High-Level Details:

GET Inc., deployed a simple web application in AWS that contains:

- Web Server
- REST API Server (Talks to MySQL DB)
- MySQL Database

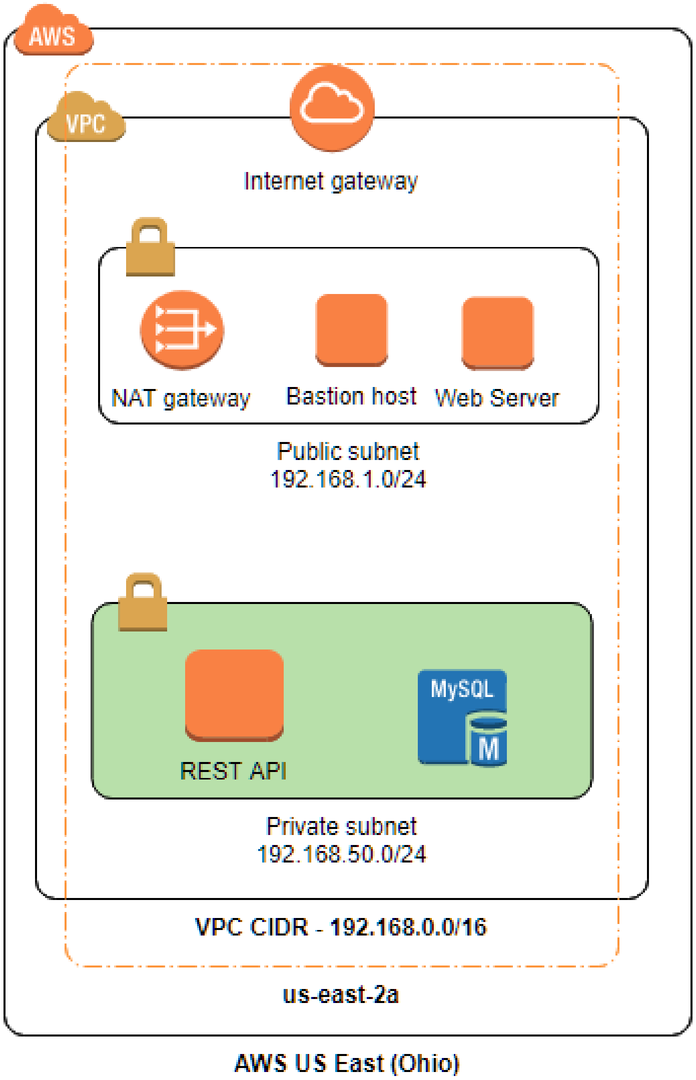
They deployed a Bastion Host and a NAT Gateway for security reasons. However, the setup is not working as expected. For example, SSH to MySQL Server from the Bastion host is not working.

The end-users use the HTTPS URL to access the web application. The web application communicates with the REST API server, which has business logic. The REST API server interacts with the MySQL server for database operations.

All EC2 instances should be able to access the internet (Ex: download OS patches). All inbound connections to the EC2 instances in the private subnets must be blocked. However, the EC2 instances in the private subnet should be able to communicate with internet resources.

EC2 Instance	TCP Ports	Comments
Bastion Host	22 for SSH	Admins should be able to SSH from the internet. However, it would nice to restrict access from one pre-determined public IP address.
Web Server	22 for SSH 443 for HTTPS	Admins should be able to SSH into the webserver from public subnet only. For security reasons, direct SSH access is not allowed from the internet.
Rest API	22 for SSH 443 for HTTPS	Admins should be able to SSH into the REST API server from the public subnet only. For security reasons, direct SSH access is not allowed from the internet. Only Web Server should be able to make REST API calls.
MySQL	22 for SSH 3306 for MySQL	Admins should be able to SSH into the MySQL server from the public subnet only. For security reasons, direct SSH access is not allowed from the internet. Only REST API Server should be able to communicate with the MySQL Server.

