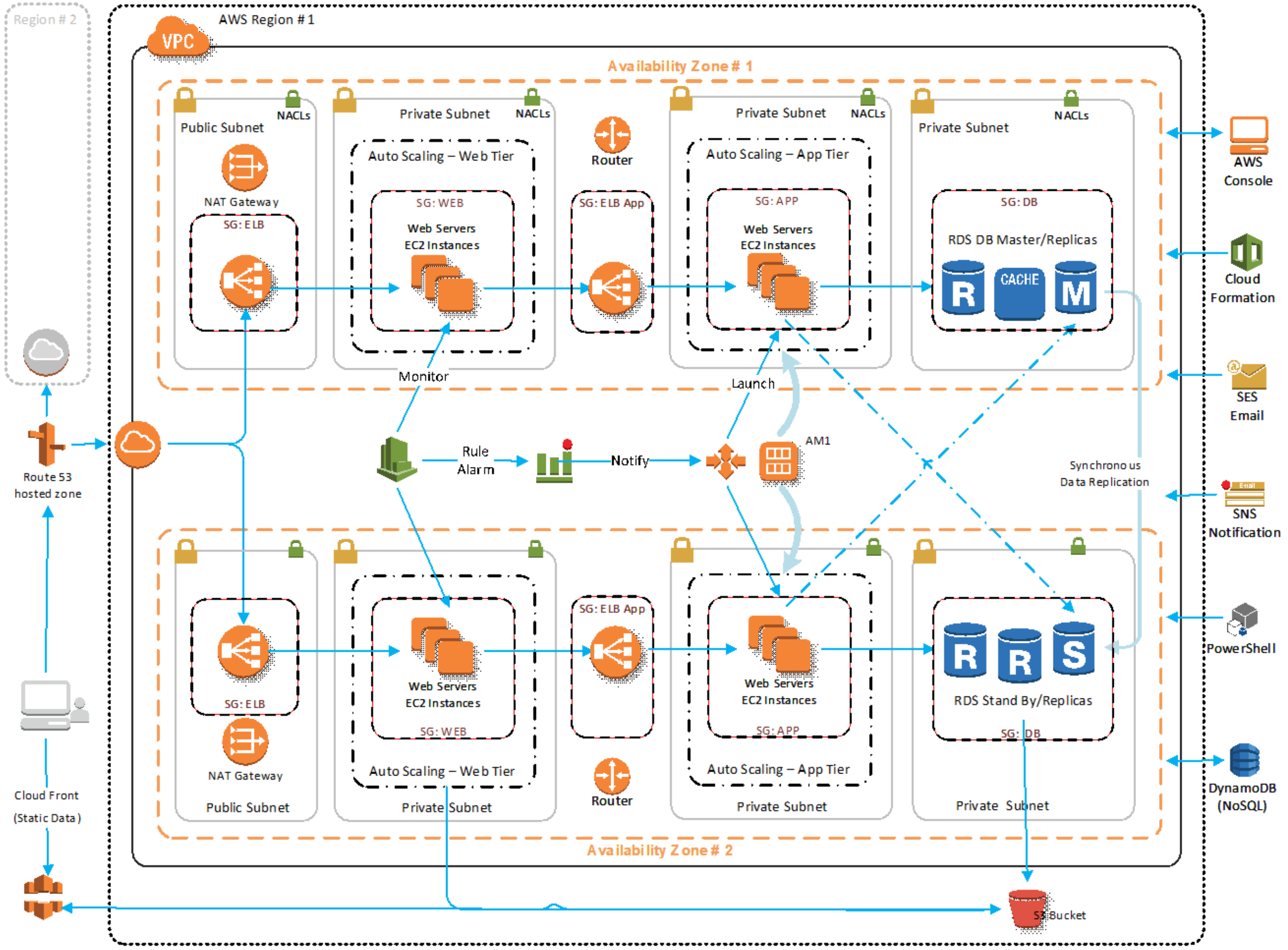
Project Security design consideration

- Region/Availability Zones High Availability (Active/Active, Active/standby or multi-region active)
- Edge router iBGP/eBGP failover design
- GSLB configuration for Zones HA
- service failover for web zone, app zone, and DB zone(clustering)
- Traffic segregation (web/app/DB) and subnet design
- security route table design
- VPC security group and rules design
- load balancing and NAT GW design
- DB tier data sync/replication
- SSL offloader/CA/ certificate manager
- application layer security (XML, HTTPS head/URL filter/read write access permit, etc)
- transit gateway for VPN/VPLS/direct access (routing table, security ACL rules)
- branch (site to site) VPN/VPLS/ remote access design
- user group and members roles, access
- remote monitoring, alerting and change management

