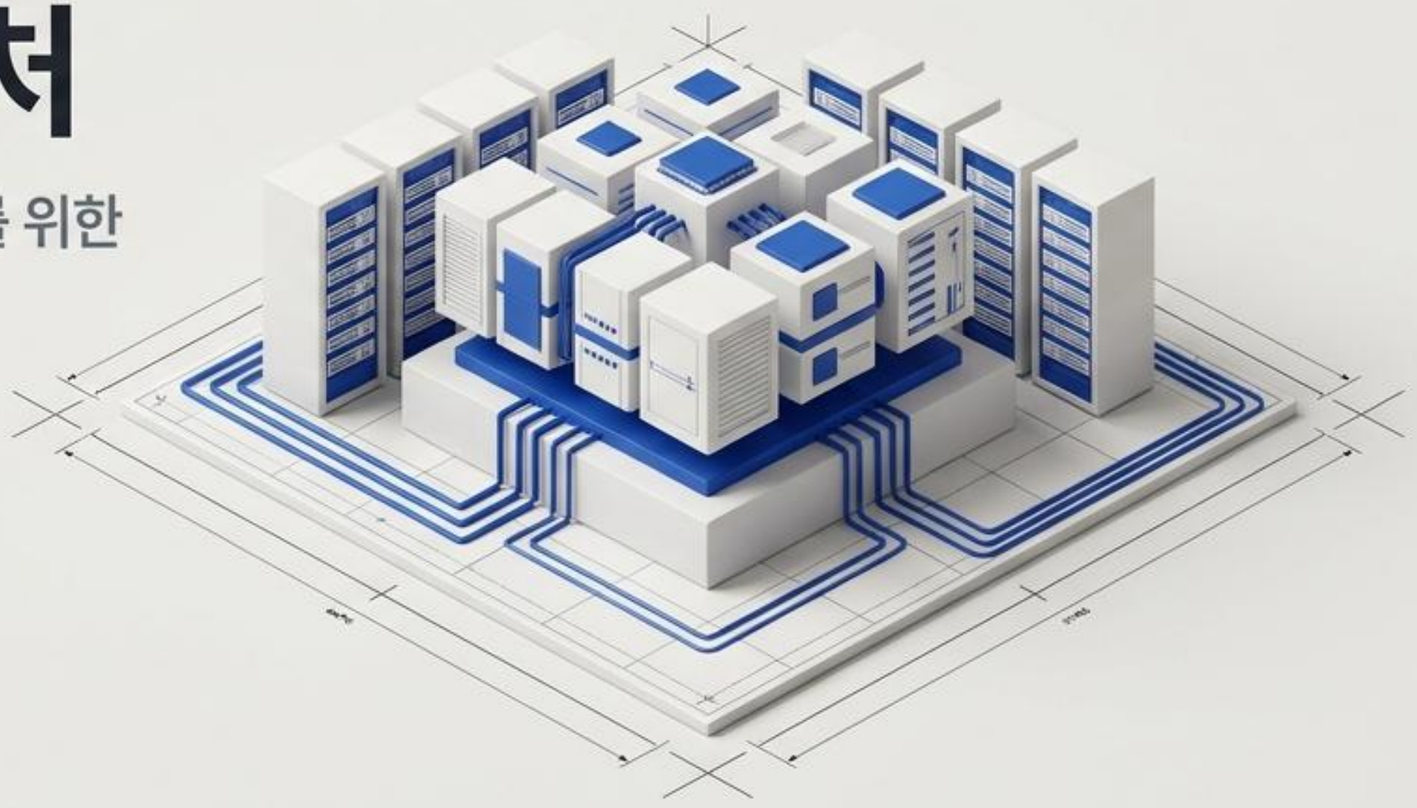
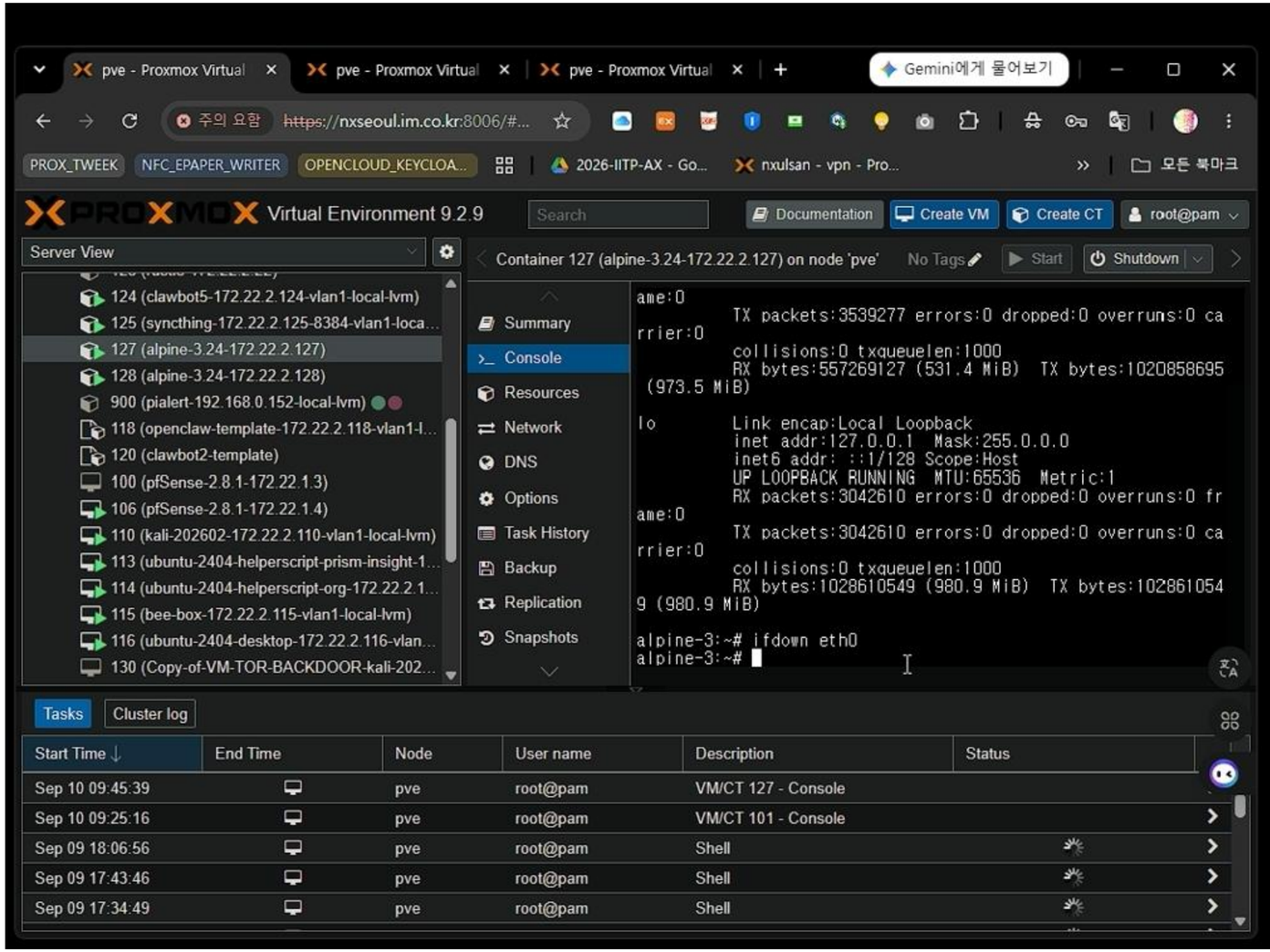
C-Level 및 IT 아키텍트를 위한 실행 가능한 청사진

