**Private Subnet**

**Outbound**

Rule

Type

Protocol

Port Range

Destination

Allow/Deny

100

Custom TCP Rule

TCP (6)

80

10.14.0.0/24

ALLOW

101

Custom TCP Rule

TCP (6)

1024 - 65535

0.0.0.0/0

ALLOW

**100 - Connects to the App to get DB changes**

**101 - Sends out the request for updates to the DB**

**Inbound**

Rule

Type

Protocol

Port Range

Source

Allow/Deny

100

Custom TCP Rule

TCP (6)

1024 - 65535

0.0.0.0/0

ALLOW

101

Custom TCP Rule

TCP (6)

27017

10.14.0.0/24

ALLOW

102

SSH (22)

TCP (6)

22

10.14.0.0/24

ALLOW

**100 - Allows the DB to update**

**101 - Allows the app to communicate with the DB**

**102 - Allows the SSH protocol to connect with the DB**

Security Group

Applied on the instance (Virtual Machine). Virtual firewall for inbound and outbound traffic. Each instance in the subnet can be associated with a security group.

Bastion Host

A Virtual Machine. Specially designed and configured to withstand attack. Stays in the public subnet.

Need to open SSH, but need to open to whole world.

Bastion Host replaces SSH NACL Rule

Spin up Bastion Host in public subnet — very hardened.

Give the Bastion Host connection to MongoDB and ssh.

Bastion Host has all extras removed.