



# MC2MC

Azure Virtual WAN for everyone

# Didier Van Hoye - @WorkingHardInIT

Technical Architect & Technology Strategist



 <http://blog.workinghardinit.work>

 @workinghardinit

 blog@workinghardinit.work

Azure Peering Services

Virtual WAN ←

ExpressRoute

VPN Gateway

S2S VPN

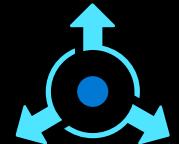
Connect & Extend

P2S VPN

MEC

# Azure Networking Services

Monitor



Internet Analyzer

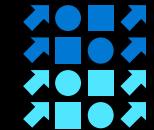
Network Watcher Traffic Analytics

Azure Monitor Insights for Virtual WAN

Log & Metrics



Protect



Deliver

Azure Firewall

Firewall Manager

Service endpoints/Private Link

WAF

Bastion

DDOS

IPv4/v6 in Azure VNETs

Virtual Network

Virtual Subnet

DNS

CDN

NAT Gateway

Load Balancer

Trafic Manager

Application Gateway

Front Door

# Dive Into Azure Virtual WAN

- What is it?
- Why use it?
- HUBs/Routing/  
Connections/Gateways
- Secured Virtual Hubs
- Azure Monitoring

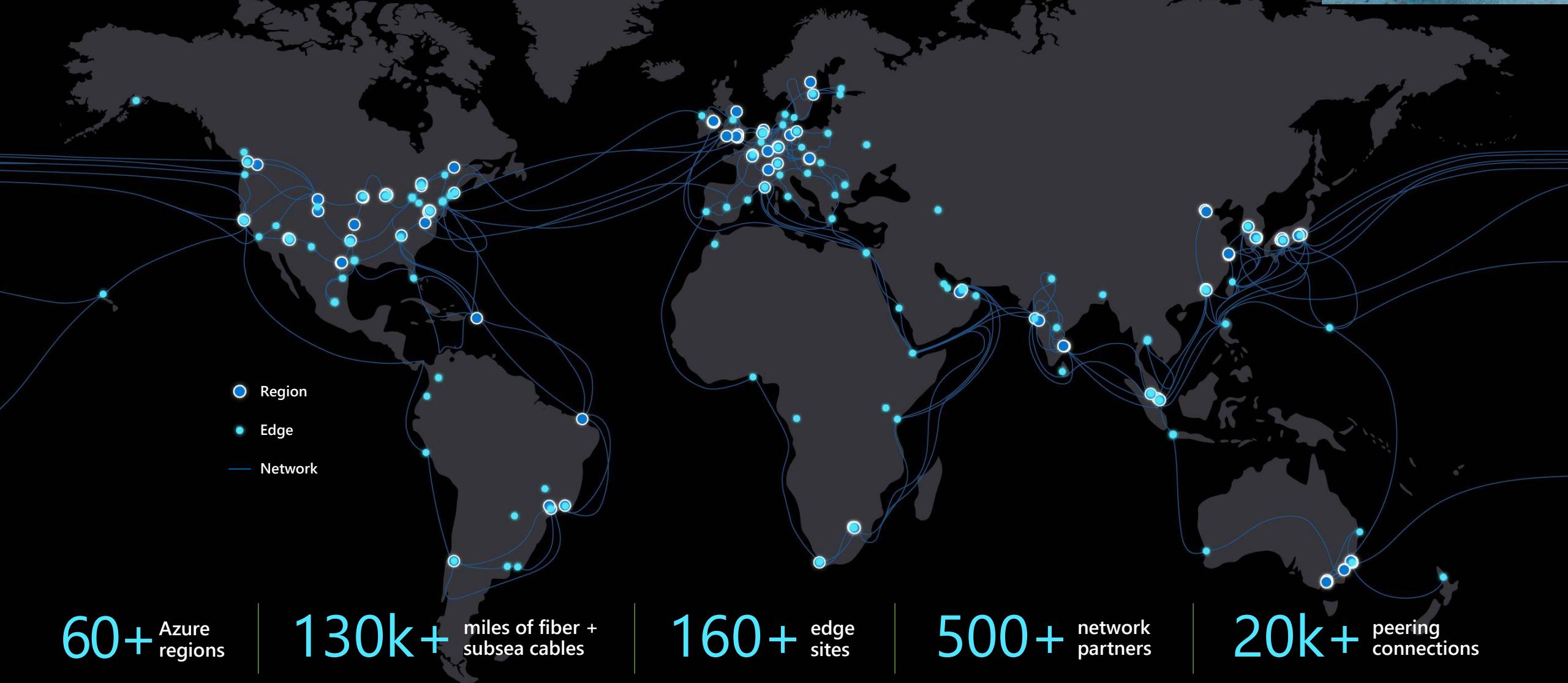


# What is Azure Virtual WAN?

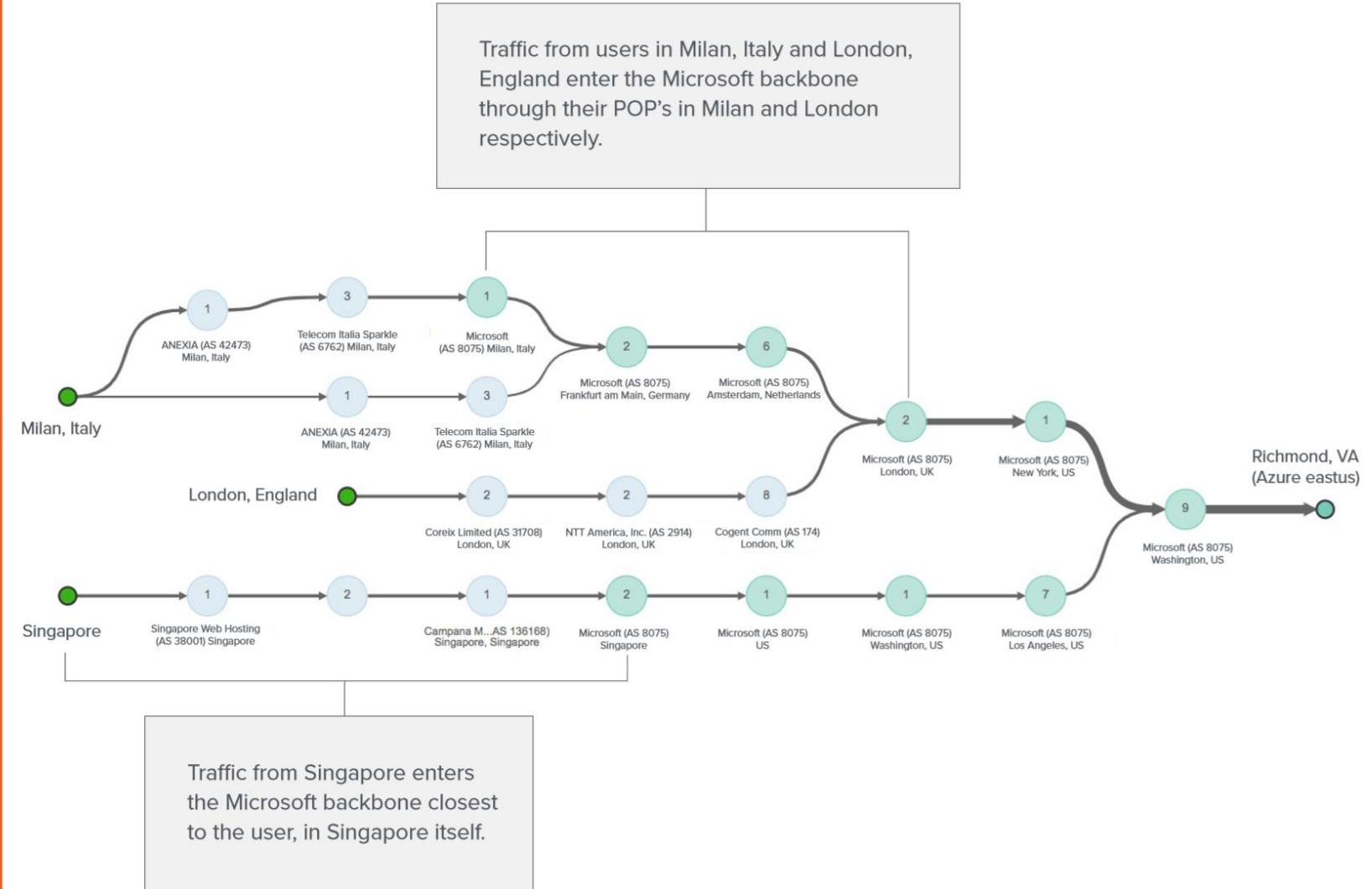
- ❑ A global networking service (GA November 2019) that allows us to easily leverage the Azure network backbone to build private, high-speed, global transit network architectures.
  - ❑ Use the Azure global network backbone to connect customer locations to Microsoft Azure & each other.
1. What is so special about the Azure Global Backbone?
  2. Wait a minute! We can already do that can we not?



# Microsoft global network



1.6 Pbps of aggregate inter-datacenter bandwidth within a region

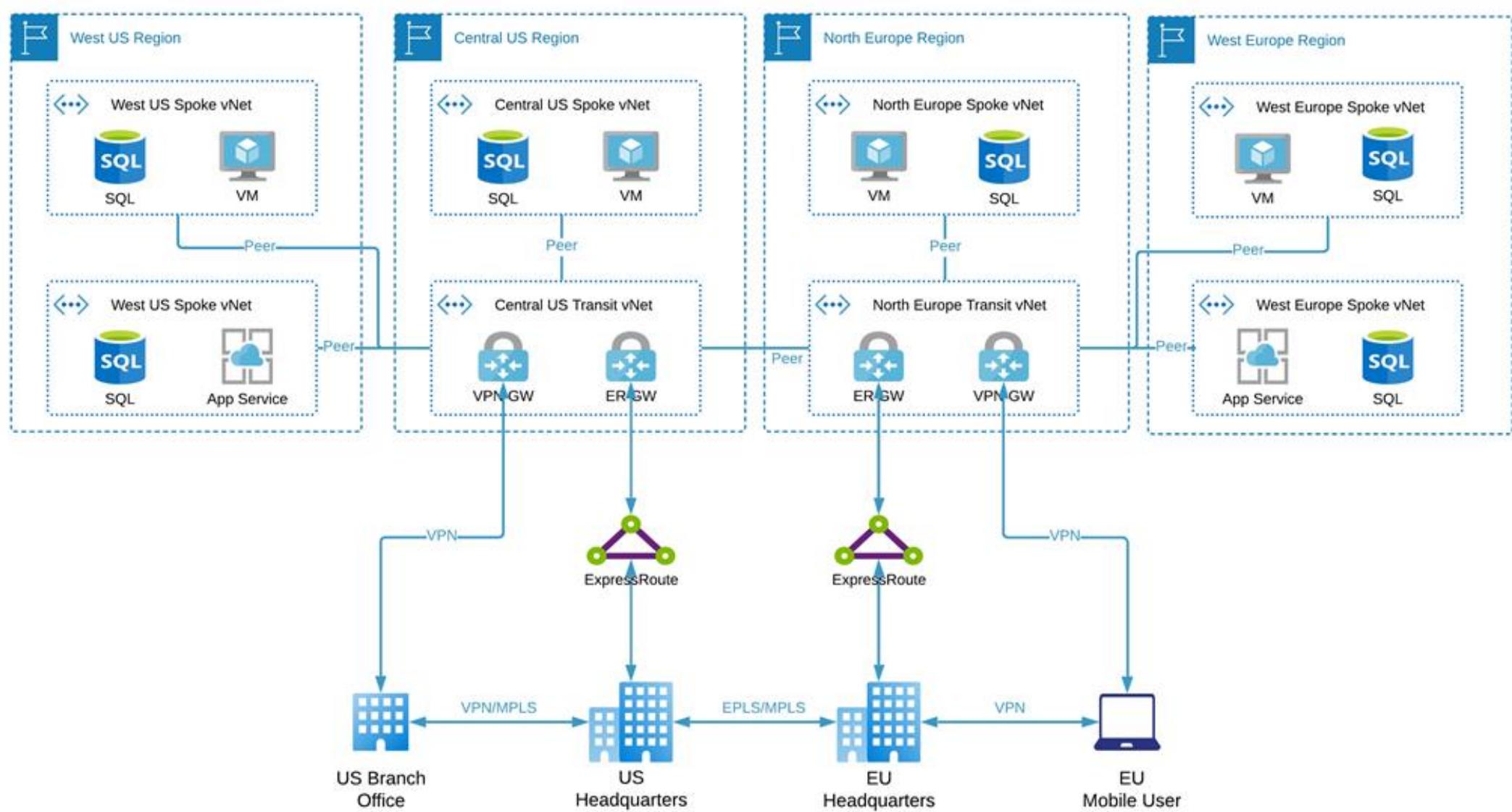


**FIGURE 6**

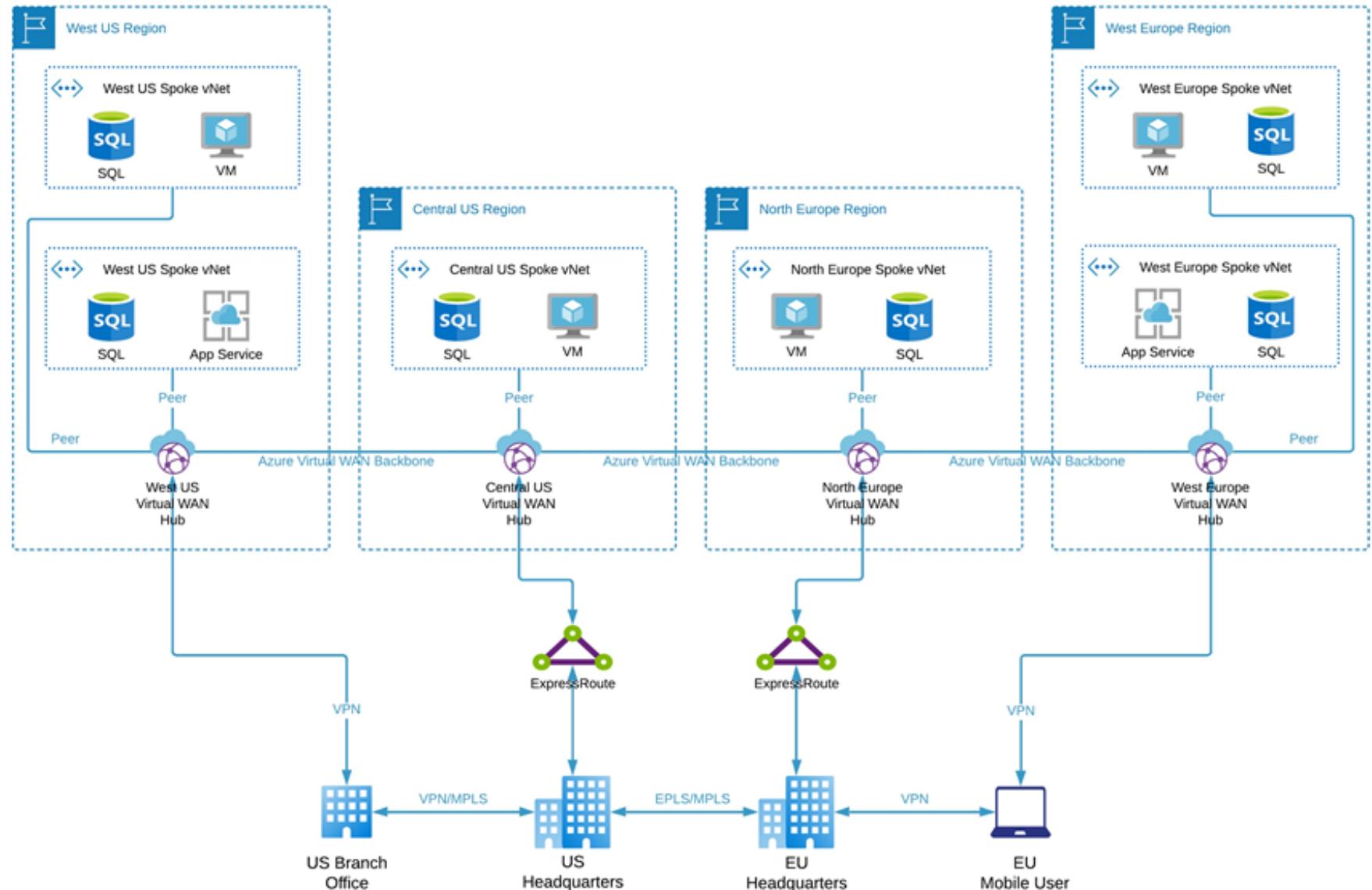
Azure connectivity architecture

<https://www.thousandeyes.com/resources/cloud-performance-benchmark-report-november-2019>

