Module 2: Design and implement hybrid networking

# Chapter 1: Design and implement Azure VPN Gateway

* VPN provides a secure encrypted connection across another network.

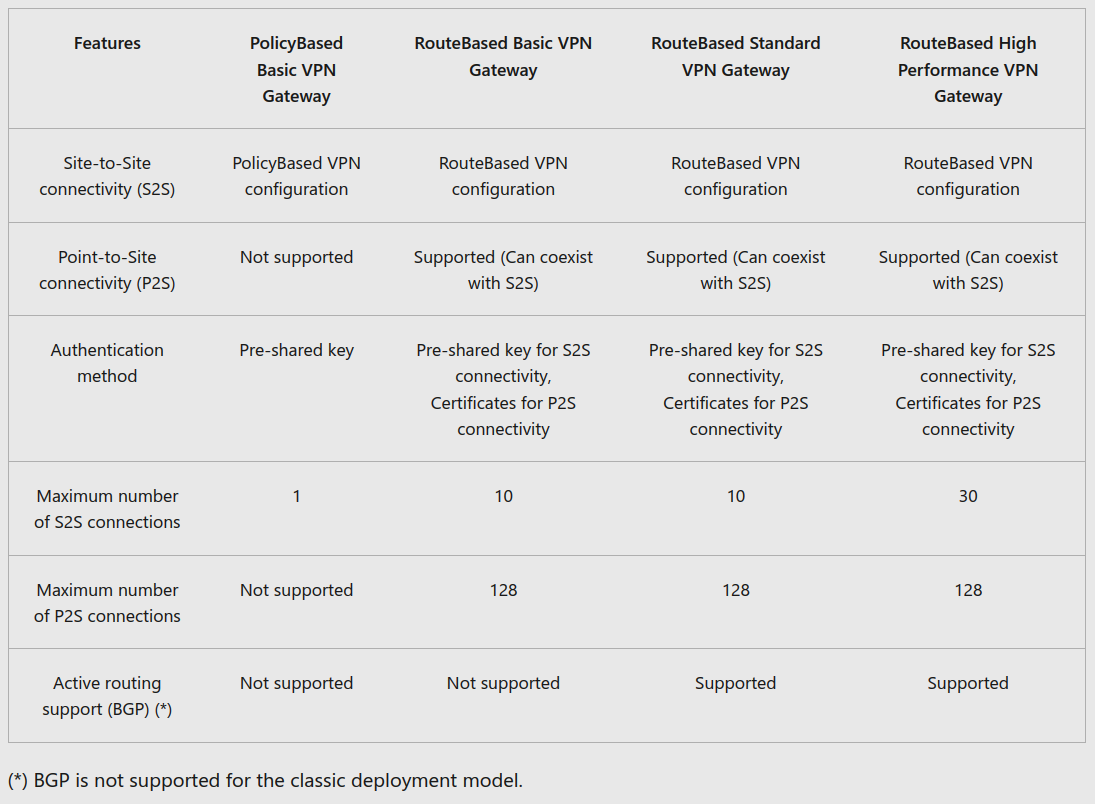
## Azure VPN Gateway

* This provides an **endpoint** for incoming connections to VNET.
  + It is used to send and receive encrypted traffic between:
    - Azure VNET and an on-premises location over the Internet.
    - Azure VNET to Azure VNET over MS Backbone
  + VNET gateway is two or more special VMs deployed to a specific subnet called the *gateway subnet*
* **3 Types of VPN Gateway Architecture**:
  + P2S over the internet
  + S3S over the internet
  + S2S over Azure ExpressRoute
* **Consider these Factors**:
  + Throughput - Mbps or Gbps
  + Backbone - Internet or private?
  + Availability of a public (static) IP address
  + VPN device compatibility
  + Multiple client connections or a site-to-site link?
  + VPN gateway type
  + Azure VPN Gateway SKU
* **Appropriate SKU and Generation**
  + *Refer*: <https://learn.microsoft.com/en-us/training/modules/design-implement-hybrid-networking/2-design-implement-vpn-gateway>

