

Helping you create a  
digitally secure future.

## PUBLIC CLOUD 202: AZURE VWAN INTERNET INBOUND

**John McDonough / Srija Reddy Allam / Robert Reris / Jeff Kopko**  
Fortinet Cloud CSE

# Azure Virtual WAN

Azure Networking and Routing

# Azure Routing

Other than Default Routing

User Defined

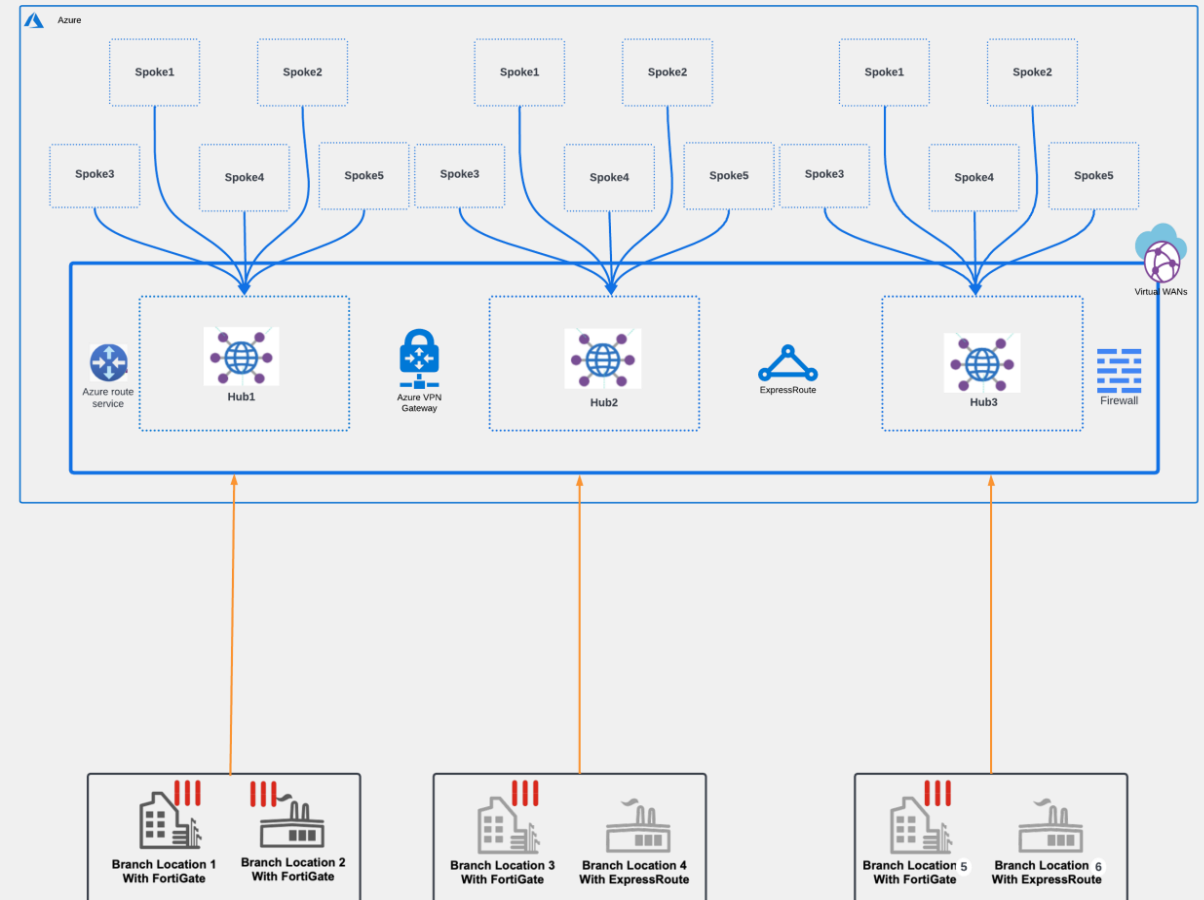
Azure Route Server

Azure Virtual WAN



