). The security of a network interconnection solution is achieved through the control of relay devices rather than the relay media itself.

Category	Description	Interconnection Method
JENERSYSTEM IEUM	❖ Korea's First Product Certified with the NIS Security Function Verification Certificate (Security Requirements Version 3.0) ❖ Unidirectional Socket Device Method ❖ IEEE802 Interface (NIC-Based) - Supports up to 40G ❖ Excellent interoperability across diverse network environments, including remote-site connectivity and N:M multi-network interconnection ❖ No limitations on relay target control (supports control of more than 500 file extensions) ❖ Provides malware blocking through real-time packet analysis	Unidirectional Socket Device Access Blocking Unidirectional Socket Device Internal Network Transfer Control Server Various Network Cables External Network Transfer Control Server
Shared Storage Device Method	❖ CC Certification EAL2 ❖ Uses storage as the relay medium between network interconnection devices ❖ Network isolation using FCP ❖ Utilizes a public malware detection engine (ClamAV) ❖ Higher initial costs due to storage and SAN deployment ❖ Storage I/O speed determines the actual interconnection performance	HBA Device FCP HBA Device Internal Network Transfer Control Server Relay Storage External Network Transfer Control Server
IEEE 1394 Device Control Method	❖ CC Certification EAL2 ❖ IEEE 1394 Serial Bus Interface - Developed by Apple Inc. ❖ Limited network interfaces available for relay target connectivity ❖ Relay targets limited to 15 types ❖ Utilizes a public malware detection engine (ClamAV) ❖ Verification of Microsoft CAL policy required	1394 Device IEEE1394 Communication 1394 Device External Network Transfer Control Server External Network Transfer Control Server
InfiniBand Device Method	❖ CC Certification EAL2 ❖ Switch-Based Serial Interface - IBTA ❖ Designed to replace conventional I/O, currently operating as PCI-to-InfiniBand ❖ Utilizes a public malware detection engine (ClamAV) ❖ CC Certified in September 2015 - Limited deployment references available	HCA Device InfiniBand Communication HCA Device External Network Transfer Control Server External Network Transfer Control Server

Remark

For a high level of security, access must be blocked at both the Device Level and Network Level within the business environment.

05

DATA TRANSMISSION SYSTEM

Secure Data Transfer Through an Approval Process

1. Data Transfer Communication Method

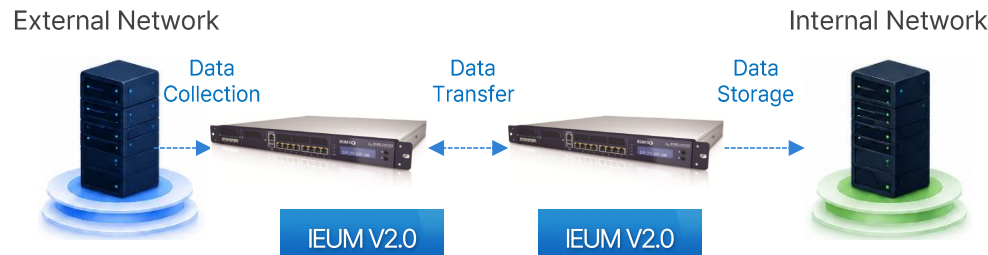
Supports data exchange between the Business Network and External Network through secure file-based data transfer.

File Transfer Method



- A method that securely collects files generated between the Business Network and Internet Network and transfers them through approved channels. Supports large-scale data transfers and provides a reliable data exchange environment through transfer history management and integrity verification.

Supports reliable data integration through secure session-based connection management



Key Features

- File-Based Data Transfer
- Large-Scale Data Transfer Support
- Transfer History Management
- Reliable Data Exchange

File Verification Method



- A security mechanism that performs malware scanning, file format validation, and integrity verification, allowing only verified and secure files to be transferred.
- Enhances security by preventing the import of unauthorized files and data.

Supports secure file-based data exchange between the Business Network and External Network



Key Features

- Malware Scanning
- File Integrity Verification
- Unauthorized File Blocking
- Secure Data Import

2. Data Transfer System

Data Transfer Products are used to transfer stored data (such as files) between user PCs located on separated networks.

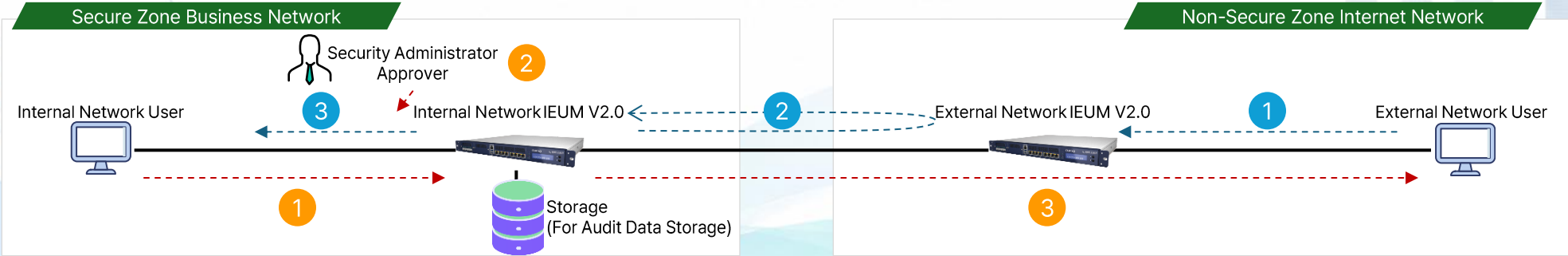
Data Transfer System

File Transfer Direction	Key Security Features	Common Security Features	
Internal Network ► External Network File Transfer	❖ Approval / Rejection of Data Export Requests ❖ Data Leakage Tracking	✓ Blocking of Tampered File Extensions ✓ Signature Verification of Approved Files	✓ Real-Time Deletion / Backup of Transferred Data ✓ Endpoint Control Based on User ID and IP/MAC Address
External Network ► Internal Network File Transfer	❖ Malware Scanning for Incoming External Files ❖ Incoming Data Tracking	✓ Encrypted File Transfer ✓ Generation of Audit Data for File Names and Import/Export Users	

