

Azure Hybrid Cloud Configuration

Ranjit Karni

VPark Innovations

Ranjit.balu@gmail.com

Ph.No: 9676976662

Agenda

1. Azure Hybrid Cloud Topologies
2. Site-to-Site Virtual Private Network
3. Point-to-Site VPN
4. ExpressRoute
5. Multi-Site VPN
6. Vnet-to-Vnet
 1. S2S VPN
 2. Vnet Peering
7. Azure Stack

Azure Hybrid Cloud Topologies

- When you want to manage your Azure IAAS Virtual machines with On-premises infrastructure.
- Manage On-Premises servers with Azure solutions like log Analytics
- Azure as a disaster recovery site
- Secure WAN Cloud between HQ and branch offices


Site-to-Site (S2S) VPN Connections

- Allows you to connect several clients to an Azure virtual network
- Uses a virtual private network device to connect Azure
- Appropriate for connecting small groups of people to your Vnet
 - A development team in a single location
 - Remote offices with a handful of employees
 - Local datacenters / production loads that do **not** need to transfer large files, does **not** need lot of bandwidth strong data security, have continuous throughput or low latency

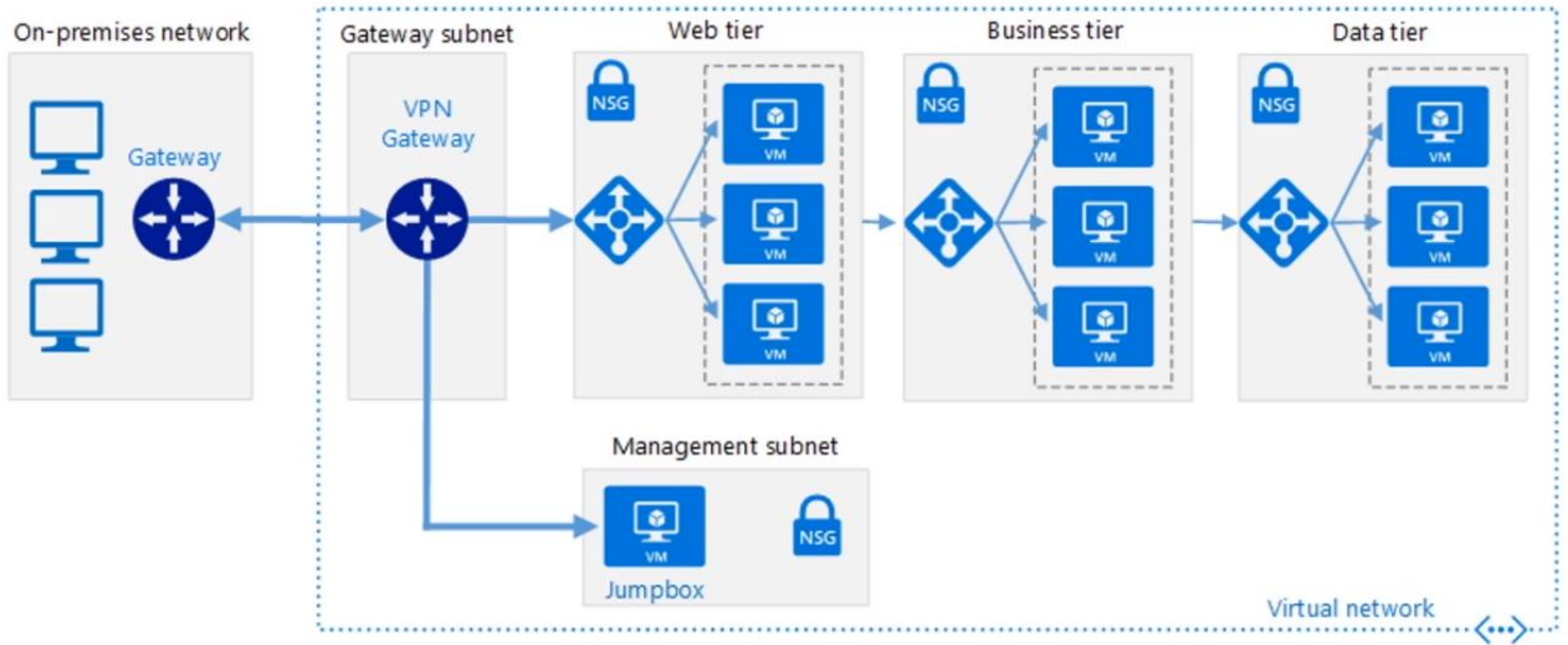
Site-to-Site (S2S) VPN Pros

- Supports just about any operating system
- VPN device provides a single point of configuration / management for all connected clients
- Allows policy-based (static) and route-based (dynamic) VPNs
- Connection is persisted; clients can automatically reconnect after a restart

