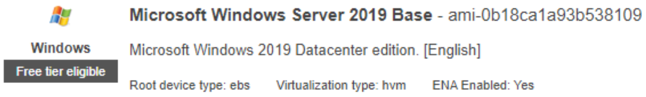
Firewalling using AWS Security Groups

The purpose of this assignment is to create a VM using [AWS] and restrict access to the VM by using AWS "firewall like" solution called Security Groups. Using your AWS account you previously you will create a Windows EC2 instance (VM), install the server role IIS (web server) and then restrict access to the VM to only allow specific IPs. This assignment will require a partner using a different public IP, as you will be whitelisting their IP to gain access to your VM. (Note: If you are working on this assignment over an extended period of time be sure to power-off / shutdown the VMs so you can reduce the cloud charges.)

1. (10 points) Create a Windows VM with the following properties (Hint: VM will connect to the default VPC):

- **Region: US East (Ohio) us-east-2**
- **Image: Windows Server 2019 Base**



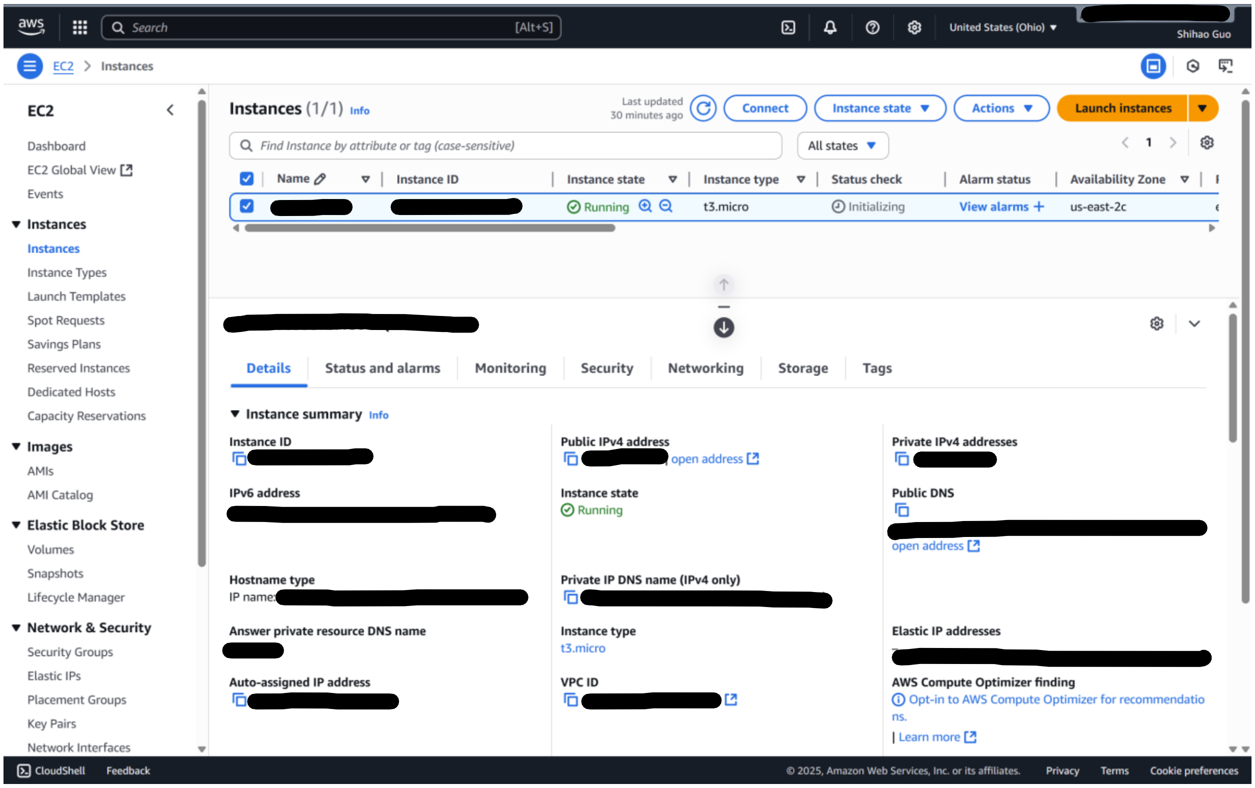
Windows
Free tier eligible
Microsoft Windows Server 2019 Base - ami-0b18ca1a93b538109
Microsoft Windows 2019 Datacenter edition. [English]
Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

- **Size: t2.micro (t2.micro is not available for free, so I go with t3.micro)**
- **Network: VPC default**
- **Use default storage (Ensure delete on termination is checked)**
- **Tags:**
  - [redacted]
  - **Value:** [redacted]
- **Create a new security group**
  - **Name:** [redacted]
  - **Description:** [redacted]
  - **For RDP rule change source to** [redacted]
- **Create VM (Launch VM)**
- **Create a new key pair and download the KeyPair (download to a safe place)**
  - **Name:** [redacted]
    - **You'll need this keypair to generate the password for your VM**

Provide as screenshot(s) showing your VM was created, as well as the following:

- **Virtual Machine Name**
- **Instance type**
- **Public IP assigned**
- **Private IP assigned**

Firewalling using AWS Security Groups



Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
[redacted]	[redacted]	Running	t3.micro	Initializing	View alarms +	us-east-2c

[redacted]

Instance summary Info

Instance ID: [redacted]

Public IPv4 address: [redacted] open address

Private IPv4 addresses: [redacted]

IPv6 address: [redacted]

Instance state: Running

Public DNS: [redacted] open address

Hostname type: IP name: [redacted]

Private IP DNS name (IPv4 only): [redacted]

Answer private resource DNS name: [redacted]

Instance type: t3.micro

Elastic IP addresses: [redacted]

Auto-assigned IP address: [redacted]

VPC ID: [redacted]

AWS Compute Optimizer finding: Opt-in to AWS Compute Optimizer for recommendations. | Learn more

3. (5 points) Is the public IP static or dynamic? What does AWS call a static IP?