Major Integrated Systems

Major Integrated Systems	① Integrated Authentication (SSO, AD, DB, and Third-Party Security Solution Login Integration)	③ Personal Information Detection System for Preventing Sensitive Data Leakage
	② HR Organizational Information for Approval Workflow Management	④ DLP, Document Security, and File Encryption Systems for Integrated Approval Management

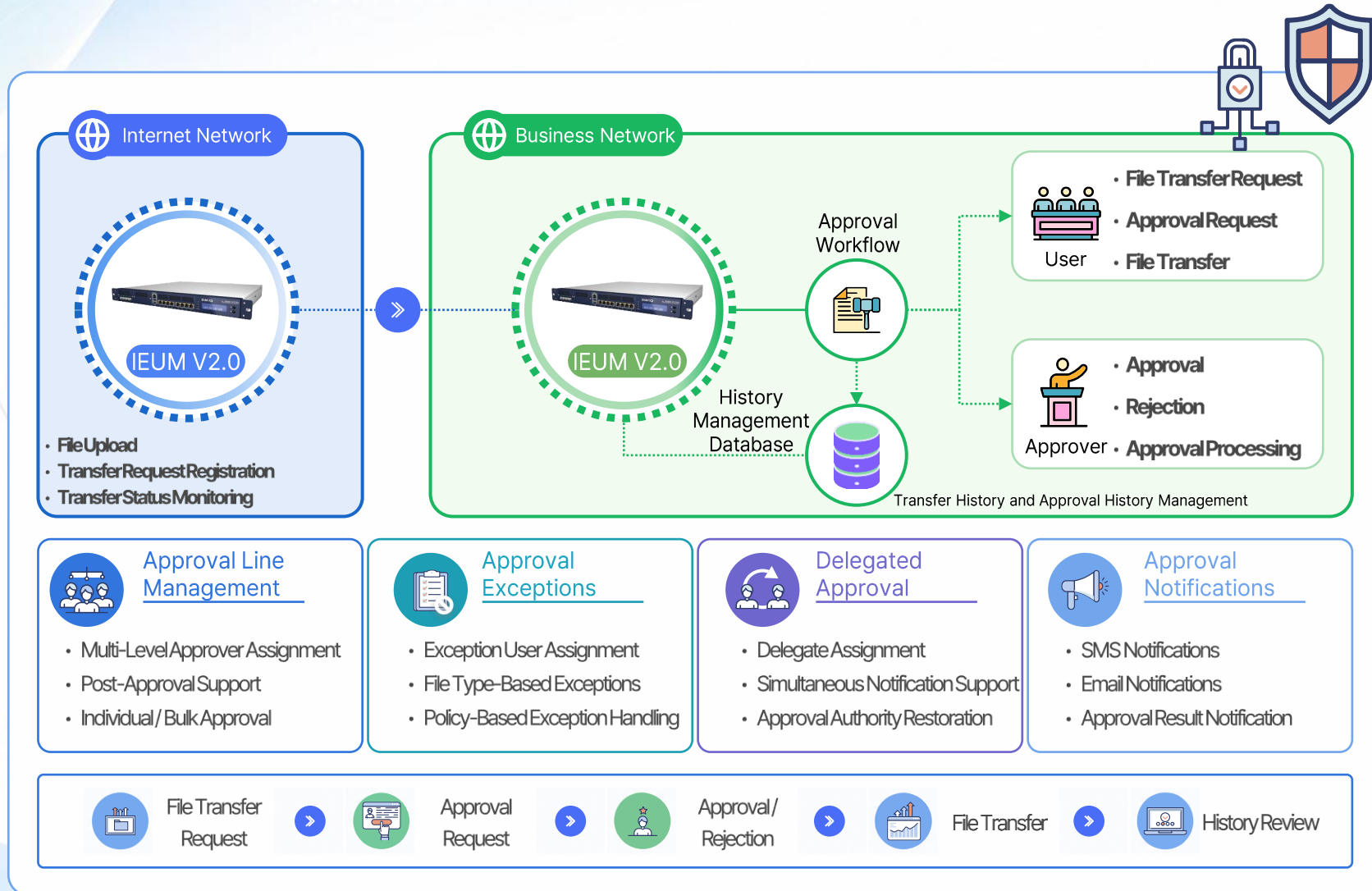
Data Transfer Process



We propose an integrated secure gateway solution to protect your valuable information assets.

3. File Transfer Approval Workflow

Provides a secure data transfer and systematic data import/export management environment through a robust approval workflow process.



06

STREAMING SYSTEM

Real-Time Secure Streaming Architecture

1. Streaming Gateway System

Streaming Gateway Products are used for service transmission between servers located on different networks (e.g., service integration between external web servers and internal database servers).