Site-to-Site (S2S) VPN Drawbacks

- Requires a public IP address in your local network that is not allowed by a network address translation or NAT
 - Requires a compatible VPN device
 - Throughput is limited to 1.25 GBPS. You may see slower throughput since the connection takes place over the public internet.
 - Traffic is sent over the public internet via IPSec
 - Access limited to VMs and cloud services
 - Limited to 10 or 30 IPSec tunnels, depending on VPN gateway service tier
- 

Site-to-Site Virtual Private Network



Point-to-Site (P2S) VPN Connections

- Allows you to connect a specific client to an Azure Virtual Network
- Appropriate when a single user or machine needs access to your Azure Vnet:
 - A single outside contractor
 - A small group of people in a remote location, where the cost of buying and maintaining a VPN device would be prohibitive
 - An employee who works from home or is on the road
 - Someone who temporarily needs access to your network
 - A specific machine within your network that is the only device which needs to connect to your VNet

Point-to-Site (P2S) VPN Pros Compared to S2S / Express Route

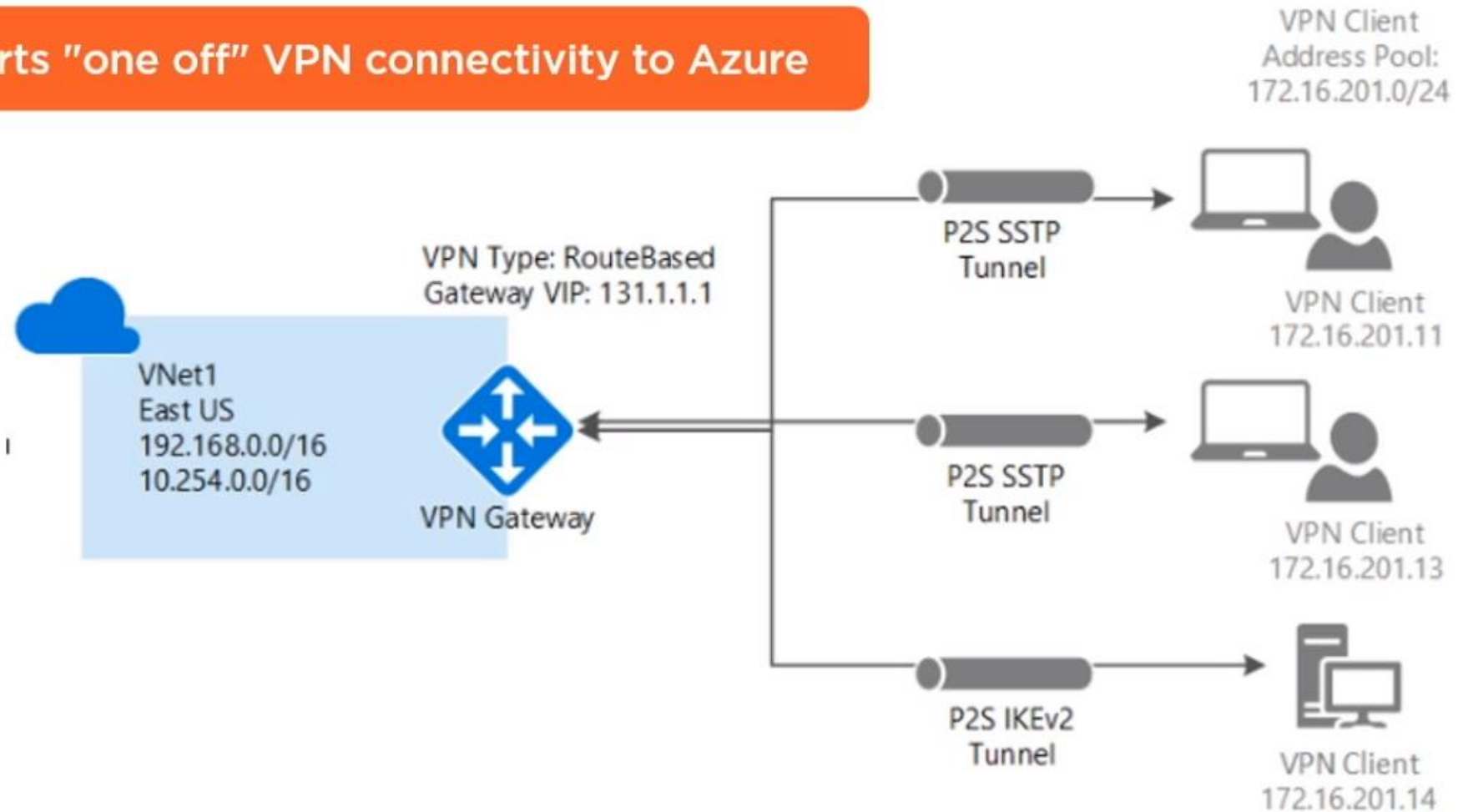
- Does **not** require a VPN device
- Does **not** require a local public IP address
- Certificate-based, making privilege revocation as simple as revoking the client's certificate
 - Uses self-signed certificates and / or your own certificate authority. So there wont be any cost associated with it.
- Can be used alongside site-to-site (S2S) VPNs
- Can (in theory) support multiple network connections

