Cisco SD-WAN Cloud OnRamp for Multicloud Whitepaper

Use Cases for Cloud OnRamp for Multicloud

October 2025

Cisco SD-WAN Cloud OnRamp for Multicloud Solution Overview

Increasingly, companies are deploying applications and workloads where they will best perform business functions while optimizing costs wherever possible. This requires careful planning and attention when designing a hybrid network which connects these environments together, whether they are deployed in a customer-owned data center, a colocated data center, in one or more clouds, or a combination of these.

The intersection of networking domains is where the greatest complexity associated with hybrid networking appears, and so it is important that a resilient, performant networking solution that is easy to deploy and operate is utilized in a modern network. The Cisco SD-WAN Cloud OnRamp for Multicloud deployment workflow can deliver simple, automated, resilient outcomes without increased complexity for organizations that have a Cisco SD-WAN deployment and want to extend their connectivity policy while maintaining control and application visibility across multiple transport environments. Cloud OnRamp for Multicloud can accelerate an organization's cloud integration without requiring extensive cloud expertise. Please note that Cloud OnRamp not only automates SD-WAN extension to public clouds, but also simplifies Day N Operations featuring cloud audit, which can detect and even fix configuration drift between the SD-WAN deployment and cloud deployment.

Tech tip: Cisco SD-WAN Cloud OnRamp for Multicloud supports AWS, AWS GovCloud, Azure, Azure GovCloud, and Google Cloud as of version 20.18. AWS GovCloud and Azure GovCloud are functionally the same as AWS and Azure for the purposes of this whitepaper.

Tech tip: Customers can still manually connect SD-WAN routers to other clouds and 3rd-party network using unencapsulated, IPsec or GRE connectivity as normal without using this workflow.

Frequently used terminology in this paper

- CSP or Cloud Service Provider or Hyperscaler
- VPCs or VNets – Virtual Private Cloud or Virtual Network
- Cloud Gateway or CGW – the gateway deployed at the edge of cloud regions, usually comprising of 2 or more virtual routers and the native cloud networking construct like AWS Transit Gateway, AWS Core Network Edge, Azure Virtual Hub or Google Cloud Router
- NVA – Network Virtual Appliance. In this paper the virtual router is deployed as an NVA in the cloud

Center of Gravity Considerations

When designing an SD-WAN OnRamp for Multicloud deployment, there are several options to consider; the most important may be associated with the organization's cloud maturity and current or future connectivity plans. Organizations commonly split their application workloads between cloud and on-prem in whatever environment is most advantageous, but from a networking perspective, what matters is the level of hybrid connectivity desired, the amount of visibility and control required, and the current maturity of a cloud deployment. In short, where is most of the data located and where are the users?

Option 1: SD-WAN Extended into the Cloud via Cloud Gateway Deployment

This is historically the most common type of deployment as the automation greatly simplifies the primary goal of on-premises to cloud workload connectivity. With this type of Cloud OnRamp deployment (called Cloud Gateway), the Cisco Catalyst SD-WAN Manager will automate the creation of cloud-based WAN Edges and connect them to the native cloud constructs that are supported for this kind of integration, such as AWS Transit Gateway, AWS Cloud WAN, Azure vWAN, or Google NCC / Cloud WAN. Furthermore, the

SD-WAN Manager will allow tagging and manage onward connectivity from the native cloud constructs to the workload VPCs/VNets. This option is also known as site-to-cloud.

With this type of integration, the focus is on extending the SD-WAN fabric into the cloud network space. This type of extension allows increased control, visibility and security at the cost of requiring network virtual appliances in the form of WAN Edges. This introduces slightly more complexity over depending directly on cloud native constructs. There are tradeoffs to be considered, discussed below:

Pros:

- SD-WAN Manager can automate the deployment and integration of cloud-native constructs and the SD-WAN fabric.
- In-built resiliency offered by the cloud gateway deploying multiple virtual routers in a high-availability pattern, usually in different availability zones/datacenters
- Visibility of application connectivity extends into the cloud, across the hybrid connectivity boundaries that otherwise require collation of multiple telemetry sources to understand the network conditions.
- WAN Edges can overcome many native cloud limitations associated with scale, such as maximum number of routes, as well as offering traffic engineering options that exceed what native cloud can provide.
- Catalyst SD-WAN policy can be extended and enforced into the cloud itself, potentially improving the performance and security of the cloud network and simplifying the traffic flows between the cloud workloads and on-premises resources.
- SD-WAN security features can be used much closer to the cloud workloads, and traffic can be inspected for north-south and east-west flows.

Cons:

- The addition of network virtual appliances (NVAs) introduces a measure of complexity in terms of integration with native cloud constructs. SD-WAN Manager handles this integration in an automated way, but this may increase routing complexity over exclusively using cloud native constructs.
- Lifecycle management is required for NVAs that are not required for native cloud constructs; this is made much simpler by the mature lifecycle management options in Cisco Catalyst SD-WAN, but it does need to be considered when deciding whether to utilize this option.
- Because the Cloud OnRamp workflow is automated and prescriptive, it may or may not fit the network design of an organization that is already deployed in or across clouds. Cloud OnRamp supports brownfield use cases, where existing cloud infrastructure can be used with SD-WAN, but in case of very specific or rare cloud designs, Cloud OnRamp automation may not work. It also may not fit the Infrastructure as Code requirements or workflows already present in a mature cloud organization.

