

High-Level Solution Summary

Two virtual networks were created—one in the East US for the database tier and another in Southeast Asia for the application tier—each hosting a test VM. Azure Bastion was deployed in the East US VNet to provide secure access to VM1, since both VMs were configured without public IP addresses. VNet peering was established between the two VNets to enable private, region-to-region communication. Separate NSGs were applied to each VM's subnet/NIC, with rules permitting VM1-to-VM2 RDP, and ICMP traffic restricted between the two VMs. As Windows Server blocks ICMP by default, ping was enabled inside each VM through the Windows Firewall. Connectivity between the VNets will be validated by successfully pinging between the two VMs using their private IP addresses.

Solution steps :

- Create VNets in East US and Southeast Asia.
- Set up **VNet Peering** between the VNets.
- Deploy VMs in both VNets.
- Modify **NSG rules** to allow ICMP traffic (Ping) in both VM's, RDP from **HQ** to **Branch** VM
- **Test connectivity** using the **ping** command