**1. Virtual Network (VNet) Peering**

Virtual Network (VNet) Peering in Azure allows seamless connectivity between two Azure VNets. Peered VNets can communicate as if they are part of the same network. This feature eliminates the need for gateways and provides low-latency and high-bandwidth connectivity.

**Key Features**

* **Low Latency and High Bandwidth**: Direct network connectivity between VNets.
* **Cost Efficiency**: No need for VPN gateways; only pay for ingress and egress traffic.
* **Secure Communication**: Traffic between peered VNets remains within Azure’s backbone network.
* **Support for Different Subscriptions and Regions**: Global VNet peering enables peering between VNets in different Azure regions.

**Use Cases**

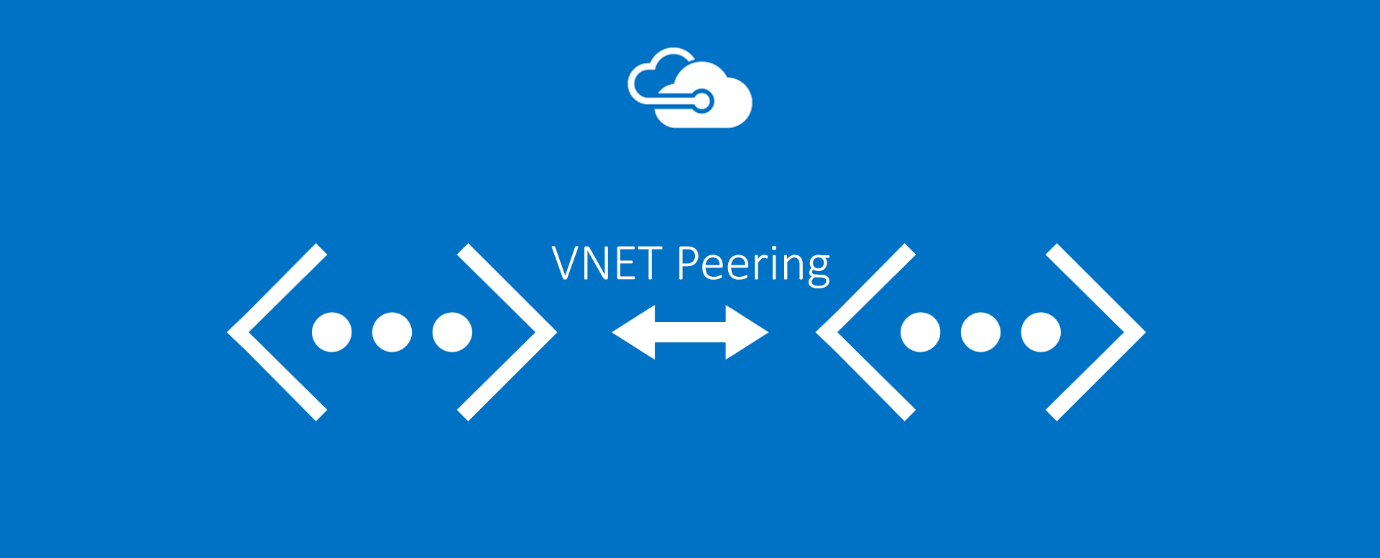
* Application and database separation for enhanced security.
* Extending workloads across VNets for scalability.
* Integrating VNets owned by different departments or teams.

**Configuration Steps**

1. **Create VNets**: Set up VNets that you want to peer.
2. **Initiate Peering**: Configure VNet peering from one VNet to the other.
3. **Accept Peering**: Confirm the peering connection in the second VNet.
4. **Validate Connectivity**: Test connectivity between resources in the peered VNets.

**Considerations**

* Both VNets must have non-overlapping IP address spaces.
* Cross-region peering incurs additional bandwidth costs.
* Some Azure services may have region-specific limitations.



**2. Network Address Translation (NAT)**

Azure Virtual Network NAT (Network Address Translation) provides outbound internet connectivity for virtual machines in a subnet. It simplifies outbound access management without requiring public IP addresses for each resource.