# What is Azure Virtual WAN

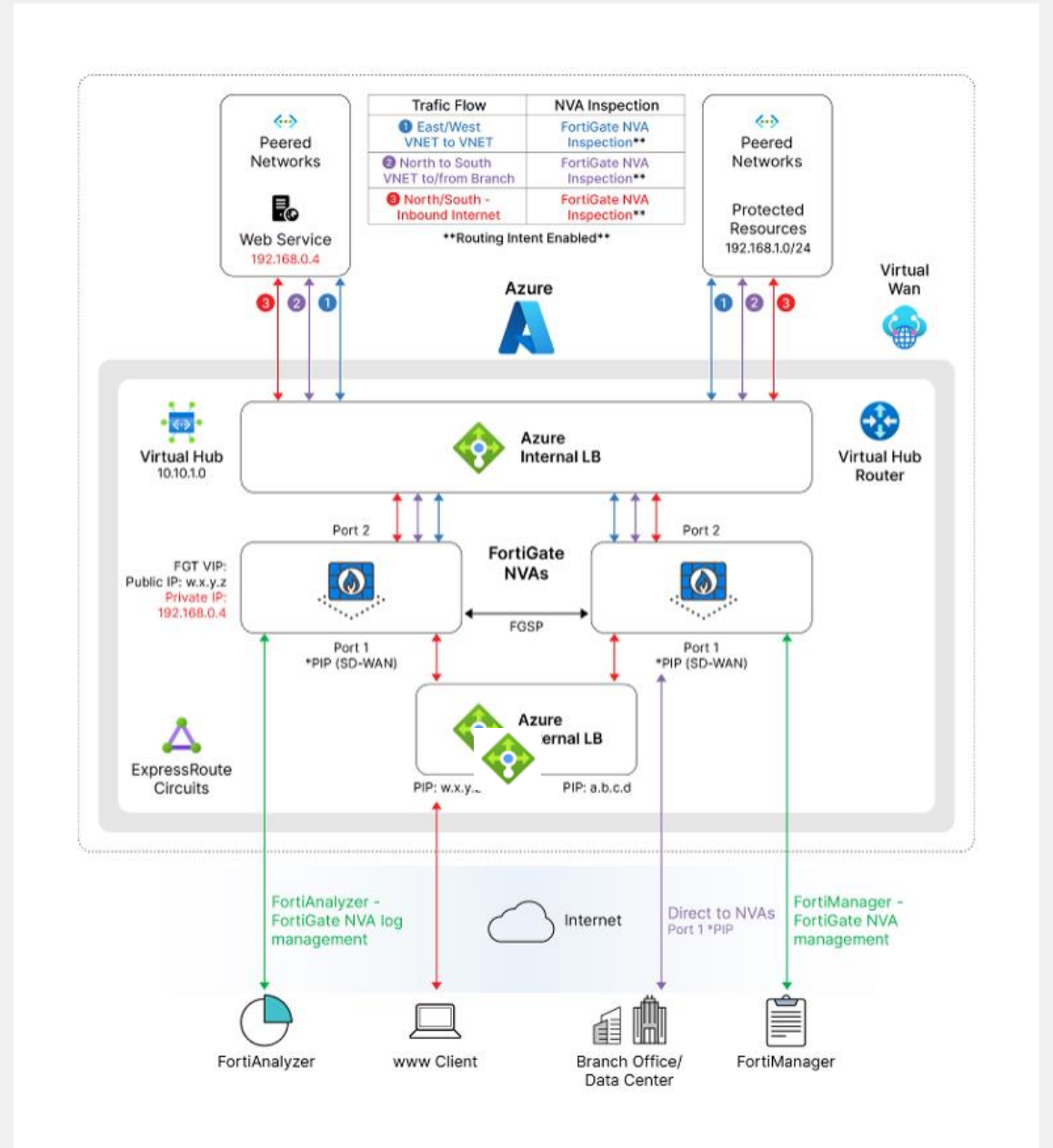
- Simplifies management hub and spoke deployments
- Large-scale branch connectivity with VPN and Express Route
- Unified network and policy management
- Optimized routing with Microsoft global network
- Advanced Routing – BGP and Routing Intent
- Integrates with Fortinet FortiGate solutions providing SD-WAN and NGFW services