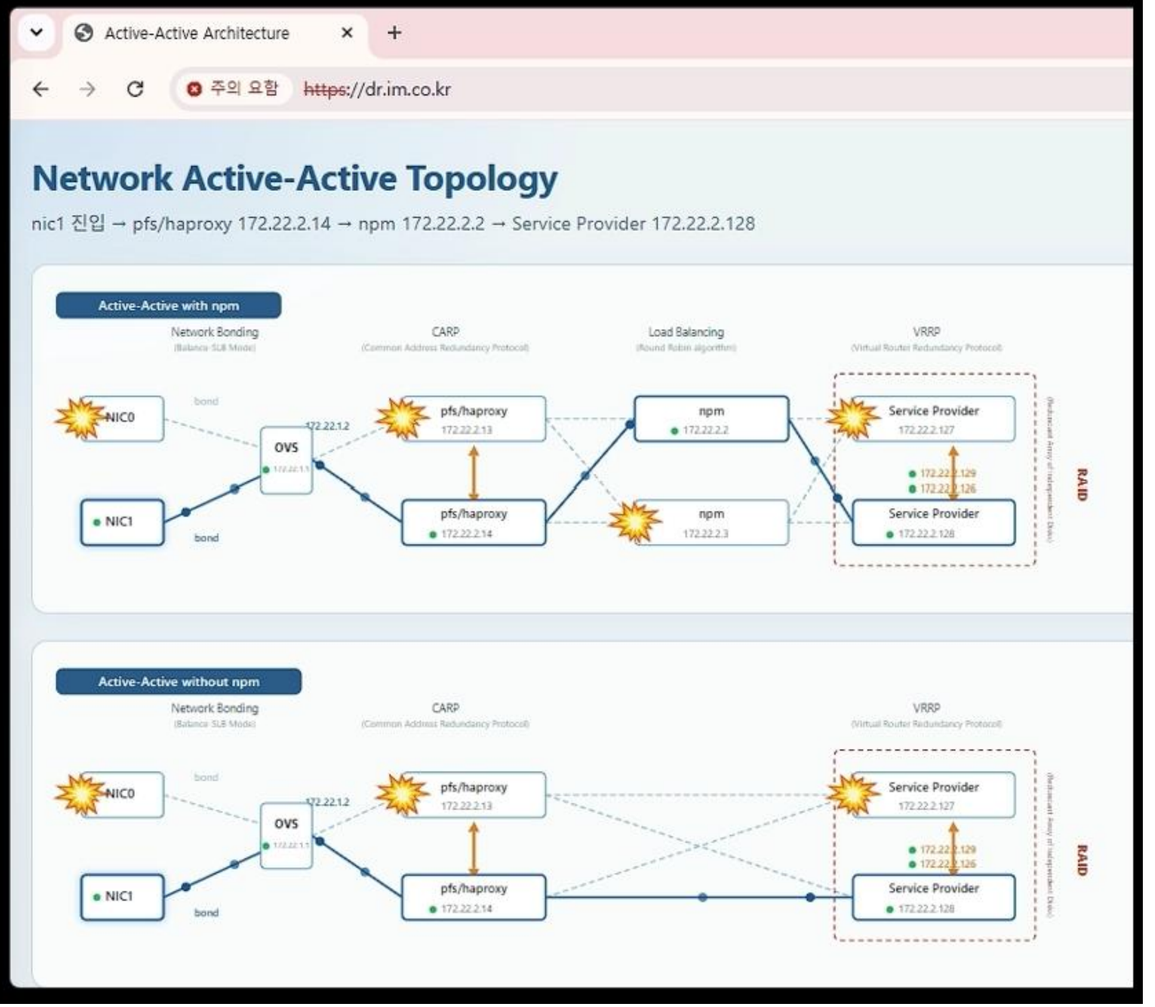
오픈소스 기반 사이버 복원력(Cyber Resilience) 레퍼런스 아키텍처

글로벌 규제 대응 및 비즈니스 연속성 확보를 위한
차세대 인프라 전환 가이드

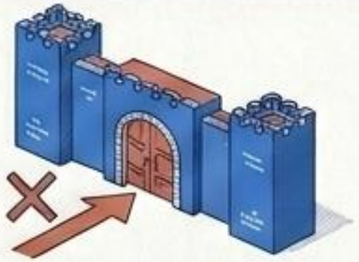
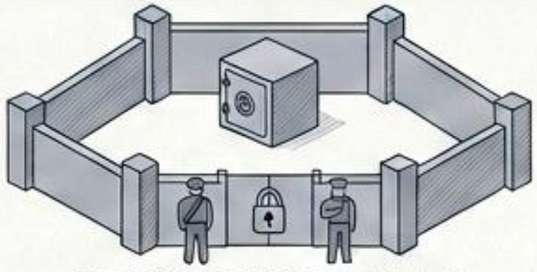
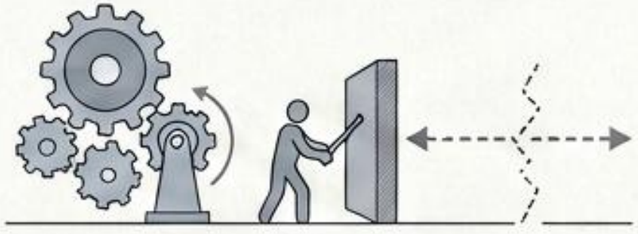


결론(미리보기)


pve - Proxmox Virtual
Gemini에게 물어보기
https://nxseoul.im.co.kr:8006/#...
PROX_TWEEK
NFC_EPAPER_WRITER
OPENCLOUD_KEYCLOA...
2026-IITP-AX - Go...
nxulsan - vpn - Pro...
모든 북마크
Virtual Environment 9.2.9
Search
Documentation
Create VM
Create CT
root@pam
Server View
124 (clawbot5-172.22.2.124-vlan1-local-lvm)
125 (syncthing-172.22.2.125-8384-vlan1-loca...
127 (alpine-3.24-172.22.2.127)
128 (alpine-3.24-172.22.2.128)
900 (pialert-192.168.0.152-local-lvm)
118 (openclaw-template-172.22.2.118-vlan1-l...
120 (clawbot2-template)
100 (pfSense-2.8.1-172.22.1.3)
106 (pfSense-2.8.1-172.22.1.4)
110 (kali-202602-172.22.2.110-vlan1-local-lvm)
113 (ubuntu-2404-helperscript-prism-insight-1...
114 (ubuntu-2404-helperscript-org-172.22.2.1...
115 (bee-box-172.22.2.115-vlan1-local-lvm)
116 (ubuntu-2404-desktop-172.22.2.116-vlan...
130 (Copy-of-VM-TOR-BACKDOOR-kali-202...
Container 127 (alpine-3.24-172.22.2.127) on node 'pve'
No Tags
Start
Shutdown
Summary
Console
Resources
Network
DNS
Options
Task History
Backup
Replication
Snapshots
ame:0
TX packets:3539277 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:557269127 (531.4 MiB) TX bytes:1020858695 (973.5 MiB)
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:65536 Metric:1
RX packets:3042610 errors:0 dropped:0 overruns:0 frame:0
TX packets:3042610 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:1028610549 (980.9 MiB) TX bytes:1028610549 (980.9 MiB)
alpine-3:~# ifdown eth0
alpine-3:~#
Tasks
Cluster log
Start Time
End Time
Node
User name
Description
Status
Sep 10 09:45:39 pve root@pam VM/CT 127 - Console
Sep 10 09:25:16 pve root@pam VM/CT 101 - Console
Sep 09 18:06:56 pve root@pam Shell
Sep 09 17:43:46 pve root@pam Shell
Sep 09 17:34:49 pve root@pam Shell