# Traditional approach

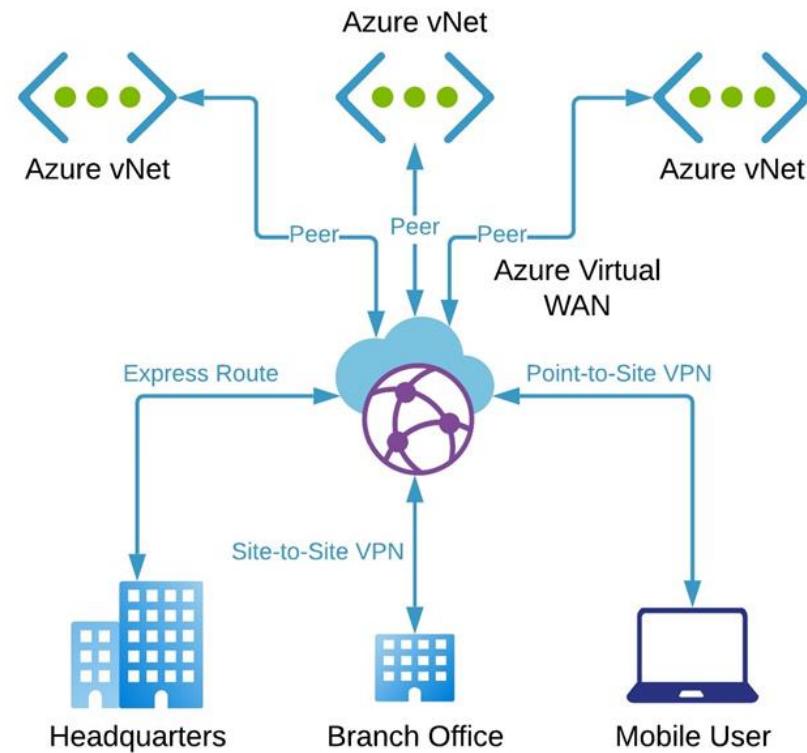


# Azure Virtual WAN approach

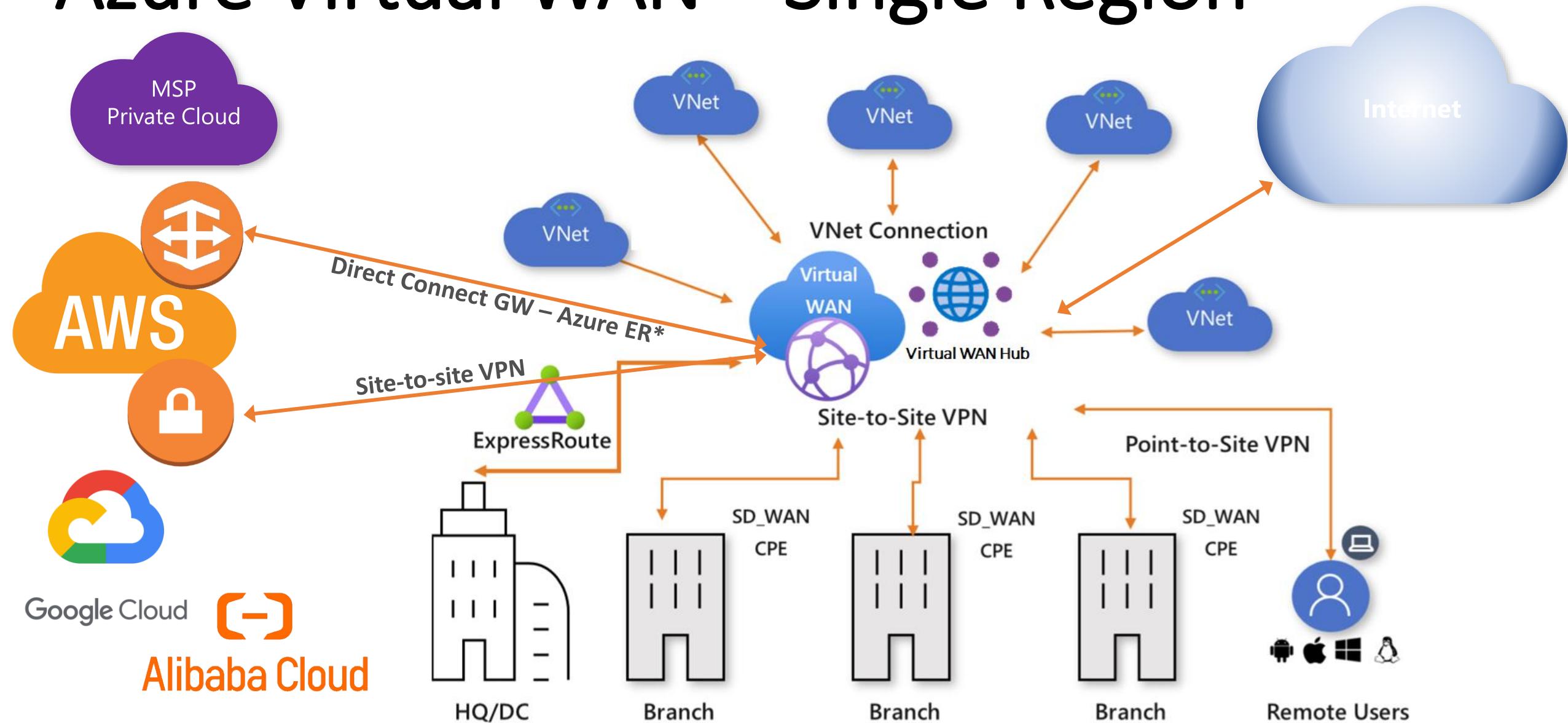


# Azure Virtual WAN offers more

- ❑ Global Transit: centralized, easier, **transitive** vNET-to-vNET, branch-to-vNet and branch-to-branch connectivity
- ❑ Connectivity options: Use Site-to-Site VPN, Point-to-Site VPN and Express Route to link sites to Virtual WAN Hubs.
- ❑ Routing: Default, None, Custom
- ❑ Integrates with Azure Firewall via Firewall Manager
- ❑ Partners => integrated solutions provide automated branch connectivity, NVA's and services
- ❑ Monitoring in Azure



# Azure Virtual WAN – Single Region



# Azure Virtual WAN Components (1/4)

## ❑ Virtual WAN



- ❑ The control plane of your private, globally distributed network which contains multiple resources that comprise the Azure Virtual WAN.

## ❑ Virtual WAN Hub: the regional core of a virtual WAN



- ❑ Contains a hub gateway that serves as a connection point for branches, users and virtual networks.
- ❑ You can deploy only 1 hub/region based on proximity to datacenters, branch offices and end users.
- ❑ Replaces DIY Transit vNET hub construct with its VNG, virtual networks, firewall, route tables) along with manual peering and full mesh peering required. All traffic flows through the Virtual WAN Hub.
- ❑ They are assigned an address space upon creation

# Azure Virtual WAN Components (2/4)

## ❑ Hub Connectivity

- ❑ Site-to-site VPN, point-to-site VPN and Express Route (Branch Connections).
- ❑ Virtual Network Connection: virtual networks (spokes) to the Virtual WAN Hub
- ❑ Max 500 spokes (peering limitation)

### Connectivity

---



Hubs



VPN sites



User VPN configurations



ExpressRoute circuits



Virtual network connections

# Azure Virtual WAN Components (3/4)

## ❑ Hub-to-Hub Connectivity

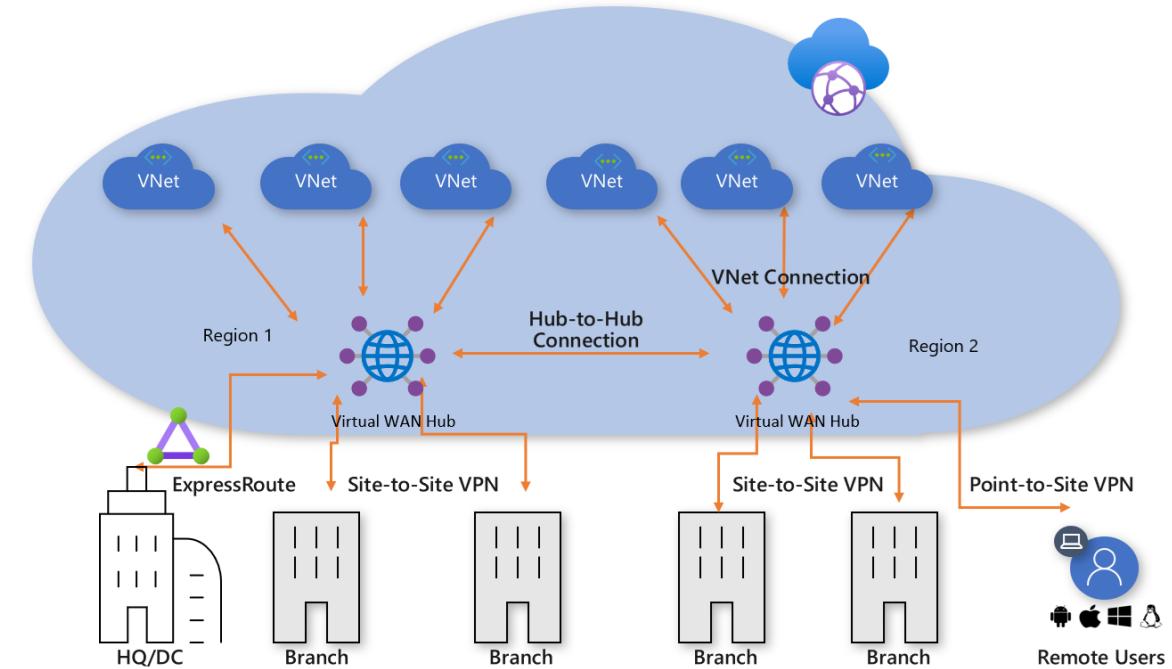
- ❑ Provides global interconnection of hubs deployed in various regions under a common Virtual WAN Service

## ❑ Hub Route Tables

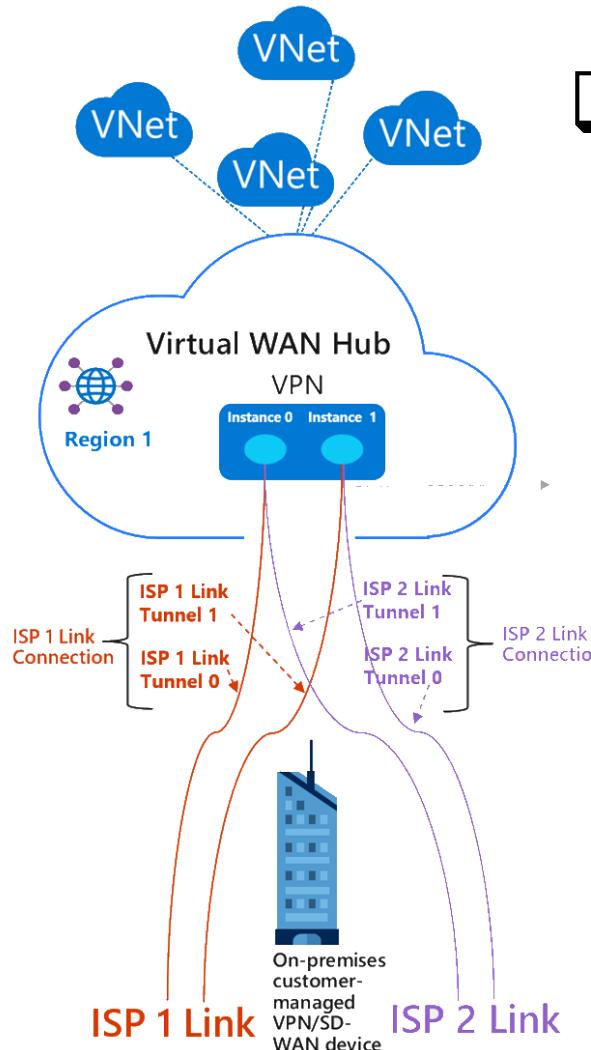
- ❑ The regional routing construct
- ❑ Populated manually or dynamically using BGP

## ❑ None Route tables

## ❑ Custom Route Tables for vNETs



# Azure Virtual WAN Components (4/4)

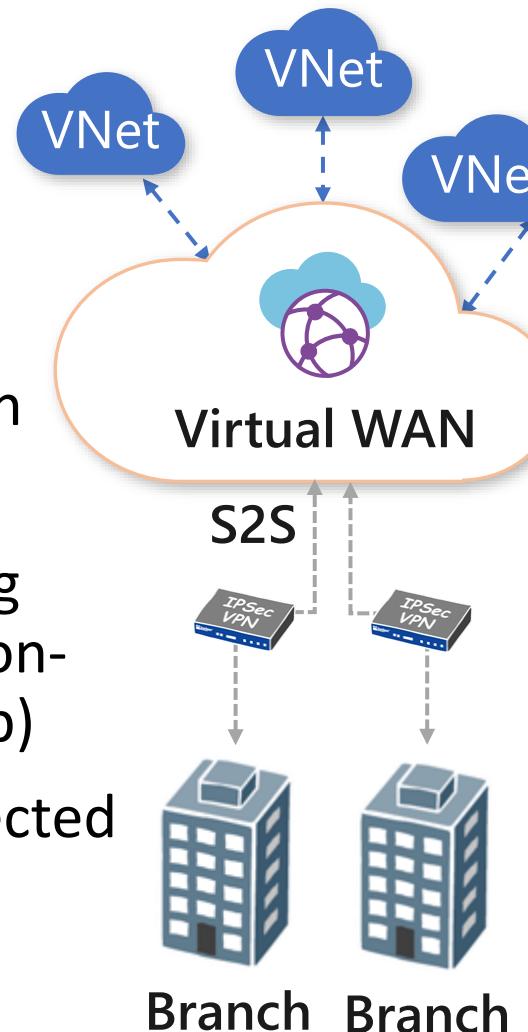


- ❑ **VPN Site:** customer end branch location for site-to-site VPN connections into Virtual WAN Hubs.
- ❑ **Links:** Represents the actual connectivity between the site & the remote site.
  - ❑ A site link has an active-active tunnel construct for failover.
  - ❑ A site can have multiple links (max 4) for bandwidth aggregation & redundancy (failover, auto path selection)

# Azure Virtual WAN Types

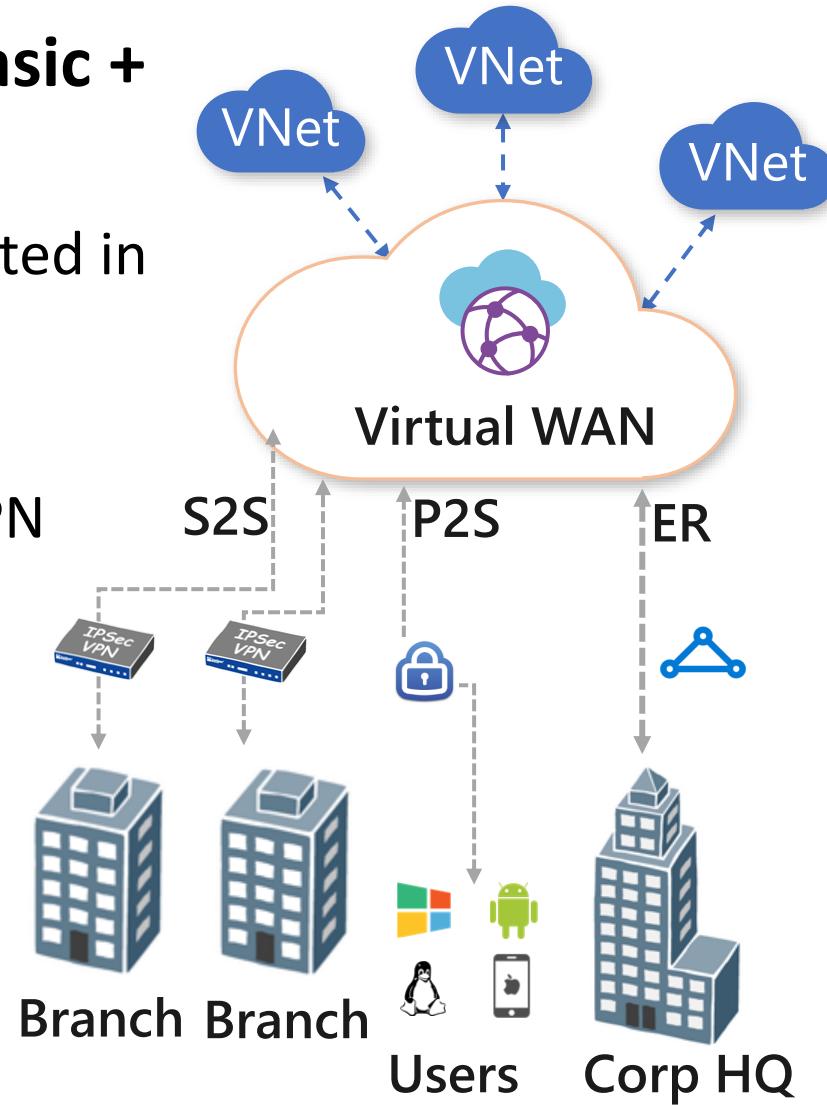
## Basic

- S2S VPN only
- Branch to Azure
- Azure to Branch
- Branch to Branch
- Connect VNET
  - DIY VNet Peering (VNet to VNet non-transitive via hub)
- Hubs are not connected
- Scale!



## Standard = Basic + following

- Hubs connected in full mesh
- ExpressRoute
- User (P2S) VPN
- Any-to-any transitive connectivity
- Scale!



