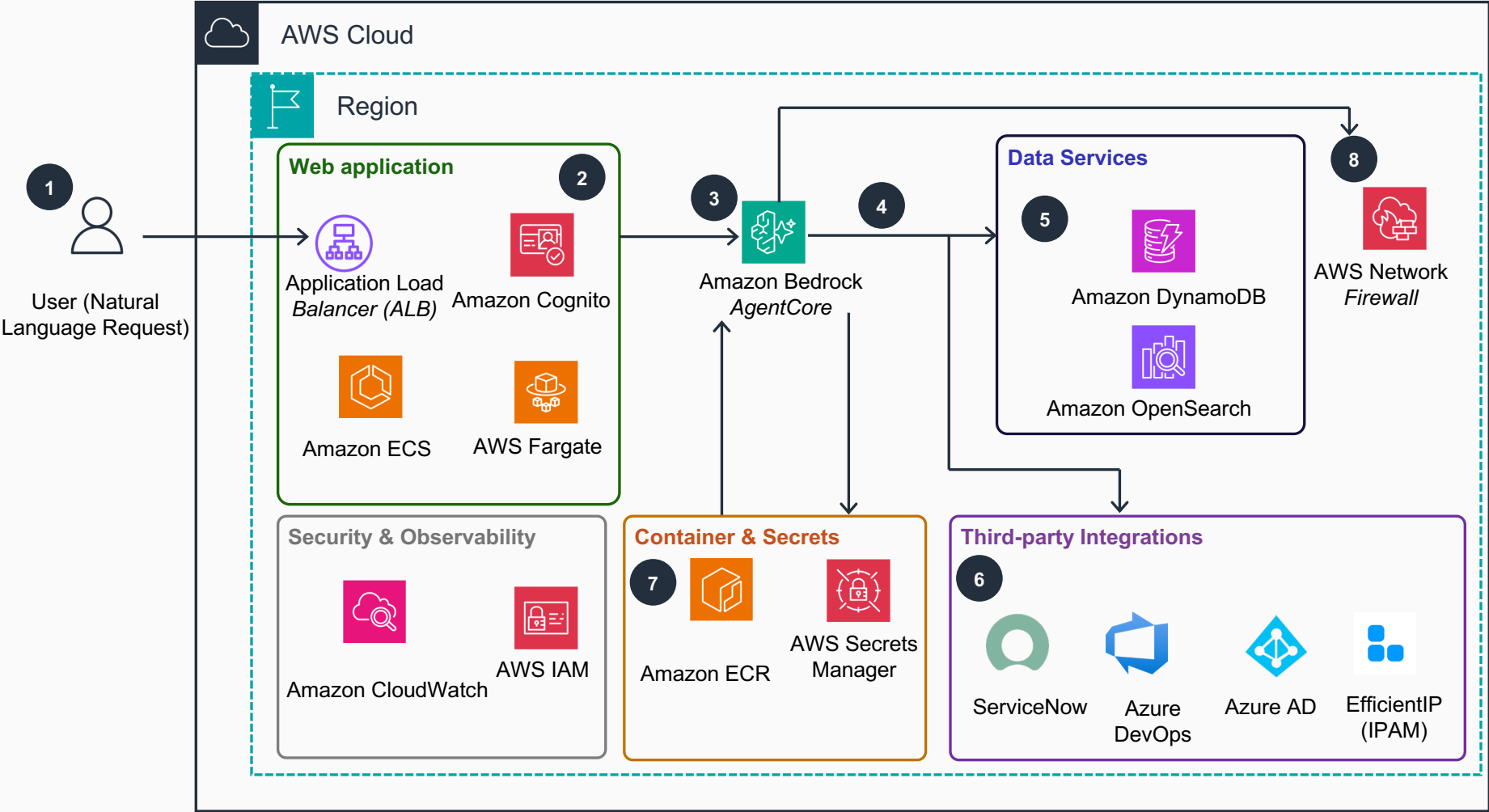


Guidance for Agentic Network Firewall Automation on AWS

This architecture diagram illustrates how a multi-agent system automates AWS Network Firewall rule management through natural language commands, integrating IPAM validation, GitSecOps workflows, and change management to streamline security operations.



- 1 A user submits a natural-language request to the web application, served by **Amazon ECS** on **AWS Fargate** behind an **AWS Application Load Balancer (ALB)**.
- 2 **Amazon Cognito** authenticates the user, federated with Azure Active Directory (Azure AD) for enterprise single sign-on.
- 3 The web app streams chat with **Amazon Bedrock AgentCore** via the `InvokeAgentRuntime` API; the supervisor agent runs on the Strands Agents SDK with **Amazon Bedrock** (Claude Sonnet 4) and AgentCore Memory.
- 4 The supervisor delegates to five specialist agents (Account Details, Firewall Logs, GitSecOps, IPAM, and ServiceNow).
- 5 Agents query **Amazon DynamoDB** for account metadata and **Amazon OpenSearch Service** for firewall alert, flow, and TLS logs.
- 6 Agents integrate with third-party systems: ServiceNow (change requests), Azure DevOps (Git commit and pull request), and EfficientIP IPAM (IP/CIDR validation).
- 7 **Amazon Elastic Container Registry (Amazon ECR)** stores the agent and web-app container images; **AWS Secrets Manager** holds the integration credentials read by AgentCore.
- 8 Validated Suricata rules are staged via Git pull request and change request and, after approval, applied to **AWS Network Firewall**; responses stream to the user over Server-Sent Events (SSE).

