Please note – the views/opinions in this presentation are entirely my own. This presentation will not be kept updated after the Welsh Azure User Group (November 2024) – so may be outdated if downloaded afterwards.

If in any doubt, please check latest documentation and MS Links for updated info!

creditsafe Servent <packt>

Welsh Azure User Group

@welshazure

Building a Cloud Centric Network with Azure Virtual WAN

Jake Walsh

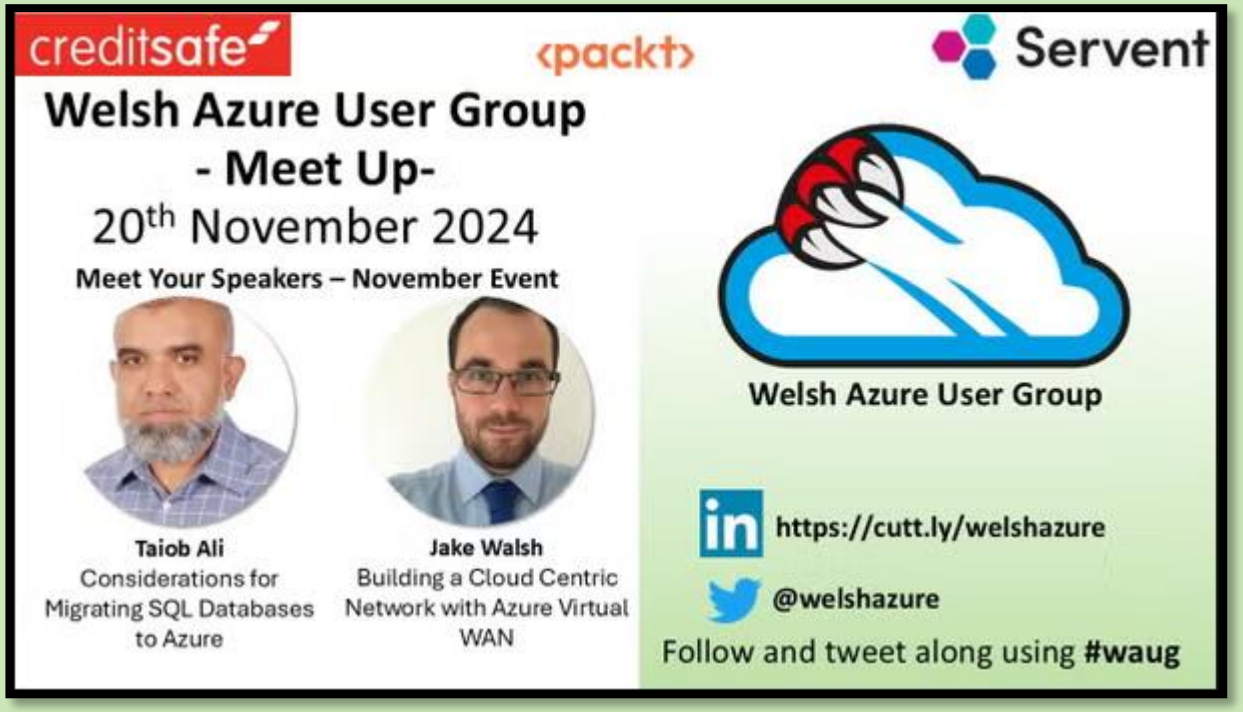
Hello!

Jake Walsh

Senior Solution Architect @ CDW UK

@jakewalsh90
jakewalsh.co.uk

Please note – the views/opinions in this presentation are entirely my own. If in any doubt, please check latest documentation etc!



Microsoft MVP Most Valuable Professional

HashiCorp Ambassador 2024

CTA Citrix Technology Advocate

@welshazure

Agenda

- What is Azure Virtual WAN?
- Use Cases
- Core Components
- Why Azure Virtual WAN? Core Benefits
- Security
- Expansion
- Where do we begin?
- Resources

What is Azure Virtual WAN?

- Azure Virtual WAN is a **Networking Service** that brings various elements together in a single operational interface.

- Key Features Include:
  - Software-defined connectivity
  - Centralised network management
  - Optimised security and agility thanks to the Microsoft Global Network

What is Azure Virtual WAN?

Azure Virtual WAN is a **Networking Service** that brings various aspects together in a single Azure Service:

Hub / Spoke – replaced with Virtual WAN Hub and VNET Peering to Spokes	Routing and Route Tables – Automated	VPNs/ExpressRoute – Centralised Management	Firewalling – Azure native options and 3rd Party NVAs

@welshazure

Virtual WAN is always improving....

Learn / Azure / Networking / Virtual WAN /

What's new in Azure Virtual WAN?

Article • 06/19/2024 • 7 contributors

Feedback

In this article

Recent releases
Preview
Known issues
Next steps

Azure Virtual WAN is updated regularly. Stay up to date with the latest announcements. This article provides you with information about:

- Recent releases
- Previews underway with known limitations (if applicable)
- Known issues
- Deprecated functionality (if applicable)

You can also find the latest Azure Virtual WAN updates and subscribe to the RSS feed here.

- https://learn.microsoft.com/en-us/azure/virtual-wan/whats-new

@welshazure

Virtual WAN is always improving....

Preview

The following features are currently in gated public preview. After working with the listed articles, you have questions or require support, reach out to the contact alias (if available) that corresponds to the feature.

Expand table

Type of preview	Feature	Description	Contact alias	Limitations
Managed preview	Route-maps	This feature allows you to perform route aggregation, route filtering, and modify BGP attributes for your routes in Virtual WAN.	preview-route-maps@microsoft.com	Known limitations are displayed here: About Route-maps.
Managed preview	Aruba EdgeConnect SD-WAN	Deployment of Aruba EdgeConnect SD-WAN NVA into the Virtual WAN hub	preview-vwan-aruba@microsoft.com	

- https://learn.microsoft.com/en-us/azure/virtual-wan/whats-new

Where is Virtual WAN available?

Geopolitical region	Azure regions
Australia Government	Australia Central, Australia Central 2
Europe	France Central, France South, Germany North, Germany West Central, North Europe, Norway East, Switzerland North, Switzerland West, West Europe, UK West, UK South
North America	East US, West US, East US 2, West US 2, Central US, South Central US, North Central US, West Central US, Canada Central, Canada East
Asia	East Asia, Southeast Asia
India	India West, India Central, India South
Japan	Japan West, Japan East
Oceania	Australia Southeast, Australia East
South Africa	South Africa North, South Africa West
South America	Brazil South
South Korea	Korea Central, Korea South
UAE	UAE North, UAE Central

Geopolitical region	Azure regions
US Government cloud	US Gov Arizona, US Gov Iowa, US Gov Texas, US Gov Virginia, US DoD Central, US DoD East
China East	China East2
China North	China North2

- Wide range of locations
- US Government and Azure China also available
- Availability Zones – key consideration

https://learn.microsoft.com/en-us/azure/virtual-wan/virtual-wan-locations-partners

Use Cases

@welshazure

- The key aspect – **Bringing together** core networking features:

  - Branch connectivity – route your branch to branch traffic via Microsoft's Network.
  - Site-to-site VPN connectivity.
  - Remote user VPN connectivity (point-to-site).
  - Private connectivity (ExpressRoute).
  - Intra-cloud connectivity (transitive connectivity for virtual networks).
  - VPN ExpressRoute inter-connectivity.
  - Routing Configuration – Route Tables, Custom Routing etc.
  - Azure Firewall & Firewall Manager integration
  - Transit & Internal Connectivity – Hub/Hub/Spoke/Spoke

Virtual WAN is like a buffet…

Virtual WAN provides many services – you can choose which you want to use.

Some organisations will use many, others will use only a few.

Some will go back for a second helping!

Two SKUs

Virtual WAN type	Hub type	Available configurations
Basic	Basic	Site-to-site VPN only
Standard	Standard	ExpressRoute User VPN (P2S) VPN (site-to-site) Inter-hub and VNet-to-VNet transiting through the virtual hub Azure Firewall NVA in a virtual WAN

Note

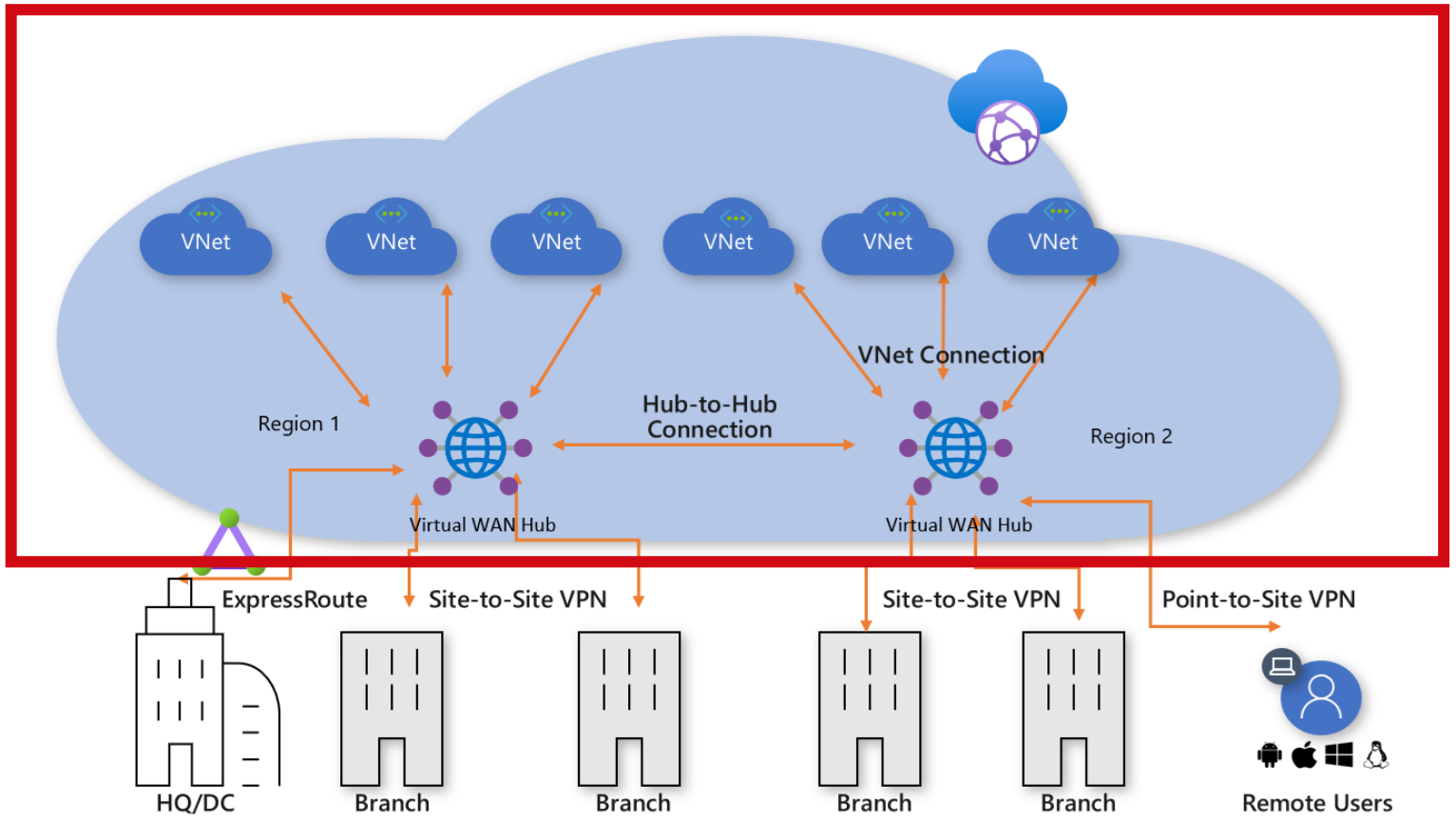
You can upgrade from Basic to Standard, but can't revert from Standard back to Basic.