# Site-to-Site (S2S) VPN

## Multi Link support

### Dynamic traffic distribution across ISP at the branch site

- 1 connection with path selection across multiple links ( $\neq$  ISP's) to Azure
- Lots of hardware & Virtual appliance partners

### Always-on redundant access to cloud-based resources

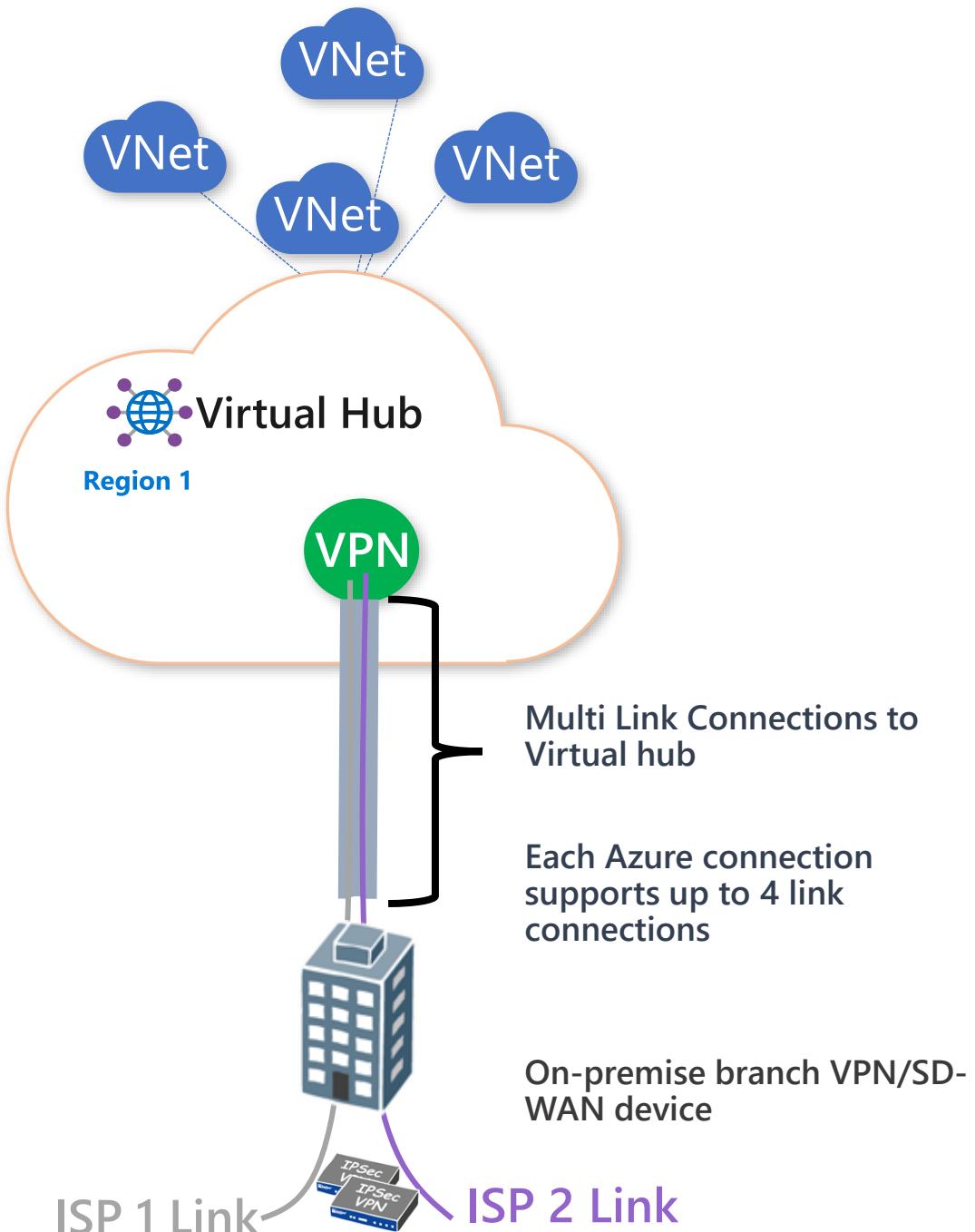
- Automatic path failover in case of ISP failure
- Improved reliability
- Possible TCO reduction

## Scale

- Up to 20 Gbps aggregate throughput (1 scale unit = 500 Mbps)
- 1000 S2S connections per hub

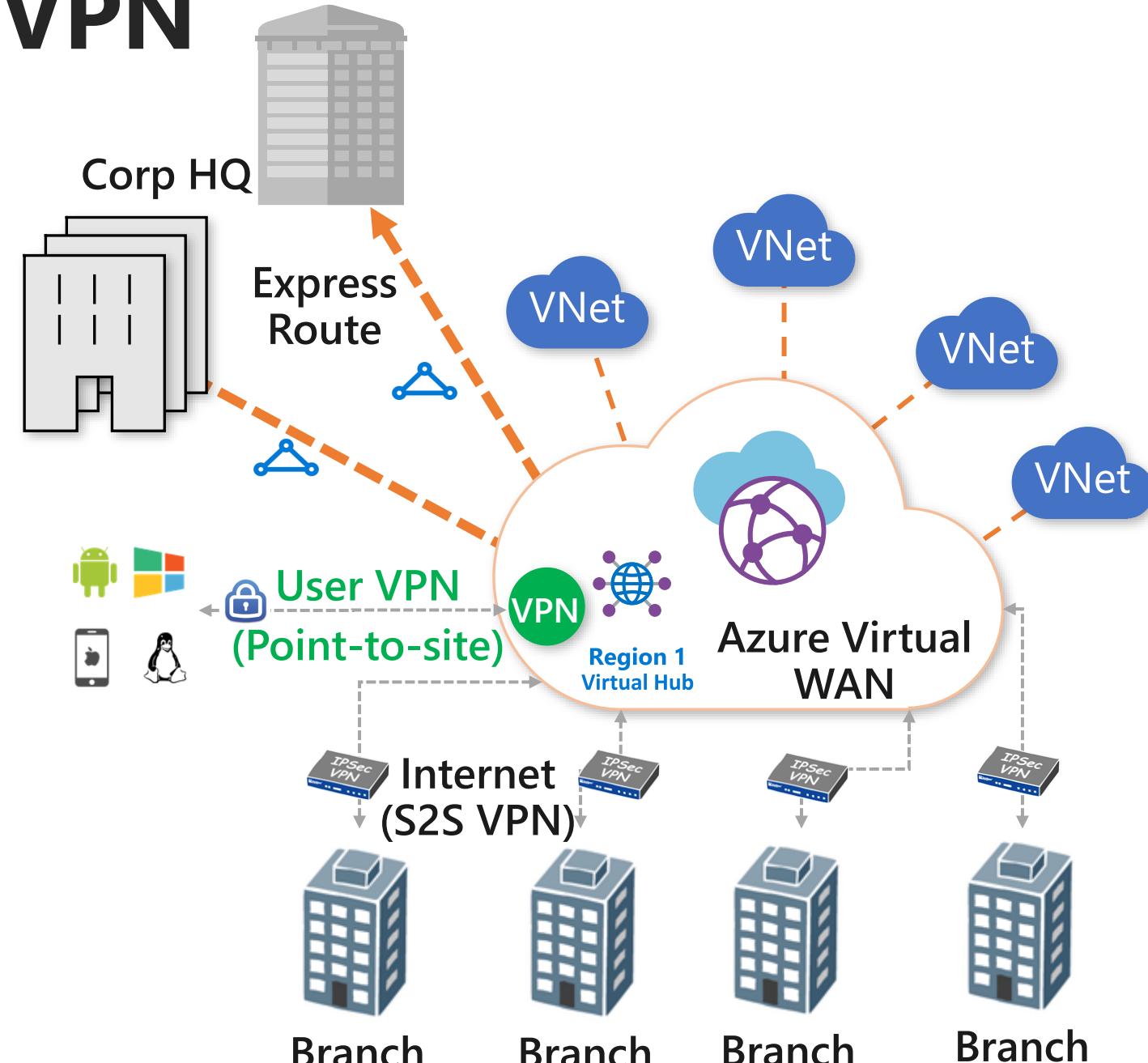
## IKEv1 & IKEv2

## FQDN based IPsec, Dynamic DNS support in Azure, CustomBGP/APIPA (AWS)



# Point-to-Site (P2S)VPN

- Only in **Standard Virtual WAN**
- Scale:**
  - Up to 20 Gbps aggregate throughput & 10K users per hub
- Cloud based secure remote access**
  - Works with OpenVPN (Azure VPN client) and IKEv2 client
  - Cert based & RADIUS authentication or Azure AD
  - IP or **FQDN** Based & **Custom DNS**
- Any-to-any**
  - User to Branch , User to Azure VNET
- Integrated with Azure Monitor**
  - Metrics



# ExpressRoute

Only in **Standard Virtual WAN**

**Scale:** Up to 20 Gbps aggregate throughput (1 scale unit = 2 Gbps)  
Up to **8** circuits/region (up from 4)

**Private Connectivity**

Premium Circuit in Global Reach Location

**Standard** Circuit within geopolitical region (disables branch-to-branch) or **Local** circuit (spokes in same region)

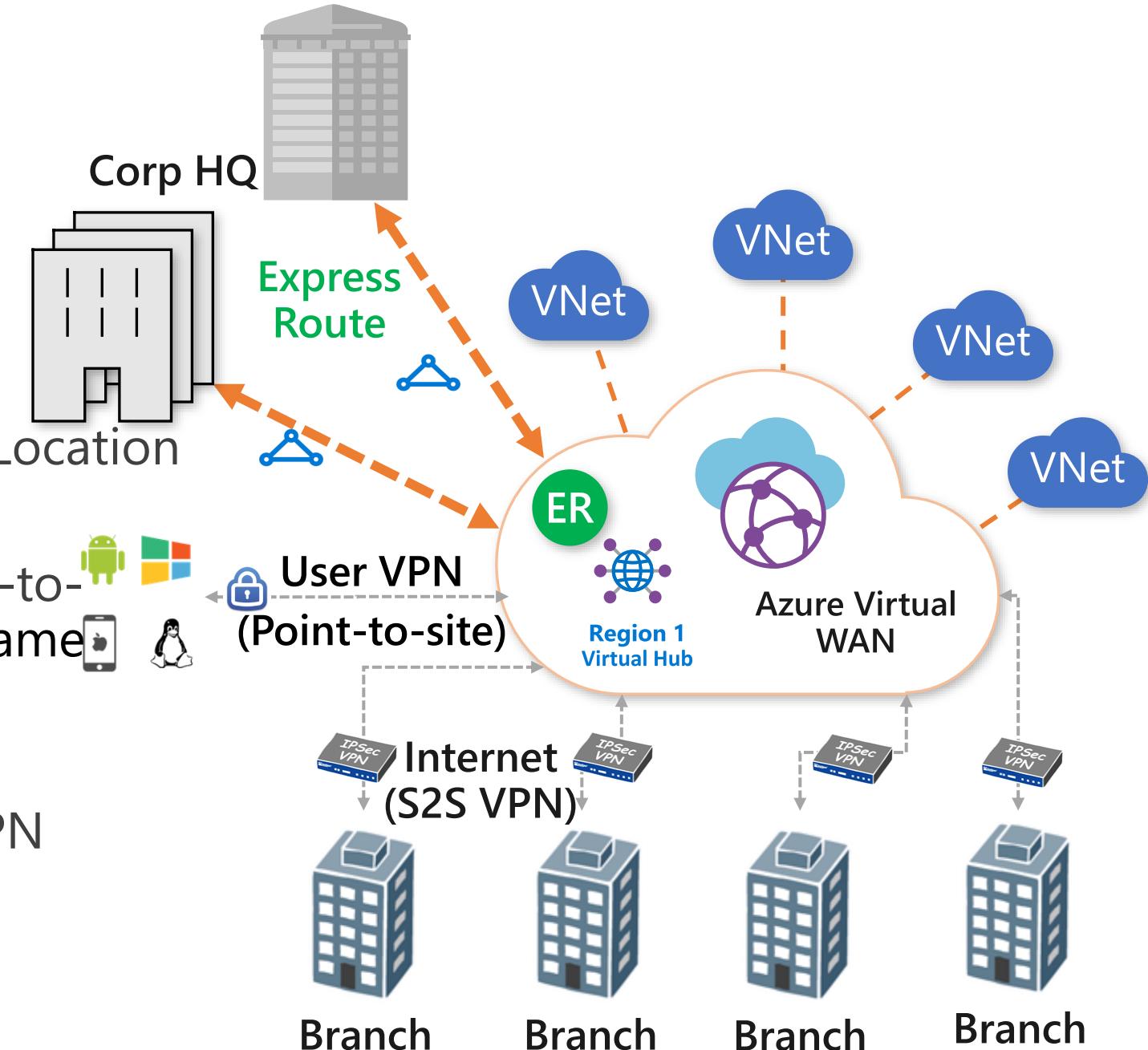
**ExpressRoute VPN Interconnect**

ExpressRoute & S2S/ P2S User VPN

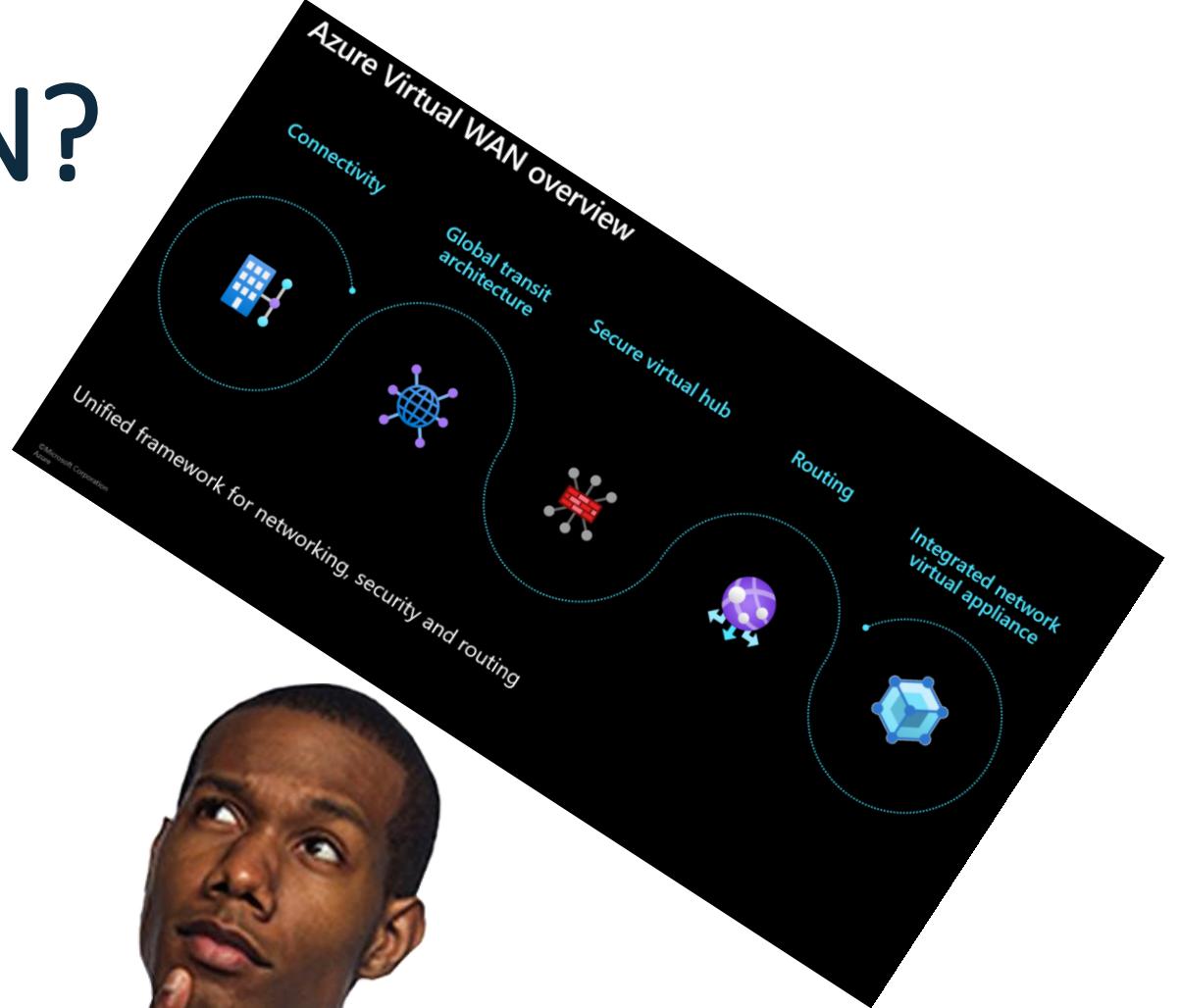
**Encrypt your traffic over ER**

**ER to ER via Global Reach**

**Integrates with Azure Monitor**

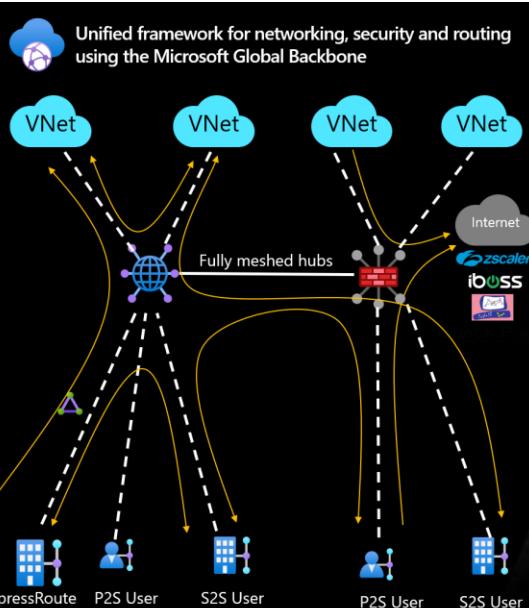


# Why Azure Virtual WAN?



## Putting it together

VPN, ER	FW : Per hr. Per GB		
- Throughput : \$/scale unit	Virtual Hub : Per hr. Per GB		
- Connection : \$/conn unit	Hub to hub : Source Destination based Egress only charges		
<b>vWAN pricing</b>			
<b>vWAN routing enabled capabilities</b>			
Microsoft managed hub	Unified framework for networking, security and routing using the Microsoft Global Backbone		
Virtual Hub Router – automatic hub to hub			
Virtual Hub Router – Fully meshed hubs			
Transit between VPN and ExpressRoute, VNets			
Custom Routing			
Integrated Network Virtual Appliance (NVA)			
<b>vWAN unique</b>			
ER	P2S	S2S	FW
Encryption	Traffic mgmt	connectivity automation	Manager Partners
8 ckt/Hub	10,000/Hub	1,000/Hub	500/Hub
20 Gbps agg	18 Gbps agg	20 Gbps agg	50 Gbps agg
<b>vWAN scale</b>			
ExpressRoute	User/P2S VPN	Site/S2S VPN	VNet
Azure FW			
<b>Connectivity &amp; Security</b>			



# Azure Virtual WAN Benefits (1/2)

- Operational efficiencies & scalability
  - Simplified architecture by replacing transit vNets with the Virtual WAN Hubs.
  - Simpler in network design and routing architecture.
  - Reduce operational cost → ease of use & automation (3<sup>rd</sup> party appliances, MSPs,...)
  - Increased scale for S2S and P2S VPN tunnels
    - 10Gbps → 20Gbps: doubles overall aggregate VPN throughput (20Gbps S2S + 20Gbps P2S)
    - 10K Users per hub
    - 1000 S2S connections per hub
  - Higher overall throughput (20Gbps S2S + 20Gbps P2S) + 20Gbps ExpressRoute
- Redundancy & high availability
  - Virtual WAN Hubs are zone redundant by default.
  - No worries about selecting zone redundant SKUs for VPN & Express Route Network Gateways.