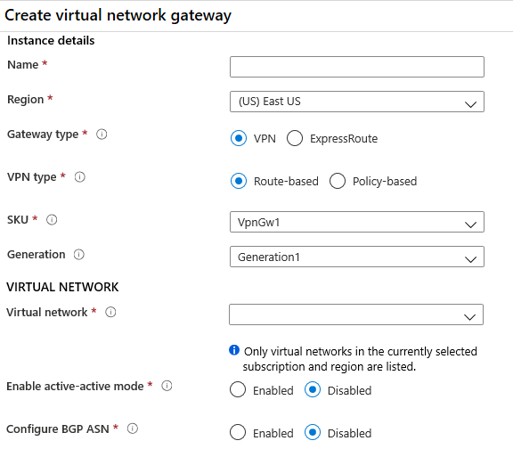
### 2 VPN Types

* *PolicyBased* (Static routing)
  + This VPN type encrypts/directs packets through IPsec tunnels based on **IPsec policies** configured between your on-premises network & Azure VNET.
    - These policies are defined as ‘access lists’ in the VPN config.
    - **Limitations**:
      * Can only be used with Basic Gateway SKUs.
      * Only 1 tunnel when using a PolicyBased VPN.
      * PolicyBased VPNs are only used for S2S connections, and only for certain configurations.
        + Most VPN Gateway configurations require a RouteBased VPN.
* *RouteBased* (Dynamic routing)
  + Use "routes" in IP forwarding/RT to direct packets into their corresponding tunnel interfaces.
    - These interfaces encrypt/decrypt the packets in and out of the tunnels.
    - The policy (or traffic selector) are configured as any-to-any (or wild cards)

### VPN Gateway Config Req.

* 

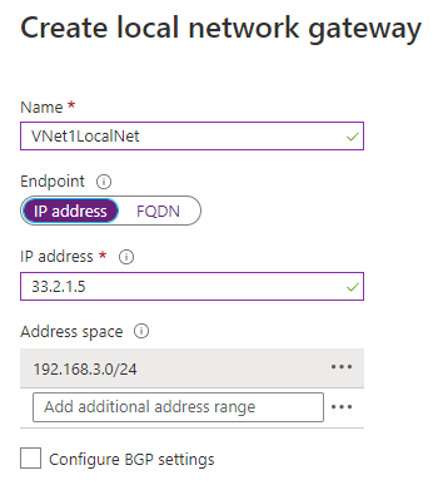
### Creating a VPN Gateway

* 

### Gateway Subnet

* The gateway subnet contains the IP addresses that the VNET gateway VMs and services use.
  + Never deploy anything else to the gateway subnet & name it **GatewaySubnet** to work properly.

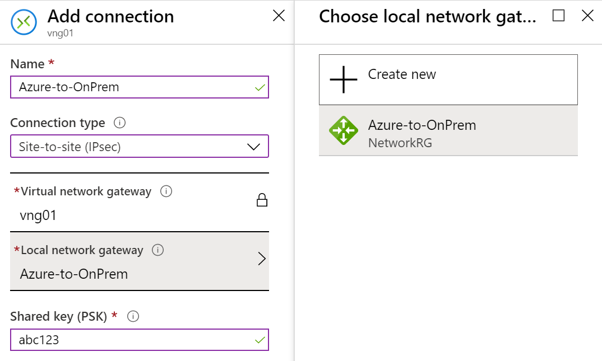
### Local Network Gateway

* This refers to the **on-prem location**, use the address prefixes located in the on-prem network
  + 
    - **IP address** = public IP of local gateway
    - **Address space** = CIDR IP ranges that define the local network’s address space
      * At least, include the prefix of the host address of your BGP Peer IP address on VPN device

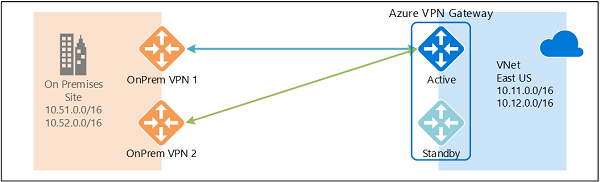
### Configuring On-Prem VPN device

* Either use the Validated List of Standard VPN devices (ex. Cisco, Juniper, Barracuda, etc.)
  + **Need**:
    - A shared key – specified when creating the VPN connection.
    - Public IP address of your VPN gateway (new or existing).

