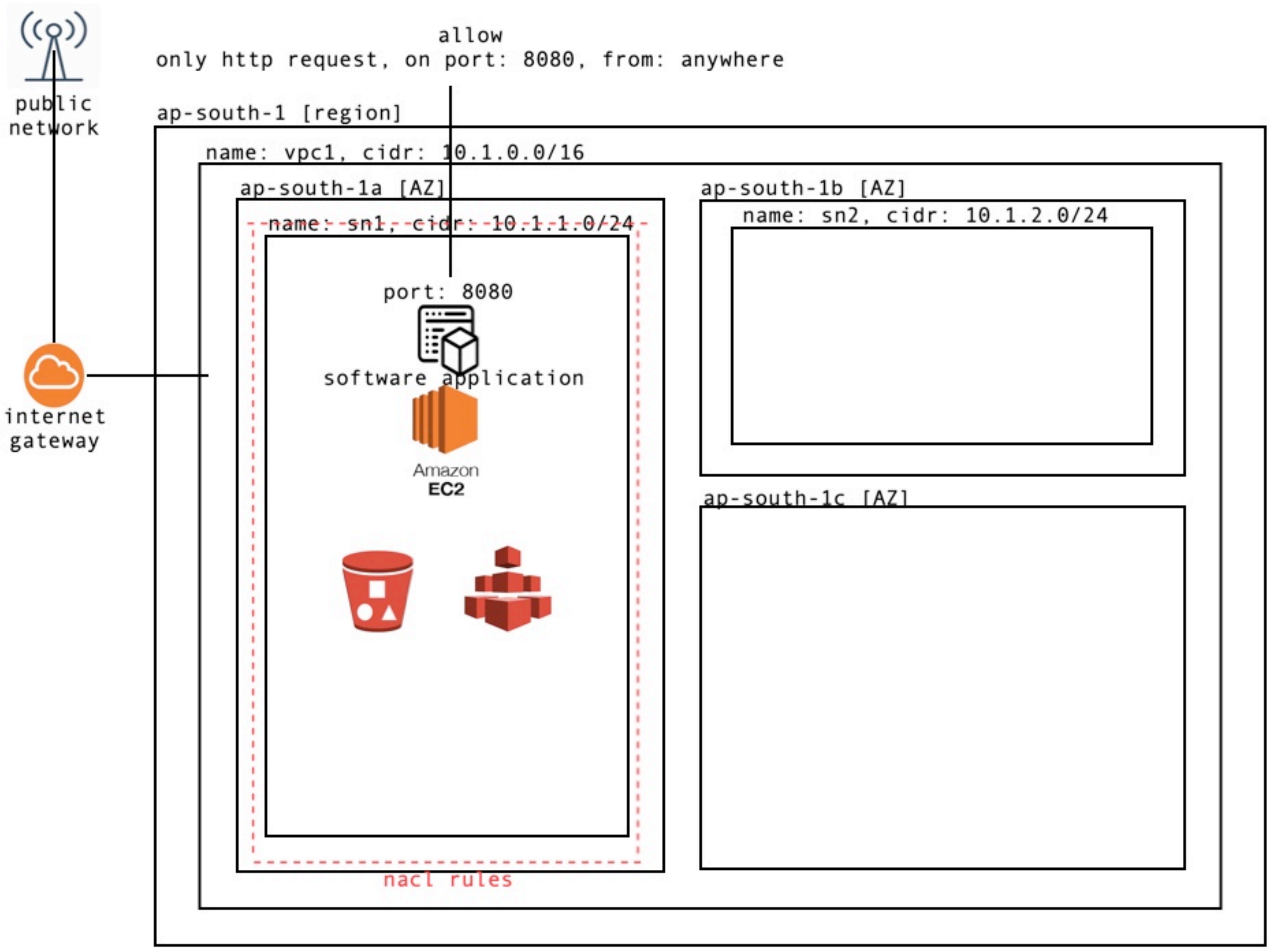

routetable: vpc1igwrt
subnet association: sn1

cidr	target
10.1.0.0/16	local
0.0.0.0/0	igw

nacl rules is an firewall configured around the subnet level, enforcing the traffic restrictions on the group of resources within an subnet

1. by default per each vpc & subnet the aws cloud platform creates an nacl rules

2. using the nacl rules we enforce traffic restrictions allowing/denying the network traffic to the subnet of resources based on
2.1 source cidr
2.2 protocol
2.3 portno

source cidr	protocol	port	action
0.0.0.0/0	ssh	22	allow

3. nacl rules are stateless
it means the request and the response is treated differently
so to allow network traffic from both the directions we need to configure 2 nac rules
3.1 ingress rules
for enforcing the network traffic towards the subnet of resources

3.2 egress rules
to enforce network traffic from the subnet resources towards the external network

4. These rules are ordered and applied in the sequence order we specified.

5. The default nacl rules applied to the subnet of resources are:
1. deny all the in-bound network traffic
2. allow all the outbound network traffic from subnet of resources to the external network

ingress rule

rule#	source cidr	protocol	action
1000	0.0.0.0/0	*	deny

egress rule

rule#	source cidr	protocol	action
1000	0.0.0.0/0	*	allow