

N-FORTRESS

운영 DB 앞에 안전한 관문을 둡니다.

DB에 대한 원격접속 해킹과 AI 공격을 방어하는 물리적 제로트러스트 네트워크 스위치

데이터는 흐르게, 해커는 들어올 수 없게

N-FORTRESS는 성벽과 해자처럼
외부와 내부의 직접 연결을 차단하고,
허용된 데이터만 안전하게 전달합니다.



직접 연결 경로 차단

외부와 내부의 네트워크를 분취하여
DB에 직접 접속할 수 없습니다.



데이터는 안전하게

허용된 쿼리에 의한 데이터만
정해진 경로로 전달됩니다.



원격 접속 및 공격 차단

임의 접근, 악성코드, 비정상 트래픽은
통과하지 못합니다.



기존 보안의 효과를 극대화

WAF, 방화벽 등 기존 보안 장비와 함께
운영되어 전체 보안 수준을 높입니다.

기존 보안장비: 수배 명단에 없는 침입자는 그대로 통과합니다.

시그니처 기반 탐지는 이미 알려진 공격만 걸러냅니다. 새 취약점과 새 악성코드는 명단에 없어 검문을 통과합니다.

현재는

경비병이 지명수배 명단만 들고 서 있습니다

명단에 있는 악성코드는 잡아냅니다.
그런데 처음 보는 악성코드는 그냥 들여보냅니다.

웹방화벽·백신: 알려진 공격 패턴을 탐지합니다.
새 취약점과 변형 악성코드는 패턴이 없습니다.



NF · 출입구 통제

얼굴을 보지 않고, 통로를 통제합니다

해커의 원격접속에 의한 데이터 탈취를 물리적으로 막습니다.
정상적인 쿼리에 의한 데이터만 보내줍니다.

N-FORTRESS: 운영 DB 앞단에서 직접 접속 경로를 차단하고,
정상적 요청에 의한 데이터 송수신만 중계합니다.

핵심 알려진 공격을 더 잘 찾는 문제가 아니라, 모르는 공격도 들어올 길이 없게 만드는 문제입니다.

제안 개요

문제

DB까지 바로 이어집니다

웹·앱 서버가 침해되면 운영 DB로 곧바로 연결됩니다. 기존 보안장비는 악성코드를 검사하지만 원격접속 경로를 막지 못합니다.

해법

경로를 끊고 중계합니다

DB 앞단에 NF를 두어 직접 접속을 차단하고, 허용된 업무 요청만 내부에서 별도 연결로 중계합니다.

효과

앞단이 뚫려도 DB는 열리지 않습니다

DB 직접 접속·스캔·임의 외부 연결이 되지 않고, DB 서버 IP도 외부에 드러나지 않습니다.

요청

PoC 실행

대상 DB 1종 · 기간 4주 정도의 PoC 실행을 제안합니다.

교체하지 않습니다

WAF · DB 접근제어 · 백업 모두 유지

구축·운영 범위

사전 검토 · PoC · 도입 설계

핵심 기술

Data Transistor · 특허출원

보안 장비는 늘었는데, DB로 가는 길은 열려 있습니다.

WAF와 방화벽은 성벽 밖을 지킵니다.
성문이 뚫린 다음, 운영 DB까지는 저항 없는 한 걸음입니다.

침해 이후 공격자가 쓰는 것은 새 취약점이 아니라,
이미 열려 있는 정상 DB 연결과 계정입니다.

1차 데이터 훼손·암호화·유출

2차 서비스 중단과 복구

3차 과징금·손해배상·신고

우선 검토 사항

“중요한 DB가 있다”와 “그 DB로 접근할 수 있는 경로가 있다”가 함께 있는 고객입니다.

01

웹 서비스와 핵심 DB가
연결돼 있다

웹.앱 서버 침해 후
DB 접근이 걱정되는 고객

02

외주 운영·원격 유지보수가
잦다

관리자·협력사 접속 경로를
함께 관리해야 하는 고객

03

AI·외부 서비스와
데이터를 연동한다

허용하지 않은 외부 연결이나
데이터 전송이 걱정되는 고객

04

데이터 유출·변조 시
업무 타격이 크다

개인정보·거래·생산 데이터를
엄격하게 보호해야 하는 고객

첫 질문 “해커에 의해 웹 서버나 관리 서버가 침해되면, 중요 DB에 직접 접속을 막을 수 있습니까?”

