# GUVI'S CLOUD COMPUTING USING MICROSOFT AZURE

## NAME : MS SIDDHARTHA

## Project 3: Design a Azure Micro-Segmentation Architecture:

## 1. Executive Summary

This project aims to enhance security within an Azure Virtual Network (VNet) through micro-segmentation and the implementation of Azure Firewall. The primary objectives include dividing the VNet into security-focused segments, enforcing strict access control policies, and integrating advanced security features like Azure Firewall and optional Application Security Groups (ASGs).

## 2. Introduction

- Project Background: The importance of network security in a cloud environment cannot be overstated, as it is crucial to minimize the attack surface and control traffic flow within VNets. This project focuses on achieving these goals through the design and implementation of a robust micro-segmentation architecture.
- Scope of Work: The scope of this project includes the design and implementation of micro-segmentation within an Azure VNet, the deployment of a centralized Azure Firewall for managing network traffic, and the optional implementation of Application Security Groups (ASGs) for further security refinement.

## 3. Network Architecture Design

### VNet Segmentation:

- Design Considerations: The VNet is divided into smaller, security-focused segments based on workload type or function. These segments ensure minimal inter-segment communication, thereby reducing the potential attack surface.
- Subnet and NSG Configuration: Subnets are created within the VNet, each governed by its own Network Security Group (NSG). These NSGs enforce strict access control policies at the subnet level, ensuring that only authorized flows are allowed between segments.

### Network Security Groups (NSGs):

- Access Control Policies: NSGs enforce specific access control policies, including rules for inbound and outbound traffic. These rules are tailored to minimize unauthorized access.

- Security Rule Implementation: NSG rules are carefully defined and prioritized to ensure that only authorized communications are allowed between different segments of the network.

## 4. Azure Firewall Implementation

- Centralized Traffic Management: A central Azure Firewall is configured to manage all inbound and outbound traffic for the VNets.
- Firewall Policies: Granular access control rules are defined within Azure Firewall, including specifics on source, destination, ports, and protocols.

### Security Feature Integration:

- Web Application Firewall (WAF): WAF is integrated with Azure Firewall to protect web applications from common attacks such as SQL injection and cross-site scripting (XSS).
- Intrusion Detection/Prevention Systems (IDS/IPS): IDS/IPS monitor network traffic, detect potential threats, and prevent unauthorized access.

## 5. Application Security Groups (ASGs):

### ASG Deployment

- Purpose: ASGs provide an additional layer of security for specific application instances within a subnet.
- Granular Access Control: ASGs are used to refine access control, focusing on individual application ports and protocols.

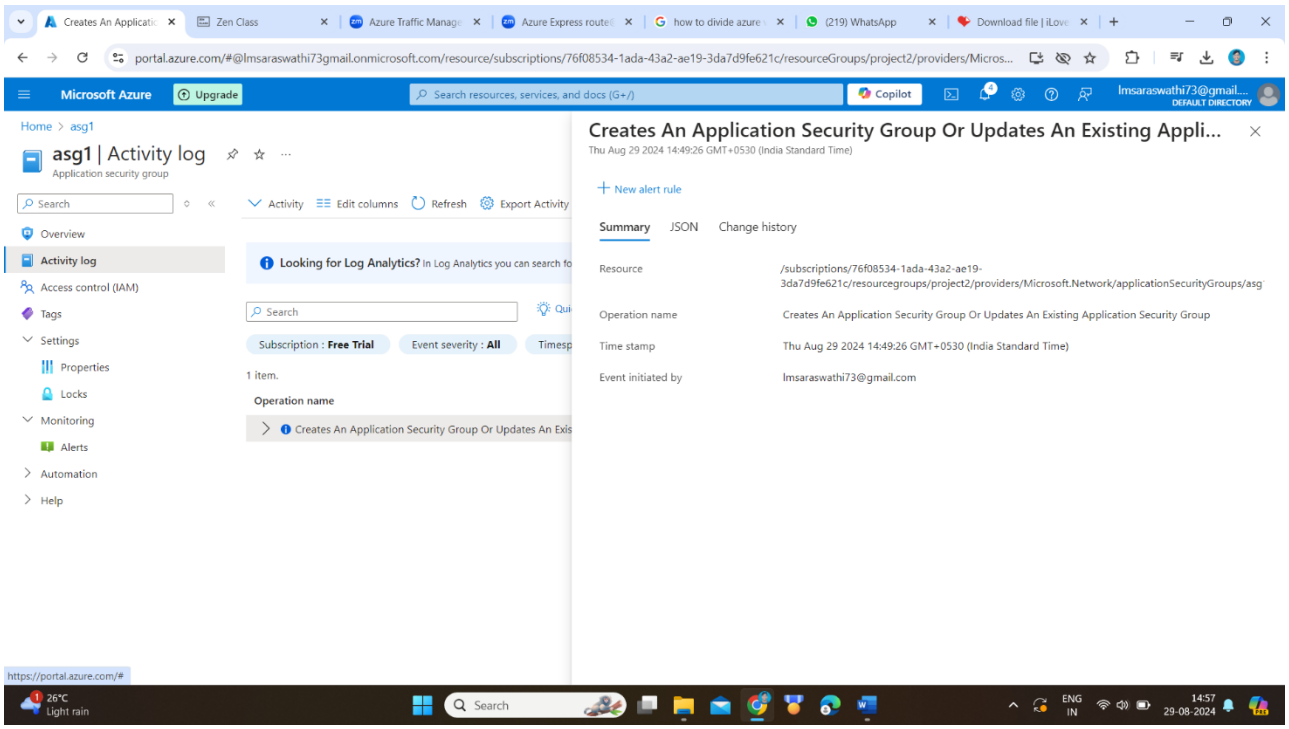



**Fig 1.1: Application Security Groups (ASGs)**

## Autoscaling

Enable autoscaling to automatically adjust the number of backend instances based on traffic demands.

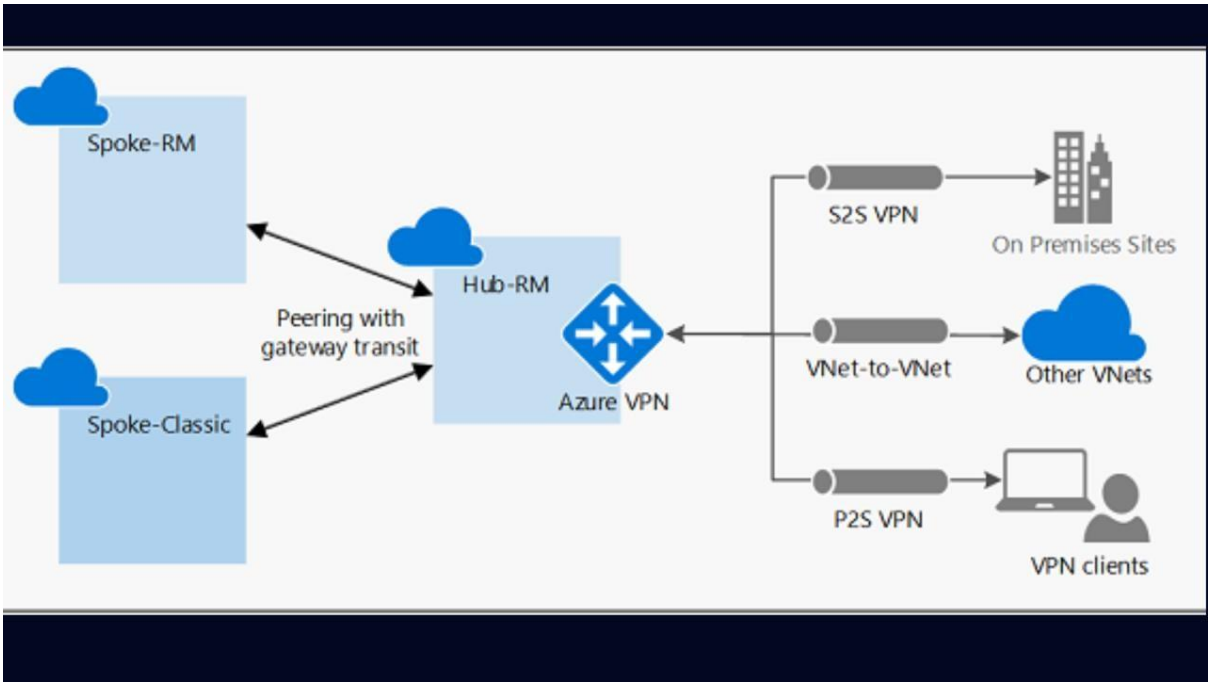



**Fig 1.2: Application Gateway Configuration**

## Multi-Tier Application Architecture

- **Web Frontend Tier:** Deploy web servers in the Web Frontend VNet. Use public and private subnets for better security.
- **Business Logic Layer:** Deploy API servers and business logic components in the Business Logic VNet.
- **Database Tier:** Deploy database servers in the Database VNet. Ensure restricted access to the database tier.
- **VNet Peering:** Implement VNet peering to enable communication between VNets while maintaining isolation.