The public IP is dynamic, which means the IP Address changes if I stop/start the VM. AWS calls a static IP Elastic IP.

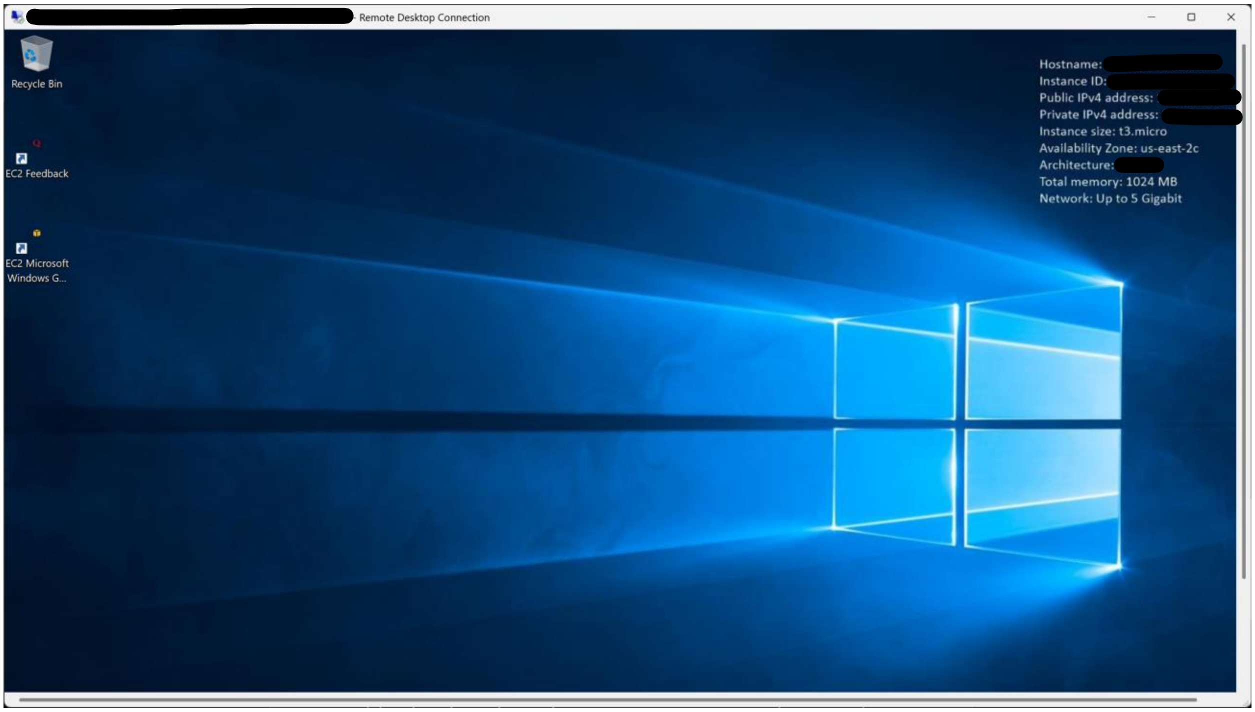
4. (5 points) Use the Remote Desktop Protocol (RDP) to connect to your newly created VM.

- **Which IP did you use to connect?**

  I used the public IP (In this session, [redacted] is the IP address) of the VM to connect.

  Provide a screenshot showing you successfully connected.

