AZURE

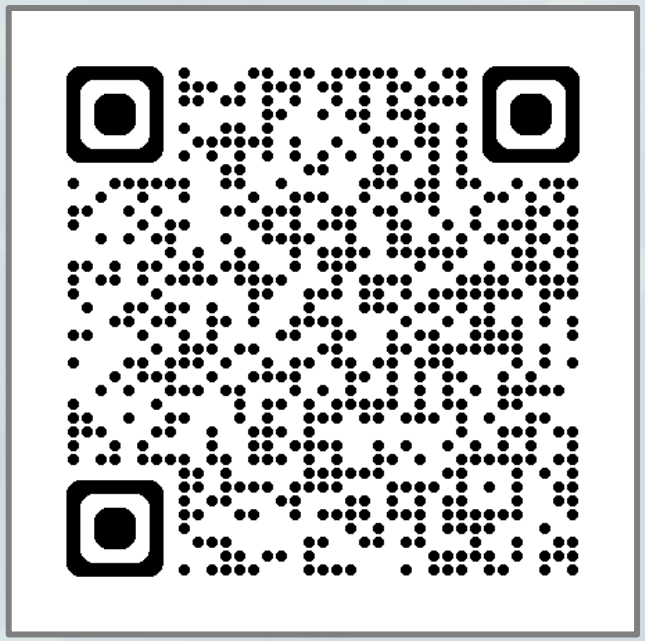
BOOTCAMP SWITZERLAND

Microsoft® Most Valuable Professional

Building a Cloud Centric Network with Azure Virtual WAN

Jake Walsh

Please note – the views/opinions in this presentation are entirely my own.
If in any doubt, please check latest documentation and MS Links for updated info!



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 and MS Links for updated info!

AZURE
BOOTCAMP SWITZERLAND

Agenda

- Overview
- Use Cases & Core Components
- Why use Azure Virtual WAN?
- Security
- Expansion
- Getting Started
- Demo Environment (Time Permitting!)
- Resources to help – to be shared in slides afterwards.

What is Azure Virtual WAN?

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

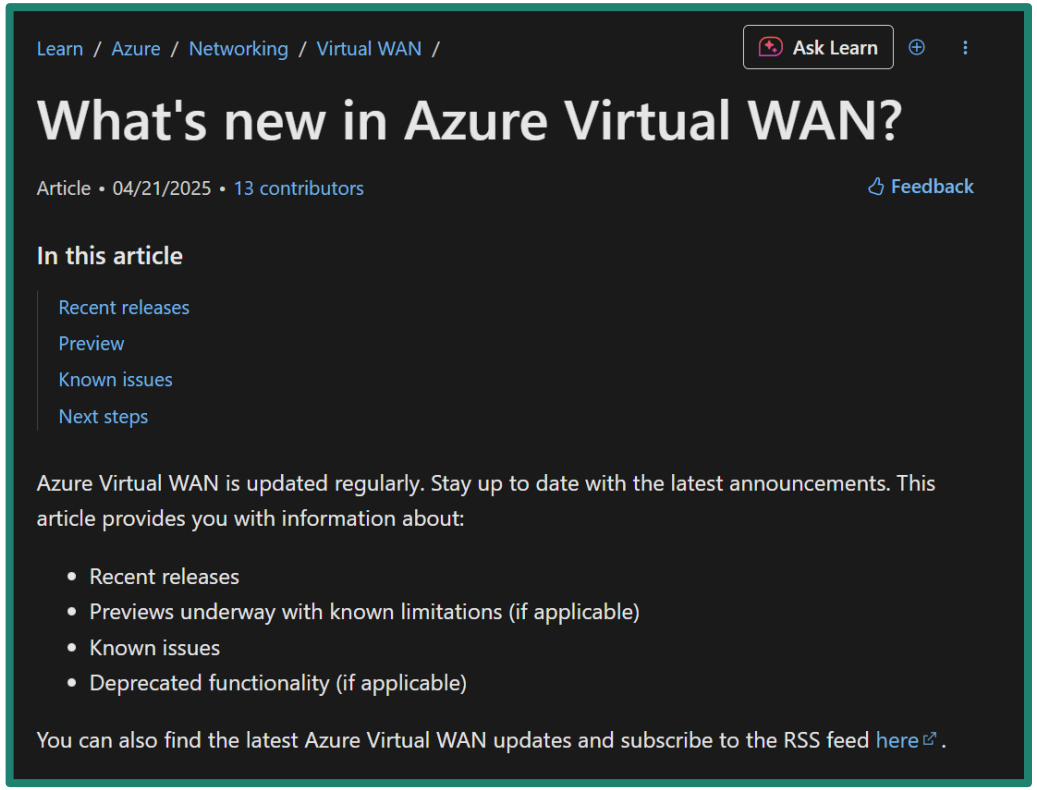
- Key Features Include:
  - Automated large-scale branch connectivity
  - Unified network and policy management
  - Optimised routing thanks to the Microsoft Global Network

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

Always improving...



Learn / Azure / Networking / Virtual WAN / Ask Learn

What's new in Azure Virtual WAN?

Article • 04/21/2025 • 13 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.

Routing

Expand table

Type	Area	Name	Description	Date added	Limitations
Feature	Routing	Route-maps	General Availability of Route-maps. Route-maps is a feature that gives you the ability to control route advertisements and routing for Virtual WAN virtual hubs.	April 2025	Known limitations
Metric	Routing	New Virtual hub metrics	There are now two new Virtual WAN hub metrics that display the virtual hub's capacity and spoke Virtual Machine (VM) utilization: **Routing Infrastructure Units** and **Spoke VM Utilization**.	August 2024	The **Spoke VM Utilization** metric represents an approximate number of deployed spoke VMs as a percentage of the total number of spoke VMs that the hub's routing infrastructure units can support.

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

- Most Azure Public Regions – some limitations around Reserved Access
- US Government and Azure China also available
- Availability Zones – key consideration

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

https://azure.microsoft.com/en-us/explore/global-infrastructure/products-by-region/table

Use Cases

- 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

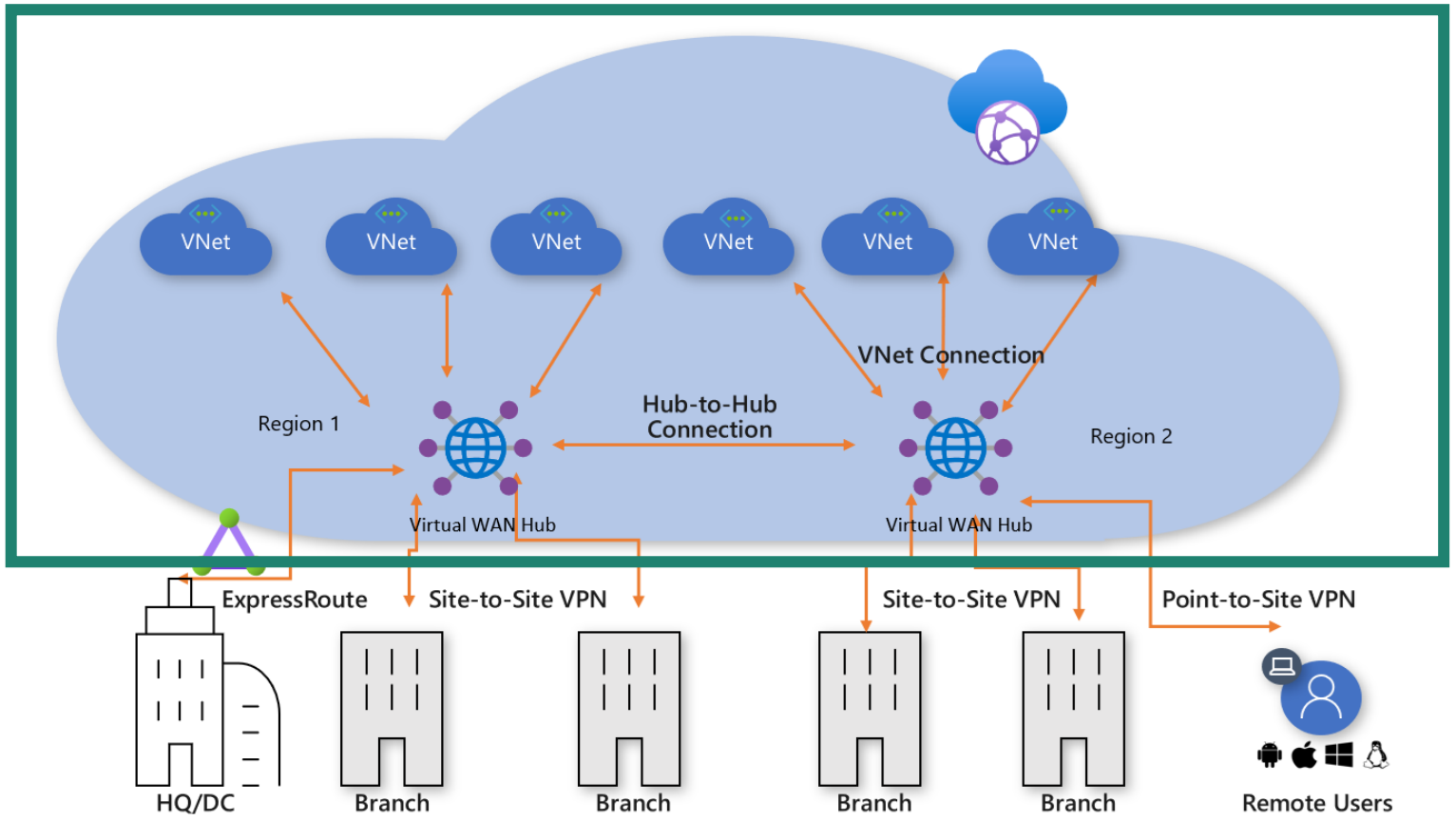
You can upgrade from Basic to Standard, but can't revert from Standard back to Basic.

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

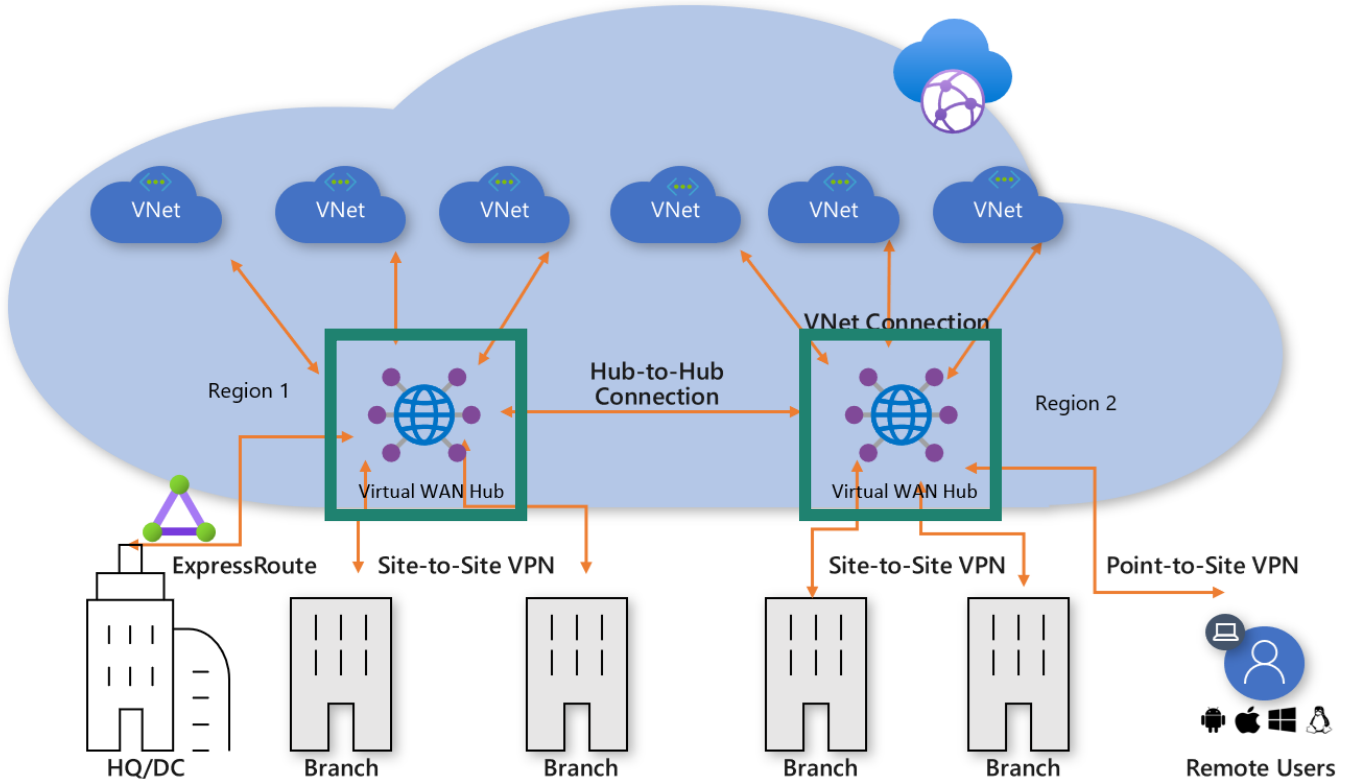
Virtual WAN



- Virtual overlay of your Azure Networking
- A collection of multiple Resources
- Contains all Virtual WAN components within your topology
- The point of administration for your Virtual WAN deployment.

