

Azure VWAN

Transit Layer Feasibility Study

November 2023



Business



Azure Virtual WAN

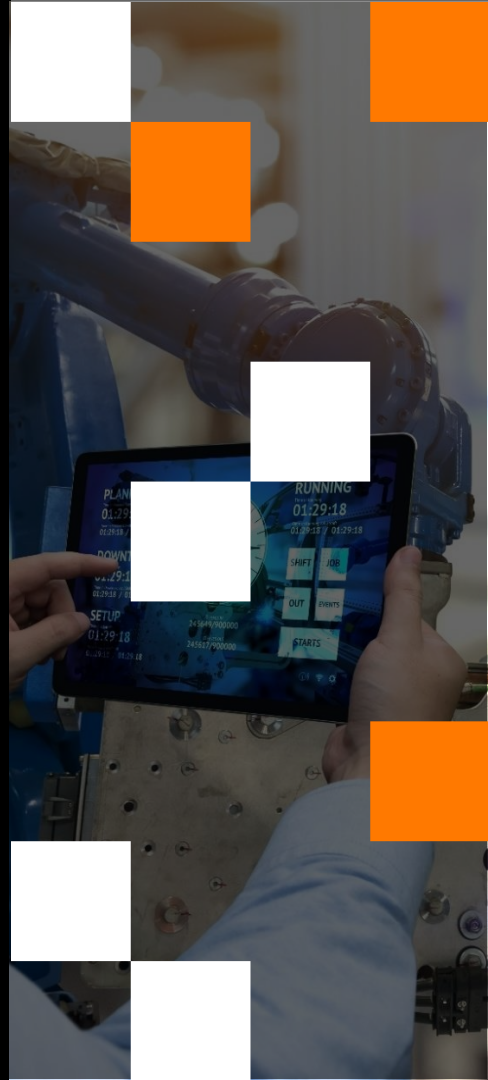
Azure Virtual WAN is a networking service that brings many networking, security, and routing functionalities together to provide a single operational interface. Some of the main features include:

- ✓ **Branch connectivity** | via connectivity automation from Virtual WAN Partner devices such as SD-WAN or VPN Customer Premises Equipment
- ✓ Site-to-site VPN **connectivity**
- ✓ **Remote user VPN** connectivity | point-to-site
- ✓ **Private** connectivity | Express Route
- ✓ **Intra-cloud** connectivity | transitive connectivity for virtual networks
- ✓ **VPN ExpressRoute** inter-connectivity
- ✓ Routing, **Azure Firewall**, and encryption for private connectivity

You don't have to have all of these use cases to start using Virtual WAN. You can get started with just one use case, and then adjust your network as it evolves.



Business



Virtual WAN Transit Network Layer Feasibility Study

This package audits your existing network set up, documents it and provides an opportunity to define your requirements to address your current challenges or future roadmap. This allows you to right-size your network in order to obtain the application performance that your business requires.



Service description

- Collection / gather data from your existing Network
- Assessment of your network management tools
- Establish interviews with key individuals to complete and review this data
- Benchmark the findings
- Workshop to review findings, understand challenges and roadmap assistance to define requirements

Output: Defined requirements and future road map recommendations

Specifications

The scope of Audit includes the following domains:

- Network topologies
- Performance indicators
- Application performance
- Cloud presence assessment
- Network optimization
- Security

Benefits

Enable you to make an informed decision to address future network or remediation

- Decide POC or new project
- Cloud Service provider integration
- Network documentation
- Future roadmap solutions
- Assistance with technical challenge

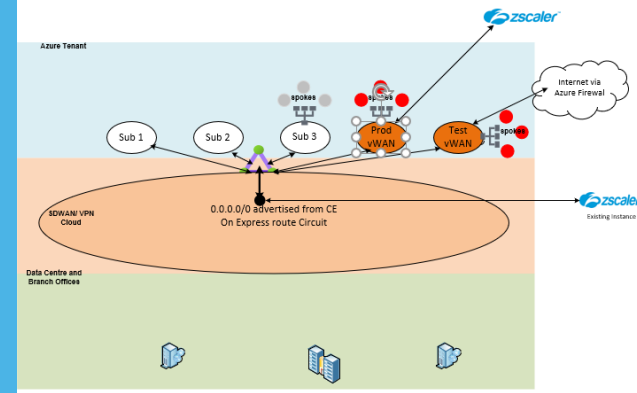
Orange Business

Use cases



Azure Virtual WAN | Replacement of an existing Azure Hub & Spoke

As part of network transformation initiative, a replacement of an existing Azure Hub & Spoke architecture, with a new Transitive Network Architecture was undertaken. It included the migration of existing spokes (spread across multiple Azure Tenants) to the new solution along with traffic filtering controls in fully automated way (infrastructure as code) using **Azure DevOps**.



The Challenges

- The communication between Azure Virtual Networks and data-centre was insecure, inefficient and uncontrolled.
- Complex and operational intensive usage of static routes causing frequent issues in the network.
- Flat network hierarchy.
- Manual infrastructure provisioning.

The Solution

Digital & Cloud Experts support in design & implementation of the Azure Virtual WAN platform.

