Week-7 | Azure Networking Demo | Azure VNet, Firewall, NSG, and Bastion

Introduction

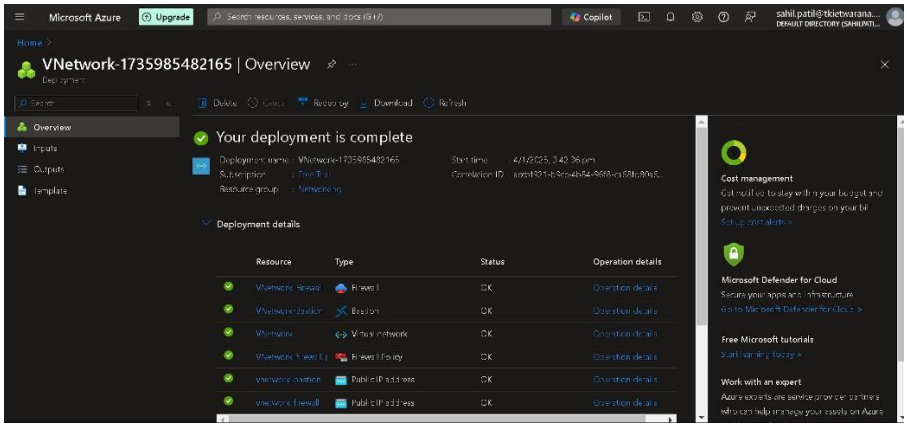
Azure networking is a crucial aspect of cloud infrastructure that ensures secure, scalable, and efficient communication between resources. This guide explores the practical implementation of key networking components in Azure, including Virtual Networks (VNets), Firewalls, Network Security Groups (NSG), and Bastion for secure VM access.

1. Azure Virtual Network (VNet) and Subnets

Azure Virtual Network (VNet) is the fundamental building block for networking in Azure. It allows different Azure resources to communicate securely. Subnets help segment the network for better security and traffic management.

Key Steps in VNet Creation:

1. **Create a Virtual Network (VNet):**
    - Define the address space for the VNet. ○
    - Name the VNet appropriately.



2. **Configure Subnets:**
    - A VNet can have multiple subnets. ○ Subnets are used to segment resources like web applications, databases, and firewalls.
    - Each subnet has its own network policies and security settings.
3. **Deploy Resources in the Subnet:**
    - Virtual Machines (VMs), Azure Kubernetes Service (AKS), and other resources are deployed within subnets.
    - Subnets can be private or public based on requirements.

---

2. Azure Firewall and Security Rules

Azure Firewall is a managed security service that helps protect cloud environments by filtering traffic and enforcing security rules.

Firewall Setup:

- Configure a firewall within a dedicated subnet.
- Define firewall policies to allow or deny traffic.
- Assign public and private IP addresses to the firewall.

Firewall Rules:

- **Network Rules:** Controls traffic between different networks.
- **Application Rules:** Filters traffic based on Fully Qualified Domain Names (FQDN).
- **NAT Rules:** Allows external users to access internal resources securely.

---

3. Network Security Groups (NSG)

NSGs act as a virtual firewall at the subnet or NIC level to control inbound and outbound traffic.

NSG Key Features:

- **Inbound Rules:** Control traffic entering a subnet or VM.
- **Outbound Rules:** Control traffic leaving a subnet or VM.
- **Priority-Based Rules:** Lower priority numbers are processed first.