Point-to-Site (P2S) VPN Drawbacks

- Only works with Windows OS
 - Windows 7/8/8.1 64 bit; Windows 10
 - Windows Server 2008 R2 / 2012 / 2012 R2, 64 bit
- Throughput is limited to 1.25 GBPS
- Traffic is sent over the public internet using SSTP
- Access limited to VMs and cloud services
- Limited to 128 clients
- Connections are not renewed after restarts
- Difficult to keep the networking straight for multi-network P2S connections because your address prefixes in subnet addresses need to be unique between those two networks and
- Does not work for static or policy-based Basic VPN gateways. You must use Dynamic / Route based routing.

Point-to-Site VPN

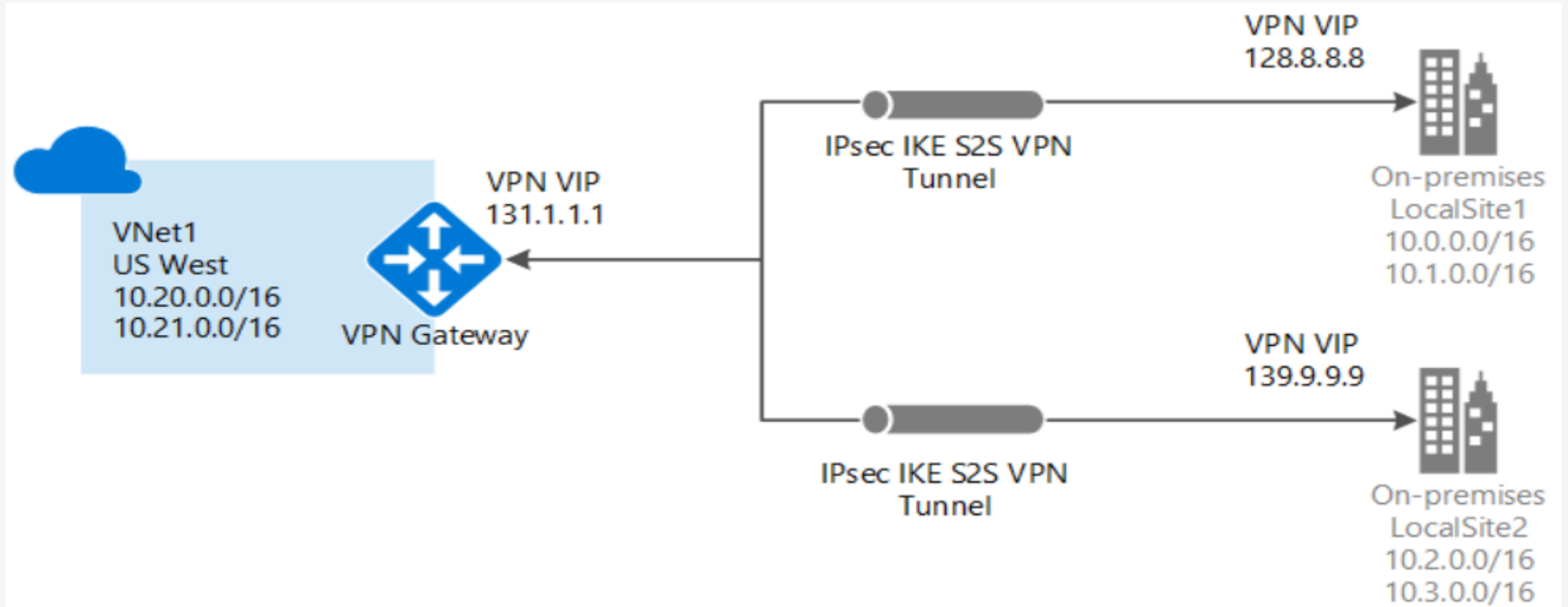
Supports "one off" VPN connectivity to Azure