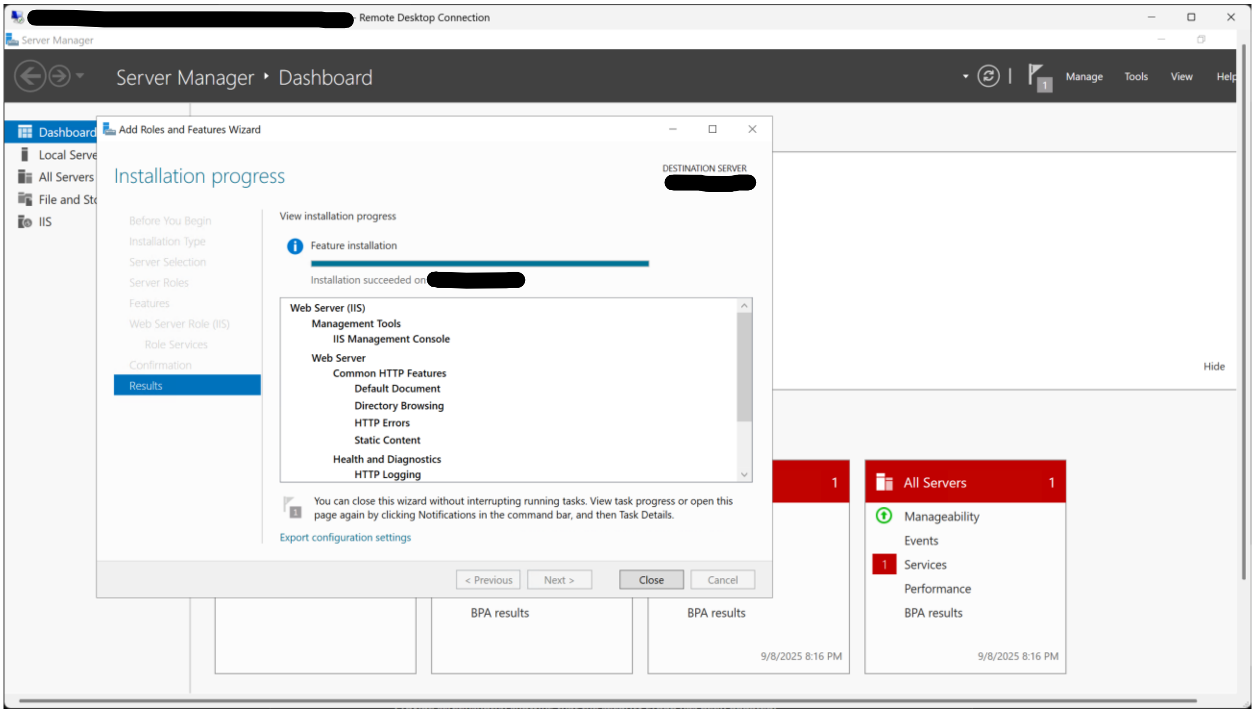
Firewalling using AWS Security Groups


[redacted] - Remote Desktop Connection
Recycle Bin
EC2 Feedback
EC2 Microsoft Windows G...

Hostname: [redacted]
Instance ID: [redacted]
Public IPv4 address: [redacted]
Private IPv4 address: [redacted]
Instance size: t3.micro
Availability Zone: us-east-2c
Architecture: [redacted]
Total memory: 1024 MB
Network: Up to 5 Gigabit

5. (10 points) Install / Add the (Web Server) ISS role within the VM you are connected to via RDP.

Provide a screenshot(s) showing the IIS role is installed and that you can access the default IIS website from the server (Hint: http://localhost/).



Installation progress

DESTINATION SERVER
[redacted]

View installation progress

Feature installation

Installation succeeded on [redacted]

```
Web Server (IIS)
    Management Tools
        IIS Management Console
    Web Server
        Common HTTP Features
            Default Document
            Directory Browsing
            HTTP Errors
            Static Content
        Health and Diagnostics
            HTTP Logging
```

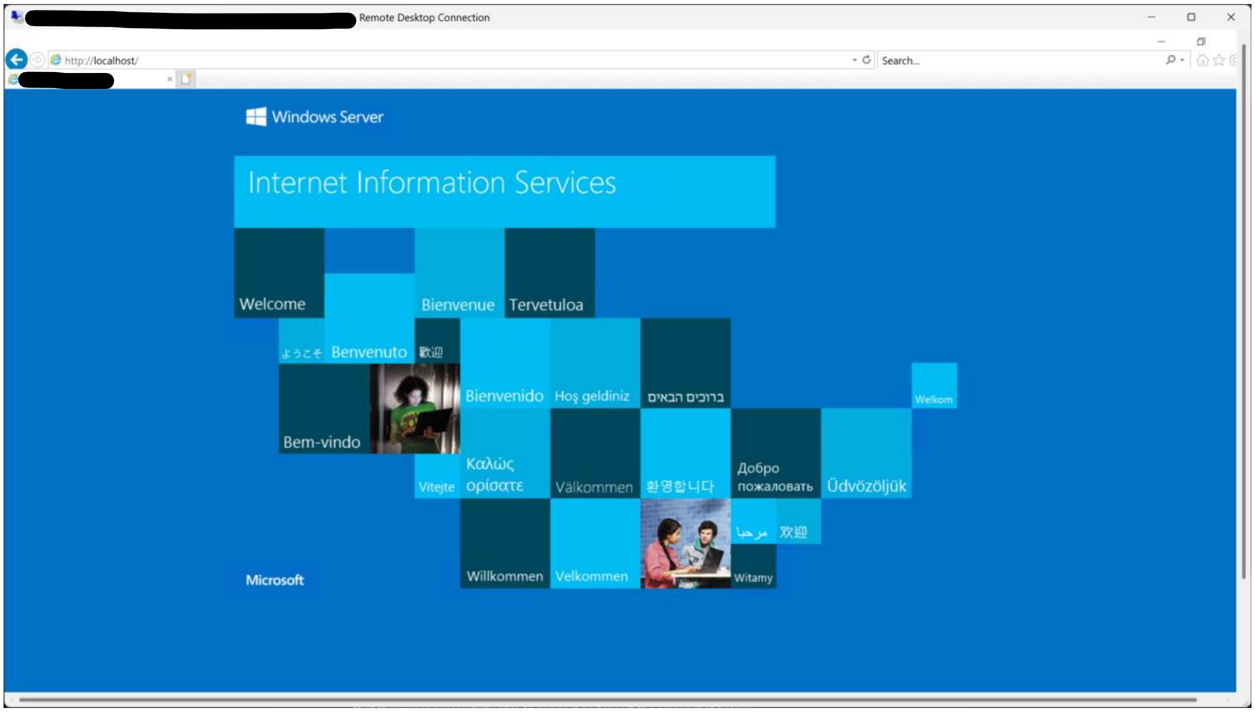
You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

