

Experiment 06

Learning objective: Create and modify the firewall rules of Virtual Private Cloud.

Tools: Azure Portal

Theory:

In cloud networks, security is very important because resources like virtual machines and applications must be protected from unwanted access. Microsoft Azure provides Azure Firewall, a managed security service that helps control traffic entering and leaving a Virtual Network (VNet). It works as a checkpoint that allows only the traffic we want and blocks everything else.

Azure Firewall is stateful, meaning it remembers the state of connections. For example, if a VM sends a request to Google, the firewall allows the reply to come back, but it blocks any unknown or unwanted connection request. The firewall is deployed in a special subnet called AzureFirewallSubnet inside a VNet. In our experiment, we created:

- **Workload-SN subnet** → where the virtual machine (VM) is placed.
- **AzureFirewallSubnet** → where the firewall is placed.

Since the VM had no public IP, all its internet traffic went through the firewall. This ensures that every request is checked against firewall rules. To force this routing, a Route Table was created with a default route (0.0.0.0/0) pointing to the firewall's private IP.

Azure Firewall uses three main types of rules:

1. **Application Rules** – These rules allow or block websites (FQDNs).
 - *Example:* Allow only www.google.com but block other websites like www.microsoft.com.
2. **Network Rules** – These rules control traffic based on IP, protocol, and port.
 - *Example:* Allow UDP traffic on port 53 so the VM can send DNS queries to external DNS servers like 209.244.0.3.
3. **NAT Rules** – These rules allow external users to access internal VMs by mapping the firewall's public IP to the VM's private IP.
 - *Example:* Create a NAT rule so that when someone connects to the firewall's public IP on port 3389, it forwards the request to the VM's private IP for Remote Desktop (RDP).

When tested, the setup worked as expected:

- We could access Google but not other sites (Application Rule worked).
- DNS name resolution was successful (Network Rule worked).
- Remote Desktop to the VM was possible through the firewall's public IP (NAT Rule worked).

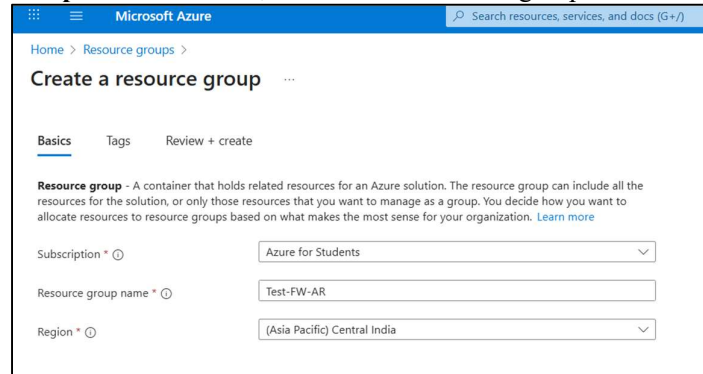
In real-world use, Azure Firewall is usually deployed in a hub-and-spoke architecture, where it sits in a central VNet (hub) and manages traffic for multiple workload VNets (spokes). This makes it easier for organizations to apply consistent security policies across all their cloud resources.

In summary, Azure Firewall provides a simple and effective way to:

- Control outbound access (e.g., allow only Google).
- Control inbound access (e.g., RDP only through firewall).
- Protect workloads by monitoring and filtering traffic.

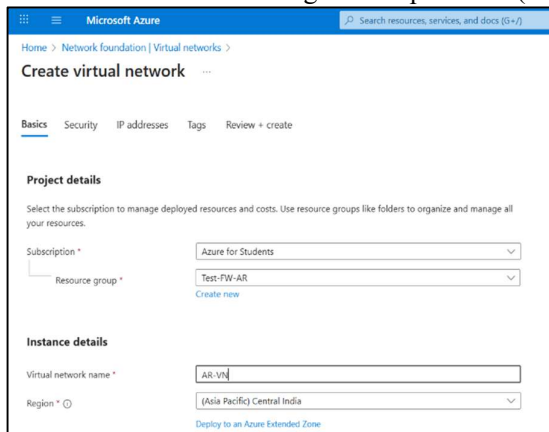
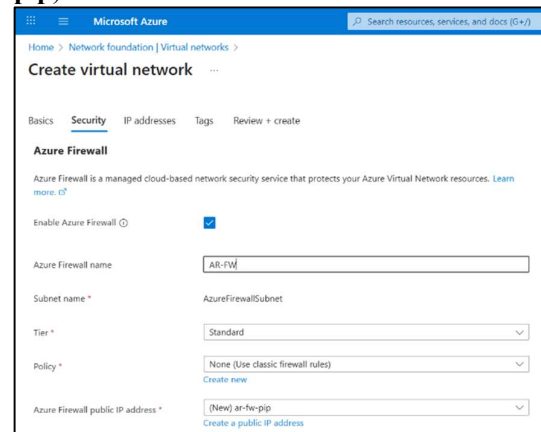
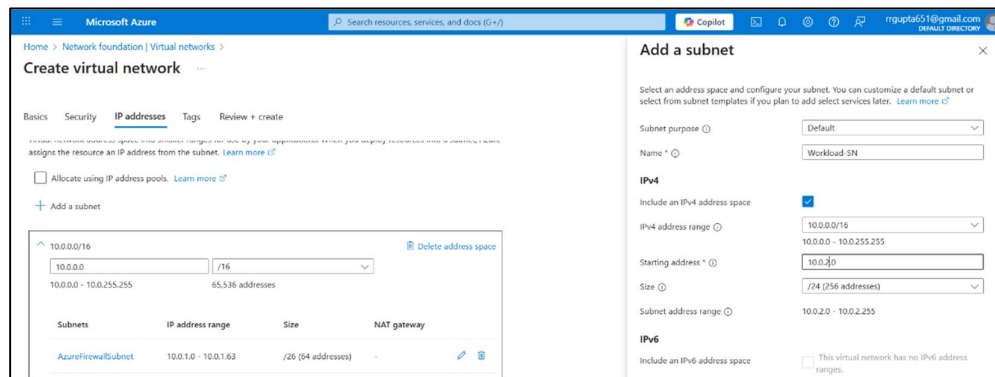
Implementation Steps