사이버 보안 관련 규제 강화!

2026.9.11부터 상한은 **전체 매출액의 10%**. 비교 대상은 보안 예산이 아니라 **사고 한 번의 비용**입니다.

국내 개인정보 유출·위반 과징금 사례			
쿠팡	3,750만 명 유출 · 무단 수집 (역대 최대)	6,247 억원	2026
SK텔레콤	가입자 2,324만 명 개인정보 유출	1,348 억원	2025
Google	동의 없는 개인정보 광고 활용	692 억원	2022
KT	개인정보 유출 · 무단 소액결제 피해	539 억원	2026
Meta	동의 없는 개인정보 광고 활용	308 억원	2022
카카오페이	알리페이 무단 제공 · 542만 명	151 억원	2024

개인정보보호위원회 공개 의결 기준 · 위 사례는 모두 개정 전 “관련 매출액 3%” 상한 아래에서 부과된 금액입니다. 2026.9.11부터는 전체 매출액 10%가 과징금이 될 수 있습니다.

기업 규모	전체 매출 가정	최대 과징금
중소기업	50 억원	5 억원
중견기업	300 억원	30 억원
대기업	3,000 억원	300 억원

2026.9.11 시행 개정법의 전체 매출액 10% 상한을 단순 적용한 예시입니다.

NF 도입 규모

장비 1식 수준

과징금이나 해킹 사고 처리 비용에 비교하면 NF 장비 도입이 훨씬 경제적입니다.

결재 논리 과징금은 사고 한 번에 수백억~수천억 단위입니다. 비교 대상이 보안 예산이 아니라 사고 비용입니다.

N-FORTRESS의 차별성

다섯 계층은 목적이 서로 다릅니다. NF는 **DB 연결 경로**를 다루면서 **질의·응답을 유지**하는 유일한 계층입니다.

구분	WAF	DB 접근제어	망분리	기존 데이터 다이오드	N-FORTRESS
무엇을 보는가	웹 요청 내용	계정·권한·질의	망 구간 전체	전송 방향	DB 연결 경로
앞단 침해 후	통과한 이후 구간은 관여하지 않음	탈취된 정상 계정은 허용됨	같은 망 안에서는 통제되지 않음	역방향 전송은 물리적으로 불가	직접 접속 자체가 되지 않음
DB 질의·응답	가능	가능	가능	불가: 단방향 전달만	가능: 요청 중계
업무 영향	낮음	낮음	높음 · 업무 구조 변경	높음 · 실시간 조회 불가	PoC로 사전 측정
NF와의 관계	그대로 유지	그대로 유지	부분 적용 시 보완	NF가 대체	DB 앞단에 추가

핵심 앞의 세 계층은 “무엇을 하는지”를 검사하고, 기존 다이오드는 “질의응답을 포기”합니다. NF는 **경로를 없애면서 업무를 유지**합니다.