### Create VPN Connection

* 
  + Verify the connection via Portal or PowerShell

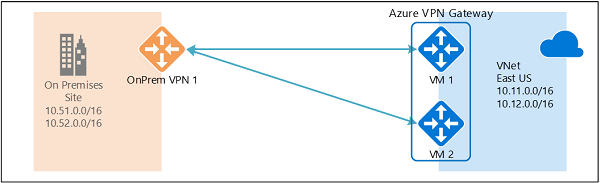
### VPN Gateway Redundancy

* Downtime for **S2S** or **VNET-2-VNET**:
  + Planned maintenance:
    - Within 10 to 15 seconds.
  + Unplanned issues:
    - 1 to 3 minutes in the worst case.
* Downtime for **P2S VPN** client connections to the gateway:
  + Users will need to reconnect from the client machines.
* 

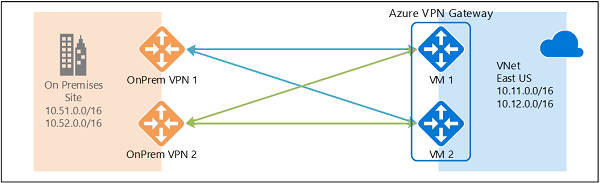
### Multiple On-Prem VPN devices

* Requirements/constraints:
  + Create multiple S2S VPN connections from your VPN devices to Azure.
    - Create one local network gateway for each VPN device,
    - Create one connection from your Azure VPN gateway to each local network gateway.
  + Local network gateways must have unique public IP addresses in the GatewayIpAddress property.
  + BGP is required for this configuration + each VPN device must have a unique BGP peer IP address (BgpPeerIpAddress property).
  + Must use Equal-cost multi-path routing (ECMP).
  + Each connection is counted against the maximum number of tunnels for Azure VPN gateway
    - 10 for Basic and Standard SKUs, and 30 for HighPerformance SKU.

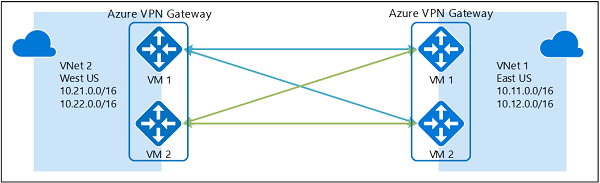
### Active-Active VPN Gateways

* Both gateway VMs will establish S2S VPN tunnels to your on-premises VPN device
  + 
  + Each Azure gateway instance has a unique public IP address, and each will establish an IPsec/IKE S2S VPN tunnel to your on-premises VPN device
* Traffic from Azure VNET to your on-premises network will be routed through both tunnels **simultaneously**
* Planned/unplanned event occurring with to one gateway instance causes the IPsec tunnel from that instance to your on-premises VPN device will be to disconnect.
  + Azure will switch this automatically, but you need to do this manually On-Prem

### Dual-redundancy: active-active VPN gateways for both Azure and on-premises networks

* 
  + Most reliable option!
  + Full mesh connectivity of 4 IPsec tunnels between Azure VNET and on-premises network.

