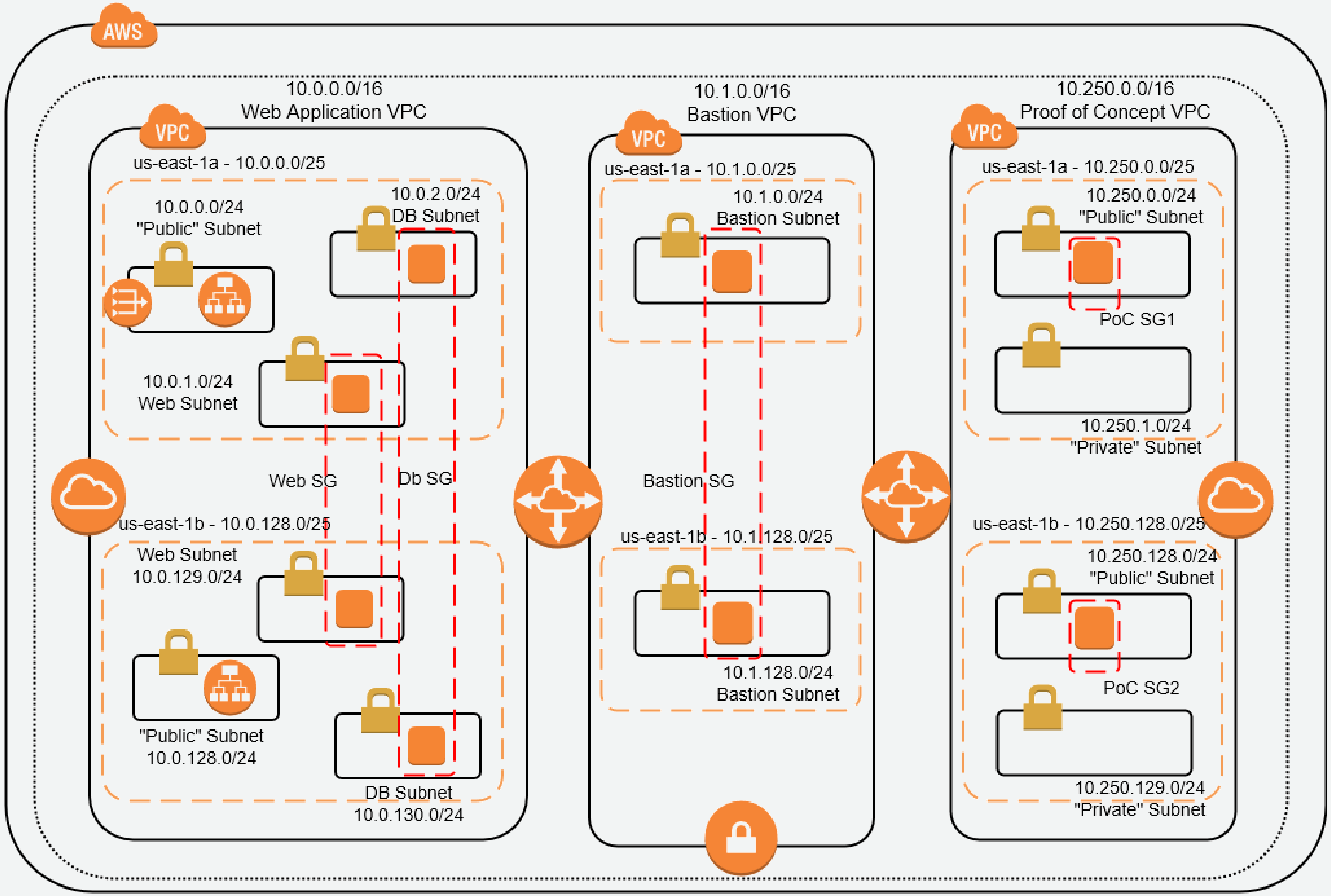
Network Reachability Demo Environment

Environmental Architecture



Routing Tables

Web App VPC Public Route Table

Destination	Target
10.0.0.0/16	Local
0.0.0.0/0	Internet Gateway
10.1.0.0/16	VPC Peer

