```
## Activity File: Interview Questions
```

```
Select one domain and one question.
```

```
#### Domain: Cloud Security
```

Question 1: Cloud Access Control

How would you control access to a cloud network? You have to create a virtual network, virtual machine, firewall, Also the only people that can gain access to the VM , jumpbox, web 1, web 2, web 3, is to ssh into using the personal IP address of users. This eliminates the ability to alter or change the data. Then install Filebeats helps generate and organize log files to send to Log stash and Elasticsearch. The Filebeat monitors the Apache server and MySQL database logs generated by DVWA. Setting up the Elk server container uses the public IP address of the Elk server that you created to navigate to the kibana website to continue to check on the data to check source, time stamps, volume and geo coordinate along with many other searches. Setting up the metricbeat to enable docker commands, run the metric beat set up commands, and -e command and enable Metric beat service on the boot.

1. Restate the Problem access to the network cloud network and control the access by creating a virtual network. Answer is: Setting up the virtual network using ssh into the VM's to eliminate others from altering and changing data. Setting up Firewalls, and as well as having a Network Security Group configured to allow incoming traffic to Elasticsearch and Kibana from the outside.
2. Provide a Concrete Example Scenario
    - In Project 1, did you deploy an on-premises or cloud network?
    - Answer: cloud network
    - Did you have to configure access controls to this network?
    - Answer: yes
    - What kinds of access controls did you configure, and why were they necessary?
    - Answer: configure the firewall exclusive to port 5601 using the personal IP address to access.
    - How do these details relate to the interview question?
    - Answer: Explaining the development of How , Why , and What was done from start to finish. Setting up a Cloud network security to protect the web servers and will only allow ssh connectivity by person and filtering all the HTTP data coming in.
3. Explain the Solution Requirements

- In Project 1, what kinds of access controls did you have to implement? Consider:
  - NSGs around the VNet?NetworkSecurityGroup Firewall (ELK-nsg and FirewallNSG) Around the VMs?we created protection from firewalls.
  - Local firewalls (ELK-nsg) on each VM?
  - Protocol allow/deny lists? virtual networks, firewall, inbound security rule,
  - a Network Security Group configured to allow incoming traffic to Elasticsearch and Kibana from the outside.
- What did each access control achieve, and why was this restriction necessary for the project?
- Answer: No one can access into out network, without a personal IP address, and
- making sure we can ssh into the VM and no one else could. Only our personal IP could ssh into . We also made sure we ssh to the web servers. We did not want to let anyone else make changes.

4. Explain the Solution Details
   - Which rules do you set for each NSG in the network?
   - Answer: 5601 Elastic 9200 allow, 80 External -IP_port_80, 22 Jump Box-access and ssh, Network Security Groups FirewallNSG
   - How does access to the jump box work? Ssh
   - Answer: The jump boxes use your IP address there for you are able to **ssh** to my jump box using my ip address only. Keeps it safe.
   - How does access from the jump box to the web servers work?
   - Answer:ssh using an encrypted IP of a person controlling cloud. and use the containers to make changes to the web servers. Keeping this safe from other people making changes.
5. Identify Advantages/Disadvantages of the Solution
   - Does your solution scale?
   - Answer:yes we can become elastic and add Web servers, and add ip to host ansible.
   - Is there a better solution than a jump box?
   - Answer: NO The jump box is the best solution because you only make changes from one serve instead of many. and effort and control which ones. As well as being expandable and elastic, and flexible and keeping environments safe.

- What are the disadvantages of implementing a VPN that kept you from doing it this time?
- Answer: Disadvantage ? 1. It slows the data and increases latency.
- 2. Also cost money.
- What are the advantages of a VPN?
- Answer: Advantages? encrypting data from target to source keeping it safe. Maintaining Integrity if the information is needing to be protected.
- When is it appropriate to use a VPN?
- Answer: When you have data that is confidential then VPN would be a safer way to send and receive info, **but** it might come down to cost.