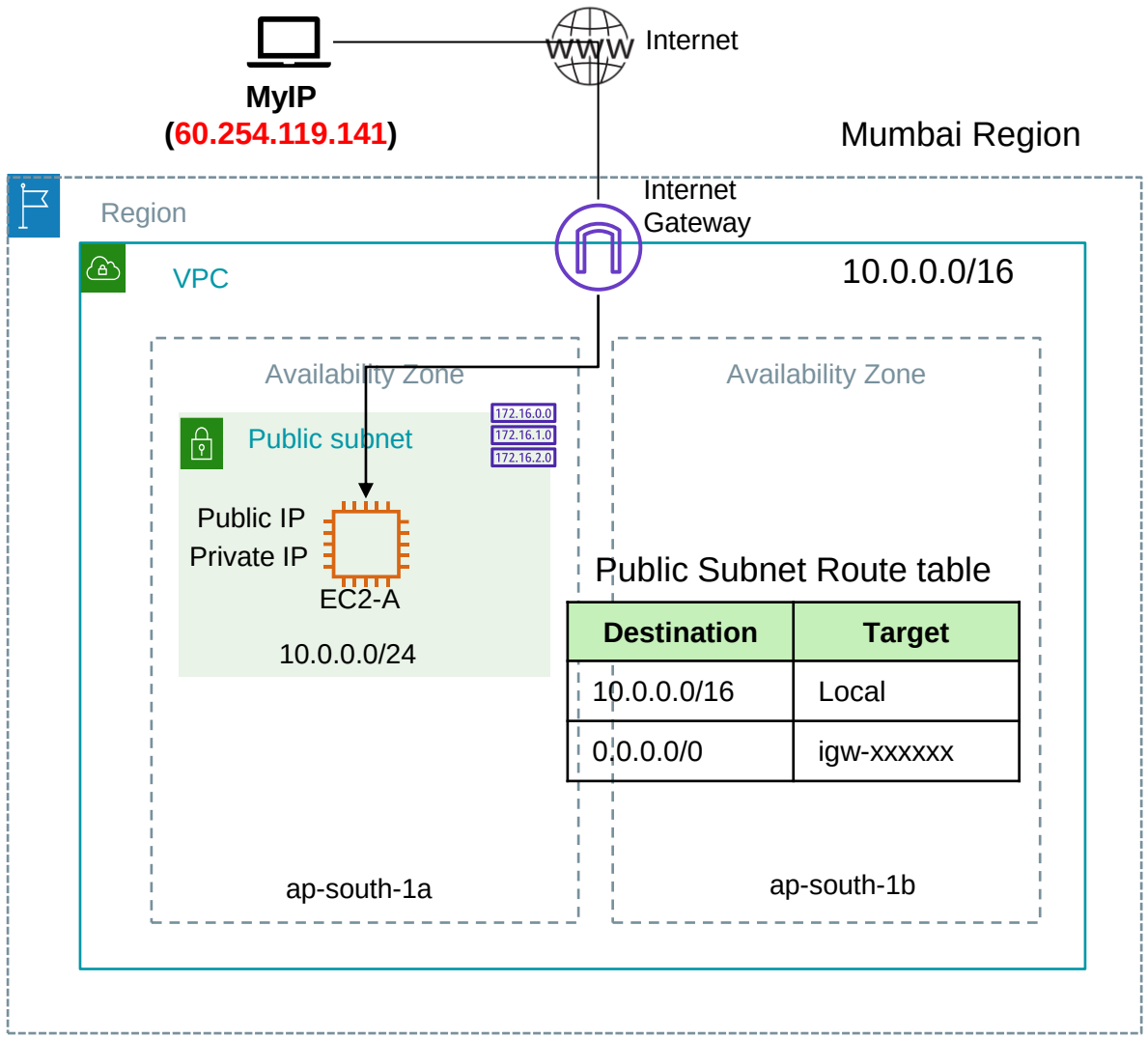
Assignment – Network ACL

Assignment – How NACL works by trying out different NACL rules



High level steps

1. Create a VPC with Public Subnet, configure route table accordingly
2. Launch EC2 instance and assign Public IP. Allow SSH and HTTP in security group.
3. Connect to instance over SSH and install a httpd web server. Refer to the commands on the next page for installing a webserver.
4. Verify that you can access web page over the internet using EC2 Elastic IP
5. Modify the Subnet NACL rules as given in the following slide and observe the behavior

Web server installation steps

- Connect to EC2 instance over SSH and execute following commands:
  - sudo yum install httpd -y
  - sudo systemctl start httpd.service
  - sudo systemctl enable httpd.service
- Create /var/www/html/index.html and add some text e.g. <h1>This is a webserver</h1>
- Save the file

Vi commands to edit the file:

- sudo vi /var/www/html/index.html
- Press i (This takes you in the edit mode) -> Write the html text
- Press ESC (This takes you out of the edit mode)
- :wq

Try following scenarios for Subnet NACL:

Modify NACL rules in the following order and then try to connect to the webserver over HTTP (port 80) from the browser. Check if you see the same as following behavior when you try to connect to the webserver after every step.

1. Remove the default inbound Allow rule -> Does not connect
2. Add default inbound Allow rule back and remove the default outbound Allow rule -> Does not connect
3. Add default outbound Allow rule back -> Connects
4. Remove default inbound Allow rule and instead add a new Inbound rule to allow only MyIP (your local IP/32) -> Connects
5. Remove default outbound Allow rule and instead add a new Outbound rule to allow destination as MyIP (your local IP/32) on port 80 -> Does not connect
6. Update the above rule port range from 80 to 1024-65535 -> Connects
7. Set NACL back to original i.e. default inbound and default outbound rules
8. In the inbound rules add a new rule (#200) after default Allow rule to block the traffic on port 80 from MyIP (your local IP/32) -> Connects but why?
9. Now change the Inbound rule numbers where above rule number (#) is lower than default Allow rule (#100) -> Does not connect