Hub

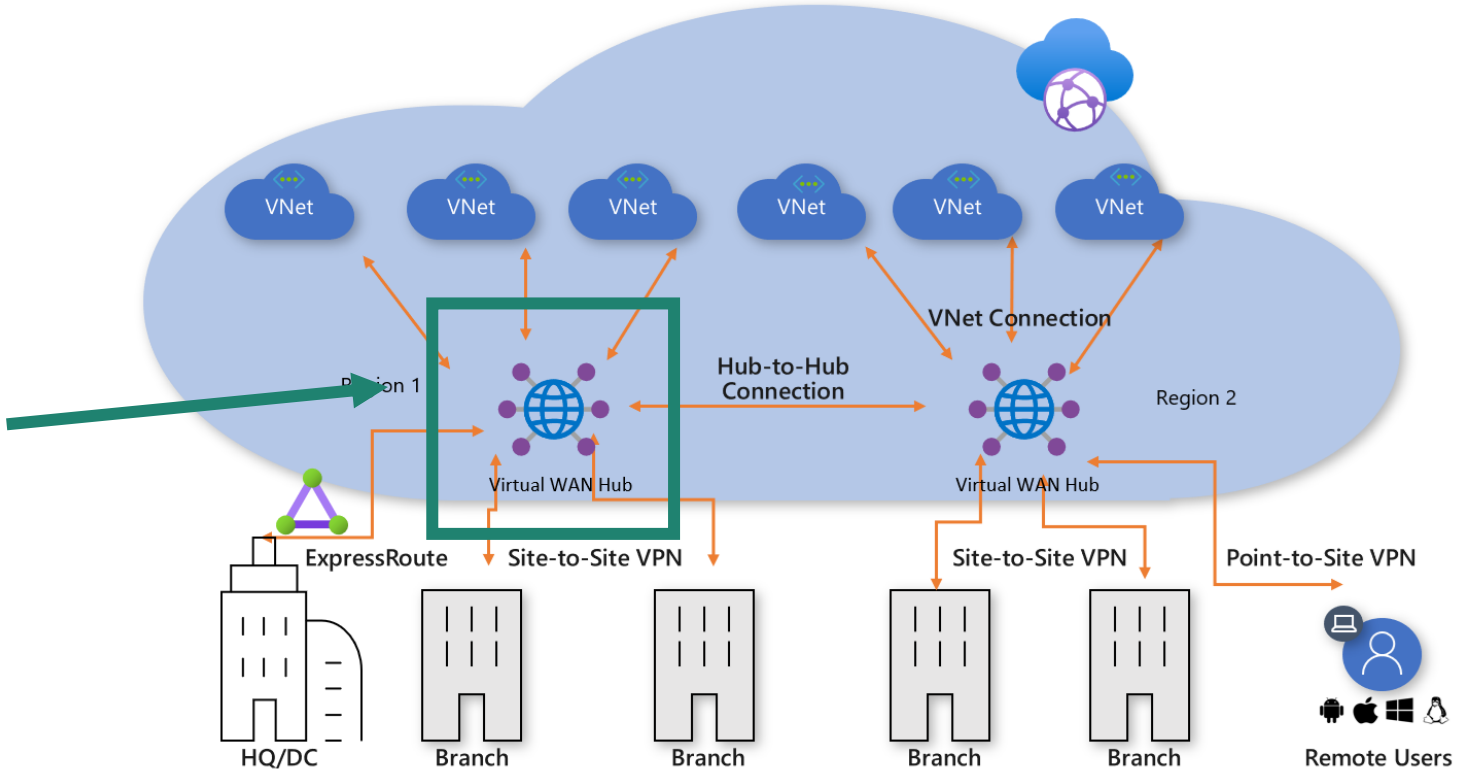
- The Virtual Hub is a Microsoft Managed Virtual Network, containing various service endpoints.
- The Hub is the Core of the Virtual WAN network in an Azure Region. Typically 1 Hub per Region but can be more.
- Gateways for VPN/ExpressRoute deployed within Hubs.
- Firewalls / NVAs deployed into Hubs.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



What's in the Hub?

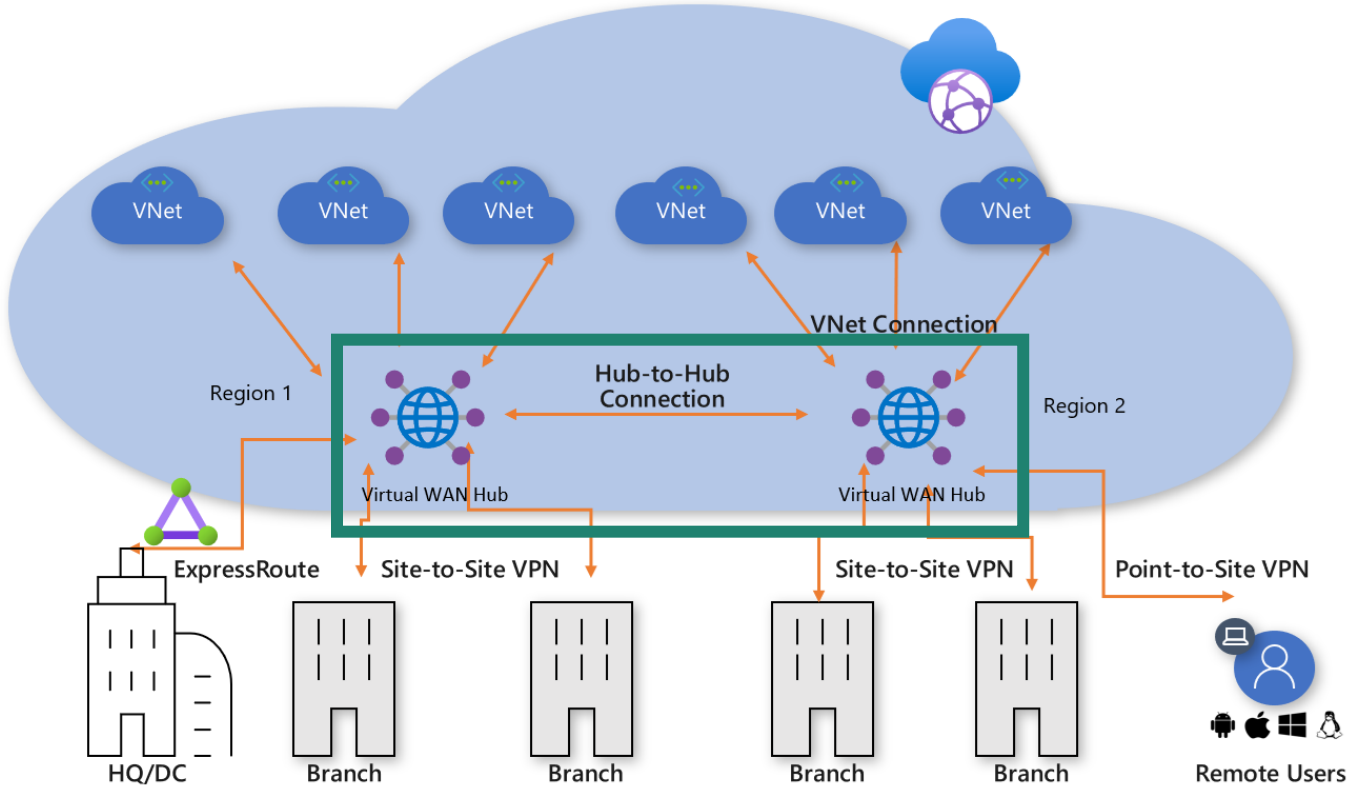
Items we can deploy into a Hub:

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



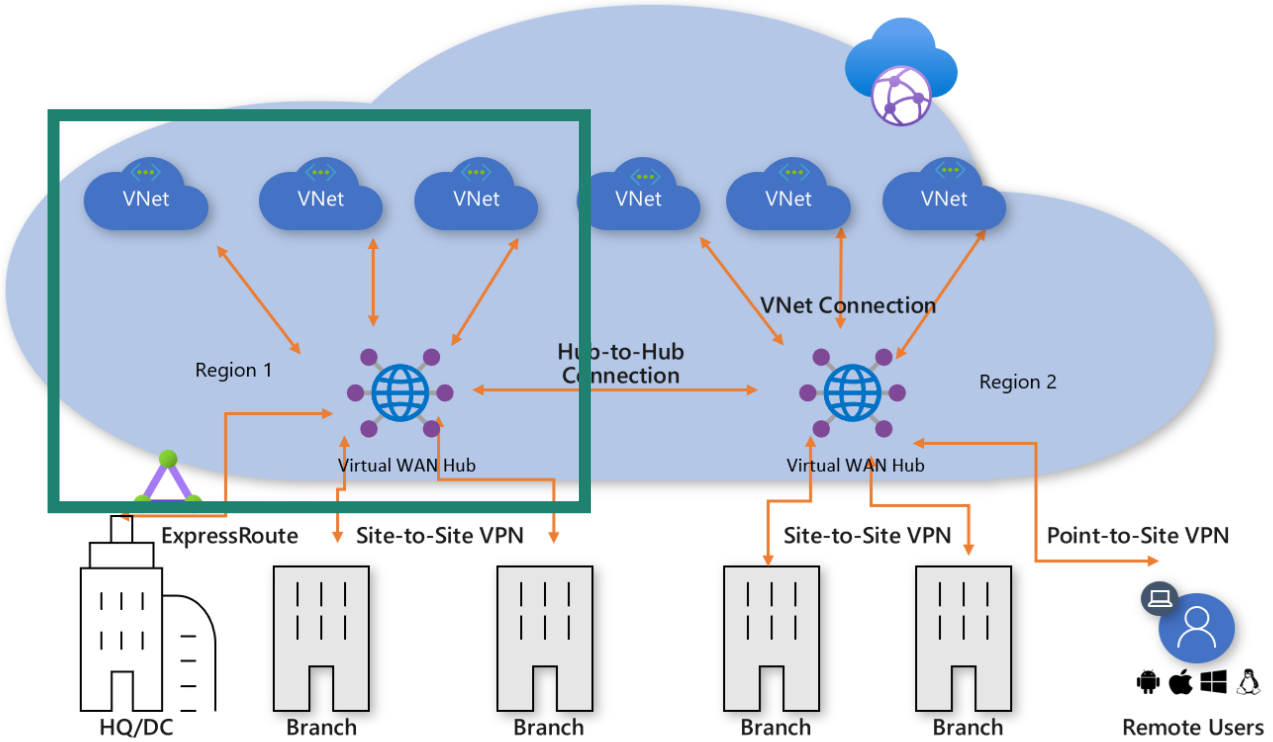
Hub to Hub Connection

- 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.