Architecture Diagram:



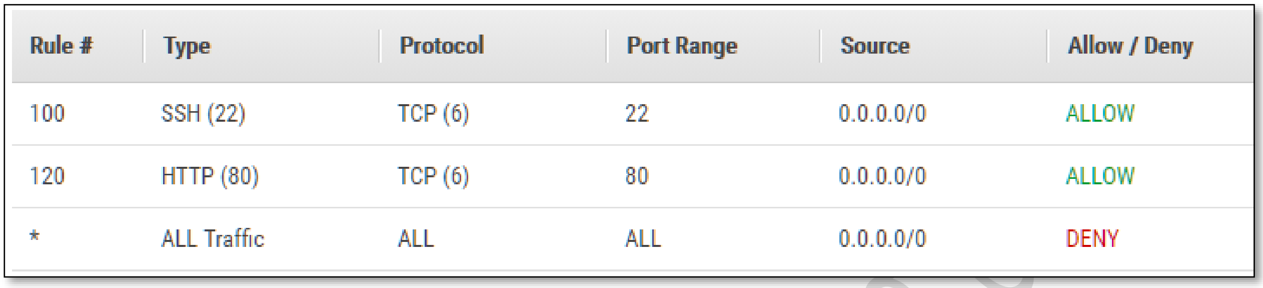
NACLs and Security Groups:

NACLs	Comments
NACL_Public_Subnet	NACL associated with the public subnet.
NACL_Private_Subnet	NACL associated with the private subnet.

Network ACLs

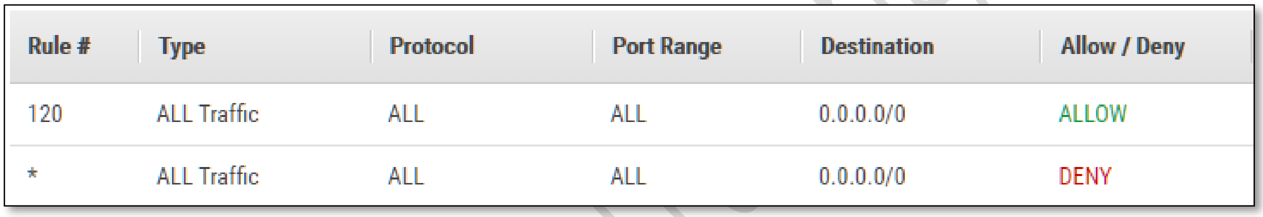
NACL_Public_Subnet

Inbound Rules



Rule #	Type	Protocol	Port Range	Source	Allow / Deny
100	SSH (22)	TCP (6)	22	0.0.0.0/0	ALLOW
120	HTTP (80)	TCP (6)	80	0.0.0.0/0	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

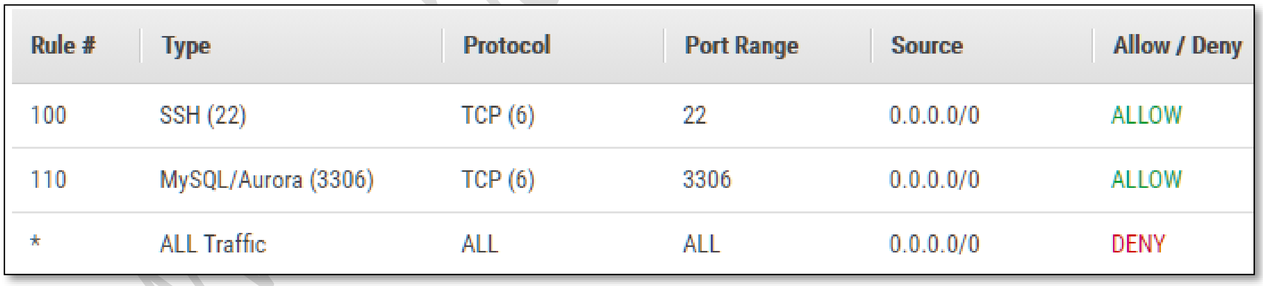
Outbound Rules



Rule #	Type	Protocol	Port Range	Destination	Allow / Deny
120	ALL Traffic	ALL	ALL	0.0.0.0/0	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

