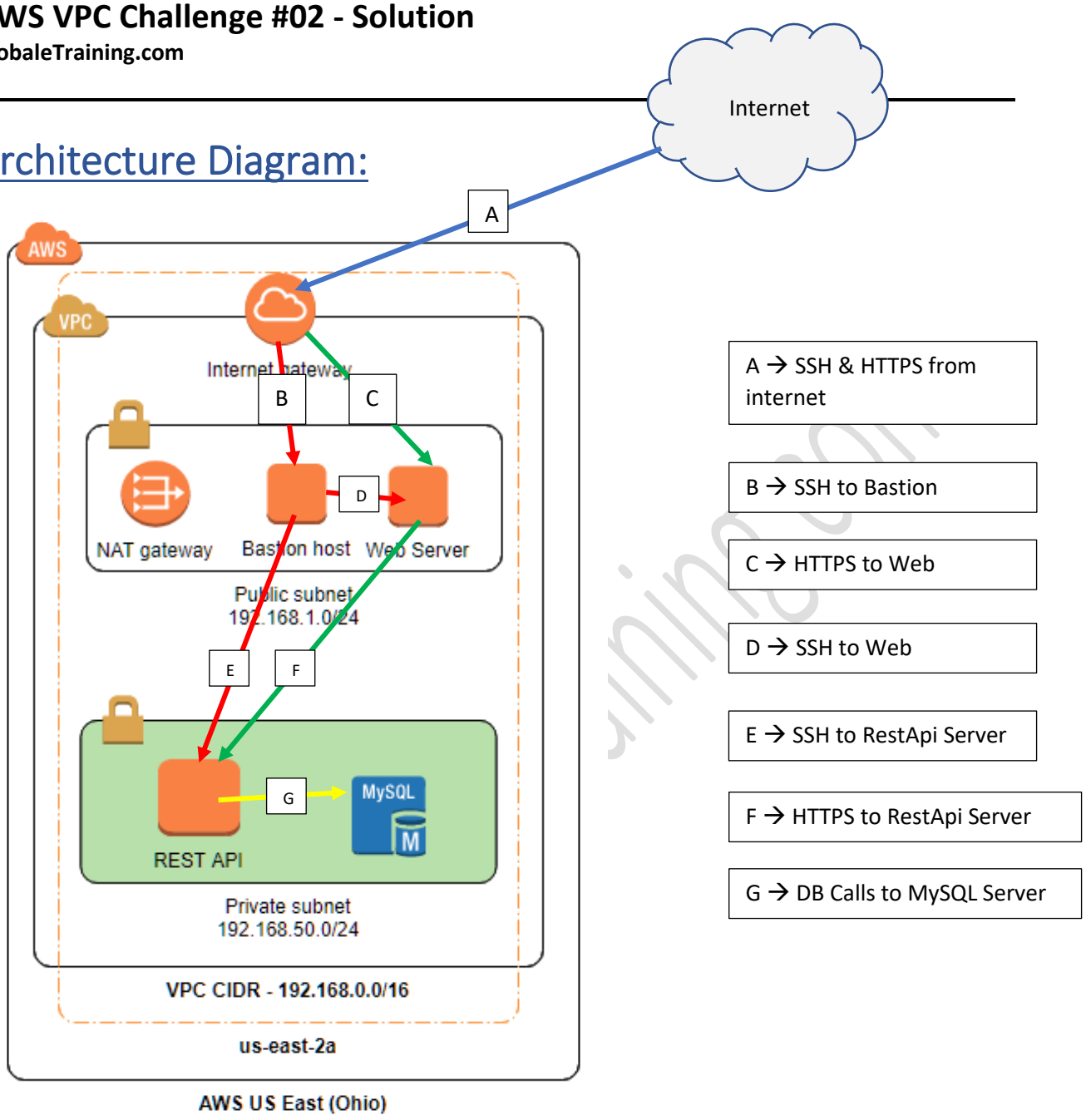
High-Level Details:

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 – Updated!

NACL_Public_Subnet

Inbound Rules - Old

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

Inbound Rules - Updated!

Rule #	Type	Protocol	Port Range	Source	Allow / Deny
100	SSH (22)	TCP (6)	22	64.65.62.32/32	ALLOW
120	HTTPS (443)	TCP (6)	443	0.0.0.0/0	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

Rule 100 → Allows SSH from 64.65.62.32 IP only. IP address was randomly picked for this scenario.
Rule 120 → Changed the port from 80 to 443. 443 is the default HTTPS port.

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 - Old

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

Inbound Rules - Updated!

Rule #	Type	Protocol	Port Range	Source	Allow / Deny
100	SSH (22)	TCP (6)	22	192.168.1.0/24	ALLOW
110	HTTPS (443)	TCP (6)	443	192.168.1.0/24	ALLOW
*	ALL Traffic	ALL	ALL	0.0.0.0/0	DENY

Time To Think:
Why were the updates made?

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 - Old

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

Inbound Rules - Updated!

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

- We updated the Source for the SSH rule to 192.168.1.0/24. It would allow any EC2 instance with-in the public subnet to SSH into the webserver.
- If an admin tries to SSH into the webserver using the Web Server' public IP address, it would be blocked. Admin must SSH into the Bastion host first, and then SSH into the webserver.

Outbound Rules

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

SG_RestApi

Inbound Rules - Old

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

Inbound Rules - Updated!

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

- The update to the HTTPS rule allows only the EC2 instances in the public subnet to make REST API calls.

Outbound Rules

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

SG_MySQL

Inbound Rules - Old

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

Inbound Rules - Updated!

Type	Protocol	Port Range	Source
SSH	TCP	22	192.168.1.0/24
MYSQL/Aurora	TCP	3306	192.168.50.0/24

- The update to the MYSQL/AURORA rule allows only the EC2 instances in the private subnet to communicate with the MySQL server, which is also in the same private subnet.
- You can further restrict by using the REST API server IP in the source field.

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

Inbound Rules - Updated!

Destination	Target	Status	Propagated
192.168.0.0/16	local	active	No
0.0.0.0/0	nat-0fe4b4626fe5aa282	active	No

The target for 0.0.0.0/0 must be a NAT Gateway.