Domain: Cloud Security

How would you control access to a cloud network?

1. Restate the Problem – How is the cloud network secured from unauthorized access?

2. Provide a Concrete Example Scenario

- In Project 1, did you deploy an on-premises or cloud network? - **In Project 1 I deployed a cloud network**
- Did you have to configure access controls to this network? - **Yes, the access controls are configured within the Inbound rules section of the Security groups.**
- What kinds of access controls did you configure, and why were they necessary? How do these details relate to the interview question? - **The access controls were configured to control the SSH and HTTP access to the Jump box and the webservers. These controls help restrict the access to only authorized users (In this case, it's only my remote computer which can access the Jump box and the VM's can only be accessed through Jump Box)**

- 3. Explain the Solution Requirements in Project 1, what kinds of access controls did you have to implement? Consider:
- NSGs around the VNet? Around the VMs?
- Local firewalls (ufw, etc.) on each VM?
- Protocol allow/deny lists?
- What did each access control achieve, and why was this restriction necessary for the project?

The following describes the access controls configured -

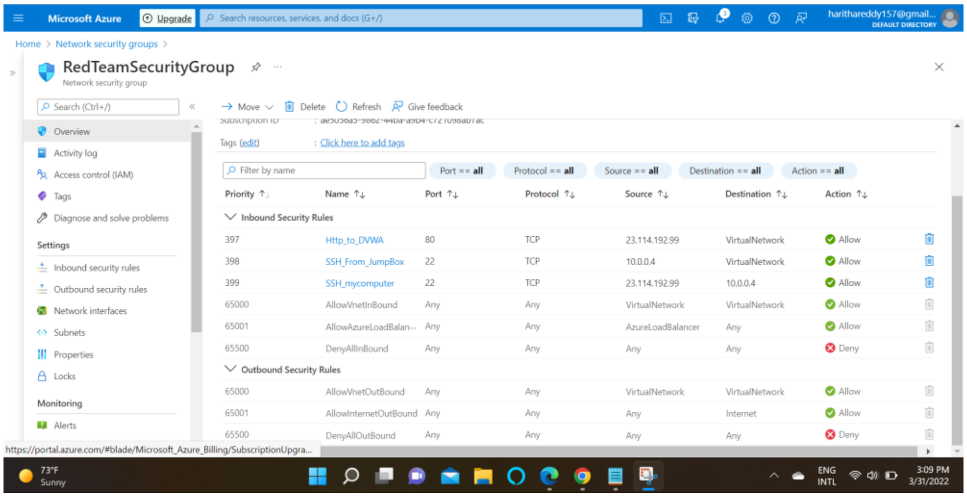
A) To establish a connection from my remote computer, I configured an inbound rule to access the Jump box's Public IP from my computer (Public IP of my computer) via SSH.

B) To access the VM's via Jump box, the access control is configured to access the VM's from jump box via SSH through the Private IP's

C) To access the DVWA and ELK server via internet, the access control is configured to access these servers via HTTP protocol from my personal computer's Public IP Address.

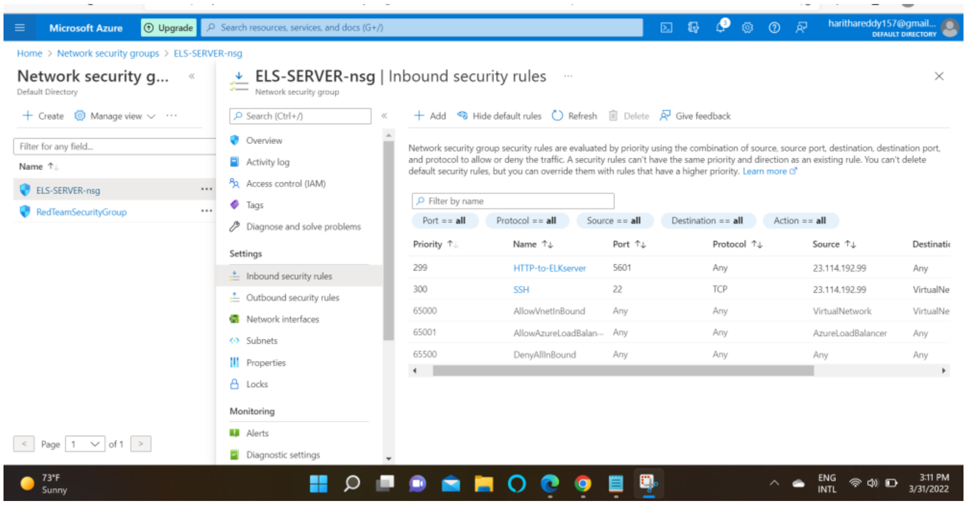
Below are the screenshots from the security groups showing the acces controls -