# FortiGate Integration with Azure VWAN

The industry's first fully Integrated network virtual appliance providing **Secure SDWAN AND Next Generation Firewall Services**

- Simple and structured deployment model
  - Deployed via Azure portal – Managed service
  - SDWAN and/or NGFW deployment options
- High Availability and Resiliency
  - Active-Active – up to 5 FortiGates (NGFW)
- Performance and Scale
- Dynamic Routing Capabilities
- Single management interface – FortiManager – Appliance / VM
- Centralized logging – FortiAnalyzer – Appliance / VM
- Flexible licensing options
  - BYOL / FortiFlex
  - PAYG – New in Q2 2024





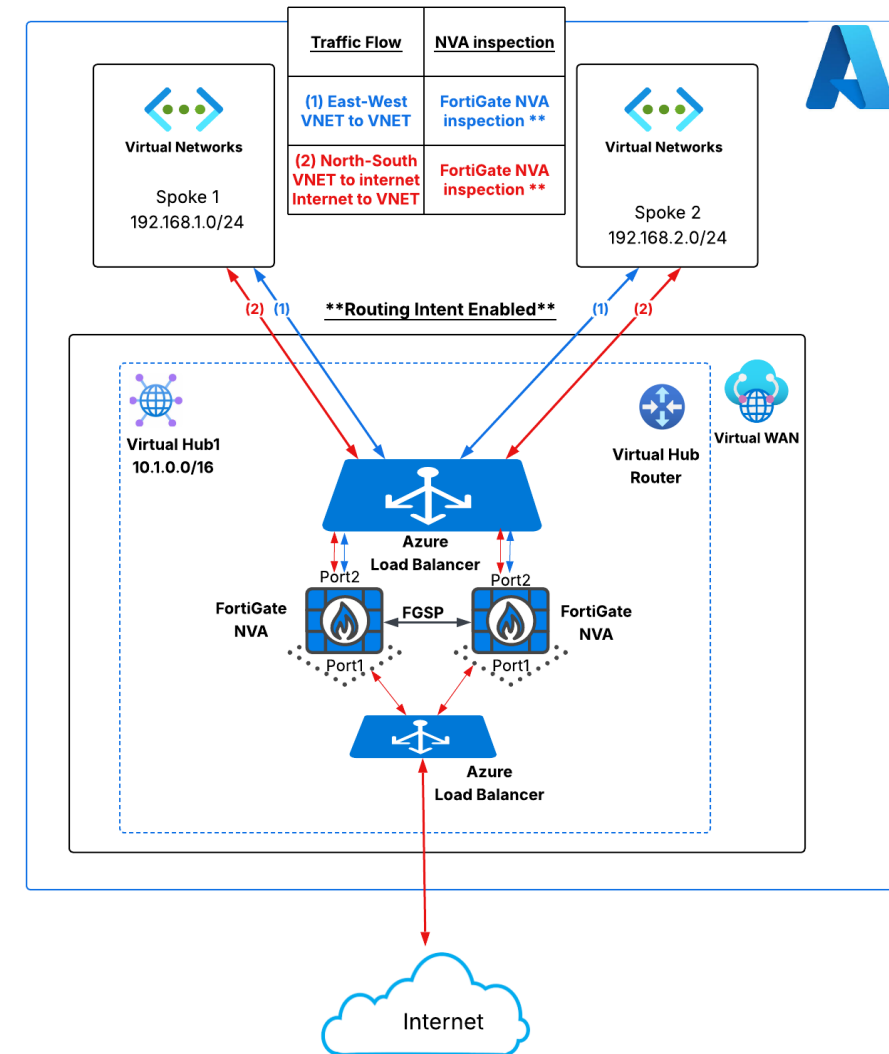
# Azure Marketplace Plan

- NGFW
- SD-WAN & NGFW

# NGFW Only - Option

- Inspects East-West and Internet bound traffic
  - Network inspection across VNETs connected to the Virtual WAN
  - Internet bound traffic inspection
- High Availability and resiliency
  - Active-Active - supports up to 5 VMs and 40 Gbps
- Performance and Scale
- Dynamic Routing Capabilities
- Single management interface – FortiManager – Appliance / VM
- Centralized logging – FortiAnalyzer – Appliance / VM
- Flexible licensing options
  - BYOL / FortiFlex
  - PAYG