Export configuration settings

9/8/2025 8:16 PM

9/8/2025 8:16 PM

Firewalling using AWS Security Groups



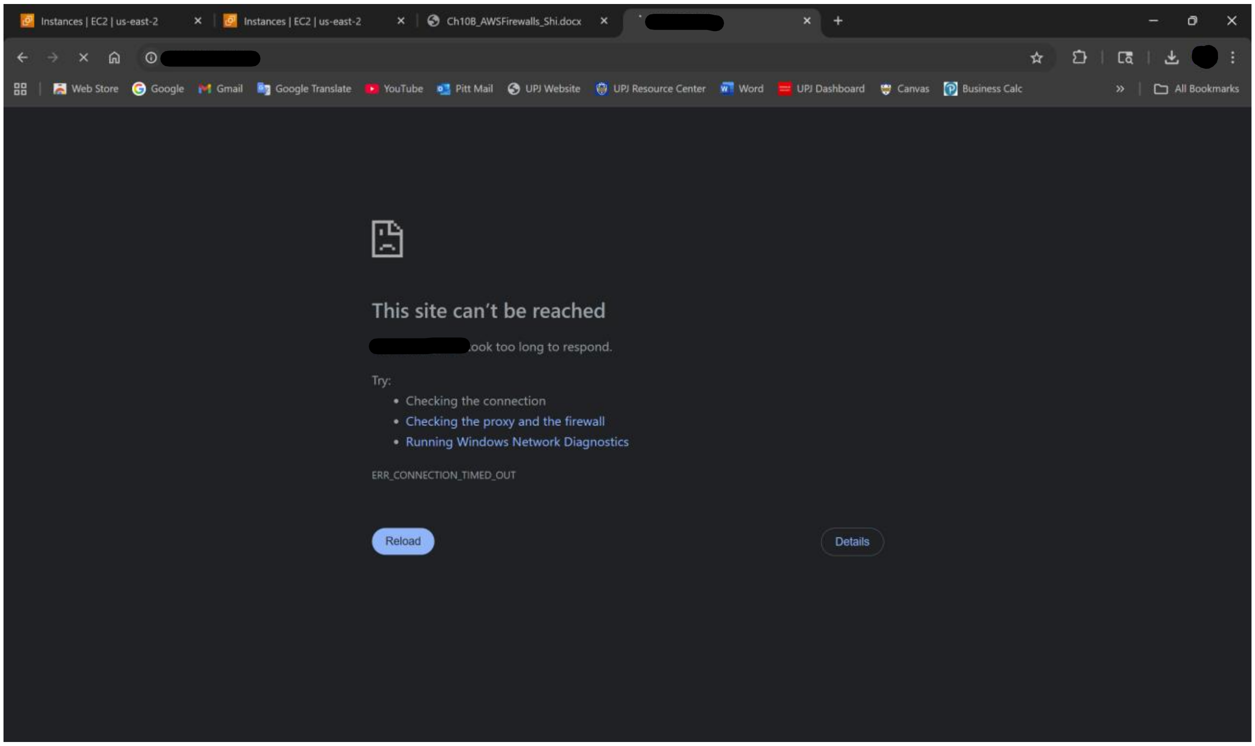
[redacted] Remote Desktop Connection

http://localhost/

[redacted]

6. (5 points) From your computer can you access the default IIS website from the public IP? If not, explain why?

No, this is because when I created the Security Group, I only allowed RDP (Port 3389) from my IP. I didn't add HTTP (Port 80) to the inbound rules. If I want to connect to the default IIS website, I will need to allow HTTP to the inbound rules.



[redacted]

[redacted]

This site can't be reached

[redacted]ook too long to respond.

Try:

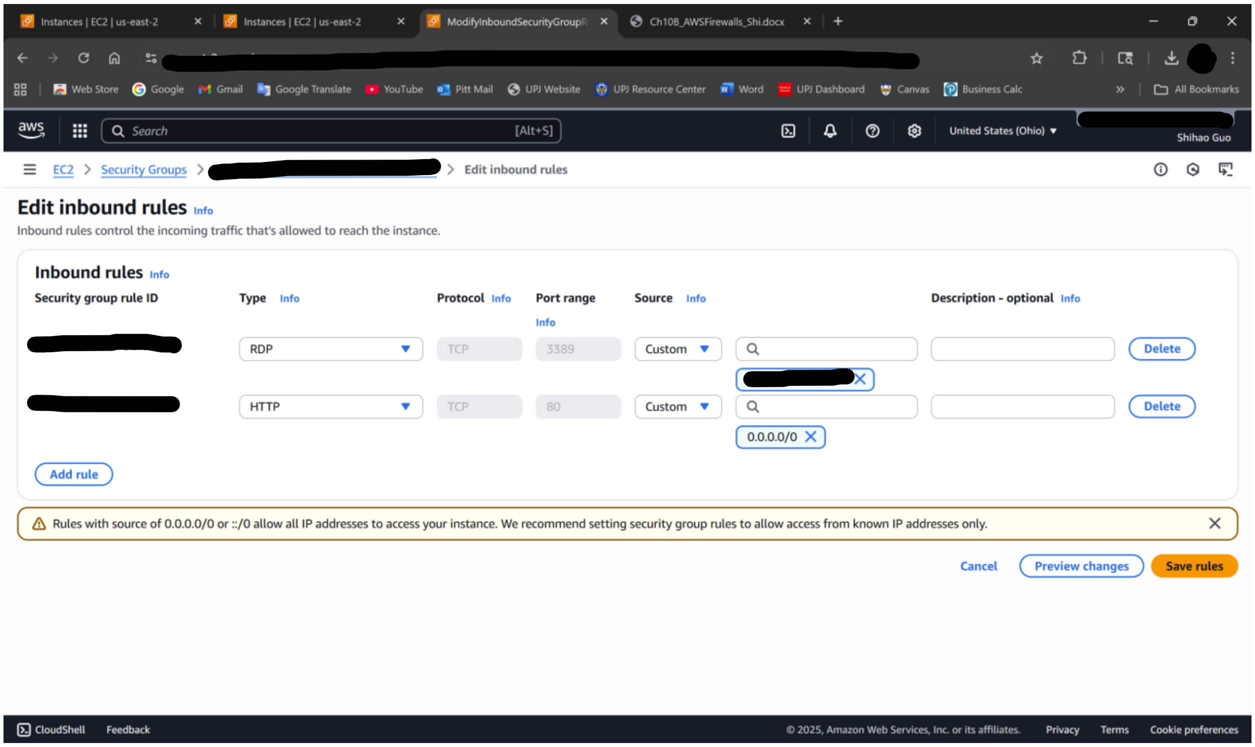
- Checking the connection
- Checking the proxy and the firewall
- Running Windows Network Diagnostics

ERR_CONNECTION_TIMED_OUT

Firewalling using AWS Security Groups

7. (5 points) Add a firewall rule to the AWS security group allowing port 80. Leave the source as 0.0.0.0/0.

