White paper
Cisco public

Modern Transit Architecture with Cisco Cloud OnRamp for Azure Virtual WAN

Contents

Today, digital transformation and cloud migration are the top priorities for most organizations. The question is not whether to migrate to the cloud but when. IT teams have started realizing the benefits of moving workloads to the cloud, such as agility, scalability, and reduced costs and time to bring up new services. Some applications have moved to the cloud, while others are still residing in the data center. This has resulted in a hybrid cloud world, in which users accessing these applications are largely unchanged. They are still accessing applications from branches, campus hubs, and now from home as well.

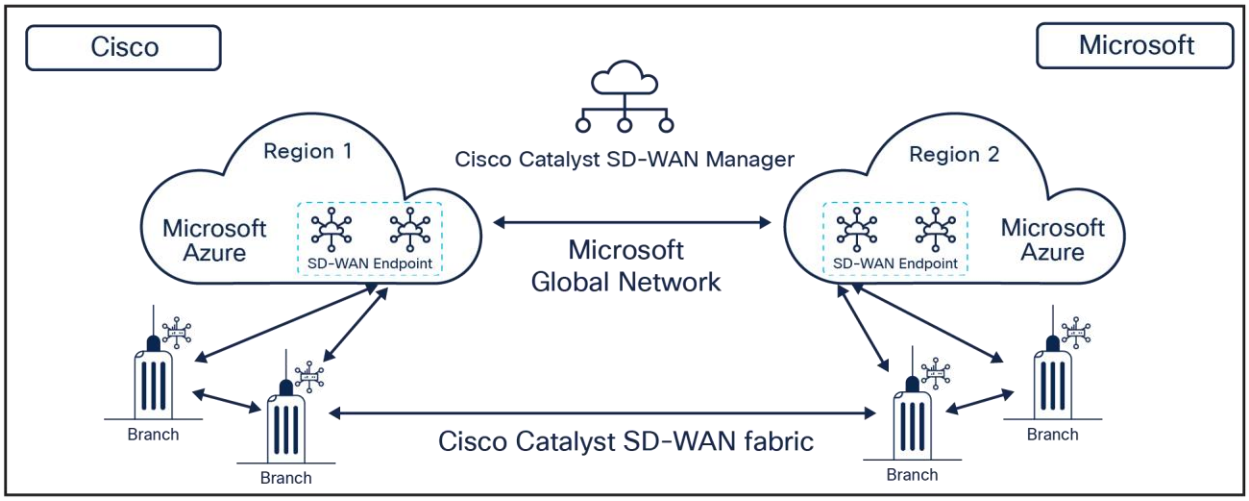

Figure 1.
Modern transit connectivity using Cisco SD-WAN Cloud OnRamp for Azure Virtual WAN

This shift to hybrid cloud has created challenges in providing connectivity to cloud-hosted applications while still meeting SLAs. The cloud has become an extension of the enterprise network, and it requires seamless connectivity and consistent policy that were previously applicable to the branch and data center.

In this document we talk about how together, Cisco and Microsoft have built a new cloud transit architecture to modernize network connectivity to Microsoft Azure by leveraging Azure Virtual WAN to route and secure traffic to and across Microsoft Azure. This modern architecture enables customers to seamlessly extend their SD-WAN to Microsoft Azure cloud with “any-to-any” secure connectivity between enterprise on-premises sites and Azure Virtual Network (VNet).

