`ARCHITECTURE DESIGN SPECIFICATION (SAD) · ISO/IEC/IEEE 42010 & 4+1 VIEW STANDARD`

[아키텍처 설계 명세서] 엔터프라이즈 하이브리드 클라우드 네트워크 아키텍처 설계서 (SAD)

문서 관리 항목	명세 내용	문서 관리 항목	명세 내용
문서 번호 (Doc ID)	`SAD-NET-2026-001`	**버전 (Version)**	`v1.0.0`
대상 시스템 / 범위	전사 하이브리드 클라우드 및 K8s 네트워크 표준	**문서 상태 (Status)**	`APPROVED (표준 규격 확정)`
설계 책임 (Architect)	클라우드 네트워크 & 보안 아키텍처 TF	**준거 표준 (Standard)**	`ISO/IEC/IEEE 42010 · 4+1 View · NIST SP 800-207`
런타임 기준 스택	`Transit Gateway + Cilium eBPF + Istio Mesh`	**보안 등급**	`대외비 (Internal Engineering Standard)`

문서 제·개정 이력 (Revision History)

버전	일자	변경 구분	작성 / 승인자	주요 설계 제·개정 내역
`v0.5.0`	2026-10-12	초안 작성	네트워크 아키텍처 파트	Hub-and-Spoke 토폴로지, 4-Zone 망분리 및 전사 IPAM 슈퍼넷(CIDR) 대역 초안 정의
`v0.9.0`	2026-10-20	검토 반영	클라우드 보안 & SRE 파트	Cilium eBPF 커널 데이터플레인, Istio Ambient mTLS, 듀얼 Direct Connect BFD 절체 규격 반영
`v1.0.0`	2026-10-26	표준 승인	아키텍처 심의 위원회	4대 아키텍처 뷰(논리·프로세스·데이터·배포) 및 OPA/Conftest 정책 검증 규칙 최종 확정

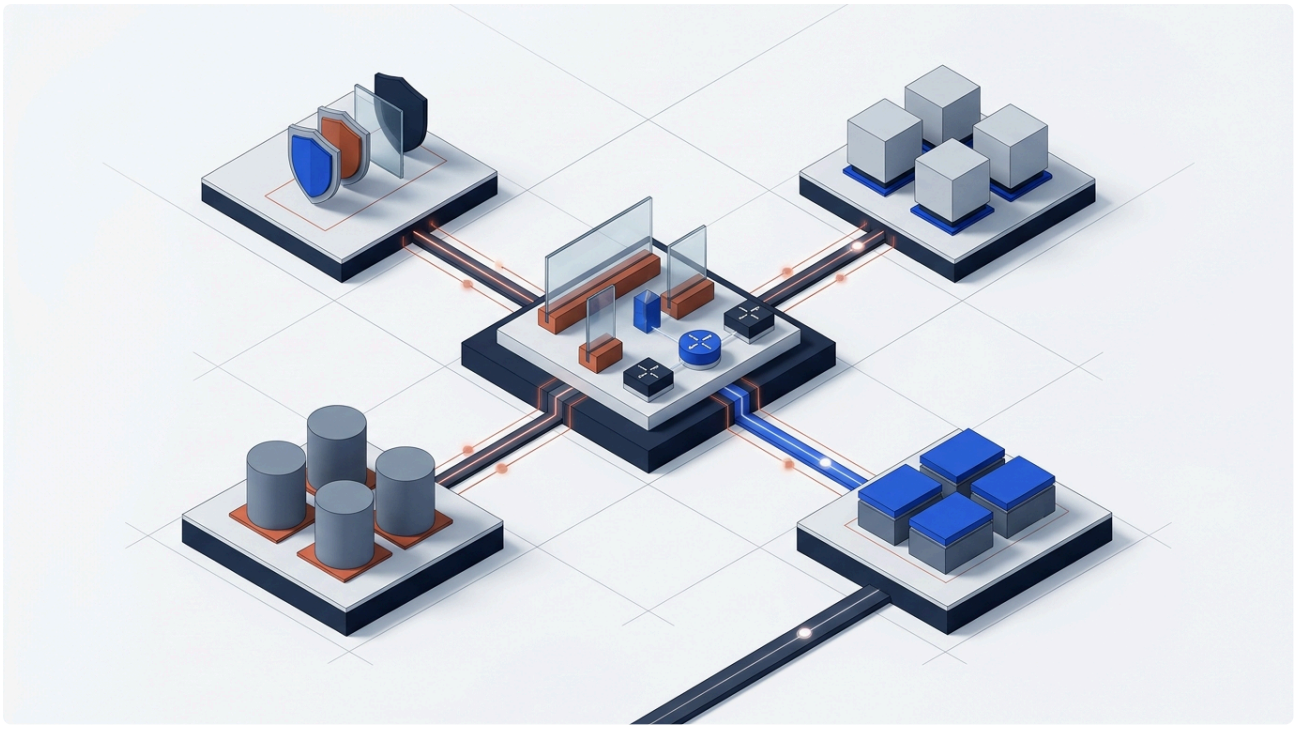
제1장. 설계 개요 및 아키텍처 원칙 (1. Architecture Overview & Principles)

> **[설계 핵심 정의 (Architecture Blueprint Summary)]**: 본 설계서는 전사 하이브리드 멀티클라우드 및 쿠버네티스(Kubernetes) 런타임의 연결성, 초저지연 패킷 처리, 무결점 보안 격리를 달성하기 위해 **중앙 집중형 Hub-and-Spoke 트랜짓 토폴로지(Centralized Transit Hub)**와 **NIST SP 800-207 기반 Zero-Trust 마이크로세그먼테이션(eBPF + mTLS)**을 결합한 표준 네트워크 참조 아키텍처(Reference Architecture)를 명세함.

1.1 시스템 컨텍스트 및 Hub-and-Spoke 망분리 개념 (System Context View)

- **시스템 경계 및 내·외부 트래픽 격리 구조**:
  - 전사 네트워크는 중심부의 **중앙 트랜짓 및 보안 허브(Central Transit & Inspection Hub)**를 단일 라우팅 코어로 두며, 외부 접점(`Public Edge/DMZ Spoke`), 비즈니스 워크로드(`Prod/Non-Prod Workload Spoke`), 핵심 데이터 금고

(`Isolated Data Vault`), 온프레미스 데이터센터(`On-Premises IDC`)가 허브를 통해서만 상호 통신하도록 물리적·논리적으로 분리됨.



