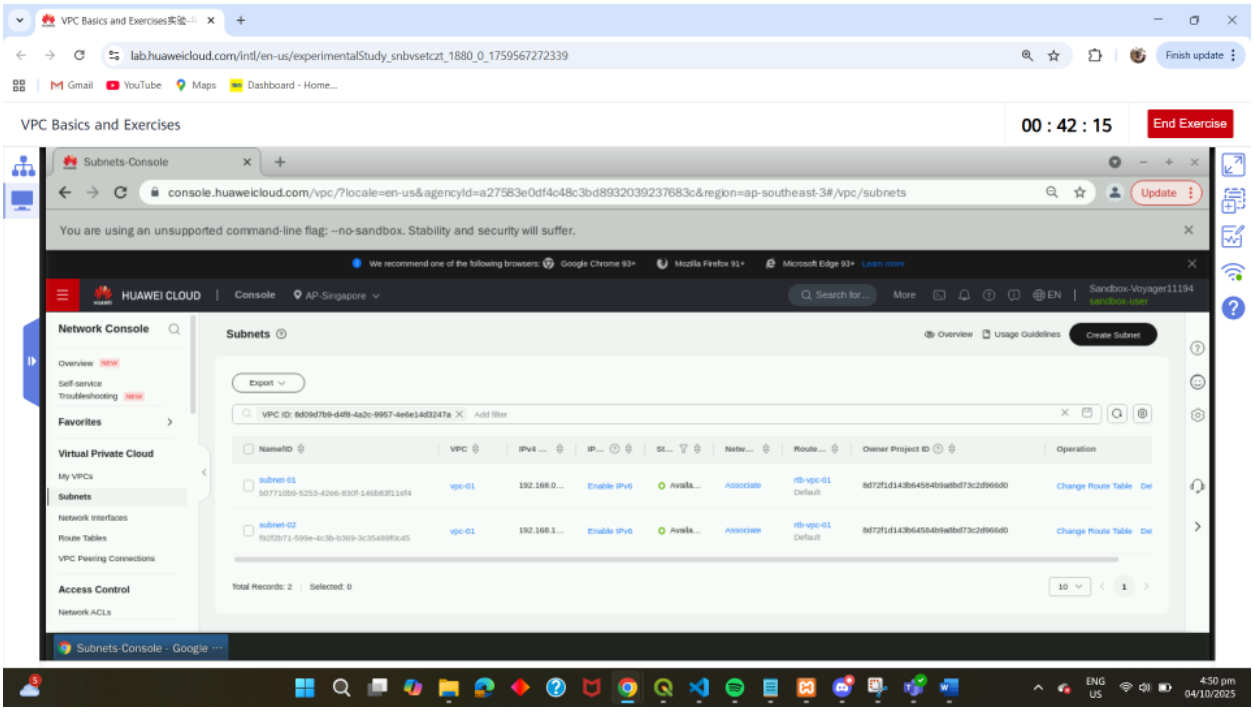
Miriam L. Vega
BSIT – 4C

04 Performance Task 1 – ARG

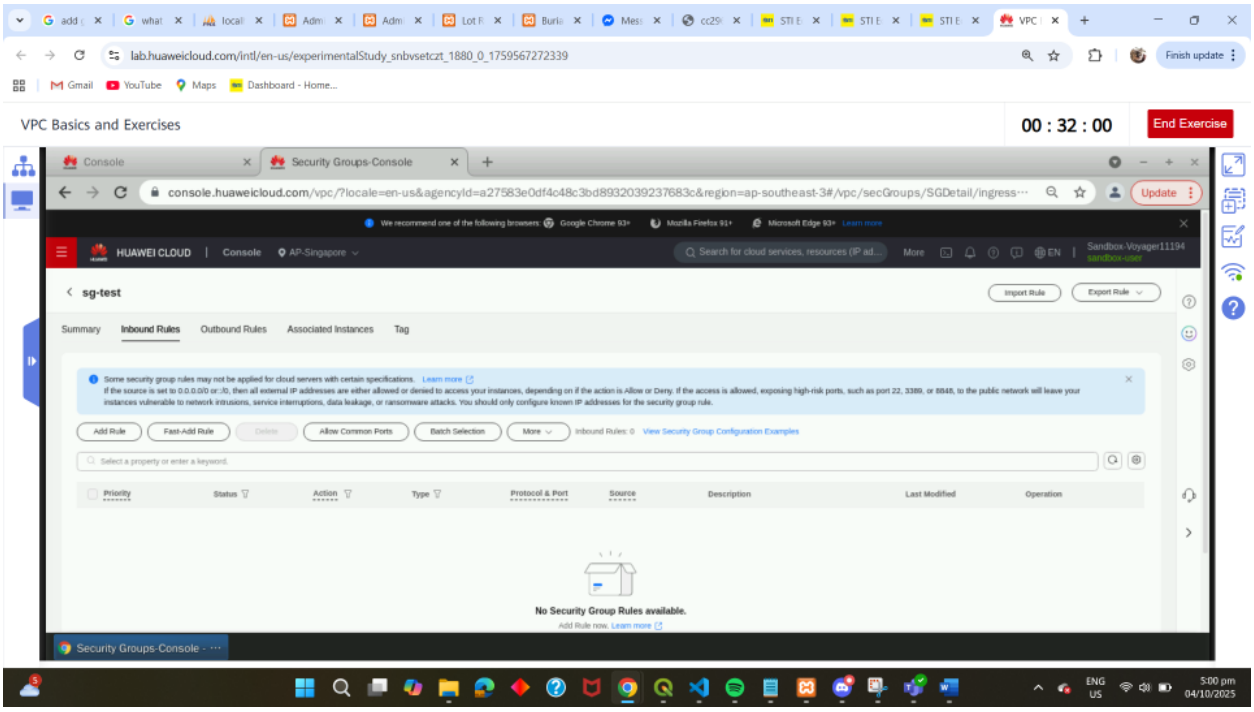
Part 1. Creating VPC, Subnet, and Security Group (20 points)

1. Log in to your Huawei CLOUD account
2. Click the Desktop (Exercise Interface) icon and launch Google Chrome. Go to any of the following links and log in using the provided Sandbox credentials as an IAM user.
3. Go to **Console** > **Service List** > **Virtual Private Cloud**.
4. Click **Create VPC** and set the following parameters:
    a. Region: **AP-Singapore**
    b. Name: **vpc-01**
    c. Default Subnet Name: **subnet-01**
5. Click **Create Now**. The Virtual Private Cloud page is displayed and you can now view your created VPC.
6. Create another subnet by clicking the name of your new VPC, **vpc-01**.
7. On the **Summary** tab, click the number beside **Subnets**.
8. Click **Create Subnet** and set the following parameters:
    a. Name: **subnet-02**
    b. IPv4 CIDR Block: **192.168.1.0/24**
9. Click **OK**. Screenshot the **Subnets** page showing the two (2) subnets. **(10 points)**