# Design a Micro Segmentation Architecture:

## 1. Divide your Azure virtual network (VNet) into smaller, security- focused segments based on workload type or function:

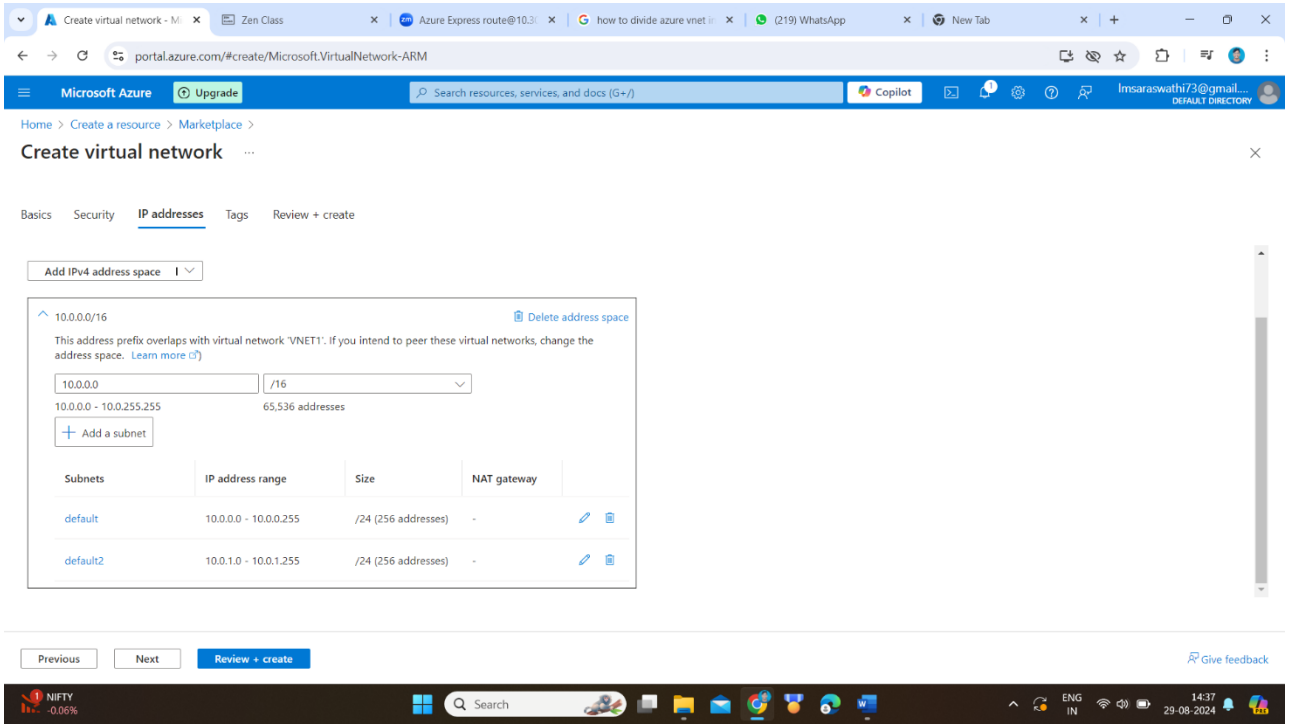



**Fig 1.3: Dividing VNET into smaller with additional Subnets**

## 2. Utilize Network Security Groups (NSGs) to enforce strict access control policies at the subnet level within the Vnet:

- Security admin rules and network security groups (NSGs) can be used to enforce network security policies in Azure. However, they have different scopes and priorities.
- Security admin rules are intended to be used by network admins of a central governance team, thereby delegating NSG rules to individual application or service teams to further specify security as needed. Security admin rules have a higher priority than NSGs and are evaluated before NSG rules.
- NSGs, on the other hand, are used to filter network traffic to and from individual subnets or network interfaces. They're intended to be used by individual application or service teams to further specify security as needed. NSGs have a lower priority than security admin rules and are evaluated after security admin rules.