Phase 1: Evolution to the Modern Transit Architecture

The introduction of the Cisco Cloud Services Router 1000V (CSR 1000V) allowed customers to extend connectivity from their branches, campuses, and data centers to Microsoft Azure. Enterprise customers migrating their workloads to Azure could deploy CSR 1000V routers in Azure to extend connectivity to Azure and reap the benefits of a modern Cisco IOS XE networking platform, as they were accustomed to doing with hardware platforms at their edges. In this design architecture, a pair of CSR 1000V routers were deployed in a transit VNet. However, this required understanding a myriad of choices available on different virtual machines to deploy and configure the CSR 1000Vs and manually build an overlay network connecting various VNets to the CSR 1000Vs deployed in the transit VNet. Networking expertise was required to bring up IPsec tunnels between the CSR 1000V router and various VNets and set up Border Gateway Protocol (BGP) peering over those tunnels. The process was complex and error prone and required several hours to complete using multiple management consoles. Although this worked for a small number of branch sites, the complexity made it difficult to scale the process to support hundreds of branch sites. Enterprise customers found it hard to maintain and troubleshoot their cloud deployments, especially when branches were spread across multiple regions. The entire process required an in-depth understanding of transit VNets, the configuration to apply to CSRs, and setting up IPsec connectivity with other VNets, making it difficult for customers to use and respond to a dynamically changing cloud environment.