**Key Features**

* **Centralized Outbound Connectivity**: All outbound traffic routes through the NAT gateway.
* **Scalability**: Automatically scales with traffic volume.
* **High Availability**: Fully managed and redundant service.
* **Ease of Management**: Simplifies network configurations compared to manually managing public IPs.

**Use Cases**

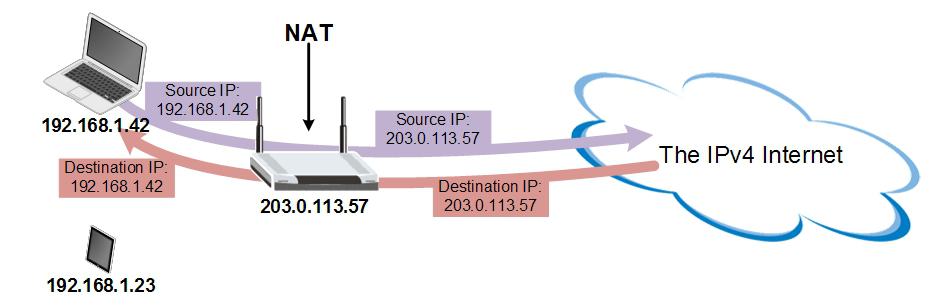
* Enable internet connectivity for VMs in private subnets.
* Centralized control of outbound connections.
* Simplify compliance with predictable outbound IPs.

**Configuration Steps**

1. **Create a NAT Gateway**:
   * Navigate to the Azure portal and create a NAT Gateway.
   * Associate a public IP address or prefix.
2. **Associate with Subnet**:
   * Link the NAT gateway to the target subnet(s).
3. **Configure Routing**:
   * Ensure the subnet’s outbound traffic routes through the NAT gateway.
4. **Validate Setup**:
   * Test outbound internet connectivity from the VM.

**Considerations**

* NAT is only for outbound traffic; it does not handle inbound traffic.
* Ensure sufficient public IP addresses are available for high-volume workloads.



**3. Azure Bastion Host**

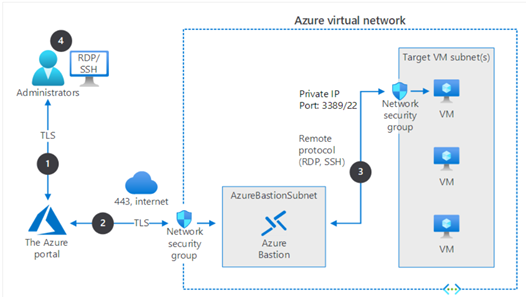
Azure Bastion provides secure and seamless RDP and SSH connectivity to Azure virtual machines without exposing them to the public internet. It acts as a jump server that users can access through the Azure portal.

**Key Features**

* **Browser-based Connectivity**: Access VMs using RDP or SSH directly from the Azure portal.
* **No Public IPs Needed**: VMs remain private, reducing attack surfaces.
* **Secure Communication**: Encrypted connections over SSL.
* **Integration with Azure Active Directory**: Provides additional access control mechanisms.

**Use Cases**

* Securely manage virtual machines without exposing them to the public internet.
* Provide developers or administrators with remote access while ensuring compliance with security policies.
* Centralize access management for multiple VMs.



**Configuration Steps**

1. **Create an Azure Bastion Resource**:
   * Navigate to the Azure portal and create a Bastion resource.
   * Associate the Bastion resource with a virtual network.
2. **Assign Subnet**:
   * Ensure the VNet has a dedicated subnet named AzureBastionSubnet with a /27 or larger CIDR block.
3. **Access VMs**:
   * Navigate to the VM in the Azure portal and select “Connect > Bastion”.
   * Authenticate with the VM’s credentials.
4. **Validate**:
   * Test the RDP/SSH connection through the Bastion interface.

**Considerations**

* Bastion is billed based on the number of hours it is active and the amount of data transferred.
* Ensure the AzureBastionSubnet is not used for other resources.
* Use network security groups (NSGs) to restrict access to the Bastion subnet.