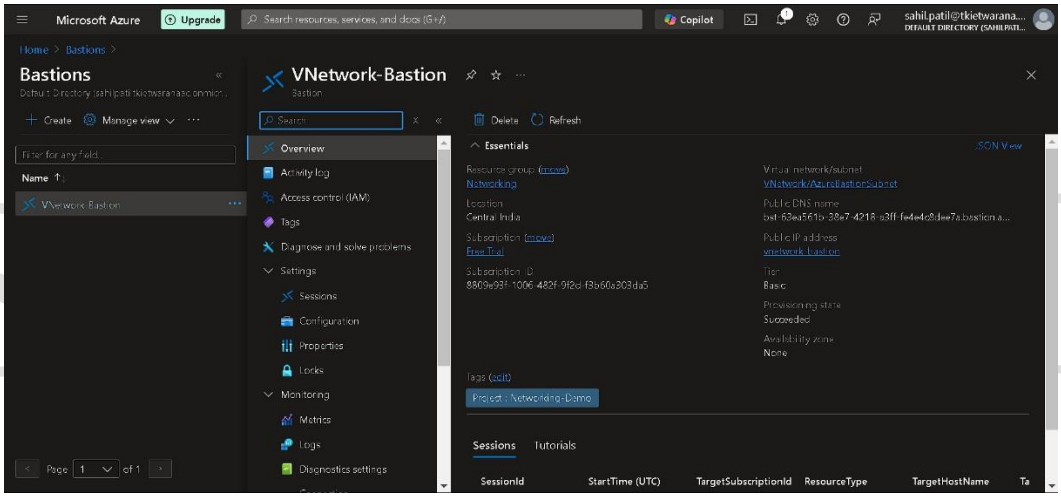
NSG Best Practices:

- Apply NSGs at both subnet and individual resource levels.
- Use Deny-All as the last rule to block unwanted traffic.
- Allow only necessary ports to limit exposure.

---

4. Azure Bastion for Secure VM Access

Azure Bastion provides secure RDP/SSH access to virtual machines without exposing them to the public internet.



Benefits of Bastion:

- Eliminates the need for a public IP on VMs.
- Prevents brute-force attacks on remote desktop connections.
- Fully managed service with built-in security controls.

Bastion Configuration:

- Enable Bastion for the VNet.
- Assign Bastion a public IP for administrative access.
- Use Azure Portal to access VMs securely via Bastion.

---

5. NAT Configuration for Secure Application Access

Network Address Translation (NAT) allows secure external access to internal applications by mapping external IPs to internal resources.

NAT Policy Implementation:

1. Assign a public IP to the firewall.
2. Configure NAT rules to translate external requests to internal resources.
3. Define access control lists to restrict unwanted traffic.