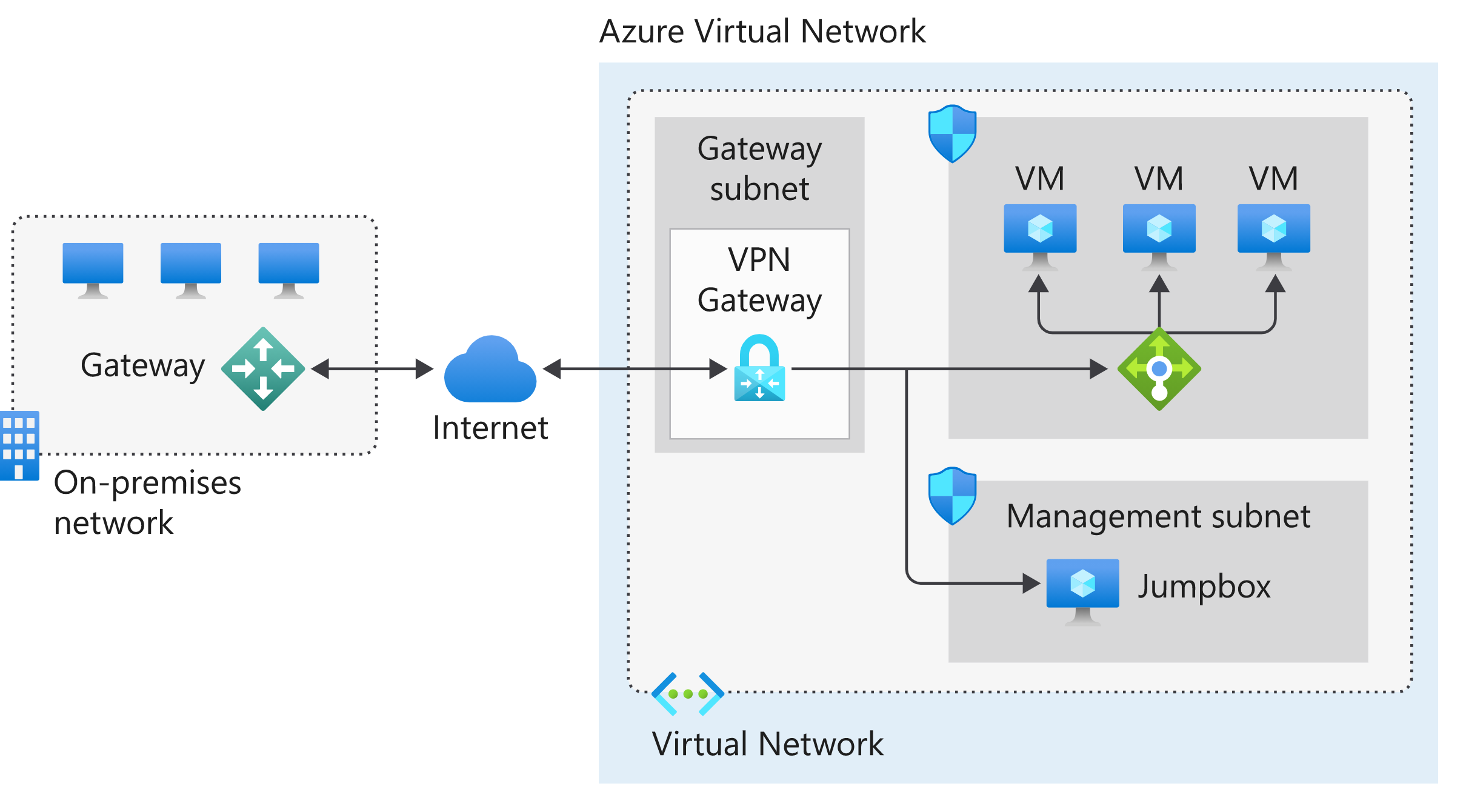
### Highly Available VNET-2-VNET

* Create active-active VPN gateways for both VNETs, and connect them together to form the same full mesh connectivity of 4 tunnels between them
  + 

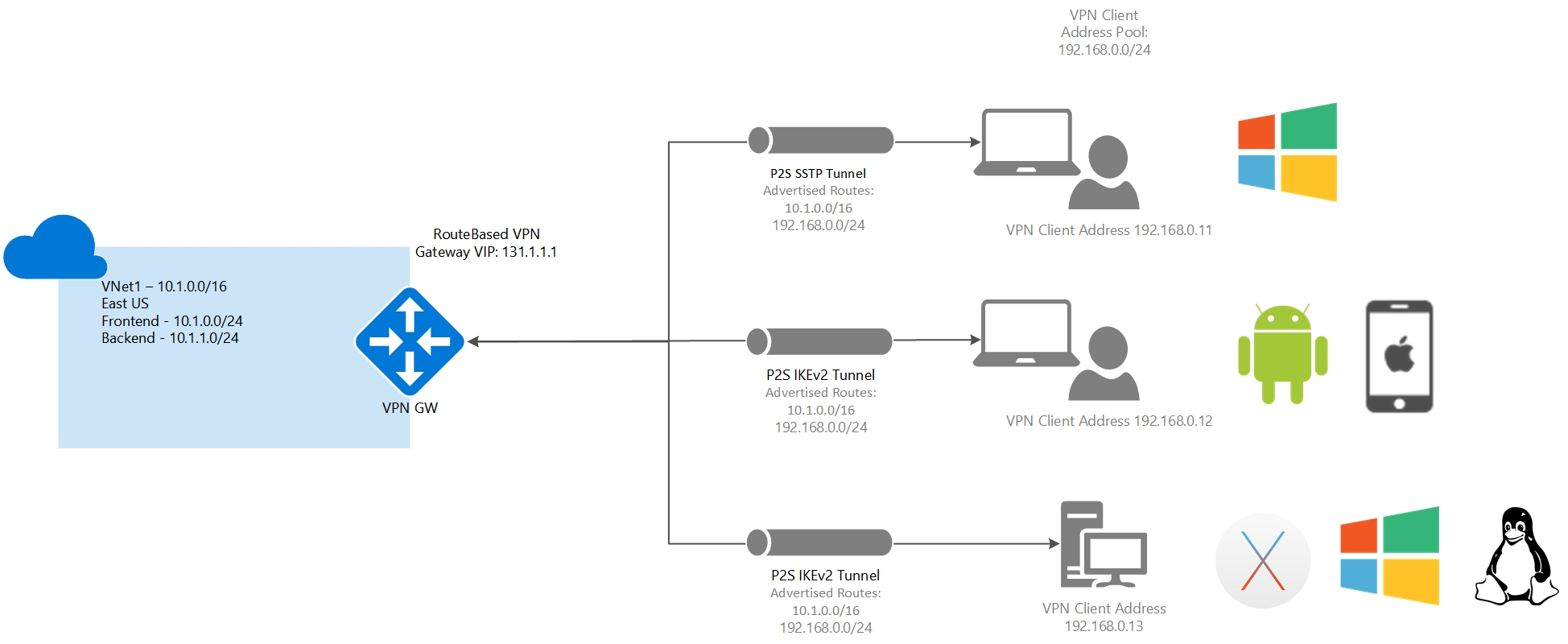
### Troubleshoot Azure VPN Gateway using diagnostic logs