PART 2 · 09-19장

해커의 원격 접속은 막고 데이터는 안전하게 방어

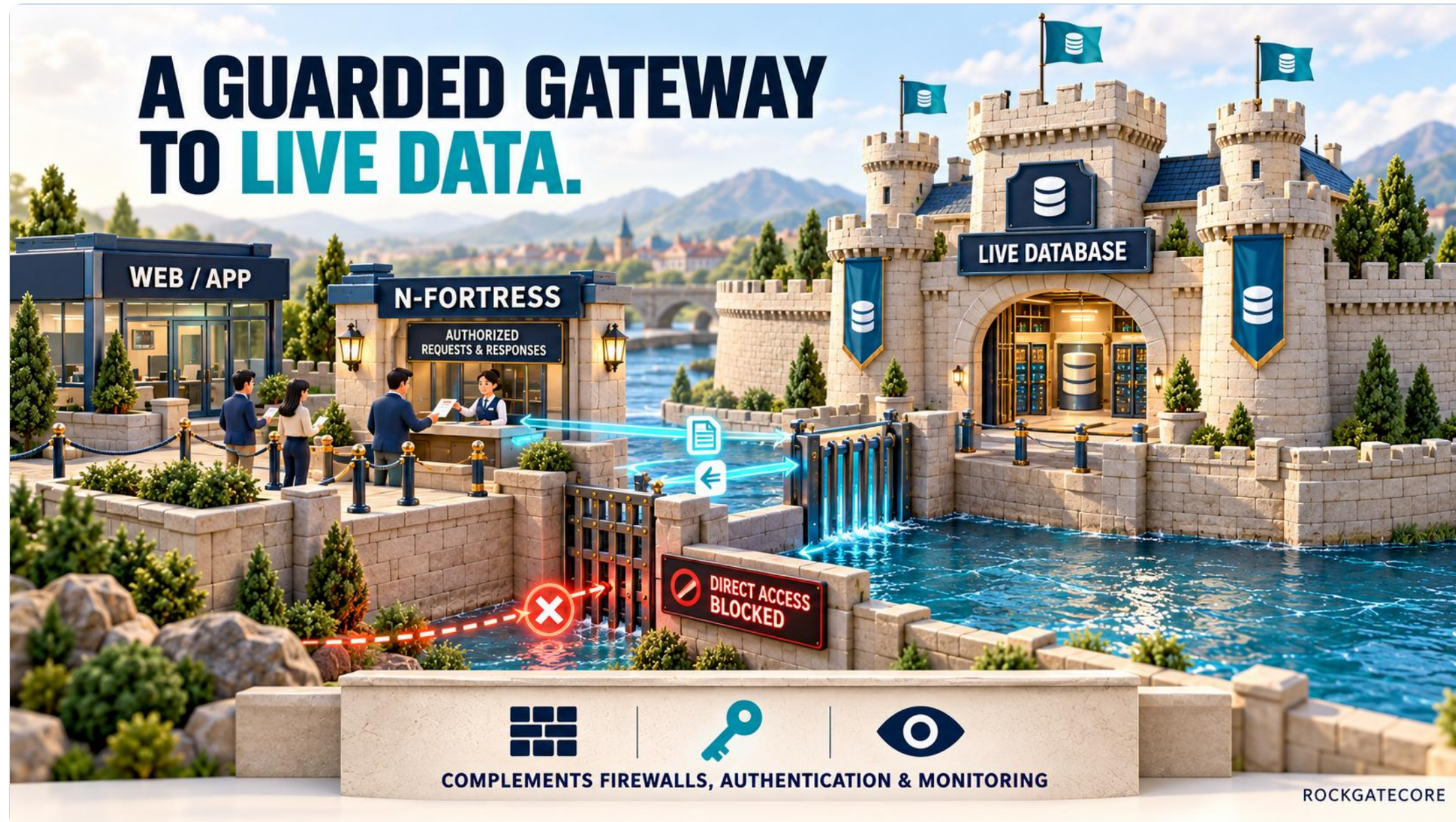
무엇을 어떻게 막는지,
어디에 어떻게 놓는지를 설명합니다.

원격 접속 · 악성코드 → 차단

정상 쿼리 · 응답 → 통과

물은 흐르지만, 사람은 들어올 수 없습니다.

성벽에 해자를 두르고 물길에 쇠창살을 설치하는 것과 같습니다. 데이터는 지나가고 침입자는 지나가지 못합니다.



해자 · 연결을 끊습니다

웹.앱 서버의 연결은 NF 앞에서 끝납니다. DB까지 이어지는 통로가 없습니다.

쇠창살 · 데이터만 통과

허용된 요청과 그 응답만 정해진 경로로 지나갑니다.

성벽 · 안에서 전달합니다

DB 연결은 보호 구간 안에서 따로 맺고, 결과만 돌려줍니다.

해커의 원격 접속은 입구에서 차단됩니다.

TCP/IP에 의한 해커의 원격접속 요청은 NF 앞에서 원천적으로 방지됩니다.



01 · 정상적인 데이터만 통신됩니다.

외부 세션은 TX 앞에서 종료됩니다.
해커는 DB 서버에 접속할 수 없습니다.

02 · TX · 새로 씁니다

허용된 질의 내용만 새 메시지로 다시 만듭니다.

03 · RX · 받기만 합니다

단방향 채널로 들어온 메시지만 DB 쪽 연결로 전달합니다.

NF 안에는 한쪽으로만 흐르는 두 개의 길이 있습니다.

단방향 데이터 다이오드를 이중으로 구성하여 물리적인 망분리 효과와 논리적 양방향 통신이 이루어집니다. - Data Transistor.



물리적 제로 트러스트 구현



TX·RX 물리 분리 · 광 절연 · OS 기반 장비

TX · RX 분리

보내는 서버와와 받는 서버가 물리적으로 분리되어 있습니다.