Active-Active Architecture
https://dr.im.co.kr
Network Active-Active Topology
nic1 진입 → pfs/haproxy 172.22.2.14 → npm 172.22.2.2 → Service Provider 172.22.2.128
Active-Active with npm
Network Bonding
CARP
Load Balancing
VRRP
NIC0
NIC1
bond
OVS
172.22.1.2
pfs/haproxy
172.22.2.13
pfs/haproxy
172.22.2.14
npm
172.22.2.2
npm
172.22.2.3
Service Provider
172.22.2.127
Service Provider
172.22.2.128
172.22.2.129
172.22.2.126
RAID
Active-Active without npm
Network Bonding
CARP
VRRP
NIC0
NIC1
bond
OVS
172.22.1.2
pfs/haproxy
172.22.2.13
pfs/haproxy
172.22.2.14
Service Provider
172.22.2.127
Service Provider
172.22.2.128
172.22.2.129
172.22.2.126
RAID

방어에서 복원으로: 패러다임의 전환

과거의 보안		현대의 사이버 복원력
 완벽한(?) 공격 차단 가능	[핵심 전제]	 공격은 피할 수 없음 (Assume Breach)
 방어벽 강화 및 접근 통제	[주요 목표]	 서비스의 신속한 회복과 비즈니스 연속성 보장
 경계 방어 중심의 수동 조치	[작동 방식]	 투명성과 협업 기반의 전 과정 자동화 (예측-견디기-복구-적응)

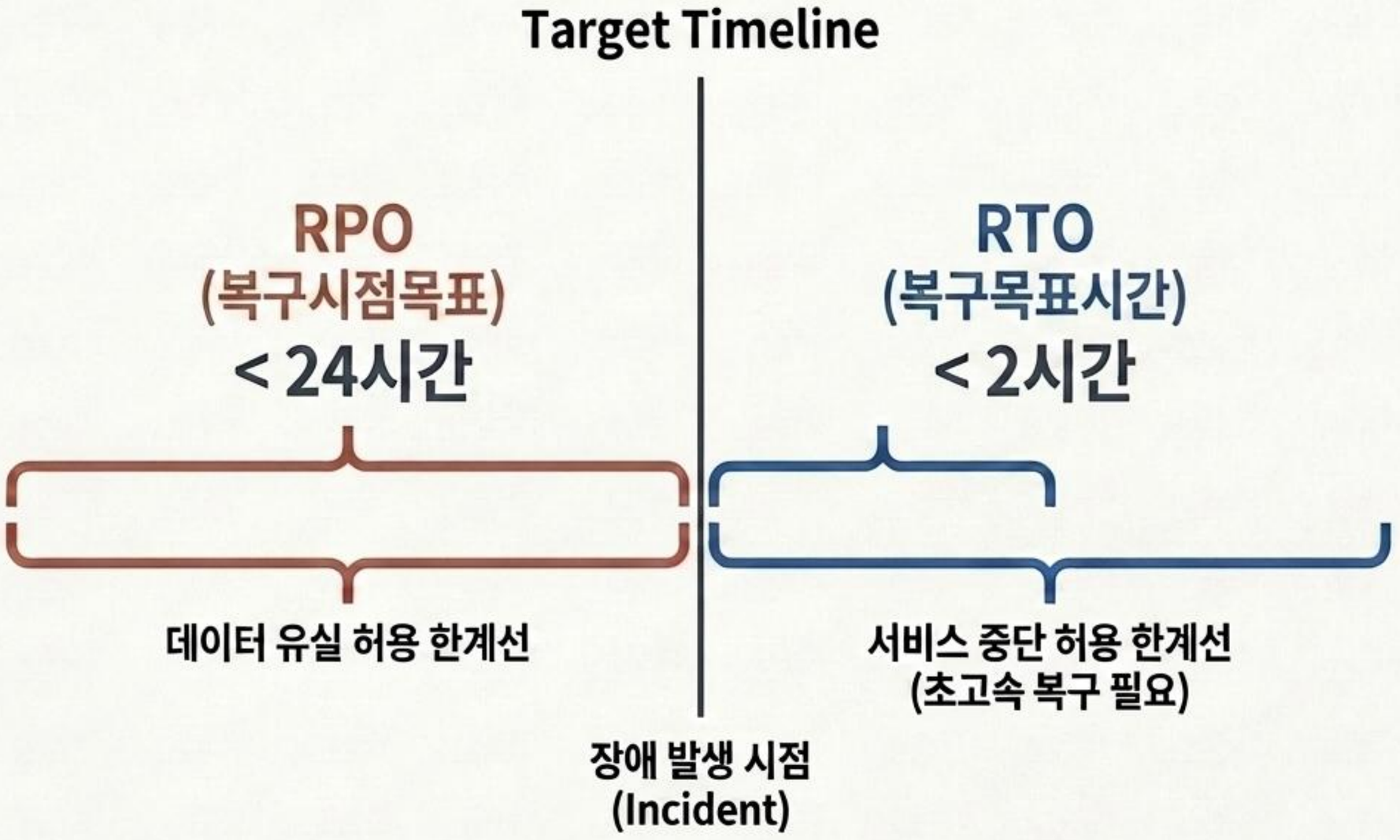
현대의 사이버 복원력은 단순한 '방패'가 아닌, 즉각적으로 인프라를 재건하는 '오뚝이' 메커니즘입니다.