Provide screenshot(s) showing the rule creation.



Edit inbound rules Info

Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules Info

Security group rule ID	Type Info	Protocol Info	Port range Info	Source Info		Description - optional Info	
[redacted]	RDP	TCP	3389	Custom	[redacted]		Delete
[redacted]	HTTP	TCP	80	Custom	0.0.0.0/0		Delete

Add rule

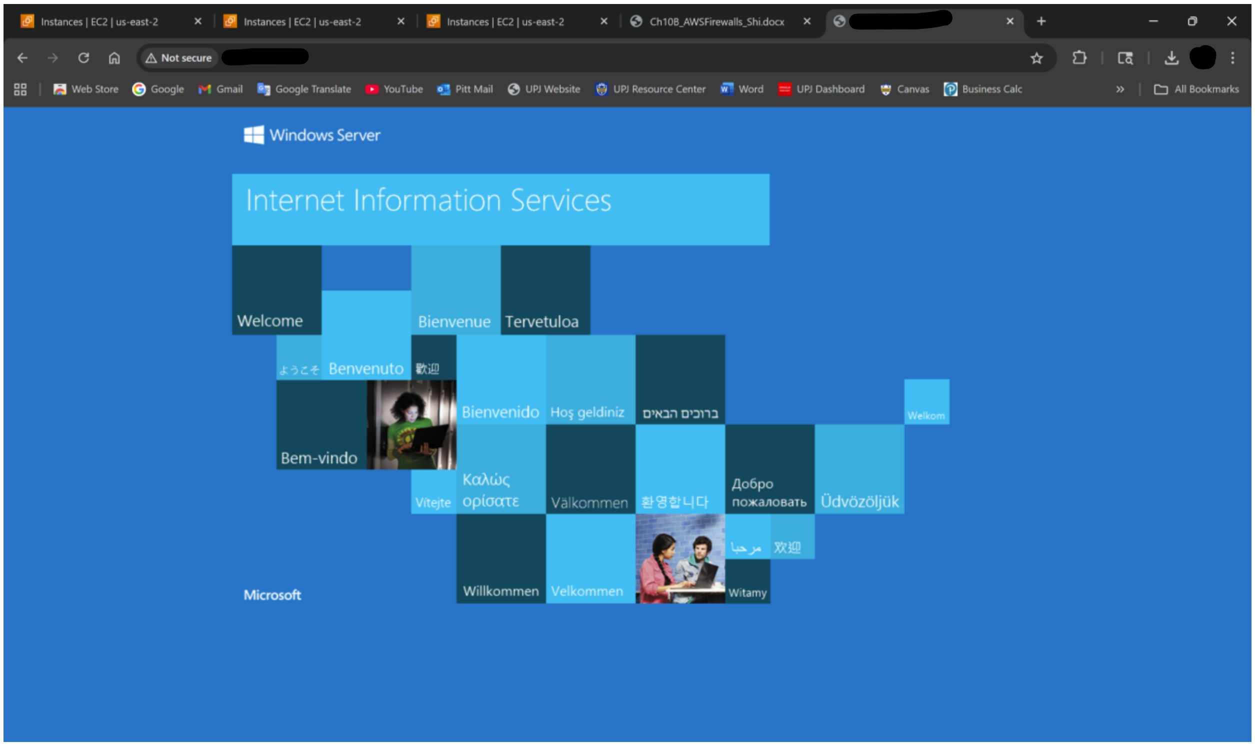
⚠ Rules with source of 0.0.0.0/0 or ::/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

8. (5 points) Are you able to access the website now from your computer?

Yes, after adding the HTTP rules, I can now access the website.

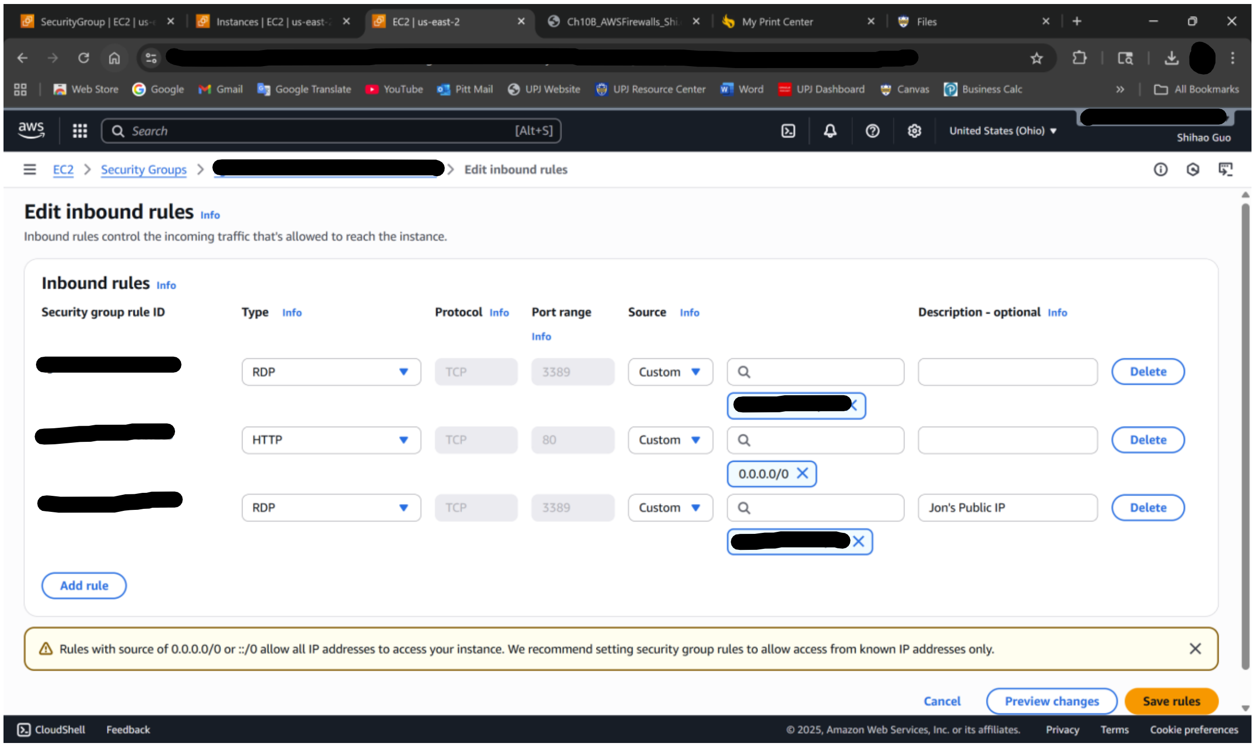
Provide screenshot(s) showing your results.

