Configure secure access to workload using azure networks

Existing Environment.

Given with

Resource Group - RG1lod46774409

Region - West Europe

VNet1	Subnet1-1	VM1
VNet2	Subnet2-1	VM2, VM3.

Configuration of Subnet1-1 to use azure firewall

Azure firewall will be used for Subnet1-1

VNet1 connect to third party Internet app Service. (PeleCloudData Service)

M T W T F S S

Relecloud Data Service - Accessible at 131.107.3.210 on TCP Port 9000.

Task.

→ To deploy Azure firewall

→ Allow access from Subnet 1-1 to Relecloud Data Service

→ Use Routetable to ensure that all other access from Subnet 1-1 to the public internet is blocked.

Prepare environment for deployment of VM4

To develop app (App1) that will be provisioned on virtual Machines in West Europe and North Europe.

→ App1 will be deployed to VM2 and VM3.

→ VM4 that will also host App1 will be deployed to the North Europe region.

Task.

→ Configure a Subnet to support the deployment of VM4.

The Subnet meet the requirements

① Be in North Europe Region

② Use an IP address Space of 10.3.1.0/24.

③ Host on the new Subnet can Communicate with host on the Same Virtual Network.

④ New Virtual Network is peered with VNet2

Configure DNS for reco Subnet

Task.

① Host on the reco Subnet automatically register to an Azure private DNS Zone named Contoso.com.

② Host on the reco Subnet can connect to VM2 on Subnet2-1 by using fully qualified Name (FQDN) of vm2.Contoso.com.

Configure Network Security.

Limit Inbound Traffic to Subnet1-1.

Task.

Create an application Security group that Contains VM2 and VM3.

→ Subnet1-1 only allows inbound connections

→ Subnet1-1 only allows inbound connections from members of the application security group over tcp port 1433.