* Diagnostic logs used troubleshoot a problem with your VPN Gateway:
  + *GatewayDiagnosticLog* - Contains diagnostic logs for gateway configuration events, primary changes, and maintenance events.
  + *TunnelDiagnosticLog* - Contains tunnel state change events. Tunnel connect/disconnect events have a summarized reason for the state change if applicable.
  + *RouteDiagnosticLog* - Logs changes to static routes and BGP events that occur on the gateway.
  + *IKEDiagnosticLog* - Logs IKE control messages and events on the gateway.
  + *P2SDiagnosticLog* - Logs point-to-site control messages and events on the gateway.

# Chapter 4: Connect networks with Site-to-site VPN connections

* (S2S) VPN gateway connection creates a secure connection to your **VNET from another VNET or a physical network** (On-prem)
  + 
  + **Key Points**:
    - On-premises === On-premises Active Directory, data, or resources.
    - The gateway sends encrypted traffic to a virtual IP address when it uses a public connection.
    - Azure VNET holds all cloud applications and Azure VPN gateway components.
    - Azure VPN gateway **provides the encrypted link between** the Azure VNET and On-premises.
      * Elements of Azure VPN gateway:
        + VNET gateway
        + Local network (LNET) gateway
        + Connection
        + Gateway subnet
    - Internal load balancer (front-end) will route cloud traffic to the correct cloud-based resource.
  + Benefits:
    - Configuration and maintenance are simplified.
    - The VPN gateway ensures encryption of traffic **between** on-premises gateway and the Azure gateway.
    - The architecture can be scaled and extended

# Chapter 5: Connect devices to networks with Point-to-site VPN connections

* P2S VPN gateway connection creates a secure connection to your VNET from an **individual-client** computer.
  + 

## Authentication Methods & Protocols

* **P2S VPN use these protocols:**
  + OpenVPN® Protocol
  + Secure Socket Tunneling Protocol (SSTP)
  + IKEv2 VPN