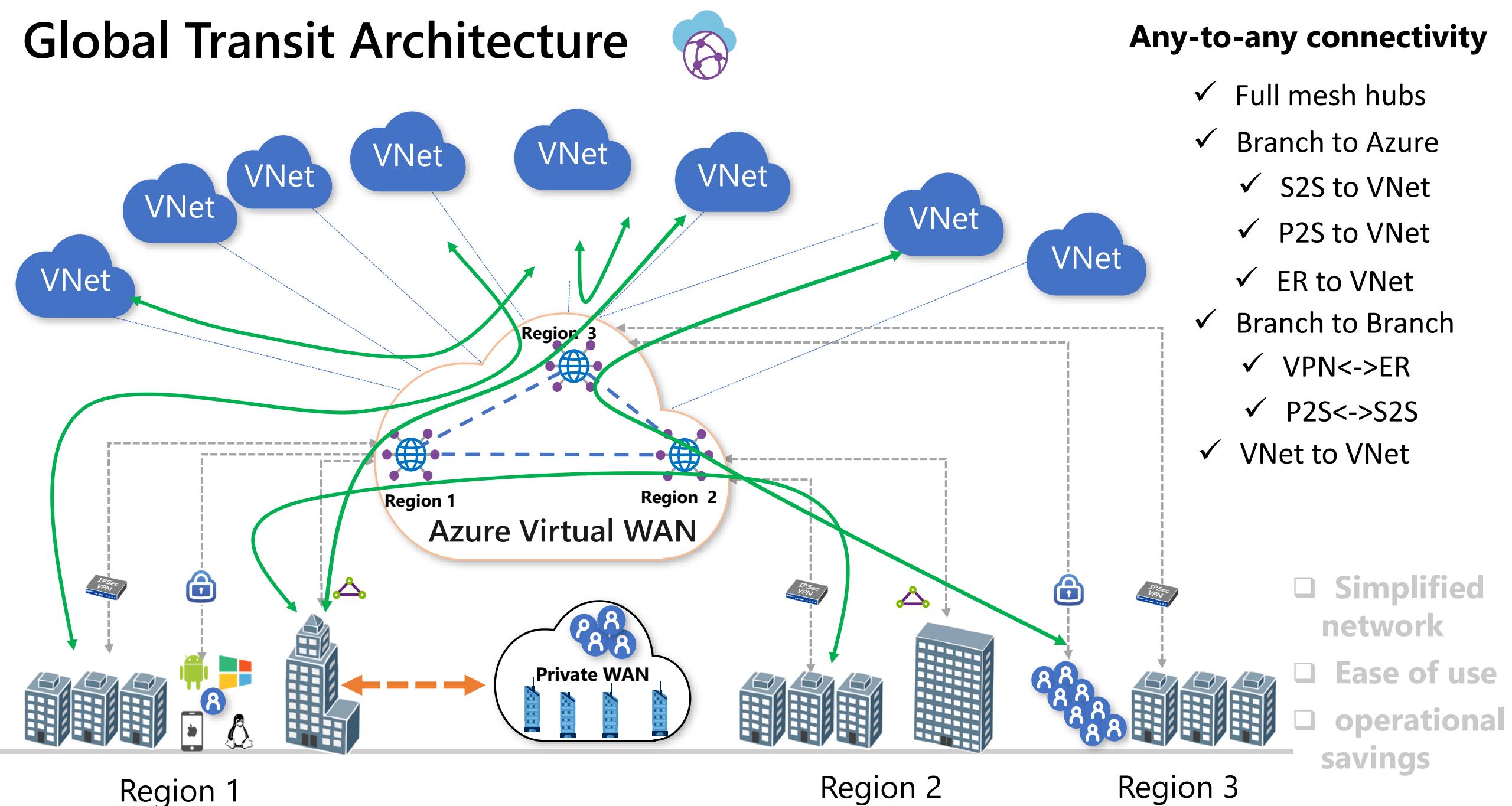
# Azure Virtual WAN Benefits (2/2)

## ❑ Any-to-Any networking

- ❑ All routing\* is performed within the Virtual WAN Hub. Any vNet that is peered to the Virtual WAN Hub will automatically trigger an update to the global routing table
- ❑ This eliminates the need to configure routing within the spoke vNet itself and/or establishing peering relationships between spoke vNets that need to communicate with each other.
- ❑ Hub-to-Hub means this is a global construct!

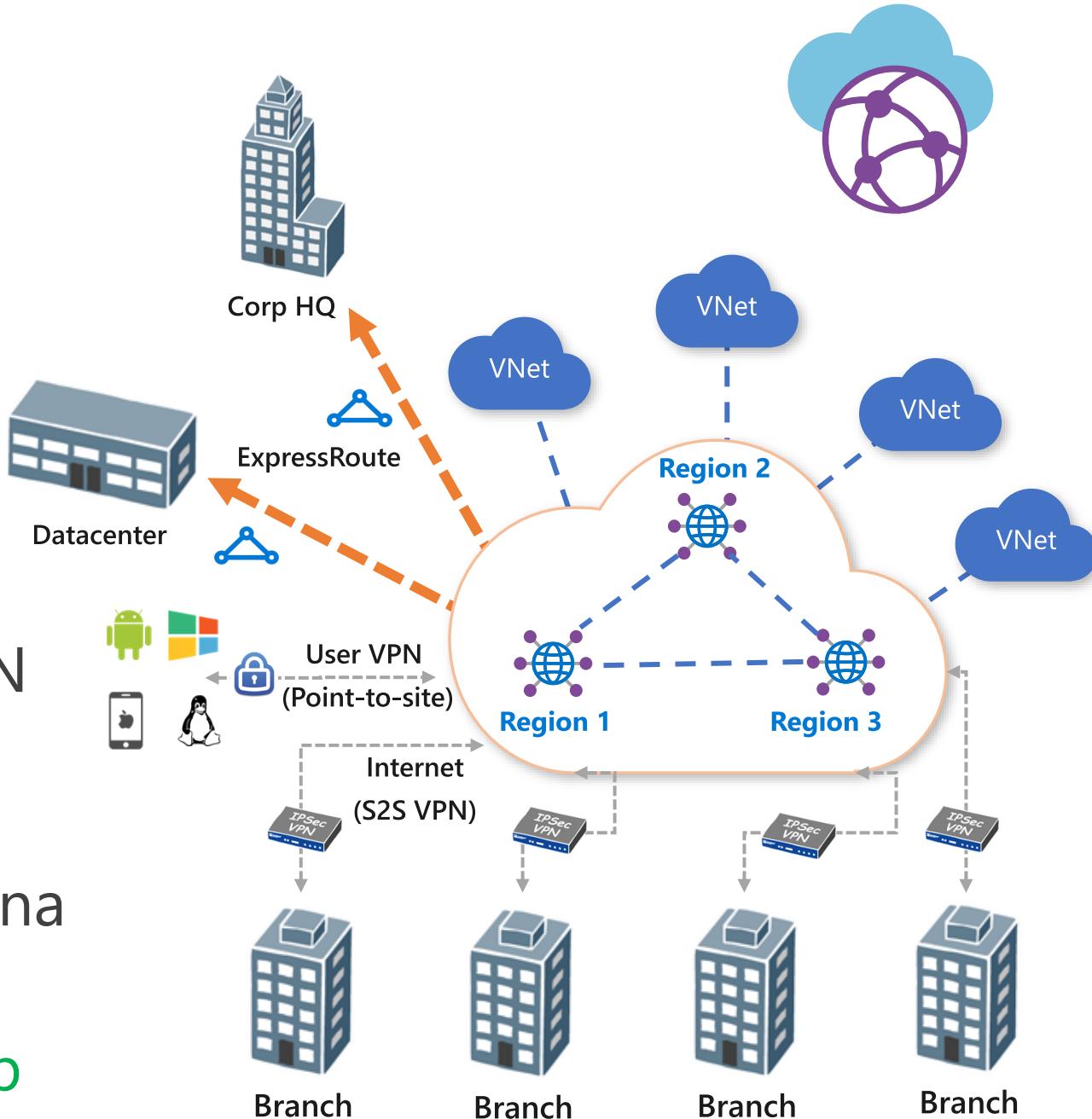
\*Exception: Express Route Premium + Global Reach bypass Virtual Hubs

# Global Transit Architecture



# State of the union

- Any-to-Any connectivity
- ExpressRoute, P2S, S2S
- ExpressRoute Encryption
- Hub-2-Hub
- Multi Link Azure Path Selection
- Custom IPsec
- Connect VNG VPN to Azure vWAN
- Azure Firewall (Manager) integration
- Also available in Gov Cloud & China
- Custom Route Tables
- Partners, NVA in Azure vWAN Hub



# 3<sup>rd</sup> Party Network Virtual & Physical Appliances

## Connectivity Automation Example



# Partner Example – Barracuda CGFW (1/2)

The screenshot shows the Barracuda Cloud Integration interface. The top navigation bar includes links for DASHBOARD, CONFIGURE, CONTROL, FIREWALL, VPN, DHCP, WI-FI, LOGS, STATISTICS, EVENTS, and SSH. The CONFIGURE tab is selected. A sub-menu for Cloud Integration is open, showing 'Cloud Integration - Azure Virtual WAN'. The main window displays the 'Azure Virtual WAN' configuration page. On the left, a sidebar under 'Configuration' lists 'Azure Networking', 'Azure Event Hub', 'Azure OMS', 'Azure Virtual WAN' (which is expanded), 'AWS Integration', 'AWS Cloudwatch', and 'AWS Autoscaling'. Below this is a section for 'Configuration Mode'. The central area shows 'Azure Virtual WAN Connections' with a table containing one row:

Name	Virtual WAN Name	Resource Group
SampleVirtual...	SampleVirtualWan	DidierTEST

A modal window titled 'Azure Virtual WAN Connections : SampleVirtualWan' is open, showing the configuration details for the connection:

Setting	Value	Description
Virtual WAN Name	SampleVirtualWan	The name of the Virtual WAN in Azure.
Resource Group	DidierTEST	The name of the resource group of the Azure Virtual WAN.
Subscription Id	[REDACTED]	The ID of the subscription containing the Virtual WAN.
Tenant Id	[REDACTED]	The tenant ID of the Azure account containing the Virtual WAN.
Client Id	[REDACTED]	The ID of the application used to authenticate to the Azure API.
Client Password	New: [REDACTED] Confirm: [REDACTED]	The password for the application used to authenticate to the Azure API.
Virtual Hub Name	SampleVirtualHub	The name of the virtual hub to which the CG will be associated.
Active	yes	

# Partner Example – Barracuda CGFW (2/2)

Site	Site Provisioning Status	Hub	Location	Link IP Address / FQDN	...
<input type="checkbox"/> F280	✓ Provisioned	▼ 1 hubs	West Europe	▼ 1 links	...
		✓ SampleVirtualHub - Con...			...
<input checked="" type="checkbox"/>					...

DASHBOARD   CONFIGURATION   CONTROL   FIREWALL   **VPN**   DHCP   WI-FI   LOGS   STATISTICS   EVENTS   SSH

Site-to-Site   Client-to-Site   Status   Filter   NAC:0 (1) - Clients:0 (9999) 0 (9999) - SSL:0   Refresh always   Refresh (F5)

Name	Info	Tunnel	Local IP	Peer IP	Transport	Encryption	Compression	bit/s	Start
vwanSampleVirtualWanSCARLETwesteuropeInstance0		IPSec-IKEv2	0.0.0.0	0.0.0.0			0%	0	7/31/2020 3:06:43 ...
vwanSampleVirtualWanSCARLETwesteuropeInstance0		IPSec-IKEv2	[REDACTED]:4500	[REDACTED]:4500	ESPoUDP	AES256	0%	0	7/31/2020 3:06:43 ...
vwanSampleVirtualWanSCARLETwesteuropeInstance1		IPSec-IKEv2	0.0.0.0	0.0.0.0			0%	0	7/31/2020 3:06:43 ...
vwanSampleVirtualWanSCARLETwesteuropeInstance1		IPSec-IKEv2	[REDACTED]:4500	[REDACTED]:4500	ESPoUDP	AES256	0%	0	7/31/2020 3:06:43 ...

# Connectivity Automation



Coming Soon



**MSP Partners**  
providing Azure  
Virtual WAN Services

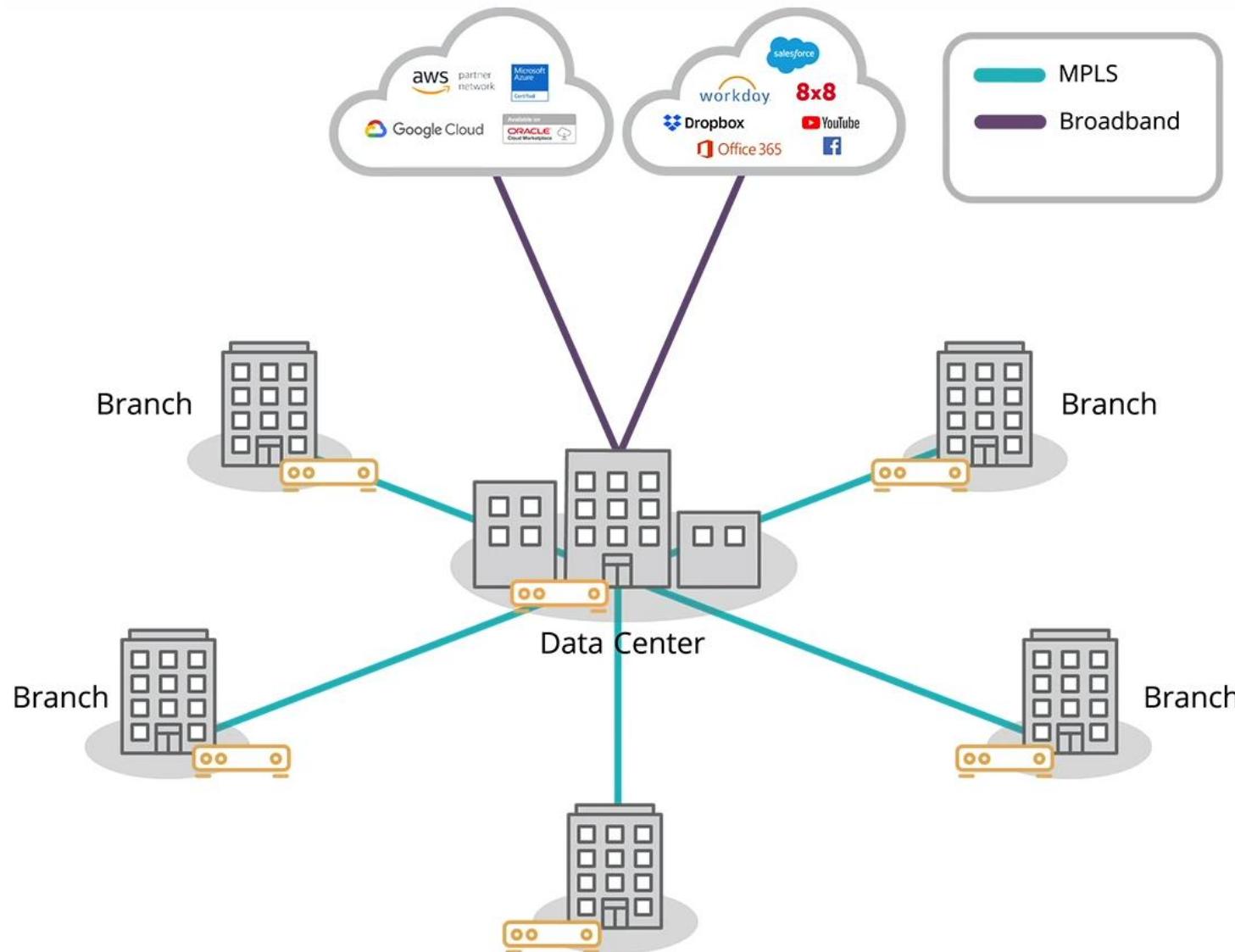


Create a NVA in an Azure Virtual WAN hub (Preview): <https://docs.microsoft.com/en-us/azure/virtual-wan/about-nva-hub>