하이브리드 멀티클라우드 Hub-and-Spoke 네트워크 토폴로지 및 4-Zone 보안 경계 격리 개념도

1.2 아키텍처 핵심 설계 원칙 명세 (Architecture Principles Specification)

원칙 ID	아키텍처 설계 원칙명	상세 설계 규격 및 강제 사항 (Design Rule Specification)	검증 방법 (Fitness Check)
`AP-01`	**Spoke 간 직접 연결 금지 및 중앙 허브 경유 (Centralized Transit)**	• 모든 VPC/VNet Spoke 간 직접 피어링(Direct VPC Peering) 생성을 전면 금지함 • 이기종 망(Prod ↔ Shared, Cloud ↔ On-Prem) 간 트래픽은 반드시 `Transit Gateway` 및 `Inspection Firewall`을 경유하여 DPI(Deep Packet Inspection) 검사를 통과함	OPA `NET-RULE-01` / AWS Config
`AP-02`	**Zero-Trust 마이크로세그먼테이션 (Default Deny & mTLS)**	• 네트워크 위치(IP 대역)만으로 신뢰를 부여하지 않으며 기본 정책은 **100% Default Deny**로 설정함 • 모든 동서(East-West) 서비스 간 통신은 `SPIFFE ID` 기반 상호 인증(`mTLS 1.3`) 및 L7 인가 정책 통과를 강제함	CiliumNetworkPolicy / Istio RBAC
`AP-03`	**비중첩 IPAM 할당 및 환경 간 VRF 물리 격리 (Strict VRF Isolation)**	• 전사 클라우드 및 온프레미스 전 구간에 걸쳐 **RFC 1918 / RFC 6598 비중첩 CIDR**을 중앙 할당함 • 운영계(`Prod VRF`)와 개발/검증계(`Non-Prod VRF`) 라우팅 테이블을 분리하여 상호 패킷 라우팅을 원천 차단함	IPAM CI 검증 / TGW Route Table
`AP-04`	**단일 장애점(SPOF) 제거 및 대칭형 다중화 (Multi-AZ Symmetry)**	• 모든 네트워크 경로(NAT GW, NLB, TGW ENI, Firewall Endpoint)는 **최소 3개 가용영역(3 AZs) Active-Active 대칭 구조**로 배치함 • 온프레미스 전용선은 서로 다른 물리 국사(POP)를 통한 듀얼 `Direct Connect` + `IPSec VPN` 삼중화를 강제함	Chaos Zonal Shift / BFD Failover Test
`AP-05`	**커널 레벨 패킷 가속 및 전 구간 플로우 가시성 (eBPF & Telemetry)**	• 레거시 `iptables` 선형 규칙 탐색을 배제하고 **Cilium eBPF 소켓 레벨 로드밸런싱(`O(1)`)**을 표준 채택함 • 모든 L3/L4/L7 패킷 흐름과 DNS/TCP 핸드셰이크 지연을 `VPC Flow Logs` 및 `Hubble`로 실시간 수집함	Hubble Relay / Grafana Mimir

1.3 비기능 품질 속성 및 목표 SLA/SLO 명세 (Quality Attribute Specification)

요구사항 ID	품질 속성 분류	정량 목표 지표 (Target SLA / SLO)	아키텍처 실현 메커니즘 (Architectural Tactics)
`NFR-01`	**전달 지연 (Network Latency)**	• 동일 AZ 내 동서(E-W) Pod 간 통신: **P99 ≤ 0.5ms** • 교차 AZ 통신: **P99 ≤ 2.0ms** / 하이브리드(Cloud-IDC): **P99 ≤ 8.0ms**	• Cilium eBPF `SocketLB` 및 `XDP` 패킷 가속으로 커널 네트워크 스택 오버헤드 최소화 • Istio Ambient Mesh(`ztunnel`) 및 AZ-local 토폴로지 인지 라우팅(`Topology Aware Hints`) 적용
`NFR-02`	**대역폭 및 처리량 (Throughput)**	• 클러스터 인그레스 대역폭 **≥ 100 Gbps**, 패킷 처리율 **≥ 1,500만 PPS** • 하이브리드 전용선 집계 대역폭 **20 Gbps (Active-Active ECMP)**	• AWS ENA(Elastic Network Adapter) 점보 프레임(`MTU 9001`) 및 멀티큐 NIC 바인딩 • Transit Gateway ECMP(Equal-Cost Multi-Path) 해싱 기반 대역폭 수평 확장
`NFR-03`	**망 가용성 (Availability)**	• 코어 네트워크 인프라 연간 가용성 **≥ 99.99%** (연간 중단 ≤ 52.6분) • 단일 AZ 또는 단일 전용선 단절 시 패킷 손실 **0.01% 이하**	• 3개 AZ 독립 NAT/NLB/TGW 구성 및 Route53 Application Recovery Controller(Zonal Shift) • BGP + **BFD(300ms 간격 × 3회 = 900ms 감지)** 기반 3초 이내 무중단 자동 경로 절체
`NFR-04`	**보안 규정 준수 (Zero-Trust Security)**	• 외부 공격 표면(Public IP 노출 워크로드/DB) **0건** • 동서(East-West) 평문 트래픽 비율 **0.00% (100% 암호화)**	• DB/Cache 서브넷 `0.0.0.0/0` 라우팅 완전 제거 및 `AWS PrivateLink` 전용 사설 통신 • 전 파드 간 `TLS 1.3 (AES-256-GCM)` 및 전용선 `IEEE 802.1AE MACsec` L2 암호화
`NFR-05`	**관측성 및 탐지 속도 (Observability)**	• 이상 트래픽(Port Scan, DDoS, 비인가 Egress) 탐지 **≤ 10초** • 패킷 드롭(`TCP Retransmit` , `DNS NXDOMAIN`) 원인 추적 **≤ 1분**	• eBPF 기반 `Hubble` L3/L4/L7 플로우 수집 + `Suricata IDS/IPS` 실시간 시그니처 차단 • 전 구간 `PingMesh` 능동 합성 프로브(1초 주기)를 통한 AZ 간 패킷 손실 매트릭스 감시

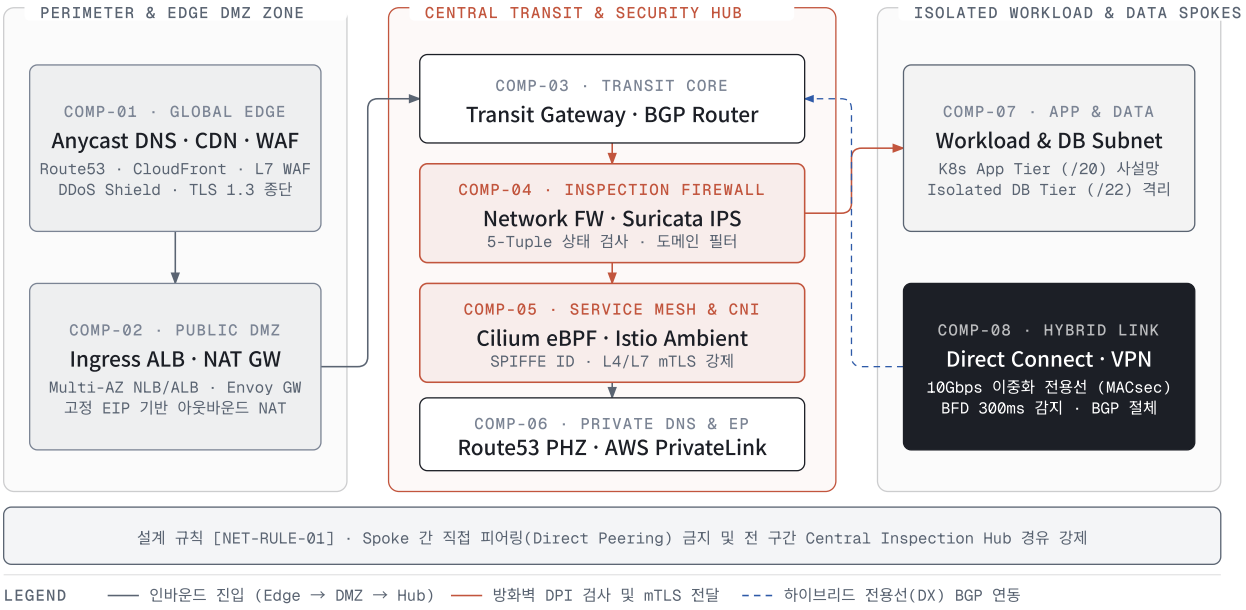
제2장. 논리 아키텍처 및 컴포넌트 설계 (2. Logical & Component View)

2.1 논리 계층 및 Hub-and-Spoke 4-Zone 세그먼테이션 구조도

- **구조 명세**: 전사 네트워크는 보안 신뢰 수준과 트래픽 방향성에 따라 **`Perimeter & Edge DMZ Zone`** → **`Central Transit & Security Hub`** → **`Isolated Workload & Data Spokes`** 의 3대 논리 영역·8개 핵심 네트워크 컴포넌트(`COMP-01` ~ `COMP-08`)로 구성됨.