Attached to: WebApp VPC
Public Subnets, Db Subnets

Web App VPC Private Route Table

Destination	Target
10.0.0.0/16	Local
0.0.0.0/0	NAT Gateway
10.1.0.0/16	VPC Peer

Attached to: WebApp VPC
Web Subnets

PoC Private Route Table

Destination	Target
10.250.0.0/16	Local
10.1.0.0/16	VPC Peer

Attached to: PoC VPC
Private Subnets

Bastion VPC Private Route Table

Destination	Target
10.1.0.0/16	Local
10.0.0.0/16	VPC Peer
192.168.0.0/16	Virtual Gateway

Attached to: Bastion VPC
Private Subnet

PoC Public Route Table

Destination	Target
10.250.0.0/16	Local
0.0.0.0/0	Internet Gateway
10.1.0.0/16	VPC Peer

Attached to: PoC VPC
Public Subnets

Security Groups

WebApp Load Balancer Security Group

Direction	Port/Protocol	Src/Dest
Inbound	80/TCP (HTTP)	0.0.0.0/0
Outbound	80/TCP (HTTP)	Web Server SG

WebApp Web Server Security Group

Direction	Port/Protocol	Src/Dest
Inbound	80/TCP (HTTP)	Load Balancers
Inbound	22/TCP (SSH)	10.1.00/16
Inbound	3389/TCP (RDP)	10.1.00/16
Outbound	All Traffic	All Traffic

WebApp Database Server Security Group

Direction	Port/Protocol	Src/Dest
Inbound	3306/TCP (MySql)	0.0.0.0/0
Inbound	22/TCP (SSH)	10.1.00/16
Inbound	3389/TCP (RDP)	10.1.00/16
Outbound	All Traffic	All Traffic

Bastion Server Security Group

Direction	Port/Protocol	Src/Dest
Inbound	22/TCP (SSH)	192.168.0.0/16
Inbound	3389/TCP (RDP)	192.168.0.0/16
Outbound	22/TCP (SSH)	10.0.0.0/16
Outbound	3389/TCP (RDP)	10.0.0.0/16

Security Groups

PoC Web Server AZ1 Security Group

Direction	Port/Protocol	Src/Dest
Inbound	80/TCP (HTTP)	0.0.0.0/0
Inbound	22/TCP (SSH)	10.1.00/16
Inbound	3389/TCP (RDP)	10.1.00/16
Outbound	All Traffic	All Traffic

PoC Web Server AZ2 Security Group

Direction	Port/Protocol	Src/Dest
Inbound	443/TCP (HTTPS)	0.0.0.0/0
Inbound	22/TCP (SSH)	0.0.0.0/0
Inbound	3389/TCP (RDP)	10.1.00/16
Outbound	All Traffic	All Traffic

IT and Security Assumptions

1. Instances in private subnets are not accessible from the internet
2. Putting servers in different Availability zones provide failover and better reliability
3. Nothing can route through the bastion VPC.
4. Access to the servers is limited by least privilege
5. The bastion hosts can access all environments

Question our Assumptions

Anything wrong with the Security Groups?

- Assuming a properly architected three-tier web application, do the Web or DB Subnets need to be open to the internet for the website to work?

No, they do not.

Anything wrong with the Security Groups?

- Then what does a properly secured solution look like from a data flow perspective? What subnets or instances need to be public?

Public	Private	SSH
Load Balancers	Everything Else	Only the Bastion Hosts

Anything wrong with the Security Groups?

- Can the Bastion servers be referenced by Security Group, or just IP address range?

With VPC Peering, SG's can be referenced across VPC's

Anything wrong with the Security Groups?

- How do we use Ingress and Egress Security Group rules in Security Groups to control Bastion Host access?

Ingress	Egress
From on-premises IP’s over ports 22/3389	Only to approved Security Groups

Failover

- Will failover work right for the Web App? What about the Proof of Concept?

WebApp	Proof of Concept
Routing Table, NACL's, and SG's look good But a Single NAT Gateway is not ideal	Too many Security Groups No consistency among rules

Transitive Routing

- But if the WebApp VPC and Proof of Concept VPC are both connected to the Bastion VPC, can’t they talk to each other too?

Nope

Least Privilege

- What are the best ways to accomplish and validate least privilege data flow? Can we use automated checks to validate this instead of doing it manually?

The Amazon Inspector Network Reachability Report

Least Privilege

- What about when someone changes something? Is connectivity built automatically?

Depends on the configuration, but when done right, No.

Back to the Demo