https://learn.microsoft.com/en-us/azure/virtual-wan/virtual-wan-about

Core Components

- 5 Key Virtual WAN components you will likely use in all deployments that span **more than 1 Azure Region**:
  - Virtual WAN
  - Hub
  - **Hub to Hub Connection**
  - Hub Virtual Network Connection
  - Hub Route Table

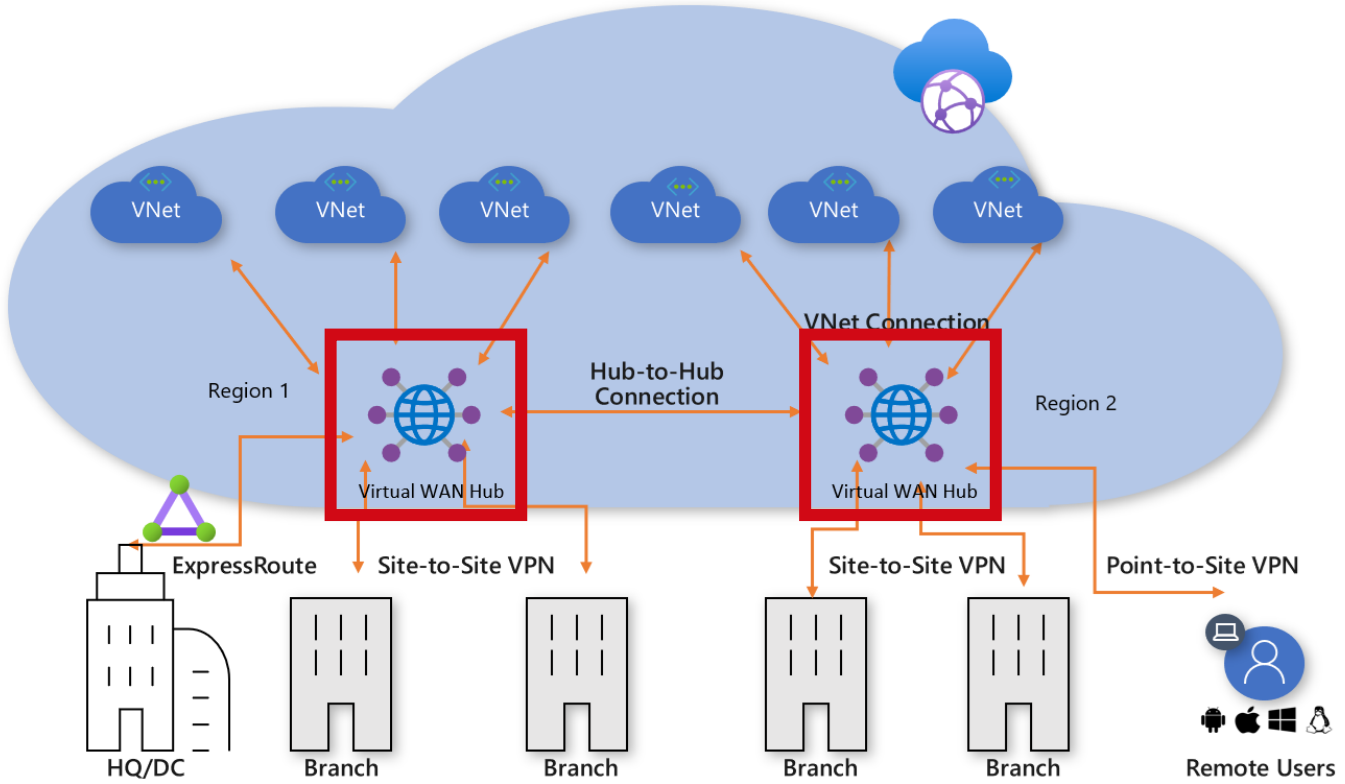
Virtual WAN



- Virtual overlay of your Azure Networking
- A collection of multiple Resources
- Contains all Virtual WAN components within your topology

Hub

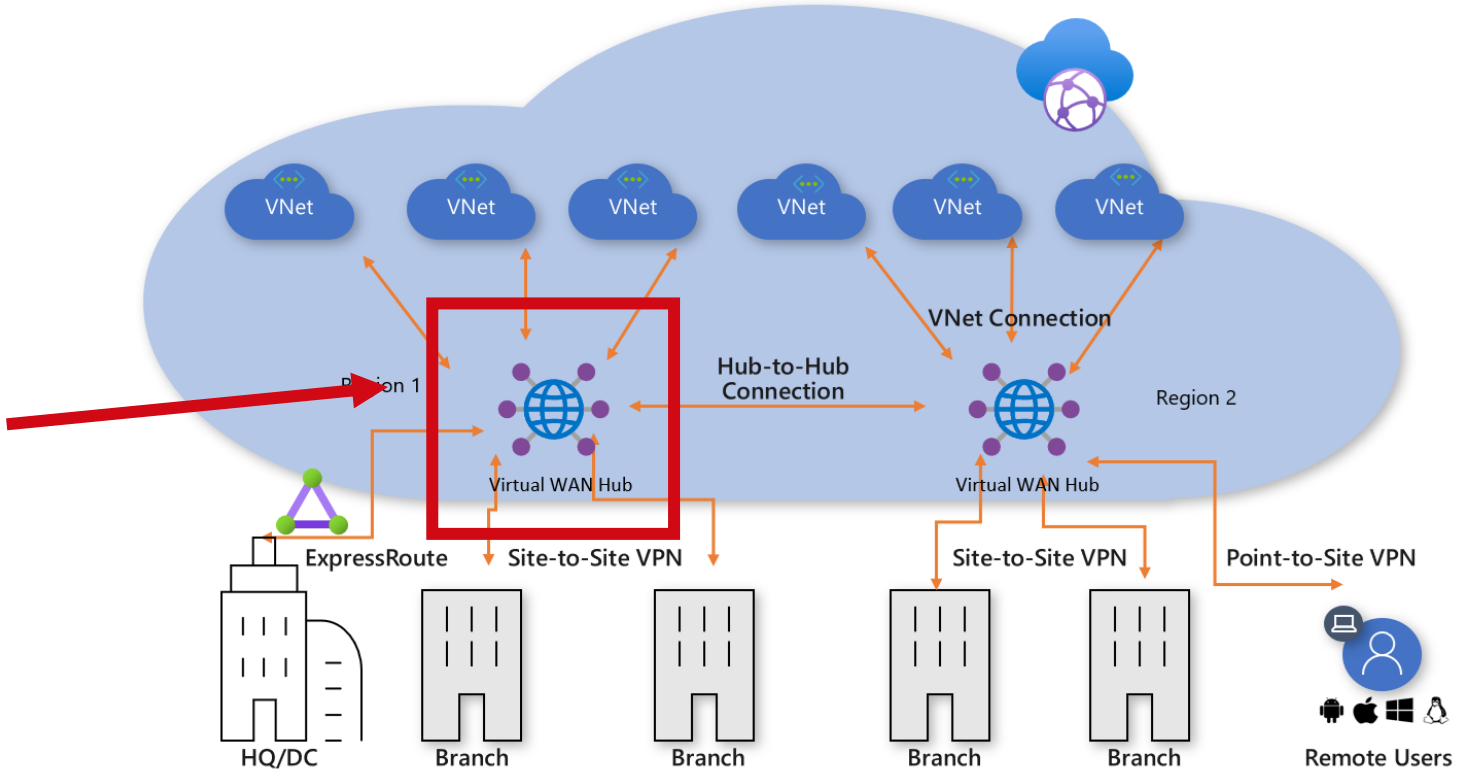
- The Virtual Hub is a Microsoft Managed Virtual Network, containing various service endpoints.
- The Hub is the Core of the Virtual WAN network in an Azure Region. Typically 1 Hub per Region but can be more.
- Gateways for VPN/ExpressRoute deployed within Hubs.
- Firewalls / NVAs deployed into Hubs.
- Note – consider routing units!



What's in the Hub?

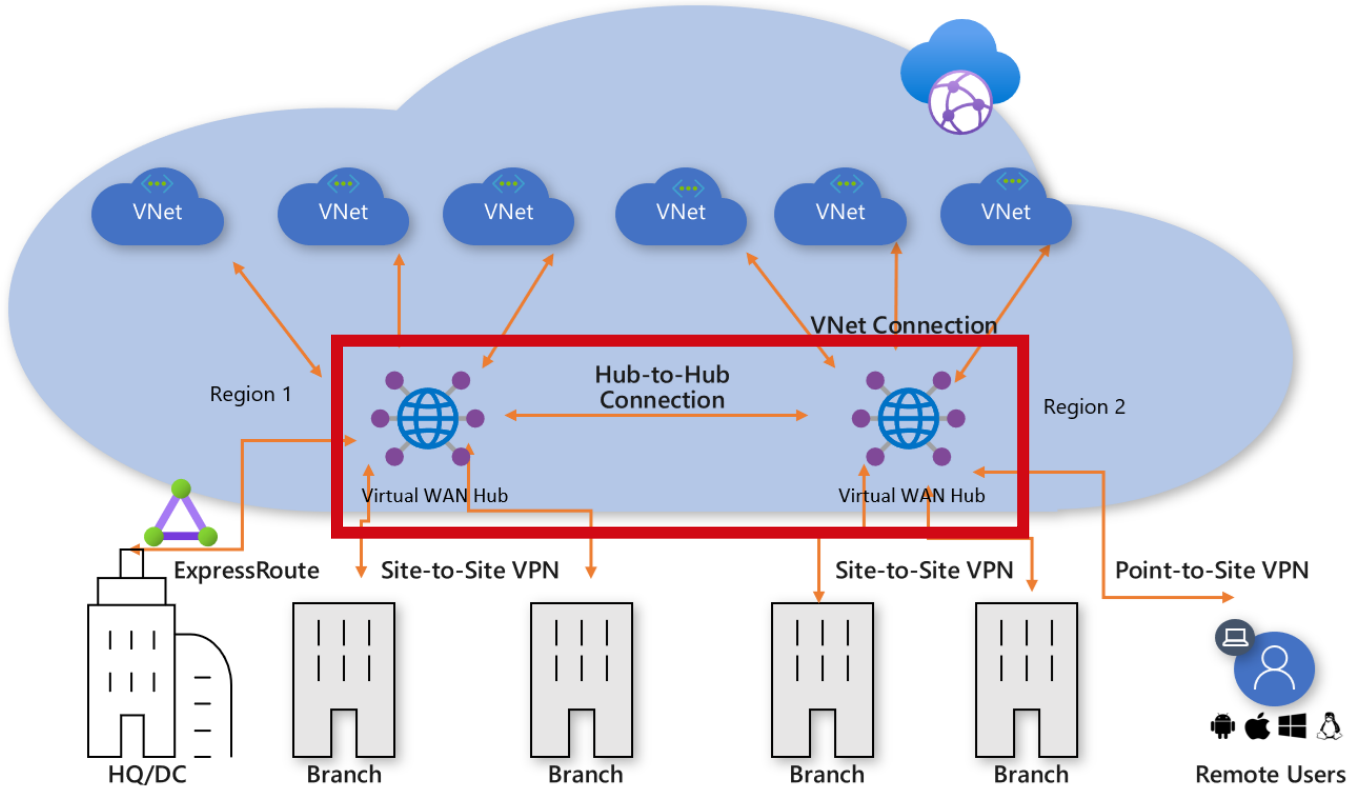
Items we can deploy into a Hub:

- Virtual Network Gateway
- ExpressRoute Gateway
- P2S Gateway
- Azure Firewall or NVA
- Route Tables
- Hub to Hub Connection



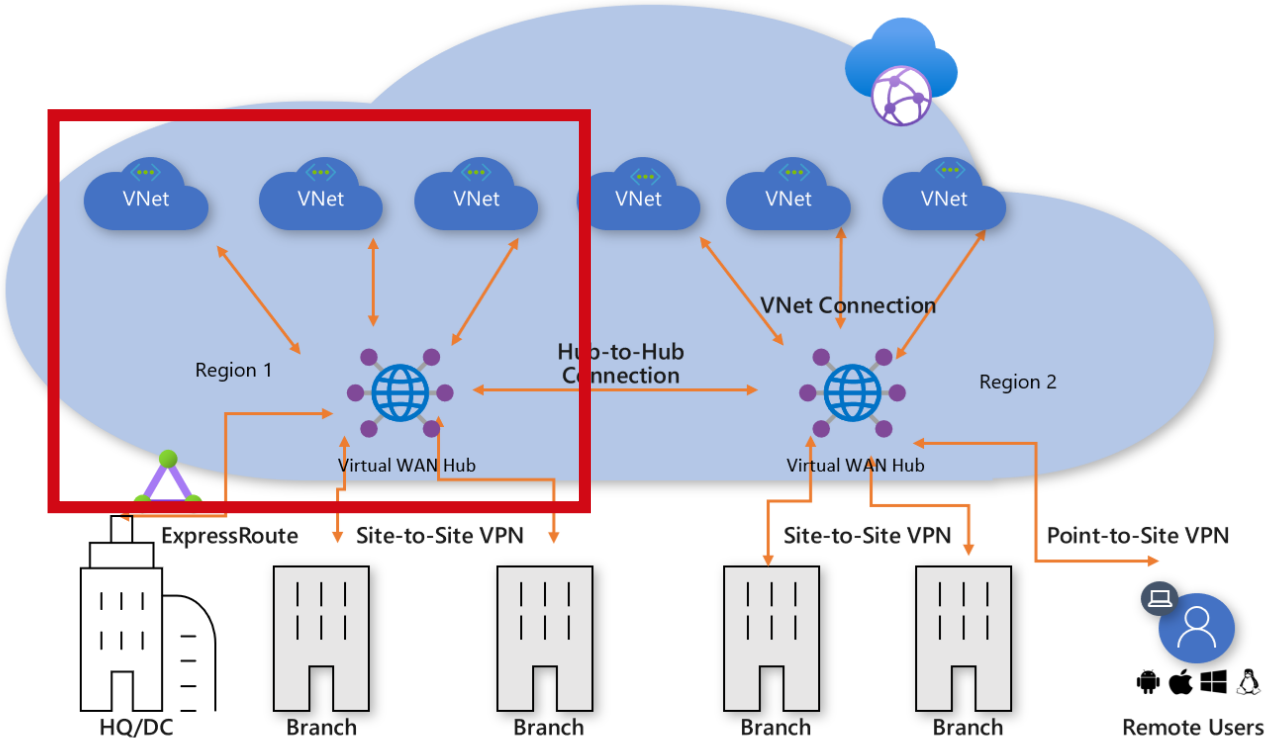
Hub to Hub Connection

- Virtual WAN Hubs are connected within a Virtual WAN.
- Hubs can communicate freely and routing is propagated.
- Inter-Region connectivity is established using Virtual WAN Hubs.
- Connectivity can be controlled using a Firewall or NVA. **Note: there ~~are~~ were limitations around inter-region communication.**



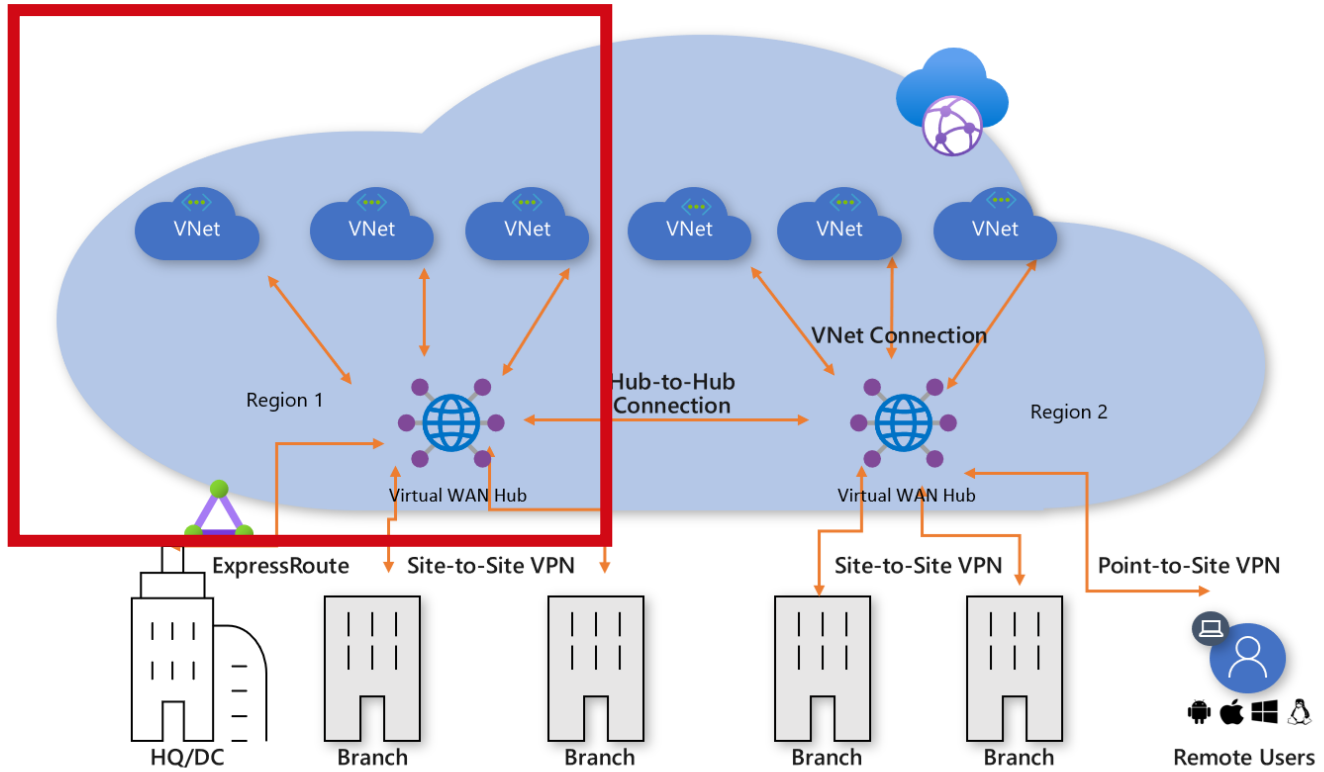
Hub Virtual Network Connection

- A Hub Virtual Network connection joins a spoke network to a Virtual WAN Hub.
- A Virtual Network can be connected to a single Virtual WAN hub.
- Traffic is enabled between the Virtual WAN Hub and Spoke Virtual Network.
- Azure Firewall or an NVA is used in many cases to control this traffic.



Hub Route Table

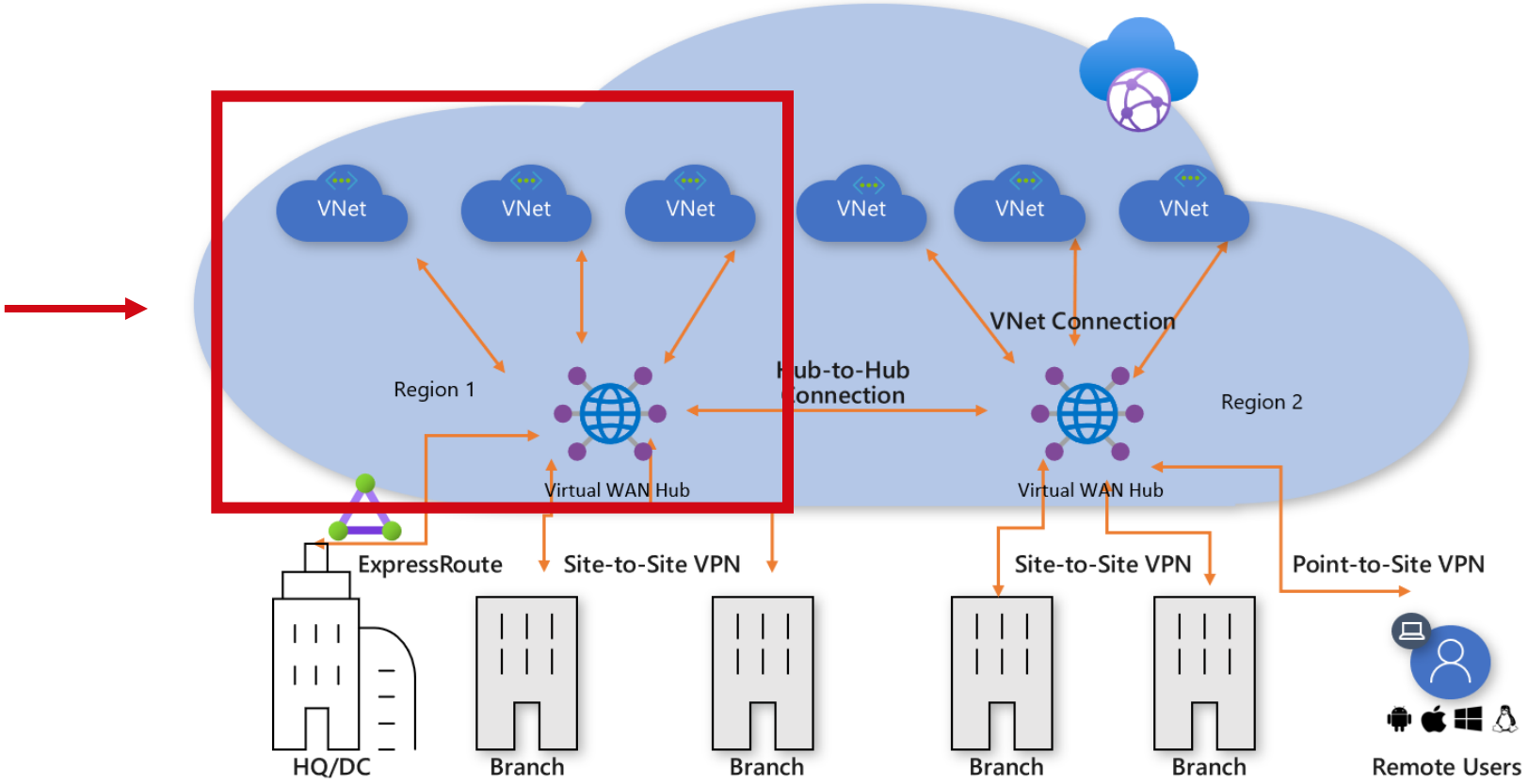
- Each Hub has its own default route table. This can be edited to add static routes if required.
- Static routes take precedence over dynamic routes.
- Associated with a Hub and it's connected Virtual Networks.
- Connections, e.g. VPN, ExpressRoute or PS2 will also have a routing configuration that propagates to a route table.
- Labels can be used to logically group route tables.