VIEW 01 · LOGICAL & COMPONENT ARCHITECTURE (HUB-AND-SPOKE & 4-ZONE SEGMENTATION)

[논리 뷰] Hub-and-Spoke 계층형 네트워크 세그먼테이션 및 컴포넌트 구조도



View 1 논리 뷰 — Hub-and-Spoke 계층형 네트워크 세그먼테이션 및 4-Zone 보안 경계 구조도

2.2 컴포넌트 카탈로그 및 책임 명세표 (Component Specification Catalog)

컴포넌트 ID	컴포넌트명	소속 네트워크 계층	핵심 설계 책임 (Core Responsibilities)	라우팅 / 보안 인터페이스 및 의존성 제약
`COMP-01`	**Global Edge & CDN/WAF**	`Perimeter Edge (L3/L4/L7)`	• Anycast BGP 기반 글로벌 최적 엣지 라우팅 및 정적 자산 캐싱 • L3/L4 DDoS 방어 (SYN Flood, UDP Amplification) 및 OWASP Top 10 L7 WAF 필터링	• 인입: 외부 공인 인터넷 (`HTTPS 443` , `QUIC/HTTP3`) • 제약: Origin(DMZ ALB)은 오직 Edge Prefix 전용 커스텀 헤더만 허용
`COMP-02`	**Public DMZ Ingress & NAT**	`Public DMZ Subnet`	• Multi-AZ NLB/ALB를 통한 외부 인입 TLS 1.3 종단 및 Ingress Gateway 전달 • 사설 워크로드의 외부 파트너 연동 시 고정 공인 IP(EIP) 기반 SNAT 수행	• 배치: 각 AZ별 `/24` Public Subnet 독립 배치 • 제약: DMZ 서브넷 내 비즈니스 애플리케이션 파 데이터 저장소 배치 엄격 금지
`COMP-03`	**Central Transit Core (TGW)**	`Central Network Hub (L3)`	• 클라우드 내 다수 VPC/VNet Spoke와 온프레미스 전용선을 연결하는 중앙 L3 라우팅 허브 • 환경별 **VRF 라우팅 테이블(Prod / Non-Prod / Shared / Inspection)** 분리 운영	• 프로토콜: `eBGP (ASN 64512)` 동적 라우팅 + ECMP 대역폭 분산 • 제약: Spoke 간 트래픽은 반드시 `COMP-04` 방 Attachment로 먼저 스티어링함
`COMP-04`	**Inspection Firewall & IDS/IPS**	`Central Security Hub (L3~L7)`	• VPC 간 동서(East-West) 교차 트래픽 및 외부 아웃바운드(Egress) 트래픽 전수 검사 • Suricata 기반 시그니처 IPS, 5-Tuple 상태 검사 및 아웃바운드 FQDN 화이트리스트 통제	• 배포: Gateway Load Balancer(GWLB) + GENEVE 캡슐화(`UDP 6081`) 투명 프록시 • 정책: 비인가 외부 도메인 및 C&C 서버 통신 즉시 Drop 및 SIEM 경보 발보
`COMP-05`	**eBPF CNI & Service Mesh**	`Workload Overlay / Kernel`	• 쿠버네티스 파드 IP 할당 (ENI Prefix Delegation) 및 커널 레벨 `eBPF` 패킷 스위칭 • `Istio Ambient (ztunnel + waypoint)` 기반 무사이드카 L4/L7 상호 인증 (`mTLS`) 및 트래픽 제어	• 신원: `SPIFFE ID (spiffe://cluster.local/ns/{ns}/sa/{` X.509 인증서 24시간 주기 자동 순환 • 성능: `iptables` 체인 완전 제거 및 `kube-pr` 대체 운영

컴포넌트 ID	컴포넌트명	소속 네트워크 계층	핵심 설계 책임 (Core Responsibilities)	라우팅 / 보안 인터페이스 및 의존성 제약
`COMP-06`	**Private DNS & PrivateLink**	`Shared Network Services`	• `Route53 Resolver` 기반 하이브리드 양방향 Split-Horizon 사설 DNS 질의응답 • `AWS PrivateLink (Interface/Gateway Endpoint)` 를 통한 인터넷 미경유 사설 서비스 연동	• 연동: S3, DynamoDB, ECR, KMS 및 내부 공유 MSA API 엔드포인트 직결 • 효과: NAT Gateway 경유 트래픽 비용 절감 및 헤어핀(Hairpin) 원천 차단
`COMP-07`	**Workload & Data Spoke**	`Private App / Isolated DB Tier`	• 비즈니스 파드가 실행되는 `Private App Subnet` 과 완전 폐쇄형 `Isolated Data Subnet` 분리 • 데이터 계층은 Security Group ID 참조 방식으로만 허용된 App 파드의 포트 접근만 개방	• 격리: Data Subnet 라우팅 테이블에는 `IGW` 및 `GW` 경로(`0.0.0.0/0`) 존재 금지 • 암호화: VPC 내부 전송 구간 TLS 1.3 강제
`COMP-08`	**Hybrid Interconnect (DX/VPN)**	`Hybrid Edge (L1/L2/L3)`	• 온프레미스 코어 라우터와 클라우드 Transit Gateway 간 전용 물리 회선 연결 • 주 회선 2개(`10Gbps Direct Connect × 2`) Active-Active 운영 및 `IPSec VPN` 백업 구성	• 가용성: 서로 다른 물리 DX Location 수용 및 `I` `802.1AE MACsec` 암호화 • 절체: `BFD(300ms × 3)` 활성화로 회선 장애 내 감지 및 BGP 우회

2.3 표준 네트워크 IaC(Infrastructure as Code) 디렉토리 구조 명세

```text
infra-network-platform/
├── modules/
│   ├── transit-hub/              # [COMP-03, COMP-04] TGW, VRF Route Tables, Network Firewa
│   ├── spoke-vpc/                # [COMP-02, COMP-07] 4-Tier Subnets (DMZ, App, Data, TGW-A
│   ├── hybrid-dx/                # [COMP-08] Direct Connect Gateway, Transit VIF, BGP + BFD
│   ├── privatelink-dns/          # [COMP-06] Route53 PHZ, Inbound/Outbound Resolver, VPC En
│   └── k8s-cilium-mesh/          # [COMP-05] Cilium Helm Values (eBPF, ENI), Istio Ambient,
├── environments/
│   ├── prod/                     # 운영계 (10.10.0.0/16, Pod Secondary 100.64.0.0/16)
│   ├── staging/                  # 검증계 (10.20.0.0/16, Pod Secondary 100.65.0.0/16)
│   └── shared-security/          # 중앙 보안/관측성 허브 (10.100.0.0/16)
└── policies/
    ├── opa-terraform/            # [NET-RULE-01~05] Terraform Plan 정적 보안/라우팅 검증 (Rego)
    └── cilium-policies/          # K8s 네임스페이스별 Default-Deny 및 L7 Zero-Trust 정책 YAML
```