광 절연 Gap

두 카드 사이는 단방향 광케이블로만 이어집니다. 전기적 연결 구간이 없습니다.

단방향 GBIC

광 모듈 자체가 한쪽 방향으로만 데이터를 보냅니다.

해킹으로 침해할 수 없습니다.
원격으로 뚫을 물리적 경로가 없습니다.

OS 기반 장비

- CPU·메모리 위에서 OS가 구동됩니다.
- 로그·정책·연동은 고객 요구에 맞춰 커스터마이징할 수 있습니다.
- 시큐어코딩으로 취약점을 방지합니다.

기존 보안장비의 보안성을 한층 강화해 줍니다.

NF가 맡는 구간과 기존 장비가 계속 맡는 구간이 겹치지 않게 나눕니다.

NF가 더하는 층

도입하는 날 없어지는 경로

✓ DB 직접 스캔·접속

웹·앱 서버에서 보호 DB로 직접 연결하는 시도

✓ 임의 원격 제어 연결

허용되지 않은 관리·제어 세션을 만드는 시도

✓ 비인가 외부 연결

보호 구간에서 임의의 외부 통신을 시작하는 시도

기존 장비가 계속 맡는 층

그대로 쓰시면 됩니다

⊕ 계정·권한·질의 통제

DB 접근제어가 계속 담당합니다

⊕ 악성코드·행위 탐지

백신·EDR과 보안 패치가 계속 담당합니다

⊕ 보호 구간 밖의 관리 경로

기존 접근통제 정책으로 함께 점검합니다

감사 추적

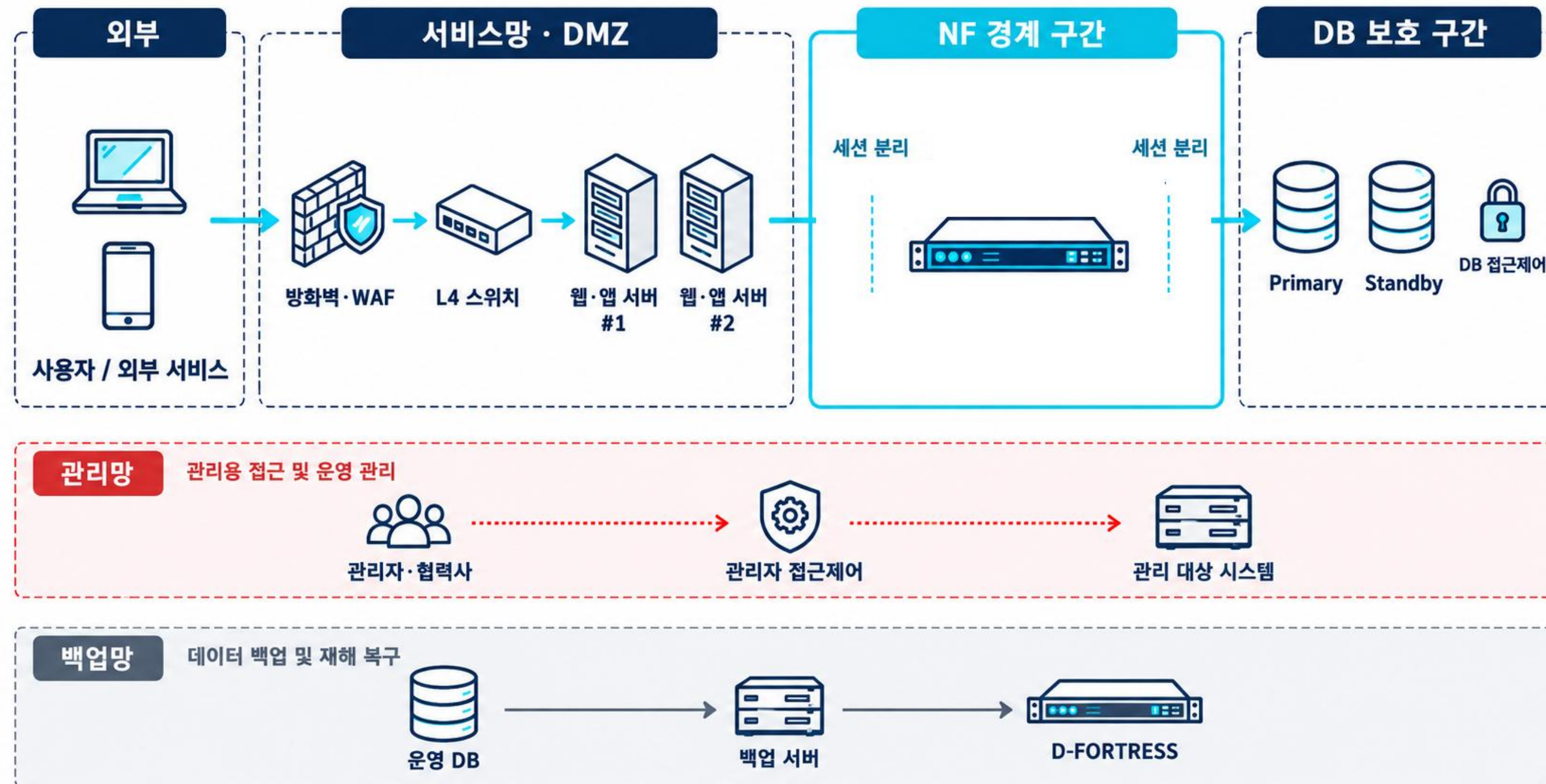
웹 서버 로그 · NF 중계 기록 · DB 접근제어 로그를 하나의 식별자로 연결 해 “누가 무엇을 조회했는지”를 남깁니다.
경로가 하나뿐이라 로그 누락이 없습니다.