https://learn.microsoft.com/en-us/azure/virtual-wan/about-virtual-hub-routing#considerations

What about Hub and Spoke?

- Virtual WAN replaces an existing Hub Spoke architecture with Spoke VNETs peered into a Virtual WAN Hub.
- Hubs become fully managed by Virtual WAN.
- Central management of all Hubs in the topology.
- All Spokes peer into a Virtual WAN Hub, with connectivity and inter-region traffic routed via the Hub.

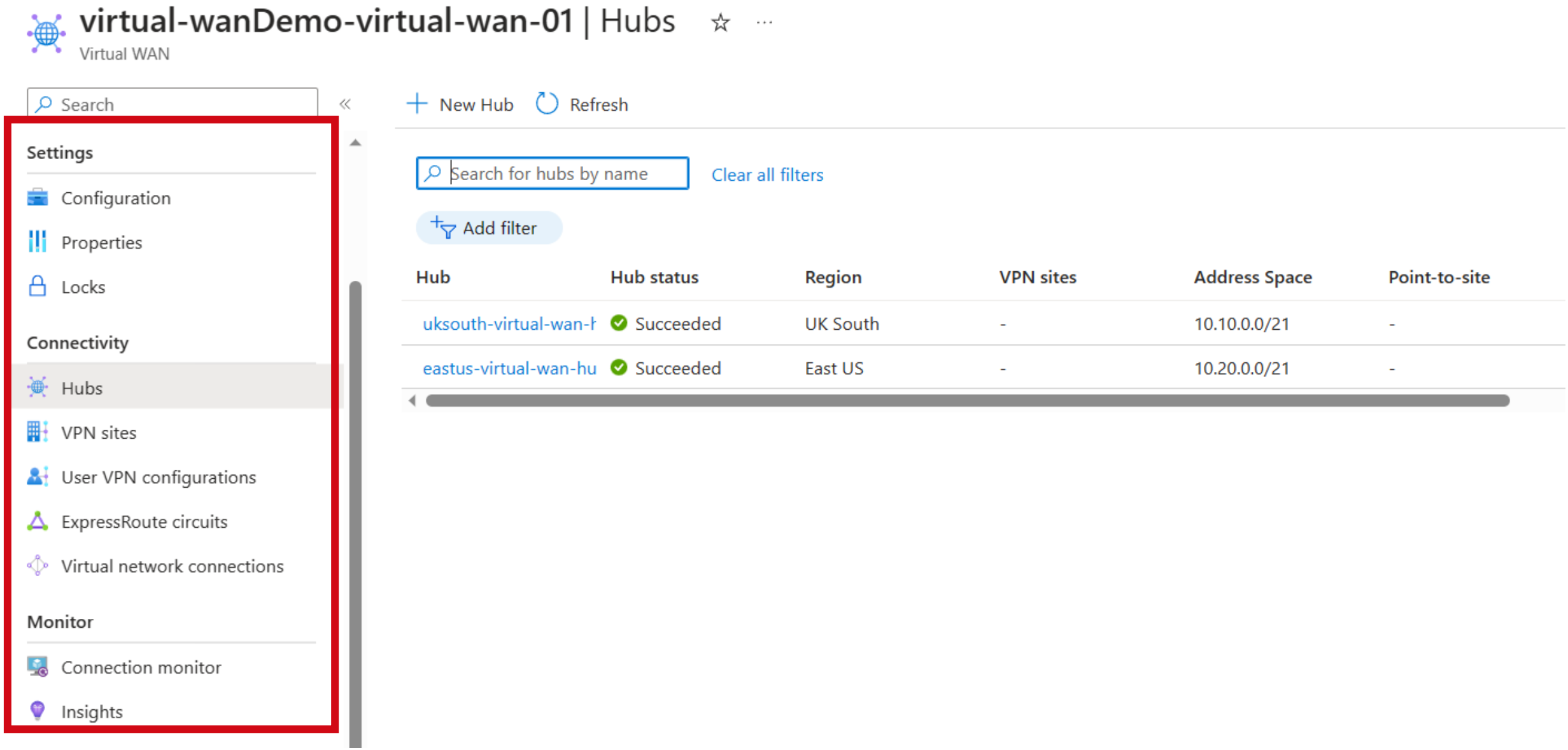


@welshazure

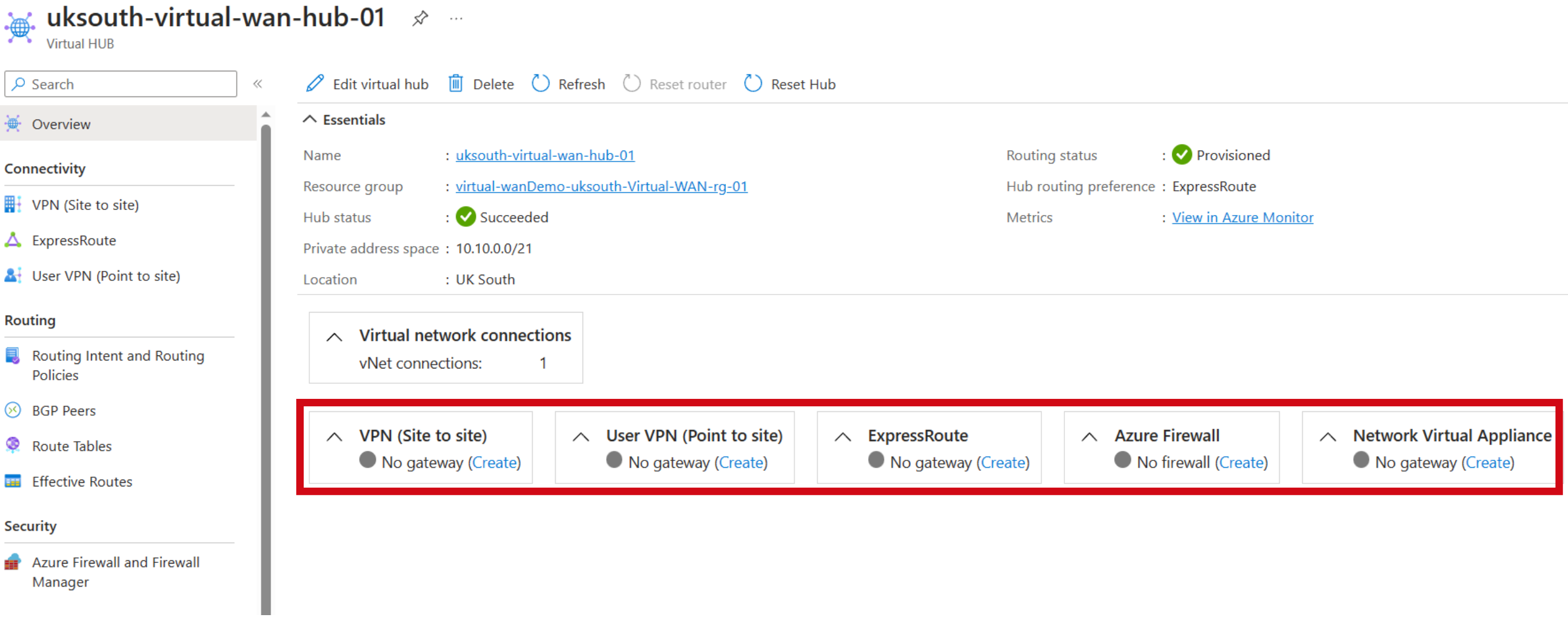
Why Virtual WAN? Core Benefits:

- **An Integrated Solution –** All core networking aspects in a single control Resource. Site to Site and Connectivity options are easily accessed and managed. **Simple administration!**
- **An Automated Solution –** Connect Virtual Networks to the Hubs easily, and also bring additional services into Virtual WAN with ease – again, centralised, simplified and automated is the key.
- **Troubleshooting –** End to End visibility, allowing rapid diagnosis of issues and simple troubleshooting.
- **Centralised Control –** A centralised service that brings core networking together, removing the need to configure and manage multiple separate resources.
- **Firewalling –** Integrations to Azure Firewall, Azure Firewall Manager, and NVA options.
- **Rapid Expansion –** Simple expansion to other Regions, with automated routing and simplified connectivity via the Global Transit Architecture.