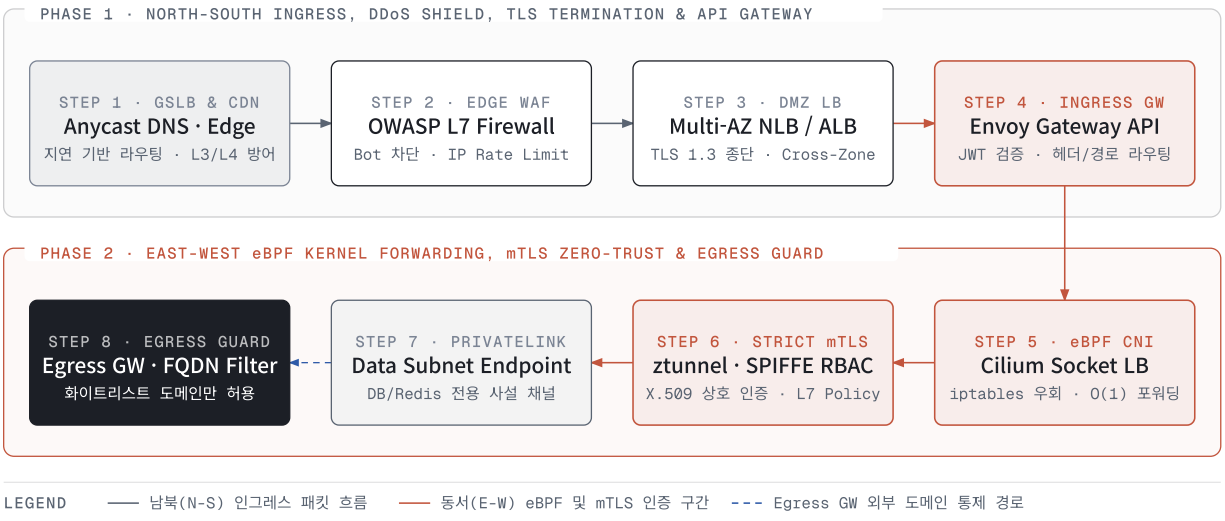
제3장. 프로세스 및 런타임 파이프라인 설계 (3. Process & Runtime Sequence View)

3.1 남북(North-South) 인그레스 및 동서(East-West) 패킷 처리 8단계 파이프라인

- **동적 패킷 라우팅 흐름**: 외부 클라이언트 요청은 `STEP 1(GSLB/CDN)` 부터 `STEP 4(Ingress Gateway)` 까지의 **남북(North-South) 경계 보안 체인**을 통과한 뒤, 클러스터 내부에서 `STEP 5(Cilium eBPF)` 와 `STEP 6(Zero-Trust mTLS)` 를 거쳐 백엔드 파드 및 사설 데이터 계층(`STEP 7~8`)으로 전달됨.

VIEW 02 · PROCESS & PACKET ROUTING PIPELINE VIEW (8-STAGE SEQUENCE)

[프로세스 뷰] 남북(N-S) 인그레스 및 동서(E-W) 서비스 메시 패킷 처리 파이프라인



View 2 프로세스 뷰 — 남북(N-S) 인그레스 및 동서(E-W) 서비스 메시 8단계 패킷 처리 파이프라인

3.2 단계별 패킷 처리 및 타임아웃/보안 계약 명세표 (Packet Pipeline Specification)

단계 ID	단계명 (Stage)	처리 컴포넌트	입력 패킷 / 프로토콜 계약	런타임 패킷 처리 규칙 및 타임아웃/보안 규격	출력 및 차단/예외 계약 (Output / Drop)
`STEP 1`	**GSLB & Anycast Edge**	Route53 + CloudFront CDN	Client `HTTPS (TCP 443 / QUIC)`	• Latency-based 라우팅 및 Anycast BGP로 최단 거리 엣지 POP 연결 • L3/L4 SYN Flood 방어 및 정적 콘텐츠 엣지 캐시 즉시 응답	정상 동적 요청 시 `STEP 2` 전달 / 리전 전체 장애 시 DR 리전 자동 Failover
`STEP 2`	**Edge L7 WAF Shield**	AWS WAF / Cloudflare WAF	Decrypted HTTP/2·HTTP/3 Request	• OWASP Core Rule Set(SQLi, XSS), Bot Control, Geo-IP 필터링 수행 • 클라이언트 IP당 Rate Limit(초당 300 req) 초과 여부 실시간 검사	통과 시 서명 헤더 주입 후 `STEP 3` / 위반 시 **엣지에서 즉시 `HTTP 403/429` 차단**
`STEP 3`	**DMZ Load Balancing**	Multi-AZ NLB / ALB (`COMP-02`)	Edge IP Prefix `TLS 1.3` 트래픽	• TLS 1.3(`TLS_AES_256_GCM_SHA384`) 종단 및 `X-Forwarded-For` 보존 • `Idle Timeout: 60s` , Cross-Zone 로드밸런싱 및 타겟 헬스체크(5초 주기)	비정상 가용영역(AZ) 타겟 즉시 제외 후 정상 K8s Ingress 노드로 `STEP 4` 전달
`STEP 4`	**K8s Gateway API**	Envoy Gateway (`COMP-05`)	HTTP Request + `traceparent`	• `HTTPRoute` 기반 헤더/경로 라우팅, 카나리 가중치 분할(예: 95:5) • OAuth2/OIDC JWT 서명 검증 및 W3C `traceparent` 분산 추적 헤더 강제 생성	검증 성공 시 클러스터 내부 서비스 VIP로 라우팅(`STEP 5`) / 미인증 시 `HTTP 401`
`STEP 5`	**eBPF Kernel Dataplane**	Cilium eBPF CNI (`COMP-05`)	Pod-to-Pod / Service VIP Packet	• `kube-proxy (iptables)` 를 우회하고 **eBPF 해시 테이블(`O(1)`)**로 목적지 Pod IP 직결 변환 • 동일 노드 내 통신 시 `sockops` 소켓 리다이렉트로 TCP/IP 스택 단축	커널 레이어에서 **0.1ms 이하** 포워딩 수행 / L3/L4 정책 위반 패킷은 `XDP_DROP`
`STEP 6`	**Zero-Trust mTLS Mesh**	Istio `ztunnel` + `Waypoint`	HBONE (`HTTP CONNECT over mTLS:15008`)	• 송수신 파드 간 `SPIFFE X.509` 인증서 상호 검증 및 TLS 1.3 터널링 • `AuthorizationPolicy` 로 호출 허용된 원본 서비스 계정	인가 통과 시 타겟 컨테이너 포트 전달 / 비인가 호출 시 `RBAC:`