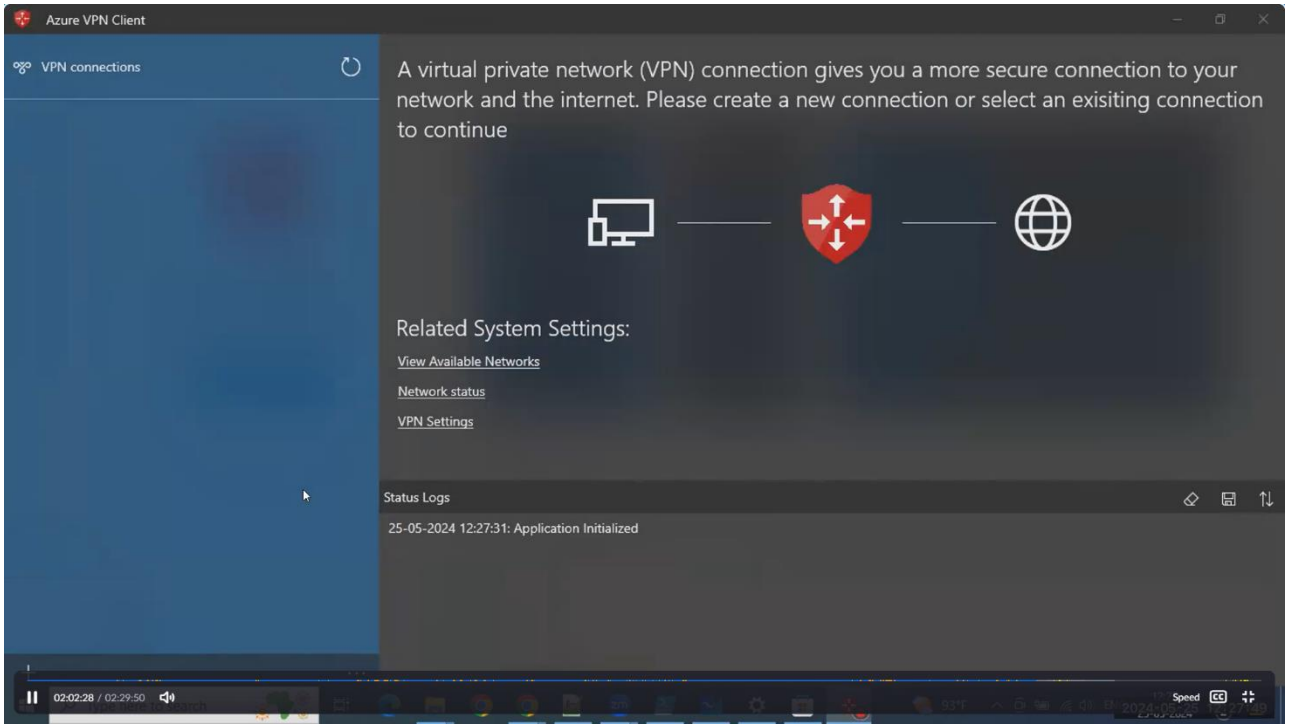



**Fig 1.4: Secure Connection for VPN and NSGs with Azure VPN cloud**

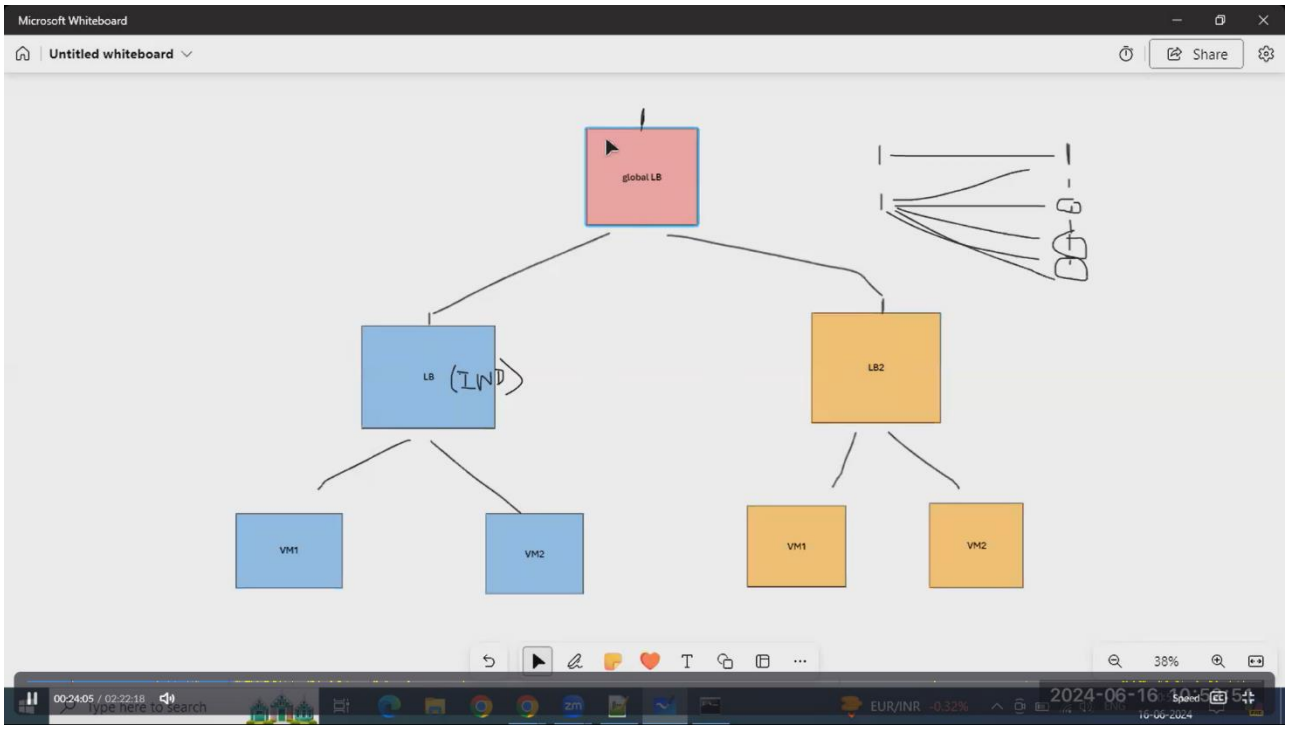
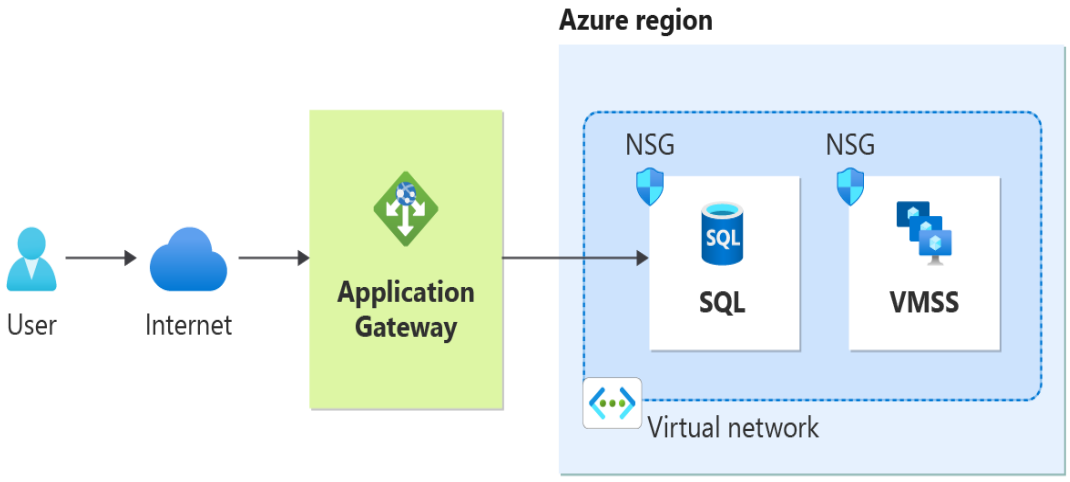
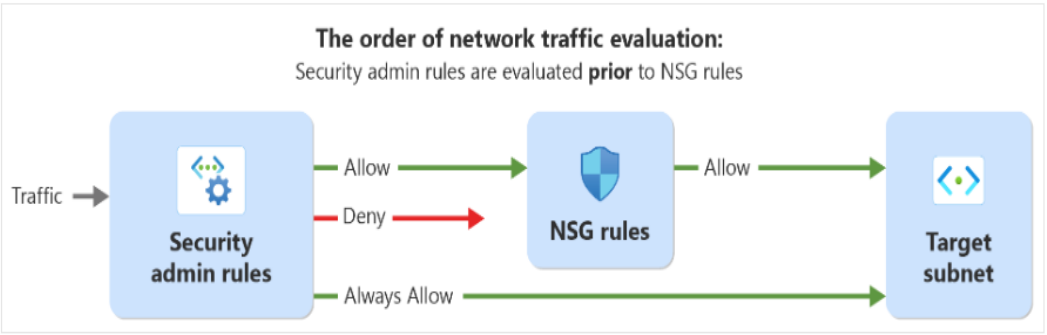



**Fig 1.5: Blueprint to ensure control policies of Azure NSGs**

## 3. Limit communication between segments only to authorized flows, minimizing the attack surface:




| Rule Type | Target Audience | Applied On | Evaluation Order | Action Types | Parameters |
|---|---|---|---|---|---|
| Security admin rules | Network admins, central governance team | Virtual networks | Higher priority | Allow, Deny, Always Allow | Priority, protocol, action, source, destination |
| Network security group rules | Individual teams | Subnets, NICs | Lower priority, after security admin rules | Allow, Deny | Priority, protocol, action, source, destination |

**Fig 1.6: Security and Admin Rules**

# MICRO-SEGMENTATION

- Microsegmentation is a security method of managing network access between workloads. With microsegmentation, administrators can manage security policies that limit traffic based on the principle of least privilege and Zero Trust. Organizations use microsegmentation to reduce the attack surface, improve breach containment and strengthen regulatory compliance.
- Microsegmentation refers to an approach to security that involves dividing a network into segments and applying security controls to each segment based on the segment's requirements.
- Microsegmentation software with network virtualization technology is used to create zones in cloud deployments. These granular secure zones isolate, securing them individually with custom, workload-specific policies. Similarly, each virtual machine (VM) in a network can be protected, down to the application level, with exact security controls.
- The granular security controls microsegmentation brings to workloads or applications is invaluable for the modern cloud environment with several applications running on the same server or virtual machine. Organizations can apply security controls to individual workloads and applications, rather than having a one security policy for the server.

**Network Segmentation Challenges:**

Network segmentation is an approach that divides a network into multiple smaller segments. This benefits performance and security:

**Performance:** Subdividing the network into smaller subnets and VLANs reduces the scope of broadcast packets and improves network performance.

**Security:** Network security teams can apply access control lists (ACLs) to VLANs and subnets to isolate machines on different network segments. In the event of a data breach, ACLs can prevent the threat from spreading to other network segments.

Leveraging network segmentation for security purposes comes with challenges. Segmentation needs don't always match the network architecture. Re-architecting the networks or reconfiguring VLANs and subnets to meet segmentation requirements is difficult and time consuming.

## How Micro-Segmentation Works:

Microsegmentation, also referred to as Zero Trust or identity-based segmentation, delivers on segmentation requirements without the need to re-architect. Security teams can isolate workloads in a network to limit the effect of malicious lateral movement. Microsegmentation controls can be assimilated into three categories:

**Agent-based solutions** use a software agent on the workload and enforce granular isolation to individual hosts and containers. Agent-based solutions may leverage the built-in host-based firewall or derive isolation abilities based on workload identity or attributes.

**Network-based segmentation** controls rely on the network infrastructure. This style leverages physical and virtual devices, such as load-balancers, switches, software-defined networks (SDN), and overlay networks to enforce policy.

**Native cloud** controls leverage capabilities embedded in the cloud service provider (e.g., Amazon security group, Azure firewall, or Google Cloud firewall).

Microsegmentation helps provide consistent security across private and public clouds alike by virtue of three key principles: visibility, granular security and dynamic adaptation.

