**Module – 5 – Intersite connectivity**

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

* **Definition & Purpose**
  + VNet peering connects two or more Azure virtual networks, allowing resources in each VNet to communicate with each other using private IP addresses.
  + Peered VNets can be in the same region (regional peering) or different regions (global peering).
  + Peering uses the Azure backbone network, ensuring low latency, high bandwidth, and secure connectivity.
* **Key Features**
  + **Cross-subscription and cross-tenant peering:** VNets in different subscriptions or tenants can be peered.
  + **No gateway required:** Peering does not require a VPN gateway, reducing cost and complexity.
  + **Full mesh connectivity:** All peered VNets can communicate with each other if peering is set up bidirectionally.
  + **Traffic stays on Azure backbone:** No public internet traversal, enhancing security and performance.
  + **No overlapping address spaces:** VNets to be peered must have non-overlapping IP address spaces.
* **Gateway Transit**
  + Allows one VNet to use the VPN gateway of another peered VNet for connectivity to on-premises networks.
  + Useful in hub-and-spoke architectures where the hub VNet contains the gateway.
* **Service Chaining**
  + Enables directing traffic from one VNet to a network virtual appliance (NVA) or VPN gateway in a peered VNet using user-defined routes.
  + Supports scenarios like centralized security or inspection.
* **Best Practices**
  + Plan address spaces to avoid overlaps.
  + Use tags and naming conventions for easy management.
  + Monitor peering status and traffic flows for troubleshooting.

**2. Network Routing in Azure**

* **System-Defined Routes**
  + Automatically created by Azure to direct traffic within and between VNets, to on-premises networks, and to the internet.
  + Examples:
    - Traffic between VMs in the same subnet or VNet.
    - Traffic to the internet from a subnet with a public IP.
    - Traffic between peered VNets.
    - Traffic to on-premises via VPN Gateway or ExpressRoute.
* **User-Defined Routes (UDRs)**
  + Custom routes created to override or supplement system routes.
  + Used to control traffic flow, force traffic through NVAs, or implement custom routing scenarios.
  + Each route table can be associated with multiple subnets, but a subnet can only be associated with one route table.
  + Next hop types include: Virtual appliance, Virtual network gateway, Internet, None.
* **Best Practices**
  + Use UDRs for advanced scenarios like forced tunneling, custom security, or traffic inspection.
  + Regularly review and document custom routes to avoid misconfiguration.

**3. Service Endpoints vs. Private Endpoints**

* **Service Endpoints**
  + Extend your VNet’s identity to Azure services (e.g., Storage, SQL Database) over the Azure backbone.
  + Restrict access to specific subnets, improving security.
  + Traffic to the service remains on the Azure backbone, not the public internet.
  + Simple to configure and provides optimal routing.
* **Private Endpoints (Azure Private Link)**
  + Assign a private IP address from your VNet to an Azure service, enabling private connectivity.
  + Traffic to the service never leaves the Microsoft network.
  + Supports integration with on-premises and peered networks.
  + Enhances security by eliminating public exposure of the service.
  + Each private endpoint is mapped to a specific resource instance.
* **Comparison**
  + Service endpoints secure access at the subnet level; private endpoints secure access at the resource instance level.
  + Private endpoints are preferred for scenarios requiring private, granular access and compliance.

**4. Intersite Connectivity Scenarios**

* **Hub-and-Spoke Topology**
  + Central hub VNet connects to on-premises and provides shared services (e.g., firewalls, NVAs).
  + Spoke VNets peer with the hub for connectivity and can be isolated from each other.
* **Site-to-Site VPN**
  + Connects on-premises networks to Azure VNets using VPN gateways.
  + Supports secure, encrypted communication over the internet.
* **Point-to-Site VPN**
  + Allows individual devices to connect securely to Azure VNets from remote locations.
* **ExpressRoute**
  + Provides private, dedicated connectivity between on-premises and Azure, bypassing the public internet.

**5. Additional Routing and Security Concepts**

* **Route Tables**
  + Collections of routes applied to subnets to control traffic flow.
  + Can be used to direct traffic to NVAs, block internet access, or implement custom routing.
* **Network Virtual Appliances (NVAs)**
  + Third-party or custom virtual machines that provide advanced network functions (firewall, IDS/IPS, etc.).
  + Often used in service chaining scenarios.
* **Azure Firewall**
  + Managed, cloud-based network security service that protects Azure VNets.
  + Supports application and network-level filtering, threat intelligence, and logging.
* **Load Balancer, NAT, Application Gateway**
  + Load Balancer: Distributes incoming traffic across multiple VMs.
  + NAT Gateway: Provides outbound internet connectivity for VMs in a VNet.
  + Application Gateway: Layer 7 load balancer with web application firewall (WAF) capabilities.

**6. Monitoring and Troubleshooting**

* **Network Watcher**
  + Provides tools for monitoring, diagnosing, and gaining insights into network traffic and connectivity.
  + Features include connection troubleshooting, packet capture, topology visualization, and NSG flow logs.
* **Best Practices**
  + Enable diagnostic logs and flow logs for auditing and troubleshooting.
  + Regularly test connectivity between VNets and on-premises networks.
  + Use tags and documentation for all intersite connectivity resources.

**7. Security and Compliance**

* **Access Control**
  + Use Network Security Groups (NSGs) and Application Security Groups (ASGs) to control traffic at subnet and NIC levels.
  + Combine with route tables for granular control.
* **Compliance**
  + Use private endpoints and service endpoints to meet regulatory requirements for data privacy and network isolation.
  + Regularly review and update security rules and routing configurations.

**Service Endpoint vs Private Endpoint in Azure**

| **Feature/Aspect** | **Service Endpoint** | **Private Endpoint** |
| --- | --- | --- |
| **Definition** | Extends VNet identity to Azure services over Azure backbone. | Assigns a private IP from your VNet to an Azure service for private connectivity. |
| **Network Traffic Path** | Traffic stays on Azure backbone, but service is accessed via public endpoint. | Traffic is fully private; service is accessed via private IP in your VNet. |
| **Access Control** | Restricted at subnet level. | Restricted at resource instance level. |
| **Supported Services** | Many Azure PaaS services (Storage, SQL, Key Vault, etc.). | Most Azure PaaS services, some partner/customer services. |
| **DNS Configuration** | No DNS changes required; uses public DNS. | Requires DNS setup to resolve service name to private IP. |
| **Security** | Restricts access to subnets; service endpoint is still public. | Highest security; service is never exposed to public internet. |
| **Integration with On-premises** | Not directly accessible from on-premises via VPN/ExpressRoute. | Accessible from on-premises if VNet is connected via VPN/ExpressRoute. |
| **Data Exfiltration Protection** | Limited; restricts access by subnet. | Strong; can be locked down to specific resources and users. |
| **Auditing and Monitoring** | Logs via service diagnostics and NSG flow logs. | Logs via Private Link and NSG flow logs. |
| **Cost** | No extra cost for enabling. | Standard data transfer rates; |