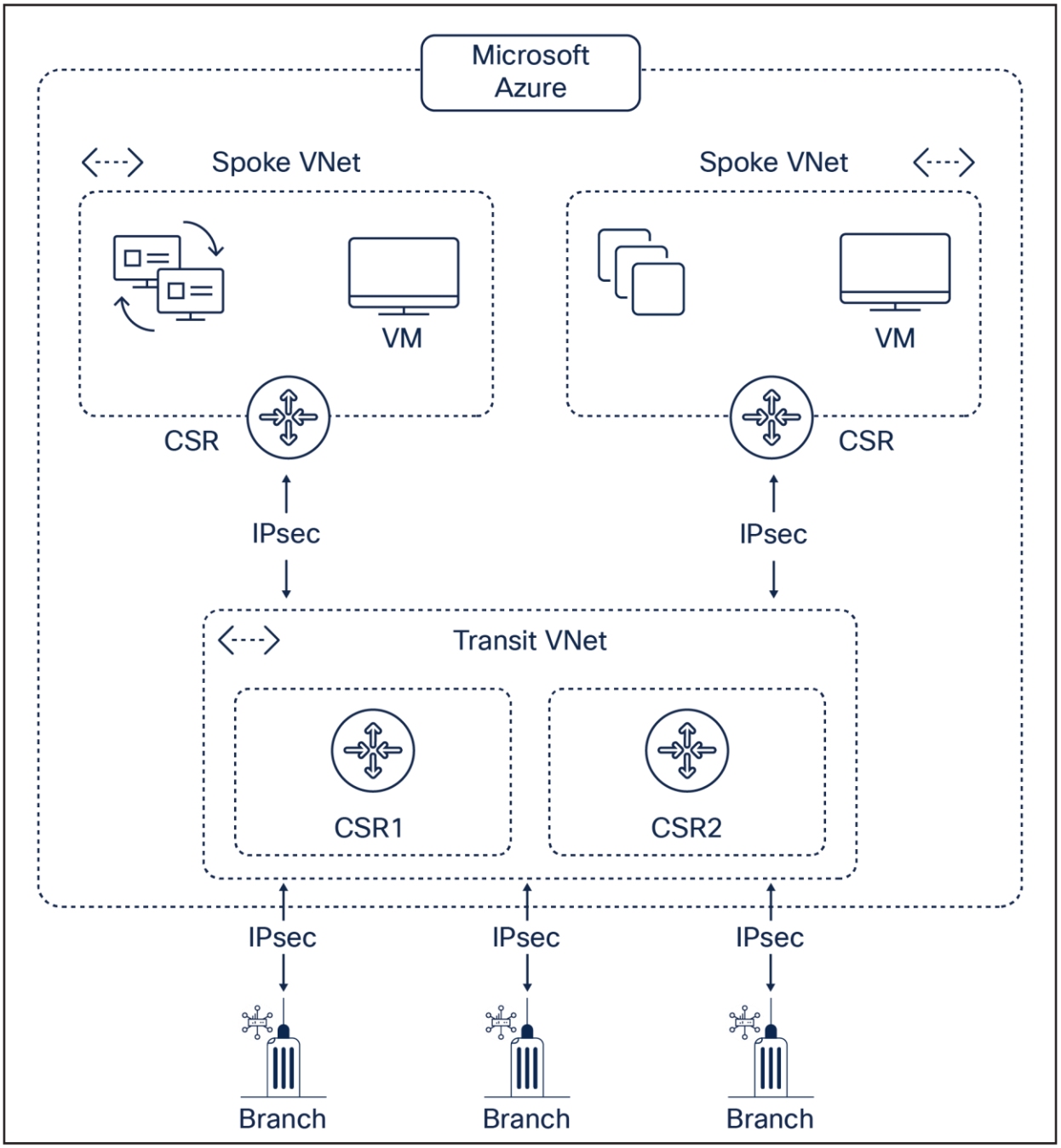

Figure 2.
Cloud connectivity with CSR 1000V routers

Phase 2: Cloud OnRamp for IaaS for Azure

To overcome these challenges and simplify things, Cisco introduced its next iteration of a cloud connectivity solution called Cisco Cloud OnRamp for IaaS for Azure. This offered automation and a single pane of glass by extending the SD-WAN fabric to Azure, addressing some of the challenges of building and maintaining an overlay transit network. With Cloud OnRamp for IaaS, various VNets hosting workloads or application VMs connected via IPsec connections to a redundant pair of CSR 1000V routers deployed in a transit VNet in Azure. The transit VNet in turn became part of the SD-WAN fabric, providing direct VPN connectivity to branch and data center sites within the private network. Cloud OnRamp for IaaS also automated the deployment of transit VNets and the bring-up of WAN edge virtual routers and interconnected VNets automatically with transit VNets. All customers had to do was enter their Azure ID and the client secret key in the Cisco Catalyst SD-WAN Manager GUI.

While Cloud OnRamp for IaaS for Azure addressed automation challenges, it still required building IPsec tunnels between the transit VNet and other VNets. Customers deployed a pair of CSR 1000V in the transit VNet for resiliency and high availability. This architecture also limited throughput, as all traffic between branch sites and VNets, as well as from VNet to VNet, had to traverse through the pair of CSR 1000V routers. The design was inflexible when a customer needed to insert other network services, such as a firewall, into the data plane. Solution validation was yet another challenge, as any change to the Azure environment had the potential to break the solution. With the need to bring up additional services in Azure, Cloud OnRamp for IaaS also posed challenges in service chaining and proved to be an intermediate stop, rather than the final destination that customers are looking for.

