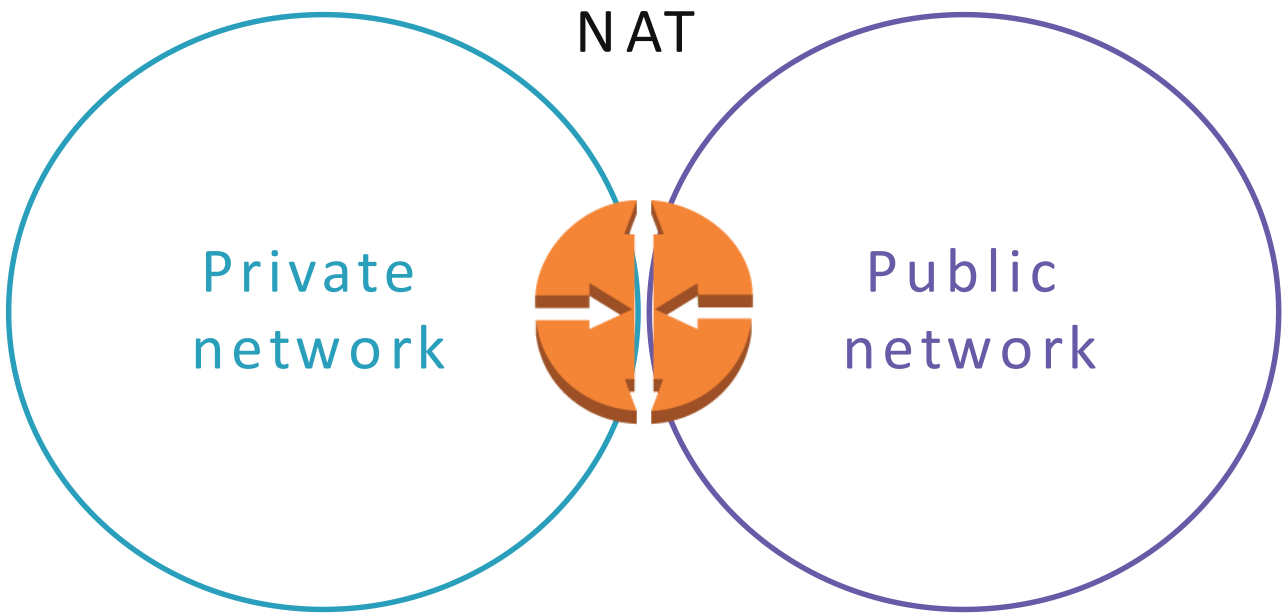
Understanding and Configuring NAT Instances, Gateways, and VPC Endpoints