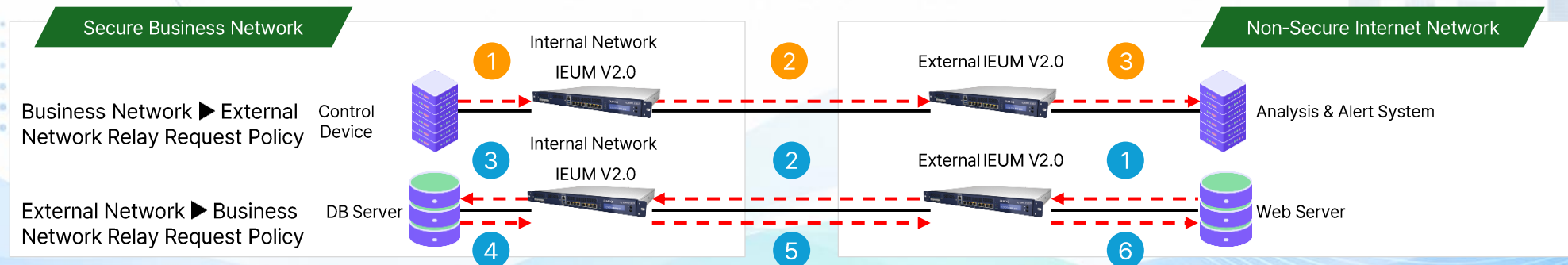
Streaming System Overview

Data Transmission Direction	Key Security Features	Common Security Features
Business Network ► External Network Relay Request Policy	❖ Collects requests from the Business Network to external servers and relays real-time communication with external servers	✓ Maintains unidirectional communication to prevent unauthorized inbound and outbound traffic. ✓ Eliminates communication paths and connectivity functions between relay zones.
External Network ► Business Network Relay Request Policy	❖ Collects requests from the Internet Network to Business Network servers and relays real-time communication with Business Network servers	✓ Relays only authorized packet data through application-layer protocol identification. ✓ Blocks relay requests from unauthorized zones and generates security audit logs.

Streaming System Use Cases

Use Cases	1. Data Integration Between Internet Web Servers and Business Network Civil Service Processing Systems 2. Remote Access to Intranet Systems (Smart Office) 3. Single Sign-On (SSO) Integration in Network Segmentation Environments	4. Integration of Shared Printer Servers and Fax Servers Between Business Network PCs and Internet Network PCs 5. Interconnection Between Internet Networks and Business Networks in Segmented Server Farm Environments 6. Establishment of an Integration Framework for Real-Time Business Processing with External Organizations
-----------	---	--

Streaming Relay Process



2. Streaming Communication Method

Streaming Gateway Products are used for service transmission between servers located on different networks (e.g., service integration between external web servers and internal database servers).

Segmented Session Connection



- Communication requests between the Business Network and Internet Network are managed on a session basis, allowing only authorized connections to be securely relayed.
- Connection status is continuously monitored and managed to block abnormal access and support stable service integration.

Supports reliable data integration through secure session-based connection management



특징

- Session-Based Connection Management
- Allows Only Authorized Communications
- Automatic Blocking of Abnormal Sessions
- Supports Stable Service Integration

Packet Filtering Method



- A security method that analyzes source, destination, protocol, and policy information of transmitted data packets and allows only authorized packets to pass.
- Enhances system security by blocking unnecessary or potentially harmful traffic.

A communication control method that enhances security by forwarding only packets permitted by policy.



특징

- Allows Only Authorized Packets
- Blocks Unauthorized Traffic
- Policy-Based Communication Control
- Enhanced Network Security

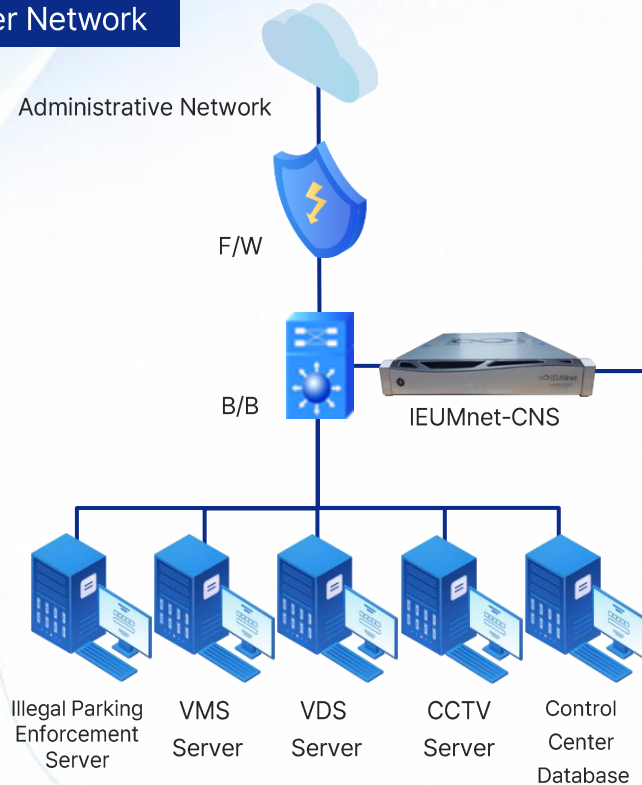
07

LINKED SERVICE

1:N and Multi-Solution Integration Architecture

1. System Integration Service – IEUMnet (CCTV Security)

Control Center Network



Remote Enclosure



Remote Enclosure



Configuration Description

1. Unauthorized device access is prevented in advance through pre-registration of MAC addresses. (Only authorized communication is permitted based on Source IP, Destination IP, and Destination Port.)
2. IEUMnet-CNS, installed and operated in the secure zone (management server area), has no response ports accessible from the non-secure zone. (Only policies configured by authorized IEUMnet administrators are applied. IEUMnet-CNS retrieves packets directed to IEUMnet-ONS through a predefined route without exposing the actual destination.)
3. Communication between the Control Center and remote CCTV sites is established through independent sessions on physically separated networks. Packets are reassembled (translated) before delivery, preventing critical data exposure during man-in-the-middle attacks and ensuring continuous service availability.

2. System Support Services – IEUM v2.0

IEUM V2.0 provides integration capabilities with a wide range of systems within the Business Network and enables customized interface configurations tailored to the customer's business environment.

Internet Network Integration



IEUM V2.0

- Supports integration with various external systems and services to ensure business continuity.