# Small & Medium Sized Enterprises

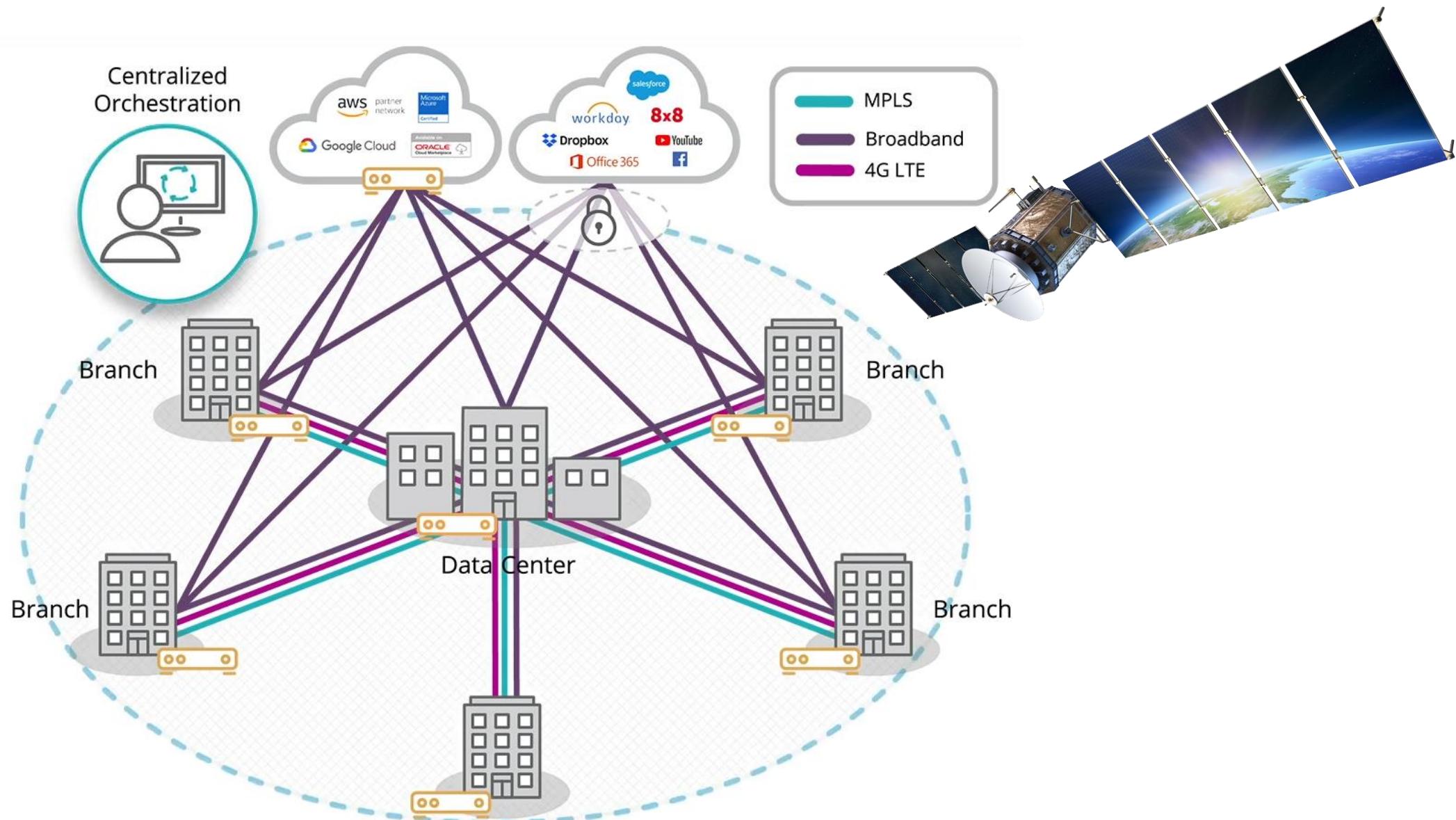


# MPLS



<https://www.silver-peak.com/sd-wan/sd-wan-explained>

# MPLS

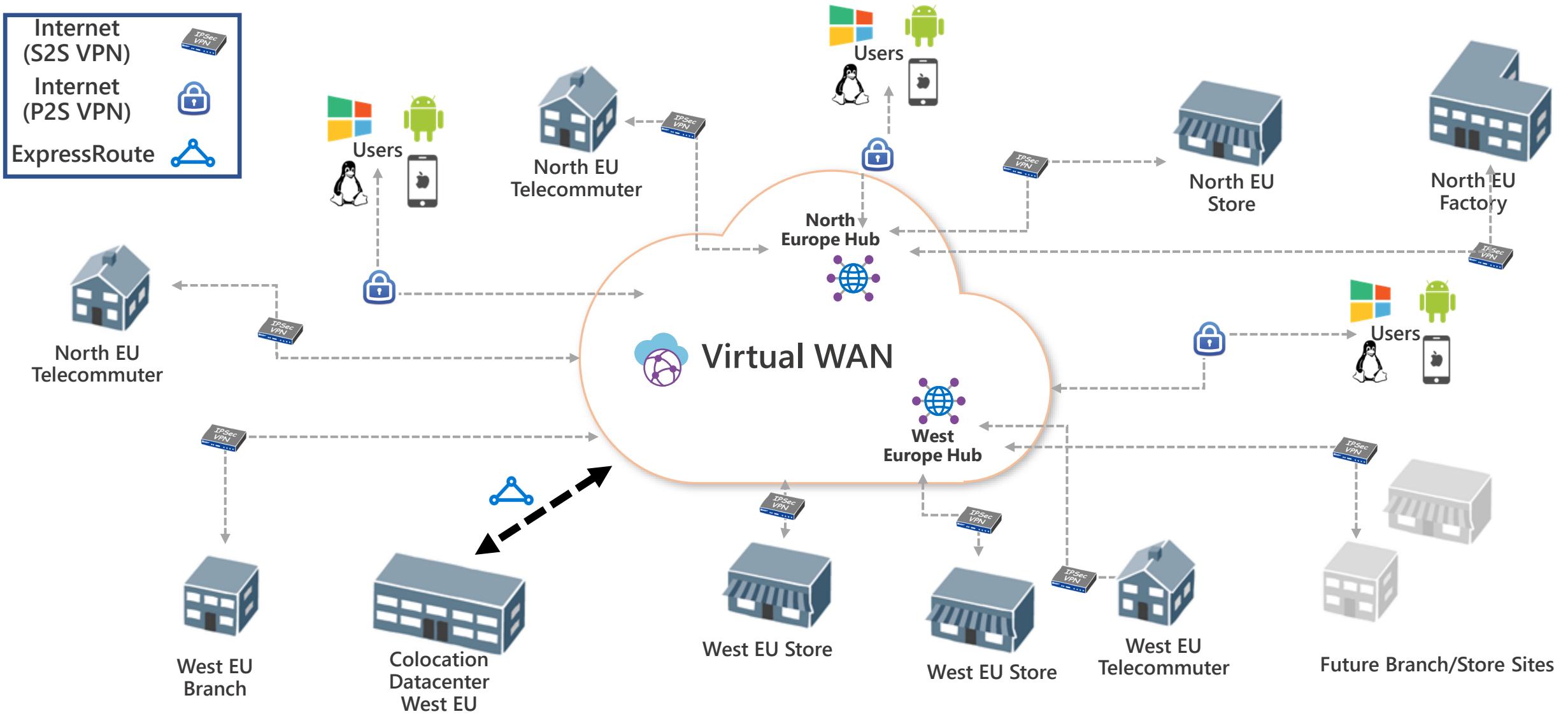


<https://www.silver-peak.com/sd-wan/sd-wan-explained>

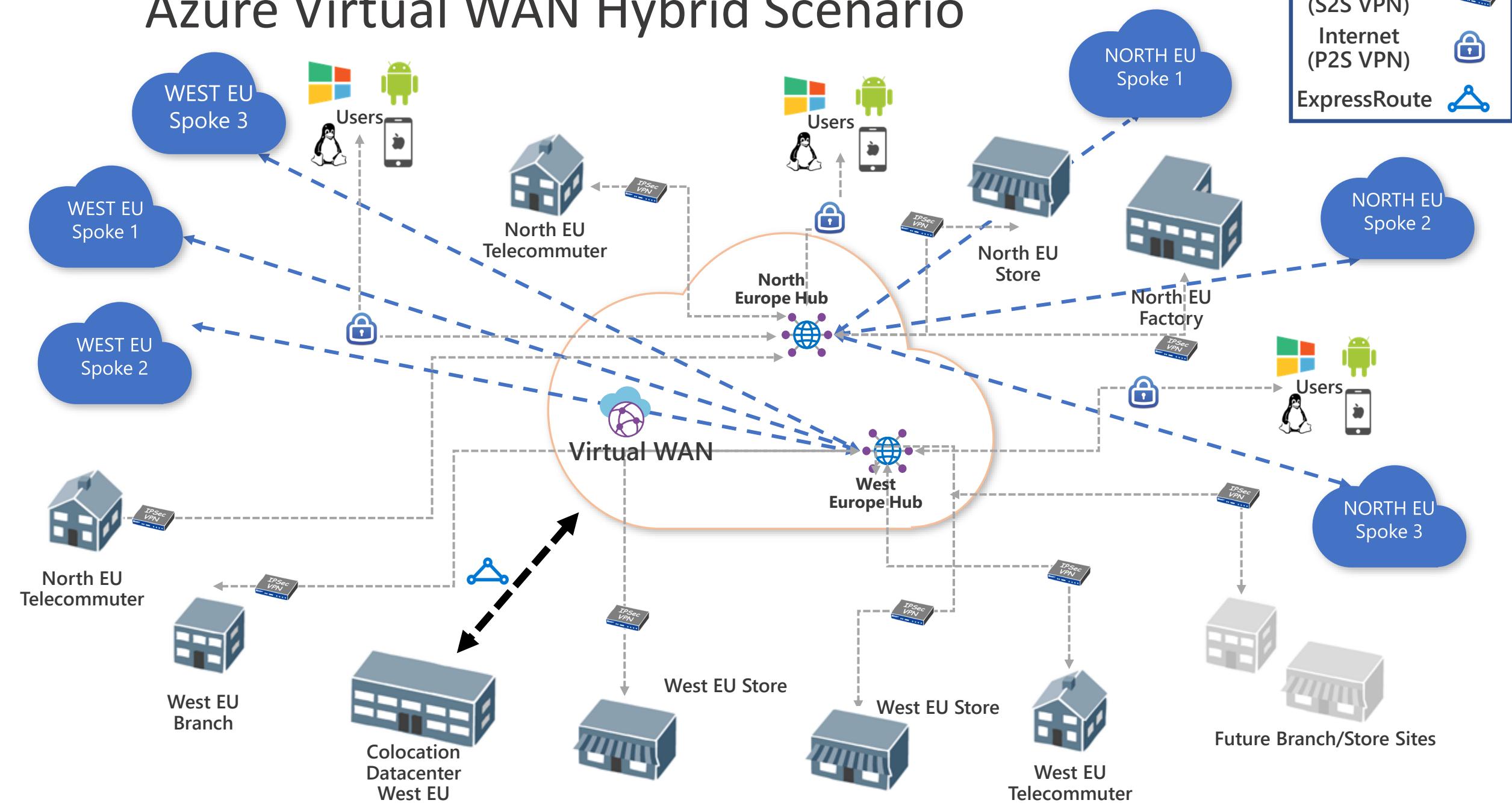
# Benefits for SME

- Same as for multinationals ...
- ... with the exception of scale
- Definitely the way to go and future proof designs
- SME also require 2 regions to design for failure

# Azure Virtual WAN only used as SD-WAN carrier

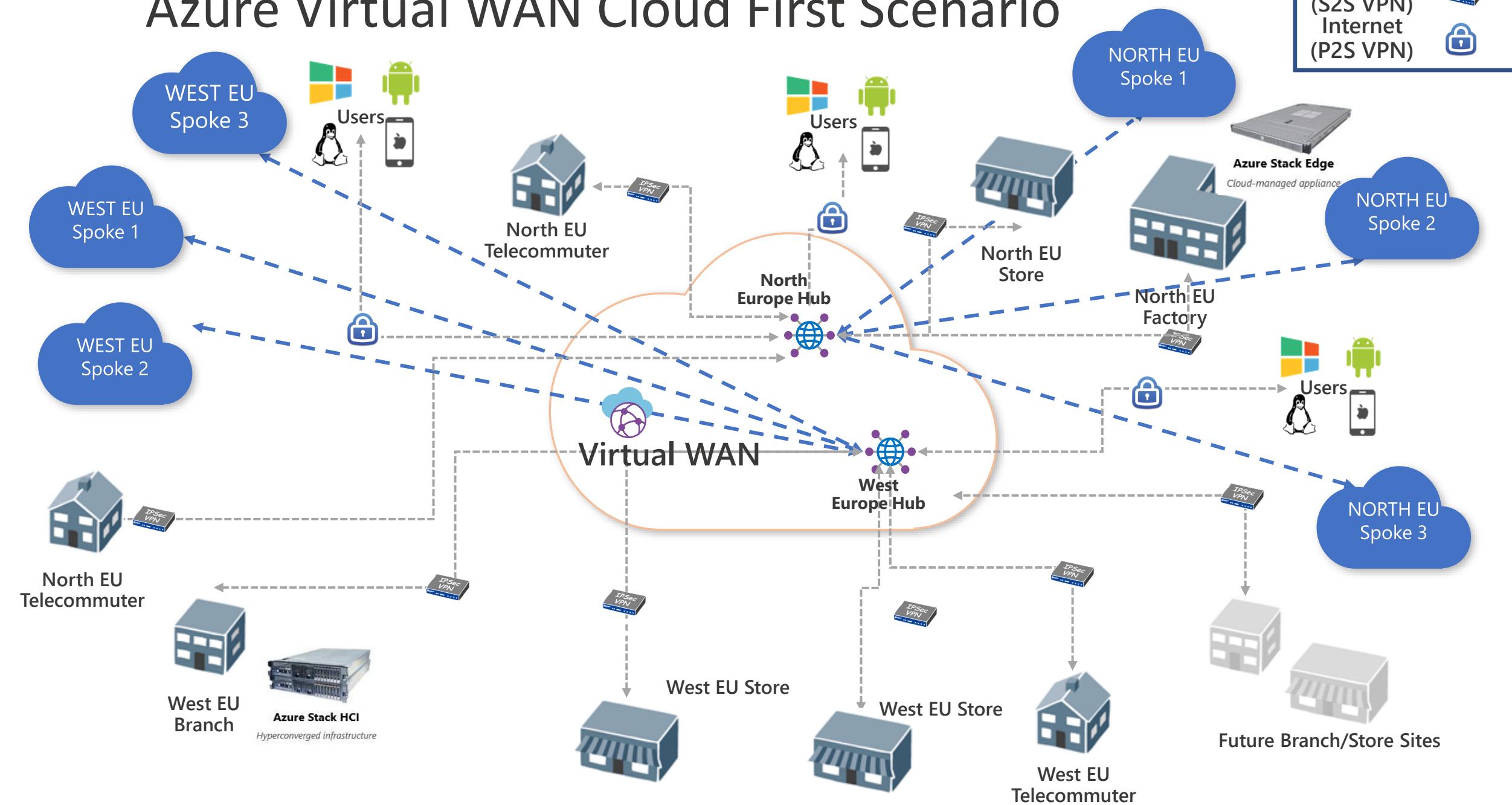


# Azure Virtual WAN Hybrid Scenario

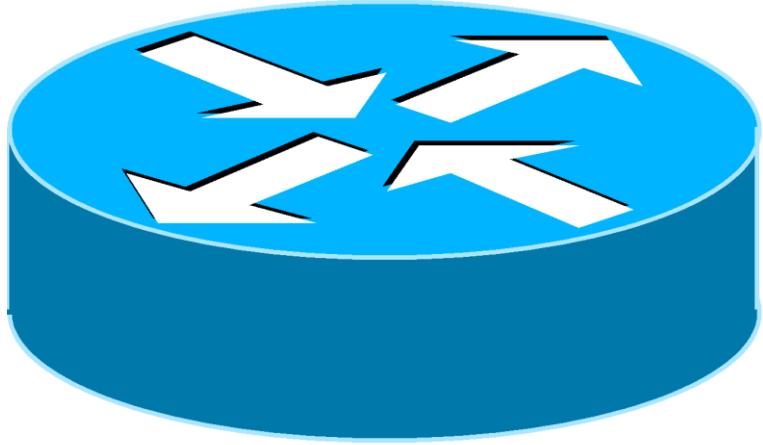


# Azure Virtual WAN Cloud First Scenario

Internet  
(S2S VPN)  
Internet  
(P2S VPN)

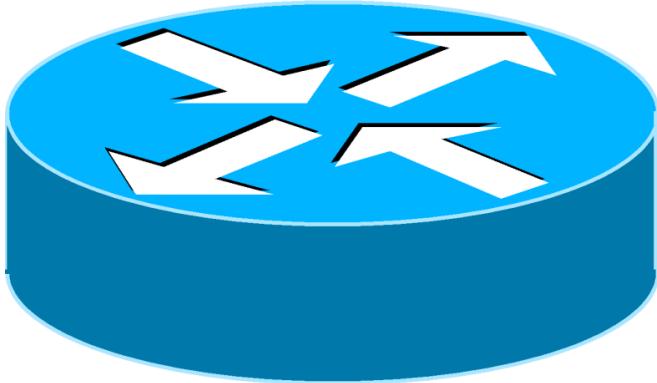


# Azure Virtual WAN - Routing



- ❑ Every virtual hub has a router (hidden)
- ❑ A virtual HUB router has a capacity of 50Gbps
- ❑ It controls the connectivity between all gateways:
  - S-2-S
  - P-2-S
  - ExpressRoute
- ❑ Delivers VNet transitive peering (hub-spoke)
- ❑ Three types route table exist:
  - Default Route Table
  - None Route Table
  - Custom route Table(s) - Optional

# Azure Virtual WAN - Custom Routing



## Create Route Table

Basics Labels Associations Propagations

Labels Name

TEST

## Create Route Table

### Current settings (Routing Configuration) of branches

Associated to: defaultRouteTable

Propagating to: defaultRouteTable

### Virtual Networks

Associating a Virtual network connection to a route table allows the traffic to be sent from the Virtual network connection to the selected route table. A connection can only be associated to one route table

Choose virtual network(s)

TEST-VNET-02

### Current settings (Routing Configuration) of Virtual Network Connections

Name	Associated to	Propagating to
itopstest-virtualwanhub-vnet	defaultRouteTable	defaultRouteTable
TEST-VNET-02	defaultRouteTable	defaultRouteTable

Review + create

Previous

Next : Associations >

Review + create

Previous

Next : Propagations >

## Create Route Table

Basics Labels Associations Propagations

ⓘ Creating propagation will allow routes to be propagated from a connection to the selected route table. A connection can be propagated to multiple route table.

### Branches (Site VPN/ExpressRoute/User VPN)

All VPN sites, ExpressRoute circuits and User VPN connections on each hub propagate to same Route Tables

Propagate routes from connections to this route table?  Yes  No

Propagate routes from all branch connections to these labels across virtual WAN

### Current settings (Routing Configuration) of branches

Associated to: defaultRouteTable

Create

Previous

Next

# Custom Routing

- Virtual WAN received routing enhancements
  - Ability to set up **custom route tables** for VNETs
  - Optimize virtual network routing via route **association & propagation**
  - Logically group route tables with **labels**
  - Helps achieve numerous network routing scenarios (isolation, access to shared services, virtual network appliances)

<https://docs.microsoft.com/en-us/azure/virtual-wan/about-virtual-hub-routing>



# Edit VNet Connection



Some of the functionality may not be accessible as it is currently being rolled out and expected to complete in the week of Aug 3rd.