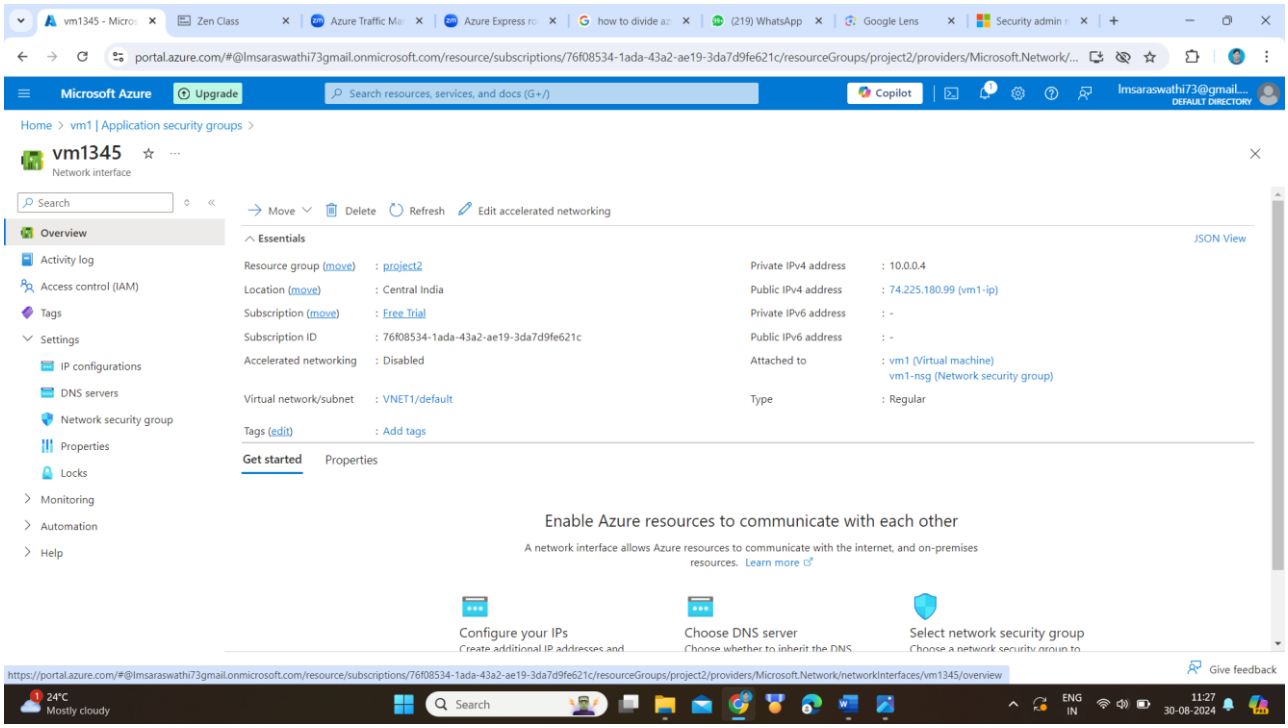



**Fig 1.7: Segmenting Network Interface**

## Benefits of Micro-Segmentation:

- **Reduced attack surface:** Microsegmentation provides visibility into the complete network environment without slowing development or innovation. Application developers can integrate security policy definition early in the development cycle and ensure that neither application deployments nor updates create new attack vectors. This is particularly important in the fast-moving world of DevOps.
- **Improved breach containment:** Microsegmentation gives security teams the ability to monitor network traffic against predefined policies as well as shorten the time to respond to and remediate data breaches.
- **Stronger regulatory compliance**: Using microsegmentation, regulatory officers can create policies that isolate systems subject to regulations from the rest of the infrastructure. Granular control of communications with regulated systems reduces the risk of noncompliant usage.
- **Simplified policy management:** Moving to a microsegmented network or Zero Trust security model provides an opportunity to simplify policy management. Some microsegmentation solutions offer automated application discovery and policy suggestions based on learned application behavior.
- **Separation of duties:** Separation of duties involves dividing responsibilities among multiple users to prevent any one user from having too much control over a system or process. This reduces the risk of fraud or errors and ensures that sensitive operations are performed by multiple users.
- **Regular access reviews:** Regular access reviews involve routinely reviewing user access rights and permissions to ensure they're still essential. Access reviews can help to identify and remove unnecessary access rights, reducing the risk of unauthorized access.