SSL / TLS – based on VPN. It uses Secure Socket Tunneling Protocol (SSTP).

Azure creates the VPN client software, the agent, the VPN client that you would require to deploy on client VM.

Multi-Site VPN



ExpressRoute

- Dedicated, private connection to Azure
- Layer 3 connection (network-level)
- Appropriate for the most demanding connectivity needs
 - Data Security
 - High through-put / low latency
 - Access to just about every Azure Service
 - Redundancy and inter-region connectivity
 - Connecting large datacenters and heavy workloads to Azure
- It is perfect choice when you need speed, low latency, reliability and connect to more than one datacenter.

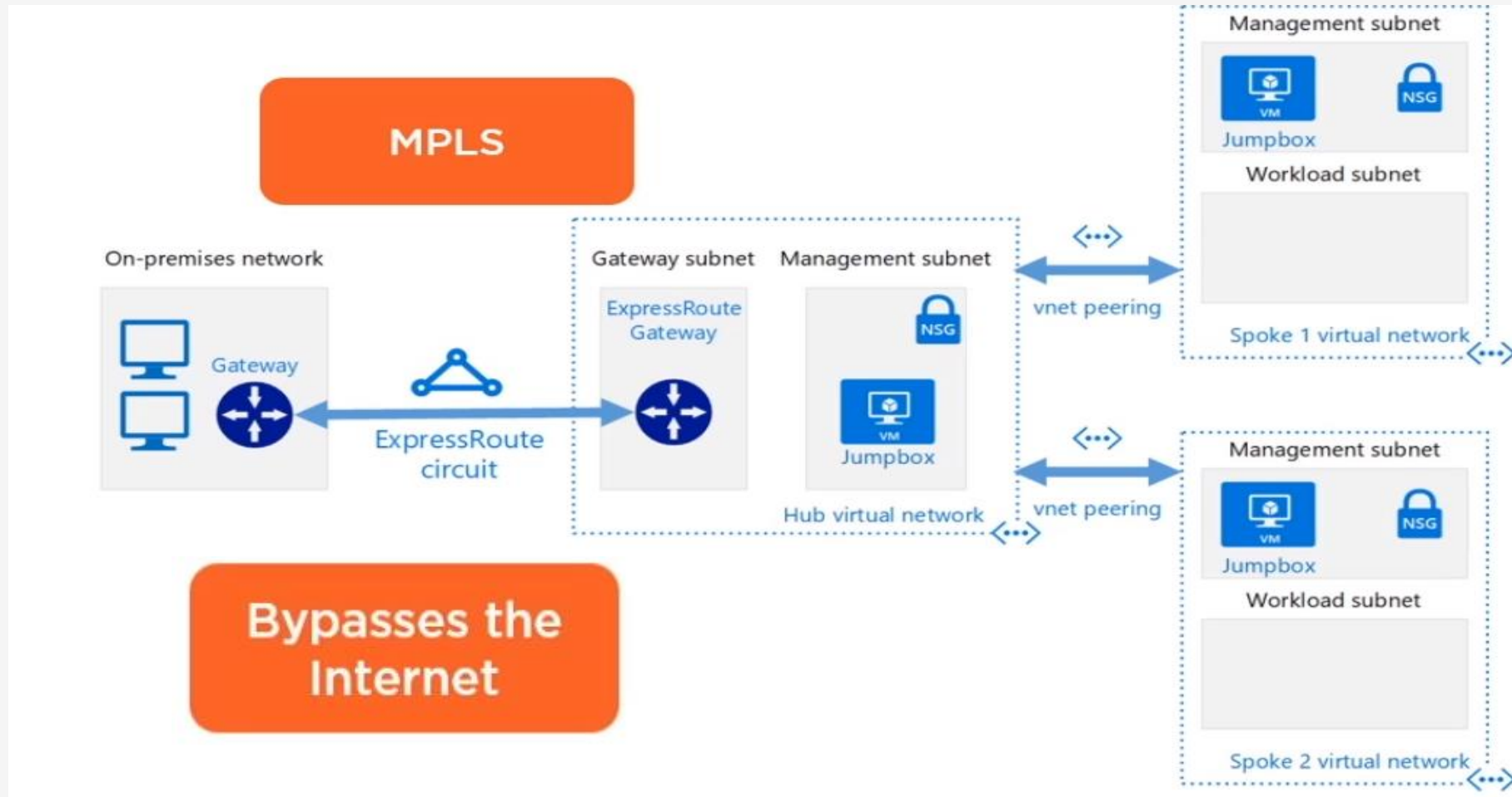
ExpressRoute Pros

- Extremely high data throughput and very low latency
 - 10 GBPS, depending on gateway SKU because this is dedicated connection with built-in redundancy
- Highly available, extremely flexible
- Can connect to all datacenters globally with premium add-on
- Data not sent over public internet, increasing security than P2S or S2S VPN.
- Supports private, public and Microsoft Peering, so ExpressRoute is pretty much reachable to any Azure service whether or not it is publicly addressable.
 - Private peering: Access to Azure VNets and resources inside them
 - Public Peering: Azure resources available over the internet, e.g. storage, SQL Database, Web Apps
 - Microsoft Peering: SaaS offerings, e.g. Dynamics 365, PowerBI, Office 365

ExpressRoute Cons

- Not available in every region
- Available only through certain partners
- Considerably more expensive than P2S and S2S VPNs

ExpressRoute Circuit



MPLS – MultiProtocol Label Switching. It's common WAN technology

Hub – and – Spoke : Virtual Network that linked to On-Premise is a Hub and then take advantage of Vnet Peering to create a logical connection between other VNets

Choosing the Right Gateway Service Tiers and their Costs

- While P2S and S2S VPNs are actually free, the VPN gateways through which they are routed are not.
- Setting up a virtual network is free of charge. However, we do charge for the VPN gateway that connects to on-premises and other virtual networks in Azure. This charge is based on the amount of time that gateway is provisioned and available.
- The VPNGateway access is charged by the hour
- Four VPN gateway service SKUs and they are called as Azure Resource Manager Lingo
 - Basic, Standard and HighPerformance are available for P2S, S2S and ExpressRoute connections.
 - UltraPerformance for ExpressRoute, too