단계 ID	단계명 (Stage)	처리 컴포넌트	입력 패킷 / 프로토콜 계약	런타임 패킷 처리 규칙 및 타임아웃/보안 규격	출력 및 차단/예외 계약 (Output / Drop)
				(`ServiceAccount`) 및 HTTP Method 검증	`access denied (403)`
`STEP 7`	**PrivateLink Data Access**	VPC Endpoint (`COMP-06` , `07`)	`TCP 5432(DB)` / `6379(Redis)` / `9094(MSK)`	• `Isolated Data Subnet` 내 ENI 엔드포인트로만 사설 통신 수행 • `TCP Keepalive (idle=60s, intvl=10s, cnt=6)` 설정으로 유휴 커넥션 단절 방지	데이터 계층 Security Group에 등록된 App SG만 연결 수락, 그 외 패킷 즉시 Drop
`STEP 8`	**Controlled Egress Guard**	Egress GW + Network Firewall	외부 파트너 API 호출 (`HTTPS 443`)	• 파드의 직접 외부 인터넷 통신 차단, 모든 외부 호출은 **전용 Egress Gateway 파드**로 집중 • `COMP-04` 방화벽에서 **허용된 FQDN 도메인 화이트리스트(SNI 검증)**만 NAT GW로 통과	미등록 외부 도메인(예: 악성 스크립트 다운로드) 호출 시 **DNS/SNI 단계에서 즉시 차단**

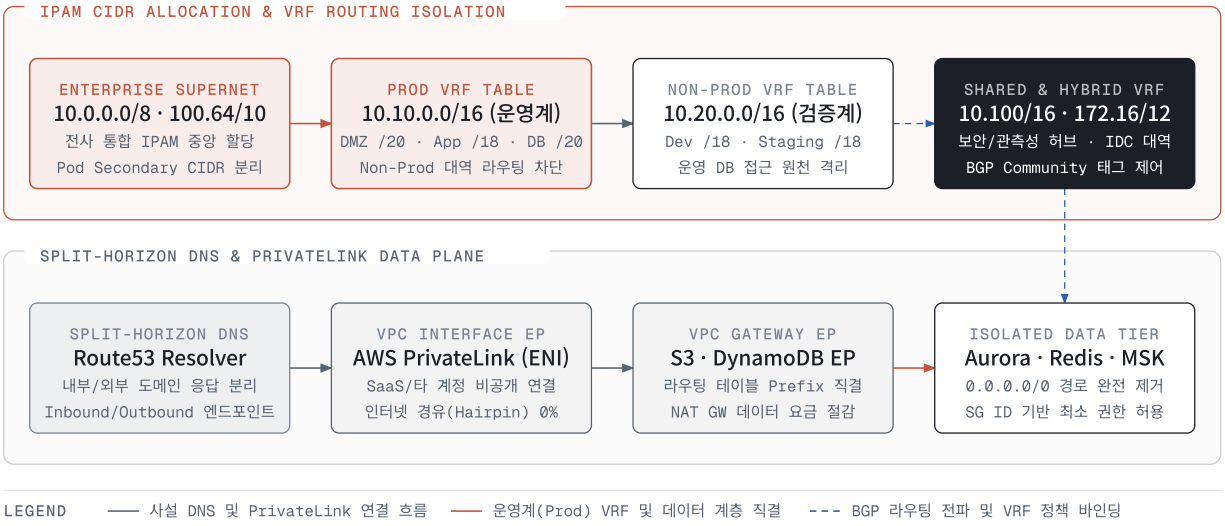
제4장. 데이터 및 영속성 아키텍처 설계 (4. Data & Persistence View)

4.1 전사 IPAM 대역 할당, VRF 라우팅 도메인 격리 및 PrivateLink 구조도

- **네트워크 데이터 뷰 명세**: 네트워크 아키텍처에서의 핵심 데이터 자산인 **IP 주소 공간(IPAM CIDR), VRF 라우팅 테이블(Route Table), DNS 레코드(Split-Horizon PHZ), 사설 엔드포인트(PrivateLink)**를 계층화하여 IP 충돌을 원천 방지하고 환경 간 트래픽 혼입을 차단함.

VIEW 03 · IPAM CIDR HIERARCHY, VRF ROUTING TABLE & PRIVATELINK ARCHITECTURE

[데이터 뷰] 전사 IPAM 대역 설계, VRF 라우팅 격리 및 PrivateLink 구조도



View 3 데이터 뷰 — 전사 IPAM 슈퍼넷(CIDR) 대역 할당, VRF 라우팅 격리 및 PrivateLink 데이터 구조도

4.2 전사 IPAM 대역 할당 및 VRF 라우팅·DNS 정책 명세표 (IPAM & Routing Specification)

구분 ID	네트워크 도메인 계층	할당 CIDR 대역 (RFC 1918 / 6598)	서브넷 분할 규격 (3 AZs 대칭)	VRF 라우팅 테이블 및 격리 정책
`NET-DATA-01`	**Production VPC (운영계)**	• Primary: **`10.10.0.0/16`** (65,536 IPs) • K8s Pod: **`100.64.0.0/16`** (CGNAT)	• Public DMZ: `/20` (AZ별 `/22`) • Private App: `/18` (AZ별 `/20`) • Isolated Data: `/20` (AZ별 `/22`) • TGW Attach: `/24` (AZ별 `/28`)	• **VRF:** **`rtb-tgw-prod`** 바인딩 • `Non-Prod(10.20.0.0/16)` 방 엔트리 완전 제거 (Blackhole 처리) • K8s 파드는 `100.64/16` Second CIDR를 사용하여 RFC 1918 고갈 방
`NET-DATA-02`	**Non-Prod VPC (개발/검증계)**	• Staging: **`10.20.0.0/16`** • Dev/QA: **`10.30.0.0/16`** • K8s Pod: **`100.65.0.0/16`**	• Public DMZ: `/21` (AZ별 `/23`) • Private App: `/18` (AZ별 `/20`) • Isolated Data: `/21` (AZ별 `/23`)	• **VRF:** **`rtb-tgw-nonprod`** 바인딩 • 운영계(`10.10.0.0/16`) 및 온프레 영 DB 대역으로의 패킷 전달 100% 차 • `Shared Security VPC(10.10` 만 방화벽 경유 통신 허용
`NET-DATA-03`	**Shared Security & Edge Hub**	• Security/Inspection: **`10.100.0.0/16`** • Shared Tools(CI/Obs): **`10.101.0.0/16`**	• Firewall/GWLB: `/24` (AZ별 `/26`) • Centralized Egress NAT: `/22` • Management/Observability: `/20`	• **VRF:** **`rtb-tgw-inspection`** 바 • 모든 Spoke 간 교차 트래픽이 1차로 Appliance Mode(`ApplianceModeSupport=` 활성화로 비대칭 라우팅(Asymmetric Routing) 방지
`NET-DATA-04`	**On-Premises IDC & Branch**	• Primary IDC: **`172.16.0.0/16`** • DR IDC: **`172.17.0.0/16`**	• Legacy Core Tier: `/18` • Enterprise DB Mainframe: `/20` • DX Transit VIF Link: `169.254.x.0/30`	• **VRF:** **`rtb-tgw-hybrid`** 바인딩 • BGP Community 태그 (`64512:100` =Active, `64512:200` =Backup) 및 `AS_PA` `Prepending` 으로 주/예비 전용선 경 위 통제