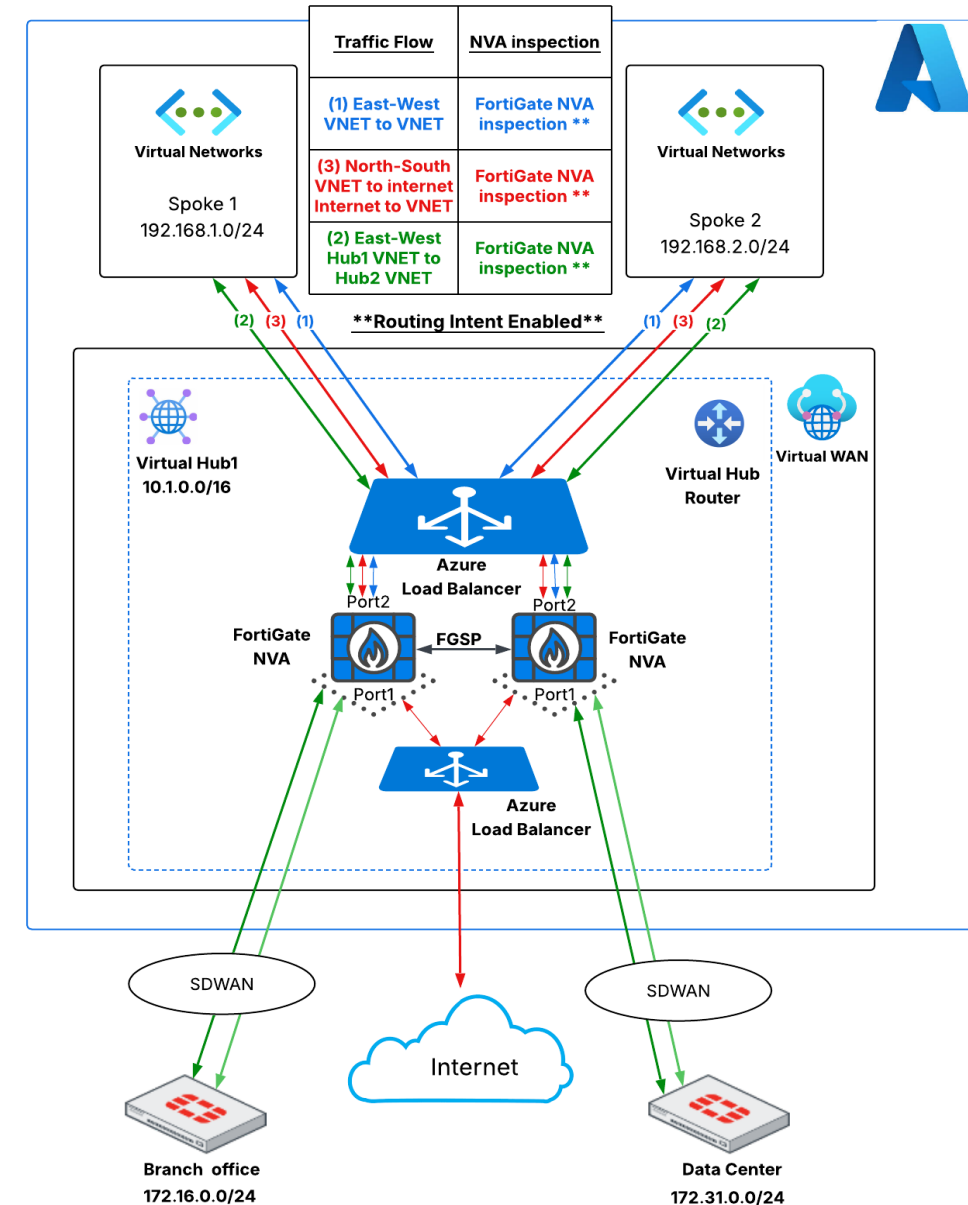
## Azure vWAN-Single Hub



# SDWAN & NGFW - Option

- North-South inspection for traffic destined to the Internet or the SDWAN connected networks. (See red & green traffic flows on the diagram)
- Inspection across vNETs connected to the virtual WAN (See blue traffic flow on the diagram)
- High Availability and resiliency
  - Active-Active – supports 2 VMs up to 10Gbps
- Performance and Scale
- Dynamic Routing Capabilities
- Single management interface – FortiManager – Appliance / VM
- Centralized logging – FortiAnalyzer – Appliance / VM
- Flexible licensing options
  - BYOL / FortiFlex
  - PAYG

## Azure vWAN-Single Hub





# Order Types in VWAN

# NGFW Only – Scale Units

The following table summarizes FortiGate vWAN license options:

Scale units	Bandwidth	Suggested license SKU	Security service (support included)	Instance count
2	1 Gbps	FortiGate-VM (2 CPU)	UTP Bundle	2
4	2 Gbps	FortiGate-VM (4 CPU)	UTP Bundle	2
10	5 Gbps	FortiGate-VM (8 CPU)	UTP Bundle	2
20	10 Gbps	FortiGate-VM (16 CPU)	UTP Bundle	2
40	20 Gbps	FortiGate-VM (16 CPU)	UTP Bundle	3
60	30 Gbps	FortiGate-VM (16 CPU)	UTP Bundle	4