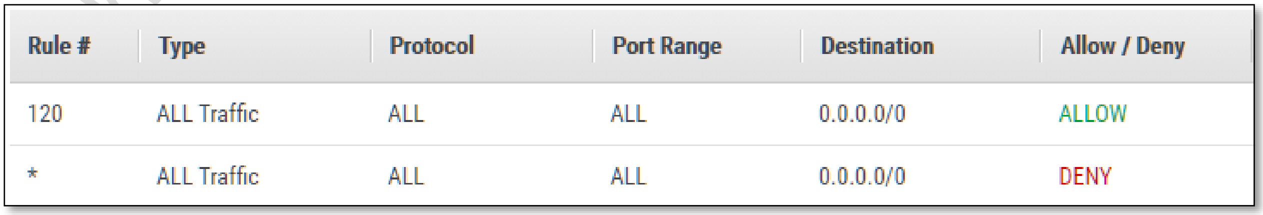
NACL_Private_Subnet

Inbound Rules



Rule #	Type	Protocol	Port Range	Source	Allow / Deny
100	SSH (22)	TCP (6)	22	0.0.0.0/0	ALLOW
110	MySQL/Aurora (3306)	TCP (6)	3306	0.0.0.0/0	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

Outbound Rules



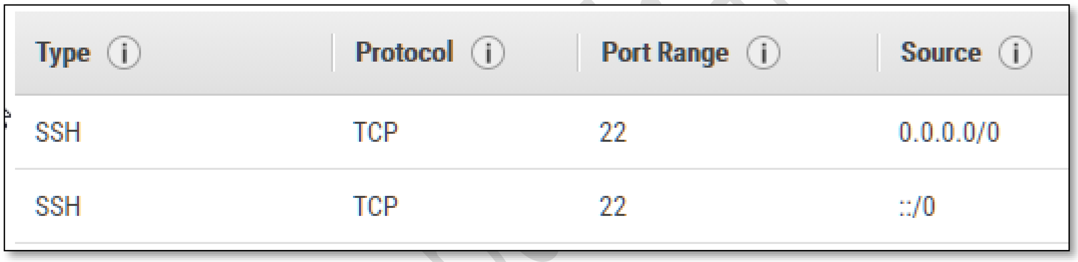
Rule #	Type	Protocol	Port Range	Destination	Allow / Deny
120	ALL Traffic	ALL	ALL	0.0.0.0/0	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

Security Groups

Security Groups	Comments
SG_Bastion	Security Group associated with the Bastion Host.
SG_Web	Security Group associated with the Web Server.
SG_RestApi	Security Group associated with the REST API EC2 instance.
SG_MySQL	Security Group associated with the MySQL Instance.