Business Network Integration



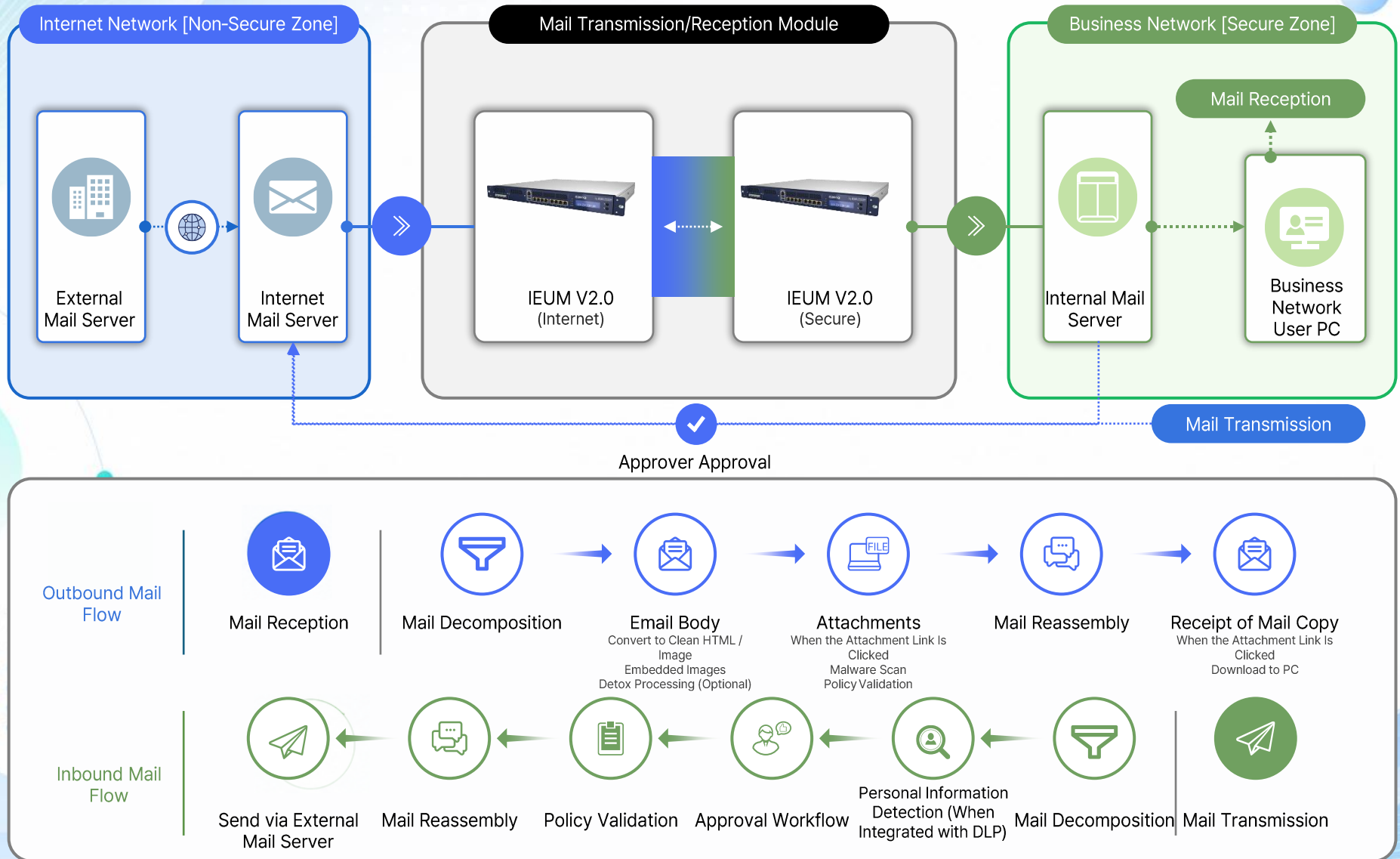
IEUM V2.0

- Supports reliable integration with HR, SSO, DRM, DLP, and other business systems within the Business Network.



Category	Business System Integration	API Integration	SSO Integration
Service Type	System Integration	Data Integration	Authentication Integration
Integration Target	Business Systems	External Systems	User Authentication
User	Business Network Users	Business Network Users	Business Network Users
Access Scope	Policy-Based Access	Policy-Based Access	Authentication-Based Access
Policy Configuration	Administrator Configuration	Administrator Configuration	Administrator Configuration
Security Features	Access Control	Data Validation	User Authentication
Key Benefits	Improved Business Efficiency	System Integration	Enhanced User Convenience
제공여부	Included	Optional	Optional