80	40 Gbps	FortiGate-VM (16 CPU)	UTP Bundle	5



Scale units cannot change dynamically. If you want to use a different scale unit after deploying the NVAs, you must redeploy the NVAs.

# SDWAN & NGFW – Scale Units

The following table summarizes FortiGate vWAN license options:

Scale units	Bandwidth	Suggested license SKU	Security service (support included)	Instance count
2	1 Gbps	FortiGate-VM (2 CPU)	UTP Bundle	2
4	2 Gbps	FortiGate-VM (4 CPU)	UTP Bundle	2
10	5 Gbps	FortiGate-VM (8 CPU)	UTP Bundle	2
20	10 Gbps	FortiGate-VM (16 CPU)	UTP Bundle	2



Scale units cannot change dynamically. If you want to use a different scale unit after deploying the NVAs, you must redeploy the NVAs.

# Lab Overview



# 5x columns

Paragraph Text



## Overview

- Connect to Azure Environment
- Review Resources



## Deploy

- Deploy FortiGate NVAs in Azure VWAN Hub
- Deploy 2nd vWAN Hub
- Deploy Linux VMs



## Configure

- Configure FortiGates
- Configure FGSP
- Firewall Policies
- Configure VNET peering



## Route

- Configure FortiGate Static Routes
- Ensure BGP peering
- Configure Azure Routing Intent
- Configure Internet Ingress