감사 추적 설계안 · NF는 OS가 구동되는 장비이므로 로그 연결 방식은 요구에 맞춰 구현합니다 · 세부 범위는 사전 검토에서 확정합니다.



NF 시스템 구성도

세션 분리 · 후면 통제 경로



산업별 적용 방안

같은 NF라도 보호 대상과 시험할 업무가 다릅니다. 고객의 실제 데이터 흐름부터 확인합니다.

 병원·의료 진료·검사 DB 진료정보 연계 시험할 것 업무 조회가 유지되는지 민감정보 접근이 제한되는지	 금융·핀테크 고객·거래 DB 거래·조회 서비스 시험할 것 거래 정합성이 유지되는지 응답 지연이 허용 범위인지	 제조·물류 생산·업무 DB 생산·ERP 연계 시험할 것 업무 처리에 지장이 없는지 장애 시 운영이 가능한지	 공공·국방 기관 업무 DB 기관·시스템 연계 시험할 것 허용 경계가 분명한지 검증 증거가 남는지
--	---	---	---

우선순위 “사고 영향이 크고, 직접 접속 경로를 줄일 수 있는 구간”부터 제안합니다.

적용 검토 예시 · 업종별 규제 충족·특정 시스템 호환성·도입 실적을 의미하지 않습니다.

AI의 탈주에 의한 보안 사고 방지

AI의 판단이 잘못되어 외부로 탈출을 시도할 때, 정책이 아니라 물리적으로 막습니다.



허용된 업무는 그대로

등록된 연결과 정상 응답만 지나갑니다.
AI의 정상 업무는 그대로 동작합니다.

목록 밖 연결은 실패

외부와 허용되지 않은 통신을 하거나, 다른 AI를
원격으로 조정하려고 할때 물리적 원천 방어

권한은 함께 설계

허용된 연결 안의 오용은 반출 정책·도구 권한 설계
로 함께 통제합니다.

AI 적용은 구성별 검증 대상 · 참고: OWASP LLM 취약점(과도한 자율성·민감정보 노출)

연결은 허용하고, 위협은 경계에서 끊습니다

NF는 침입과 AI의 무단 외부 통신을 통제하고, DF는 핵심 데이터를 격리 백업합니다.

연결 관리

Mapping & Coordination



범례

승인된 통신

차단 대상

Fortress Net

보안 연결망 · 100.x.x.x

적용 개념도 · 실제 도입·연결 현황 아님 · 주소는 예시

국내 공공·AI 인프라 거점



Sovereign AI Center

연산 운영 · 데이터 보호 · 격리 백업

DATA TRANSISTOR

허용된 데이터만 전달하는 보안 경계



01 NF · 침입 차단

외부의 비인가 접근을 통신 경계에서 통제

02 NF · AI 통신 통제

무단 외부 통신과 데이터 반출 경로를 제한

03 DF · 격리 백업

핵심 데이터를 보호하고 복구 기반을 확보

PART 3

PoC 실행 방안

합격 기준을 먼저 정하고, 정상 업무와 차단 범위를
같은 조건에서 확인합니다.