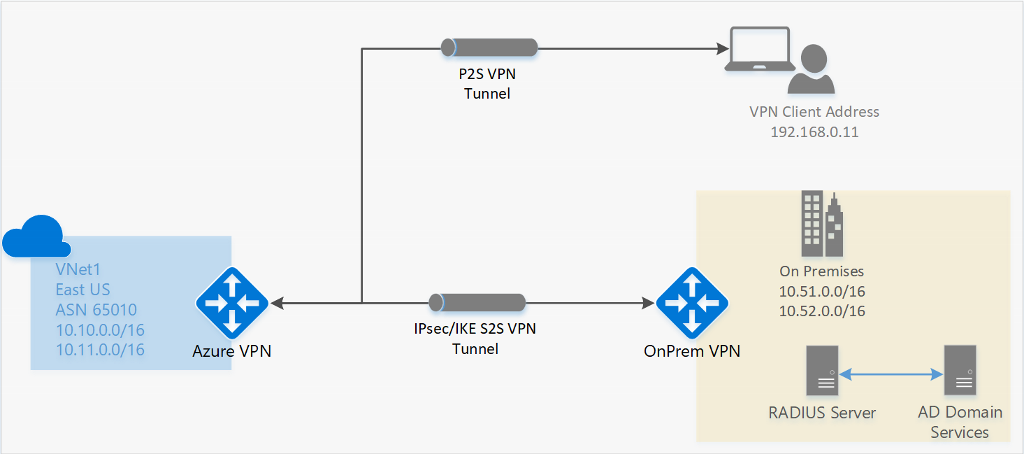
### Using Native Azure Cert Authentication

* Client cert on device is used to authenticate the connecting user.
  + Certs generated from a trusted root certificate and then installed on each client computer.
    - Either Enterprise solution or self-signed certificate.

### Using Native Azure AD Auth

* Connect to Azure using their *Azure AD credentials*.
  + Use Azure AD's conditional access + (MFA) features for VPN.
  + Steps to configure Azure AD authentication:
    - Configure an Azure AD tenant
    - Enable Azure AD authentication on the gateway
    - Download and configure Azure VPN Client

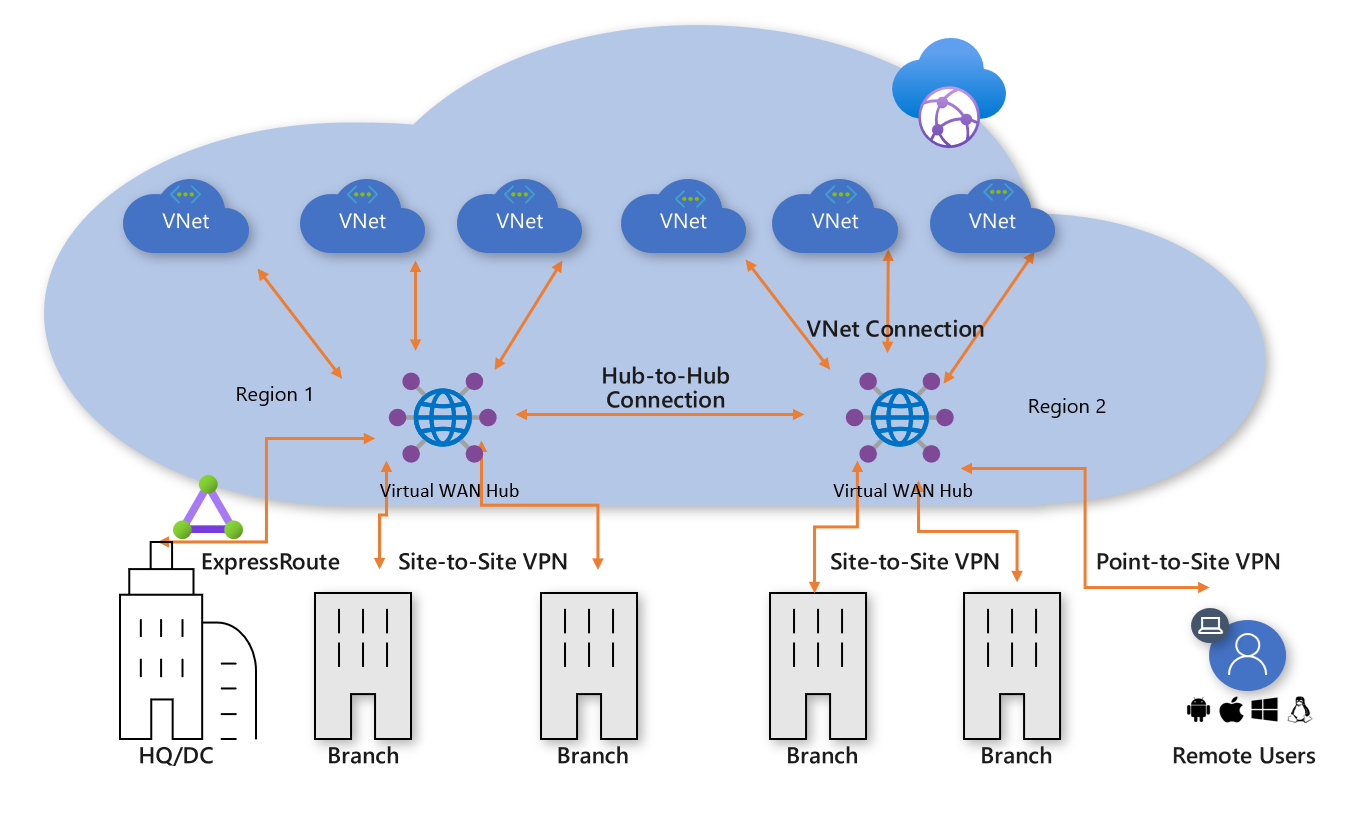
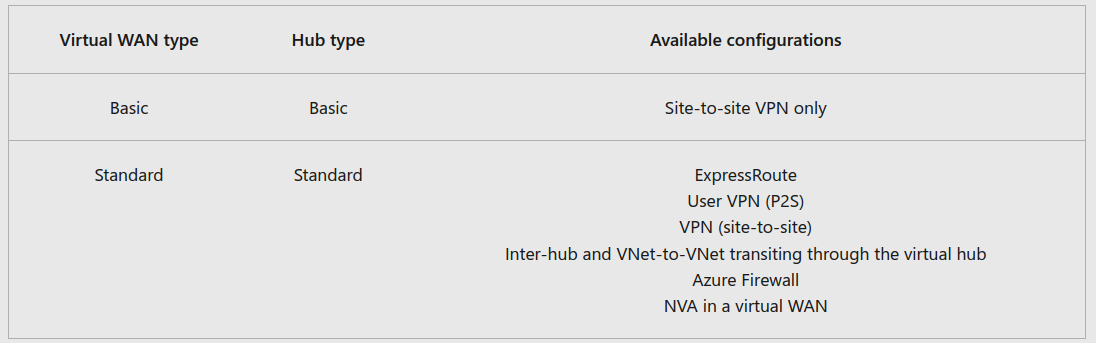
### Using Active Directory (AD) Domain Server