Propagate Default Route ⓘ Enable Disable

Routing configuration

Select Route Tables for this connection

Associate Route Table

Propagate to Route Tables

0 selected

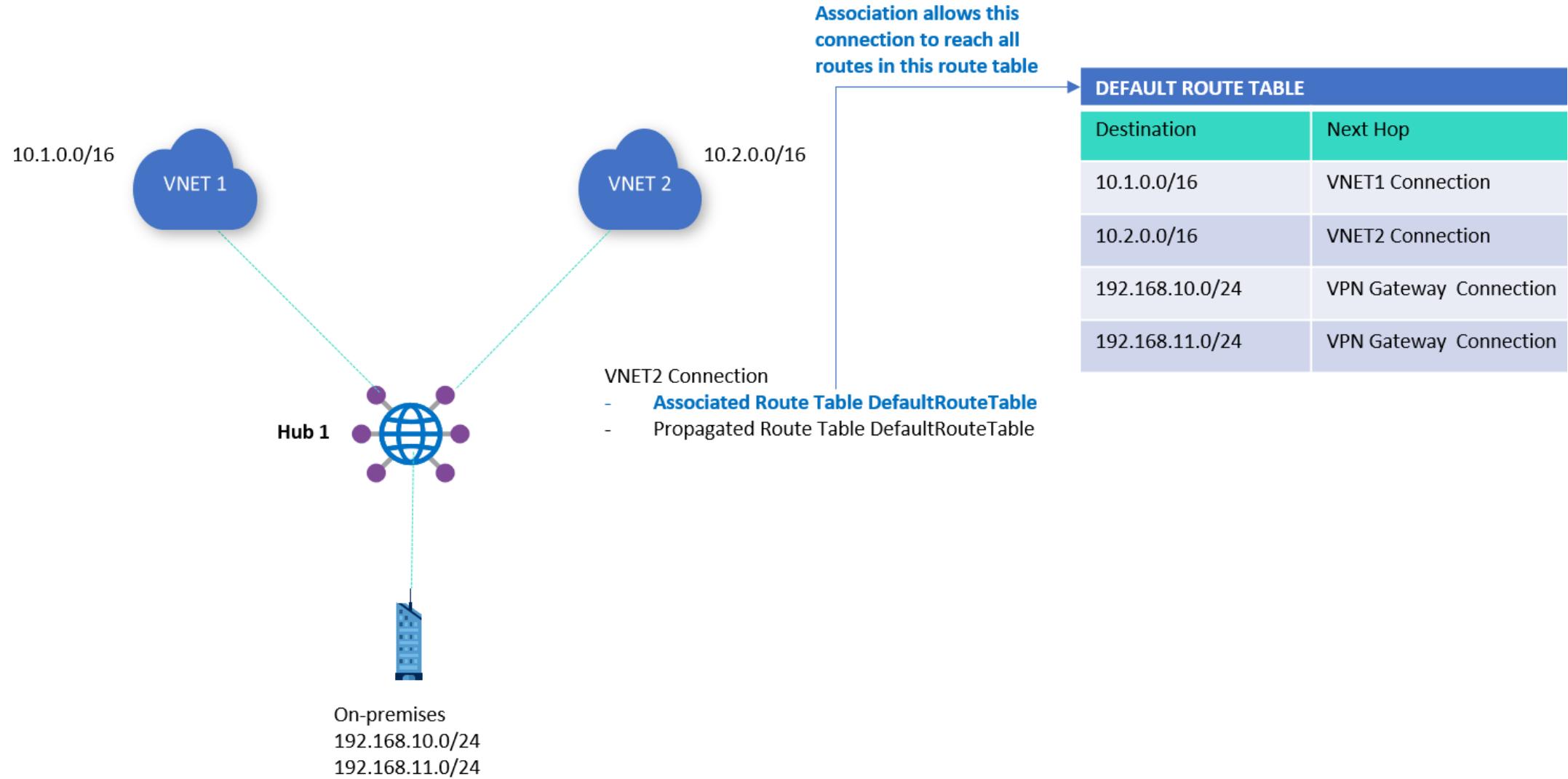
Propagate to labels ⓘ

0 selected

Static routes ⓘ

Route name	Destination prefix	Next hop

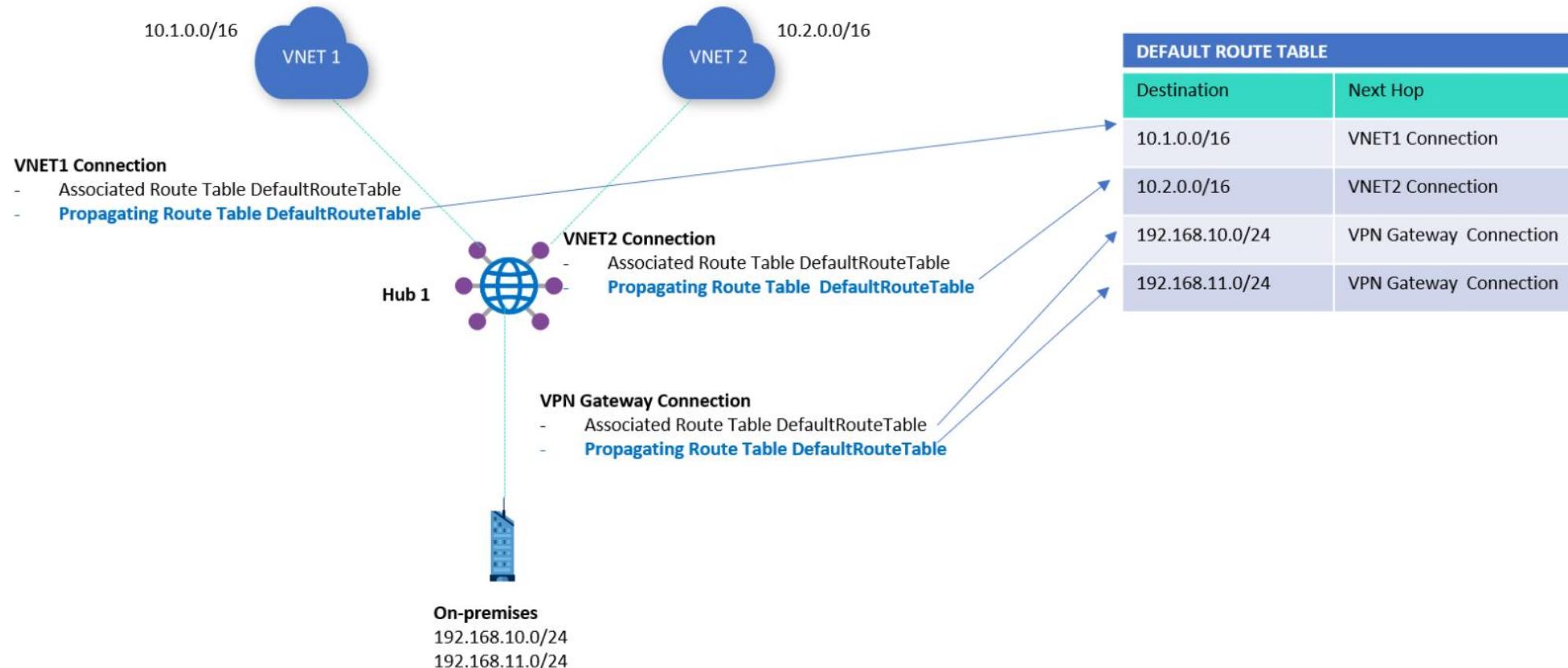
# Association



# Association

- Each connection is associated to one route table.
- The association allows the connection to reach all the routes in the route table (destination/next hop).
- Multiple connections can be associated to the same route table.
- All S2S and P2S VPNs as well as ExpressRoute connections are associated to the same (default) route table.
- By default, all connections are associated to a **default route table** in a virtual hub.
- Each virtual hub has its own default route table, to which you can add a static route(s). Static routes take precedence over dynamically learned routes for the same prefixes.

# Propagation



# Propagation

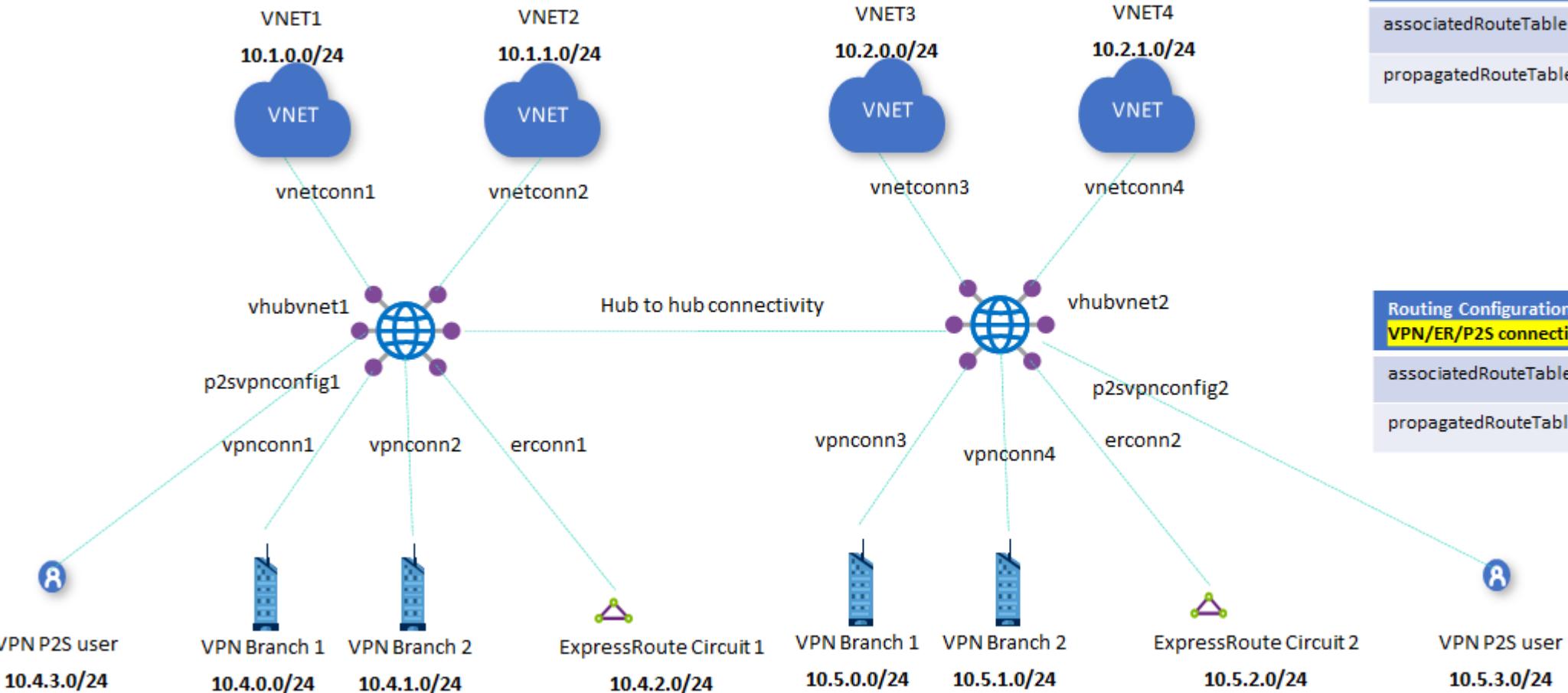
- Connections dynamically propagate routes to a route table.
- Routes can be propagated to one or multiple route tables.
- A **None route table** is also available for each virtual hub.  
Propagating to the None route table implies that no routes are required to be propagated from the connection.
- S2S and P2S VPNs as well as ExpressRoute connections propagate routes to the same set of route tables. This happens via the “Default” label, which means the Default Route Table in every Virtual WAN HUB.

# LABELS

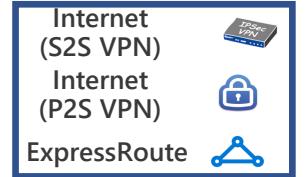
- Labels are a logical grouping of route tables
- Helps propagate routes from connections to multiple route tables.
  - The Default Route Table has a built in label called 'Default' . When users propagate connection routes to 'Default' label, it automatically applies to all the Default Route Tables across every hub in the Virtual WAN.
- Define your own labels

# Custom Routes – Example 1

- Any-2-Any
- This is the default situation

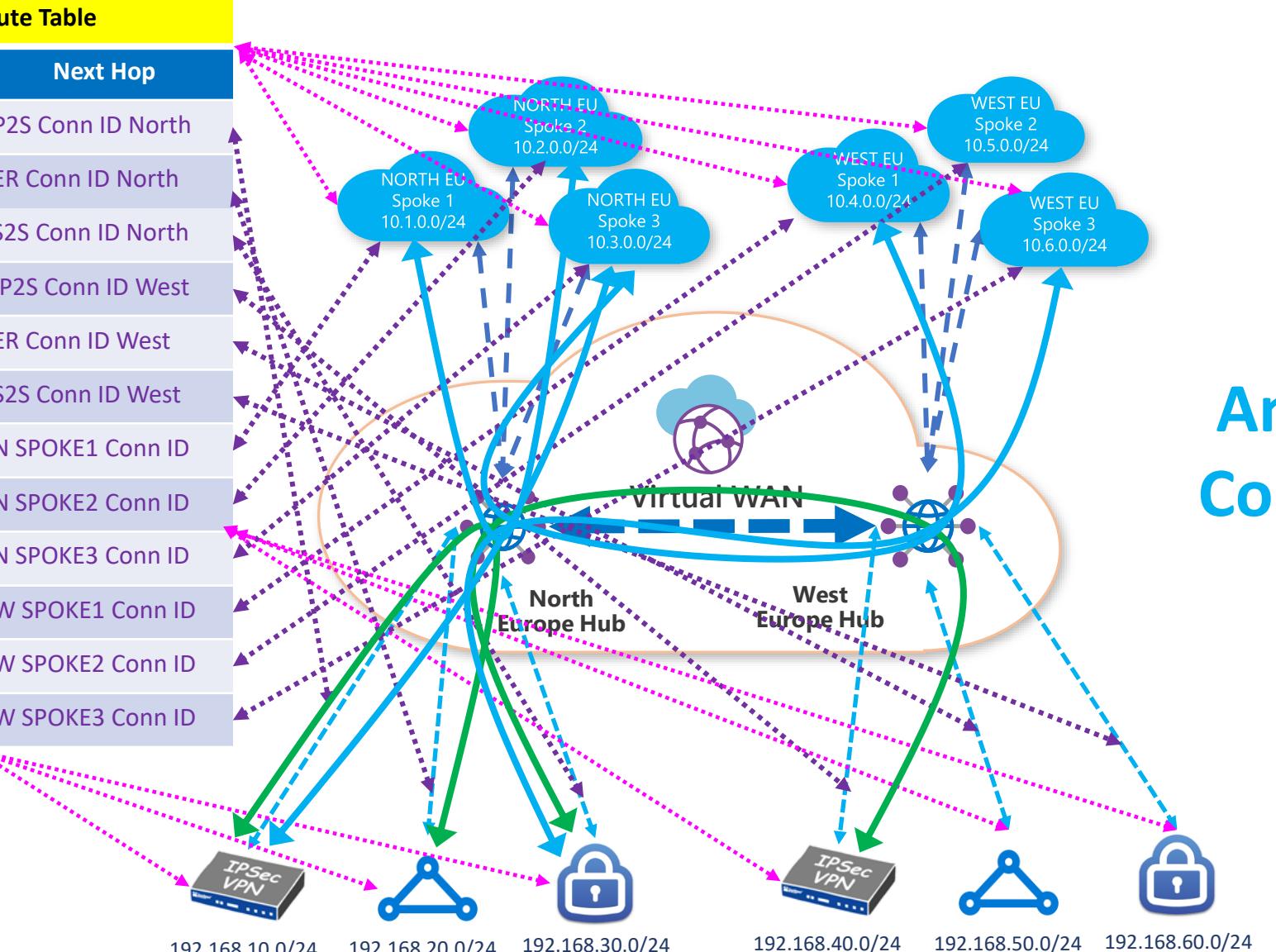


# Walk Trough Exercise:



Branches ↔ Branches  
 Branches ↔ VNET  
 VNET ↔ VNET

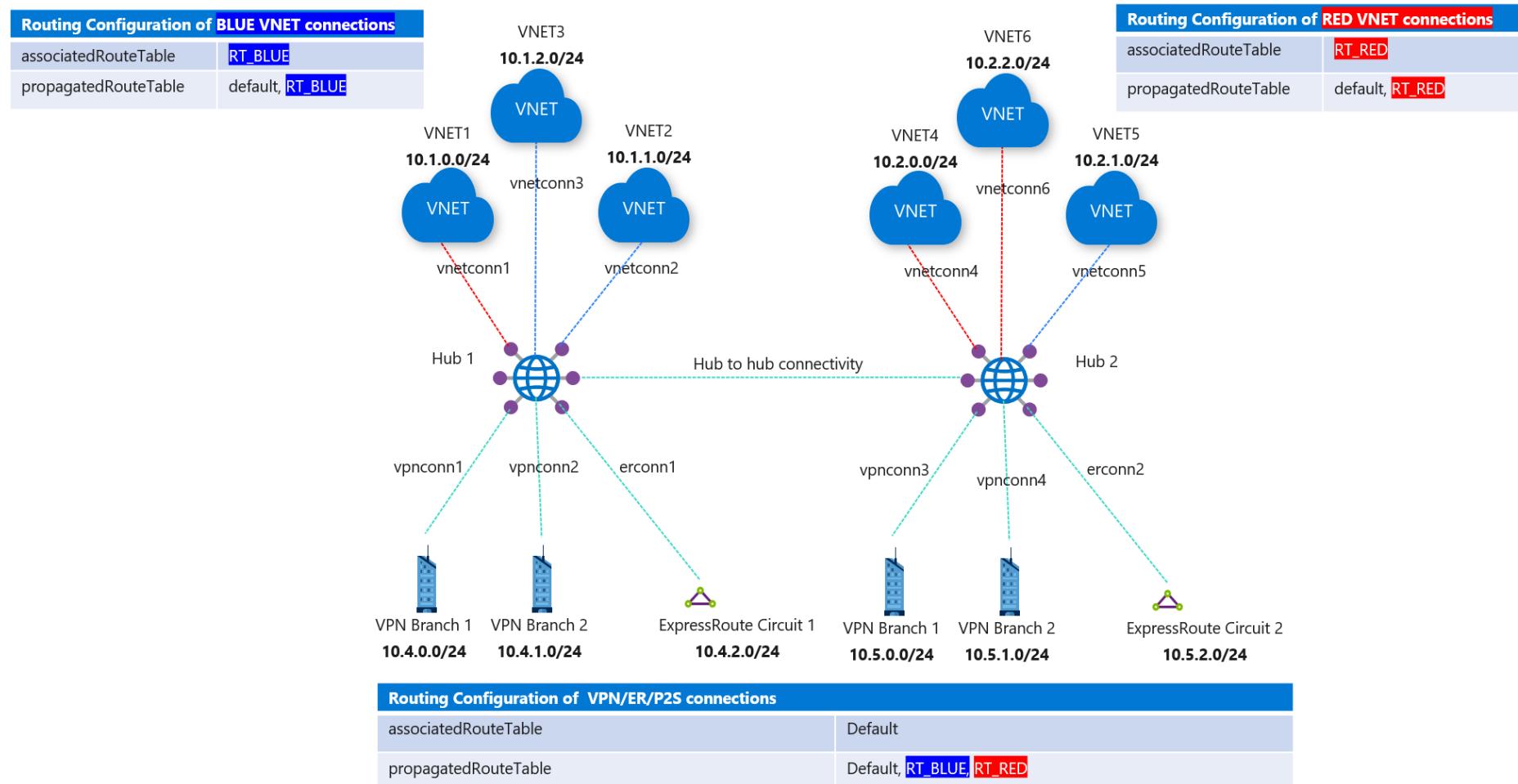
Default Route Table	
Route	Next Hop
192.168.10.0/24	P2S Conn ID North
192.168.20.0/24	ER Conn ID North
192.168.30.0/24	S2S Conn ID North
192.168.40.0/24	IP2S Conn ID West
192.168.50.0/24	ER Conn ID West
192.168.60.0/24	S2S Conn ID West
10.1.0.0/24	N SPOKE1 Conn ID
10.2.0.0/24	N SPOKE2 Conn ID
10.3.0.0/24	N SPOKE3 Conn ID
10.4.0.0/24	W SPOKE1 Conn ID
10.5.0.0/24	W SPOKE2 Conn ID
10.6.0.0/24	W SPOKE3 Conn ID