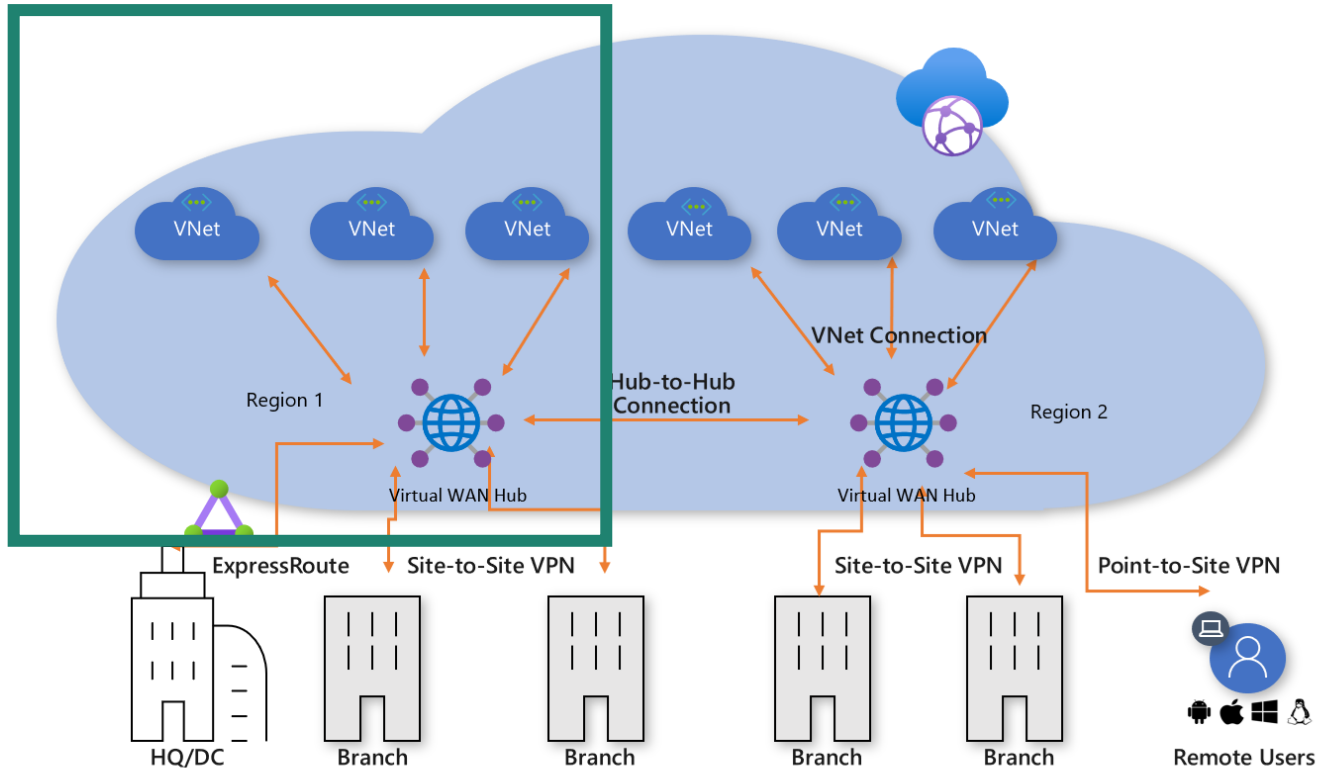
Hub Virtual Network Connection

- 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

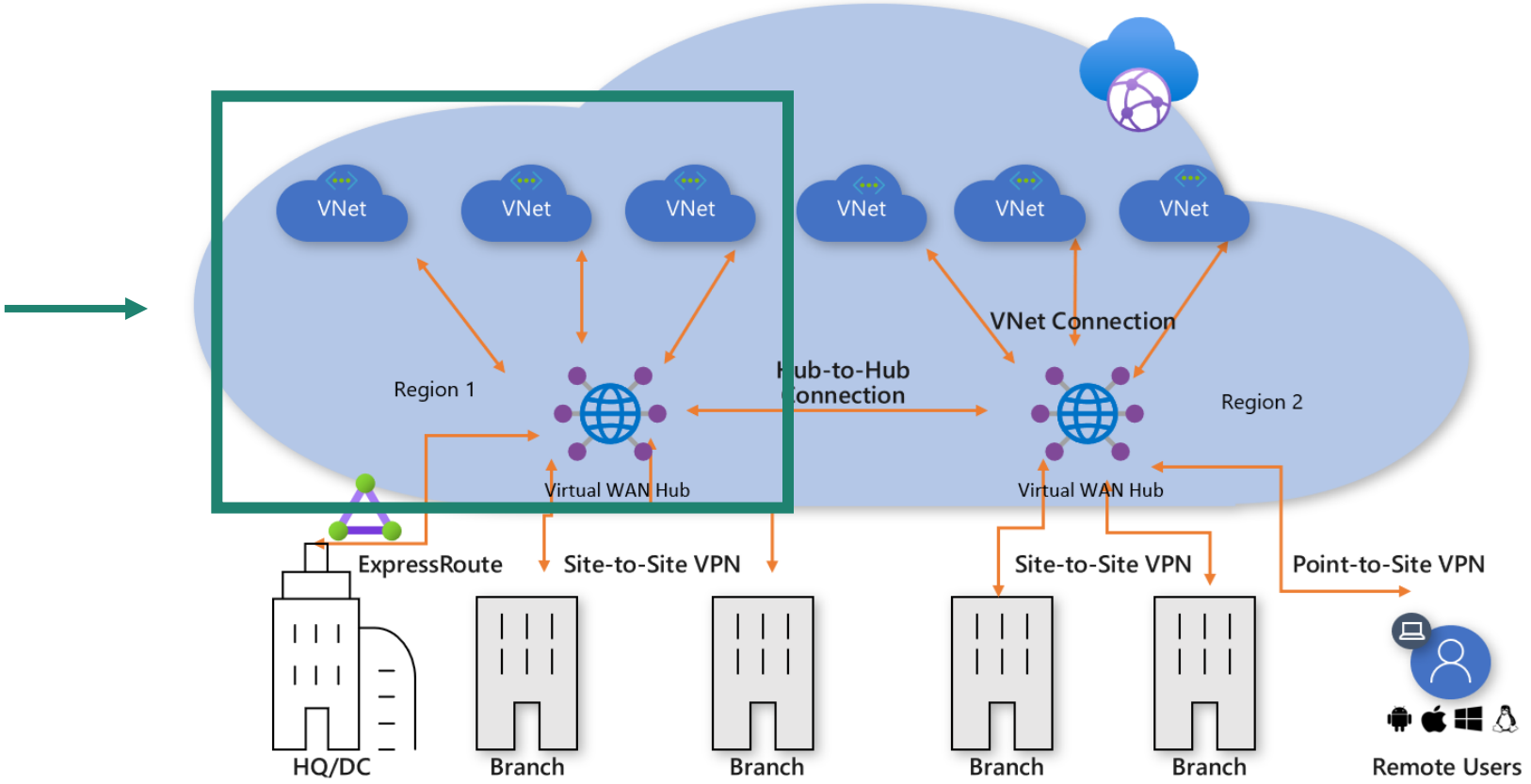
- Each Hub has its own default route table. This can be edited to add static routes if required.
- Static routes take precedence over dynamic routes.
- Associated with a Hub and it's connected Virtual Networks.
- Connections, e.g. VPN, ExpressRoute or PS2 will also have a routing configuration that propagates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

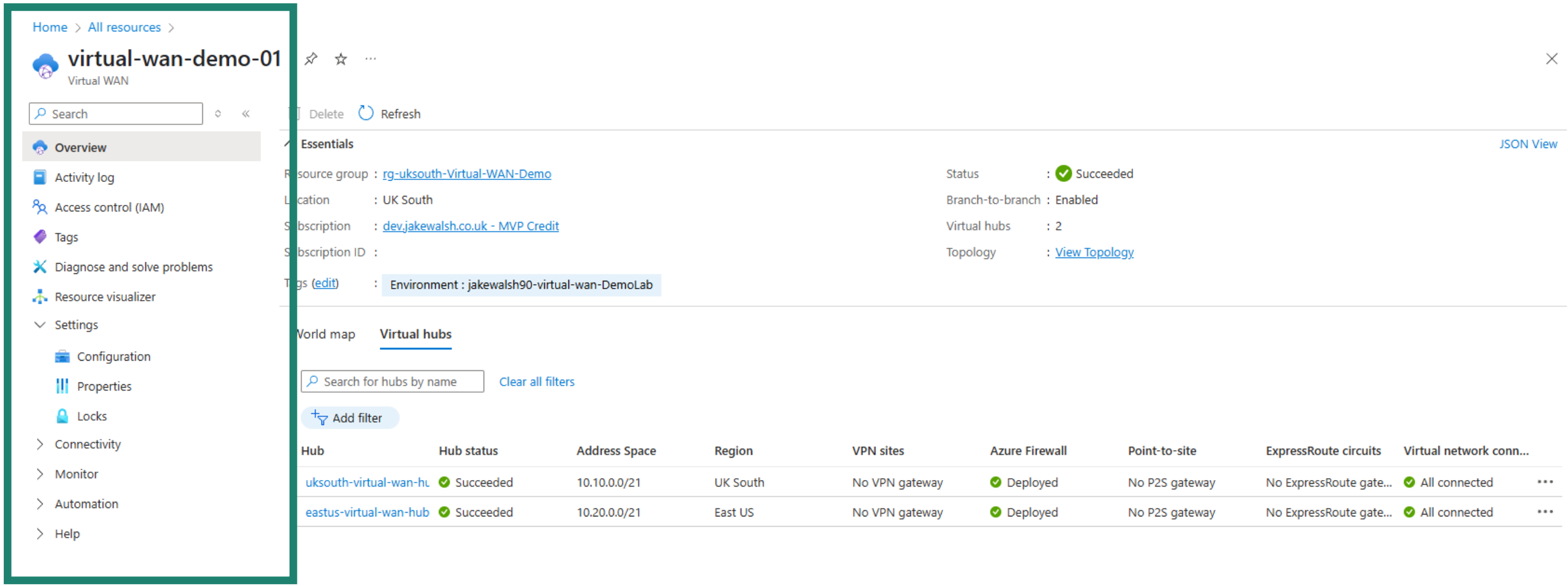
- Virtual WAN replaces an existing Hub Spoke architecture with Spoke VNETs peered into a Virtual WAN Hub.
- Hubs become fully managed by Virtual WAN.
- Central management of all Hubs in the topology.
- All Spokes peer into a Virtual WAN Hub, with connectivity and inter-region traffic routed via the Hub.



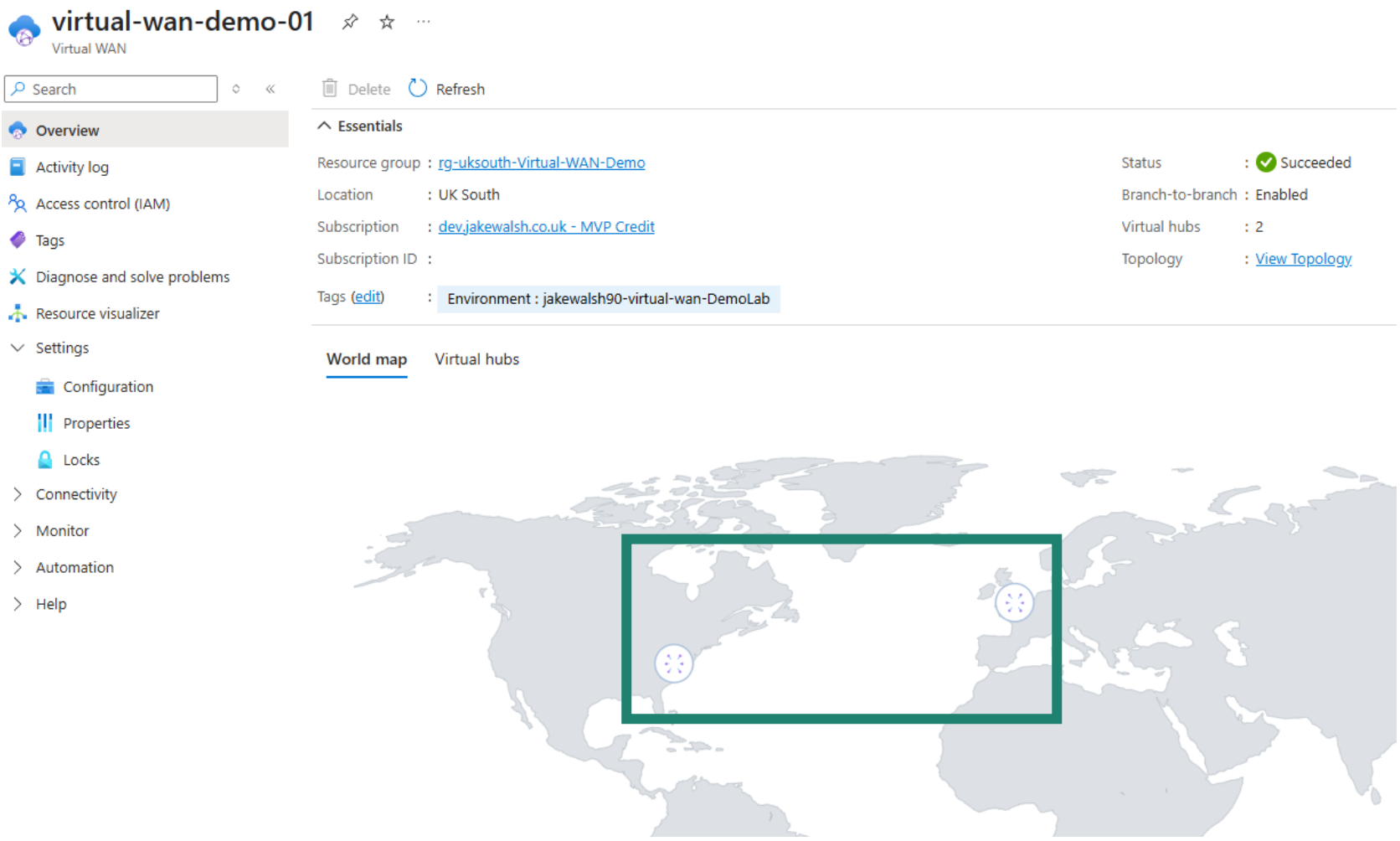
Why Virtual WAN? Core Benefits:

- **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.

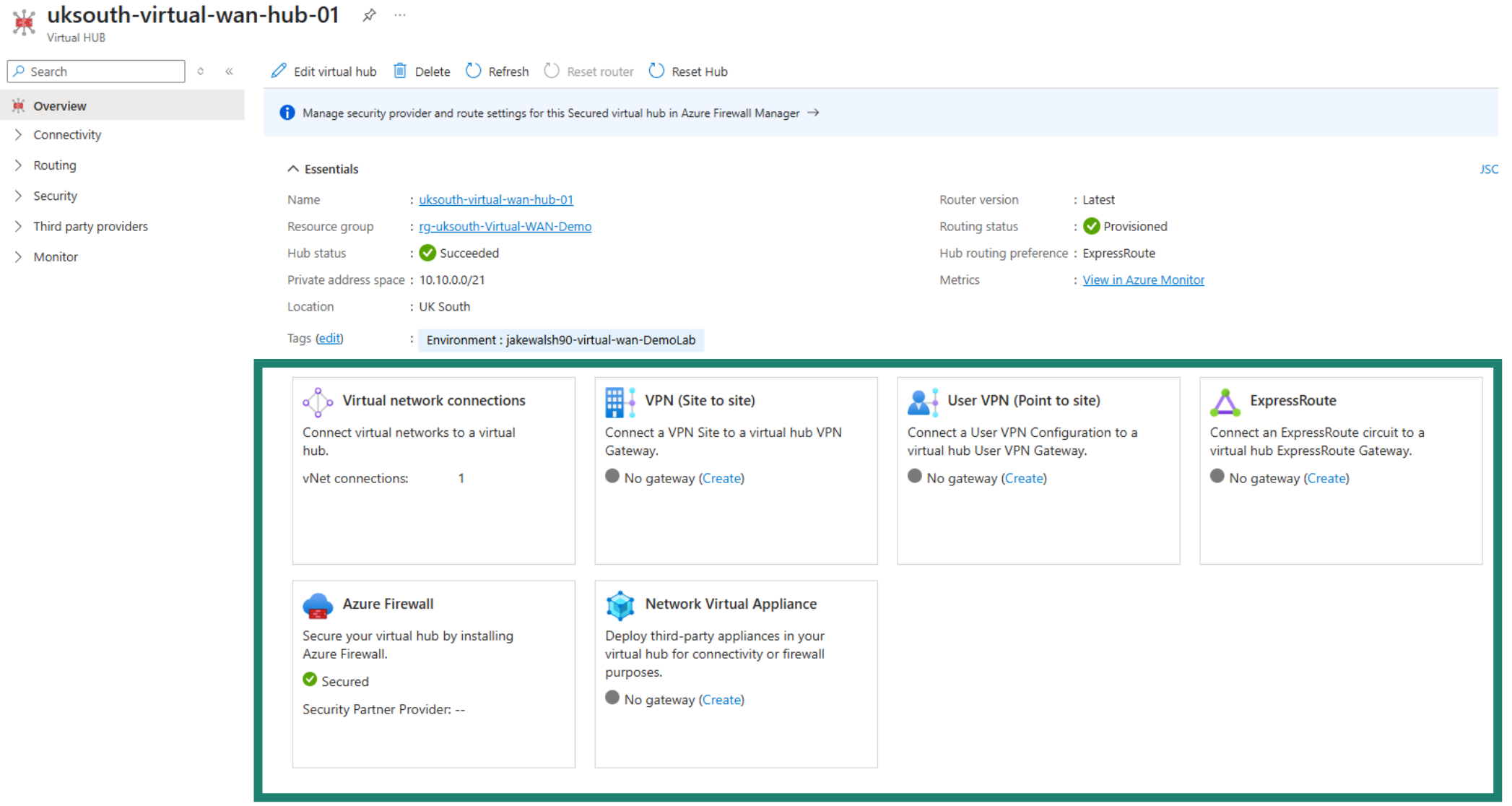
An Integrated Solution – All core networking aspects in a single control Resource. Site to Site and Connectivity options are easily accessed and managed. **Simple administration!**