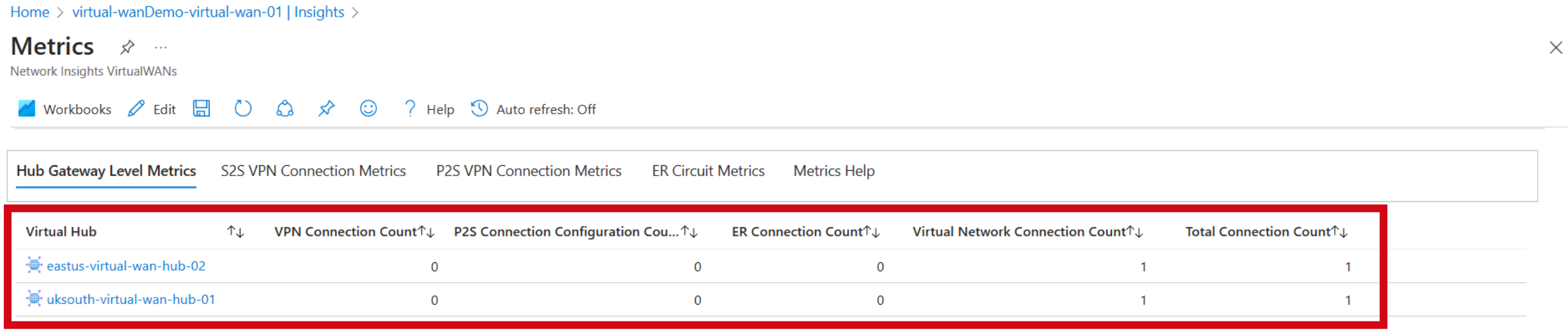
An Integrated Solution – All core networking aspects in a single control Resource. Site to Site and Connectivity options are easily accessed and managed. **Simple administration!**



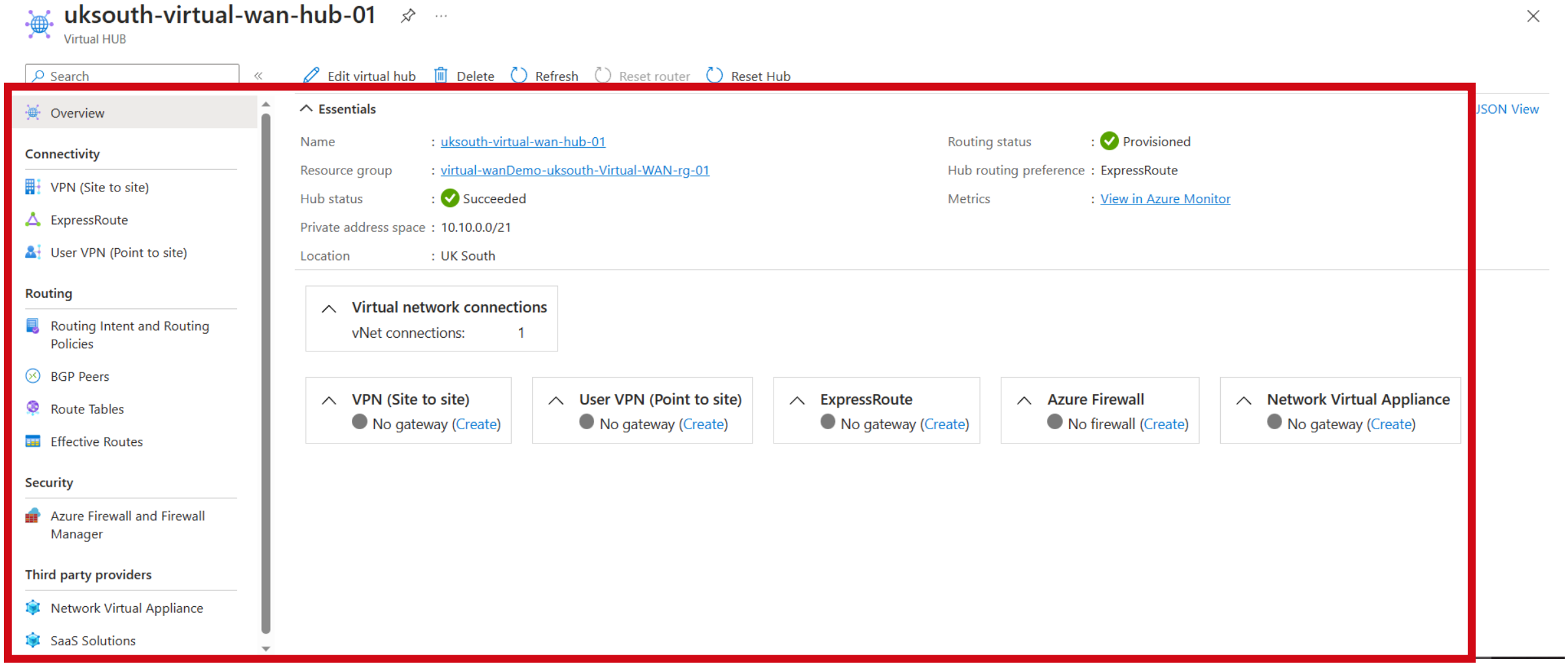
An Automated Solution – Connect Virtual Networks to the Hubs easily, and also bring additional services into Virtual WAN with ease – again, centralised, simplified and automated is the key.



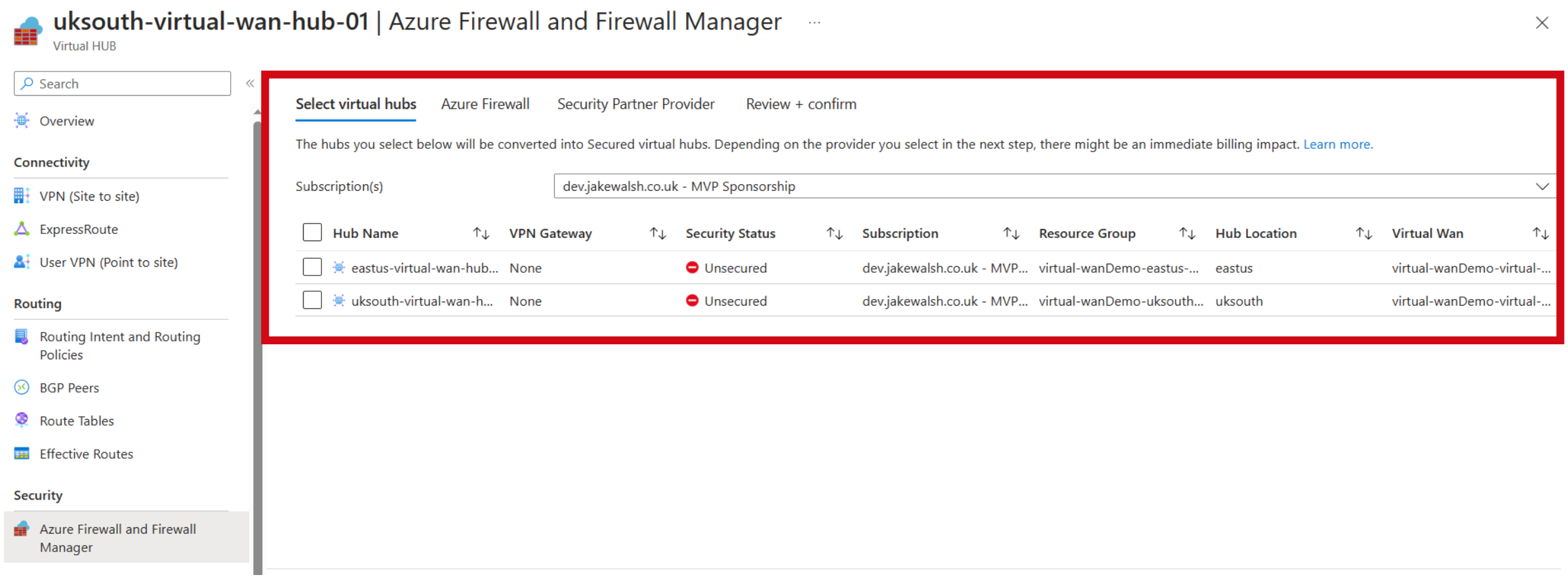
Troubleshooting – End to End visibility, allowing rapid diagnosis of issues and simple troubleshooting.



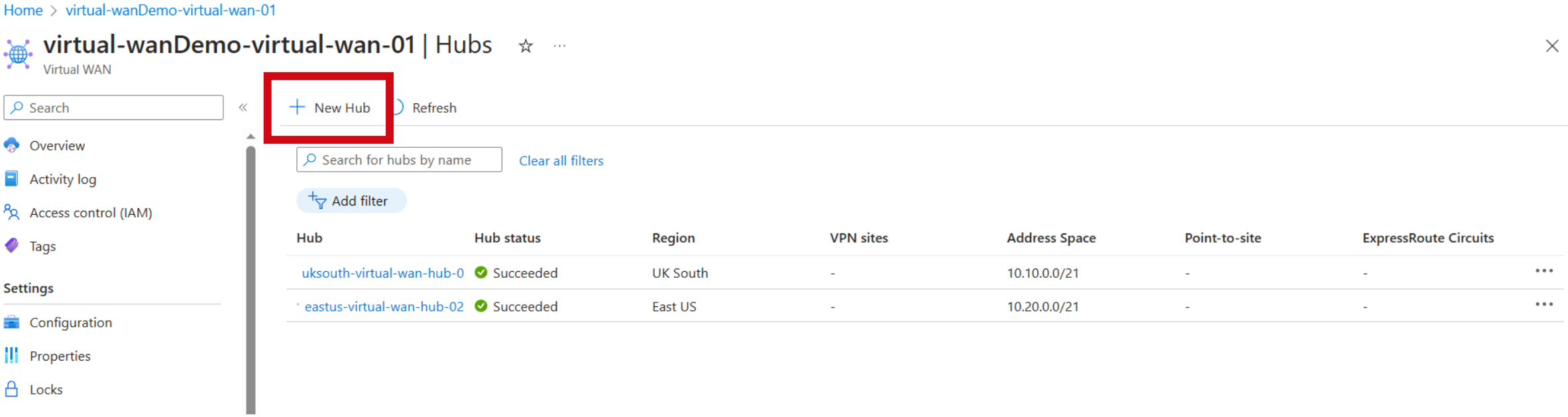
Centralised Control – A centralised service that brings core networking together, removing the need to configure and manage multiple separate resources.



Firewalling – Integrations to Azure Firewall, Azure Firewall Manager, and NVA options.



Rapid Expansion – Simple expansion to other Regions, with automated routing and simplified connectivity.



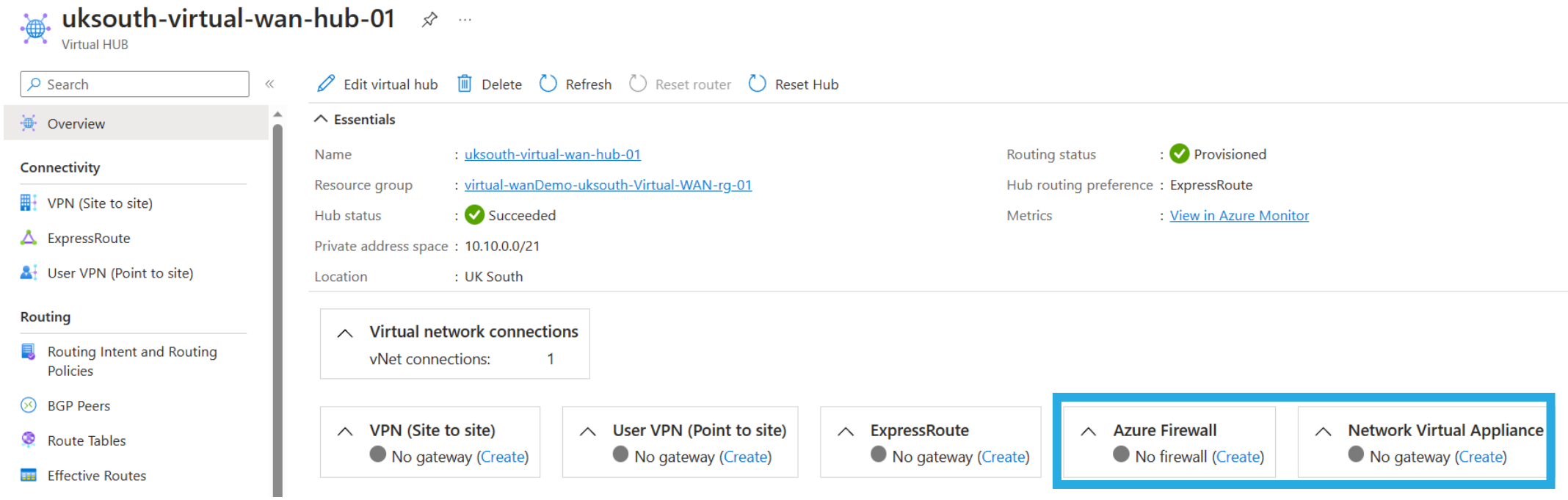
@welshazure

Security!