제조업 사례 연구: 계획된 비즈니스 연속성 목표 달성

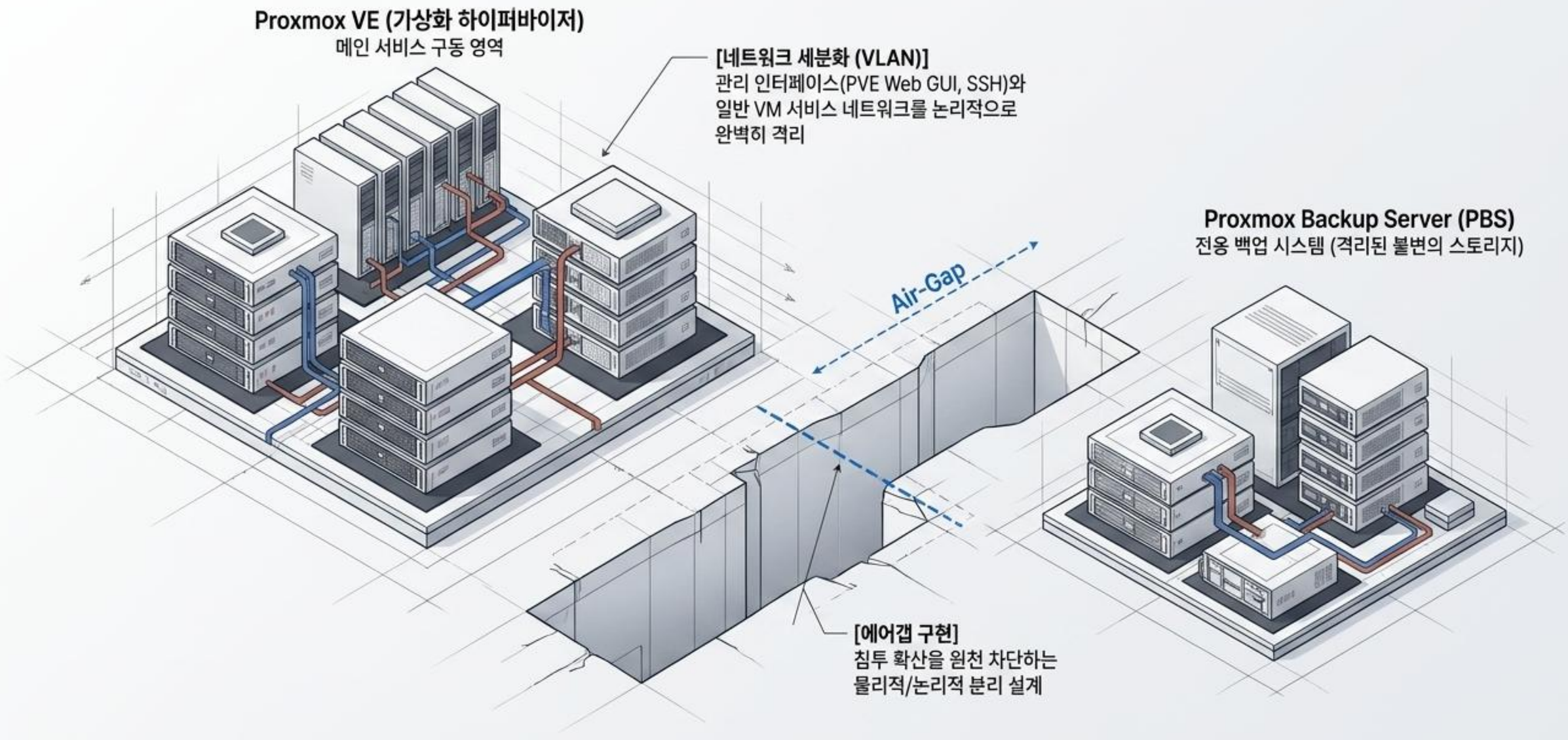
[대상 기관]
제조업 기반 중견기업

[기존 환경]
상용 인프라(VMware)
종속 상태

[핵심 과제]
서비스 크래시,
랜섬웨어 감염 등
시스템 타격시
계획된 복구 지표 충족

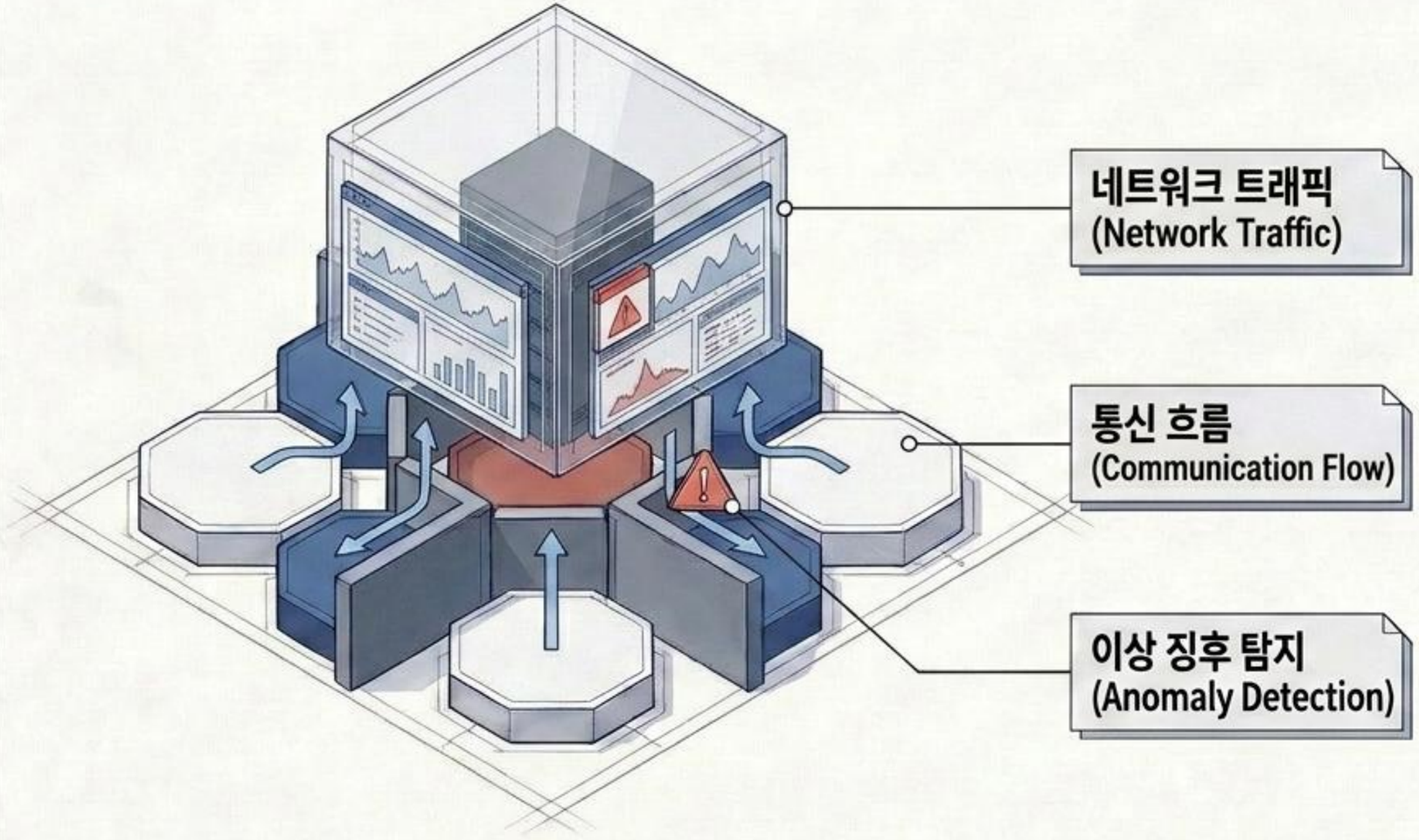


인프라 전환 청사진: Proxmox 기반의 에어갭(Air-Gap) 아키텍처



사이버 복원력 라이프사이클: 4단계 연속성 프레임워크

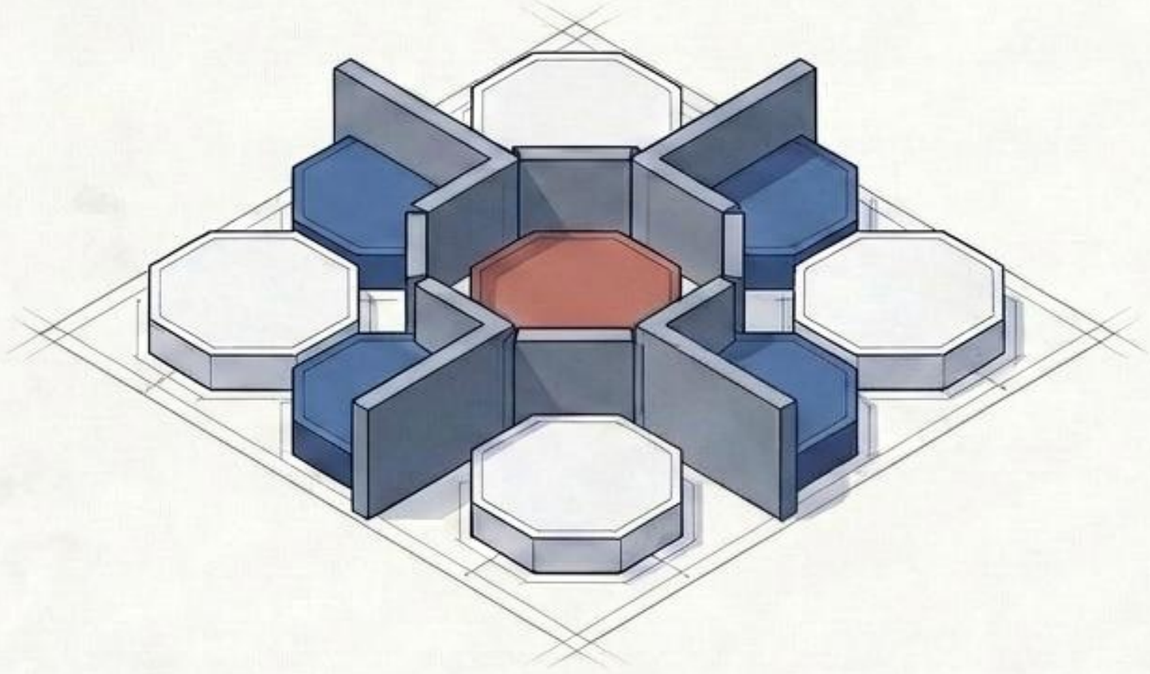
[1단계] 예측 : 실시간 위협 및 네트워크 모니터링



1. 세분화된 네트워크 트래픽 및 이상 징후 실시간 모니터링
2. VM 및 서비스 간 통신 흐름 가시성 확보
3. 잠재적 취약점 및 내부 이동 (Lateral Movement) 시도 감지