# IMPLEMENT AZURE FIREWALL:

# 4. Configure a central Azure Firewall to manage all inbound and outbound network traffic for your VNets.

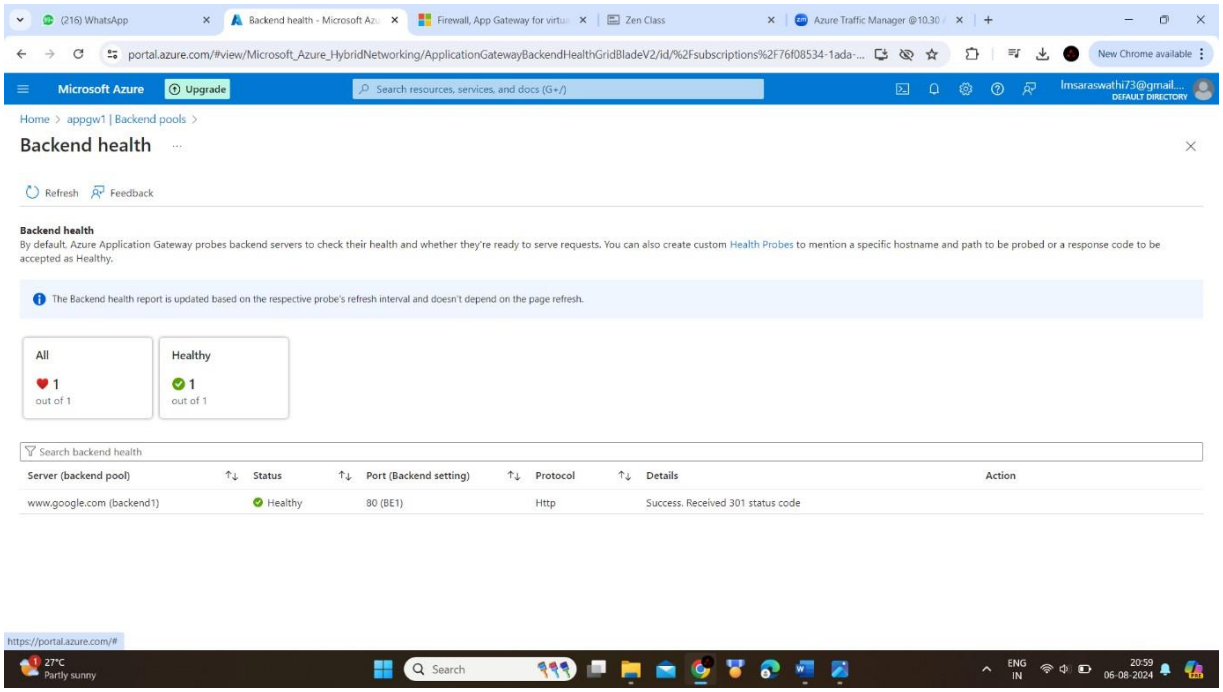



**Fig 2.1: Backend health check**

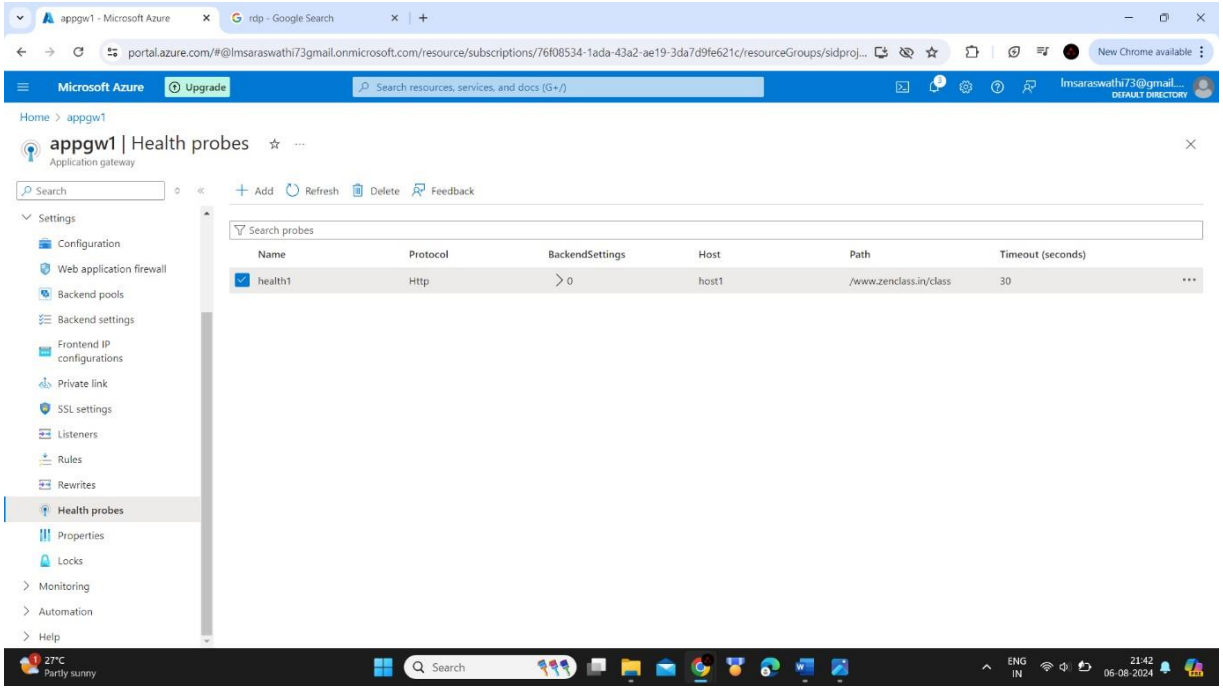



**Fig 2.2: Checking of health probes**

# Application Gateway Framework:

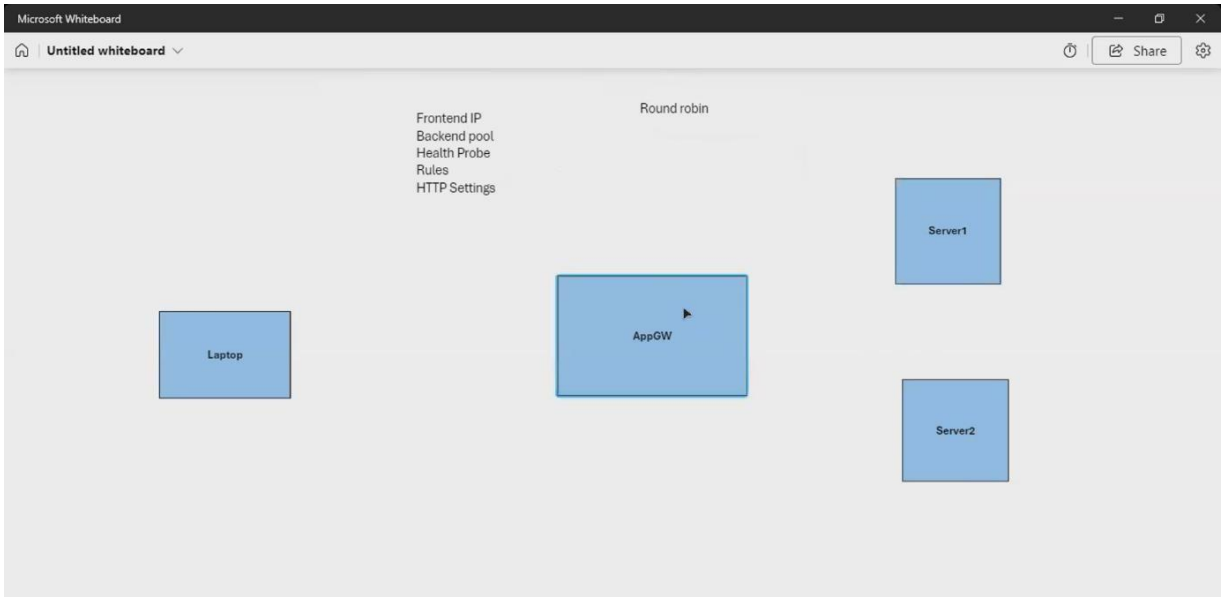
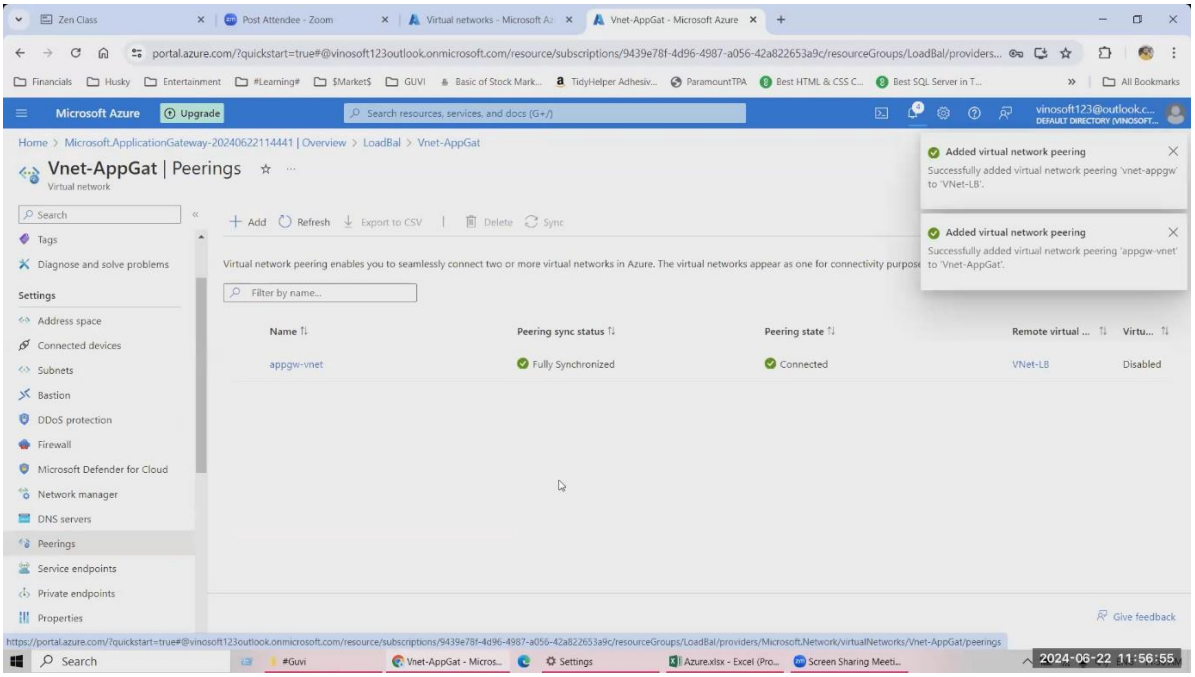



**Fig 2.3: AppGw Framework**

# 1. Application gateway network which is associated with Backend pool:



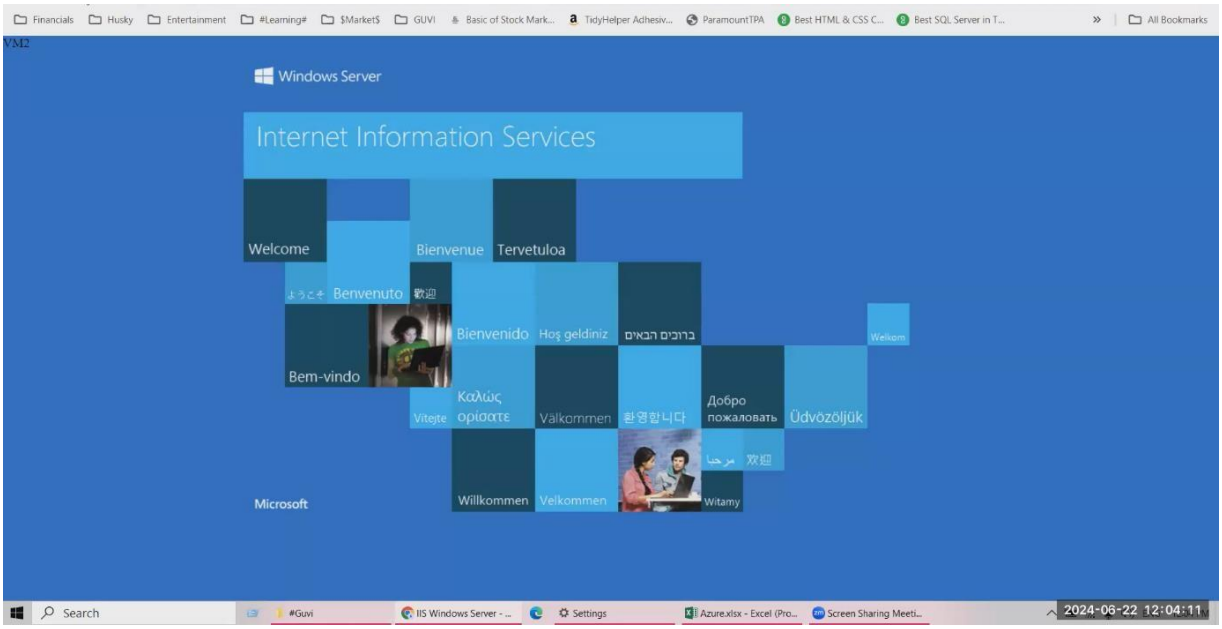



**Fig 2.4: AppGw Created Successfully**

# 5. Integrate security features like web application firewalls (WAF) and intrusion detection/prevention systems (IDS/IPS) for enhanced protection:

## 1. Web Application Firewall (WAF) rules for enhanced security and protection against common attacks:

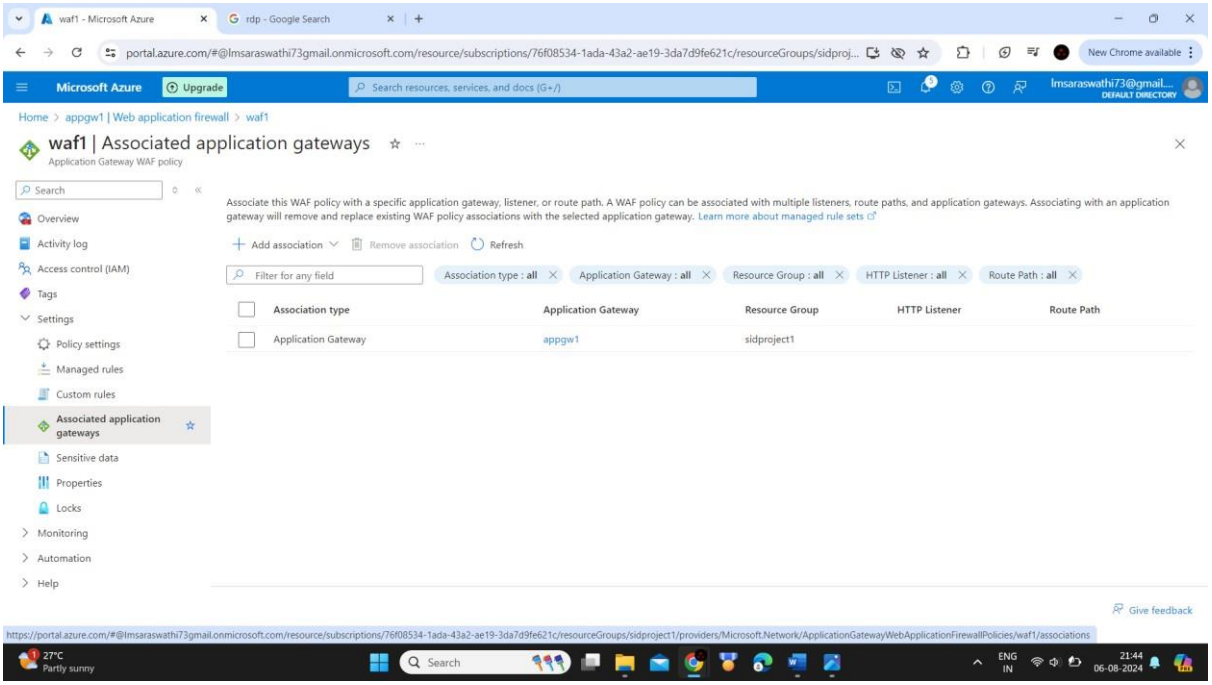



**Fig 2.5: WAF Created**

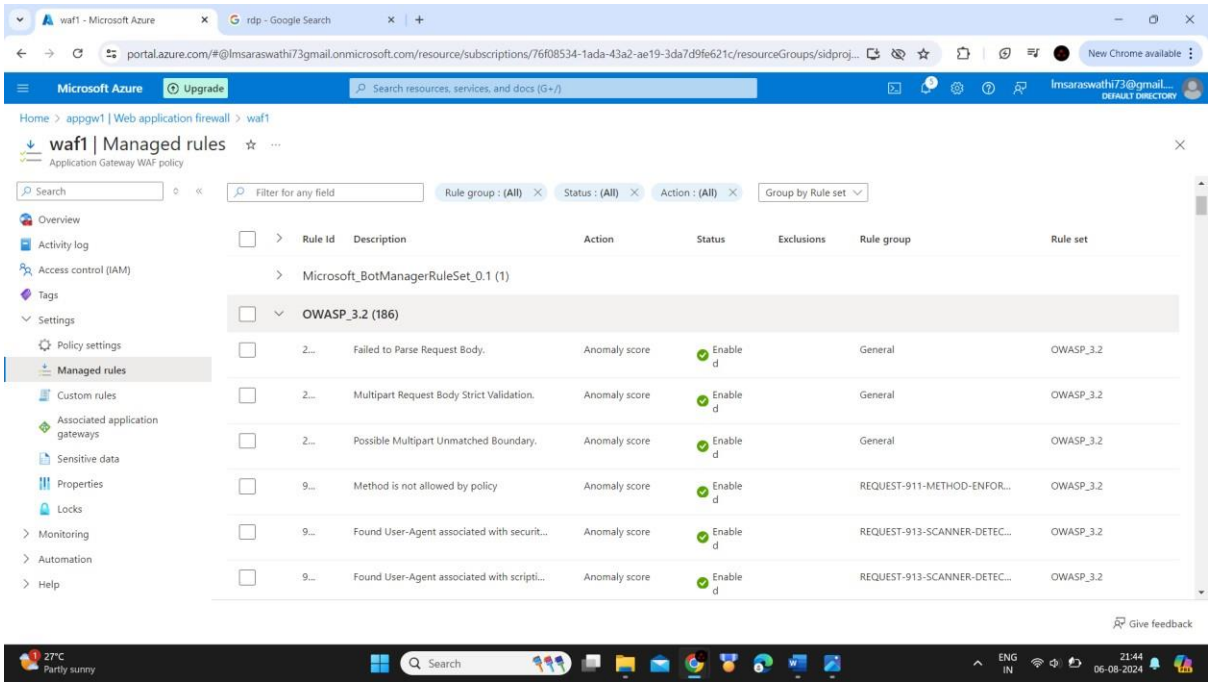



**Fig 2.6: WAF Rules for enhanced Security**

## 6. Configure Application Security Groups (ASGs) (Optional): Introduce an additional layer of security by deploying ASGs for specific application instances within a subnet:

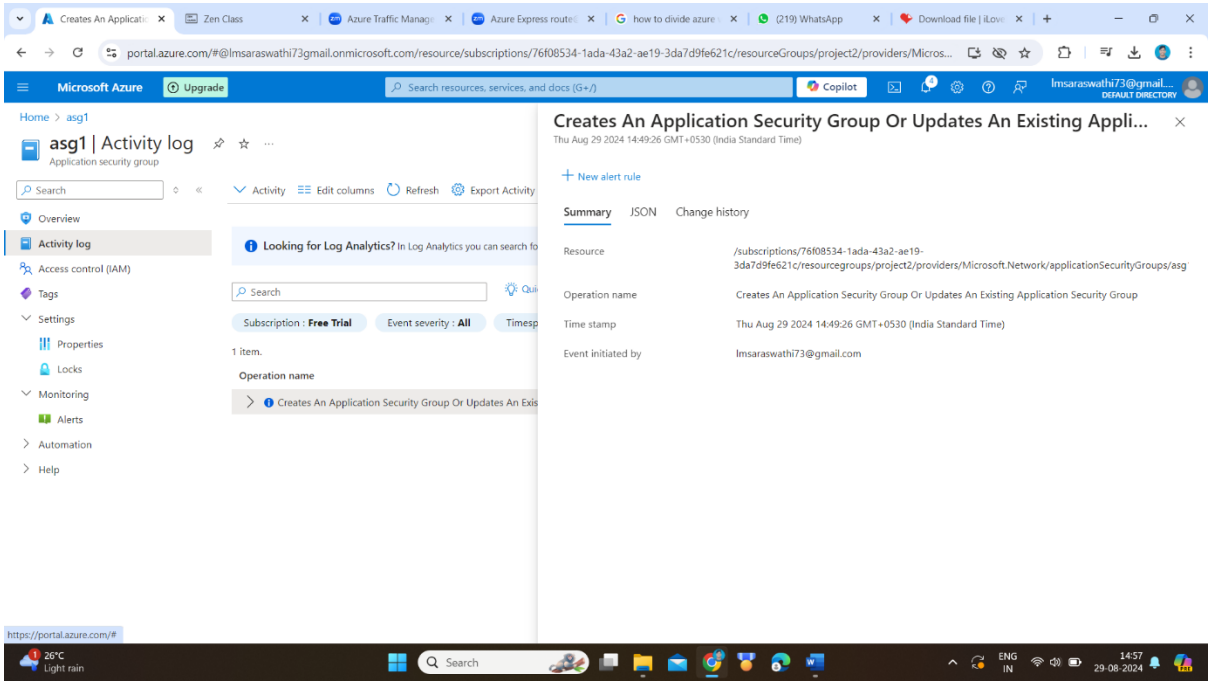



**Fig 2.7: Created ASGs**

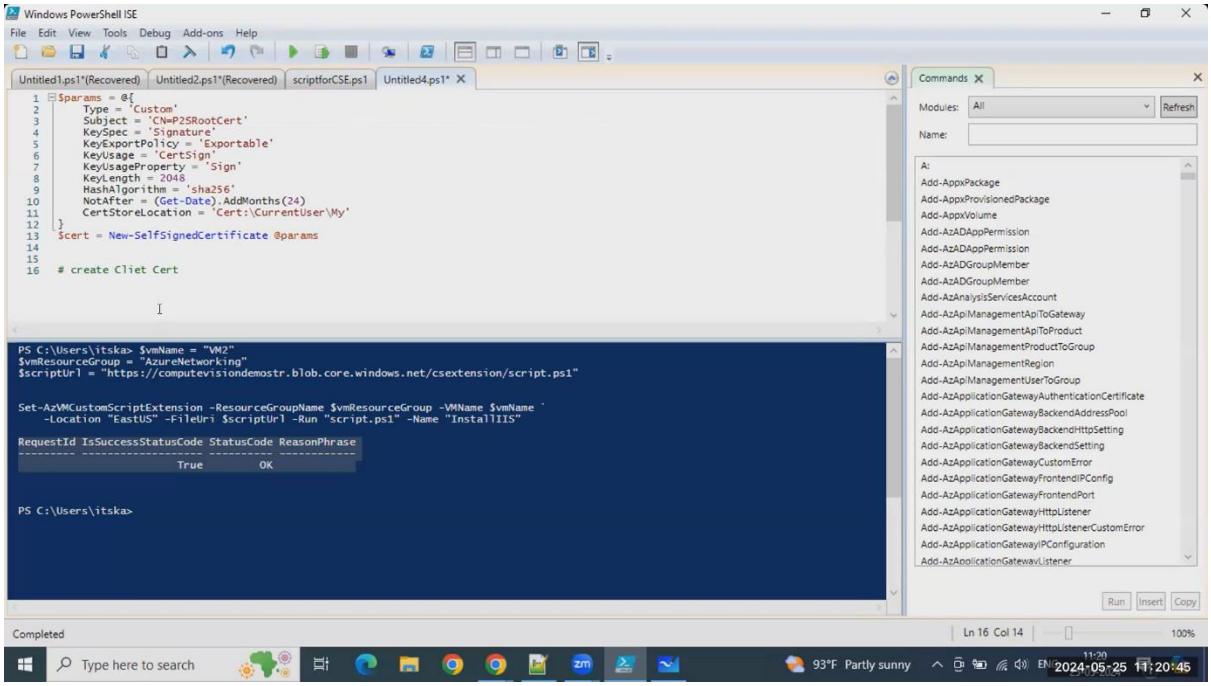
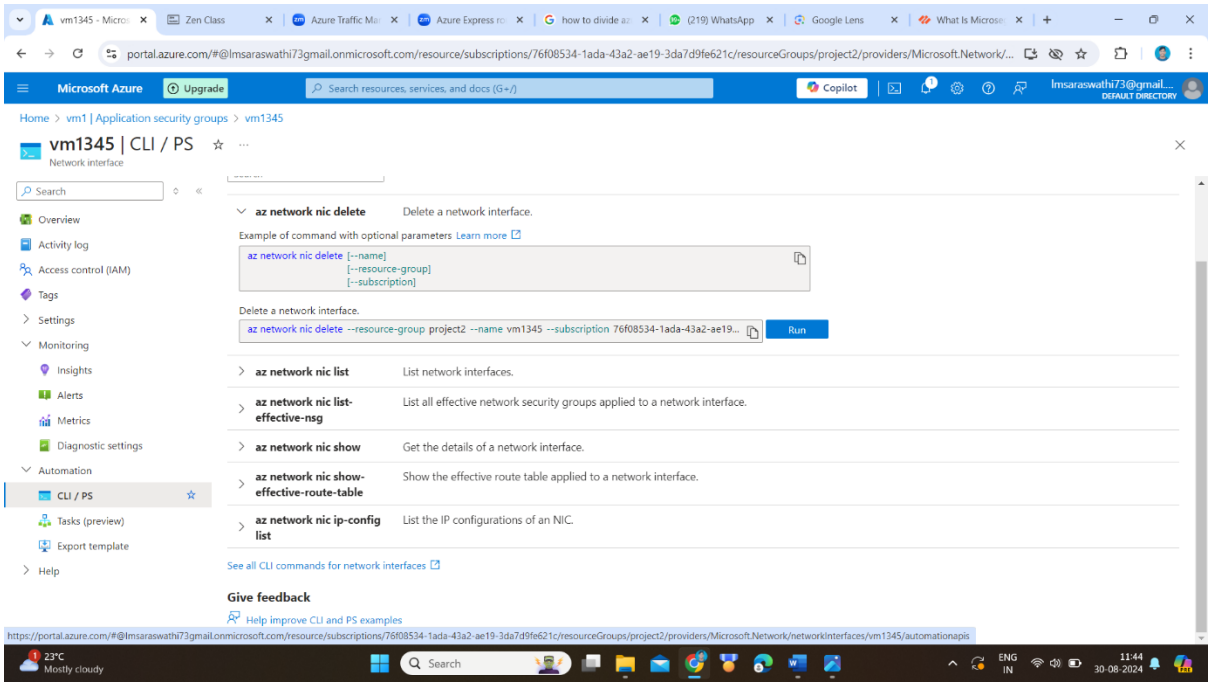