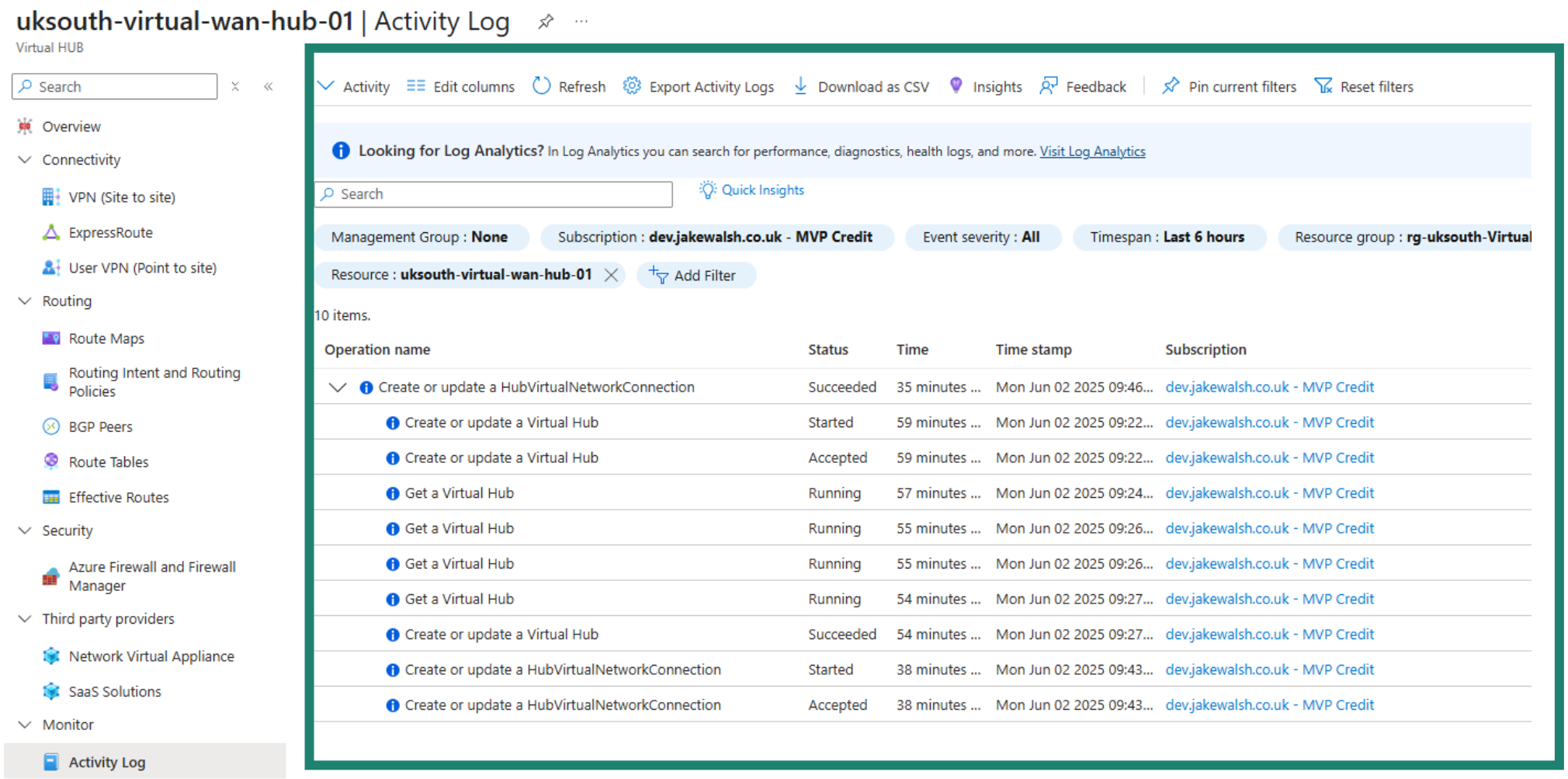
An Integrated Solution – All core networking aspects in a single control Resource. Site to Site and Connectivity options are easily accessed and managed. **Simple administration!**



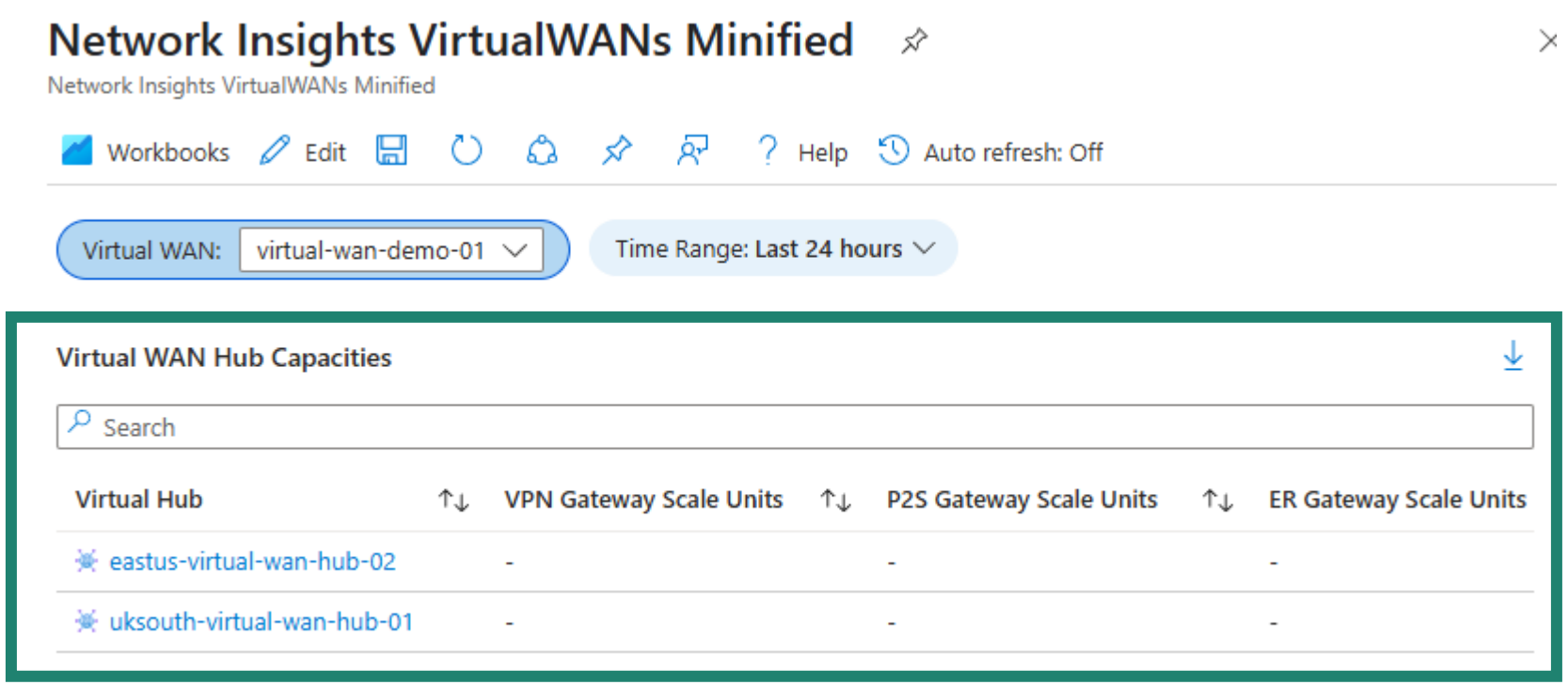
An Automated Solution – Connect Virtual Networks to the Hubs easily, and also bring additional services into Virtual WAN with ease – again, centralised, simplified and automated is the key.



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



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



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

AZURE BOOTCAMP SWITZERLAND

Metrics

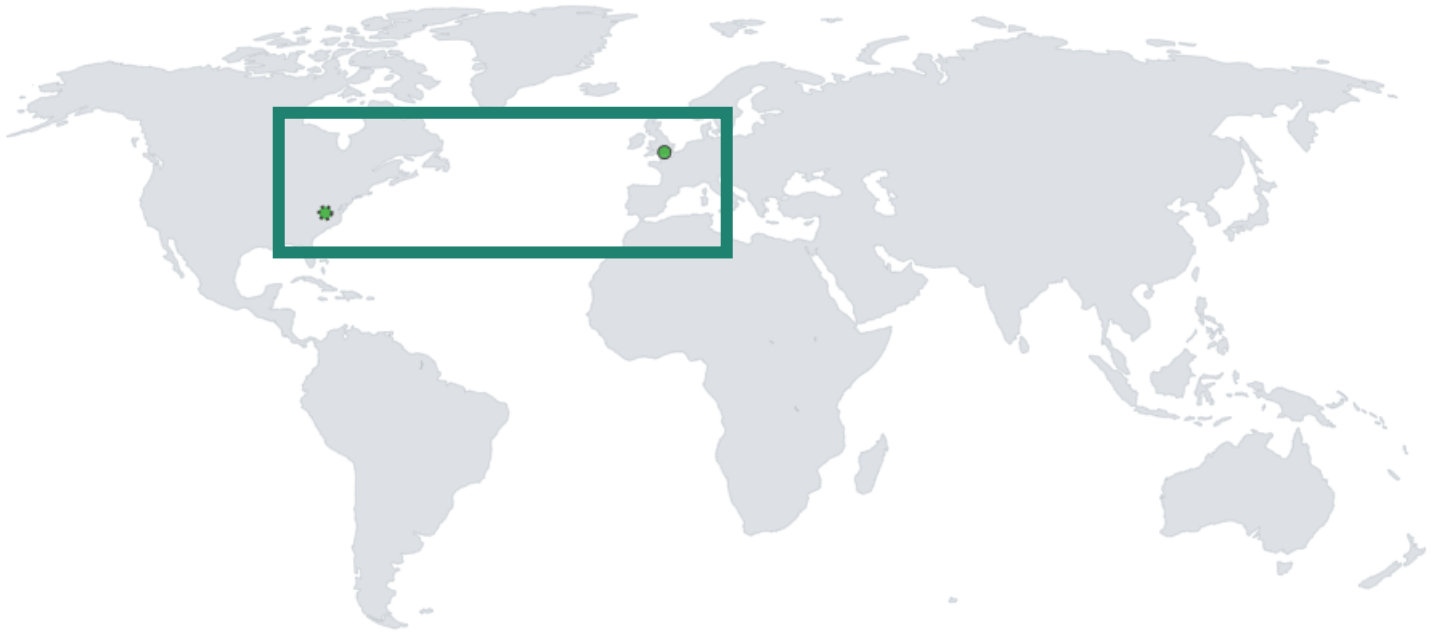
Network Insights VirtualWANs

Workbooks | Edit | Help | Auto refresh: Off

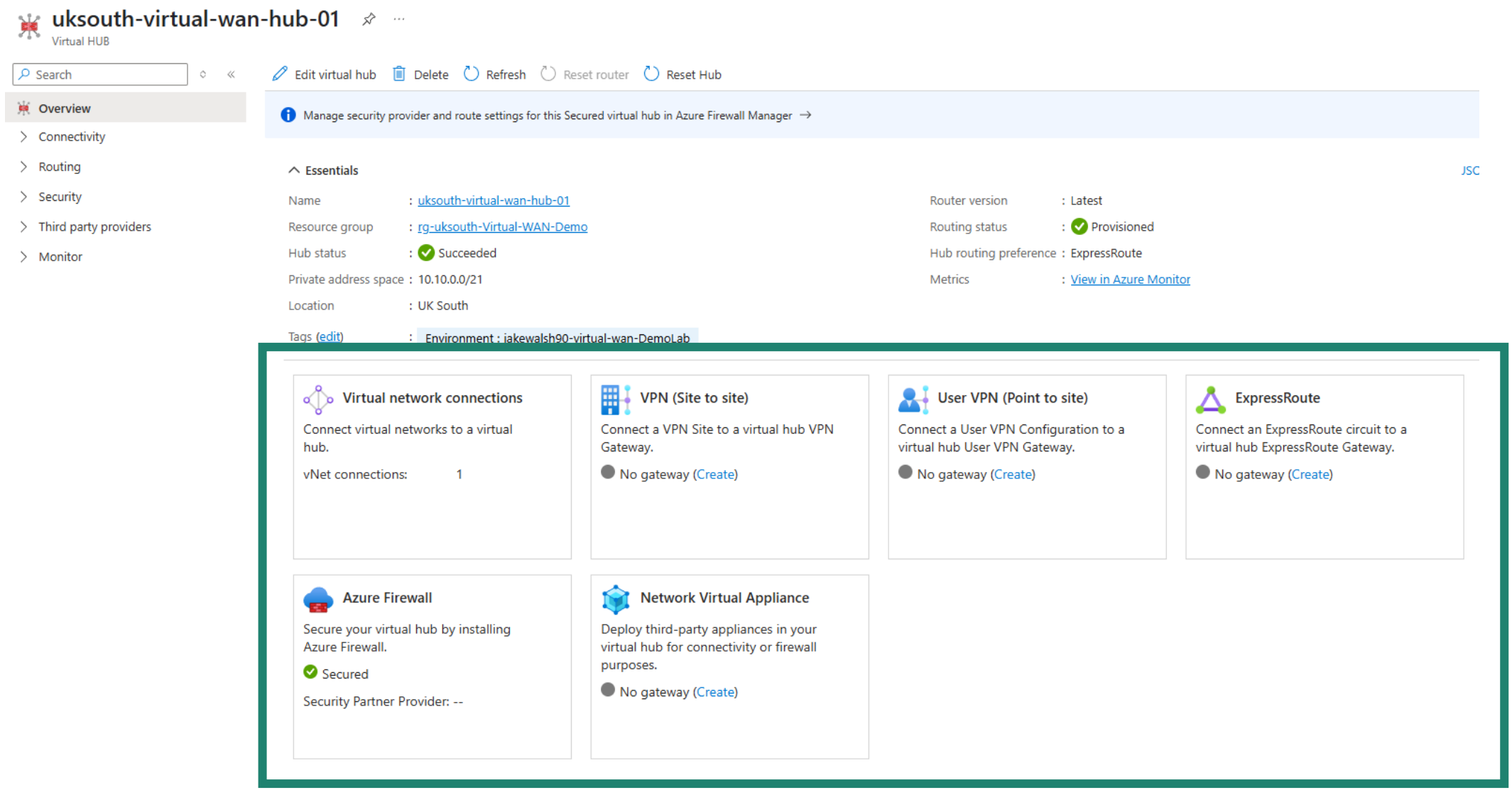
Virtual WAN: **virtual-wan-demo-01** | Time Range: **Last 24 hours**

