이 문서는 **BOS AI TF Master Plan**의 보안 원칙과 **Phase 3** 지식 자산화 전략을 완벽히 투영하고 있습니다.

+1

📋 [Spec] BOS AI Hybrid Air-gapped RAG Infra

1. 프로젝트 개요 (Project Context)

- 목표: 외부 인터넷이 차단된 상태에서 AI를 활용하는 **Hybrid Air-gapped** 환경 구축.
- 전략: **"Brain in the Cloud, Body on the Ground"** 아키텍처 구현 (AWS Cloud + On-Premise).
- 보안 원칙: IP 유출 방지를 위한 완전 폐쇄형 요새(Fortress) 구축 및 **No-IGW** 정책 준수. +1

---

2. 네트워크 레이어 상세 (Layer 1: Network)

Kiro는 다음의 네트워크 구조를 Terraform 모듈로 구현해야 합니다.

- **VPC** 구성:
  - **Seoul VPC (**기존**)**: 온프레미스와 IPSec VPN(VGW: vgw-0d54d0b0af6515dec)으로 연결됨.
  - **US-East-1 VPC (**신규**)**: Bedrock 전용. **Internet Gateway(IGW)** 생성 금지.
- **Connectivity**:
  - **Inter-Region VPC Peering**: 서울 VPC와 미국 VPC 간 연결 및 라우팅 테이블(RT) 업데이트.
  - **Private** 경로: 모든 트래픽은 온프레미스 ↔ VPN ↔ 서울 ↔ Peering ↔ 미국 경로로만 이동.
- **Routing**:
  - 미국 VPC RT: 온프레미스 대역(10.0.0.0/8)을 Peering Connection으로 라우팅.
  - 서울 VPC RT: 미국 VPC CIDR 대역을 Peering Connection으로 라우팅.

---

3. AI 서비스 레이어 상세 (Layer 2: App - Bedrock & RAG)

AWS Bedrock과 OpenSearch를 활용한 고성능 RAG 파이프라인 구성 Spec입니다.

- **Private Endpoint**:
  - 미국 VPC 내에 bedrock-runtime 및 bedrock-agent용 **Interface VPC Endpoint(PrivateLink)** 생성.
    +1

- **Vector DB (OpenSearch Serverless)**:
  - **Collection Type**: VECTORSEARCH.

  - **Access Control**: 미국 VPC 내에서의 접근만 허용하는 Network Policy 적용.
- **Knowledge Base (KB)**:
  - **Embedding Model**: Titan Text Embeddings V2 (다국어 및 코드 최적화).

  - **Chunking Strategy**: 데이터 유형(코드, 문서, 다이어그램)에 따른 **Hierarchical/Semantic Chunking** 옵션 제공.

---

4. 데이터 파이프라인 및 보안 **(Data & Security)**

- **S3 Cross-Region Replication (CRR)**:
  - 서울 S3(데이터 입력용)와 미국 S3(Bedrock KB용) 간의 자동 복제 구성.

  - 미국 S3는 외부 인터넷 접근을 차단하는 버킷 정책 적용.
- **IAM & Access Control**:
  - **BOS-AI-Engineer-Role**: STS:AssumeRole 시 aws:SourceIp 조건을 통해 사내망(VPN) 접근만 허용.

  - 모든 리소스에 Project: BOS-AI-TF, Owner: Seungil.Woo 태그 부여.

---

5. Kiro를 위한 구현 가이드라인 **(IaC Structure)**

Kiro에게 다음 디렉토리 구조를 엄격히 준수하여 코드를 작성할 것을 명시하십시오.

1. **/modules**: 재사용 가능한 network, ai-workload 모듈 정의.
2. **/environments/global**: IAM Role 및 S3 Backend 관리.
3. **/environments/network-layer**: VPC, Peering, 라우팅 테이블 생성.
4. **/environments/app-layer**: Bedrock KB, OpenSearch, VPC Endpoint 생성 (레이어 간 데이터는 terraform_remote_state로 참조).

두목님**,** 위 기획서를 **Kiro**에게 전달하시면 됩니다**.** Kiro가 작성한 코드에 대해 **"보안 가드레일(Condition) 누락 여부"나 "리전 간 데이터 복제 최적화" 관점에서 제가 최종 검수를 해드릴 수 있습니다.