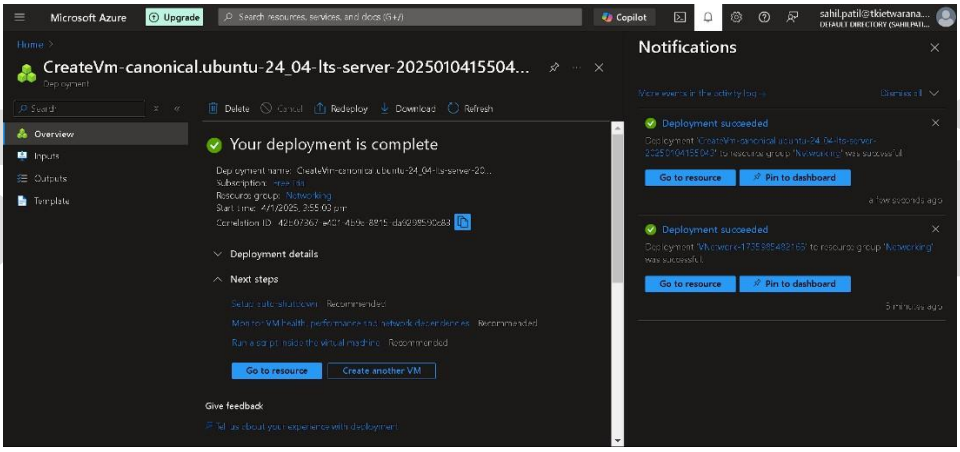
---

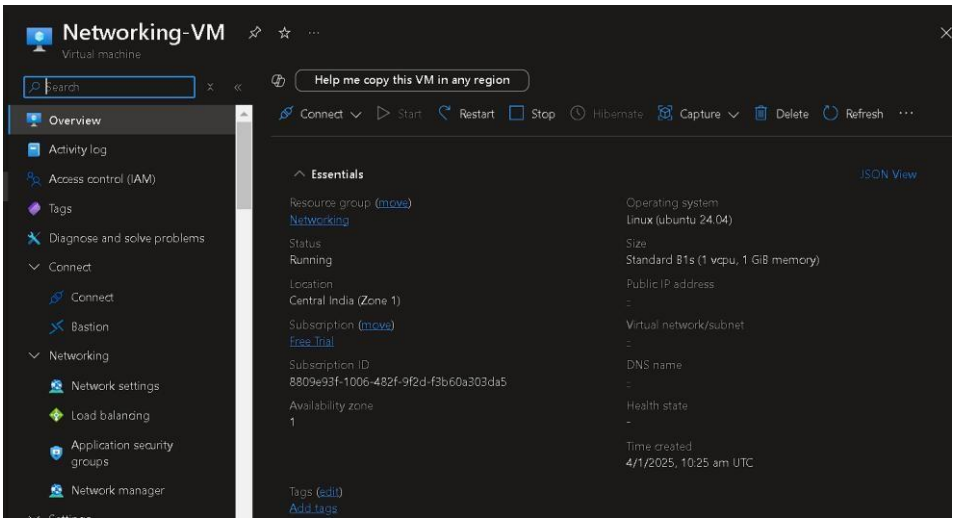
6. Web Application Deployment in a Secure Environment

After setting up networking components, a sample web application is deployed inside a secure subnet.

Deployment Steps:

1. **Provision a Virtual Machine (VM):**
   - Deploy an Azure VM in the web application subnet.
   - Assign a private IP (no public IP for security).

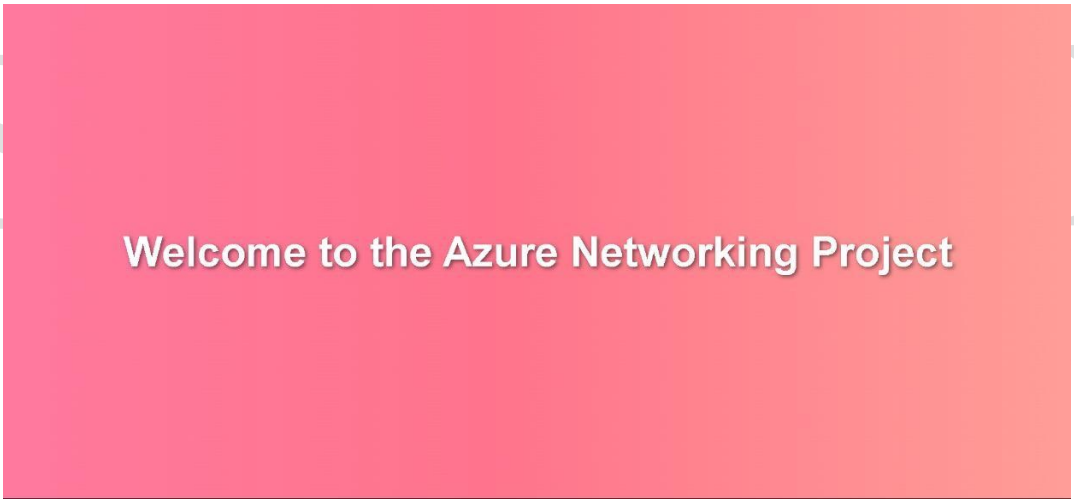




2. **Install and Configure Web Server:**

- Install Nginx or Apache to serve a static HTML page.
- Set up firewall and NSG rules to allow controlled access.

3. **Test Access via Firewall Public IP:**
   - Use the firewall's NAT policy to access the application.
   - Ensure only authorized IPs can reach the web application.



---

7. Best Practices for Azure Networking Security

- **Minimize public exposure:** Use private IPs and Bastion instead of public IPs.
- **Implement layered security:** Combine NSG, Firewall, and Bastion for enhanced security.
- **Regularly review and update security rules:** Ensure only necessary access is allowed.
- **Monitor network traffic:** Use Azure Monitor and Security Center for insights.

Conclusion

By combining VNets, Firewalls, NSGs, and Bastion, Azure provides a robust networking environment that balances security and accessibility. Following best practices and implementing proper configurations ensures that applications and infrastructure remain secure while maintaining operational efficiency.