* Connect to Azure using org domain credentials + RADIUS server integrated w/ AD server.
  + Deploy RADIUS either on Azure or On-Prem
  + 

### Configure P2S clients

* Users use the native VPN clients on Windows/Mac devices for P2S.
  + Azure provides a VPN client configuration zip file you need to install

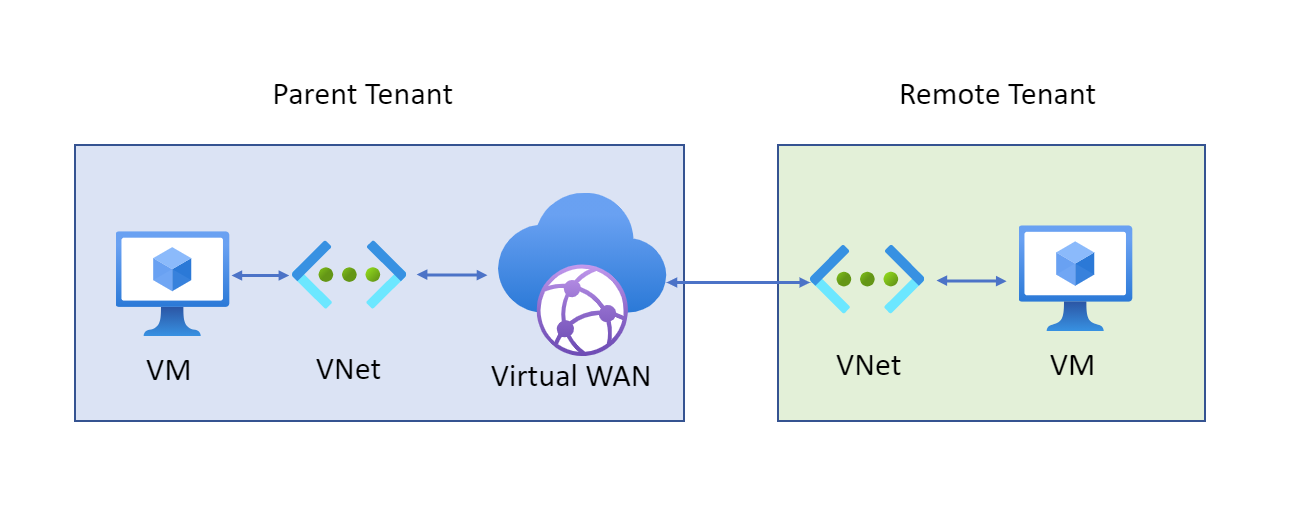
# Chapter 6: Connect remote resources by using Azure Virtual WANs