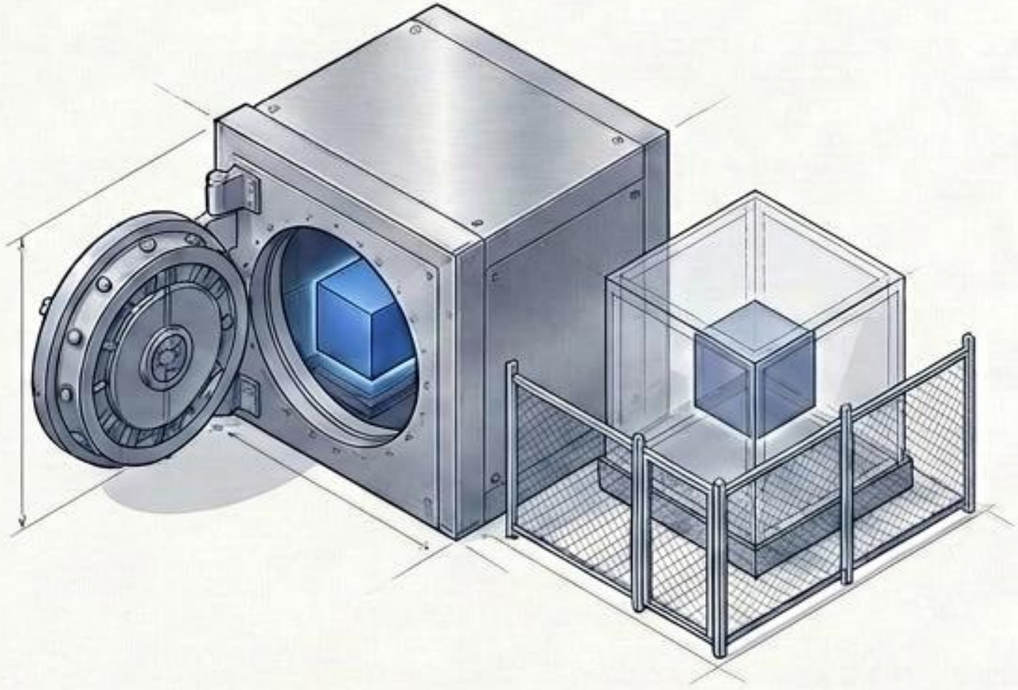
[2단계] 견디기: 마이크로 서비스 세분화 및 이중화와 불변의 백업

마이크로 서비스 세분화 및 이중화



네트워크를 초소형 단위(VLAN)로 격리하여 랜섬웨어의 내부 이동 (Lateral Movement)을 원천 차단하고 피해 범위를 최소화합니다.

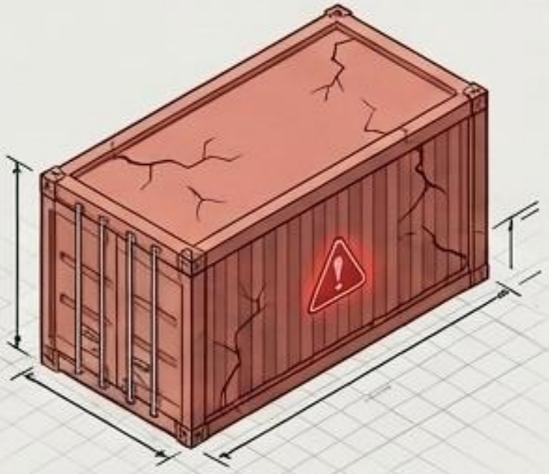
불변(Immutable) 백업 & 샌드박싱



공격 시에도 데이터 변조가 물리적으로 불가능한 오픈소스 스토리지 아키텍처. 의심스러운 환경은 샌드박스로 완벽히 격리합니다.

[3단계] 신속 복구: IaC를 통한 즉각적 재생성(Rehydration)

[1. 감염 탐지]



리눅스 하이퍼바이저 및
컨테이너 환경 내 침해 발생.

[2. 즉시 파기]

감염된 인프라를 수동으로
치료하지 않고 통째로 폐기.