- There are numerous security aspects within Azure Virtual WAN – 5 key areas:
  - Azure Firewall or NVA Options
  - Monitoring
  - Packet Capture
  - Administration
  - Azure Security Baseline for Virtual WAN

Azure Firewall and NVA Options

- Virtual WAN supports Azure Firewall and NVA options via supported vendors
- NVAs = Deployment Process
- Azure Firewall – convert Standard to Secured Hub



Azure Firewall and NVA Options

Key benefits

When an NVA is deployed into a Virtual WAN hub, it can serve as a third-party gateway with various functionalities. It could serve as an SD-WAN gateway, Firewall, or a combination of both.

Deploying NVAs into a Virtual WAN hub provides the following benefits:

- **Pre-defined and pre-tested selection of infrastructure choices (NVA Infrastructure Units)**: Microsoft and the partner work together to validate throughput and bandwidth limits prior to solution being made available to customers.
- **Built-in availability and resiliency**: Virtual WAN NVA deployments are Availability Zone (AZ) aware and are automatically configured to be highly available.
- **No-hassle provisioning and boot-strapping**: A managed application is prequalified for provisioning and boot-strapping for the Virtual WAN platform. This managed application is available through the Azure Marketplace link.
- **Simplified routing**: Leverage Virtual WAN's intelligent routing systems. NVA solutions peer with the Virtual WAN hub router and participate in the Virtual WAN routing decision process similarly to Microsoft Gateways.
- **Integrated support**: Partners have a special support agreement with Microsoft Azure Virtual WAN to quickly diagnose and resolve any customer problems.
- **Optional platform-provided lifecycle management**: Upgrades and patches are managed either directly by you or as part of the Azure Virtual WAN service. For best practices related to software lifecycle management for NVAs in Virtual WAN, please reach out to your NVA provider or reference provider documentation.
- **Integrated with platform features**: Transit connectivity with Microsoft gateways and Virtual Networks, Encrypted ExpressRoute (SD-WAN overlay running over an ExpressRoute circuit) and Virtual hub route tables interact seamlessly.

https://learn.microsoft.com/en-us/azure/virtual-wan/about-nva-hub

Azure Firewall and NVA Options

Partners	Virtual WAN NVA Vendor Identifier	Configuration/How-to/Deployment guide	Dedicated support model
Barracuda Networks	barracudasdwanrelease	Barracuda SecureEdge for Virtual WAN Deployment Guide	Yes
Cisco SD-WAN	ciscosdwan	The integration of the Cisco SD-WAN solution with Azure virtual WAN enhances Cloud OnRamp for Multi-Cloud deployments and enables configuring Cisco Catalyst 8000V Edge Software (Cisco Catalyst 8000V) as a network virtual appliance (NVA) in Azure Virtual WAN hubs. View Cisco SD-WAN Cloud OnRamp, Cisco IOS XE Release 17.x configuration guide	Yes
VMware SD-WAN	vmwaresdwaninvwan	VMware SD-WAN in Virtual WAN hub deployment guide. The managed application for deployment can be found at this Azure Marketplace link.	Yes
Versa Networks	versanetworks	If you're an existing Versa Networks customer, log on to your Versa account and access the deployment guide using the following link Versa Deployment Guide. If you're a new Versa customer, sign-up using the Versa preview sign-up link.	Yes
Aruba EdgeConnect	arubaedgeconnectenterprise	Aruba EdgeConnect SD-WAN deployment guide. **Currently in Preview:** Azure Marketplace link	No

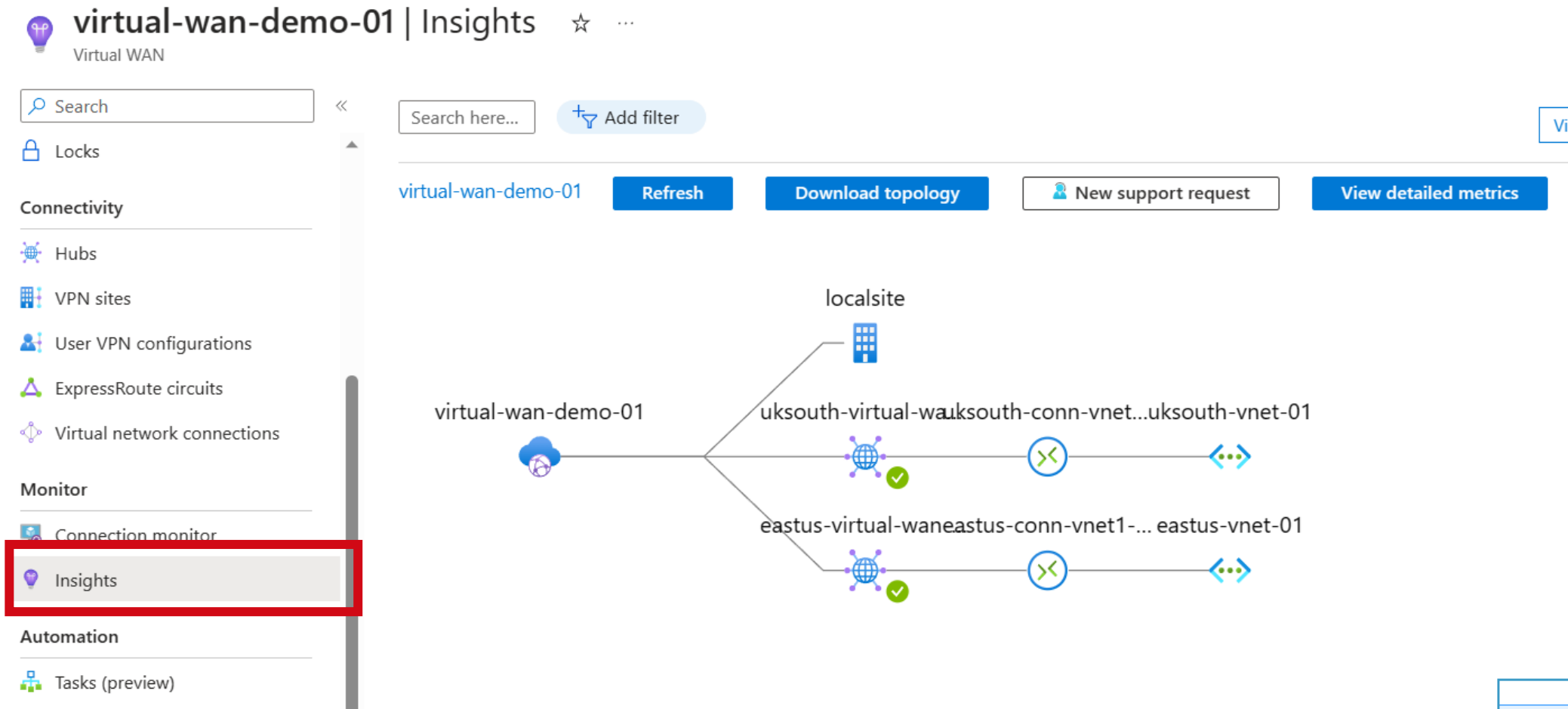
https://learn.microsoft.com/en-us/azure/virtual-wan/about-nva-hub#partners

Azure Firewall and NVA Options

- Azure Firewall provides an Azure Native Firewall option that can be controlled and Managed using Azure Firewall Manager.
- Security Partner Providers bring Security as a Service (SECaaS) to Azure Virtual WAN – Zscaler, CheckPoint, iboss…
- Hub Routing Intent – GA 18/05/2023: https://learn.microsoft.com/en-us/azure/virtual-wan/how-to-routing-policies

Monitoring

- A wide range of options using Azure Monitor
- Insights Dashboard for Virtual WAN



Monitoring – let's talk metrics!

Metric	Description
Virtual Hub Data Processed	Data in bytes/second on how much traffic traverses the virtual hub router in a g period. Note that only the following flows use the virtual hub router: VNet to VI and VPN/ExpressRoute branch to VNet (interhub).

Metric	Description
Gateway P2S Bandwidth	Average point-to-site aggregate bandwidth of a gateway in bytes per second.
P2S Connection Count	Point-to-site connection count of a gateway. To ensure you're viewing accurate Azure Monitor, select the **Aggregation Type** for **P2S Connection Count** as **Sum** select **Max** if you split By **Instance**.
User VPN Routes Count	Number of User VPN Routes configured on the VPN gateway. This into **Static** and **Dynamic** Routes.

Metric	Description
Tunnel Egress Packet Drop Count	Count of Outgoing packets dropped by tunnel.
Tunnel Ingress Packet Drop Count	Count of Incoming packets dropped by tunnel.
Tunnel NAT Packet Drops	Number of NATed packets dropped on a tunnel by drop type and NAT rule.
Tunnel Egress TS Mismatch Packet Drop	Outgoing packet drop count from traffic selector mismatch of a tunnel.
Tunnel Ingress TS Mismatch Packet Drop	Incoming packet drop count from traffic selector mismatch of a tunnel.

Metric	Description
BGP Peer Status	BGP connectivity status per peer and per instance.
BGP Routes Advertised	Number of routes advertised per peer and per instance.
BGP Routes Learned	Number of routes learned per peer and per instance.
VNET Address Prefix Count	Number of VNet address prefixes that are used/advertised by the gateway.

Monitoring – let's talk metrics!