## Verify

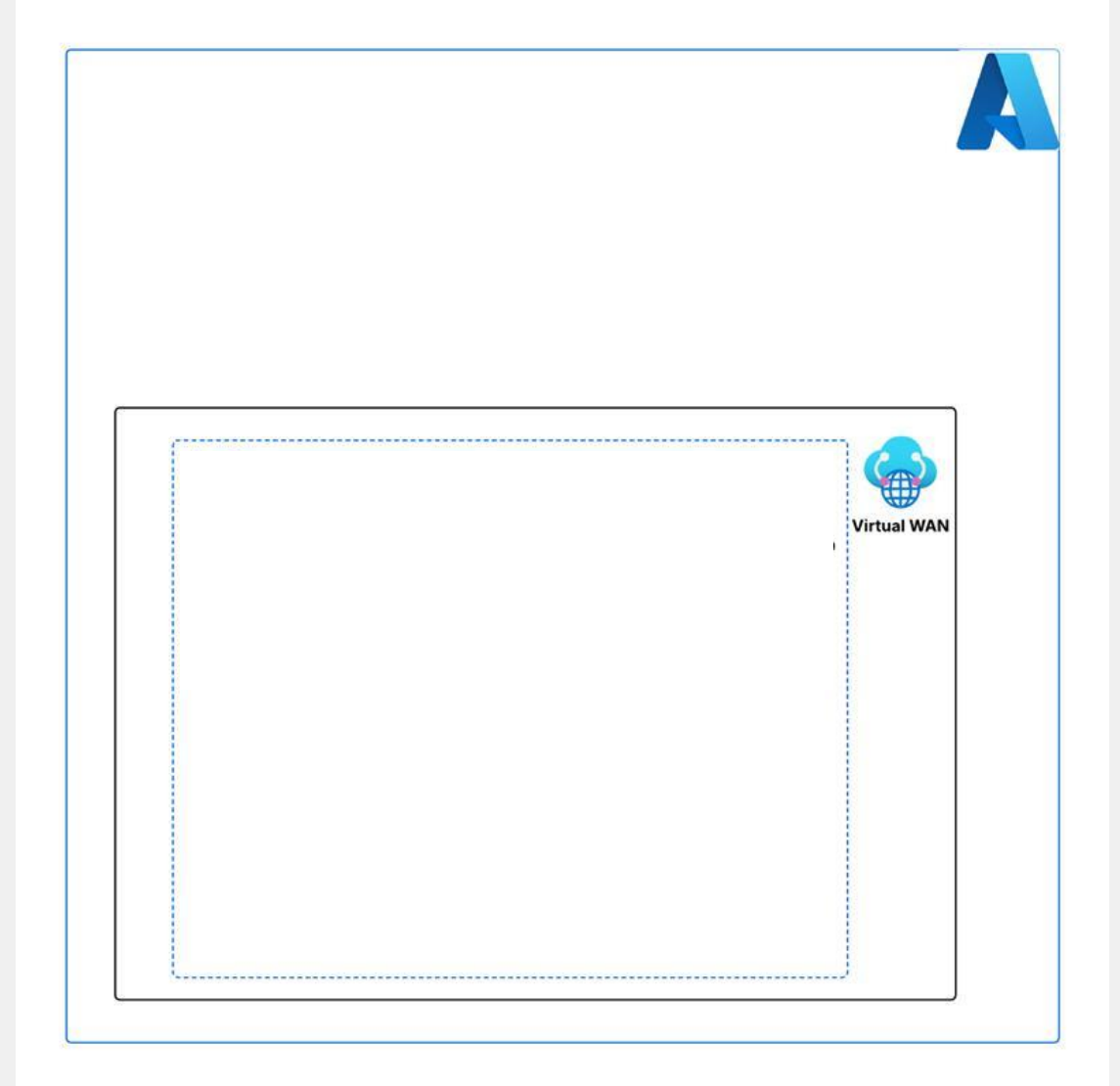
- Verify Spoke to Spoke
- Verify Spoke to Internet
- Verify Internet to Spoke
- Verify Hub to Hub



# Virtual WAN Components – Virtual WAN

- Managed Service deployed from Azure portal
- Simple deployment template
  - Name
  - Region
  - Resource Group
  - Type (connectivity options)
    - Standard
    - Basic