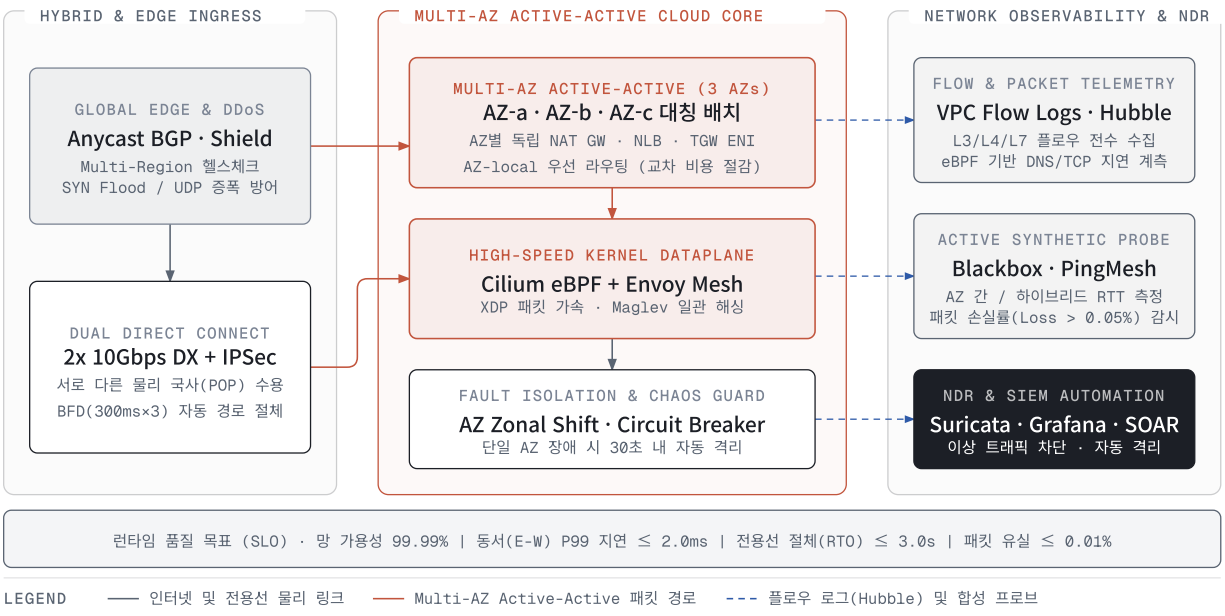
제5장. 물리 배포 및 회복탄력성·관측성 설계 (5. Deployment, Resilience & Observability View)

5.1 Multi-AZ Active-Active 물리 토폴로지 및 하이브리드 이중화 다이어그램

- **물리 배치 및 고가용성 명세**: 모든 클라우드 네트워크 인프라는 **3개 가용영역(`AZ-a` , `AZ-b` , `AZ-c`) 대칭형 Active-Active 구조**로 배포되며, 온프레미스 데이터센터와는 서로 다른 물리 국사(POP)에 수용된 **듀얼 10Gbps Direct Connect 회선 + IPSec VPN 백업**으로 연결됨.