RedTeam Security Group inbound rules-



Priority	Name	Port	Protocol	Source	Destination	Action
Inbound Security Rules						
397	Http_to_DVWA	80	TCP	23.114.192.99	VirtualNetwork	Allow
398	SSH_From_JumpBox	22	TCP	10.0.0.4	VirtualNetwork	Allow
399	SSH_mycomputer	22	TCP	23.114.192.99	10.0.0.4	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalan...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny
Outbound Security Rules						
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

ELK-Net Security Group Inbound rules -



ELS-SERVER-nsg | Inbound security rules

Network security group

Network security group security rules are evaluated by priority using the combination of source, source port, destination, destination port, and protocol to allow or deny the traffic. A security rules can't have the same priority and direction as an existing rule. You can't delete default security rules, but you can override them with rules that have a higher priority. Learn more

Priority	Name	Port	Protocol	Source	Destinati
299	HTTP-to-ELKserver	5601	Any	23.114.192.99	Any
300	SSH	22	TCP	23.114.192.99	VirtualNe
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNe
65001	AllowAzureLoadBalan...	Any	Any	AzureLoadBalancer	Any
65500	DenyAllInBound	Any	Any	Any	Any

- 4. Explain the Solution Details -
- Which rules do you set for each NSG in the network? - **As depicted in the screenshot above, the access control rules are set to access the servers within the network.**
- How does access to the jump box work? - **Jump box can be accessed via SSH from the remote computer.**
- How does access from the jump box to the web servers work? - **The access control from Jump box is configured to access the Virtual network via SSH. The Web serves' private IP will be accessed through the Jump box's private IP**
- 5. Identify Advantages/Disadvantages of the Solution

Does your solution scale? - **The advantage of the security groups is that the access can be controlled from a central repository. The access can be configured as required. The con of using the security groups is that it may not be scalable. Since every rule has to be configured individually, the method of adding every remote user access is not scalable for a medium to large organization. If the rules are not**

configured carefully, there is chance that the server will be locked out and no one will be able to access it and if the necessary controls are not in place, an unauthorized user can access the servers.

- Is there a better solution than a jump box? - **VPN is a better solution than Jump Box**
- What are the disadvantages of implementing a VPN that kept you from doing it this time? - **VPN is a costlier option than Jump Box and also it would be a better solution if implemented at a corporate level.**
- What are the advantages of a VPN? - **A VPN encrypts the traffic and hence ensures security of the connection. If an organization owns a VPN server, the traffic/VPN credentials will be decrypted within the organization.**
- When is it appropriate to use a VPN? - **VPN would be appropriate for a corporation or scenarios where VPN server is owned by the trusted source.**

Question 2:

Corporate VPN

What are the advantages and disadvantages of using a corporate VPN, and under what circumstances is using one appropriate?

1. Restate the Problem – **Does VPN protect the security in all circumstances? What is the appropriate scenario to use it?**

2. Provide a Concrete Example Scenario

- In Project 1, which VMs did you have on the network? - **I have Jumpbox, RedTeamWeb-1, RedTeamWeb-2, RedTeamWeb-3 and ELK-server**
- Which tools did you use to control access to and from the network? - **Network Security Groups was used to control the access**
- If you didn't use a VPN, what did you use? - **Security Groups**
- What disadvantage(s) did your non-VPN solution have? - I**t can be used when the connections to the server are limited in number. It is not scalable.**
- What advantage(s) did your non-VPN solution have? - **It is affordable and is effective when the connections to the server are limited in number.**

3. Explain the Solution Requirements

- Would a VPN meet the access control requirements you had for Project 1? - **Yes, it would meet the requirements.**
- How would a VPN protect the network just as well, or better, than your current solution? - **Once connected to the VPN, VPN encrypts the traffic coming into the network and it is only decrypted at the VPN server and then the traffic is routed to the destination. It is a better solution than the current one as the traffic is not encrypted using the security groups or a Jump box.**

4. Explain the Solution Details

- Which Azure tools would you use to implement a VPN to your Project 1 network? - **Azure VPN Gateway and Microsoft Authenticator can be used to implement VPN. The VPN gateway can be created for every Virtual Network, if needed.**
- How would you onboard users to the new VPN system? - **The users can be added to the VPN directory. Since the VPN is secured by credentials and multi-factor authentication, only authenticated users can access the system.**

5. Identify Advantages and Disadvantages of the Solution

- In Project 1, would a VPN have been an appropriate access control solution? **VPN would not be appropriate in the project as access control solution. A secure and good VPN would cost more. Also, VPN would be appropriate when too many connections are made to the server remotely and the security is high priority. VPN is secure when the VPN server is also owned by the same individual/organization who owns the network and web servers. That would make it more costly. I did not require a top-notch security for my project, so it was not appropriate.**

- Under what circumstances is a VPN a good solution? When, if ever, is a VPN "overkill"? **VPN would be an "overkill" solution when the security is not a priority.**

Question 3:

Containers

When is it appropriate to use containers in cloud deployments, and what are the security benefits of doing so?