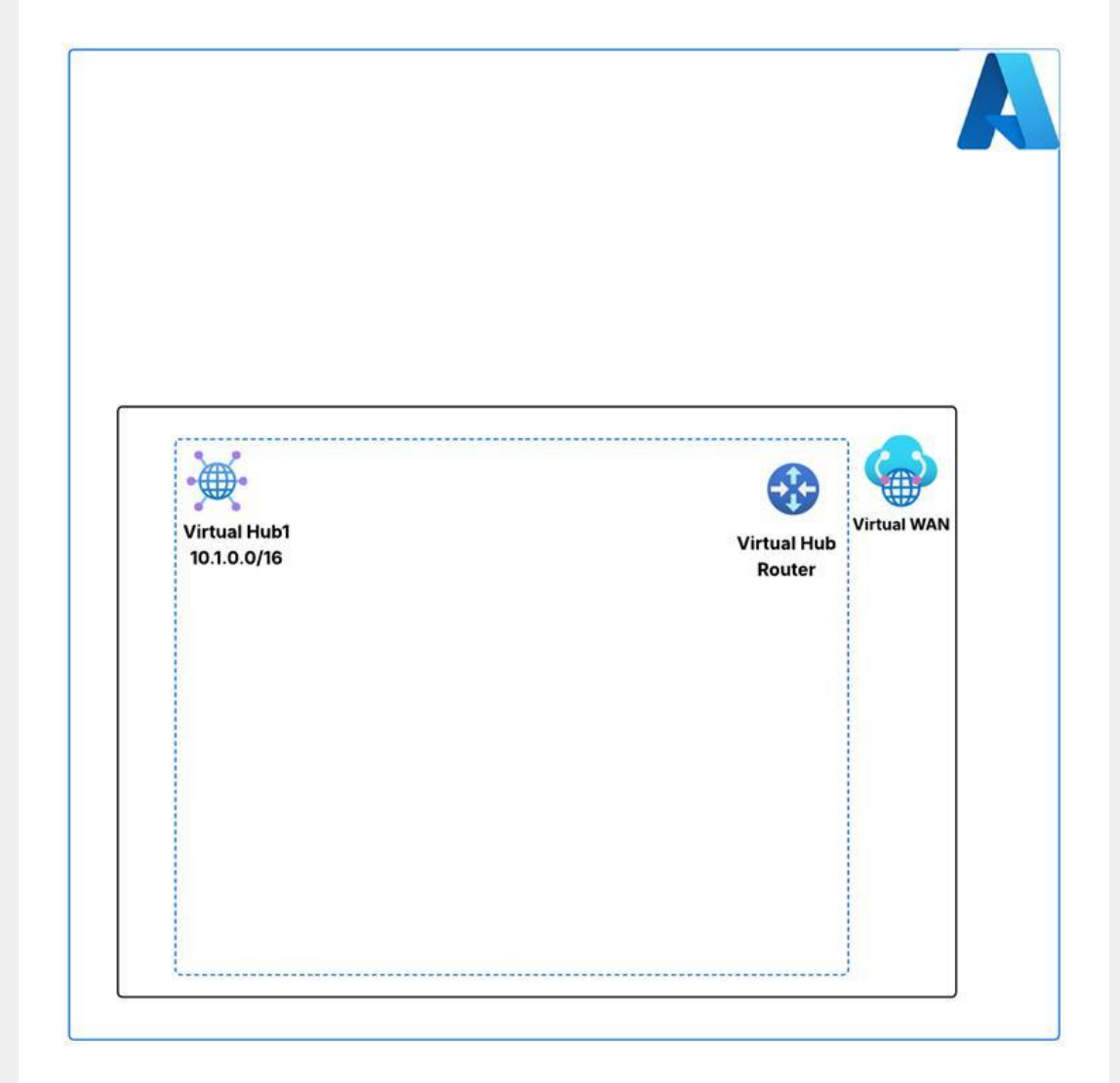
\*\*Already deployed



# Virtual WAN Components – Virtual Hub

- Managed Service deployed from Azure portal
- Simple deployment template
  - Name
  - Region
  - Resource Group
  - Address space
  - Capacity (Scale Units)
  - Routing Preference
    - AS Path
    - Express Route
    - VPN
    - Additional Services

\*\*Already deployed



# Virtual WAN Components – Virtual Networks

- VNETS deployed from Azure portal
- Comprehensive deployment template
  - Name
  - Region
  - Resource Group
  - Address space
  - Subnets
  - Additional Services
  - Virtual Machines