Azure Stack



Azure VPN Gateway SKUs

<https://azure.microsoft.com/en-in/pricing/details/vpn-gateway/>

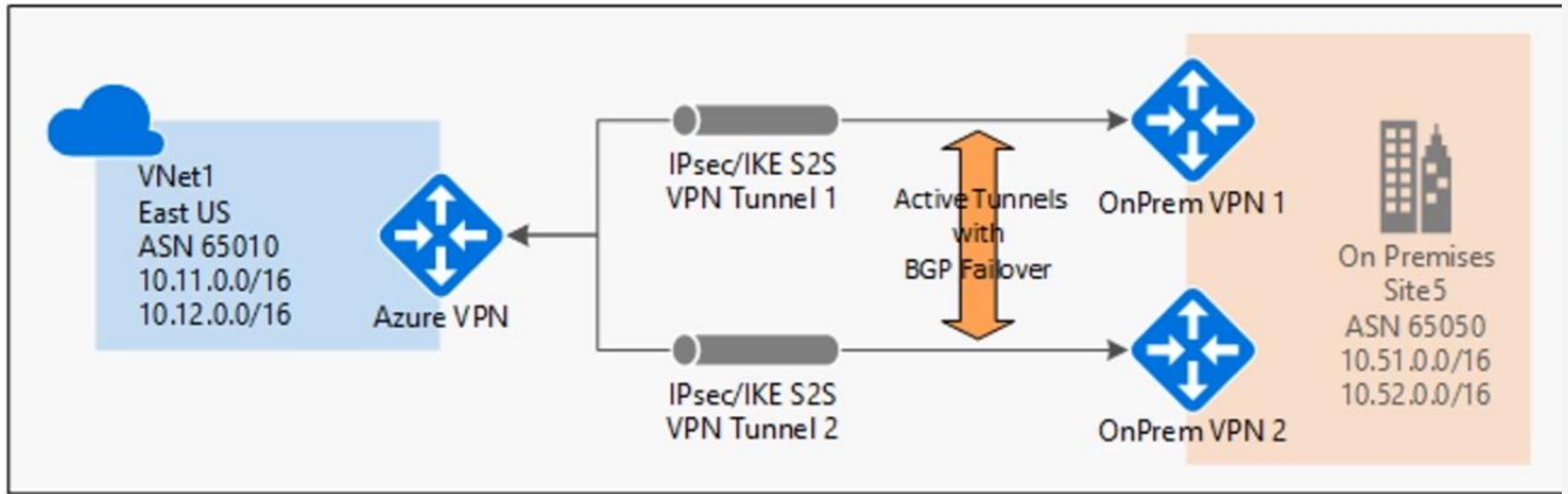
VPN GATEWAY TYPE	PRICE	BANDWIDTH	S2S TUNNELS	P2S TUNNELS
Basic	₹2.38/hour	100 Mbps	Max 10 1-10: Included	Max 128 1-128: Included
VpnGw1	₹12.56/hour	650 Mbps	Max 30 1-10: Included 11-30: ₹1.00/hour per tunnel	Max 128 1-128: Included
VpnGw2	₹32.39/hour	1 Gbps	Max 30 1-10: Included 11-30: ₹1.00/hour per tunnel	Max 128 1-128: Included
VpnGw3	₹82.63/hour	1.25 Gbps	Max 30 1-10: Included 11-30: ₹1.00/hour per tunnel	Max 128 1-128: Included

ExpressRoute Gateway SKUs

<https://azure.microsoft.com/en-in/pricing/details/vpn-gateway/>

GATEWAY TYPE	PRICE	BANDWIDTH (UP TO)
Standard ExpressRoute Gateway	₹12.56/hour	1 Gbps
High Performance ExpressRoute Gateway	₹32.39/hour	2 Gbps
Ultra Performance ExpressRoute Gateway	₹123.60/hour	9 Gbps

Active / Active Tunnels with BGP Failover



Highly available Azure VPN gateway

Azure always deploys a standby VPN gateway

VNet-to-Vnet Configuration

- You can use Site-to-Site connection / VPN Peering for Vnet-to-Vnet Configuration.
- Microsoft recently released Vnet Peering.
 - For Vnet Peering, it is mandatory that both Vnets should be in the same region
 - Microsoft provide 25 GBPS throughput for Vnet Peering.
 - Vnet peering is also possible across subscription provided both subscriptions are in same Azure AD tenant.

VPN Gateway

- A **VPN Gateway** is a type of virtual network gateway that sends encrypted traffic across a public connection to an on-premises location or to an Azure virtual networks over the Microsoft network.
- **Every virtual network can have only one VPN Gateway**, however, you can create multiple connections to the same VPN gateway.
- **Connection Topology**
- **Site-to-Site**: A Site-to-Site (S2S) VPN Gateway connection is a connection over **Ipsec / IKE (IKEv1 or IKEv2)** VPN tunnel
- **Point-to-Site**: A P2S connection allows you to create a secure connection to your virtual network from an individual client computer
- **Vnet-to-Vnet**: Connecting a virtual network to another virtual network (Vnet-to-Vnet) is similar to connecting a Vnet to an On-Premises site location
- **Vnet Peering**: Virtual Network Peering enables you to connect two virtual networks in the same region through the Azure backbone network. It doesn't require use of VPN gateway

Questions?

Ranjit Karni

Vpark Innovations

Ranjit.balu@gmail.com

Ph No: +91-9676976662