**Fig 2.8: Configuring ASGs**

# WAF Policies and Custom rules:



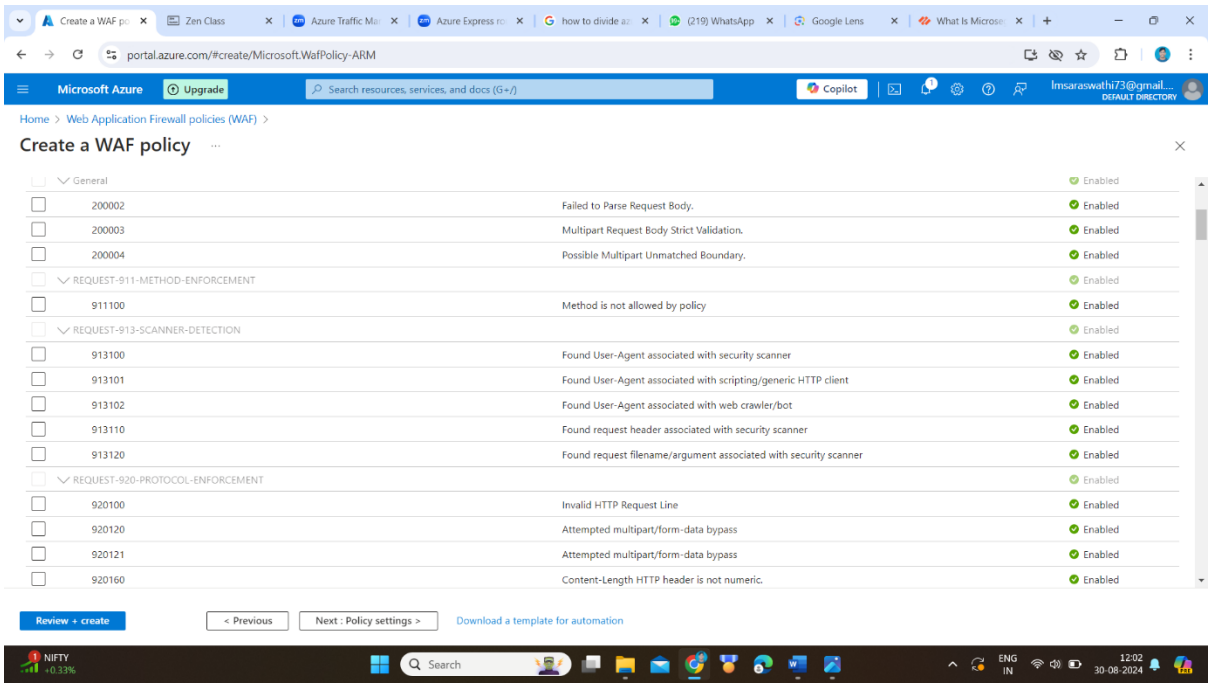



**Fig 2.9: WAF policies**

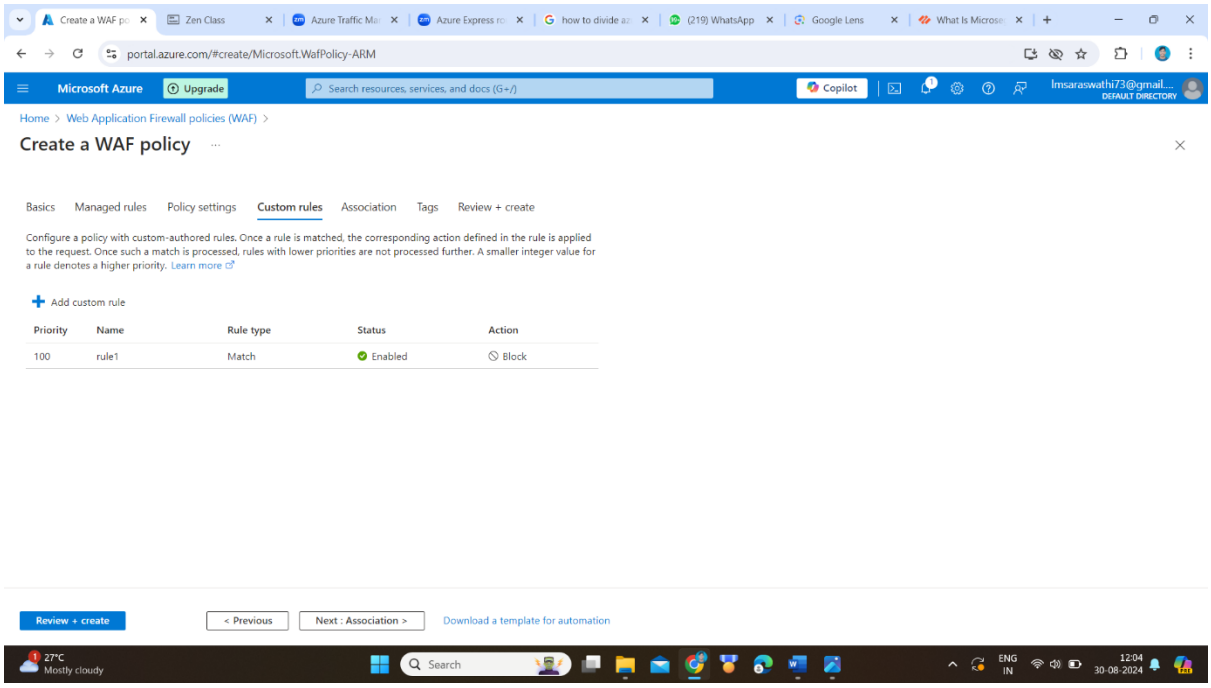



**Fig 2.10: WAF Custom Rules**

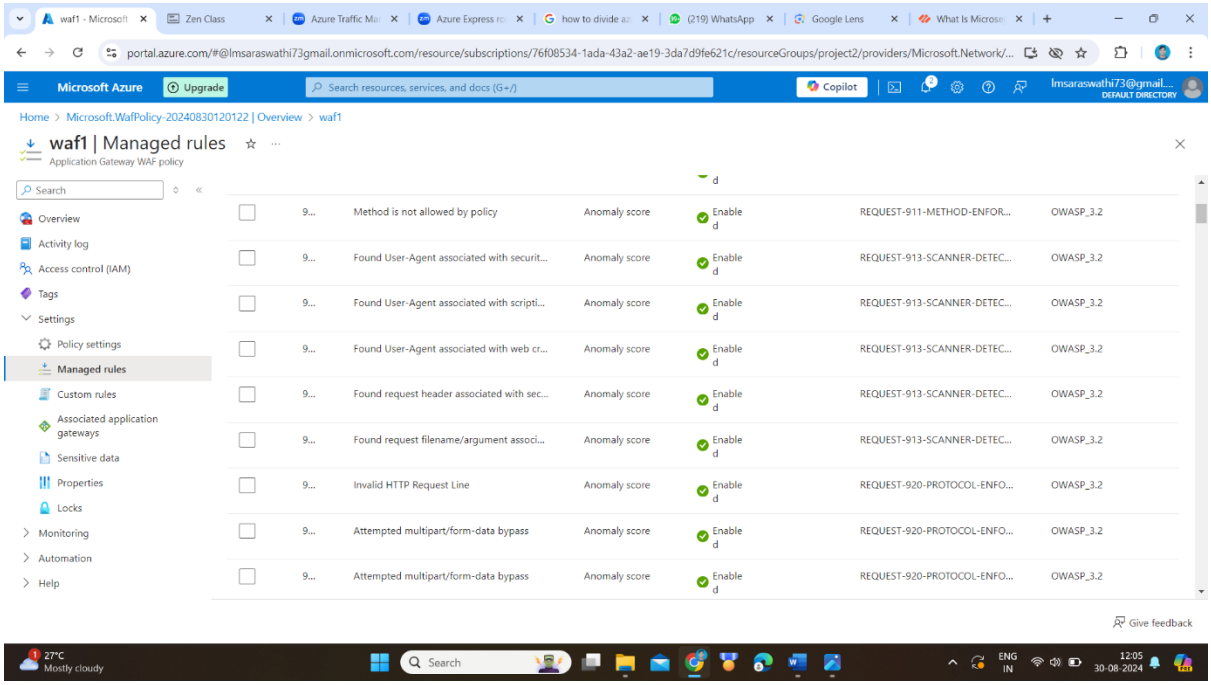



**Fig 2.11: WAF Managed Policies and rules**

## 7. Security Considerations and Best Practices

- Minimizing Attack Surface: Strategies for minimizing the attack surface include limiting inter-segment communication and enforcing the principle of least privilege.
- Monitoring and Logging: The importance of monitoring and logging network traffic is emphasized, with tools like Azure Monitor and Log Analytics being used for continuous oversight.
- Compliance and Regulatory Requirements: Compliance and regulatory requirements that impact the design and implementation of this architecture are addressed.

## 8. Conclusion

The proposed architecture enhances security within the Azure environment through micro-segmentation, the implementation of Azure Firewall, and optional ASG deployment. The Azure Micro-Segmentation Architecture project successfully addresses the critical need for enhanced network security within cloud environments, particularly within an Azure Virtual Network (VNet). By implementing a micro-segmentation approach, this project minimizes the attack surface, enforces stringent access control policies, and ensures that only authorized communication occurs between different segments of the network. This layered security strategy is crucial in protecting sensitive workloads and maintaining the integrity of the network.

Key Achievements:

**1. VNet Segmentation:**

The project successfully divided the Azure VNet into smaller, security-focused segments based on workload type and function. Each segment is isolated, reducing the risk of lateral movement by potential attackers. This segmentation ensures that even if a breach occurs within one segment, the impact on other segments is minimized.

**2. Network Security Groups (NSGs):**

NSGs were meticulously configured to enforce strict access control at the subnet level. These NSGs play a pivotal role in defining and enforcing policies that govern which traffic is allowed to enter and exit each segment. The careful prioritization and implementation of NSG rules ensure that only necessary and authorized traffic flows between segments, thereby maintaining a high level of security.

**3. Azure Firewall Integration:**

The deployment of a central Azure Firewall further strengthens the security posture by managing all inbound and outbound traffic for the VNets. The firewall's ability to define granular access control rules based on source, destination, ports, and protocols adds an additional layer of defense. The integration of advanced security features, such as Web Application Firewall (WAF) and Intrusion Detection/Prevention Systems (IDS/IPS), provides comprehensive protection against a wide range of threats, including common web attacks and unauthorized access attempts.

**4. Application Security Groups (ASGs):**

Although optional, the implementation of ASGs offers another level of security by refining access control for specific application instances within a subnet. This approach is particularly useful in scenarios where more granular control is required over individual application ports and protocols, further minimizing the risk of unauthorized access to critical applications.

## 9. Challenges and Considerations:

- While the architecture provides robust security, it is essential to continuously monitor and update the network configurations to address evolving threats. The complexity of managing multiple NSGs, firewall rules, and ASGs requires ongoing attention and expertise. Additionally, the organization should remain vigilant about ensuring that all segments and policies are aligned with business objectives and compliance standards.

- In conclusion, the Azure Micro-Segmentation Architecture project represents a significant advancement in securing cloud-based networks. By leveraging Azure's native security tools and adopting a proactive, segmented approach to network design, the organization can confidently protect its critical assets while maintaining the flexibility to scale and adapt to future needs.

## 10. Moving forward, it is recommended to:

- **Conduct thorough testing of the implementation to ensure that all security policies and configurations are functioning as intended.**
- **Refine access control rules based on real-world usage patterns and emerging threats.**
- **Implement continuous monitoring and logging to detect and respond to any potential security incidents in real-time.**
- **Perform regular security assessments and audits to maintain compliance with industry standards and best practices.**