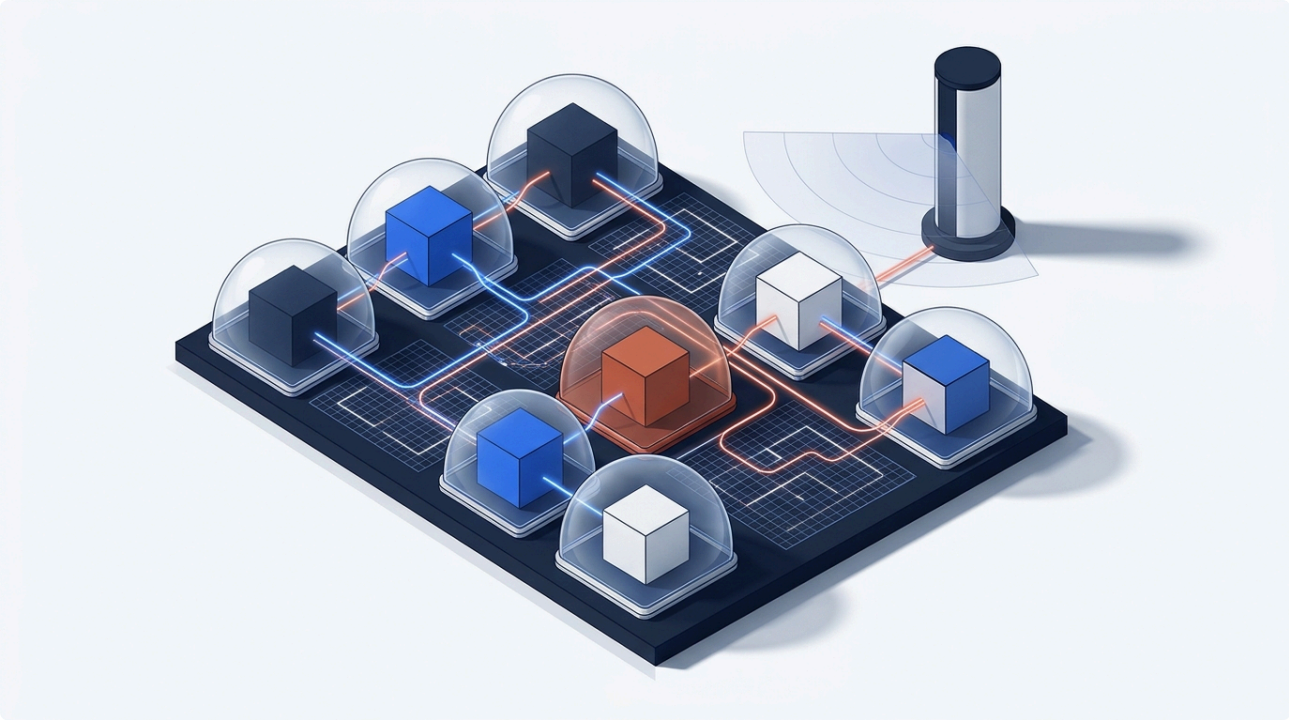
VIEW 04 · MULTI-AZ HA TOPOLOGY, HYBRID DX RESILIENCE & TELEMETRY

[배포 뷰] Multi-AZ Active-Active 물리 토폴로지 및 네트워크 관측성 설계도



View 4 배포 뷰 — Multi-AZ Active-Active 물리 토폴로지, 하이브리드 전용선 이중화 및 네트워크 관측성 설계도

5.2 Zero-Trust 보안, 무중단 장애 절체(Resilience) 및 네트워크 관측성 상세 설계



Zero-Trust 마이크로세그먼테이션(mTLS + eBPF) 및 Multi-AZ 자동 장애 절체·관측성 개념도

- **회복탄력성·보안·관측성 엔지니어링 파라미터 명세표 (Network Engineering Specification)**

규격 ID	설계 영역	적용 컴포넌트	표준 설정 파라미터 및 임계치 명세 (Parameter Specification)	동작 및 장애 격리 규칙
`NET-RES-01`	**하이브리드 전용선 초고속 절체 (BGP + BFD)**	Direct Connect + Core Router	• `eBGP Keepalive: 10s` , `Holdtime: 30s` • **양방향 포워딩 감지(`BFD`): `Interval 300ms × Multiplier 3 = 900ms`** • Primary DX1/DX2 ECMP 활성 + Backup IPSec VPN(`AS_PATH +2`) 대기	• 광케이블 단선 또는 장비 장애 발생 시 기본 BGP 타이머(30~90초)를 기다리지 않고 **0.9초 내 링크 다운 감지 → 3.0초 이내 무중단 우회 완료**
`NET-RES-02`	**단일 가용영역(AZ) 장애 격리 (Zonal Shift)**	NLB / ALB + Route53 ARC + TGW	• TGW Attachment 및 NAT Gateway 3개 AZ 독립 배포 (Cross-AZ 의존성 0%) • `Topology Aware Routing (service.kubernetes.io/topology-mode: Auto)` 활성화 • `AWS Zonal Shift` 및 Istio `OutlierDetection(consecutive5xx: 5, baseEjectionTime: 30s)`	• 특정 AZ 전력/냉각 장애 또는 패킷 블랙홀 발생 시 **30초 이내 해당 AZ의 NLB DNS 레코드 및 엔드포인트 가중치를 0%로 격리**하여 타 정상 AZ로 100% 전환
`NET-RES-03`	**리눅스 커널 네트워크 튜닝 및 MTU 표준화**	K8s Worker Node `sysctl` & CNI	• VPC 내부 점보 프레임: `MTU 9001` / DX Transit VIF: `MTU 8500` / IPSec VPN: `MTU 1400 (TCP MSS Clamping 1360)` • `net.core.somaxconn = 65535` , `net.ipv4.tcp_tw_reuse = 1` • `net.ipv4.ip_local_port_range = 10240 65535` , `tcp_Keepalive_time = 60`	• 터널링(GENEVE/HBONE/VPN) 구간 패킷 단편화(Fragmentation Drop) 0% 보장 • 대규모 동시 연결(10만 Conntrack) 시 Ephemeral Port 고갈 및 SYN Backlog 드롭 방지
`NET-RES-04`	**실시간 플로우 관측성 및 능동 프로브 (Telemetry)**	VPC Flow Logs v5 + Cilium Hubble + PingMesh	• **Flow Logs**: 1분 집계 주기, `pkt-srcaddr` , `pkt-dstaddr` , `tcp-flags` , `az-id` , `sublocation-id` 확장 필드 수집 • **Hubble Metrics**: `dns_queries_total` , `drop_total(reason)` , `tcp_flags_total` , `http_request_duration_seconds` • **PingMesh**: 전 노드/AZ 간 1초 주기 UDP/TCP 합성 패킷 송수신	• 알람 임계치: AZ 간 패킷 손실률 `> 0.05%` , DNS 응답 지연 `P99 > 15ms` , `Cilium Policy Denied` 급증 시 PagerDuty/Slack 즉시 경보 발보

제6장. 표준 인터페이스 및 코드 템플릿 명세 (6. Standard Interface & Code Specification)

6.1 네트워크 인프라(IaC) 및 Zero-Trust 정책 표준 코드 블루프린트

- **[Template 1] Hub-and-Spoke Transit Gateway 및 Inspection VRF 격리 (`Terraform HCL` — `COMP-03` , `COMP-04`)**

HCL

```
resource "aws_ec2_transit_gateway" "enterprise_hub" {
  description                     = "Enterprise Central Transit Hub (SAD-NET-2026-001)"
  amazon_side_asn                 = 64512
  auto_accept_shared_attachments  = "disable"
  default_route_table_association = "disable"
  default_route_table_propagation = "disable"
  dns_support                     = "enable"
  vpn_ecmp_support                = "enable"
  tags                            = { Name = "tgw-enterprise-hub-prod", Standard = "SAD-NE
}

# Inspection VPC Attachment: 비대칭 라우팅 방지를 위해 Appliance Mode 필수 활성화
resource "aws_ec2_transit_gateway_vpc_attachment" "inspection_hub" {
  transit_gateway_id                                = aws_ec2_transit_gateway.enterprise_hub
  vpc_id                                            = var.inspection_vpc_id
  subnet_ids                                        = var.inspection_tgw_subnet_ids # 3 AZs
  appliance_mode_support                            = "enable"
  transit_gateway_default_route_table_association = false
  transit_gateway_default_route_table_propagation = false
}

# Prod VRF 라우팅 테이블: Non-Prod(10.20.0.0/16) 블랙홀 차단 및 기본 경로 Inspection Firewall 강제
resource "aws_ec2_transit_gateway_route" "prod_block_nonprod" {
  destination_cidr_block         = "10.20.0.0/16"
  blackhole                      = true
  transit_gateway_route_table_id = aws_ec2_transit_gateway_route_table.prod_vrf.id
}

resource "aws_ec2_transit_gateway_route" "prod_to_inspection_firewall" {
  destination_cidr_block         = "0.0.0.0/0"
  transit_gateway_attachment_id  = aws_ec2_transit_gateway_vpc_attachment.inspection_hub.i
  transit_gateway_route_table_id = aws_ec2_transit_gateway_route_table.prod_vrf.id
}
```

- **[Template 2] Cilium eBPF L3/L4/L7 마이크로세그먼테이션 및 DNS Egress 통제 (`YAML` — `COMP-05`)**

YAML

```yaml
apiVersion: cilium.io/v2
kind: CiliumNetworkPolicy
metadata:
  name: order-service-zero-trust-policy
  namespace: prod-commerce
spec:
  endpointSelector:
    matchLabels:
      app.kubernetes.io/name: order-service
      env: prod
  ingress:
    # [Ingress 규칙] 오직 API Gateway 및 Payment 서비스(SPIFFE 인증 파드)의 지정된 HTTP 경로만 허용
    - fromEndpoints:
        - matchLabels:
            app.kubernetes.io/name: api-gateway
            io.kubernetes.pod.namespace: istio-ingress
      toPorts:
        - ports:
            - port: "8080"
              protocol: TCP
          rules:
            http:
              - method: "POST"
                path: "/api/v1/orders"
              - method: "GET"
                path: "/api/v1/orders/[0-9a-zA-Z-]+"
  egress:
    # [Egress 규칙 1] CoreDNS 질의 허용 및 허용된 외부 PG사 도메인 패턴만 DNS 응답 가로채기 허용
    - toEndpoints:
        - matchLabels:
            io.kubernetes.pod.namespace: kube-system
            k8s-app: kube-dns
      toPorts:
        - ports:
            - port: "53"
              protocol: ANY
          rules:
            dns:
              - matchPattern: "*.rds.amazonaws.com"
              - matchPattern: "api.tosspayments.com"
    # [Egress 규칙 2] Isolated Data Subnet(10.10.128.0/20) 내 Aurora PostgreSQL(5432)만 사설 인
    - toCIDRSet:
        - cidr: 10.10.128.0/20
      toPorts:
        - ports:
            - port: "5432"
              protocol: TCP
```

- **[Template 3] Istio Ambient `Strict mTLS` 강제 및 K8s `Gateway API` 카나리 라우팅 (`YAML` — `COMP-02` , `COMP-05`)**