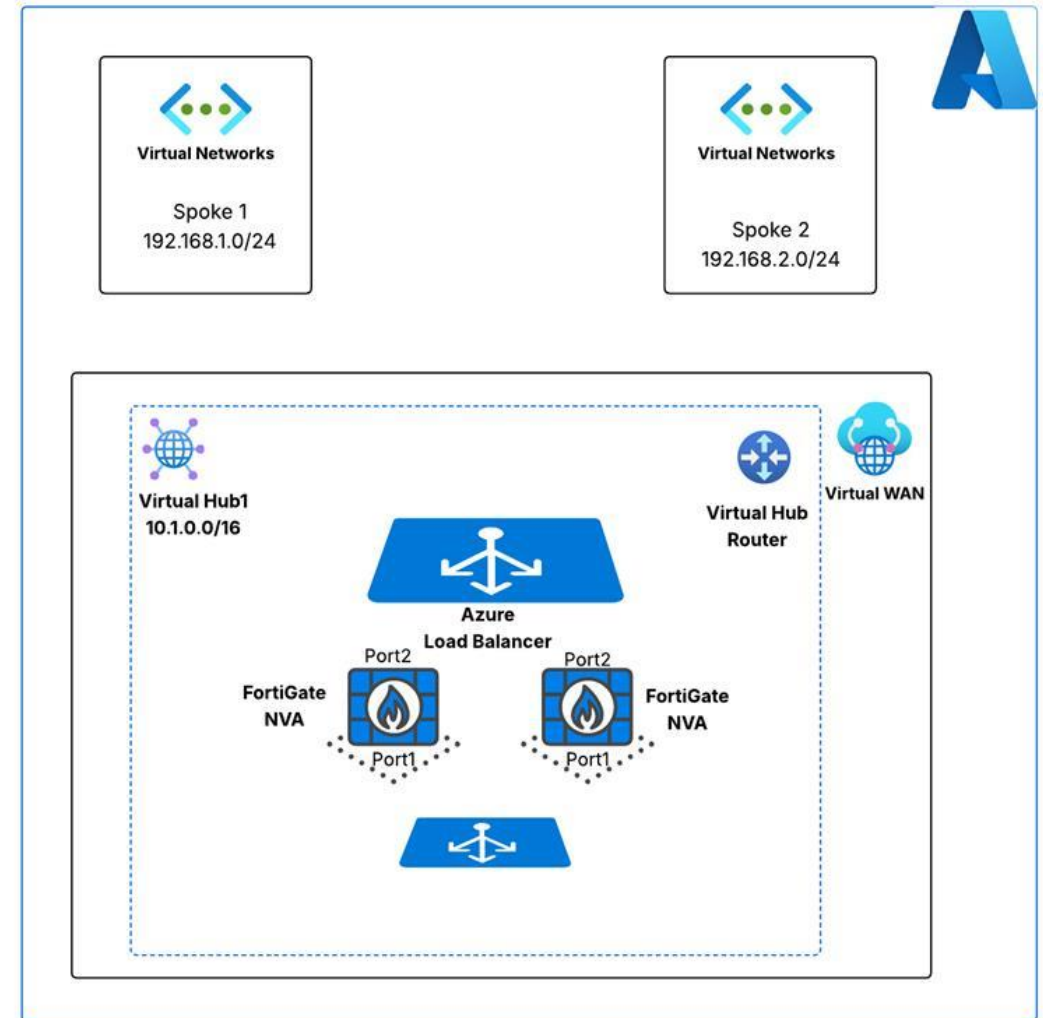
\*\*Already deployed



# Virtual WAN Components – FortiGate NVA

- FortiGate NVAs deployed from Azure portal - VWAN Hub page
- Simple deployment template
  - Name
  - Region
  - Resource Group
  - Address space
  - Subnets
  - Additional Services
    - Ingress Public IP
    - Ingress External Load Balancer
  - Virtual Machines

\*\*Attendee will deploy



Questions



# Getting Started

- Moderated by instructors
- Username assignments
- <https://fortinetcloudcse.github.io/azure-202-advanced>
- Review lab material



**FORTINET**