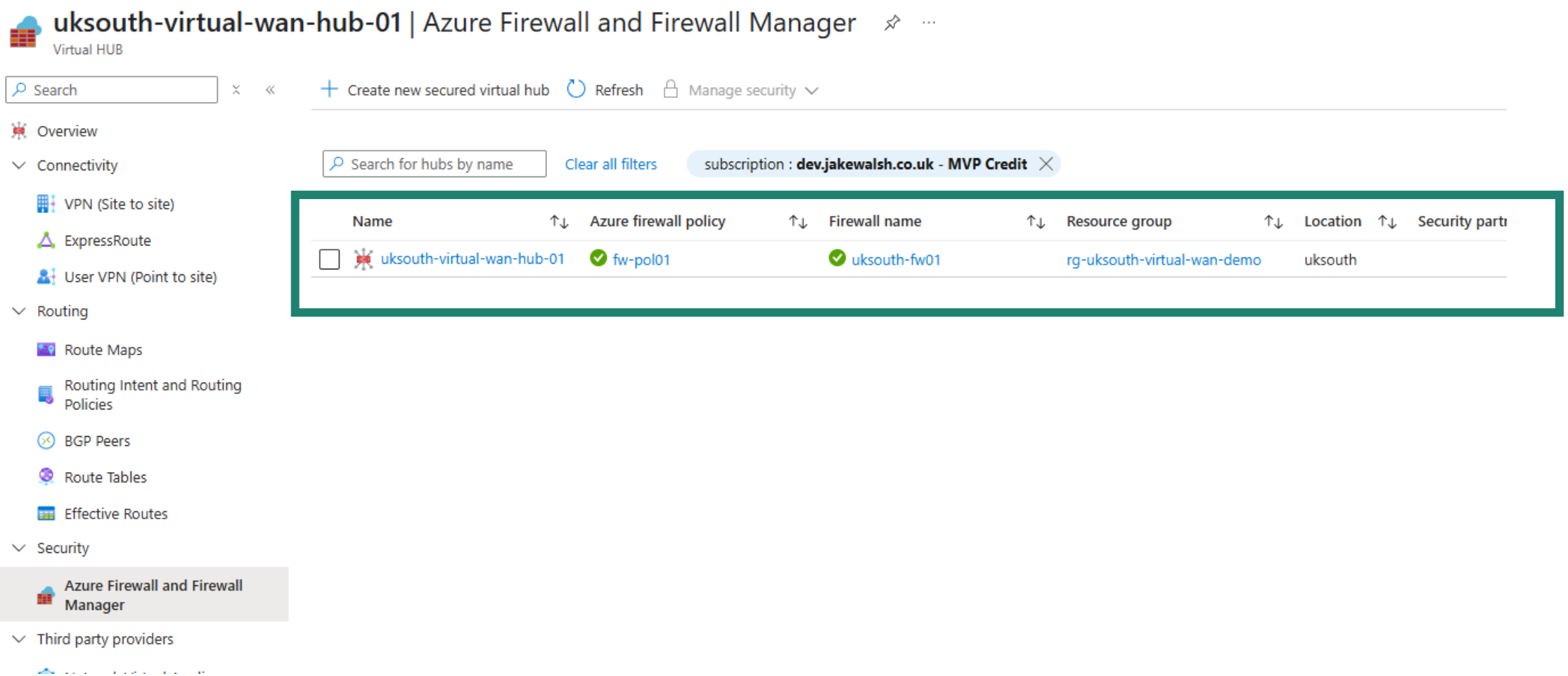
Virtual WAN Regional Hub Status and Hub Capacities (Gbps)

Geographical Hub Location Map displays the Virtual WAN hubs that are deployed in various Azure regsions. **Virtual WAN Hubs Status** is indicated by Green or Red color - Gr
that one or more of the gateways are in a failed state. **Virtual WAN Hub Capacity** is the total capapcity in Gbps of each hub displayed below the map. The hub capapcity is deri
by # of gateway scale units * bandwidth of each scale unit in Gbps)

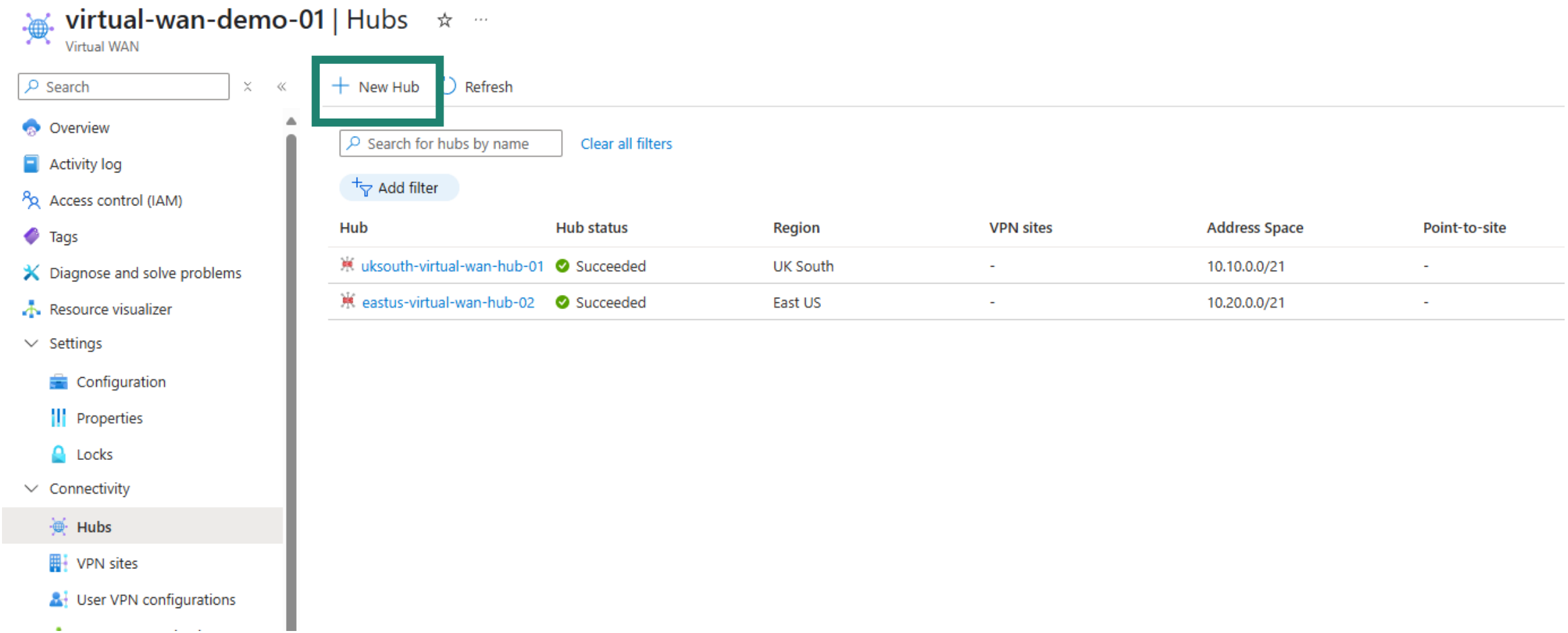


Centralised Control – A centralised service that brings core networking together, removing the need to configure and manage multiple separate resources.




uksouth-virtual-wan-hub-01 | Azure Firewall and Firewall Manager
Virtual HUB
Search
Create new secured virtual hub
Refresh
Manage security
Overview
Connectivity
VPN (Site to site)
ExpressRoute
User VPN (Point to site)
Routing
Route Maps
Routing Intent and Routing Policies
BGP Peers
Route Tables
Effective Routes
Security
Azure Firewall and Firewall Manager
Third party providers
Search for hubs by name
Clear all filters
subscription : dev.jakewalsh.co.uk - MVP Credit
Name
Azure firewall policy
Firewall name
Resource group
Location
Security parti
uksouth-virtual-wan-hub-01
fw-pol01
uksouth-fw01
rg-uksouth-virtual-wan-demo
uksouth

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

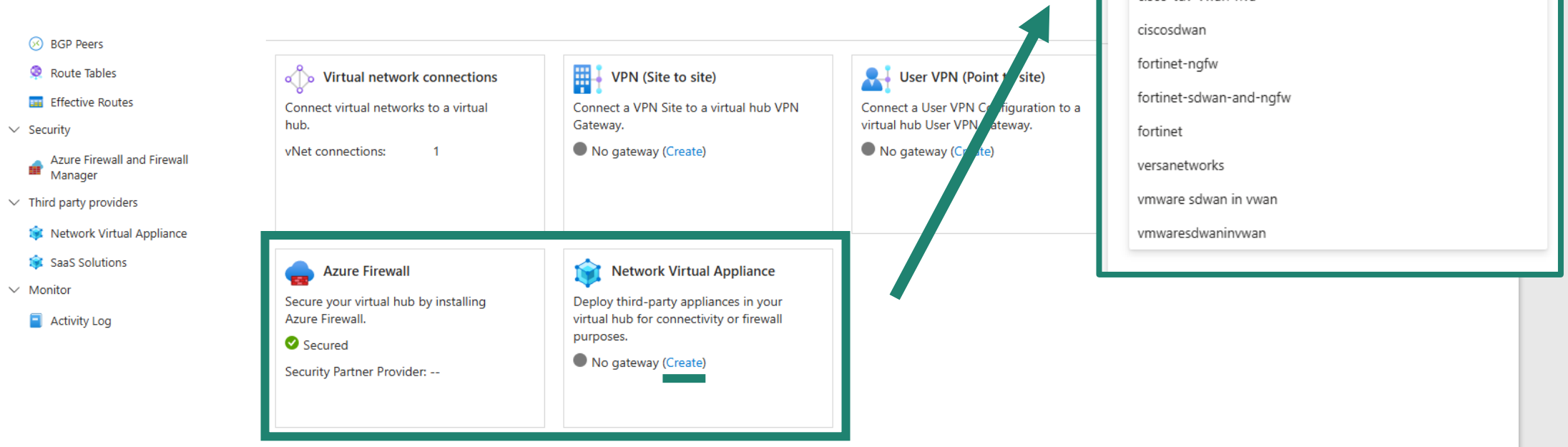


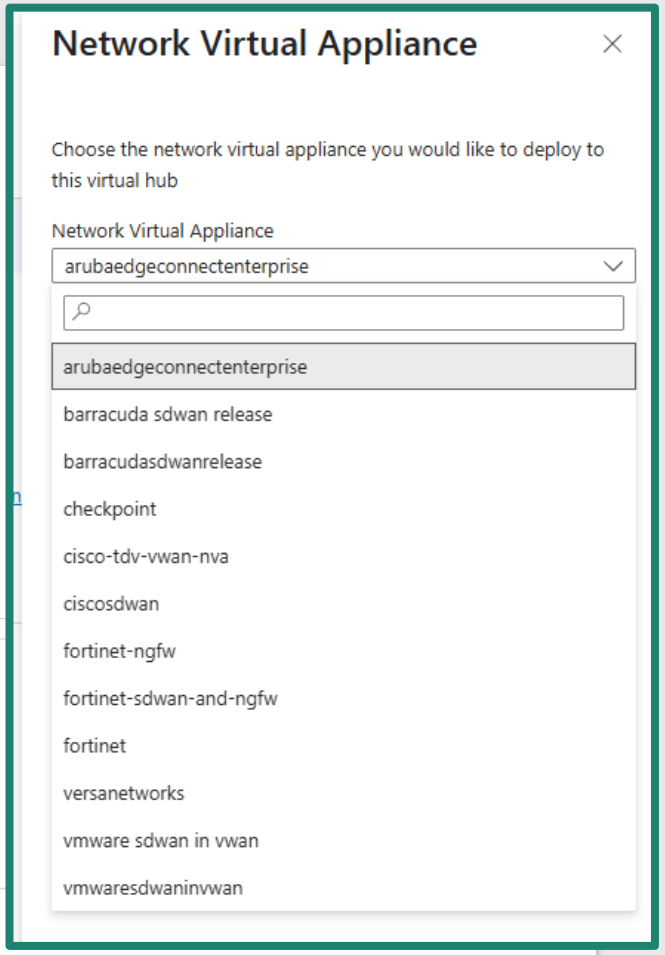
Security Options

- There are numerous security aspects within Azure Virtual WAN – I'll cover a few key aspects today (there is **far** too much to cover on security in just this session!):
  - Azure Firewall, NVA, SaaS Options
  - Monitoring
  - Administration
  - Azure Security Baseline for Virtual WAN

Azure Firewall, SaaS, and NVA Options

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





SAAS Offering: https://learn.microsoft.com/en-us/azure/virtual-wan/how-to-palo-alto-cloud-ngfw

Azure Firewall and NVA Options

- Pre-defined and pre-tested selection of infrastructure choices (NVA Infrastructure Units)
- Built-in availability and resiliency
- No-hassle provisioning and boot-strapping
- Simplified routing
- Integrated support
- Optional platform-provided lifecycle management
- Integrated with platform features

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

Azure Firewall and NVA Options

The following SD-WAN connectivity Network Virtual Appliances can be deployed in the Virtual WAN hub.