3. Mail Integration Service



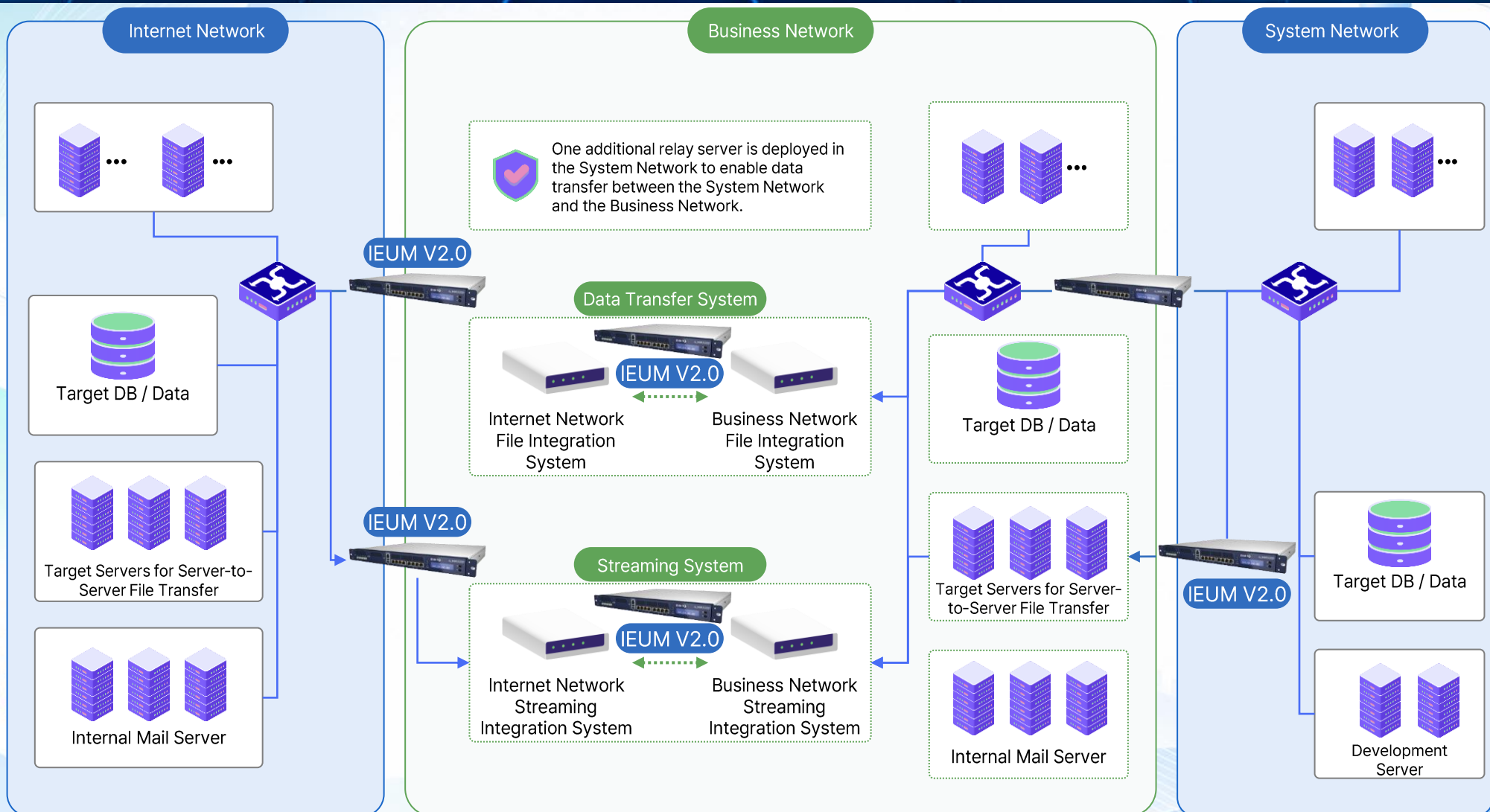
We propose an integrated secure gateway solution to protect your valuable information assets.

08

CASE OF CONSTRUCTION

Deployment Examples Across Various Environments

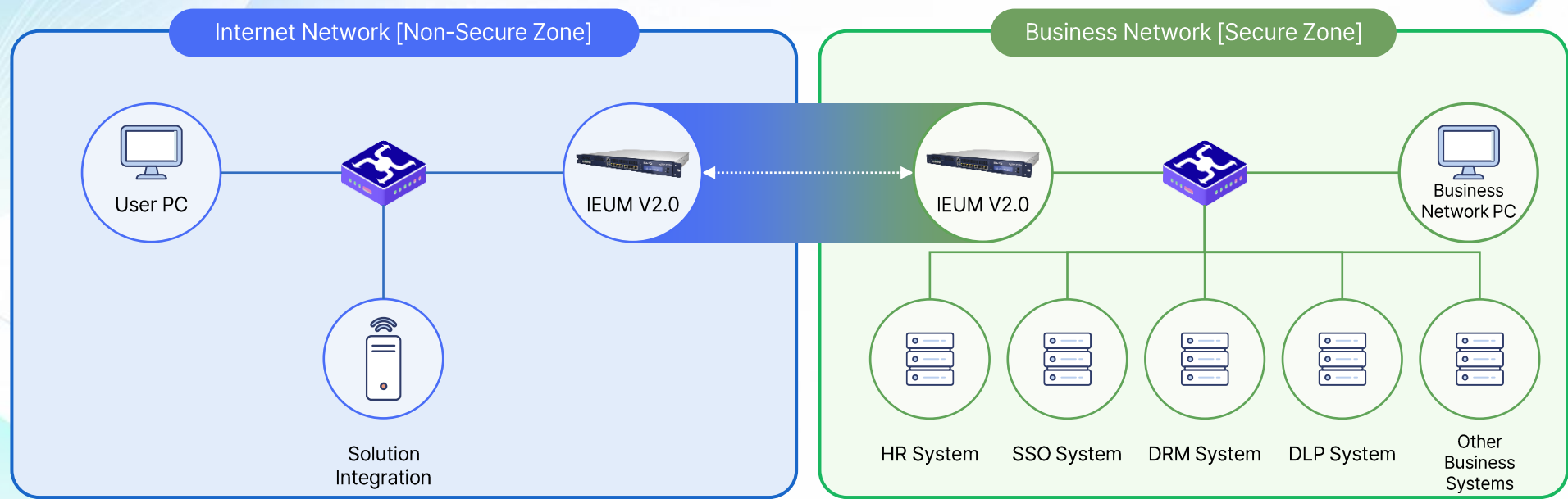
1. Three-Network Segmentation Deployment Example



* In a three-network architecture, an additional 0.5-unit External Network Relay Server is deployed in the System Network to enable outsourced maintenance providers to securely manage Business Network systems.

We propose an integrated secure gateway solution to protect your valuable information assets.

