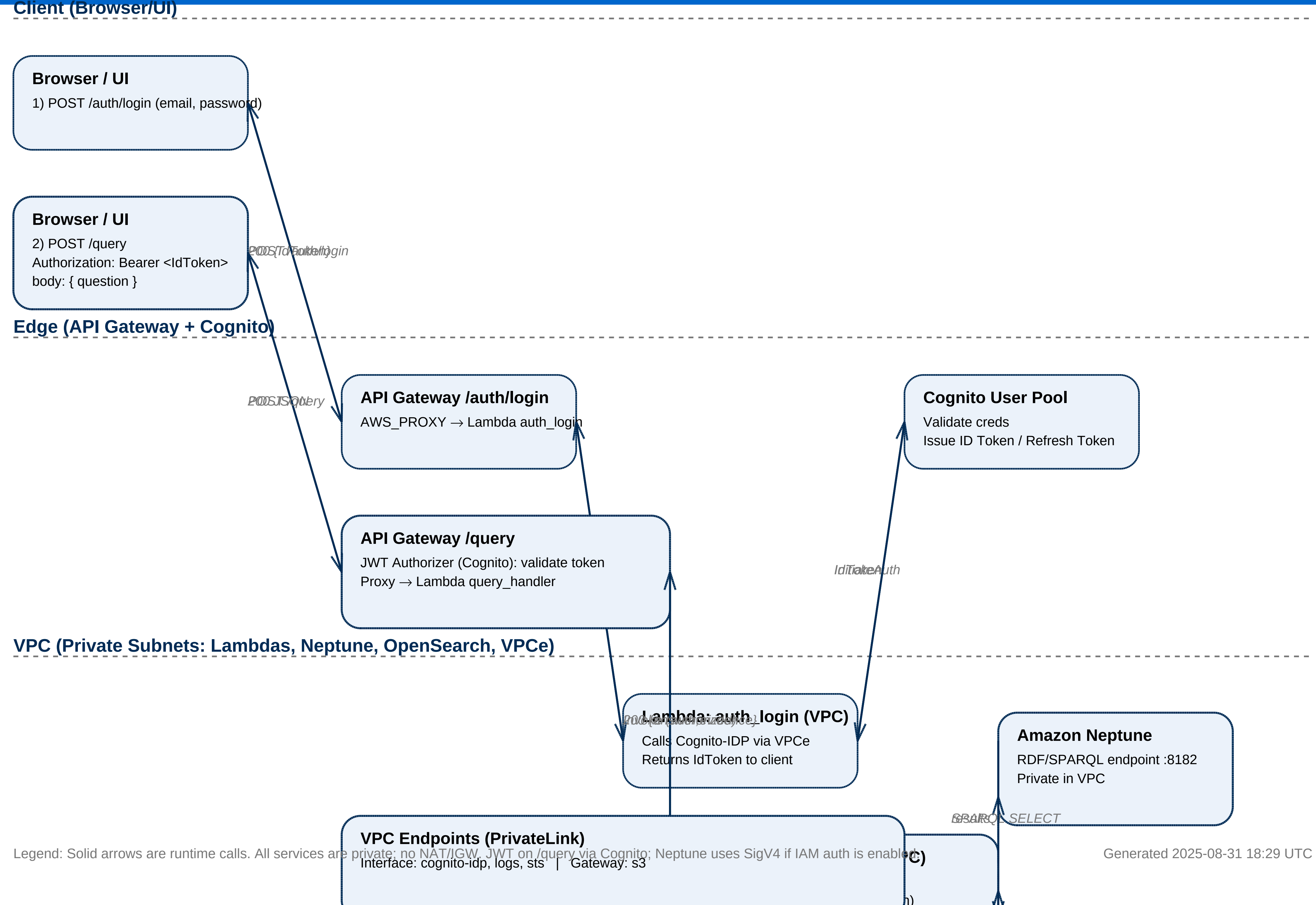
End-to-End Request Flow — No-NAT VPC, Cognito JWT, OpenSearch, Neptune

Auth & Query paths; VPC-only egress with VPC Endpoints; API Gateway JWT protection on /query

YOUR LOGO



Client (Browser/UI)

Browser / UI
1) POST /auth/login (email, password)

Browser / UI
2) POST /query
Authorization: Bearer <IdToken>
body: { question }

Edge (API Gateway + Cognito)

API Gateway /auth/login
AWS_PROXY → Lambda auth_login

Cognito User Pool
Validate creds
Issue ID Token / Refresh Token

API Gateway /query
JWT Authorizer (Cognito): validate token
Proxy → Lambda query_handler

VPC (Private Subnets: Lambdas, Neptune, OpenSearch, VPCe)

Lambda: auth_login (VPC)
Calls Cognito-IDP via VPCe
Returns IdToken to client

Amazon Neptune
RDF/SPARQL endpoint :8182
Private in VPC

VPC Endpoints (PrivateLink)
Interface: cognito-idp, logs, sts | Gateway: s3

Legend: Solid arrows are runtime calls. All services are private; no NAT/IGW. JWT on /query via Cognito; Neptune uses SigV4 if IAM auth is enabled.

Generated 2025-08-31 18:29 UTC