@welshazure

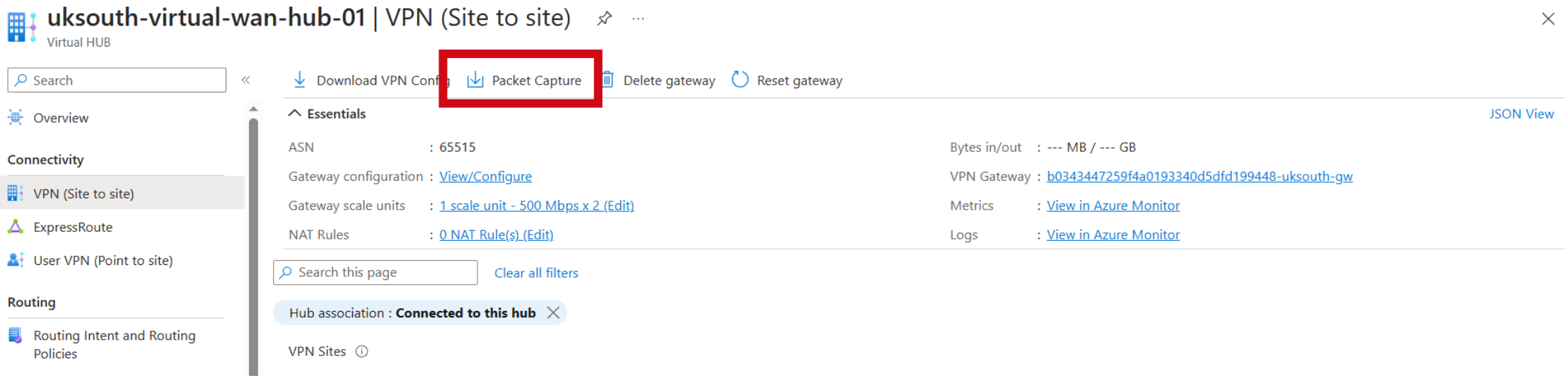
Metric	Description
BitsInPerSecond	Bits per second ingressing Azure via ExpressRoute gateway that can be split for specific connections.
BitsOutPerSecond	Bits per second egressing Azure via ExpressRoute gateway that can be split for specific connections.
Bits Received Per Second	Total Bits received on ExpressRoute gateway per second.
CPU Utilization	CPU Utilization of the ExpressRoute gateway.
Packets per second	Total Packets received on ExpressRoute gateway per second.
Count of routes advertised to peer	Count of Routes Advertised to Peer by ExpressRoute gateway.
Count of routes learned from peer	Count of Routes Learned from Peer by ExpressRoute gateway.
Frequency of routes changed	Frequency of Route changes in ExpressRoute gateway.
Number of VMs in Virtual Network	Number of VMs that use this ExpressRoute gateway.

Metric	Description
Gateway Diagnostic Logs	Gateway-specific diagnostics such as health, configuration, service updates, and additional diagnostics.
Tunnel Diagnostic Logs	These are IPsec tunnel-related logs such as connect and disconnect events for a site-to-site IPsec tunnel, negotiated SAs, disconnect reasons, and additional diagnostics.
Route Diagnostic Logs	These are logs related to events for static routes, BGP, route updates, and additional diagnostics.
IKE Diagnostic Logs	IKE-specific diagnostics for IPsec connections.

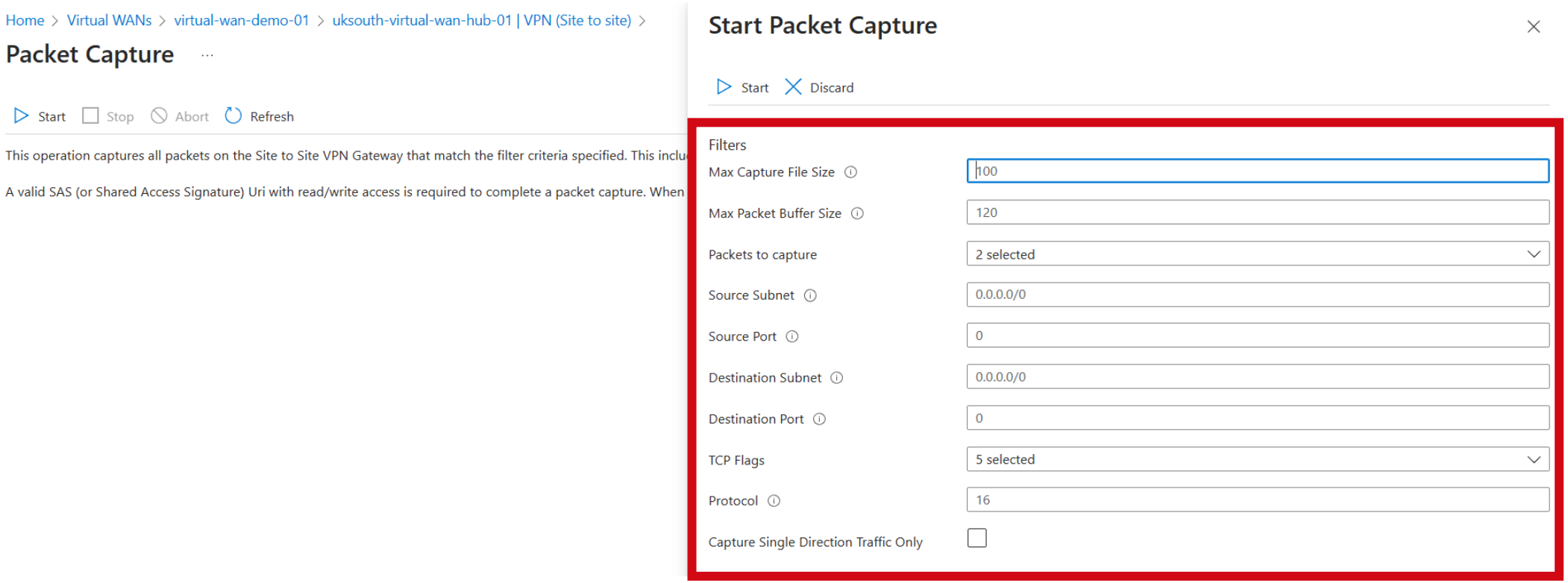
https://learn.microsoft.com/en-us/azure/virtual-wan/monitor-virtual-wan-reference

Packet Capture – available for S2S VPNs

- Requires a Virtual WAN and Hub, with a S2S VPN Gateway deployed.
- Logs captures to a Storage Account Container
- Supports optional filters, e.g. TCPFlags or MaxFileSize



Packet Capture – available for S2S VPNs



Administration – obvious, but relevant…

- Centralised Cloud Network - use Entra ID credentials for Administration
- Entra ID means PIM / MFA etc.
- No need for a jump host or Bastion to administrate network appliances (even more so with PAAS offerings like Azure Firewall/Gateway).
- Management via ARM / Azure Portal

Azure Security Baseline – a very worthwhile read!

Learn / Security / Benchmark / Security baselines for Azure (MCSB v1) /

Azure security baseline for Virtual WAN

Article • 09/20/2023 • 1 contributor

Feedback

In this article

Security profile
Identity management
Data protection
Asset management
Show 2 more

This security baseline applies guidance from the Microsoft cloud security benchmark version 1.0 to Virtual WAN. The Microsoft cloud security benchmark provides recommendations on how you can secure your cloud solutions on Azure. The content is grouped by the security controls defined by the Microsoft cloud security benchmark and the related guidance applicable to Virtual WAN.

You can monitor this security baseline and its recommendations using Microsoft Defender for Cloud. Azure Policy definitions will be listed in the Regulatory Compliance section of the Microsoft Defender for Cloud portal page.

When a feature has relevant Azure Policy Definitions, they are listed in this baseline to help you measure compliance with the Microsoft cloud security benchmark controls and recommendations. Some recommendations may require a paid Microsoft Defender plan to enable certain security scenarios.

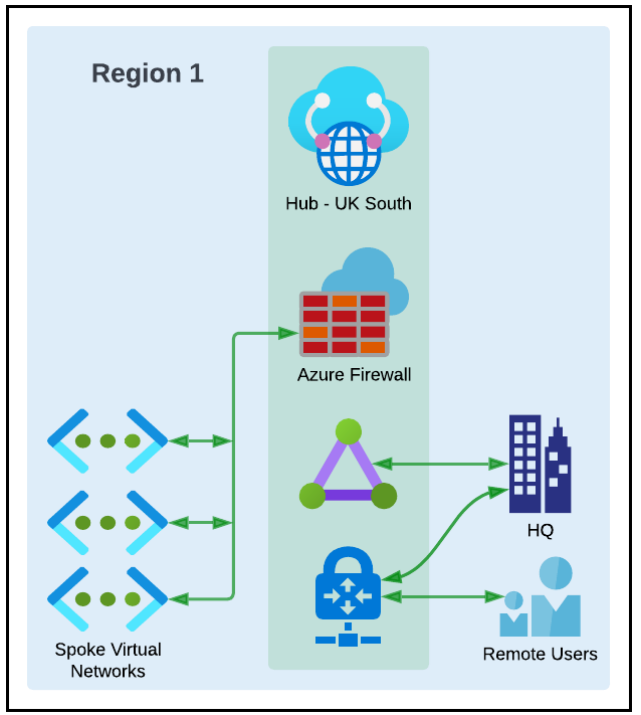
https://learn.microsoft.com/en-us/security/benchmark/azure/baselines/virtual-wan-security-baseline

Expansion Options

Expansion is easy with Virtual WAN:

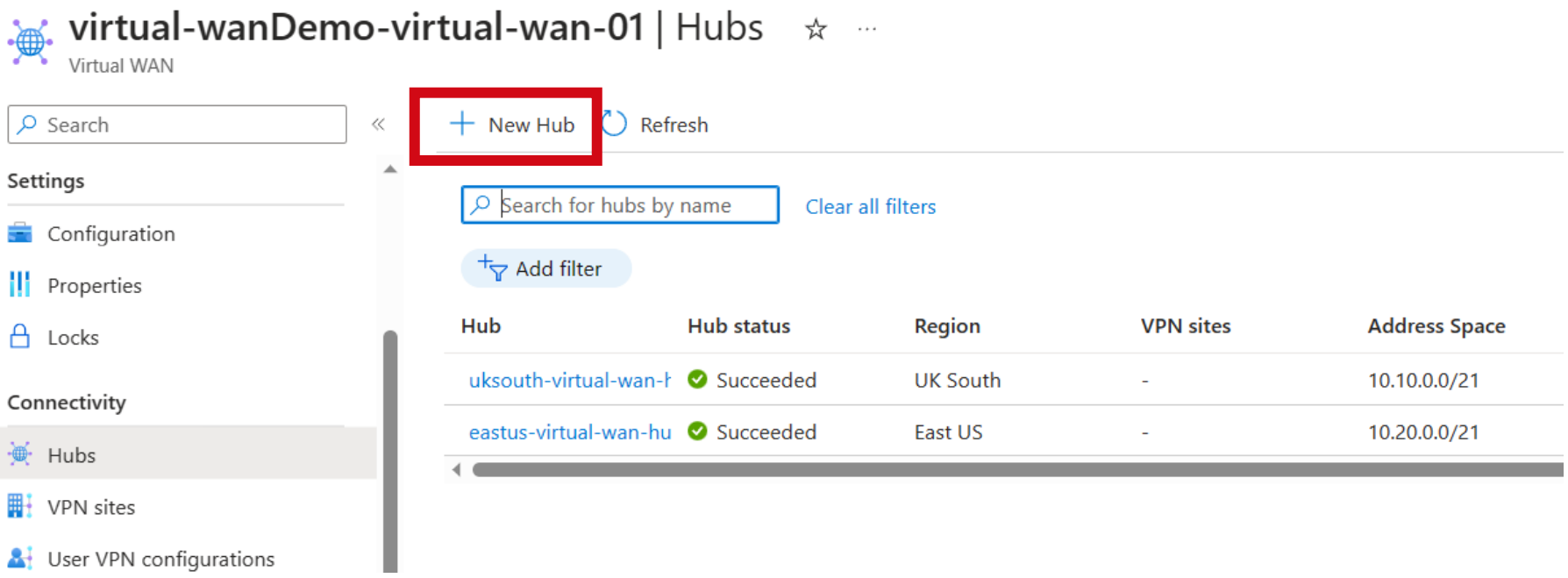
- Our start – Single Virtual WAN hub, ExpressRoute and a VPN Gateway for IPsec or P2S Users.
- Spoke Virtual Networks peered into Virtual WAN hub.
- All Traffic via Single Azure Firewall instance.