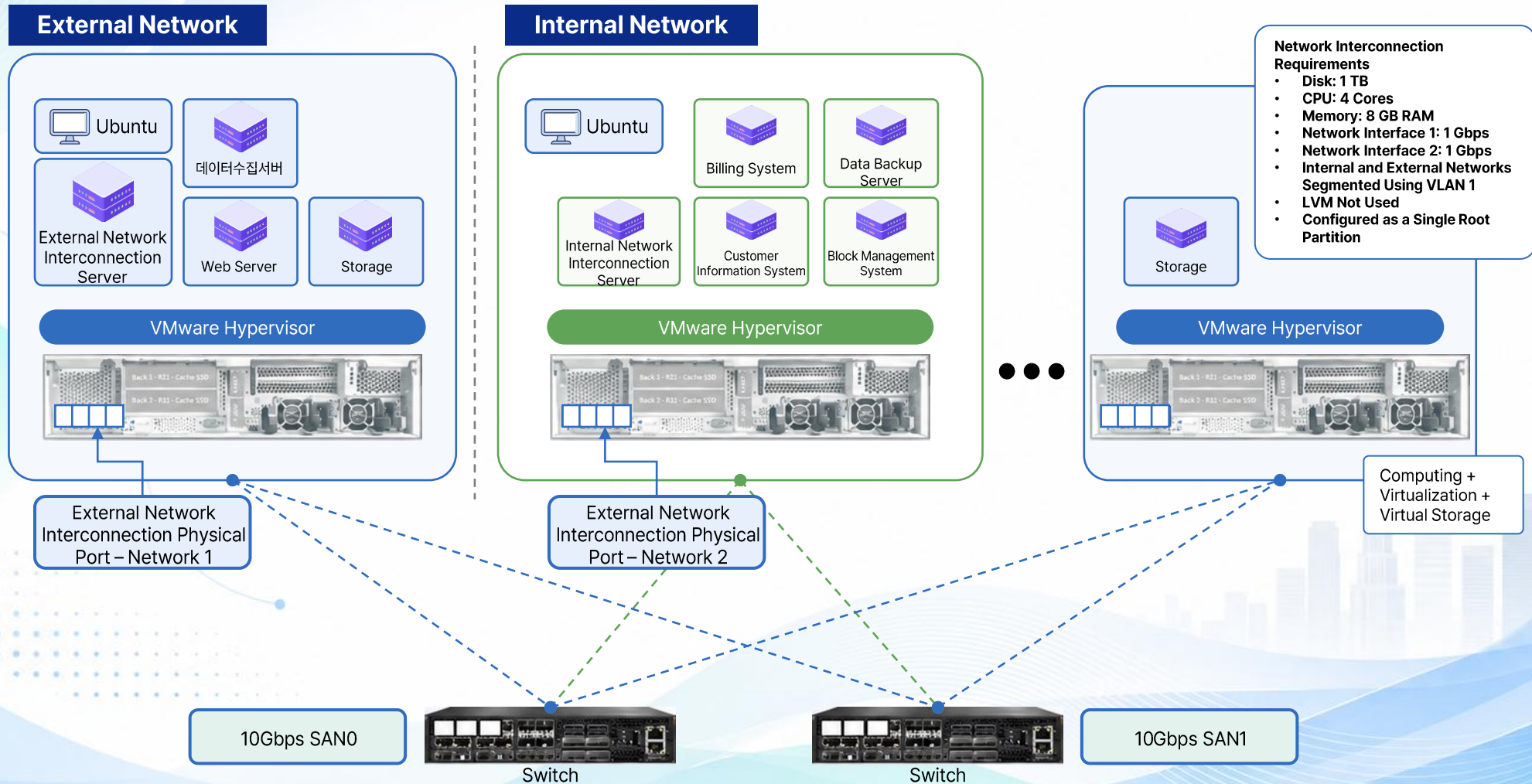
2. IEUM Deployment Architecture



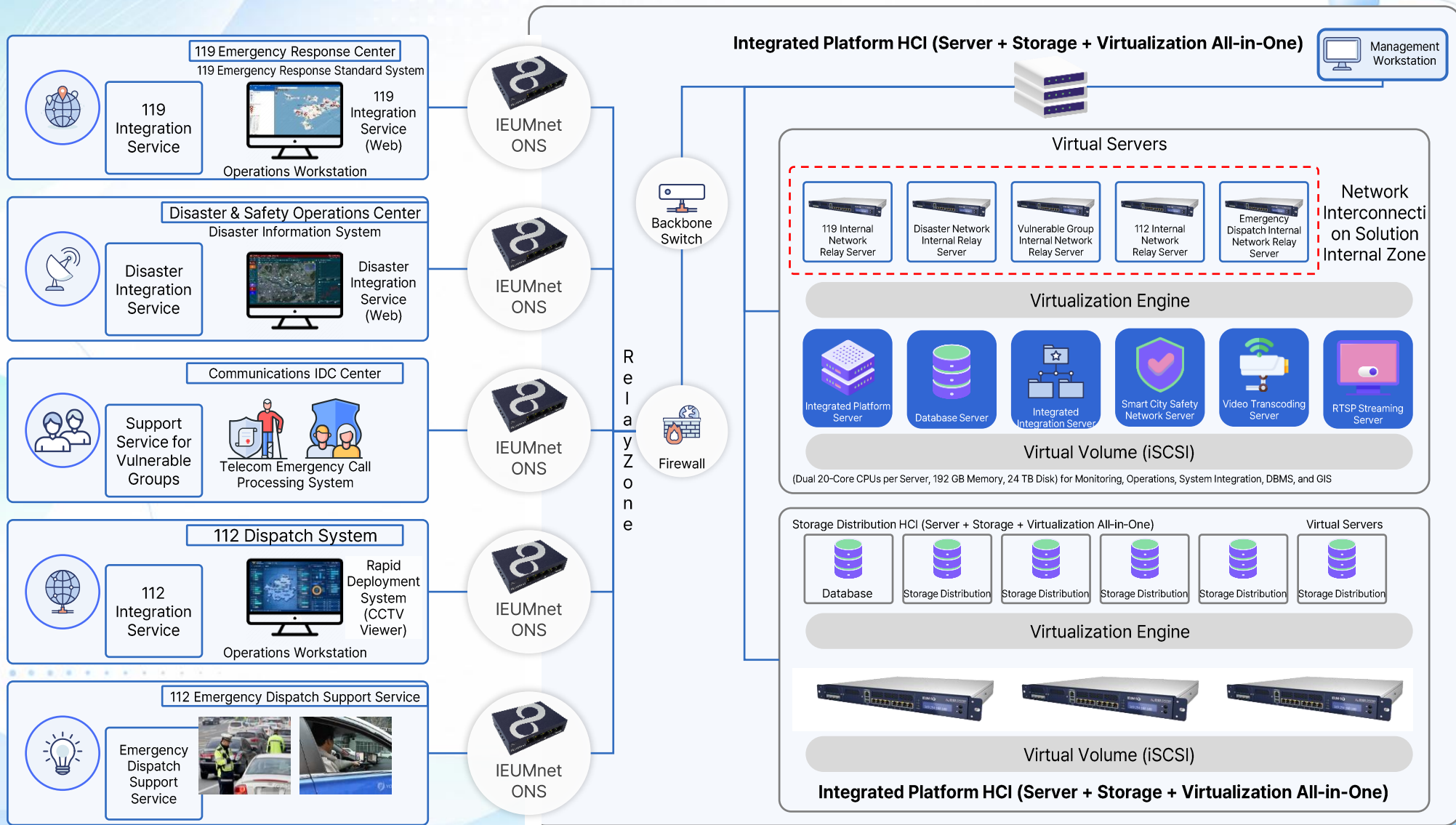
Category	HR System Integration	SSO Integration	DRM Integration	DLP Integration	Others
Integration Method	DB/API Integration	SSO Authentication Integration	API Integration	API Integration	API/DB Integration
Key Features	User Information Synchronization	Single Sign-On (SSO)	Document Security Enforcement	Personal Information Detection	Business System Integration
Requirements	DB or API Availability	Authentication Server Integration	API Availability	Policy Configuration	Interface Coordination
Expected Benefits	Automated Account Management	Improved Login Convenience	Enhanced Document Security	Prevention of Information Leakage	Improved Business Efficiency
Integration Examples	- Automatic User Information Synchronization - Organization Structure Integration - Automatic Account Creation and Update	- Provides Single Sign-On (SSO) - Unified User Authentication - Improved Login Convenience	- Document Encryption - Protection of Exported Data - Application of Document Security Policies	- Personal Information Detection - Sensitive Information Filtering - Export Approval Integration	- Groupware Integration - Electronic Approval System Integration - Business Portal Integration

