VNet – Logical Isolation of the azure cloud dedicated to your subscription

VNNets has own CIDR block

VNets must not overlap

All resources in VNet can communicate outbound to the internet by default

To communicate inbound, you need public IP or Public Load Balancer.

Communicate between Azure Resources

1. VNet Peering
2. VNet Service Endpoints – (connect to SQL DB and Storage Accounts)
3. VNets

Services and VMs within a VNet can communicate directly securely with each other in cloud

Communicate between on premise

1. Point to Site VPN
2. Site to Site VPN
3. Azure Express Route

Filtering Network Traffic between subnets

1. Virtual Firewall appliance
2. Gateways
3. Proxies
4. NAT services

Routing Network Traffic

Azure routes traffic between Virtual Networks, Subnets, On Prem networks and the Internet by default

You can also implement BGP and route tables to override default azure routes

You can create multiple Virtual networks per Region per Subscription

You can create multiple subnets within each virtual network

You cannot add the following address ranges in VNet

224.0.0.0/4 (Multicast)

255.255.255.255/32 (Broadcast)

127.0.0.0/8 (Loopback)

169.254.0.0/16 (Link-local)

168.63.129.16/32 (Internal DNS)

Azure Reserves first 4 and last IP – total 5 IP addresses within each subnet

For example, the IP address range of 192.168.1.0/24 has the following reserved addresses:

192.168.1.0 : Network address

192.168.1.1 : Reserved by Azure for the default gateway

192.168.1.2, 192.168.1.3 : Reserved by Azure to map the Azure DNS IPs to the VNet space

192.168.1.255 : Network broadcast address.

**Subnet Considerations**

Smallest supported IPV4 subnet is /29

Largest supported is /2

IPv6 must be /64

You can limit access to azure resources to specific subnets with a virtual network service endpoint

Control access to subnet using NSG. NSG contains rules which allow/deny traffic to and from source and

Destinations

You can associate 0 or 1 NSG each subnet in a VNet. 1 Subnet = 0 or 1 NSG

1 NSG can be applied to different subnets

A resource group must have resources with unique names.

Resources with same name can be created in another resource group

Subnets are scoped to VNets. Each subnet in a VNet must have unique name

In the Create virtual network tab, you can enable security features like BastionHost,

DDoSProtectionStandard, and Firewall.

Azure Bastion – PaaS Services provisioned inside the Virtual Network.

Seamless SSH and RDP connectivity to VM from portal over SSL  
 VMs do not need PIP when connecting from Bastion

DDoS -

|  |  |
| --- | --- |
| Standard | Basic |
| Paid service plan  Enhanced DDoS mitigation capabilities via adaptive tuning  Attack Notification Telemetry | Integrated into Azure  No cost |

Firewall – Managed cloud based network security service for Azure virtual network resources