* **Azure Virtual WAN** is a service that brings together networking, security, and routing functionalities as a single operational interface.
  + - **Features**:
      * Branch connectivity (via connectivity automation from Virtual WAN Partner devices such as SD-WAN or VPN CPE).
      * S2S, P2S VPN connectivity.
      * ExpressRoute.
      * Intra-cloud connectivity (transitive connectivity for virtual networks).
      * VPN ExpressRoute inter-connectivity.
      * Routing, Azure Firewall, and encryption for private connectivity.
  + 
  + **2 types of Virtual WANs**:
    - Basic and Standard.
      * 
  + **Hub Private Address Space**
    - The minimum address space is /24 to create a hub.
    - Because Azure Virtual WAN is a managed service
      * Azure creates the appropriate subnets in the virtual hub for the different gateways/services

### Gateway scale

* A hub gateway !== VNET gateway used for ExpressRoute and VPN Gateway.
  + Traffic ALWAYS goes through hub gateway (each VNET doesn’t need its own gateway)

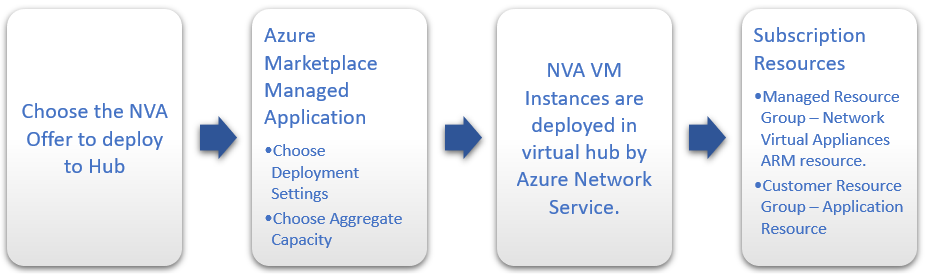
### Connect cross-tenant VNETs to a Virtual WAN hub

* Virtual WAN can connect a VNET to a virtual hub in a different tenant.
  + Useful for client workloads that must be connected to be the same network but are on different tenants.
  + 

# Chapter 8: Create a network virtual appliance (NVA) in a virtual hub

* Examples of network virtual appliances (NVAs) are:
  + ExpressRoute, a VPN Gateway, or from a networking partner
    - They have externally facing public IP address.

## Manage an NVA in a Virtual Hub

* MS NVAs are deployed directly into VHUB only & cannot be deployed within an arbitrary VNET
  + Each is deployed as a Managed Application,
    - Allows Azure Virtual WAN to manage the configuration of the NVA
      * 

## Deploy an NVA in your Virtual Hub

* When chosen in Azure Portal’s marketplace:
  + **2 RGPS are created in your Sub**.
    - *Customer RGP* 
      * Contains an app placeholder for the Managed Application.
      * Partners can use this RGP to expose whatever customer properties they choose here.
    - *Managed Resource Group* - Customers cannot affect resources here directly.
      * It contains the NVA resource.
  + NVA is configured automatically as part of the deployment process (can’t access NVA directly)
  + No need to create S2S, P2S connections (all managed by NVA partner)
* Steps are found here:
  + <https://learn.microsoft.com/en-us/training/modules/design-implement-hybrid-networking/8-create-network-virtual-appliance-virtual-hub>

## NVA Infrastructure Units

* When creating NVA in the Virtual WAN hub:
  + Choose # of NVA Infrastructure Units
    - NVA Infrastructure Unit === unit of aggregate bandwidth capacity for an NVA in the VHUB.
      * One NVA Infrastructure Unit === 500 Mbps of aggregate bandwidth for all branch site connections coming into this NVA.
      * Azure supports from 1-80 NVA Infrastructure Units per NVA virtual hub deployment.