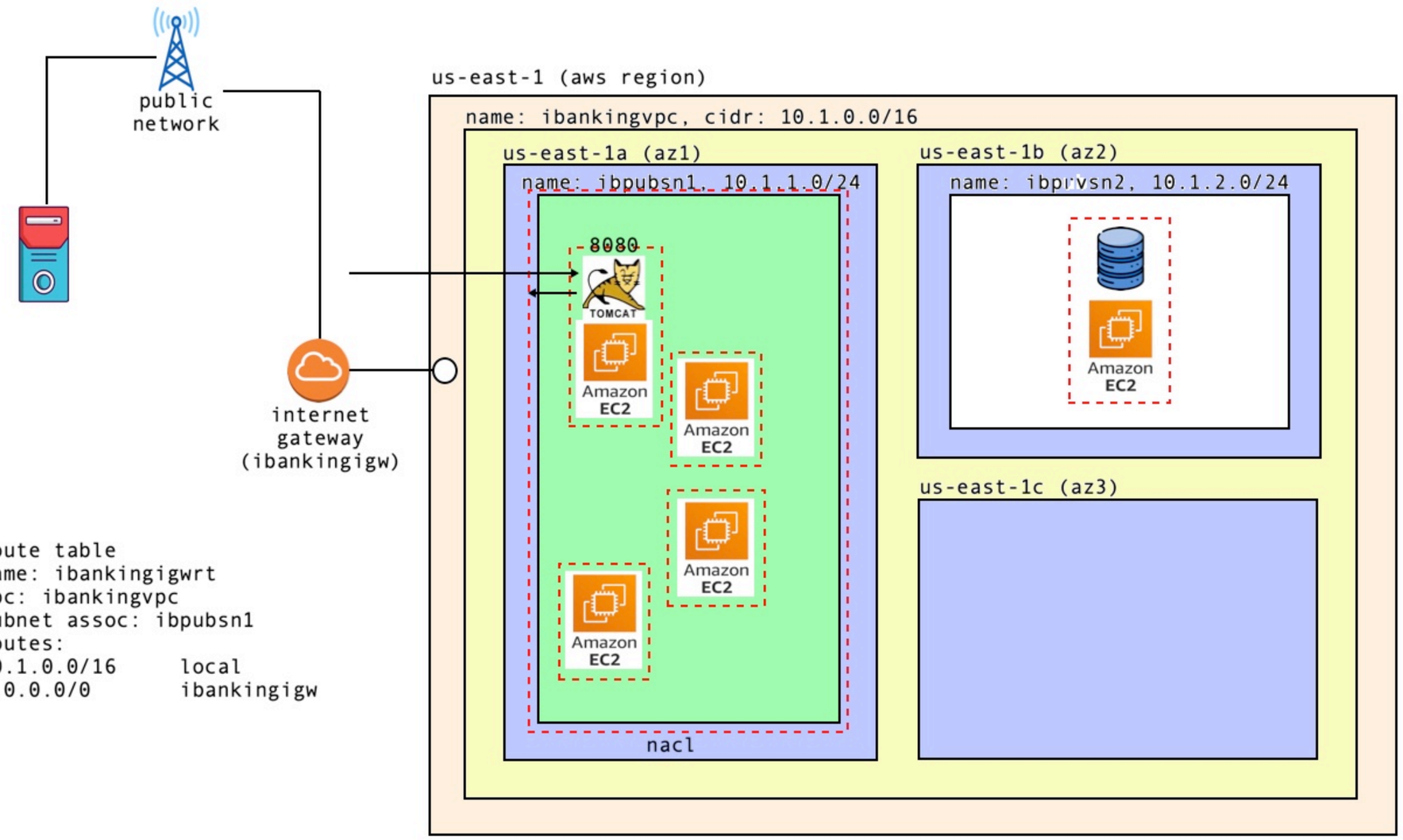

database:
1. database should be accessible from the sn1 only

2. database should be accessible within the vpc network only

application:
1. app ec2 instance to be ssh from anywhere

2. tomcat (8080) should be accessible from anywhere

Route table
name: ibankingigwrt
vpc: ibankingvpc
subnet assoc: ibpubsn1
routes:

10.1.0.0/16	local
0.0.0.0/0	ibankingigw

diff traffic restrictions
- #3 security groups (2 restrictions)

few restrictions seems to be common across all the ec2's
and few are different from one to another

#1. nacl rules are stateles
stateless means request and response are treated separately. So we need to always define #2 rules allowing inbound and outbound traffic irrespective of how the traffic is being generated.
#2. nacl rules are ordered, each rule is assigned with rule# and is applied in that order of definition
#3 default nacl rule is allow all inbound/outbound network traffic without any restriction

Nacl rules

Inbound

rule#	protocol	source_cidr	port	action
100	ssh	anywhere	22	allow
101	customTcp	anywhere	8080	allow
*	all	anywhere	any	deny

Outbound

rule#	protocol	source_cidr	port	action
*	all	anywhere	any	allow