Private link

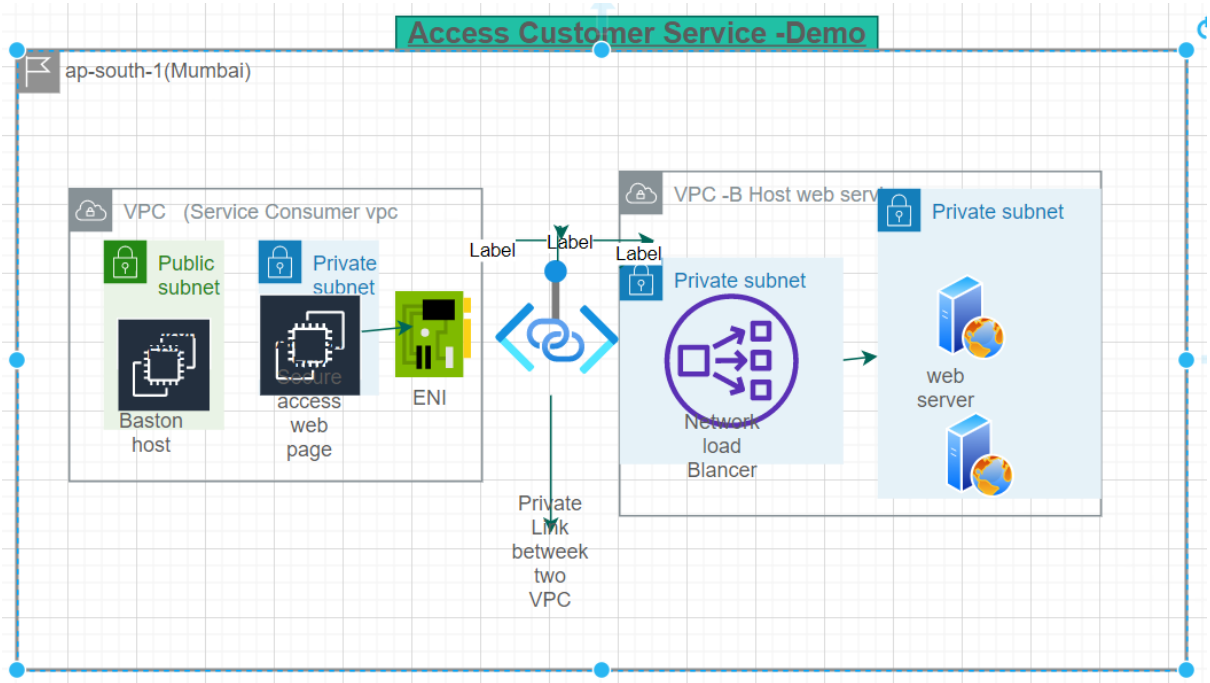
What is AWS PrivateLink?

AWS PrivateLink is a highly available, scalable technology that enables you to privately connect your VPC to services as if they were in your VPC. You do not need to use an internet gateway, NAT device, public IP address, AWS Direct Connect connection, or AWS Site-to-Site VPN connection to allow communication with the service from your private subnets. Therefore, you control the specific API endpoints, sites, and services that are reachable from your VPC.

Most secure & scalable way to expose a service to 1000s of VPC (own or other accounts) • Does not require VPC peering, internet gateay, NAT, route tables…gateway

• Requires a network load balancer (Service VPC) and ENI (Customer VPC) •

If the NLB is in multiple AZ, and the ENI in multiple AZ, the solution is fault tolerant!



1. **Pre-requisites – Create EC2 AMI having httpd webserver. We need this to launch Private EC2 instance in VPC-B to host the dummy service.**
2. **Create VPC-B with 2 Private Subnets**
3. **Launch EC2 instance in a Private Subnet using AMI created earlier**
4. **Create NLB in another Private Subnet and Register EC2 instance behind NLB**
5. **Create VPC Endpoint Service in VPC-B and associate NLB**

6. **Whitelist the VPC-A AWS account (if both VPCs are in different AWS accounts)**
7. **Create Service Consumer VPC (VPC-A) with Public and Private subnets**
8. **Create VPC endpoint in VPC-A and search for endpoint service created above**
9. **Login to Private EC2 instance in Consumer VPC and access VPC endpoint DNS**

The following diagram shows how you share your service that's hosted in AWS with other AWS customers, and how those customers connect to your service. As the service provider, you create a Network Load Balancer in your VPC as the service front end. You then select this load balancer when you create the VPC endpoint service configuration. You grant permission to specific AWS principals so that they can connect to your service. As a service consumer, the customer creates an interface VPC endpoint, which establishes connections between the subnets that they select from their VPC and your endpoint service. The load balancer receives requests from the service consumer and routes them to the targets hosting your service.

Share your services through AWS PrivateLink