High Level Security design for NBS internet trading migration project)



Low Level Security design 1

Web Zone Subnet routing table for Zone A

Destination	Target
10.0.0.0/16	VPC-ID-AZ-A
0.0.0.0/0	IGW-ID

Web Zone security group ACL rules

Source	Destination	TCP
0.0.0.0/0	Web VIP 10.0.0.1/32	443

App Zone Subnet routing table for Zone A

Destination	Target
10.0.0.0/16	VPC-ID-AZ-A
10.1.0.0/16	VPC-ID-AZ-B

APP Zone security group Ingress ACL rules

Intern Zone A traffic Source	Destination	TCP
10.0.0.0/24	APP_VIP1 10.0.1.1/32	8001
10.0.0.0/24	APP_VIP2 10.0.1.2/32	8002
10.0.0.0/24	APP_VIP3 10.0.1.3/32	8003

APP Zone Security Egress ACL rules
Intra Zone A-B traffic Source Destination TCP
10.0.1.0/24 Zone B DB 10.1.2.0/24 3306

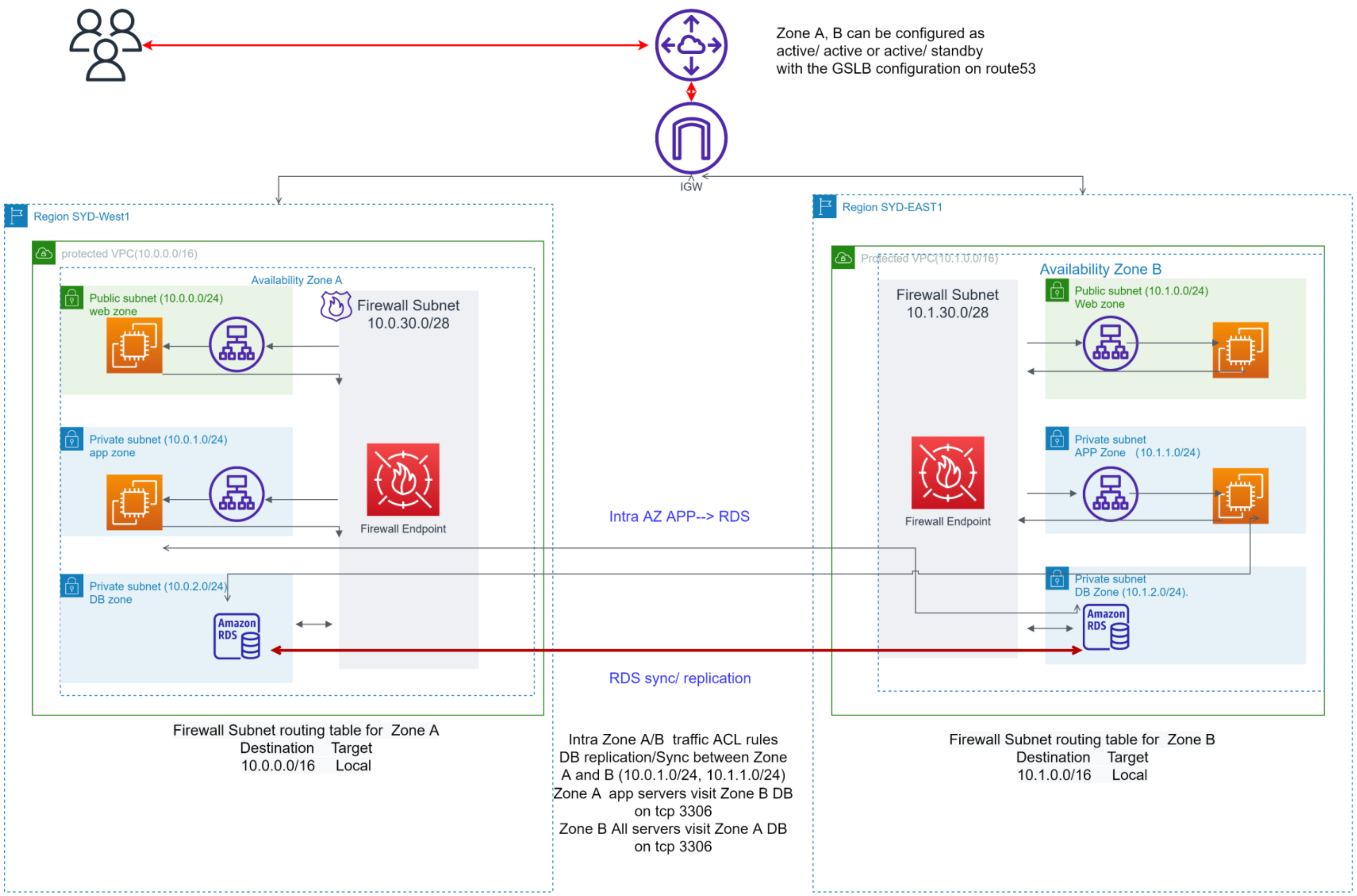
DB Zone Subnet routing table for Zone A

Destination	Target
10.0.0.0/16	VPC-ID-AZ-A
10.1.1.0/24	VPC-ID-AZ-B

DB Zone security group ingress ACL rules

Source	Destination	TCP
10.0.1.0/24	DB_VIP1 10.0.2.1/32	3306
10.1.1.0/24	DB_VIP 1 10.0.2.1/32	3306

DB Zone security Egress ACL rules
Intra Zone A-B DB Sync/Replication TCP
10.0.2.0/24 10.1.2.0/24 3307



Zone A, B can be configured as
active/ active or active/ standby
with the GSLB configuration on route53

Firewall Subnet routing table for Zone A