Any-to-Any  
Connectivity

# Custom Routes – Example 3

- Isolate Red VNETs from Blue VNETs but let red reach red & blue reach blue
- Allow all VNETs and Branches to reach each other

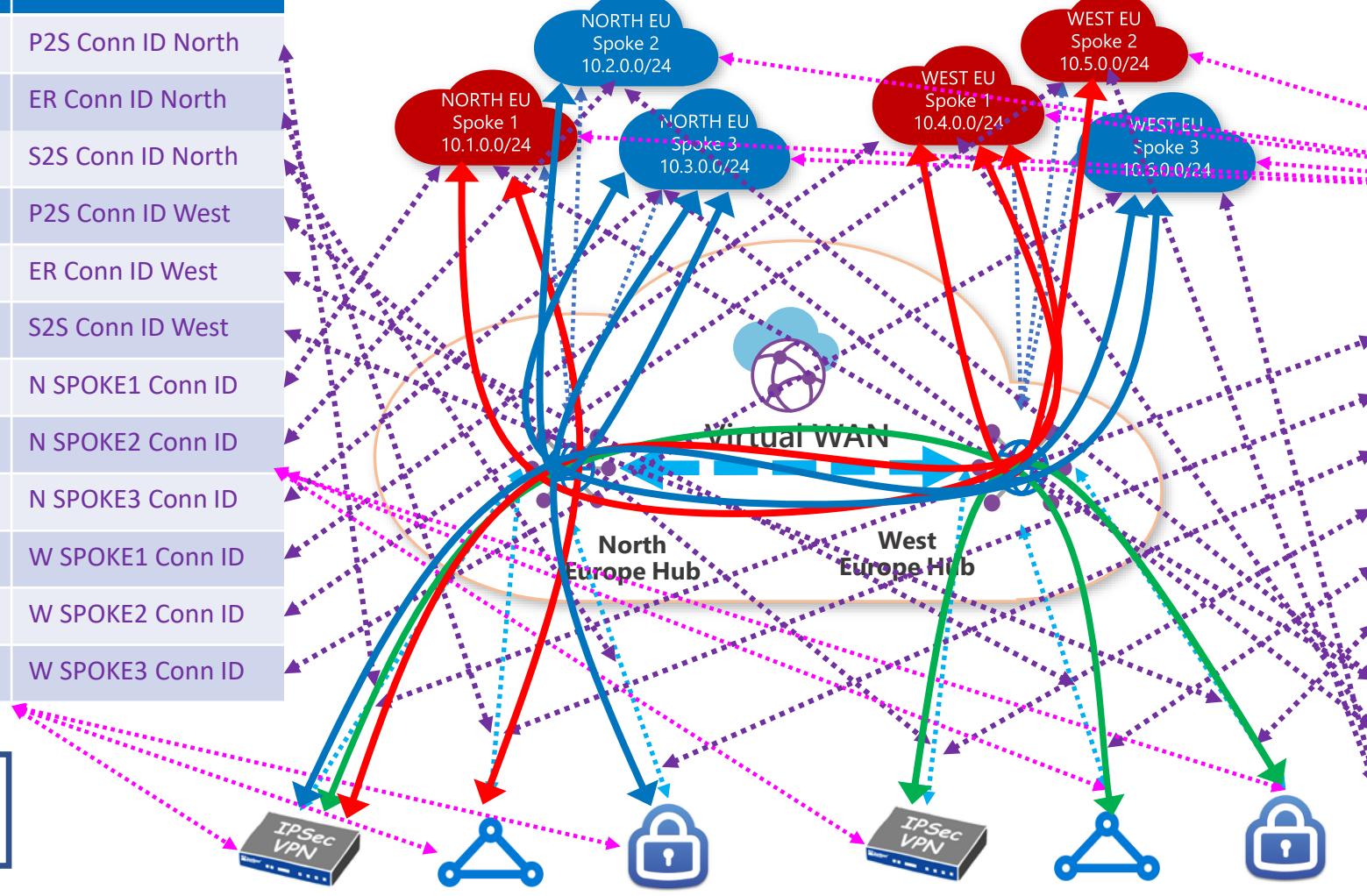


# Walk Trough Exercise:

Branches → Branches  
 Branches → VNET  
 Red VNET → Red VNET  
 Blue VNET → Blue VNET

Internet (S2S VPN)	
Internet (P2S VPN)	
ExpressRoute	

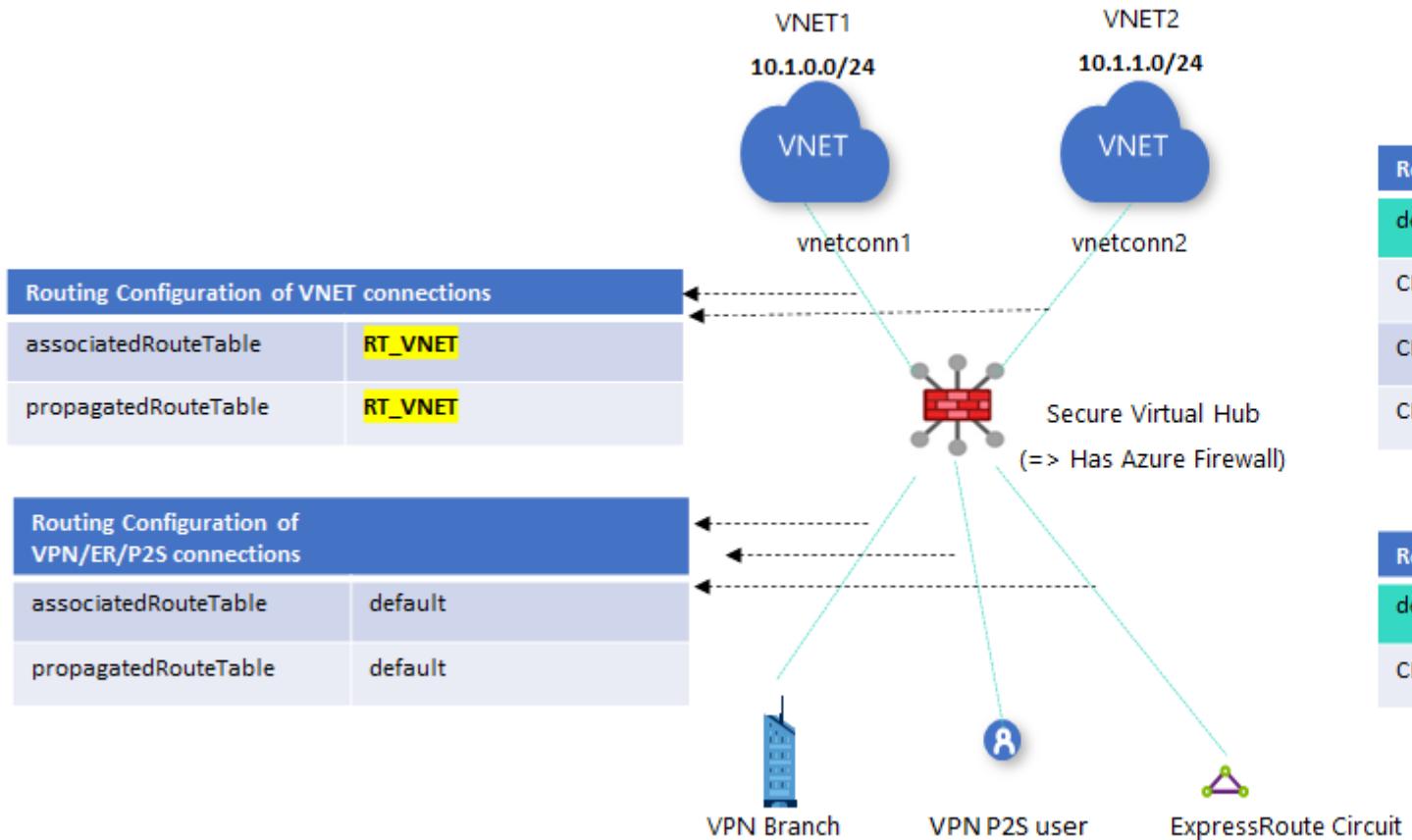
Default Route Table	
Route	Next Hop
192.168.10.0/24	P2S Conn ID North
192.168.20.0/24	ER Conn ID North
192.168.30.0/24	S2S Conn ID North
192.168.40.0/24	P2S Conn ID West
192.168.50.0/24	ER Conn ID West
192.168.60.0/24	S2S Conn ID West
10.1.0.0/24	N SPOKE1 Conn ID
10.2.0.0/24	N SPOKE2 Conn ID
10.3.0.0/24	N SPOKE3 Conn ID
10.4.0.0/24	W SPOKE1 Conn ID
10.5.0.0/24	W SPOKE2 Conn ID
10.6.0.0/24	W SPOKE3 Conn ID



Custom BLUE_RT_VNET	
Route	Next Hop
192.168.10.0/24	P2S Conn ID North
192.168.20.0/24	ER Conn ID North
192.168.30.0/24	S2S Conn ID North
192.168.40.0/24	S2S Conn ID West
192.168.50.0/24	ER Conn ID West
192.168.60.0/24	P2S Conn ID WEST
10.2.0.0/24	N SPOKE2 Conn ID
10.3.0.0/24	N SPOKE3 Conn ID
10.6.0.0/24	W SPOKE3 Conn ID

# Azure Firewall & Custom Routes

- VNET-2-VNET Direct / Branch-2-Branch Direct
- VNET-2-Branch/Internet via Azure Firewall



Route Table RT_VNET		
destType	destination	nextHop
CIDR	10.1.0.0/24	vnetconn1 resourceid
CIDR	10.1.1.0/24	vnetconn2 resourceid
CIDR	0.0.0.0/0	AZFW resourceid

Route Table Default Route Table		
destType	destination	nextHop
CIDR	10.1.0.0/16	AZFW resourceid

Propagated routes from VNET connections being more specific for VNETs activates V2V bypassing AZFW

Static route added activates V2I, V2B via AZFW

Static route with aggregated routes for VNets activates B2V via AZFW

# Secure Virtual Hub



Azure Peering Services

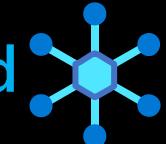
Virtual WAN

ExpressRoute

VPN Gateway

S2S VPN

Connect & Extend



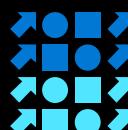
P2S VPN

MEC

# Azure Networking Services



Protect



Deliver

Internet Analyzer

Network Watcher Traffic Analytics

Azure Monitor Insights for Virtual WAN

Azure Virtual WAN Log & Metrics

Azure Firewall

Firewall Manager

Service endpoints/Private Link

WAF

Bastion

DDOS

IPv4/v6 in Azure VNETs

Virtual Network

Virtual Subnet

DNS

CDN

NAT Gateway

Load Balancer

Trafic Manager

Application Gateway

Front Door

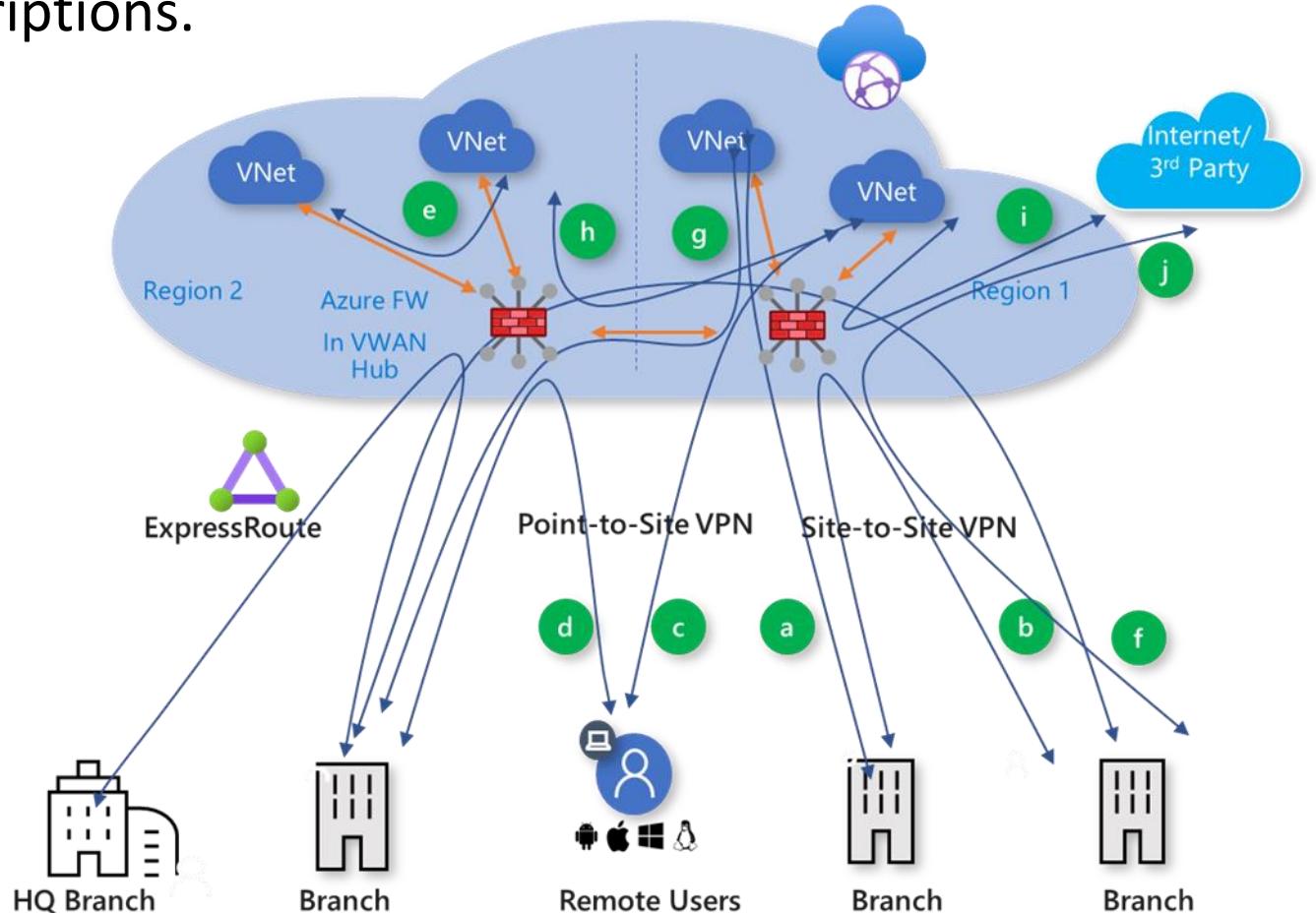
# Any-to-Any ... meet the CISO!

- A transitive global Azure virtual WAN leads to security concerns
- You have a firewall at the branch offices, data centers, 3<sup>rd</sup> party clouds and even at the clients with P2S connections
- You might want (need) a firewall and manage routing at the Azure Virtual WAN Hub

# Azure Firewall Manager

Central Azure Firewall deployment, configuration & management

- You can centrally deploy and configure multiple Azure Firewall instances that span different Azure regions and subscriptions.
- Policy driven



# What is a Secured Virtual Hub?

- A virtual hub is a Microsoft-managed virtual network that enables connectivity from other resources. When a virtual hub is created from a Virtual WAN in the Azure portal, a virtual hub VNet and gateways (optional) are created as its components.
- An Azure Virtual Hub becomes a *[secured virtual hub](#)* when security and routing policies are associated with it via an Azure Virtual Firewall Manager
- Use secured virtual hubs to easily create hub-and-spoke and transitive architectures **with native security services** for traffic governance and protection.