Single NAT can lead to bottlenecks

If too much traffic passes through

NAT gateway instead

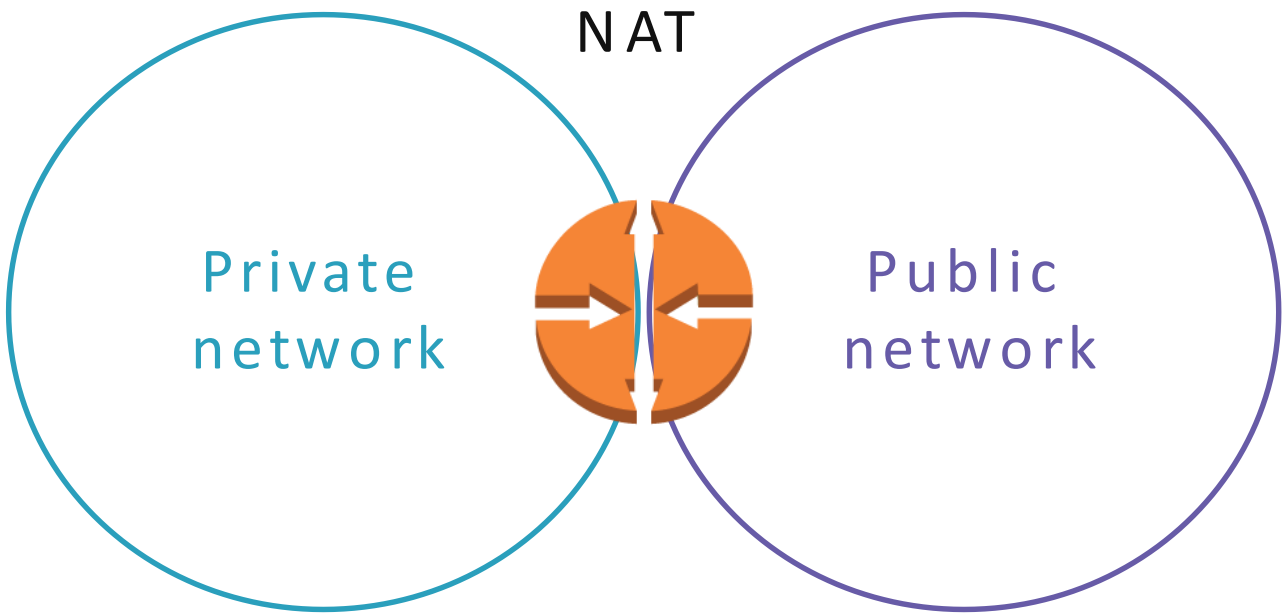


VPC NAT Bottlenecks

Scale Up:
Increase instance size

Choose instance that supports enhanced networking

Scale Out:
Add NATs / subnets and migrate workloads

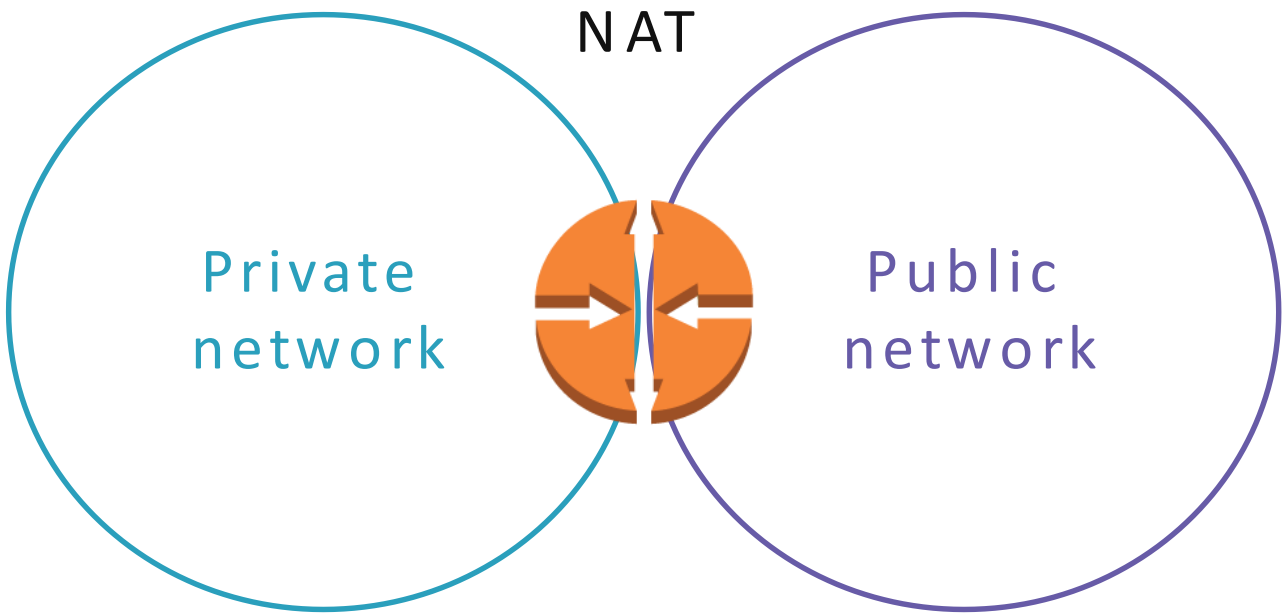


VPC NAT Bottlenecks

HA for NAT is possible
Each subnet can route to a single NAT at a time

Subnet failover to another NAT is supported

For more information:
https://aws.amazon.com/articles/2781451301784570

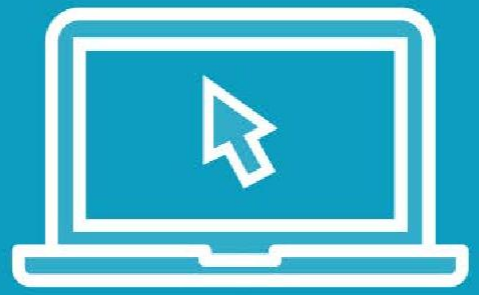


VPC NAT High Availability

