Introduction to Virtual network

Introduction to Virtual network



A Virtual Network (VNet) is a logical representation of your network in the cloud.

Azure VNet

capabilities

Connect networks

Peer you virtual networks irrespective of where they are located.

Monitor network traffic

Use NSG logs and traffic analytics monitoring solution to monitor the network traffic.

Route network traffic

Use Route tables to configure user defined routes and propagate your on-premise routes to virtual networks.

Filter network traffic

Filter network traffic by using Network security groups, Application security groups, Azure firewall or NVA.

Isolation and segmentation

By virtue of deploying resources such as VMs into Virtual networks, they will be isolated from other resources. Use Subnets to further segment the same.

Communication with Internet

All resources in a virtual network can communicate outbound to the internet, by default.

Use Public IP or load balancer for inbound.

Communication between resources

Resources communicate securely via virtual network or virtual network service end points.

Communicate with on-premise resources

Communication with on-premise resources can be enabled via Point to Site VPN, Site to Site VPN or Express Route.

Subnets



- Subnet is a range of IP addresses in the VNet
- VNet can be divided into multiple subnets based on different design considerations
- VMs & PaaS services deployed to subnets (same or different) in the same VNet and can communicate with each other without any extra configuration
- Route tables, NSGs, Service end points and policies are configured to the subnets