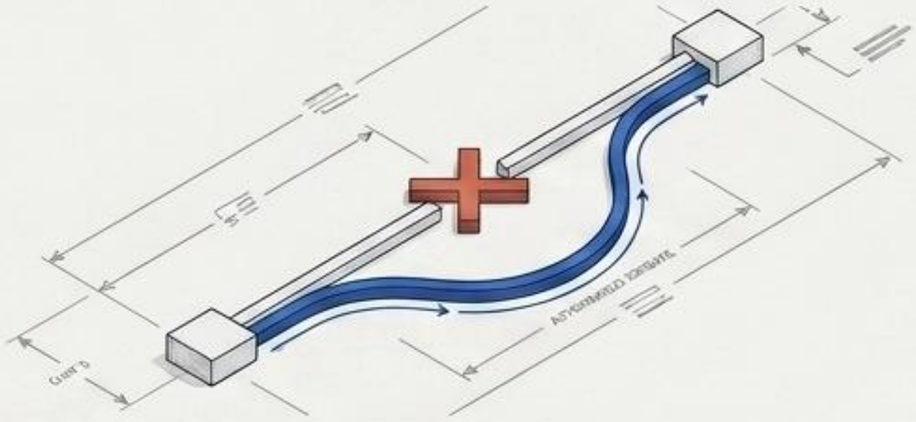
[3. 즉각 재생성]

IaC를 통해 감염 이전의 깨끗한 코드로
인프라를 수 분 내에 재생성(Rehydration)

치료(Cure)가 아닌 재생성(Rebuild)을 통해 RTO 2시간 목표를 완벽하게 달성합니다.

[4단계] 적응 & 진화: SDN 자동 복구와 지속적인 면역력 진화

소프트웨어 정의 네트워크(SDN) 자율 복구



네트워크 장애 및 공격 발생 시 즉각적인 트래픽 우회.
수동 조치 없이 실시간으로 가상화된 정상 네트워크
토폴로지를 자율적으로 재구축합니다.

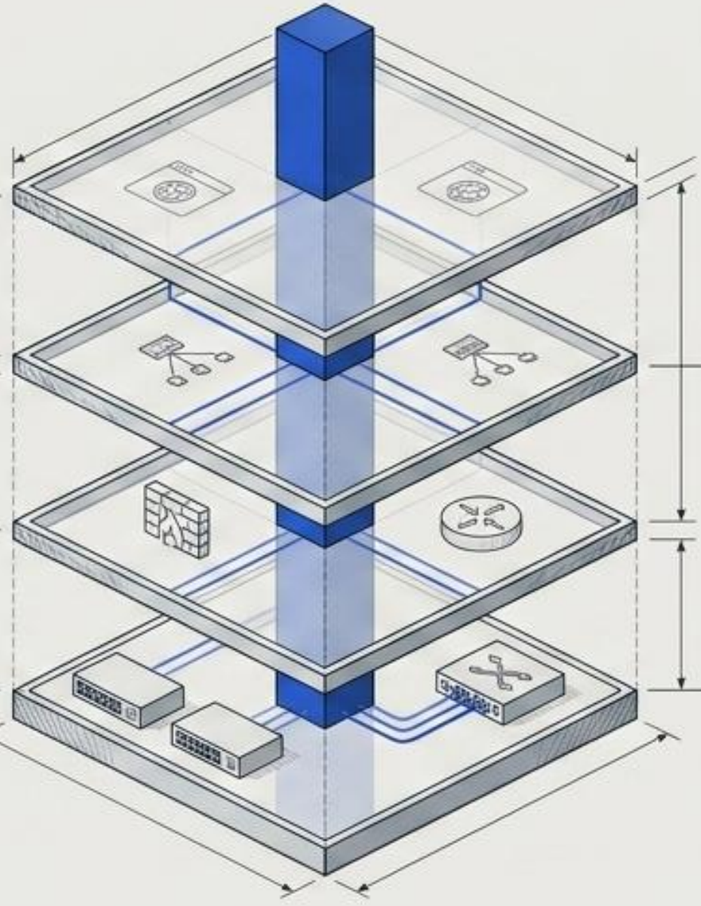
커뮤니티 위협 인텔리전스 (Threat Intelligence)

전 세계 개발자 집단 지성을 통한 제로데이 취약점 조기 발견.
수 시간 내에 패치를 제작 및 배포하여 전체 시스템의
면역력을 지속적으로 강화합니다.

다계층 복원력 스택: 단일 장애점(SPOF)을 제거한 생존성 검증

[L7 Web Layer]
Web Server VRRP
(keepalived) 무중단 전환

[L3 Network Layer]
pfSense CARP
방화벽 장애 조치

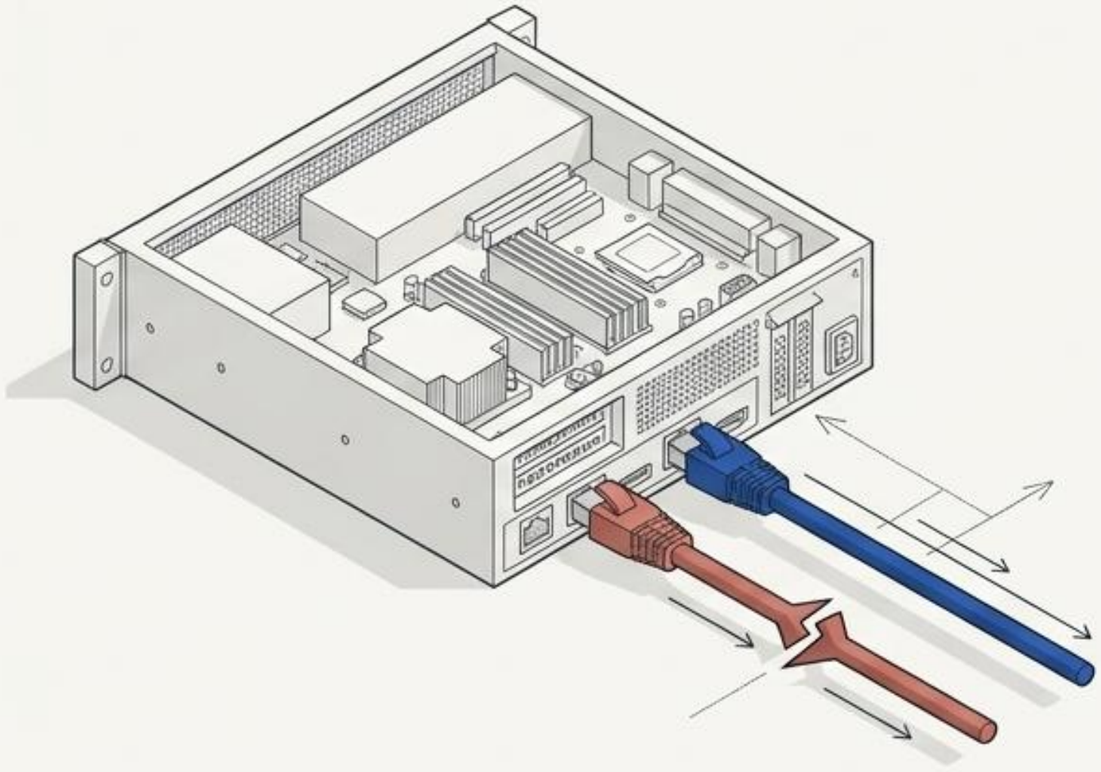


[L4 Transport Layer]
HAProxy
로드밸런싱 자동 우회

[L2 Data Link Layer]
Open vSwitch(OVS) Bond
물리 링크 자동 복구

개별 툴의 합이 아닌, 물리적 링크부터 웹 서비스까지 유기적으로 맞물려 돌아가는 무결점의 '도미노 방어선'을 구축했습니다.