Expand tab

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

Partners	Virtual WAN NVA Vendor	Configuration/How-to/Deployment guide	Dedicated support model
Check Point CloudGuard Network Security for Azure Virtual WAN	checkpoint	Check Point Network Security for Virtual WAN deployment guide	No
Fortinet Next-Generation Firewall (NGFW)	fortinet-ngfw	Fortinet NGFW deployment guide. Fortinet NGFW supports up to 80 scale units and isn't recommended to be used for SD-WAN tunnel termination. For Fortigate SD-WAN tunnel termination, see Fortinet SD-WAN and NGFW documentation.	No
Cisco Secure Firewall Threat Defense for Azure Virtual WAN	cisco-tdv-vwan-nva	Cisco Secure Firewall Threat Defense for Azure Virtual WAN for Virtual WAN deployment guide	No

The following dual-role SD-WAN connectivity and security (Next-Generation Firewall) Network Virtual Appliances can be deployed in the Virtual WAN hub. These Virtual Appliances can be used to inspect all North-South, East-West, and Internet-bound traffic.

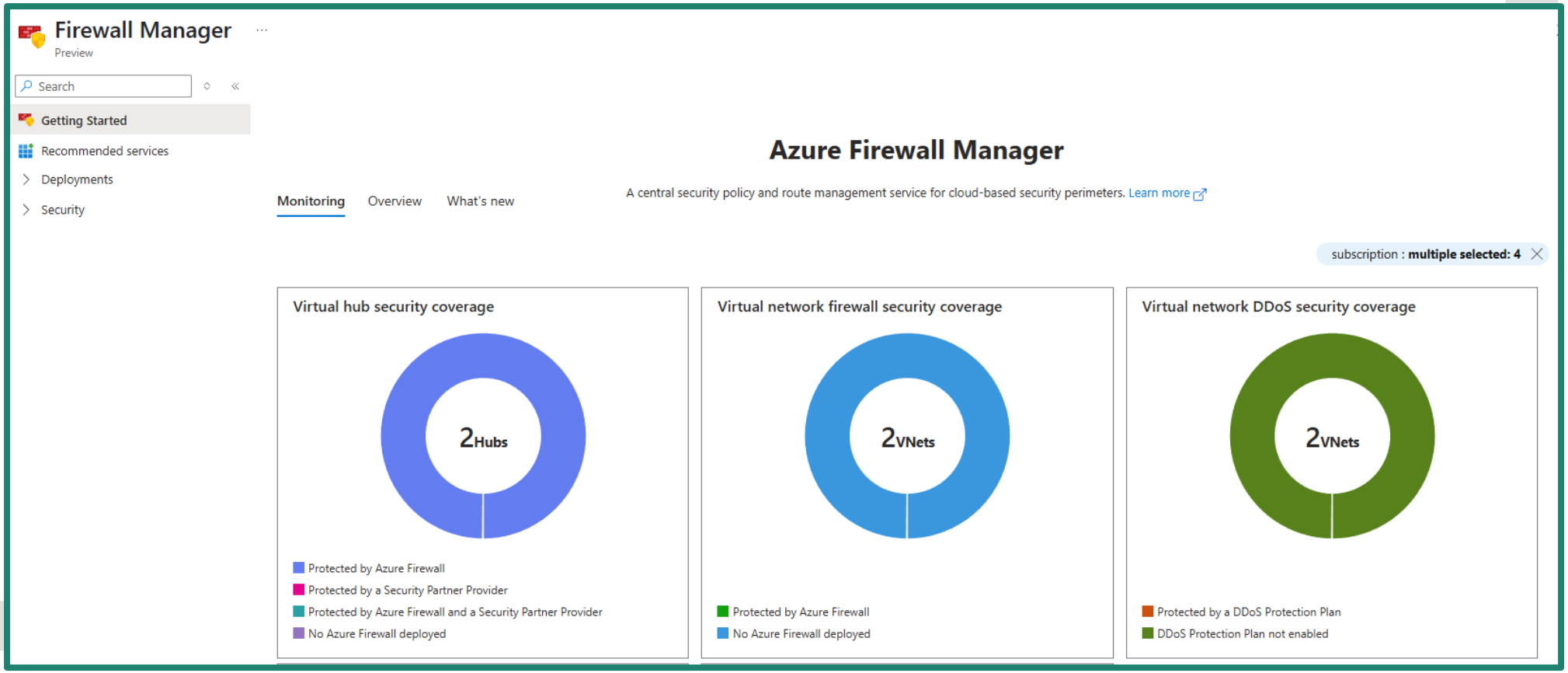
Expand table

Partners	Virtual WAN NVA Vendor	Configuration/How-to/Deployment guide	Dedicated support model
Fortinet Next-Generation Firewall (NGFW)	fortinet-sdwan-and-ngfw	Fortinet SD-WAN and NGFW NVA deployment guide. Fortinet SD-WAN and NGFW NVA support up to 20 scale units and supports both SD-WAN tunnel termination and Next-Generation Firewall capabilities.	No

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

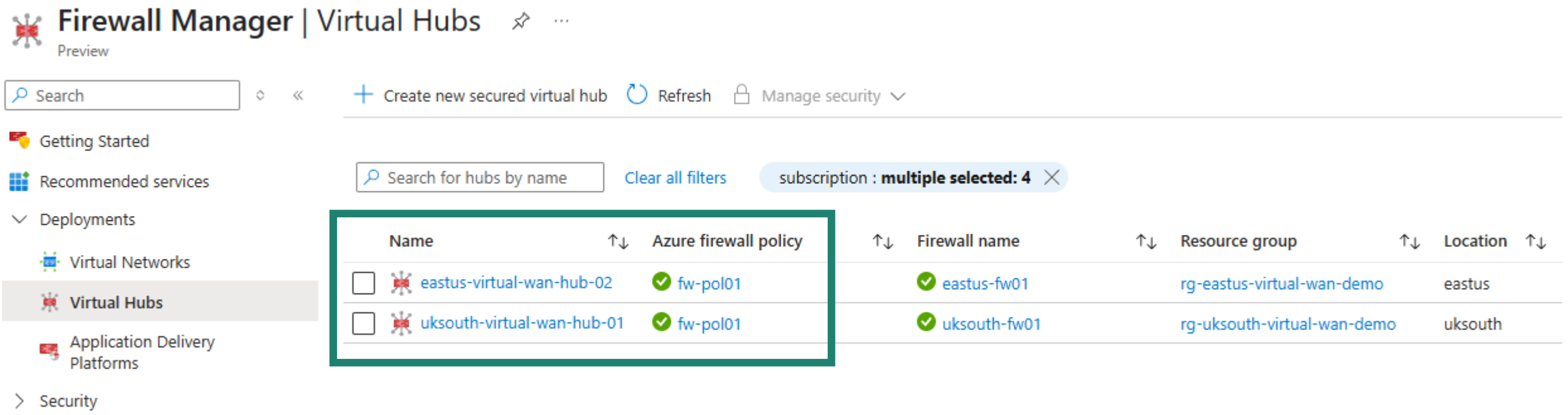
Azure Firewall!

- Azure Firewall provides an Azure Native Firewall option that can be controlled and Managed using Azure Firewall Manager



Azure Firewall

- Central Hub Management and Policy control:

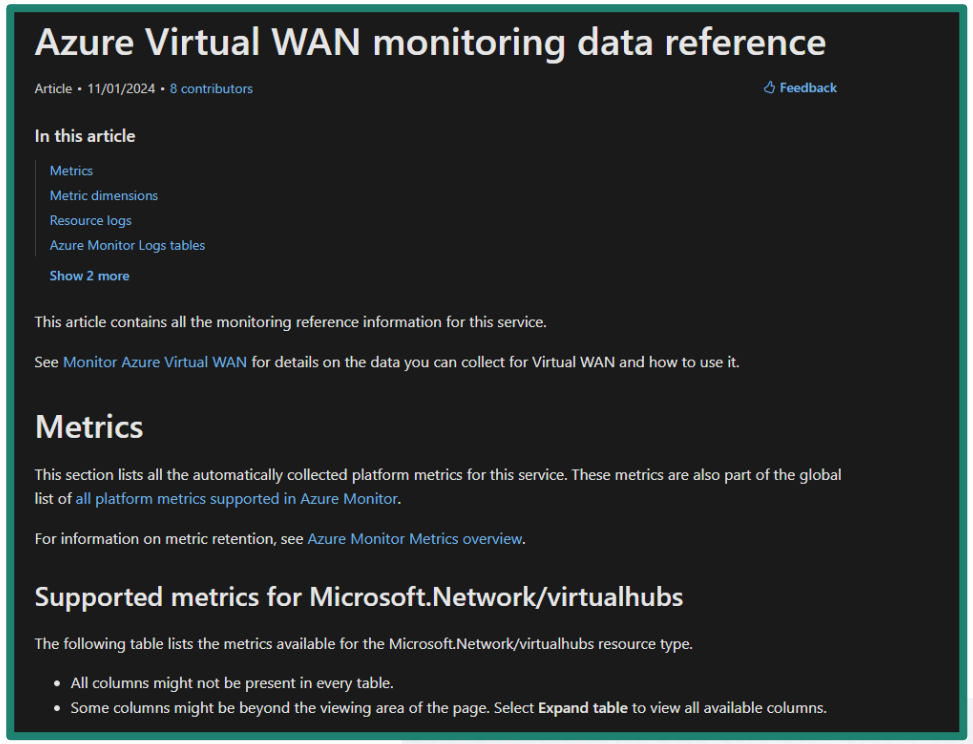


https://learn.microsoft.com/en-us/azure/virtual-wan/howto-firewall

Monitoring – the importance of Metrics!

- Like many Azure Services – Virtual WAN has a huge range of Metrics you can monitor.

- The Azure Virtual WAN monitoring data reference is the guide to these metrics.



Azure Virtual WAN monitoring data reference

Article • 11/01/2024 • 8 contributors

Feedback

In this article

Metrics
Metric dimensions
Resource logs
Azure Monitor Logs tables

Show 2 more

This article contains all the monitoring reference information for this service.

See Monitor Azure Virtual WAN for details on the data you can collect for Virtual WAN and how to use it.

Metrics

This section lists all the automatically collected platform metrics for this service. These metrics are also part of the global list of all platform metrics supported in Azure Monitor.

For information on metric retention, see Azure Monitor Metrics overview.

Supported metrics for Microsoft.Network/virtualhubs

The following table lists the metrics available for the Microsoft.Network/virtualhubs resource type.

- All columns might not be present in every table.
- Some columns might be beyond the viewing area of the page. Select **Expand table** to view all available columns.

Category: Traffic

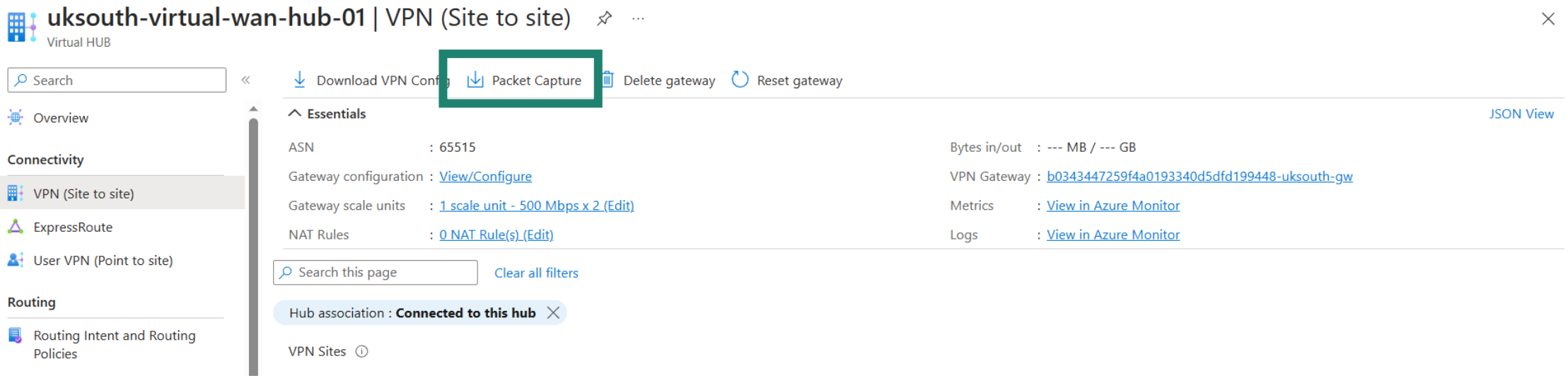
Expand table

Metric	Name in REST API	Unit	Aggregation	Dimensions	Time Grains	DS Export
Gateway S2S Bandwidth Site-to-site bandwidth of a gateway in bytes per second	`AverageBandwidth`	BytesPerSecond	Average	`Instance`	PT5M, PT15M, PT30M, PT1H, PT6H, PT12H, P1D	Yes
Gateway Inbound Flows Number of 5-tuple flows entering into a VPN gateway	`InboundFlowsCount`	Count	Maximum, Minimum	`Instance`	PT5M, PT15M, PT30M, PT1H, PT6H, PT12H, P1D	Yes
Gateway Outbound Flows Number of 5-tuple flows exiting a VPN gateway	`OutboundFlowsCount`	Count	Maximum, Minimum	`Instance`	PT5M, PT15M, PT30M, PT1H, PT6H, PT12H, P1D	Yes
Tunnel Bandwidth Average bandwidth of a tunnel in bytes per second	`TunnelAverageBandwidth`	BytesPerSecond	Average	`ConnectionName`, `RemoteIP`, `Instance`	PT5M, PT15M, PT30M, PT1H, PT6H, PT12H, P1D	Yes
Tunnel Egress Bytes	`TunnelEgressBytes`	Bytes	Total (Sum)	`ConnectionName`, `RemoteIP`, `Instance`	PT5M, PT15M, PT30M,	Yes