Firewalling using AWS Security Groups



9. (5 points) Ask your partner (Jon) what their public IP is and update the AWS Security Group to allow their IP access to your server via RDP (Hint: obtaining public IP can be done by using websites like www.whatismyip.com).

Provide screenshot(s) showing that the security group has been updated.



EC2 > Security Groups > [redacted] > Edit inbound rules

Edit inbound rules Info

Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules Info

Security group rule ID	Type Info	Protocol Info	Port range Info	Source Info		Description - optional Info	
[redacted]	RDP	TCP	3389	Custom	[redacted]		Delete
[redacted]	HTTP	TCP	80	Custom	0.0.0.0/0 ✕		Delete
[redacted]	RDP	TCP	3389	Custom	[redacted]	Jon's Public IP	Delete

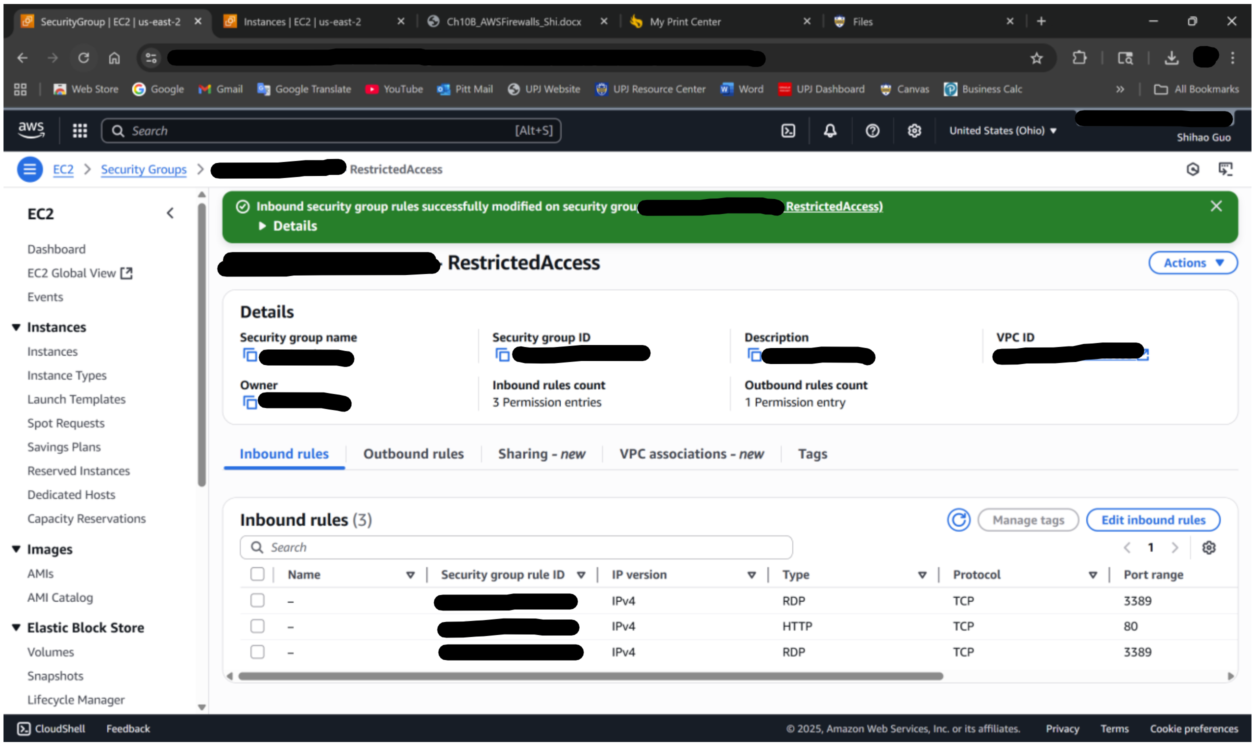
Add rule

⚠ Rules with source of 0.0.0.0/0 or ::/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only. ✕

Cancel Preview changes Save rules

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Firewalling using AWS Security Groups



[redacted]

EC2 > Security Groups > [redacted] RestrictedAccess

Inbound security group rules successfully modified on security grou[redacted] RestrictedAccess)

▸ Details

[redacted] RestrictedAccess

Details

Security group name [redacted]	Security group ID [redacted]	Description [redacted]	VPC ID [redacted]
Owner [redacted]	Inbound rules count 3 Permission entries	Outbound rules count 1 Permission entry	