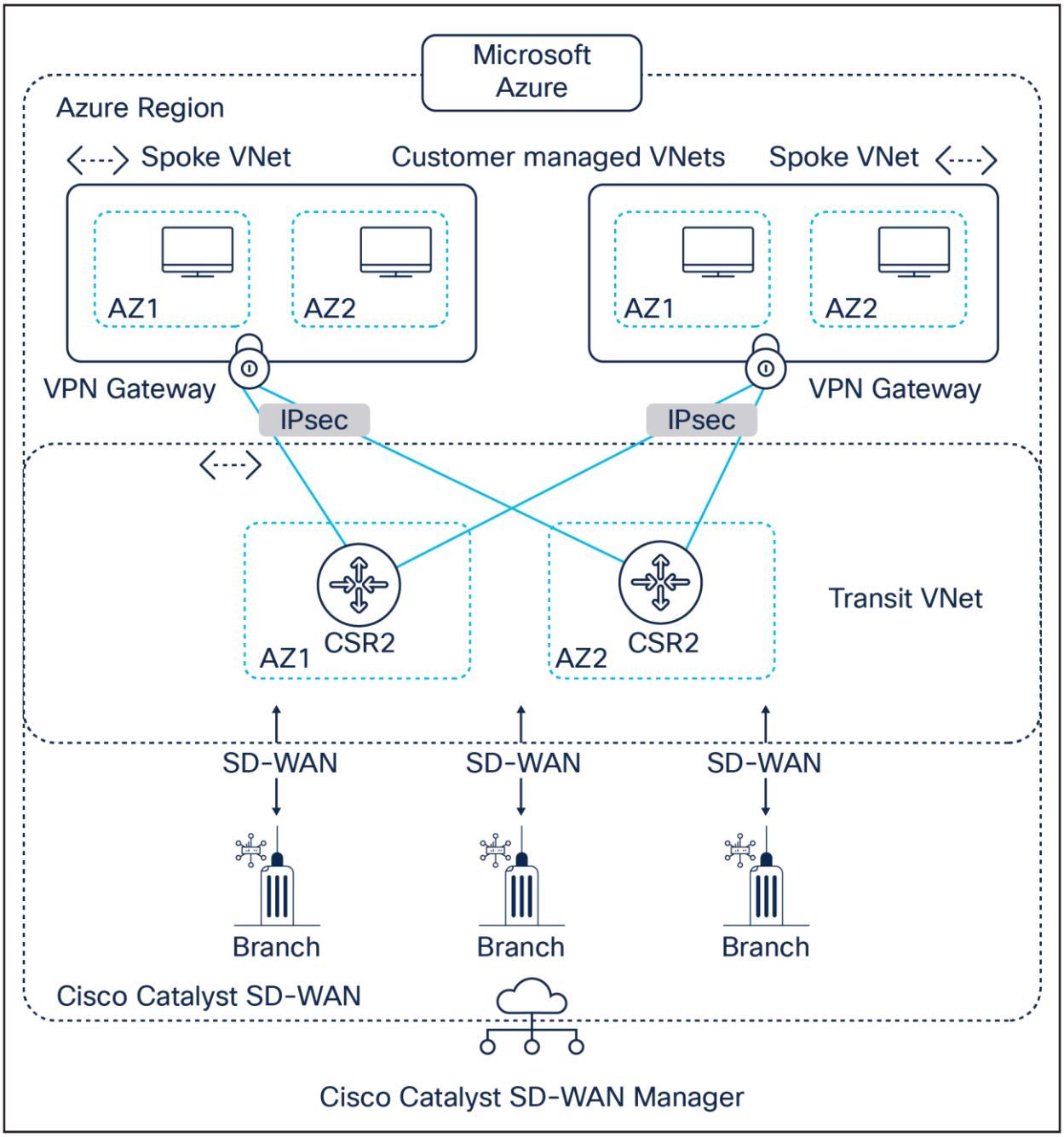

Figure 3.
Cisco Catalyst SD-WAN cloud connectivity using Cloud OnRamp for IaaS

Microsoft, on the other side, recommended that customers predominantly use transit VNets to interconnect Azure workloads and connect on-premises branches by developing a hub-and-spoke model. In this model, end users connected to workloads in Azure using a virtual network gateway VPN connection or ExpressRoute connection into a transit VNet or customer self-managed hub. The transit VNet would then peer with the spoke VNet in the same region to provide connectivity to Azure workloads. The number of transit VNets and peered VNets grew over time as customers increased their cloud footprint. Additional challenges such as increased routing complexity, throughput limitations, restrictions on the number of connected VPN sites, and limitations on the number of virtual networks that could peer with an ExpressRoute circuit made it difficult to scale the connectivity. Customers had to set up full-mesh connectivity between spoke VNets or add a network virtual appliance in the transit VNet to allow spoke VNets to communicate with each other.