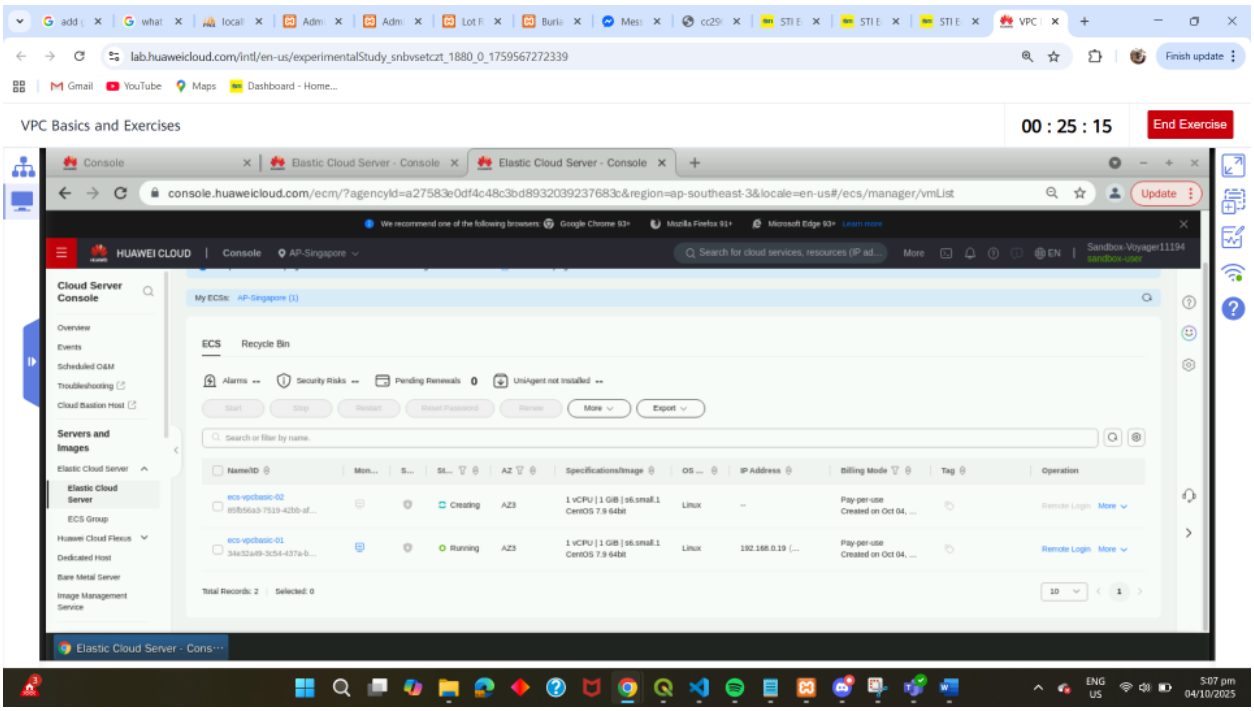
10. Under **Network Console**, go to **Access Control** > **Security Groups**.
11. Click **Create Security Group**. Name your security group **sg-test**.

12. Click **OK**. The Security Groups page is displayed and you can now view your created security group.
13. Click the name of your new security group, **sg-test** then go to the **Inbound Rules** tab.
14. Delete the two (2) rows containing **TCP : 443** and **TCP : 80**.
15. Screenshot the page showing the content of the **Inbound Rules** tab.