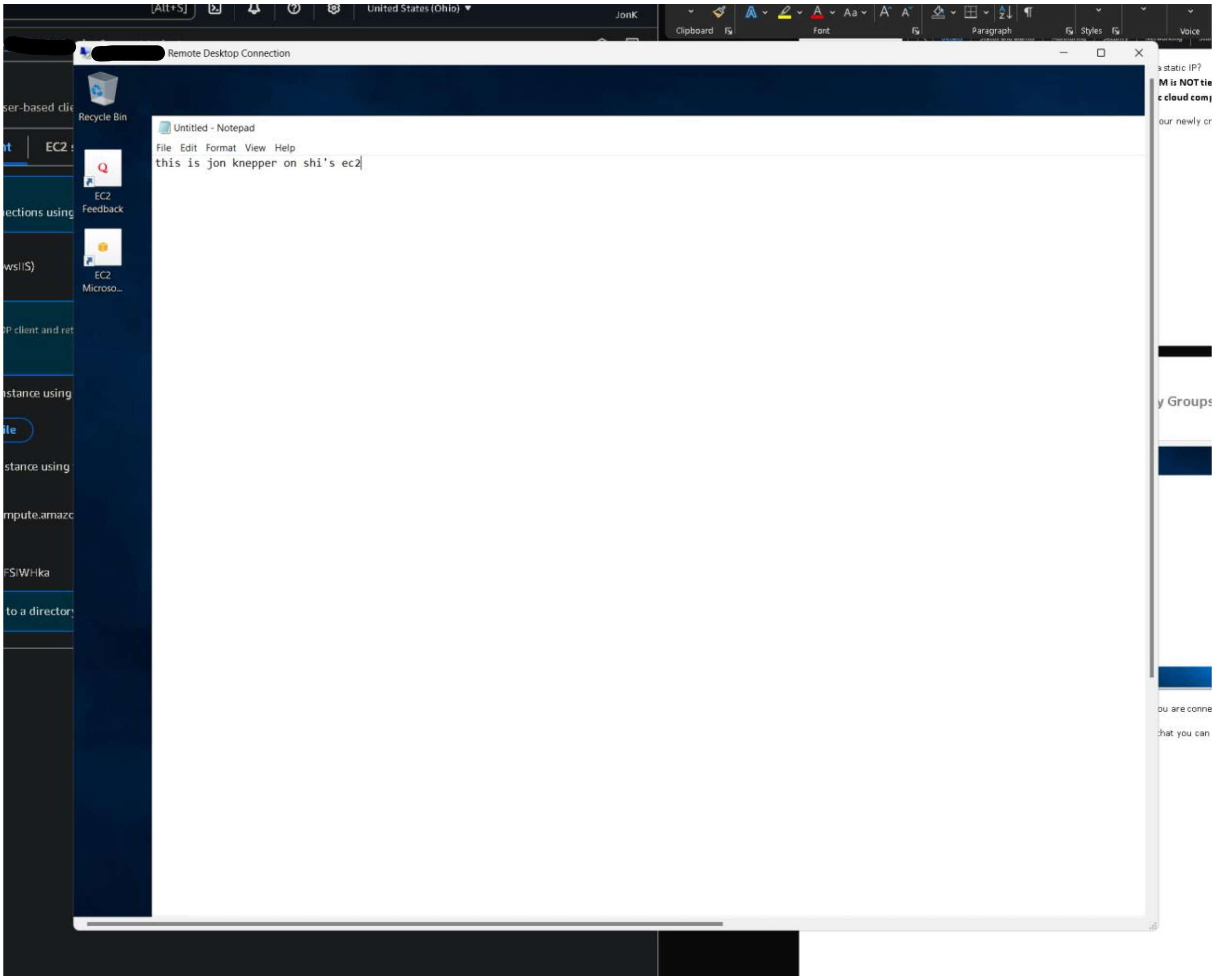
Inbound rules (3)

□	Name	Security group rule ID	IP version	Type	Protocol	Port range
□	–	[redacted]	IPv4	RDP	TCP	3389
□	–	[redacted]	IPv4	HTTP	TCP	80
□	–	[redacted]	IPv4	RDP	TCP	3389

10. (5 points) Verify your partner (Jon) can RDP to your server. Have them provide you with a screenshot that they were successfully able to connect and insert the screenshot below:

Provider partner screenshot(s):