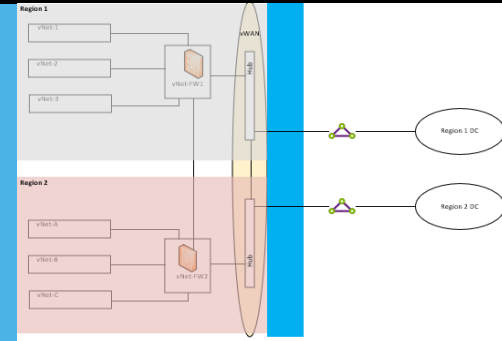
- Templated architecture pattern to deploy Azure Virtual Networks providing seamless connectivity options.
- Infrastructure as code delivered and release pipelines implemented to manage the infrastructure.
- Centralised management of firewall policies and secure virtual hub configurations using Azure Firewall Manager.
- ExpressRoute Circuits and Z-Scaler integrations with Secured Virtual Hub/Azure Virtual WAN environment.
- Documentation

The Benefits

- Common transit network layer implemented to enable seamless and secure connectivity with data-centre services for Azure Virtual Networks.
- Automation & auditable implementation of infrastructure using **Azure DevOps**.
- Centralized security policies for application communication flows security.
- Minimal/No usage of static routes.
- Controlled internet access using Z-Scaler proxy services.

Azure Virtual WAN | Cisco Virtual ASA

As part of the initiative to build a multi cloud transit networking capability and minimizing the usage of public address spaces, a bespoke solution was envisioned and implemented to allow cross-region full mesh connectivity between Azure Virtual Networks and various regional data-centres using customer's public address space.



The challenges

- Traffic between Azure Virtual Networks and Data centre to be NATed using customer public address space.
- Inter-region traffic required to traverse through ExpressRoute Circuits.
- Full mesh communication should be enabled between various regional data centres and multi-region Azure Virtual Networks.

The solution

Digital and Cloud Experts provided expertise to design & implement a be-spoke solution using NVA and Azure Virtual WAN platform to deliver

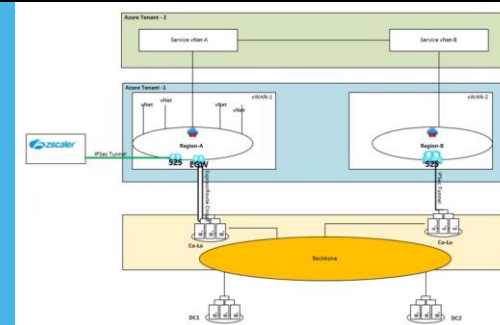
- Connectivity enabled between various regional data centres and multi-region Azure Virtual Networks
- Delivered NATing capability in Azure Cloud to use customer public address space while communication with data-centre resources using ExpressRoute circuits.
- Documentation

The benefits

- Cross-Region full mesh connectivity.
- Common transit network layer implemented to enable seamless connectivity with data-centre services for Azure Virtual Networks.
- NATing capability in Azure Cloud using customer public address space.
- Scalable design pattern for extension into new Azure regions.

Azure Virtual WAN | Site-to-Site VPN's and ExpressRoute Failover

Orange was requested to enable capabilities in Azure Tenant to be able to inspect and filter North-South, East West Traffic between Data Centre, PoPs, Customer Networks and Azure Virtual Networks. Azure Infrastructure was required to be re-architected to enable above feature centrally, optimization of resources and provide customer ability to use repeatable design patterns to meet diverse connectivity requirements. Automated Failover connectivity in case of ExpressRoute infrastructure failure was also required for critical services hosted in Azure.



The challenges

- An organically grown environment, with no proper structure, without a common hop for all traffic to flow.
- Traffic Failover Automation between ExpressRoute Circuit & IPSEC Failover links
- 3rd Party Co-ordination

The solution

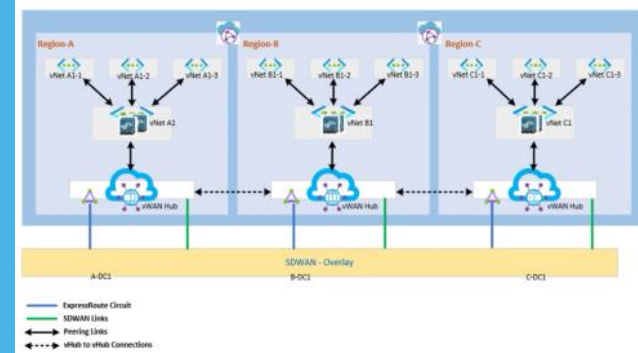
- Digital & Cloud Experts** designed & implemented Secure Azure Transit Network Layer using secure Virtual Hub and Azure Virtual WAN platform to deliver
- Dynamic Routing for Failover between ExpressRoute and IPSEC failover link.
 - Repeatable design pattern for connecting remote sites, resources in other Azure Tenants and vNets within the tenant.
 - Centralized firewall to inspect and filter North-South, East-West Traffic passing through Azure.
 - Local Breakout for Internet Bound traffic via Z-Scaler Services