합격 기준 · 사전 합의

사전 확인 3건

시험 항목 7건

4주

사전 확인 3건, 시험 항목 7건, 4주

합격 기준은 시험 전에 합의하고, 결과는 “차단된 것 · 허용된 것 · 업무 영향”으로 나누어 제출합니다.

사전 확인

- 01

연결 환경 사용 중인 DB와 버전, 접속 방식, 동시 연결 수
- 02

업무 영향 드라이버·접속 설정·세션 유지 방식 변경 여부
- 03

보호 경계 관리망·백업망 우회 경로, 장애 시 통신 정책, 복구 절차

PoC 시험 항목 · 4주

- 01 DB 직접 접속

탐색·직접 연결 제한 확인
- 02 비인가 요청

허용 범위 밖 요청 처리 확인
- 03 외부 연결

임의 외부 연결·우회 경로 확인
- 04 업무 호환성

조회·입력·수정과 응답 정합성
- 05 성능 영향

처리량·응답시간 동일 조건 비교
- 06 장애 동작

장비·전원 장애 영향과 복구 절차
- 07 감사 추적

웹·NF·DB 로그가 하나로 이어져 “누가 무엇을 조회했는지” 재구성되는지 확인

운영 데이터는 지키고, 복구 기반은 남깁니다.

N-FORTRESS는 운영 DB의 접속 경로를, D-FORTRESS는 백업 데이터의 물리 격리를 말합니다.



N-FORTRESS

운영 DB 보호 게이트웨이

Flyocto 서비스 망과 고객사 실망 운영 중

D-FORTRESS

물리 격리 백업 솔루션

코스닥 상장사 구축 완료

- 135 TB · 2,443만 파일 무손실 백업

핵심 기술 Data Transistor

특허출원 10-2026-0062192

FAQ

기존 장비 교체 여부, 프로그램 변경 범위, 보호 범위, 장애 시 동작, 그리고 유지보수 방식입니다.

Q WAF나 DB 접근제어를 대체합니까?

아닙니다. 웹 공격 탐지와 계정·질의 통제는 유지하고, NF는 운영 DB 앞단의 직접 통신을 분리합니다.

Q 기존 프로그램을 수정해야 합니까?

애플리케이션 코드는 수정하지 않습니다. **접속 주소를 NF로 바꾸는 것이 기본이며**, 표준 DB 포트를 그대로 받습니다. 드라이버·접속 설정 호환성은 PoC에서 확인합니다.

Q 모든 데이터 유출을 막을 수 있습니까?

직접 접속 차단과 모든 유출 방지는 다릅니다. 허용 요청의 악용은 권한·반출 통제로 함께 관리합니다.

Q 장비 장애 시 서비스도 멈추니까?

현재는 단일 장비 구성입니다. 장애 시 통신을 차단할지 우회할지 정책을 도입 전에 정하고, 예비 장비와 복구 절차를 함께 설계합니다. 실제 동작은 PoC 06번 항목에서 확인합니다.

Q DB 구간은 원격으로 유지보수할 수 있습니까?

네트워크를 통한 접근은 되지 않습니다. 관리·유지보수 경로까지 끊는 것이 이 구조의 목적이기 때문입니다. **보호 구간 작업은 현장 접근으로 수행** 하며, 작업 주기와 절차를 도입 전에 정합니다. 운영 편의는 줄지만, 원격으로 뚫릴 경로가 남지 않습니다.

철저한 현장 테스트 후 도입을 결정하셔도 됩니다.

업무 구간 한 곳을 골라 실제 DB 연결 구조를 확인하고, 정상 업무와 차단 범위를 함께 검증합니다.

01

기술 검토

대상 DB와 연결 경로 확인

02

대상 구간 선정

1주 · 합격 기준 사전 합의

03

PoC 진행

4주 · 보안·업무·성능 동일 조건 검증

04

도입 제안 확정

구성·공급·운영 조건 확정

기존 보안을 유지하면서, DB 직접 접속을 분리합니다.

문의처: cmo@rockgatecore.com · 070-8080-4910



N-FORTRESS

AI 시대에 데이터는 가장 소중한 자산입니다.

주식회사 락게이트코어 · rockgatecore.com / 김재원 마케팅총괄 이사: 010-4937-3413

ROCKGATE
CORE