Firewalling using AWS Security Groups



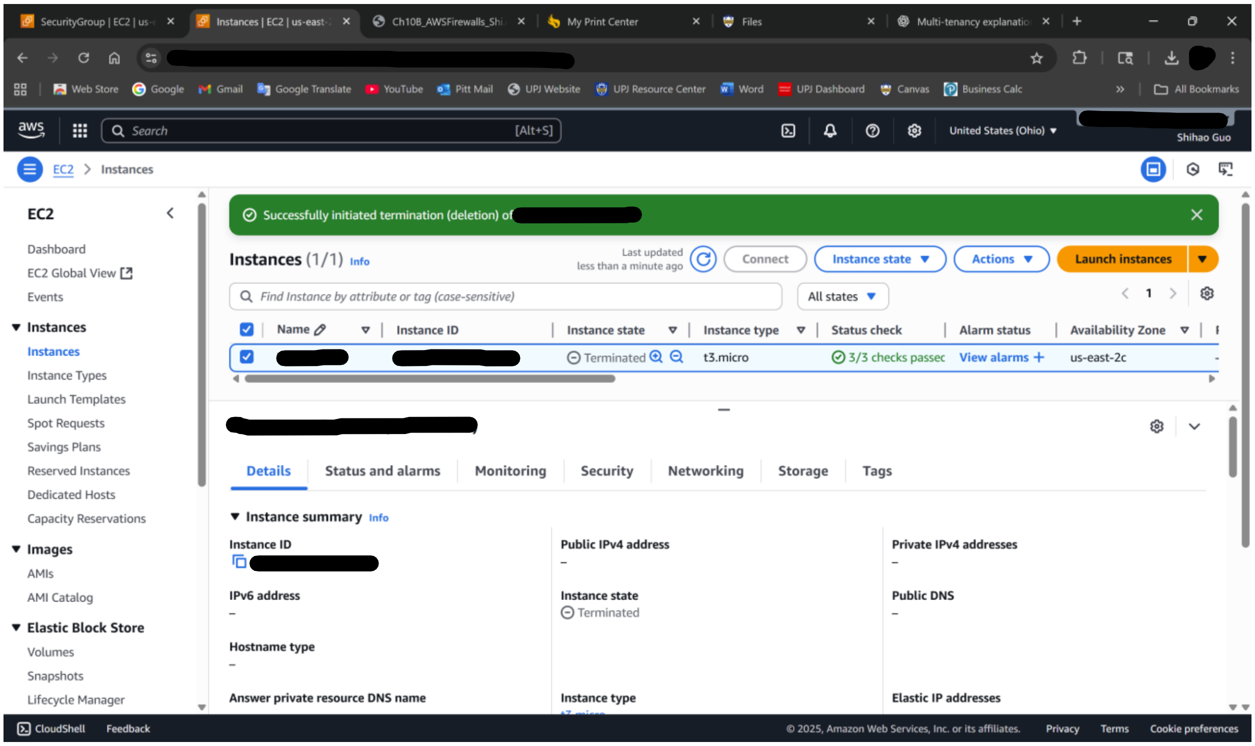
```
this is jon knepper on shi's ec2
```

11. (5 points) When completed with this assignment delete your VM and Security Group.

Provide screenshots showing this is completed.

Note: This clean-up is very important to reduce cloud charges.

Firewalling using AWS Security Groups



[redacted]

Successfully initiated termination (deletion) of [redacted]

Instances (1/1) Info

☑	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
☑	[redacted]	[redacted]	Terminated	t3.micro	3/3 checks passec	View alarms +	us-east-2c

[redacted]

Instance summary Info

Instance ID
[redacted]

Public IPv4 address
–

Private IPv4 addresses
–

IPv6 address
–

Instance state
Terminated

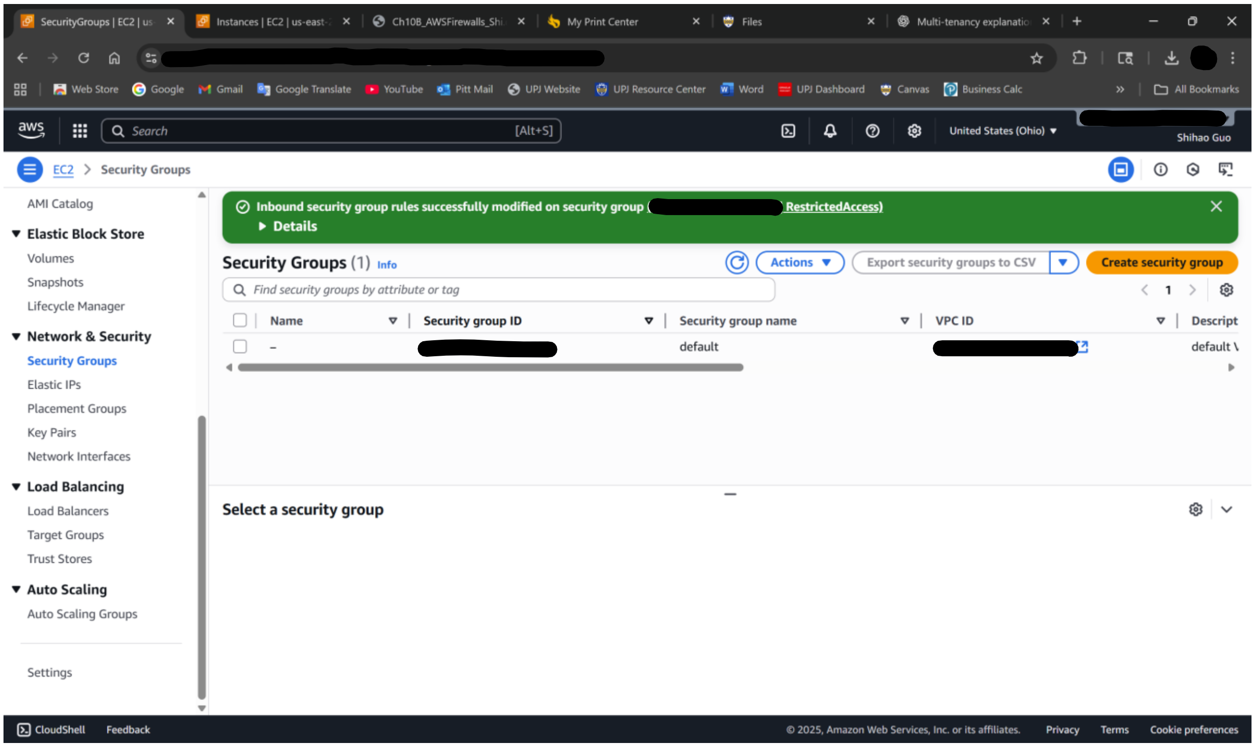
Public DNS
–

Hostname type
–

Answer private resource DNS name

Instance type

Elastic IP addresses



[redacted]

Inbound security group rules successfully modified on security group ([redacted] RestrictedAccess)
Details

Security Groups (1) Info

□	Name	Security group ID	Security group name	VPC ID	Descript
□	–	[redacted]	default	[redacted]	default \

Select a security group