YAML

```yaml
apiVersion: security.istio.io/v1
kind: PeerAuthentication
metadata:
  name: global-strict-mtls
  namespace: istio-system
spec:
  mtls:
    mode: STRICT # 클러스터 내 모든 동서(East-West) 평문(Plaintext) 통신 100% 거부
---
apiVersion: gateway.networking.k8s.io/v1
kind: HTTPRoute
metadata:
  name: order-api-canary-route
  namespace: prod-commerce
spec:
  parentRefs:
    - name: prod-external-envoy-gateway
      namespace: istio-ingress
  hostnames:
    - "api.company.com"
  rules:
    - matches:
        - path:
            type: PathPrefix
            value: /api/v1/orders
      timeouts:
        request: 5s
        backendRequest: 3s
      backendRefs:
        - name: order-service-stable
          port: 8080
          weight: 95
        - name: order-service-canary
          port: 8080
          weight: 5
```

제7장. 아키텍처 적합성 검증 및 기술 스택 명세 (7. Architecture Fitness & Tech Stack BOM)

7.1 OPA(Open Policy Agent) / Conftest 기반 네트워크 적합성 자동 검증 규칙 (Fitness Functions)

모든 네트워크 Terraform 변경 사항(`tfplan.json`)과 Kubernetes 네트워크 매니페스트는 아래 5대 자동화 검증 규칙(`NET-RULE-01` ~ `NET-RULE-05`)을 통과해야 하며, 단 1건이라도 위반 시 CI/CD 파이프라인에서 인프라 배포가 즉시 차단됨.

규칙 ID	네트워크 적합성 검증 규칙명	검증 대상 리소스	위반 판정 조건 (Violation Condition)
`NET-RULE-01`	**Spoke 간 직접 VPC Peering 생성 금지**	`aws_vpc_peering_connection`	중앙 Transit Gateway(`COMP-03`)를 우회하는 `aws_vpc_peering_connection` 리소스가 코드에 포함될 시
`NET-RULE-02`	**Public Ingress `0.0.0.0/0` 관리 포트 개방 금지**	`aws_security_group_rule` , `aws_vpc_security_group_ingress_rule`	`0.0.0.0/0` 또는 `::/0` 을 대상으로 `SSH(22)` , `RDP(3389)` , `DB(3306, 5432, 6379)` 포트가 허용될 시
`NET-RULE-03`	**데이터 서브넷 외부 인터넷 경로 (`IGW` / `NAT`) 연결 금지**	`aws_route` , `aws_route_table`	`Isolated Data Subnet` 에 연결된 라우팅 테이블에 `gateway_id(igw-*)` 또는 `nat_gateway_id(nat-*)` 경로가 존재할 시
`NET-RULE-04`	**프로덕션 네임스페이스 Default-Deny 및 Strict mTLS 필수**	`CiliumNetworkPolicy` , `PeerAuthentication`	`prod-*` 네임스페이스 생성 시 기본 Ingress/Egress 차단 정책 또는 `PeerAuthentication(mode: STRICT)` 가 누락될 시
`NET-RULE-05`	**VPC Flow Logs 및 Multi-AZ 3중화 배치 강제**	`aws_vpc` , `aws_lb` , `aws_ec2_transit_gateway_vpc_attachment`	신규 VPC 생성 시 `aws_flow_log` 가 누락되거나, NLB/ALB/TGW Attachment의 서브넷 개수가 3개 AZ 미만일 시

REGO

```
package enterprise.network.fitness

import rego.v1

# [NET-RULE-01] Spoke 간 직접 VPC Peering 생성 원천 차단 (반드시 Central Transit Gateway 경유)
deny contains msg if {
    some rc in input.resource_changes
    rc.type == "aws_vpc_peering_connection"
    rc.change.actions[_] != "delete"
    msg := sprintf("[NET-RULE-01 위반] 직접 VPC Peering(%s) 생성 금지: 모든 망 간 연결은 Central Trans
}

# [NET-RULE-02] 0.0.0.0/0 대상 관리/데이터베이스 포트 개방 원천 차단
forbidden_public_ports := {22, 3389, 3306, 5432, 6379, 9092, 27017}

deny contains msg if {
    some rc in input.resource_changes
    rc.type == "aws_vpc_security_group_ingress_rule"
    rc.change.after.cidr_ipv4 == "0.0.0.0/0"
    port := rc.change.after.from_port
    forbidden_public_ports[port]
    msg := sprintf("[NET-RULE-02 위반] 보안그룹(%s)에서 0.0.0.0/0 대상 위험 포트(%d) 개방이 감지됨", [rc
}

# [NET-RULE-03] Isolated Data Subnet 라우팅 테이블 내 IGW / NAT Gateway 경로 연결 금지
deny contains msg if {
    some rc in input.resource_changes
    rc.type == "aws_route"
    contains(rc.address, "isolated_data")
    after := rc.change.after
     (after.gateway_id != null; startswith(after.gateway_id, "igw-"))
    msg := sprintf("[NET-RULE-03 위반] 데이터 전용 서브넷(%s)에 외부 Internet Gateway 경로 연결 금지", [
}
```

7.2 전사 표준 네트워크 기술 스택 명세서 (Standard Network Technology BOM)

기술 분류	표준 채택 기술 (Engine / Appliance)	표준 버전 / 규격	아키텍처 역할 및 필수 설정 규격
Global Edge & WAF	AWS Route53 + CloudFront + AWS WAF v2	**TLS 1.3 / HTTP/3**	Anycast GSLB, OWASP CRS 3.3, Bot Control, L3/L4 Shield Advanced
Core Transit & Firewall	AWS Transit Gateway + Network Firewall (Suricata)	**eBGP (ASN 64512)**	VRF 라우팅 테이블 분리, `ApplianceMode=enable`, DPI/FQDN Egress 필터링
Hybrid Interconnect	AWS Direct Connect (듀얼 10G) + Site-to-Site VPN	**802.1AE MACsec / BFD**	이원화 POP 수용, `BFD(300ms×3)`, ECMP 로드밸런싱, BGP Community 제어
Kubernetes CNI & Dataplane	Cilium (eBPF Native Routing / ENI Mode)	**v1.16.x LTS**	`kubeProxyReplacement=true`, `bpf.masquerade=true`, XDP 가속, Secondary CIDR
Ingress & Service Mesh	Envoy Gateway (K8s Gateway API) + Istio Ambient	**v1.1.x / Istio 1.23.x**	무사이드카 `ztunnel(HBONE mTLS)`, SPIFFE ID 인증, `Waypoint` L7 정책 제어
Private Connectivity & DNS	AWS PrivateLink + Route53 Resolver (Inbound/Outbound)	**Split-Horizon DNS**	S3/DynamoDB Gateway EP, SaaS/MSA Interface EP, 온프레미스 조건부 포워딩
Network Observability	Cilium Hubble + VPC Flow Logs v5 + PingMesh	**OpenTelemetry / Prom**	L3/L4/L7 플로우 그래프, TCP Retransmit/DNS 지연 메트릭, 1초 주기 AZ 간 합성 프로브
Network IaC & Governance	OpenTofu / Terraform + OPA (Conftest) + Batfish	**v1.8.x / OPA v0.68.x**	네트워크 변경 사항 정적 정책 검증(`NET-RULE-01~05`), 라우팅 도달 가능성 사전 시뮬레이션