1. Create Resource Group: In Azure Portal, create a new resource group named **Test-FW-AR**



2. Create Virtual Network and Subnets

Create a VNet named **AR-VN**, Add two subnets: **AzureFirewallSubnet** → required for the firewall. **Workload-SN (10.0.2.0/24)** → where the workload VM will run. Deploy firewall named **AR-FW** inside **AzureFirewallSubnet**. Assign a new public IP (**ar-fw-pip**) for external access

Subnets	IP address range	Size	NAT gateway
AzureFirewallSubnet	10.0.1.0 - 10.0.1.63	/26 (64 addresses)	-
Workload-SN	10.0.2.0 - 10.0.2.255	/24 (256 addresses)	-

3. Create Workload Virtual Machine

Deploy a Windows Server 2019 VM named **AR-Srv-Work** in **Workload-SN** subnet. Do not assign a public IP (traffic should go via firewall).

4. Configure Route Table

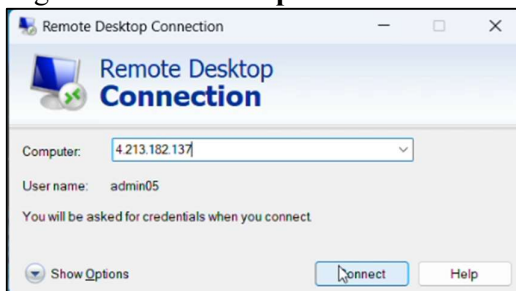
- Create a Route Table named **AR-FW-Routes**.
- Add a default route (0.0.0.0/0) with **next hop = firewall private IP**.
- Associate this route table only with **Workload-SN**.

5. Add Firewall Rules

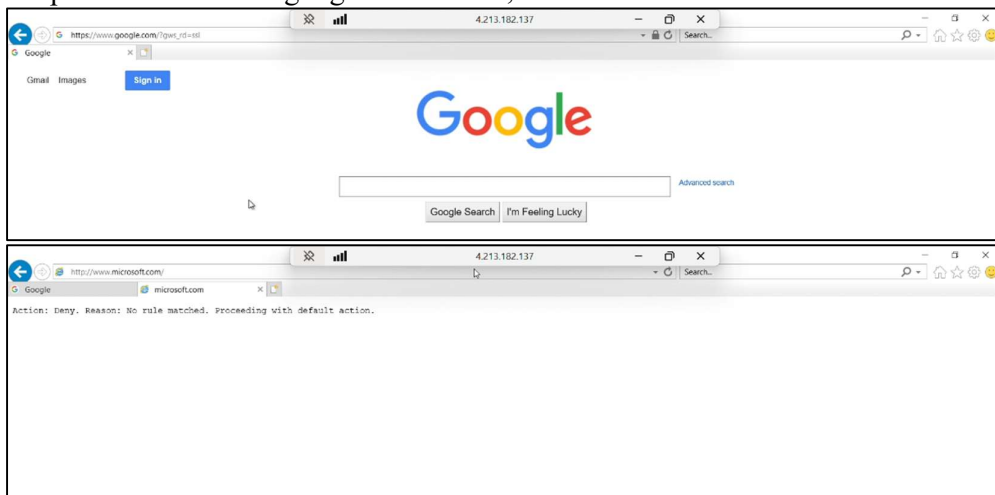
- **Application Rule** → Allow outbound HTTP/HTTPS to www.google.com.

7. Testing

- Connect to VM using **RDP via firewall public IP**.



- Open browser: www.google.com works, but www.microsoft.com is blocked.



Learning Outcomes:

LO1: Learned how to deploy and configure Azure Firewall to control inbound & outbound traffic in a Virtual Network.

LO2: Understood the use of Application, Network, & NAT rules with example to secure workloads.

Course Outcomes: how to apply **cloud security in Azure** using firewall rules and routing.

Result & Discussion:

Conclusion:

For Faculty Use

Correction Parameters	Formative Assessment [40%]	Timely completion of Practical [40%]	Attendance / Learning Attitude [20%]	
Marks Obtained				