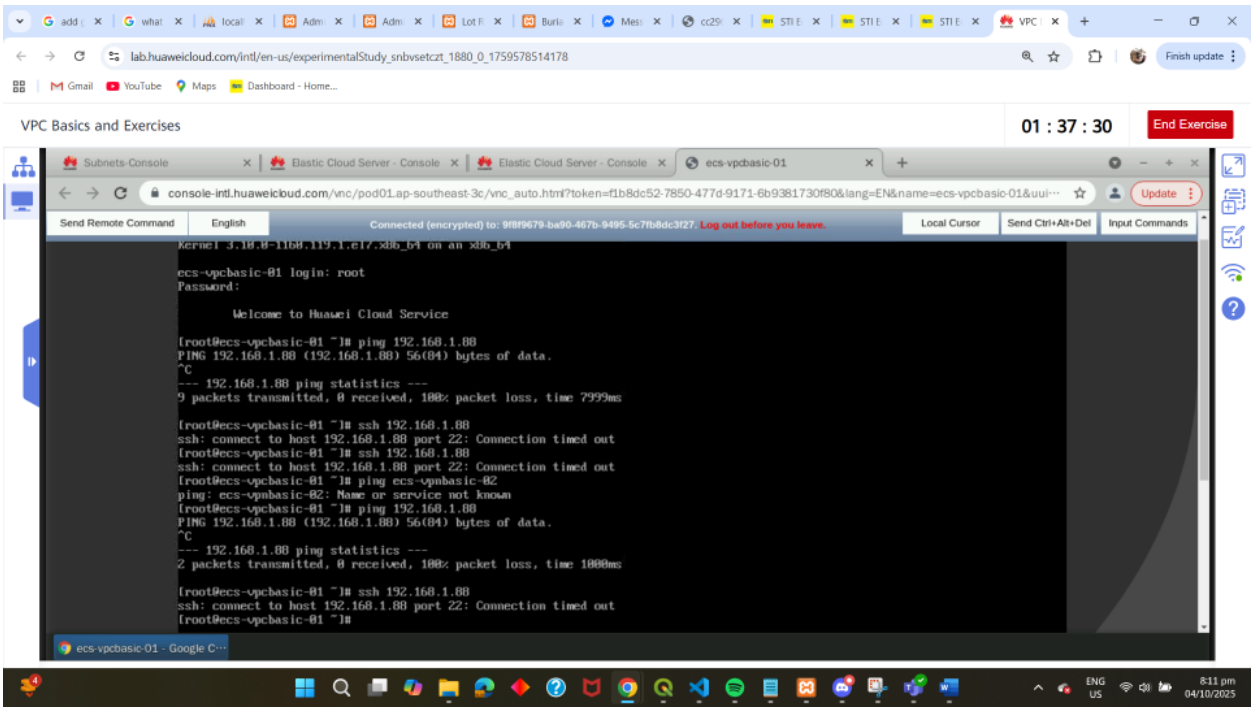


Part 2. Communication Between Two Elastic Cloud Servers (20 points)

1. Create a Linux ECS with the following parameters:
    - Region: **AP-Singapore**
    - Billing Mode: **Pay-per-use**
    - AZ: **Random**
    - CPU Architecture: **x86**
    - Specifications: **General computing, s6.small.1**
    - OS: **CentOS 7.9**
    - Network: **vpc-01, subnet-01**
    - Security Group: **sg-test**
    - EIP: **Not required**
    - ECS Name: **ecs-vpcbasic-01**
    - Password: **Huawei@1234**
2. Tick the **Agreement** checkbox, then click **Submit**.
3. Go to the Elastic Cloud Server Page to create another ECS. Click the name of your new ECS, **ecs-vpcbasic-01**.
4. Click **More > Buy Same ECS.** Follow the parameters in Step 1 but this time, select **subnet-02** and name your ECS **ecs-vpcbasic-02**.
5. Screenshot the **Elastic Cloud Server** page showing the two (2) ECSs. **(10 points)**



6. Log in to your first ECS, **ecs-vpcbasic-01**. Click **Remote Login** and click **Log In** under **Other Login Modes**.
7. Enter the username, **root**, and the password from Step 1.
8. View your ECS page and check the IP address of your second ECS, **ecs-vpcbasic-02**.
9. Go back to your running Linux ECS, then ping your second ECS. You should be able to ping successfully.
10. Press **Ctrl + C** to stop and view the ping statistics.
11. This time, access the second ECS using the **ssh** command. (Ex. ssh 192.168.1.37)
12. Enter the same password. Now that you are logged in to the second ECS, ping the first ECS. Screenshot the entire console. **(10 points)**



13. Stop your two (2) ECSs to save your cloud coupon credits.

Part 3. In exactly four (4) sentences, discuss the benefit of implementing a security group. (10 points)

- A security group keeps your cloud setup safe by controlling what kind of traffic can reach your servers. It lets you set clear rules for who or what can access your resources, keeping unwanted connections out. This reduces the risk of security breaches and keeps your network protected. In short, it helps you manage access and maintain a secure cloud environment without the extra hassle.