Destination	Target
10.0.0.0/16	Local

Intra Zone A/B traffic ACL rules
DB replication/Sync between Zone A and B (10.0.1.0/24, 10.1.1.0/24)
Zone A app servers visit Zone B DB on tcp 3306
Zone B All servers visit Zone A DB on tcp 3306

Firewall Subnet routing table for Zone B

Destination	Target
10.1.0.0/16	Local

Web Zone Subnet routing table for Zone B

Destination	Target
10.1.0.0/16	VPC-ID-AZ-B
0.0.0.0/0	IGW-ID

Web Zone security group ACL rules

Source	Destination	TCP
0.0.0.0/0	Web VIP 10.1.0.1/32	443

App Zone Subnet routing table for Zone A

Destination	Target
10.0.0.0/16	VPC-ID-AZ-A
10.1.0.0/24	VPC-ID-AZ-B

APP Zone security group inbound ACL rules

Source	Destination	TCP
10.1.0.0/24	APP_VIP1 10.1.1.1/32	8001
10.1.0.0/24	APP_VIP2 10.1.1.2/32	8002
10.1.0.0/24	APP_VIP3 10.1.1.3/32	8003

outbound ACL rules
intra Zone A-B traffic Source Destination TCP
10.1.1.0/24 Zone A DB 10.0.2.0/24 3306

DB Zone Subnet routing table for Zone A

Destination	Target
10.1.0.0/16	VPC-ID-AZ-B
10.0.1.0/24	VPC-ID-AZ-A

DB Zone security group ACL rules

Source	Destination	TCP
10.1.1.0/24	DB_VIP1 10.1.2.1/32	3306
10.0.1.0/24	DB_VIP1 10.1.2.1/32	3306

DB Zone security Egress ACL rules
Intra Zone A-B DB Sync/Replication TCP
10.1.2.0/24 10.0.2.0/24 3307