The benefits

- Repeatable Design Patterns for all connectivity requirements
- Centralized Firewall for all traffic flowing through Azure to inspect and filter.
- 50% reduction in Bandwidth Utilization on ExpressRoute Circuits.
- Organization's uniform policy application on all Internet bound traffic from Azure.
- Optimization of Azure Resources.
- Orange Managed Service for Managing Azure Network & Security Infrastructure

Azure Virtual WAN | Integration with Hub and Spoke Topology

As part of Network Infrastructure upgrade and optimization program, Customer have been looking to integrate its Cloud environments with SDWAN cloud. Delivered Azure Transit Network layer using vWAN with ExpressRoute Circuits & Cisco Cloud On-Ramp solution to provide direct connectivity between Azure Transit Network Layer and SDWAN cloud.



The challenges

- Customer Security requirement to use Palo Alto as a Firewall, to inspect and filter all North-South & East West traffic between different regions and On Prem and Cloud Environments
- Customer Cloud environment, did not have Azure vWAN as a transit network layer to enable connectivity with Cisco Cloud OnRamp Solution
- Azure vWAN doesn't support Palo Alto Firewall NVA's as part of Secure hub architecture.

The solution

Digital & Cloud Experts designed & implemented a be-spoke solution to enable Azure Transit Network Layer with existing Hub and Spoke infrastructure in Azure Regions, with Palo Alto in Hub vNets, and Cisco Cloud onRamp integration to deliver SDWAN connectivity to Azure Infrastructure delivering:

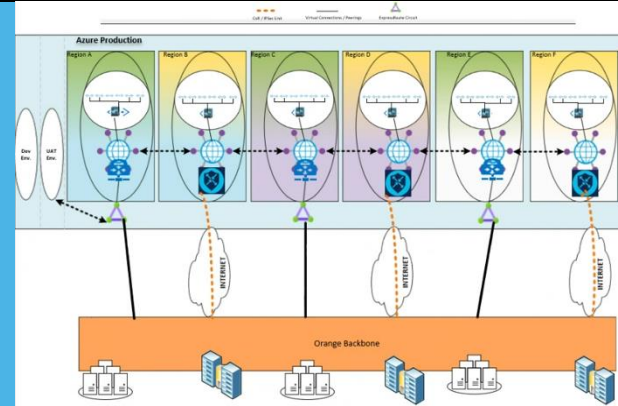
- Secure Connectivity enabling all North-South & East-West traffic to pass via Palo Alto Firewalls in each region.
- Re-architected the Transit Hub vNet (in Hub and Spoke architecture) to facilitate integration of the same with Azure vWAN Hub. (Bespoke traffic control plane)
- Cisco Cloud OnRamp Integration with Dynamic routing between ExpressRoute Circuits and SDWAN links to deliver failover capabilities.

The benefits

- Azure vWAN Transit Network Solution implemented to enable integration with SDWAN cloud.
- Dynamic Failover and un-interrupted traffic flow between Azure vWAN Hub and Rest of environment.
- Optimum use of Azure resources such as ExpressRoute Circuits, ExpressRoute Gateways etc.
- Extending cost-effective reach from remote regions to Azure Infrastructure.

Azure Virtual WAN and Cloud on Ramp solution using 3rd party NVA

As part of Network Infrastructure upgrade and optimization program, Customer have been looking to integrate its Cloud environments with SDWAN cloud. Delivered Azure Transit Network layer using vWAN with ExpressRoute Circuits & Cisco Cloud On-Ramp solution to provide direct connectivity between Azure Transit Network Layer and SDWAN cloud.



The challenges

- Customer Security requirement to use Palo Alto as a Firewall, to inspect and filter all North-South & East West traffic between different regions and On Prem and Cloud Environments
- Customer Cloud environment, did not have Azure vWAN as a transit network layer to enable connectivity with Cisco Cloud OnRamp Solution
- Azure vWAN doesn't support Palo Alto Firewall NVA's as part of Secure hub architecture.

The solution

- Digital & Cloud Experts** designed & implemented a be-spoke solution to enable Azure Transit Network Layer with existing Hub and Spoke infrastructure in Azure Regions, with Palo Alto in Hub vNets, and Cisco Cloud onRamp integration to deliver SDWAN connectivity to Azure Infrastructure delivering:
- Secure Connectivity enabling all North-South & East-West traffic to pass via Palo Alto Firewalls in each region.
 - Re-architected the Transit Hub vNet (in Hub and Spoke architecture) to facilitate integration of the same with Azure vWAN Hub. (Bespoke traffic control plane)
 - Cisco Cloud OnRamp Integration with Dynamic routing between ExpressRoute Circuits and SDWAN links to deliver failover capabilities.

The benefits

- Azure vWAN Transit Network Solution implemented to enable integration with SDWAN cloud.
- Dynamic Failover and un-interrupted traffic flow between Azure vWAN Hub and Rest of environment.
- Optimum use of Azure resources such as ExpressRoute Circuits, ExpressRoute Gateways etc.
- Extending cost-effective reach from remote regions to Azure Infrastructure.



Business