NAT Instances vs NAT Gateways

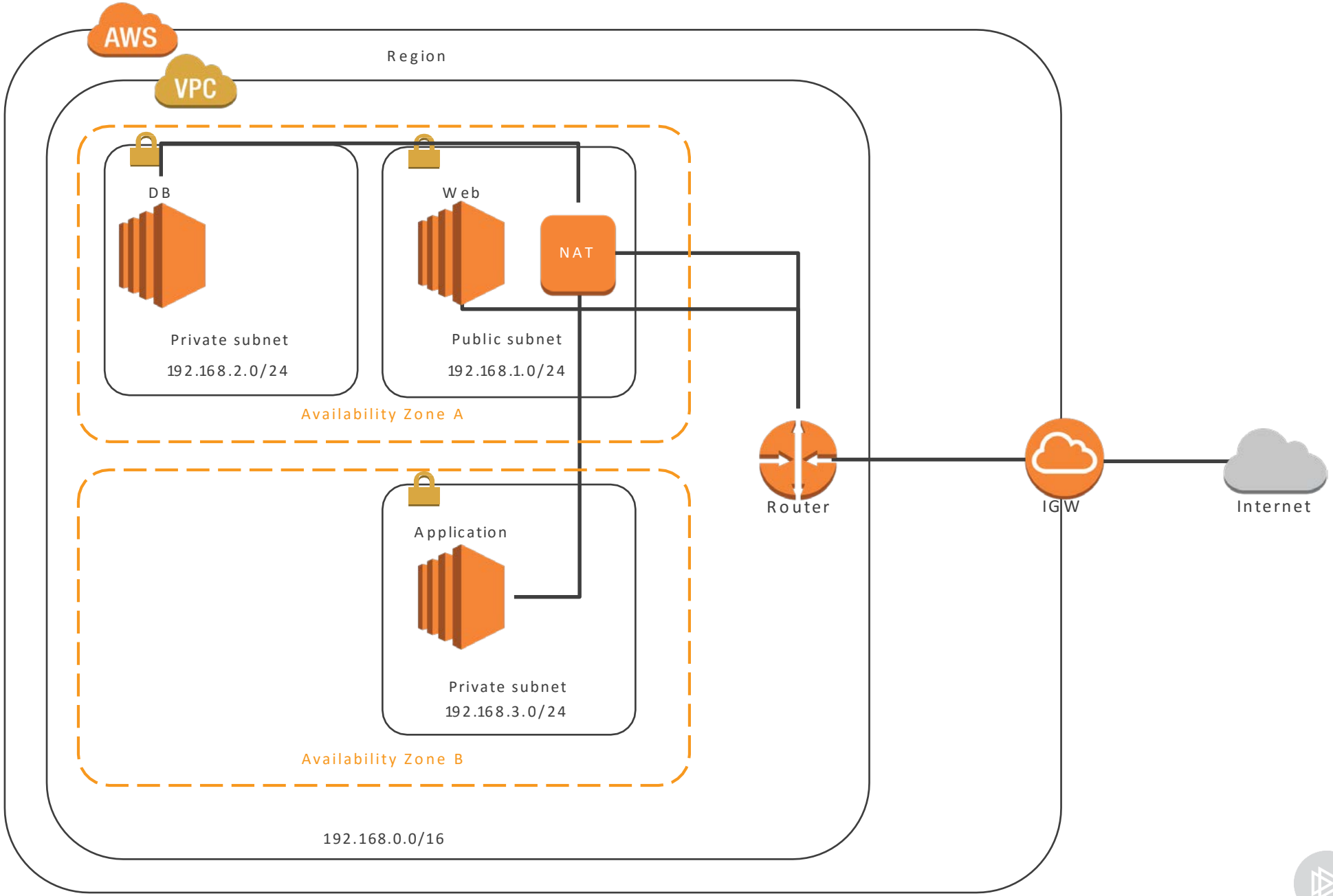
NAT Instances	NAT Gateways
Use a script to manage failover between instances	Highly available. NAT gateways in each Availability Zone are implemented with redundancy
Depends on the bandwidth of the instance type	Supports bursts of up to 10Gbps
Managed by you	Managed by AWS
A generic Amazon Linux AMI that's configured to perform NAT	Software is optimized for handling NAT traffic
Manual port forwarding	Port forwarding is not supported
Use a bastion server	Bastion servers not supported
View CloudWatch alarms	Traffic metrics not supported