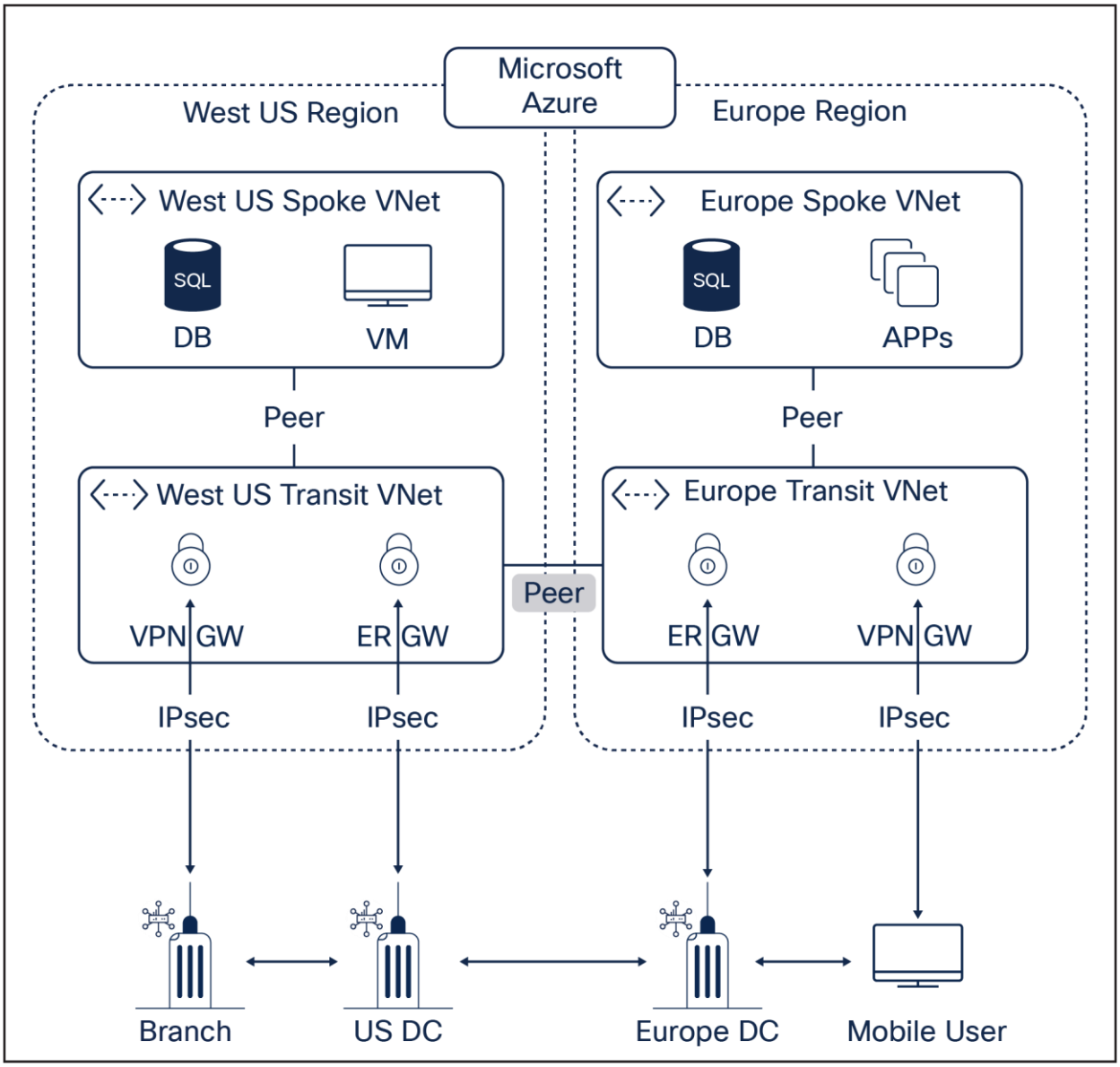

Figure 4.
Microsoft Azure connectivity using hub-spoke and transit VNets

Phase 3: Modern Transit Architecture

The hub-and-spoke model using the transit VNet approach does offer cloud transit but has several limitations that restrict its usability in large-scale deployments. A modern transit architecture is required to seamlessly extend branch sites to cloud and facilitate spoke VNet-to-VNet communication that can scale to support a large number of sites with higher throughput and performance. It should eliminate the need to build additional overlay IPsec connectivity between the transit VNet and host VNets, leverage firewall capabilities in the cloud to secure the loads and traffic going in either direction, and use Azure inter-region connectivity to easily extend to other regions to create a single fabric. It should allow consistent policies, bring ease of use to the forefront, hide the complexity of the choices that customers have to make on virtual machines, and provide a close handshake between Cisco and Microsoft to build and validate the solution together. To make all this possible, Microsoft introduced Azure Virtual WAN and Cisco introduced Cloud OnRamp for Azure Virtual WAN starting with Cisco IOS XE Release 17.4.1 and Cisco Catalyst SD-WAN Manager Release 20.4.

Microsoft Azure Virtual WAN and Cisco Cloud OnRamp for Azure Virtual WAN enables the Modern Transit Architecture

To simplify connectivity to the Azure cloud, Microsoft introduced a new networking service, Azure Virtual WAN, that brings networking, routing, and security services together to provide a single operational interface. It replaces the transit VNet with the new Virtual WAN hub concept. The Virtual WAN architecture is a hub-and-spoke architecture with scale and performance built in for branches, users, ExpressRoute circuits, and virtual networks. It enables a global transit network architecture in which the cloud-hosted network "hub" enables transitive connectivity between endpoints that may be distributed across different types of "spokes."