[L2 계층 복원력 증명] Open vSwitch Bond 동작 테스트



물리적 링크 이중화 및 장애 시뮬레이션

[정상 상태] 이중화된 물리적 링크 상태 확인

```
# ip link show nic0
```

[장애 발생] 의도적인 물리 링크 단절 시뮬레이션

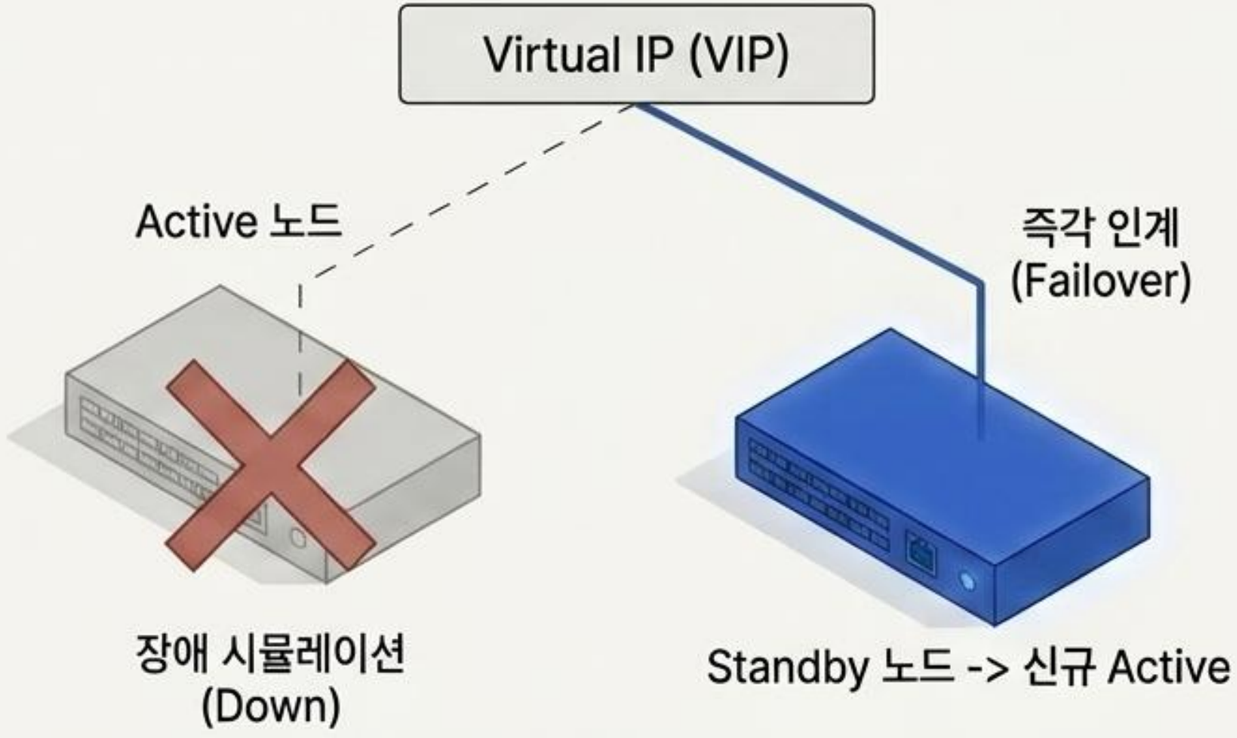
```
# ip link set dev nic0 down
```

[자동 복구] 즉각적인 백업 링크 활성화 및 트래픽 정상화

```
# ip link set dev nic0 up
```

물리적인 케이블 단절이나 NIC 장애가 발생해도 OVS Bond 설정을 통해 네트워크 L2 연결이 끊김 없이 유지됩니다.

[L3 계층 복원력 증명] pfSense CARP 방화벽 장애 조치



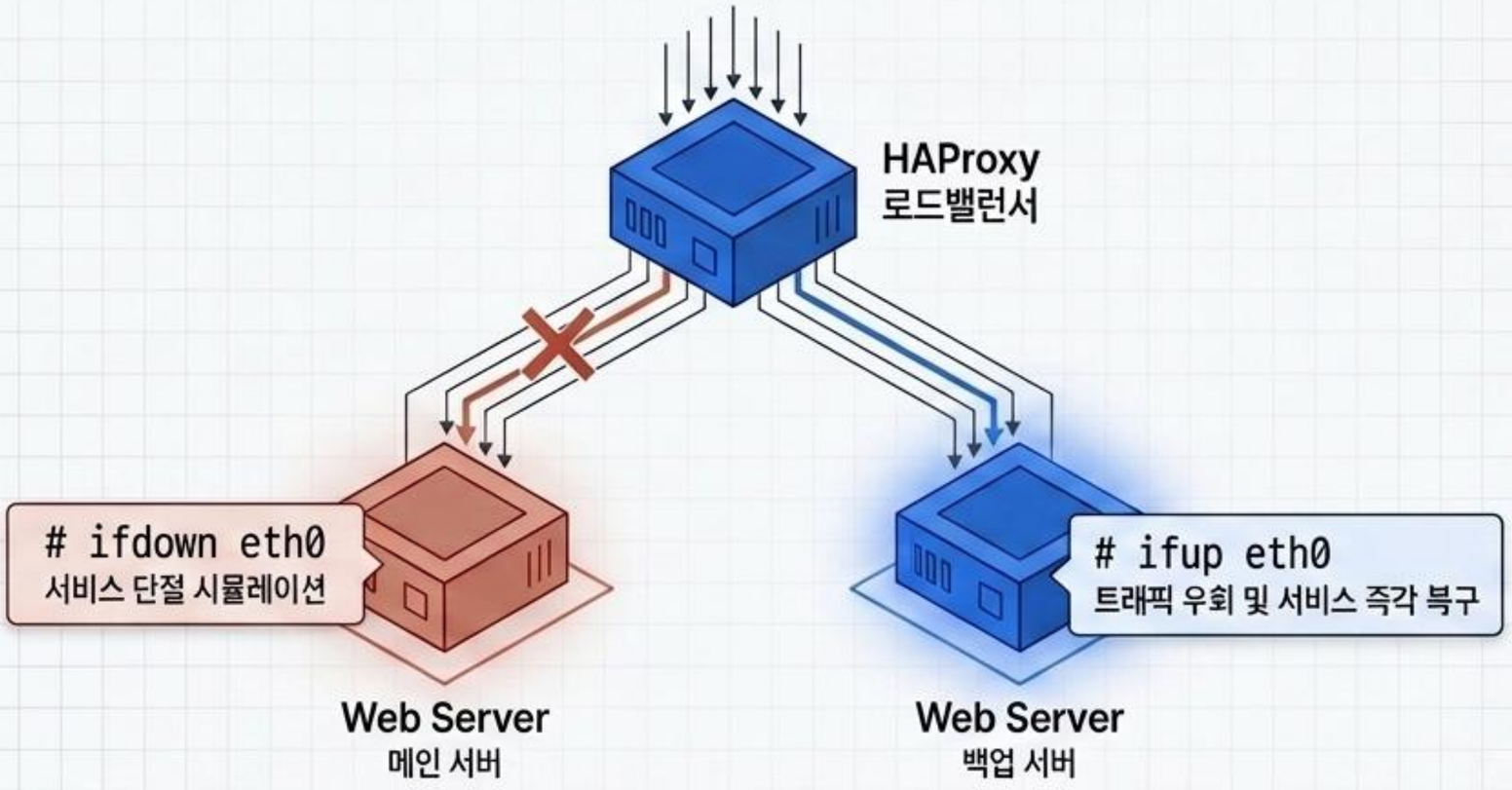
pfSense CARP (Common Address Redundancy Protocol) Setup

[장애 시뮬레이션]
Active 방화벽 노드 다운 시뮬레이션.