# Azure Firewall Manager

 **Firewall Manager**

Search (Ctrl+ /) <>

-  **Getting Started**
-  **Secured virtual hubs**
-  **Hub virtual networks**
- Security**
  -  **Azure Firewall Policies**
  -  **Security Partner Providers**

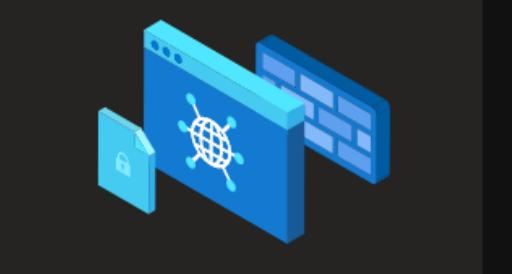
## Azure Firewall Manager

A central security policy and route management service for cloud-based security perimeters. [Learn more](#) 



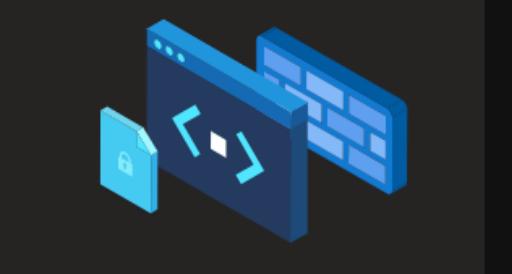
**Create Azure firewall policies**  
Define rules for traffic filtering across multiple Azure Firewall instances in Secured Virtual Hubs and Hub Virtual Networks.

[View Azure firewall policies](#)



**Add security to virtual hubs**  
Associate an Azure Firewall policy or a trusted security partner with new or existing virtual hubs to enforce consistent security and routing policies across multiple hubs.

[View secured virtual hubs](#)

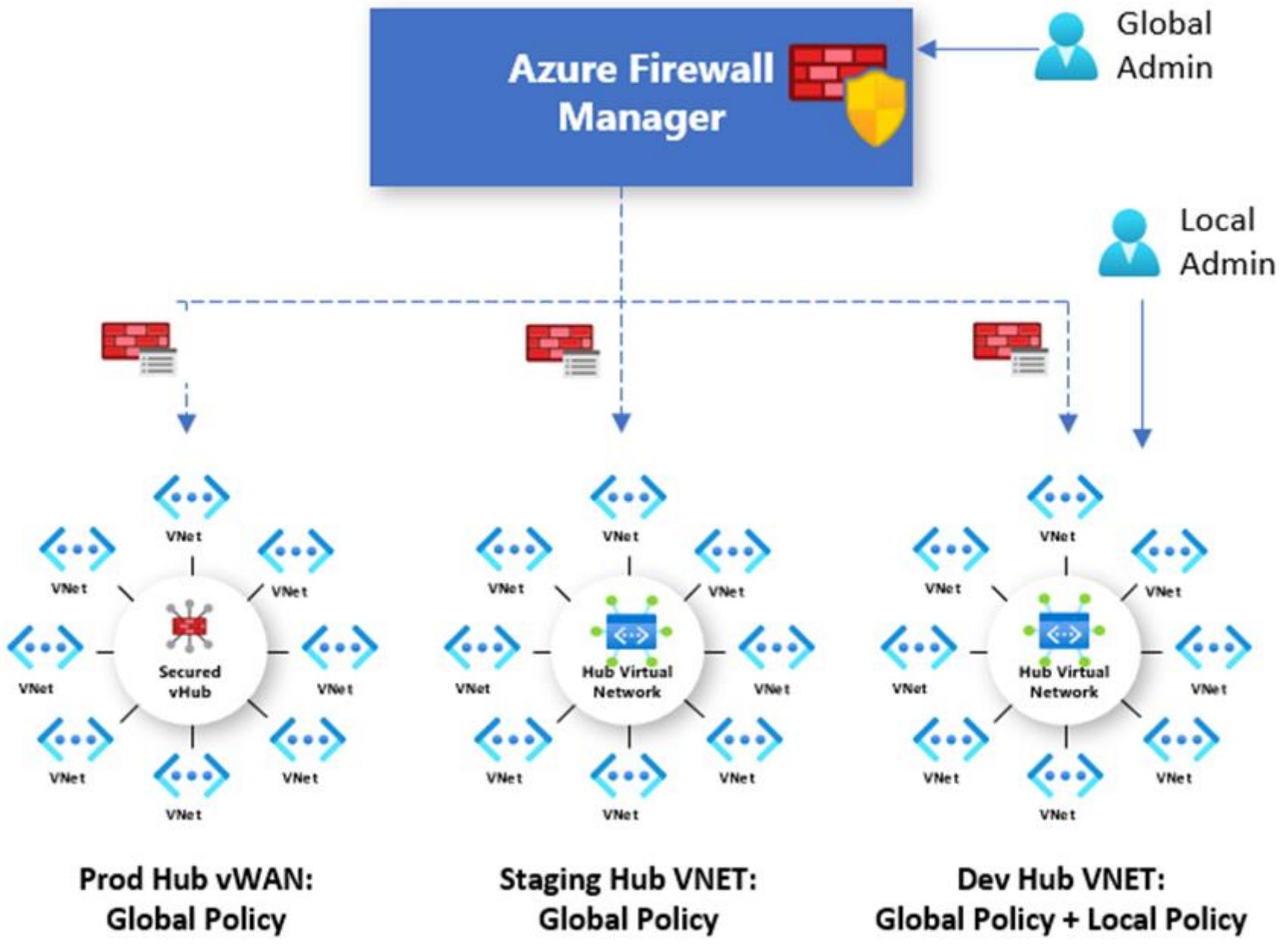


**Add security to virtual networks**  
Associate an Azure Firewall policy with new or existing virtual networks to enforce consistent firewall policies across multiple hub virtual networks.

[View hub virtual networks](#)

# Options for using a Secured Virtual Hub

- **As a managed central VNet with no on-prem connectivity**
  - Replaces the central VNet previously required for an Azure Firewall deployment.
  - Provides automated routing, without configuring your own UDRs (user defined routes) to route traffic through your firewall.
- **As part of a full Virtual WAN architecture**
  - This provides secured, optimized, and automated branch connectivity to and through Azure.
  - You can choose the services used protect and govern your network traffic, including Azure Firewall and other third-party security as a service (SEaaS) providers.



# Azure Hierarchical Firewall Policies

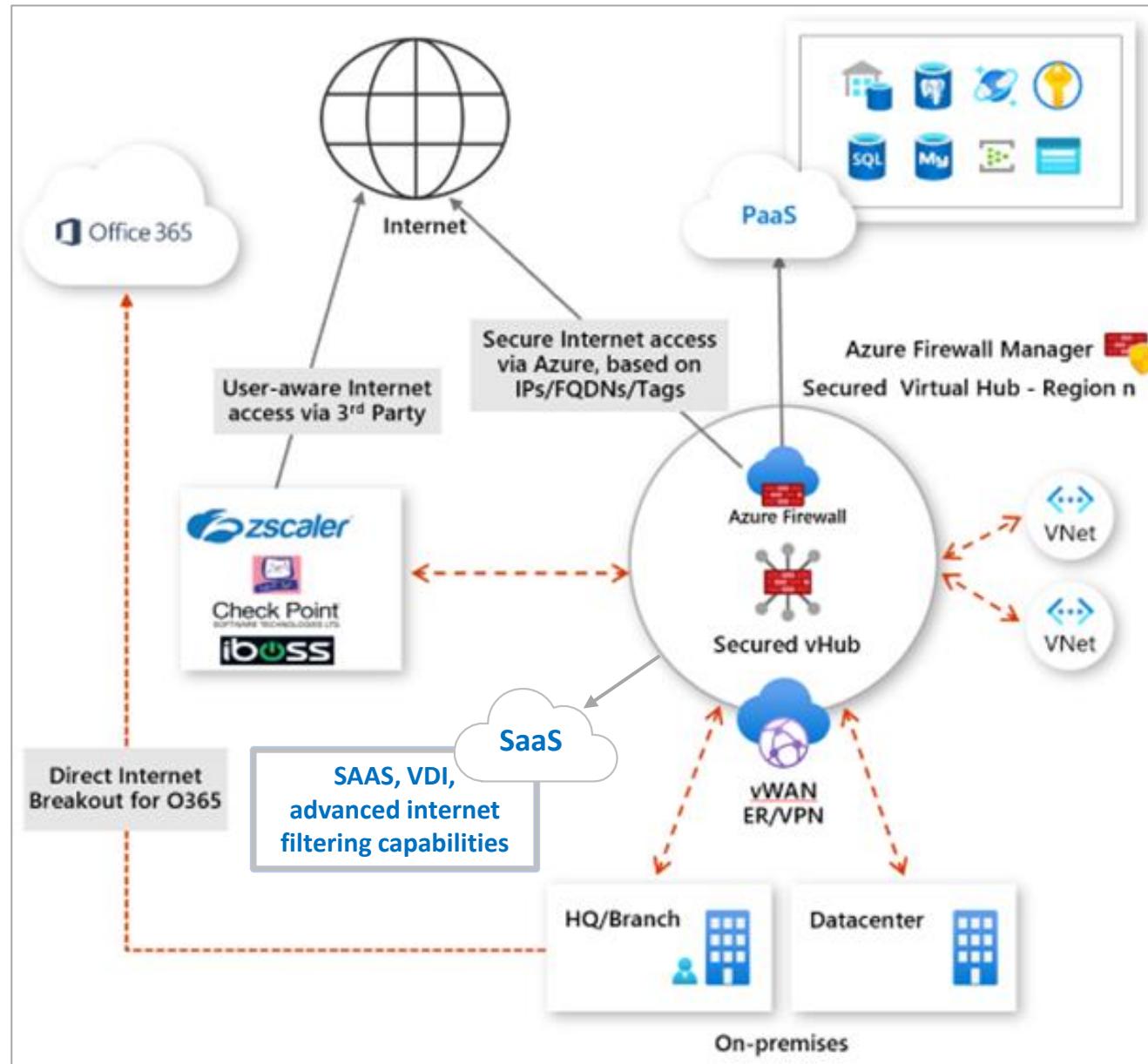
- ❑ Policies are hierarchical (global and local)
  - ❑ You can use Azure Firewall Manager to centrally manage Azure Firewall policies across multiple secured virtual hubs and hub virtual networks.
  - ❑ Your central IT teams can author global firewall policies to enforce organization wide firewall policy across teams.
  - ❑ Locally authored firewall policies allow a DevOps self-service model for better agility.

# Azure Firewall Policy Hierarchies

## ➤ **Creating new policies**

- A policy is created from scratch or inherited from existing policies
- With inheritance, any changes to the parent policy are automatically applied down to associated firewall child policies.
- A policy can also be imported from an existing Azure Firewall (\*NAT inheritance)

# Secured Virtual Hub Internet traffic filtering



# Integrate with 3<sup>rd</sup> party SECaaS

- Integrate 3<sup>rd</sup> party security-as-a-service (SECaaS) providers to deliver additional network protection for VNet and branch Internet connections.
- Only available for secured virtual hubs!

Examples:

- VNet to Internet (V2I) traffic filtering
  - Filter outbound virtual network traffic with your preferred third-party security provider.
  - Leverage advanced user-aware Internet protection for your cloud workloads running on Azure.
- Branch to Internet (B2I) traffic filtering
  - Leverage your Azure connectivity and global distribution to easily add third-party filtering for branch to Internet scenarios.

# Azure Virtual WAN Monitoring



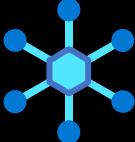
Azure Peering Services

Virtual WAN

ExpressRoute

VPN Gateway

S2S VPN

**Connect & Extend** 

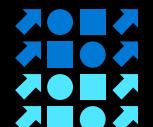
P2S VPN

MEC

# Azure Networking Services



**Protect**



**Deliver**

Internet Analyzer

Network Watcher Traffic Analytics

Azure Monitor Insights for Virtual WAN

Azure Virtual WAN Log & Metrics



**Monitor**

Azure Firewall

Firewall Manager

Service endpoints/Private Link

WAF

Bastion

DDOS

IPv4/v6 in Azure VNETs

Virtual Network

Virtual Subnet

DNS

CDN

NAT Gateway

Load Balancer

Trafic Manager

Application Gateway

Front Door

# Monitor – Insights (preview)

Dashboard >

**vwan** Virtual WAN

Search (Ctrl+ /) Delete Refresh

Resource group : rg Status : Succeeded

Location : West US Branch-to-branch : Enabled

Subscription : Virtual hubs : 3

Subscription ID : Tags (change) : Click here to add tags

Overview Activity log Access control (IAM) Tags

Settings Configuration Properties Locks Export template

Connectivity Hubs VPN sites User VPN configurations ExpressRoute circuits Virtual network connections

Monitor Connection monitor Insights (preview)

Support + troubleshooting Getting started New support request

Each point represents a hub.

Hub	Hub status	Address Space	Region	VPN sites	Azure Firewall	Point-to-site	ExpressRoute circuits	Virtual network connectio...
westus2-hub	Succeeded	10.35.0.0/16	West US 2	1 VPN site(s)	Not deployed	No P2S gateway	1 ExpressRoute circuit(s)	All connected ***
eastus-hub	Failed	10.55.0.0/24	East US	2 VPN site(s)	Deployed	sukishenp2s	1 ExpressRoute circuit(s)	All connected ***
WestEU-hub	Succeeded	10.75.0.0/24	West Europe	No VPN gateway	Not deployed	No P2S gateway	No ExpressRoute gateway	Not applicable ***

# Monitor – Insights (preview)

Dashboard >

vwan | Insights (preview)

Virtual WAN

Search (Ctrl+ /) Search here for dependent resources Add filter

New support request View detailed metrics

The network graph displays the following components and connections:

- Hubs:** vwan, eastus-hub, westeu-hub, westus2-hub.
- Sites:** multi-link-site, cisco-asa-site, branchroutetable, spokevnet-eastus, sukishen-vnet-east, cust12-vnet1-er, hub-spokewesteu, nestedthirdpartyres..., hub-to-spokewestu..., spokevnet-westus2, spokevnet-weurope, connection-nfsite-01, connection-versa-s..., exconnection-east..., exconnection-west..., connection-versa-s..., spoke-vnet-wsteu, spokevnet-westus2.
- Connections:** vwan connects to eastus-hub, westeu-hub, and westus2-hub. eastus-hub connects to multi-link-site, cisco-asa-site, branchroutetable, spokevnet-eastus, and sukishen-vnet-east. westeu-hub connects to westus2-hub. westus2-hub connects to hub-spokewesteu, nestedthirdpartyres..., hub-to-spokewestu..., spokevnet-westus2, and spokevnet-weurope. hub-spokewesteu connects to spokevnet-westus2. nestedthirdpartyres... connects to hub-to-spokewestu....

Red boxes highlight the network graph and the "Insights (preview)" menu item in the left sidebar.

Metrics Network Insights VirtualWANs Minified

Virtual WAN: Time Range: Last 24 hours

Virtual WAN Hub Capacities

Virtual Hub	VPN Gateway Scale Unit
westeu-hub	-
westus2-hub	1
eastus-hub	1

S2S Gateway Average Bandwidth

P2S Gateway Average Bandwidth

Support + troubleshooting

Getting started

New support request

# Metrics

 Metrics  
Azure Monitoring

+ New chart ⏪ Refresh ⏪ Share ⏪ Feedback ⏪

Chart Title 🖊

Add metric Add filter Apply splitting

Scope	Metric Namespace	Metric	Aggregation
f33bd50d418e41948ec4c5...	VPN Gateways standar...	Select metric	Select aggregation

100  
90  
80  
70  
60

Gateway S2S Bandwidth

- Tunnel Bandwidth
- Tunnel Egress Bytes
- Tunnel Egress Packets
- Tunnel Egress TS Mismatch Packet Drop
- Tunnel Ingress Bytes
- Tunnel Ingress Packets
- Tunnel Ingress TS Mismatch Packet Drop

+ / -

# Diagnostic logs

Search (Ctrl+ /) Refresh Provide feedback

Subscription \* Resource group Resource type Resource

Select any of the resources to view diagnostic settings.

Name	Resource type	Resource group	Diagnostics status
288b109f9ea7483596c731a7d8...	microsoft.network/expressrout...		Disabled

Type to start filtering ...

288b109f9ea7483596c731a7d8dff4d-southeastasia...  
60b4ab5259664801a5460e383198417d-westus-er-gw  
a36f677578764bacaa2db8495378150d-eastus-er-gw

**Diagnostics settings**

Save Discard Delete Provide feedback

A diagnostic setting specifies a list of categories of platform logs and/or metrics that you want to collect from a resource, and one or more destinations that you would stream them to. Normal usage charges for the destination will occur. [Learn more about the different log categories and contents of those logs](#)

Diagnostic settings name

Diagnostic settings name \*

Category details

log

- GatewayDiagnosticLog
- TunnelDiagnosticLog
- RouteDiagnosticLog
- IKEDiagnosticLog

metric

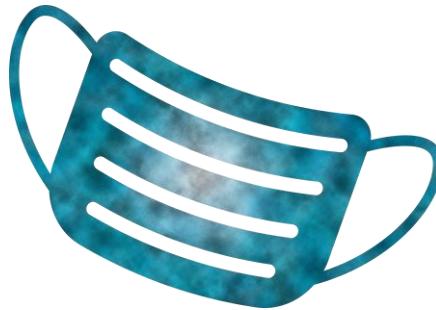
- AllMetrics

Destination details

- Send to Log Analytics
- Archive to a storage account
- Stream to an event hub

# Thank you for attending

Work from home!  
Stay safe!





# MC2MC

Azure Virtual WAN for everyone

# Didier Van Hoye - @WorkingHardInIT

Technical Architect & Technology Strategist



 <http://blog.workinghardinit.work>

 @workinghardinit

 blog@workinghardinit.work