Azure regions serve as hubs that you can choose to connect to. All hubs are connected in full mesh in a standard Virtual WAN, making it easy for the user to use the Microsoft backbone for any-to-any (any spoke) connectivity.

Cisco Cloud OnRamp for Azure Virtual WAN is a fully integrated automation solution that helps customers deploy SD-WAN Network Virtual Appliances (NVAs) in the Microsoft Virtual hubs and extend SD-WAN fabric between branch sites and on-premises data centers to the Azure cloud. This approach enables native peering with the Microsoft Virtual WAN hub, thus providing better performance and resiliency than previous-generation solutions. The SD-WAN NVAs running inside the virtual hub are Cisco Catalyst 8000V edge routers that can be managed through the Cisco Catalyst SD-WAN Manager. The solution requires Cisco Catalyst SD-WAN Manager to be at the 20.4.x or higher code version and for the Cisco Catalyst 8000V edge routers to be at 17.4.x code or higher. The latest solution is the recommended one for customers from Cisco and offers some key benefits over previous solutions:

- **Native integration in Azure:** SD-WAN endpoints are natively integrated into the Microsoft Azure Virtual WAN Hub as NVAs and thus provide better resiliency and performance compared to previous solutions.
- **Eliminates IPsec overlay connectivity between the transit VNets and/or the spoke VNets:** Azure Virtual WAN natively provides Virtual WAN hub-and-spoke VNet connectivity with dynamic "any-to-any" connectivity between branch SD-WAN sites and spoke VNets.
- **Peering with an Azure Virtual WAN Hub router:** Native BGP peering with an Azure Virtual WAN Hub router provides a better way to manage endpoints in Azure by not incurring the overhead of using IPsec to communicate.