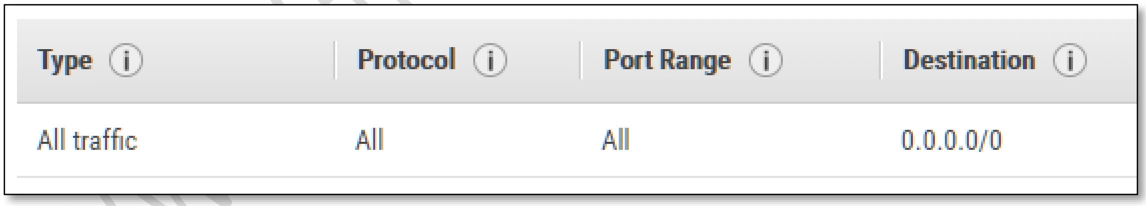
SG_Bastion

Inbound Rules



Type	Protocol	Port Range	Source
SSH	TCP	22	0.0.0.0/0
SSH	TCP	22	::/0

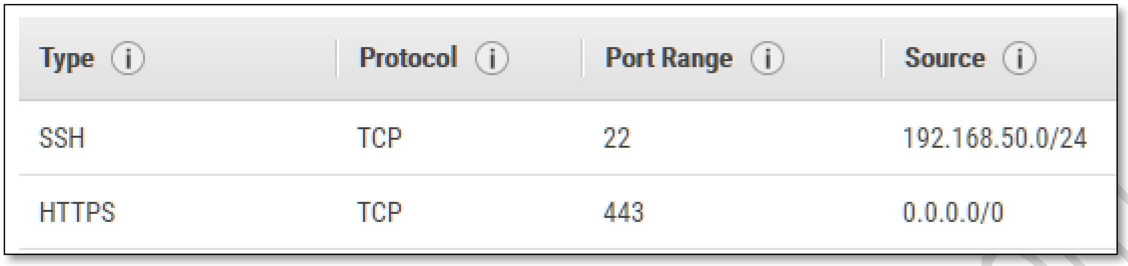
Outbound Rules



Type	Protocol	Port Range	Destination
All traffic	All	All	0.0.0.0/0

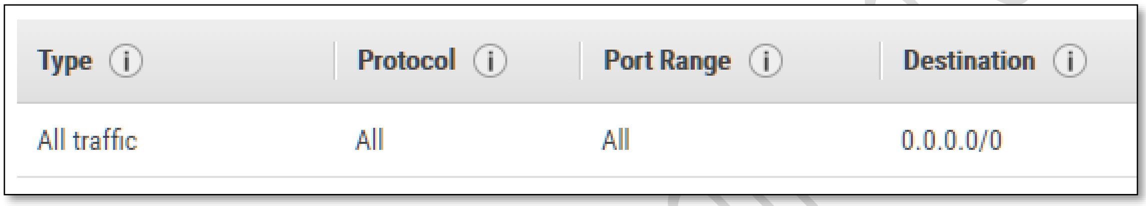
SG_Web

Inbound Rules



Type	Protocol	Port Range	Source
SSH	TCP	22	192.168.50.0/24
HTTPS	TCP	443	0.0.0.0/0

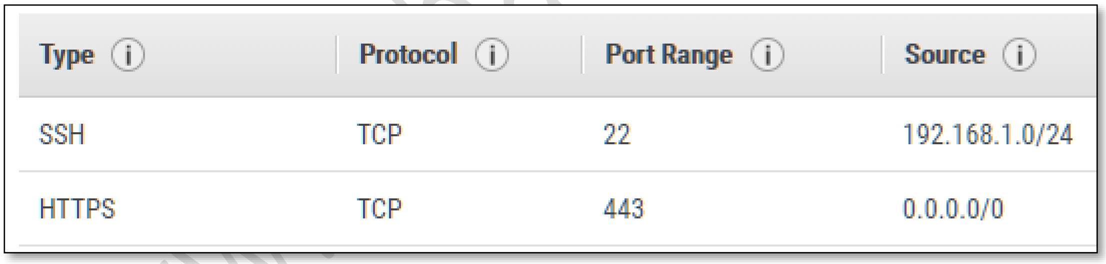
Outbound Rules



Type	Protocol	Port Range	Destination
All traffic	All	All	0.0.0.0/0

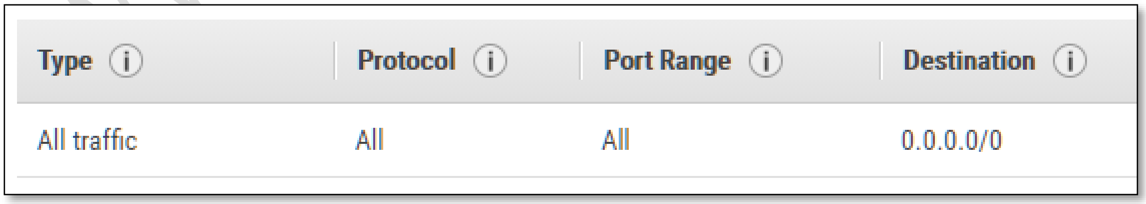
SG_RestApi

Inbound Rules



Type	Protocol	Port Range	Source
SSH	TCP	22	192.168.1.0/24
HTTPS	TCP	443	0.0.0.0/0