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

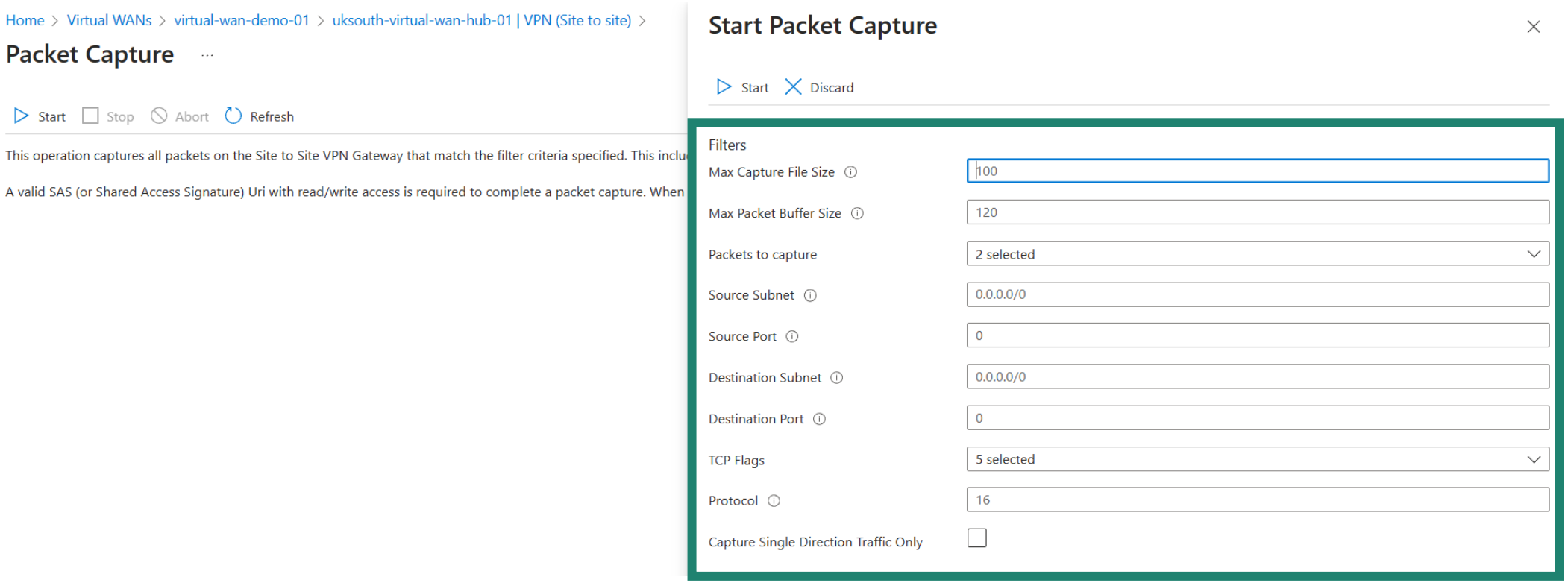
Packet Capture – available for S2S VPNs

- 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



https://learn.microsoft.com/en-us/azure/virtual-wan/packet-capture-site-to-site-portal

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 or systems.
- Management via ARM / Azure Portal
- DevOps Integration – Networking Configuration as Code

Azure Security Baseline – a worthwhile read!

Azure security baseline for Virtual WAN

Article • 02/25/2025 • 1 contributor

Feedback

In this article

Security profile
Identity management
Data protection
Asset management
Show 2 more

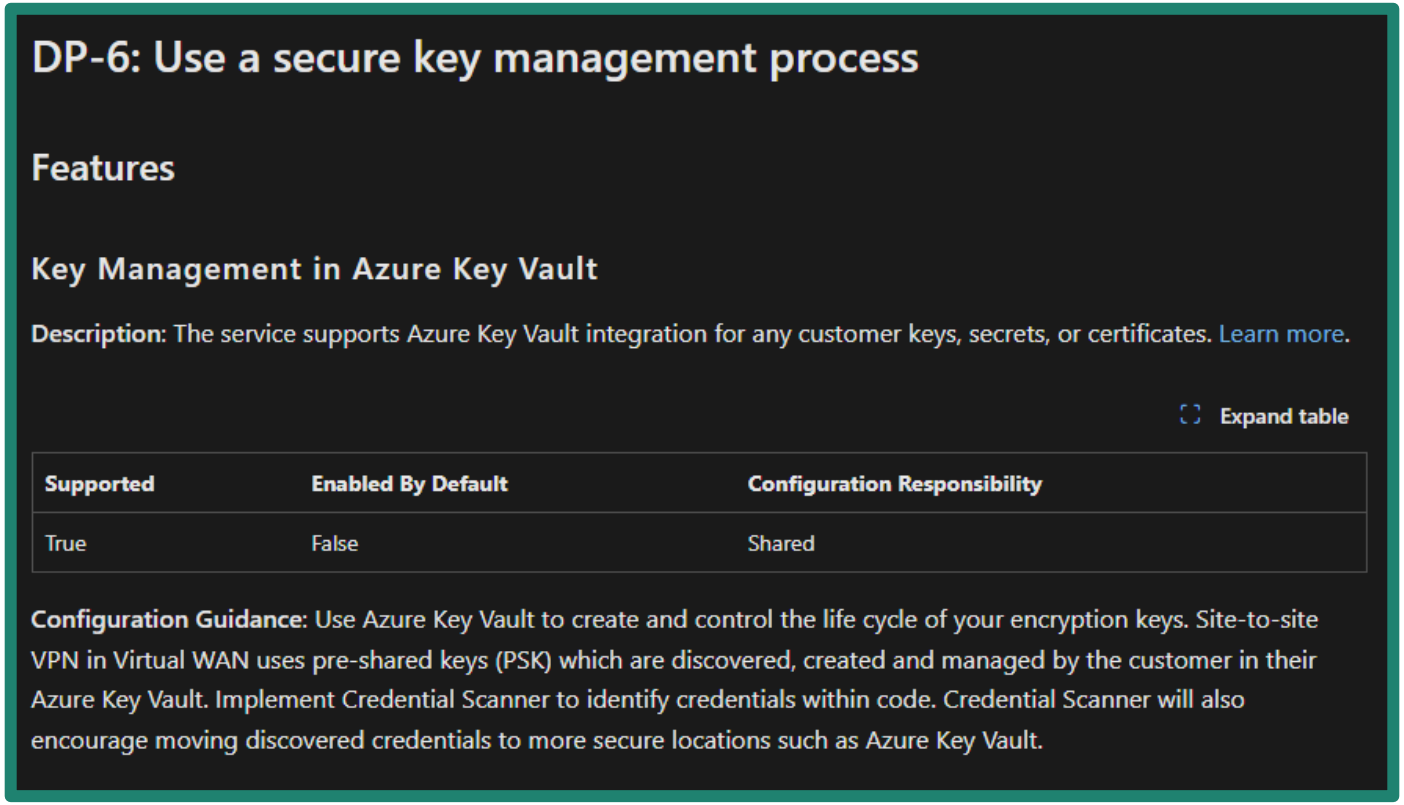
This security baseline applies guidance from the Microsoft cloud security benchmark version 1.0 to Virtual WAN. The Microsoft cloud security benchmark provides recommendations on how you can secure your cloud solutions on Azure. The content is grouped by the security controls defined by the Microsoft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

Azure Security Baseline – a worthwhile read!



DP-6: Use a secure key management process

Features

Key Management in Azure Key Vault

Description: The service supports Azure Key Vault integration for any customer keys, secrets, or certificates. Learn more.

Expand table

Supported	Enabled By Default	Configuration Responsibility
True	False	Shared

Configuration Guidance: Use Azure Key Vault to create and control the life cycle of your encryption keys. Site-to-site VPN in Virtual WAN uses pre-shared keys (PSK) which are discovered, created and managed by the customer in their Azure Key Vault. Implement Credential Scanner to identify credentials within code. Credential Scanner will also encourage moving discovered credentials to more secure locations such as Azure Key Vault.

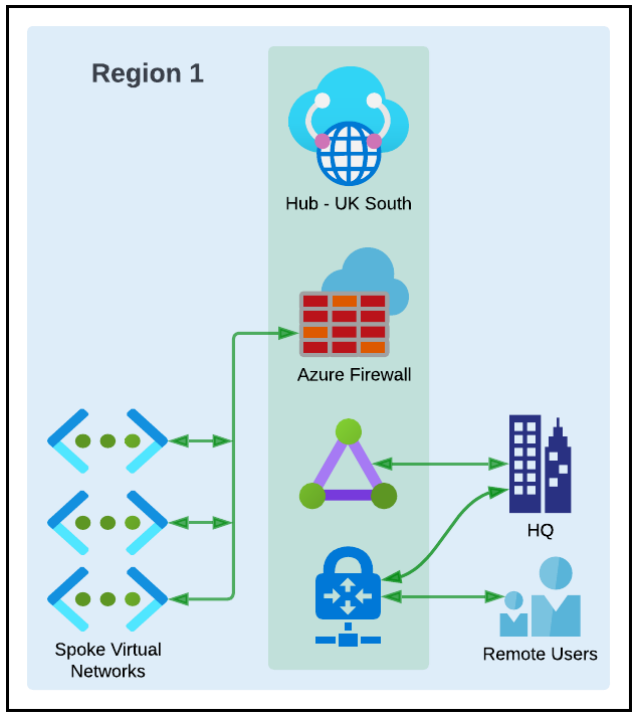
https://learn.microsoft.com/en-us/security/benchmark/azure/baselines/virtual-wan-security-baseline

Expansion Options

Expansion is easy with Virtual WAN:

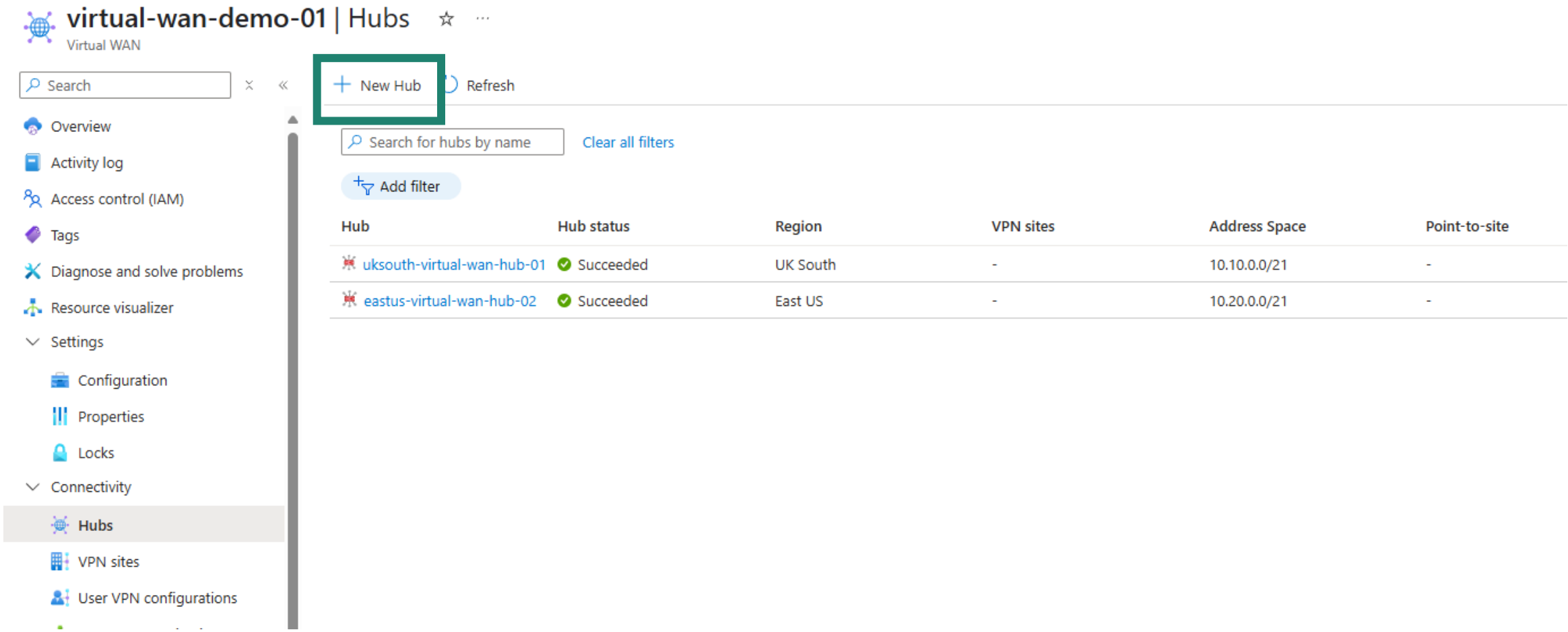
- Our start – Single Virtual WAN hub, ExpressRoute and a VPN Gateway for IPsec or P2S Users.
- Spoke Virtual Networks peered into Virtual WAN hub.
- All Traffic via Single Azure Firewall instance.

How do we expand to other Regions?