- **Inter-region connectivity:** Virtual hubs are all connected to each other over a virtual WAN, which implies that a branch, VNet, or user connected to a local hub can communicate with another branch or VNet using the full mesh architecture of the connected hubs.
- **Global site-to-site connectivity:** The solution allows customers to leverage the high speed Microsoft global backbone network as a transit to establish SD-WAN connectivity from a site in one region to a site in another region with multi-region fabric.
- **Higher speed and bandwidth:** Configuring Catalyst 8000V instances as NVAs inside Azure virtual hubs provides higher speeds and bandwidths and overcomes the limitation of using transit VNets.
- **Built-in resiliency:** Azure Virtual WAN provides enhanced resiliency for the NVAs, as it leverages the same resiliency and orchestration features as other native networking services in the Azure Virtual WAN, so if one NVA goes down, Azure will bring up another instance of it in the same Virtual WAN hub.
- **Full solution validation:** The close partnership between Cisco and Microsoft gives customers complete peace of mind that the solution is validated continuously by both Cisco and Microsoft as new changes are introduced by either side.
- **Complete automation:** The solution is completely automated through Cisco Catalyst SD-WAN Manager, thus eliminating the need to manually bring up or configure NVAs or virtual hubs as well as establish site-to-site connectivity on the Microsoft global backbone network. Cloud OnRamp for Azure does it for you.
- **Firewall service chaining:** Native integration in Azure allows for service chaining capabilities and easy bring-up of services as and when needed. The solution is validated with the Azure firewall as well, so customers can easily secure traffic going from branch to VNet, VNet to branch, branch to internet, and VNet to internet using the branch firewall.
- **Telemetry and analytics:** The close partnership between Cisco and Microsoft allows for sharing of telemetry information and easy monitoring of health of NVAs in the Azure analytics dashboard, thus enhancing troubleshooting capabilities.

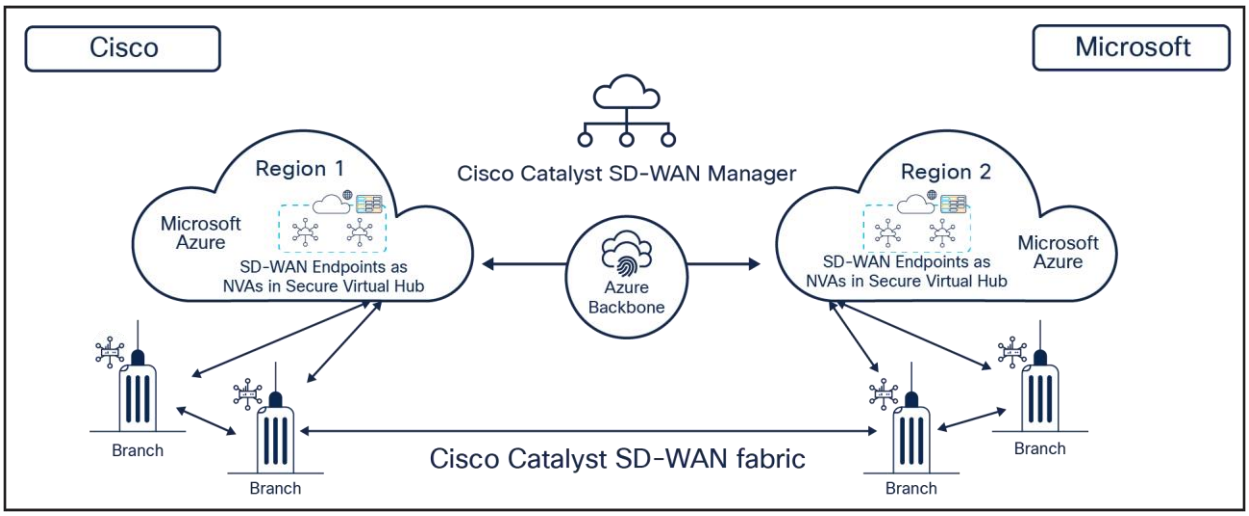

Figure 5.
Modern transit connectivity using Cisco SD-WAN Cloud OnRamp for Multicloud with Azure Virtual WAN

Summary

Cisco Cloud OnRamp for Azure Virtual WAN truly builds on a modern transit architecture that is independent of the underlay network. Whether the traffic needs to go from branch to cloud, branch to data center, or data center to cloud, Cisco Cloud OnRamp supports all scenarios. Whether the applications are residing in the data center or in a cloud or have a hybrid environment, Cisco Cloud OnRamp is built for all. Inter-region connectivity supports workloads that are both local or spread across the globe. **Cisco Cloud OnRamp for Azure Virtual WAN is the recommended solution if you are truly looking to build a modern WAN and transit architecture**.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USA C11-2708259-02 12/23