[장애 조치]
Standby 노드가 VIP를 즉시 인계받아 Active 상태로 자동 전환.

코어 라우터 및 방화벽 레벨(L3)의 치명적 장애 상황에서도 내부 네트워크와 외부 간의 통신 단절을 pfsense 이중화로 방지합니다.

[L4/L7 계층 복원력 증명]
HAProxy & Web Server VRRP 동작 테스트



L4/L7 로드밸런싱 및 VRRP 이중화

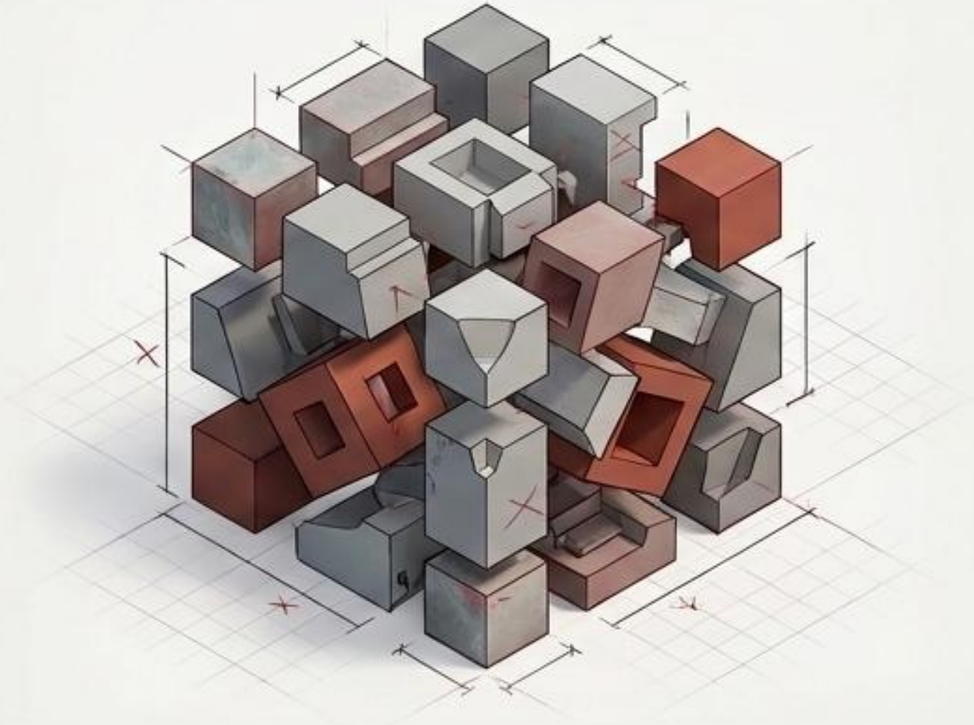
HAProxy & Web Server VRRP (keepalived) Setup

- **[상태 확인]**
  `# ip addr show eth0`
- **[서비스 단절]**
  메인 웹 서버 인터페이스 강제 다운
- **[서비스 복구]**
  트래픽 우회 및 무중단 전환

L4 로드밸런서와 L7 웹 서비스 구간의 이중화로, 사용자(Client)는 백엔드의 장애를 전혀 인지하지 못합니다.

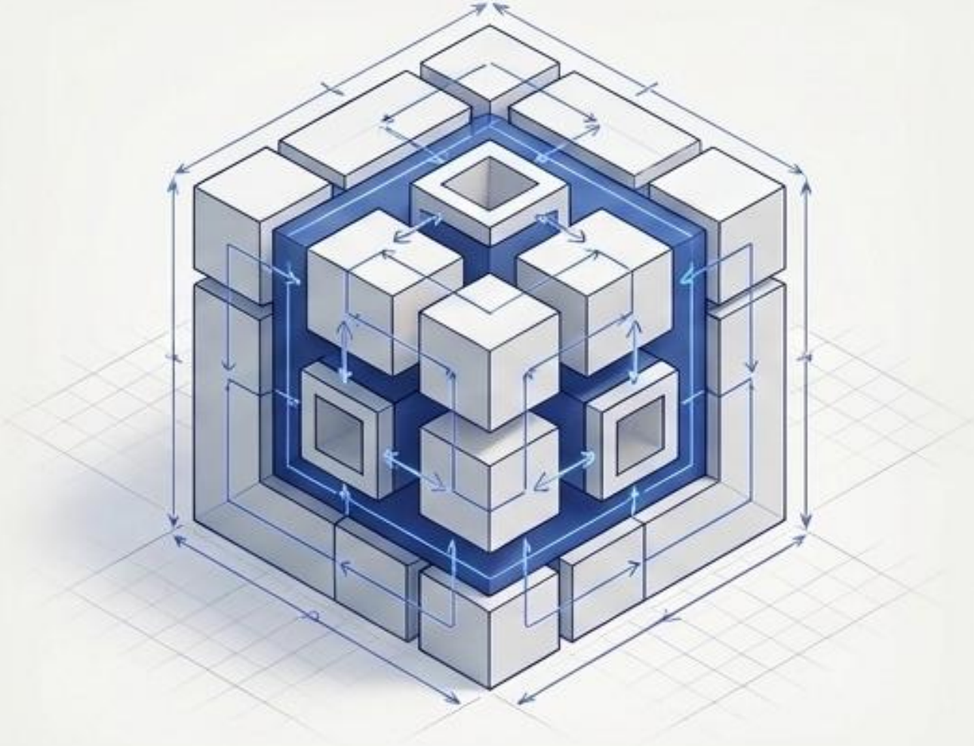
전략적 제언: 도구 중심(Tools)에서 아키텍처 중심(Architecture)으로

도구 중심 (Tool-centric)



- 파편화된 다수의 보안 솔루션 단편적 도입
- 외부 코드를 그대로 가져와 사후에 검사 진행
- **결과**: 관리 복잡성 증가 및 보안 사각지대 필연적 발생

아키텍처 중심 (Architecture-centric)



- **생태계 전반의 통합된 의존성 및 아키텍처 제어**
- ActiveState 등 검증된 소스 코드만 내부 저장소에 사전 빌드
- **결과: 예측 가능하고 투명한 'Secure by Design' 달성**

데모 환경

https://dr.im.co.kr/

데모 환경에 접속하여 직접 체험해보세요.