Demo

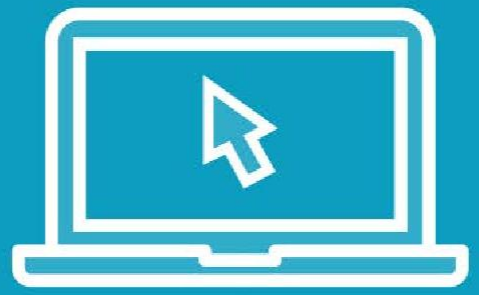


Configure NAT instance and NAT gateway

Wired Brain Coffee
VPC

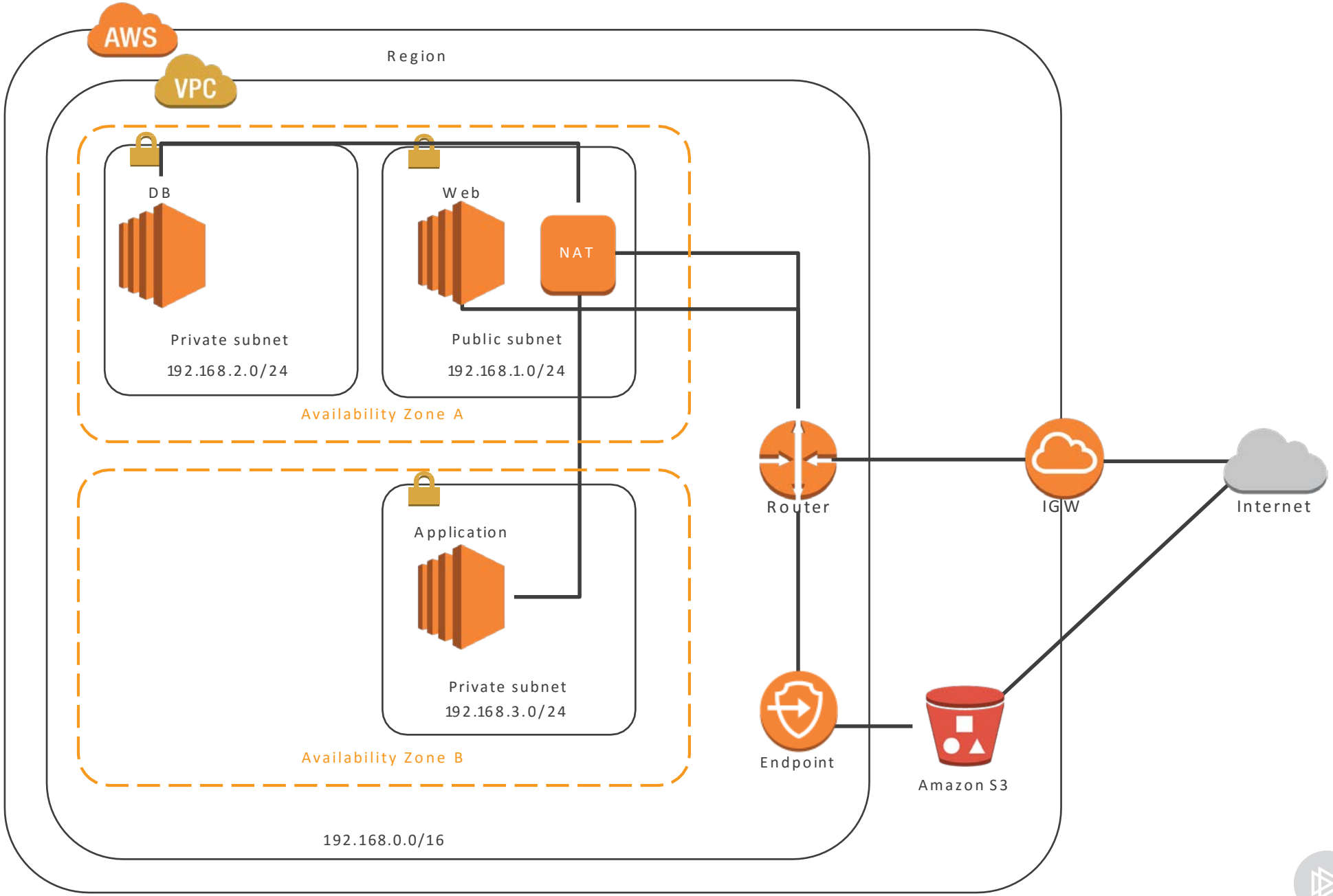


Demo



Configure Endpoint to Amazon S3

Wired Brain Coffee
VPC



Summary

NAT instances

NAT gateways

VPC endpoints