How do we expand to other Regions?

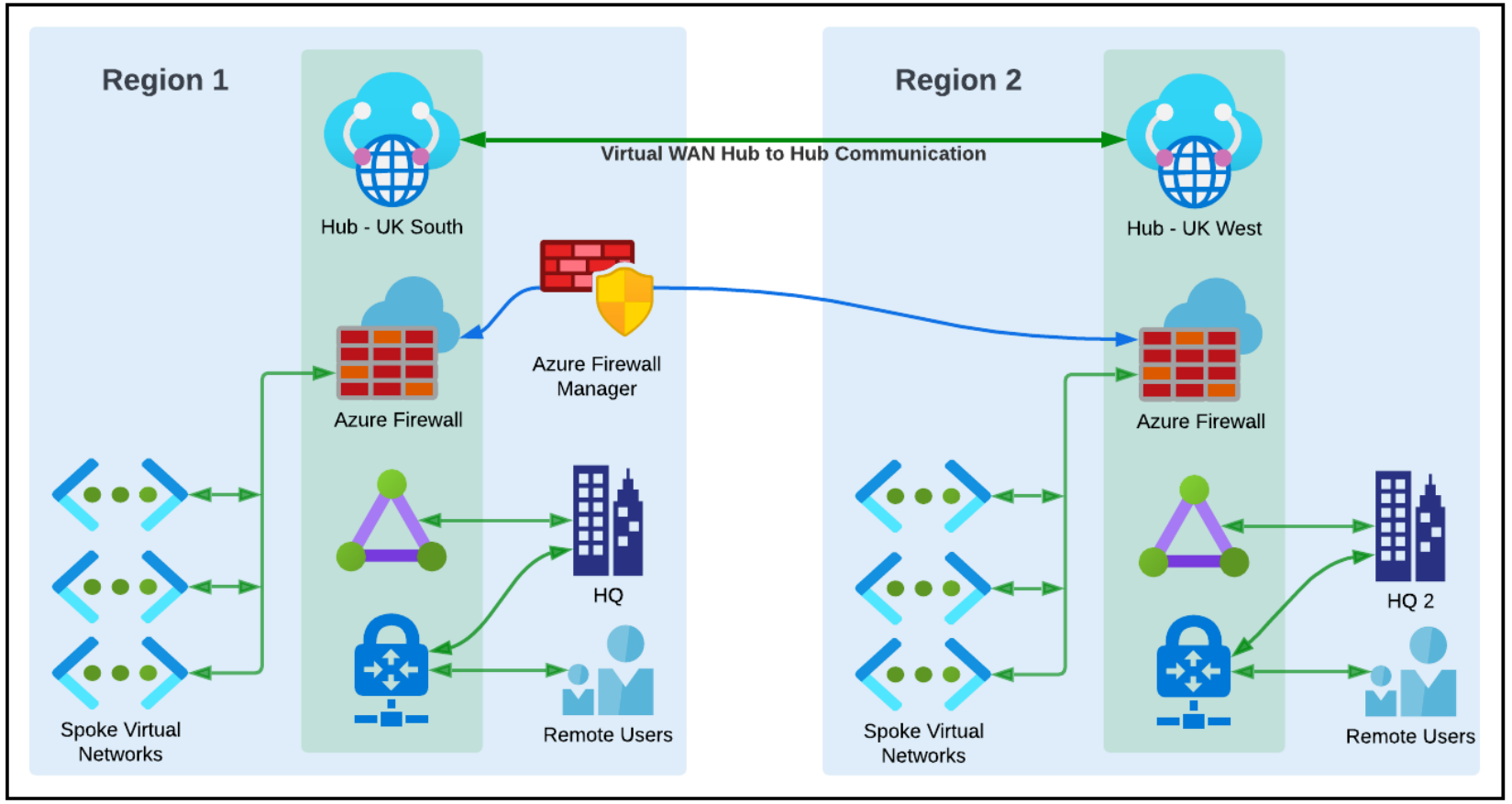


Expansion Options

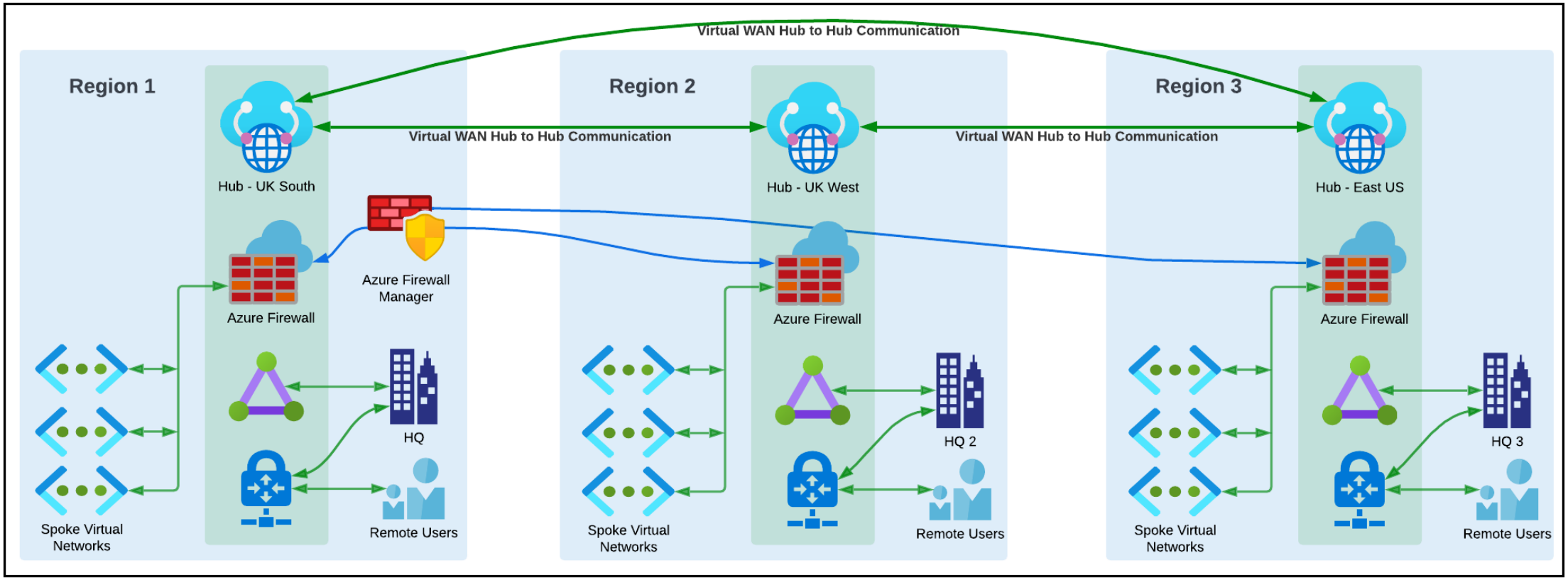
- ✓ Regional Expansion is simple – and done by adding Hubs
- ✓ Hubs are fully-meshed by default, enabling communication



Expansion Options... +1 Region



Expansion Options... +2 Regions



Expansion Options

- ✓ Regional Expansion
- ✓ Firewalling options – Scale up to Premium
- ✓ Hub Routing Intent – Cross Region & Internet traffic all via NVAs/AzFWs
- ✓ Centralised Firewall Rulesets and Management
- ✓ ExpressRoute and VPN Gateway Support (S2S and P2S)
- ✓ Full Mesh Topology – enabling communication via the MS Global Network
- ✓ Spokes can communicate (via Firewall if required).
- ✓ Automated Route Table Management & Provisioning
- ✓ Single Control of Virtual Networks via Virtual WAN
- ✓ Scale in routing units up to 50Gbps and 50,000 VMs per Hub

Where do we begin?

- **Recommendation** – Get familiar with the basics and concepts using a lab. My Terraform Environment can help here!
- Consider **upskilling and training** – AZ-700 and AZ-305 exams are helpful.
- **Have a plan!** Consider the Cloud Adoption Framework guidance and understand drivers/goals/objectives.
- Organisational deployment - **Start with a Single Hub** and expand from there.
- Consult **Guidance** – MS docs for migrating from Hub/Spoke - https://learn.microsoft.com/en-us/azure/virtual-wan/migrate-from-hub-spoke-topology
- **Engage a Partner** – Design/Implementation/Support etc.

Demo / Lab Environment - Terraform

```
# virtual-wan Resources
# virtual-wan
resource "azurerm_virtual_wan" "virtual-wan1" {
  name                = "${var.lab-name}-virtual-wan-01"
  resource_group_name = azurerm_resource_group.region1-rg1.name
  location            = var.region1

  # Configuration
  office365_local_breakout_category = "OptimizeAndAllow"

  tags = {
    Environment = var.environment_tag
  }
}
# virtual-wan Hub 1
resource "azurerm_virtual_hub" "region1-vhub1" {
  name                = "${var.region1}-virtual-wan-hub-01"
  resource_group_name = azurerm_resource_group.region1-rg1.name
  location            = var.region1
  virtual_wan_id      = azurerm_virtual_wan.virtual-wan1.id
  address_prefix      = var.virtual-wan-region1-hub1-prefix1

  tags = {
    Environment = var.environment_tag
  }
}
```

https://github.com/jakewalsh90/Terraform-Azure/tree/main/Virtual-WAN-Demo

Useful Links

- https://learn.microsoft.com/en-us/azure/virtual-wan/
- **John Savill** - https://www.youtube.com/watch?v=f-GyAURZWzg
- **Global Transit Architecture**: https://learn.microsoft.com/en-us/azure/virtual-wan/virtual-wan-global-transit-network-architecture

- https://jakewalsh.co.uk/deploying-azure-virtual-wan-using-terraform/
- https://github.com/jakewalsh90/Terraform-Azure/tree/main/vWAN-DemoLab
- https://github.com/jakewalsh90/Terraform-Modules-Azure/tree/main/azure-quick-virtualwan
- Exams – Az-700 and Az-305

- NVA Options: https://learn.microsoft.com/en-us/azure/virtual-wan/about-nva-hub
- https://learn.microsoft.com/en-us/azure/virtual-wan/about-nva-hub#partners

creditsafe Servent <packt>

Welsh Azure User Group

@welshazure

Thank You!

Building a Cloud Centric Network with Azure Virtual WAN

Jake Walsh
@jakewalsh90
jakewalsh.co.uk