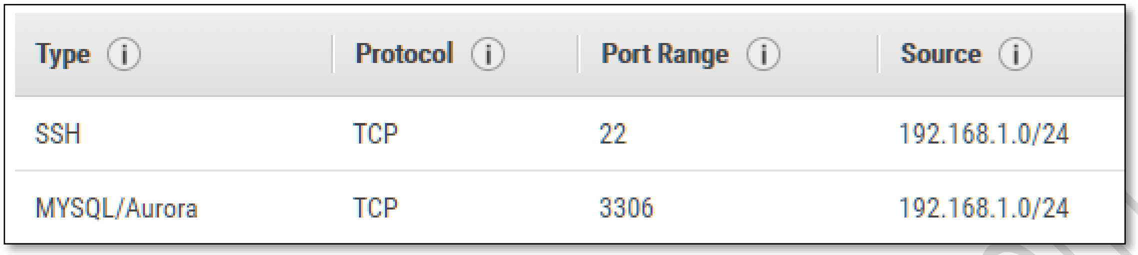
Outbound Rules



Type	Protocol	Port Range	Destination
All traffic	All	All	0.0.0.0/0

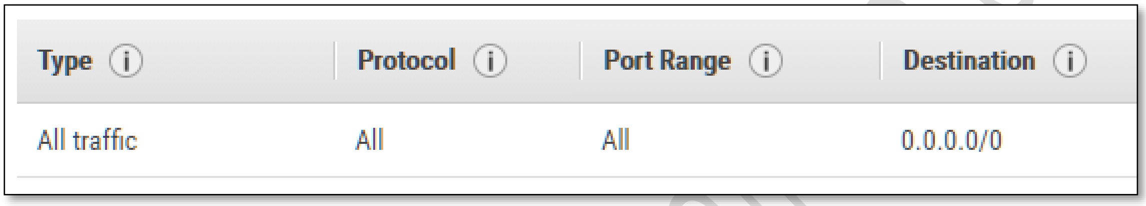
SG_MySQL

Inbound Rules



Type	Protocol	Port Range	Source
SSH	TCP	22	192.168.1.0/24
MYSQL/Aurora	TCP	3306	192.168.1.0/24

Outbound Rules

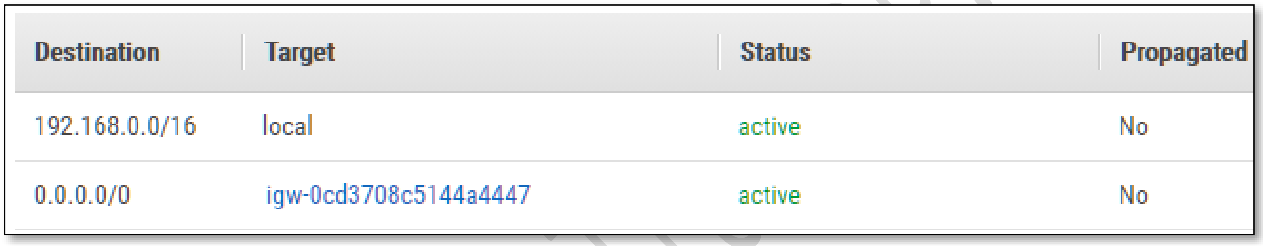


Type	Protocol	Port Range	Destination
All traffic	All	All	0.0.0.0/0

Route Tables:

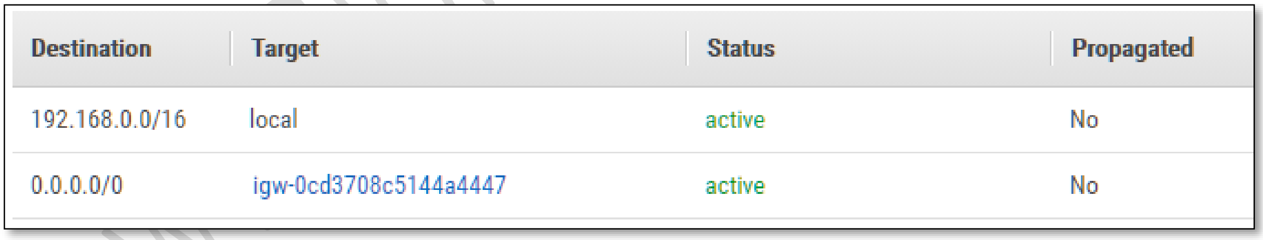
Route Table	**Comments**
RT_Public	Route Table associated with the Public Subnet.
RT_Private	Route Table associated with the Private Subnet.

RT_Public



Destination	Target	Status	Propagated
192.168.0.0/16	local	active	No
0.0.0.0/0	igw-0cd3708c5144a4447	active	No

RT_Private



Destination	Target	Status	Propagated
192.168.0.0/16	local	active	No
0.0.0.0/0	igw-0cd3708c5144a4447	active	No

Goals:

- Review the application requirements, existing architecture (diagram), NACLs, Security Groups, and Route Tables.
- Modify/Edit VPC components to meet business requirements.