We propose an integrated secure gateway solution to protect your valuable information assets.

3. Virtualized Network Interconnection Architecture

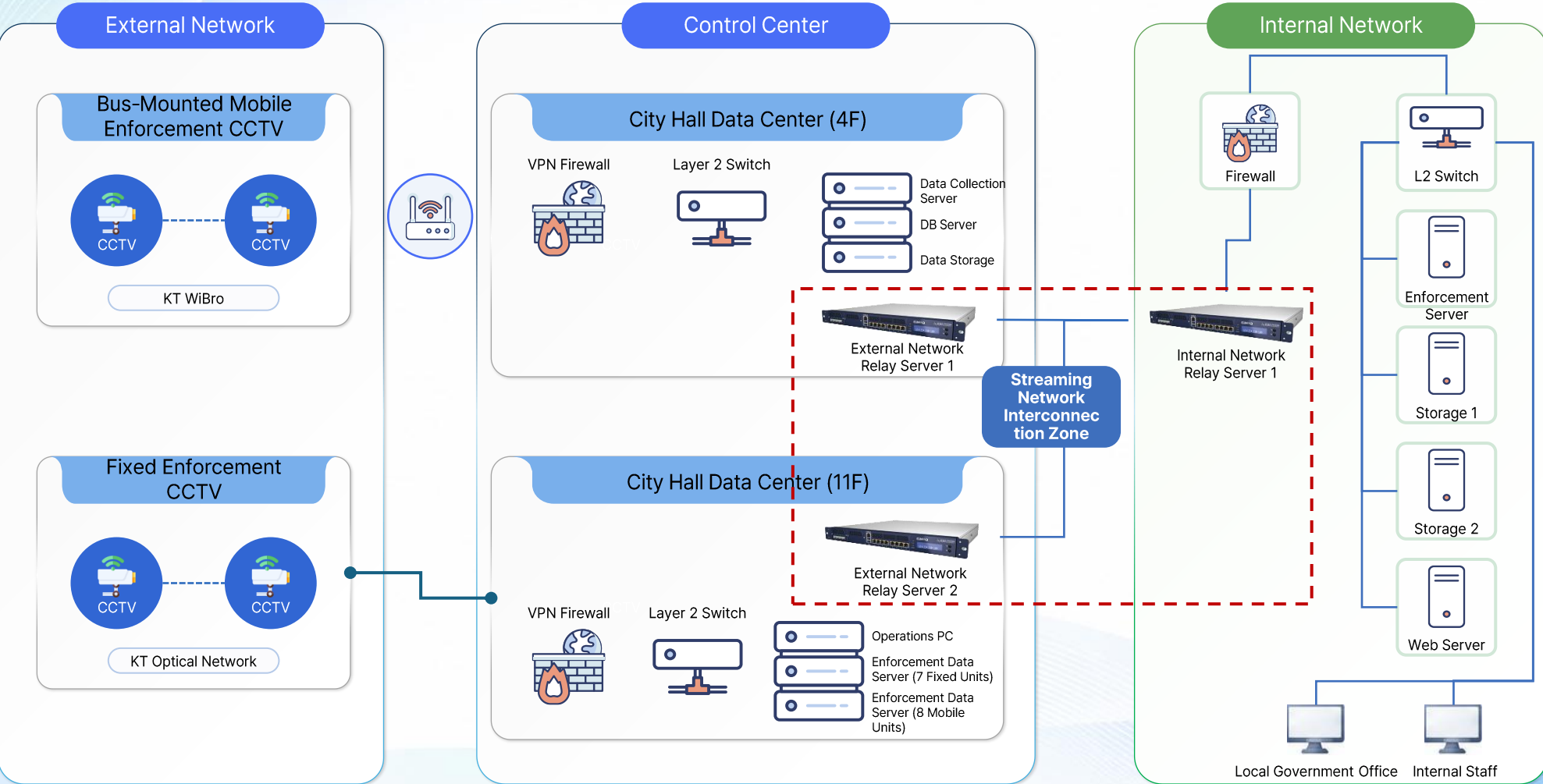


4. Integrated System Architecture



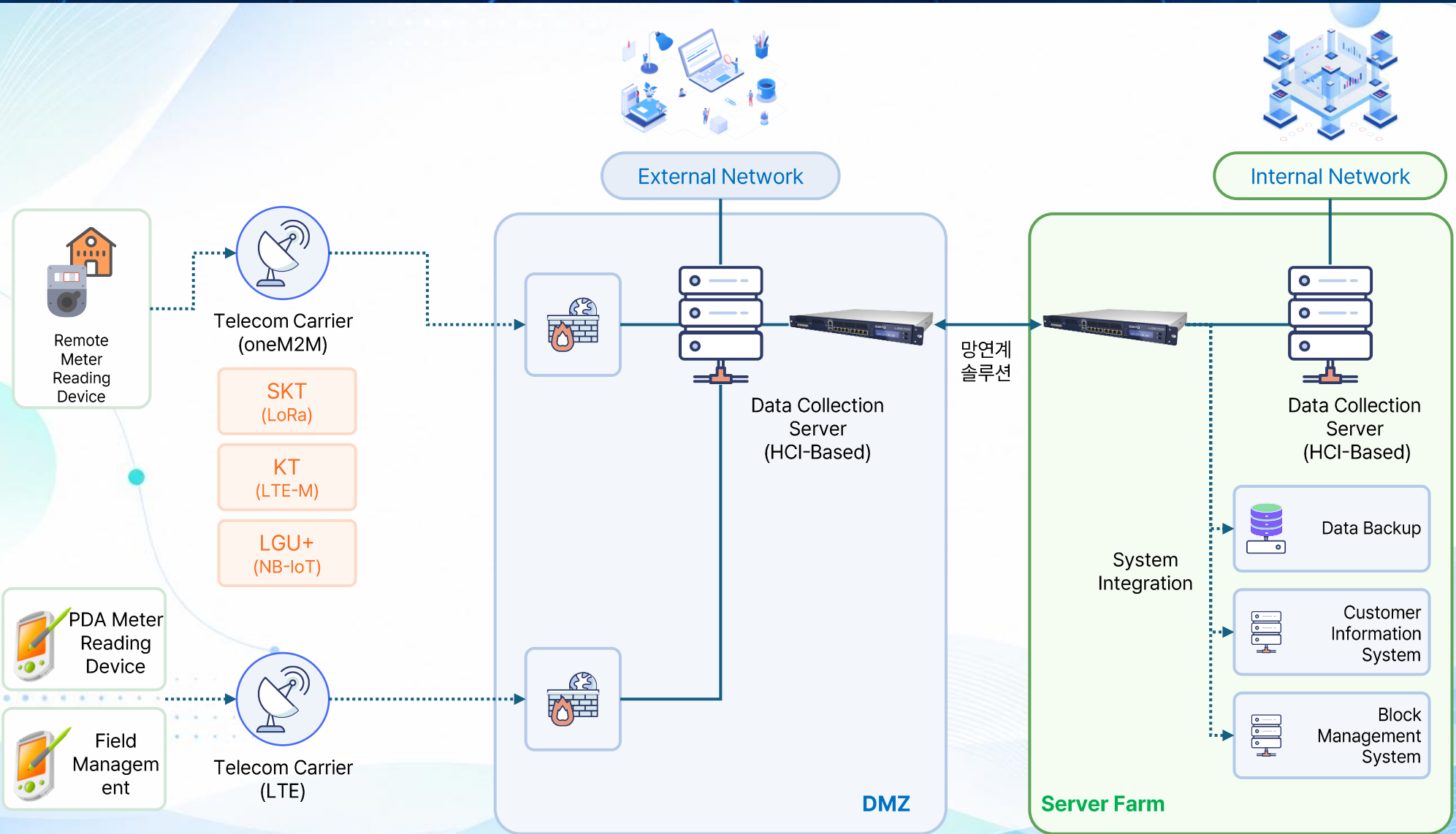
We propose an integrated secure gateway solution to protect your valuable information assets.

5. Mobile and Fixed Speed Enforcement Data Relay Deployment Example



We propose an integrated secure gateway solution to protect your valuable information assets.

6. Smart Water Remote Meter Reading System Deployment Example



We propose an integrated secure gateway solution to protect your valuable information assets.

7. Applicable Systems for Enhanced Network Security

 Remote Work	Instead of using an insecure VPN for remote work, a physical IEUM connection enables secure access to internal business systems from home while maintaining management records and audit logs.	 Wired & Wireless Integration	Can be flexibly deployed across wired networks and wireless networks such as LTE.
 Branch Office Connectivity	When connecting headquarters and branch offices, IEUM provides a higher level of security than conventional VPNs.	 Overseas Employees	Using IEUM to access internal business systems while working overseas improves management visibility and enhances security.
 Civil Service Issuance	IEUM can replace VPN-based networking in civil service issuance systems, providing a more secure architecture.	 Control Network	For remote control networks such as reservoirs and electric power networks, IEUM can be configured with unidirectional communication to enhance security.
 ATM Systems	IEUM can replace VPN-based networking for nationwide ATM systems, providing a more secure communication environment.	 Security System & Infrastructure Deployment	During infrastructure deployment, IEUM can establish secure isolation between multiple interconnected networks (M:N architecture).



Thank You

Thank You For Your Listening