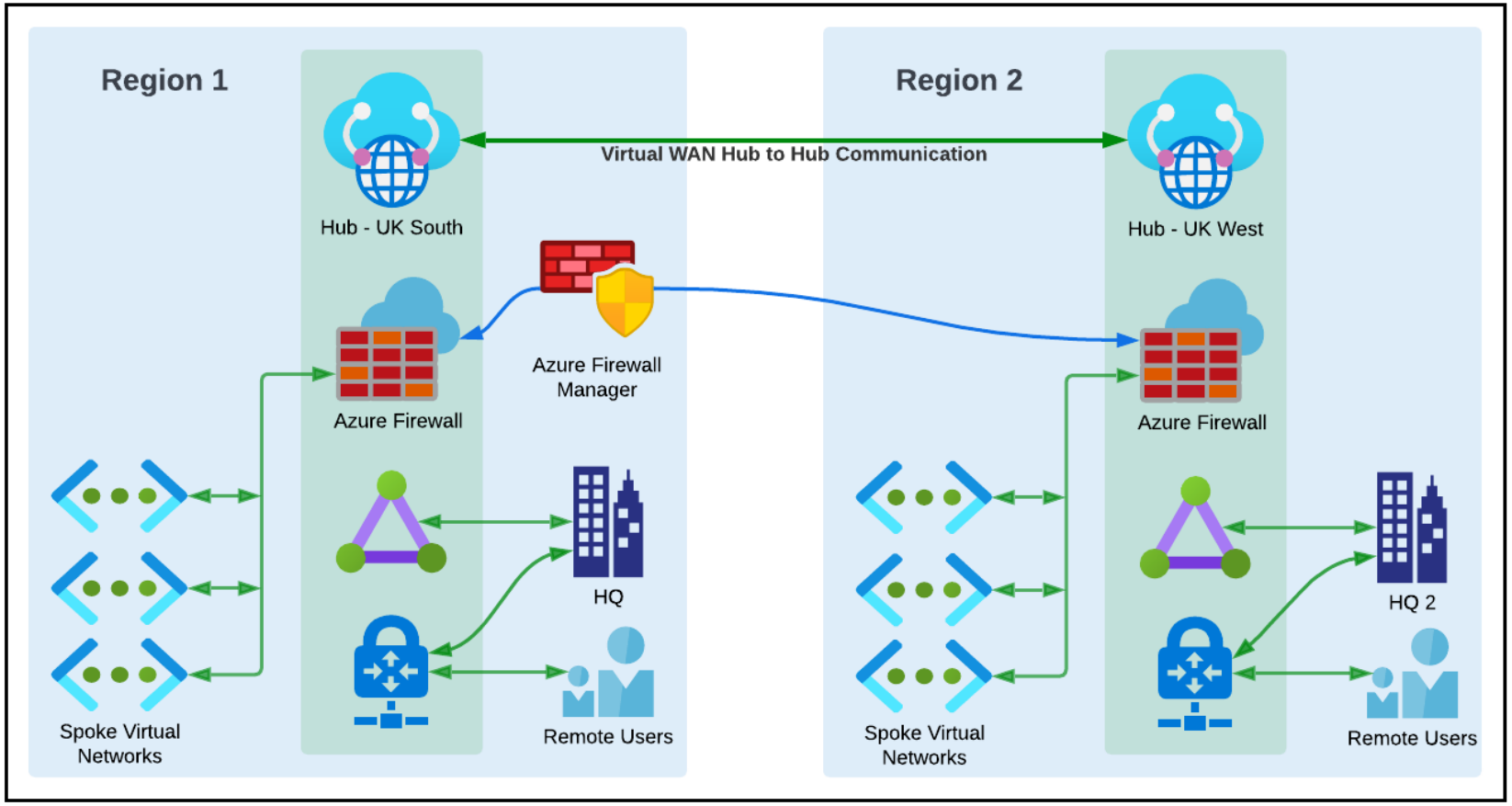


Expansion Options

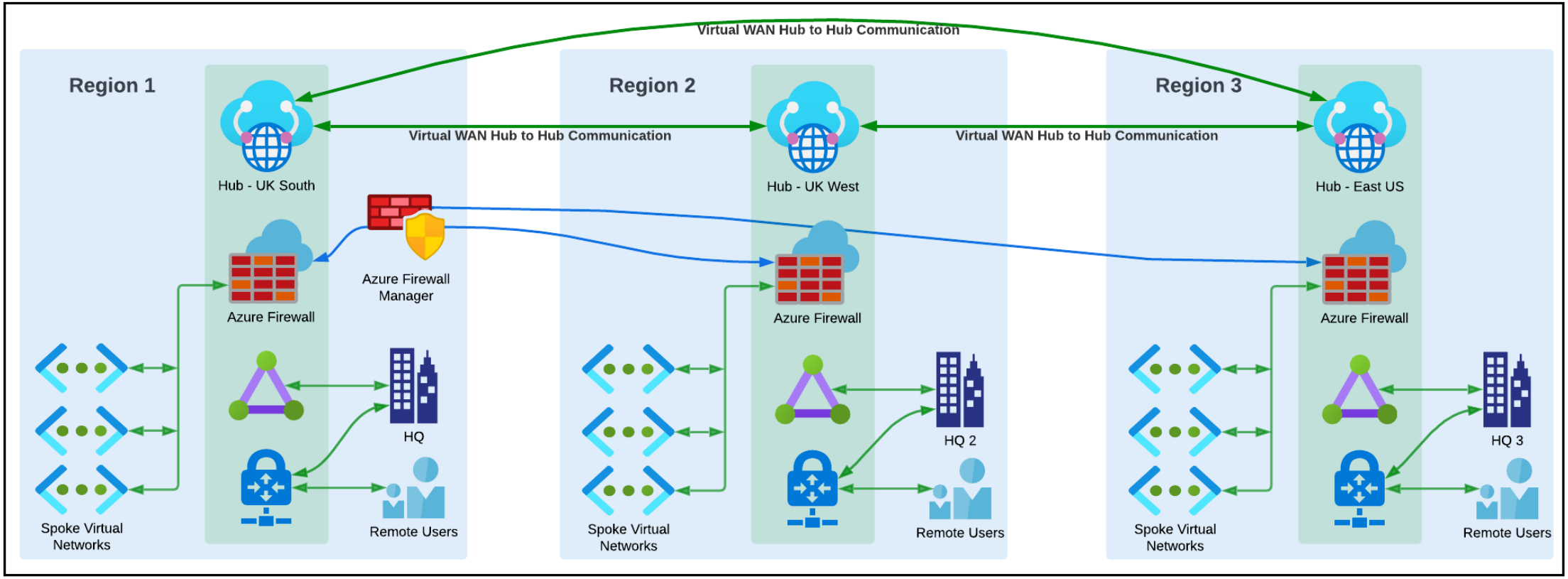
- ✓ Regional Expansion is simple – and done by adding Hubs
- ✓ Hubs are fully-meshed by default, enabling communication



Expansion Options... +1 Region



Expansion Options... +2 Regions



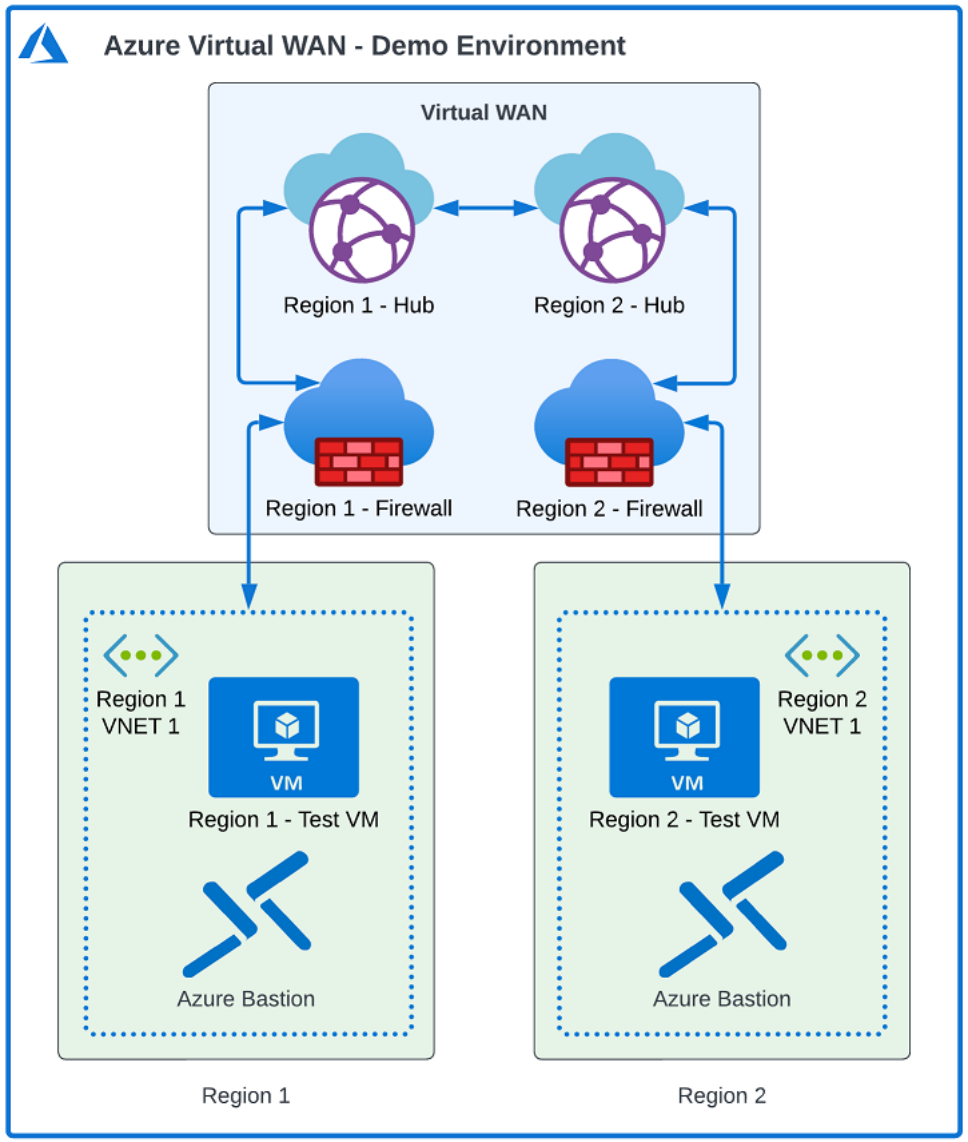
Expansion Options & Benefits

- ✓ Regional Expansion – **add a Hub, and then other services.**
- ✓ Firewalling options – Scale up to Premium
- ✓ Hub Routing Intent – Cross Region & Internet traffic all via NVAs/AzFWs/SaaS
- ✓ 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 freely (via Firewalling if required).
- ✓ Automated Route Table Management & Provisioning ★
- ✓ Single Control of Cloud Networking via Virtual WAN
- ✓ Scale in routing units up to 50Gbps (VNet to VNet) 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


Azure Virtual WAN - Demo Environment
Virtual WAN
Region 1 - Hub
Region 2 - Hub
Region 1 - Firewall
Region 2 - Firewall
Region 1
VNET 1
VM
Region 1 - Test VM
Azure Bastion
Region 2
VNET 1
VM
Region 2 - Test VM
Azure Bastion
Region 1
Region 2

Demo Lab – Costs

Service category	Service type	Region	Description	Estimated monthly cost
Networking	Virtual WAN	East US	730 Deployment hours, 0 Routing infrastructure units, 10 GB of data processed, Azure firewall integrated (standard tier) with 0 GB of data processed, Site to site VPN connection for 0 scale units, 0 deployed for 730 Hours, User VPN connection for 0 scale units for 730 Hours and 0 scale units for 730 Hours, ExpressRoute connections for 0 scale units, 0 deployed for 730 Hours	$912.70
Networking	Virtual WAN	UK South	730 Deployment hours, 0 Routing infrastructure units, 10 GB of data processed, Azure firewall integrated (standard tier) with 0 GB of data processed, Site to site VPN connection for 0 scale units, 0 deployed for 730 Hours, User VPN connection for 0 scale units for 730 Hours and 0 scale units for 730 Hours, ExpressRoute connections for 0 scale units, 0 deployed for 730 Hours	$912.70
Networking	Azure Bastion	East US	Basic Tier, 730 Hours, 5 GB Outbound Data Transfer	$138.70
Networking	Azure Bastion	UK South	Basic Tier, 730 Hours, 5 GB Outbound Data Transfer	$138.70
Compute	Virtual Machines	East US	1 B4ms (4 Cores, 16 GB RAM) x 730 Hours (Pay as you go), Windows (Licence included), OS Only; 1 managed disk – S10; Inter Region transfer type, 5 GB outbound data transfer from East US to East Asia	$138.75
Compute	Virtual Machines	UK South	1 B4ms (4 Cores, 16 GB RAM) x 730 Hours (Pay as you go), Windows (Licence included), OS Only; 1 managed disk – S10; Inter Region transfer type, 5 GB outbound data transfer from UK South to East Asia	$156.13
Networking	IP Addresses	East US	Standard (ARM), 20 Static IP Addresses X 730 Hours, 0 Public IP Prefixes X 730 Hours	$73.00
			Total	**$2,470.68**

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

Demo / Lab Environment – Bicep

Code Blame 313 lines (274 loc) · 11.1 KB

```bicep
@minLength(4)
@maxLength(80)
param vWANname string = 'vWAN'

@description('Region for the Azure Virtual WAN')
param vWANlocation string = resourceGroup().location

@description('Name of the FIRST virtual hub')
@minLength(4)
@maxLength(80)
param hub1Name string = 'Hub1'

@description('Region for the FIRST virtual hub')
param hub1Location string = resourceGroup().location

@description('Address space for the FIRST virtual hub')
param hub1AddressSpace string = '10.1.0.0/23'

@description('Address space for the first VNet (spoke1) connected to the FIRST virtual hub')
param hub1Spoke1AddressSpace string = '10.1.2.0/24'

@description('Address space for the second VNet (spoke2) connected to the FIRST virtual hub')
param hub1Spoke2AddressSpace string = '10.1.4.0/24'

@description('Name of the SECOND virtual hub')
@minLength(4)
@maxLength(80)
param hub2Name string = 'Hub2'

```

azure-quickstart-templates/quickstarts/microsoft.network/virtual-wan-routing-intent at master · Azure/azure-quickstart-templates · GitHub

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

Q & A

AZURE

BOOTCAMP SWITZERLAND

AZURE

BOOTCAMP SWITZERLAND

Microsoft® Most Valuable Professional

Thank You!

Building a Cloud Centric Network with Azure Virtual WAN

Jake Walsh

Please note – the views/opinions in this presentation are entirely my own.
If in any doubt, please check latest documentation and MS Links for updated info!

AZURE
BOOTCAMP
SWITZERLAND
glueck kanja
scopewyse
axpo
swisscom
FUJITSU
Microsoft
itnetx
techtask
die Mobiliar
GRABX
isolutions
Ad.
AdVision.
#We live IT
digicomp