1. Restate the Problem - **What are the benefits of using containers over traditional servers?**

2. Provide a Concrete Example Scenario

- In Project 1, when did you use containers? - **In Project 1, a DVWA container and ELK stack container along with file beat and Metric beat was deployed**
- What did you use containers for? **I used containers to deploy a pre-configured software on the server.**

3. Explain the Solution Requirements

- Why was this an appropriate use for containers? - **Containers are pre-configured and portable. The configurations and data within can be stored as an image. The security configurations can be viewed and updated from a docker file or image. It was easy to accomplish multiple tasks using a single playbook file on a container.**

- What security benefits did you expect from using containers? - **There are multiple benefits using a container**
- **Address the security problems of specific containers**
- **Easy application update using a docker file/image**
- **The hosted Applications/servers can be easily managed from a single docker file**

4. Explain the Solution Details

- In Project 1, how did you configure VMs to be able to run containers? **I used Ansible to deploy the containers on VM's and created specific 'playbooks' to configure the containers and list down the requirements as tasks on the playbook. The 'Hosts' file in the configuration directory of ansible (i.e /etc/ansible) should be used to add the IP addresses of the hosts I was planning to deploy the container.**
- How did you select and install the correct container? **The playbooks were created to accomplish the task of creating the container with specific requirements. The tasks section within the playbook file can be viewed to verify if the correct requirements are listed.**
- How did you verify that it was running correctly? - **Running the playbook would show if the container is running as expected on the VM's. If there is any issue running at a particular machine, an error would be thrown specific to the IP address of the machine. Also, I SSHéd into the container to verify if the connection was established successfully.**

5. Identify Advantages/Disadvantages of the Solution

- How would you have achieved the same thing without containers? - **I would have installed and configured an OS on the VM's and then install the desired software package.**
- What are the advantages to doing it without containers? - **The advantages of deployment without using a container are that the OS resources can be used effectively, as container take up lot of underlying OS kernel resources to run. Containers are best used to run the microservices. If an application is not a microservice, it is an overuse of OS resource and not cost friendly.**
- What are the disadvantages? - **The disadvantage is that, the updates and security management is not easy when not used as a container where these actions are normally accomplished through one playbook file.**

Question 4:

Cloud Infrastructure as Code

What are the security benefits of defining cloud infrastructure as code?

1. Restate the Problem – **Why defining an Infrastructure as code is preferrable to traditional infrastructure**

2. Provide a Concrete Example Scenario

- In Project 1, when did you use infrastructure as code (IaC)? - **In Project 1, Ansible was used to deploy the containers on VM's. The Ansible is the IaC package used.**
- What tool did you use? **Ansible.**
- What did you use it to do? **I used Ansible to deploy, configure and manage the containers on VM**

3. Explain the Solution Requirements

- Were there any alternatives to IaC? - **The traditional server or a whole different infrastructure set up can be used as an alternative**
- What benefits does IaC have over alternative approaches? - **Setting up the VM is easy using the IaC tool such as Ansible rather than configuring the whole infrastructure. It's quicker and easily manageable. It's portable and can be done from any remote system. It reduces the attack surface on the infrastructure.**

4. Explain the Solution Details

- In Project 1, which specific configurations did your IaC set up? **The Ansible was set up on the Jump Box. The ansible configuration file is used to configure the username of the 'remote user' that would login into the containers. The 'hosts' file was configured to list the hosts/VM's the ansible should**

establish connection and accomplish the tasks. Playbooks to deploy containers were configured and run using Ansible.

- How did you run and test these configurations? **I created a sample playbook that deploys the DVWA container and ran the playbook successfully and also, I SSHéd into the containers to test the connection was established as configured in the Ansible configuration files.**

5. Identify Advantages/Disadvantages of the Solution

Are there any disadvantages to using IaC over the "traditional" approach?

(Source: https://www.bmc.com/blogs/infrastructure-as-code/#:~:text=Advantages%20of%20IaC,-Here%20are%20the&text=Enabling%20version%2Dcontrolled%20infrastructure%20and,configurations%20in%20their%20desired%20state.) Some of the advantages of using IaC over the "traditional "approach are that

- **The infrastructure can be easily standardized and the configuration can be easily reproduced**
- **Version control in the infrastructure can be enabled**
- **It is faster than traditionally configuring the infrastructure**