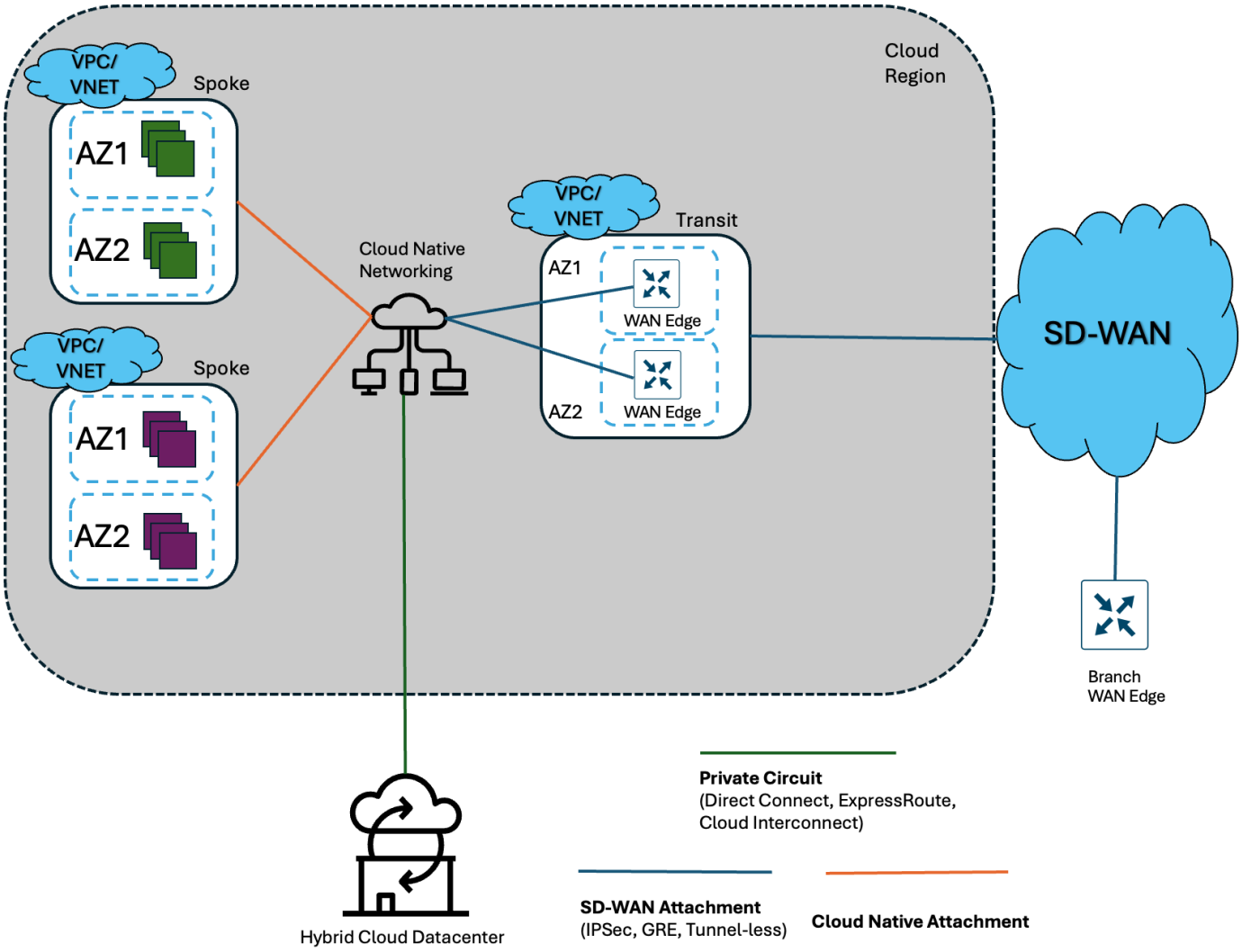

Figure 1. SD-WAN Cloud OnRamp for Multicloud Deployed with Cloud Gateway

Option 2: SD-WAN connecting to the cloud using Branch Connectivity (AWS Only)

With this type of Cloud OnRamp deployment, the SD-WAN Manager will automate the creation of direct site-to-site IPsec tunnels between SD-WAN Edges and the AWS Transit Gateway directly, without a Cloud Gateway. Note that, in this case, a standard IKE-based IPsec tunnel is used and not an SD-WAN tunnel. In this deployment, the SD-WAN is not extended into the cloud, but instead, the cloud workloads are connected to the SD-WAN. This is an important distinction, because connectivity is more direct but less scalable.

Pros:

- Simple and efficient connectivity for VPCs to be accessible via the SD-WAN over an AWS TGW
- Automated deployment of a standard IKE-based IPsec tunnel
- SD-WAN policy can be enforced once traffic enters the SD-WAN from the cloud, including security policy

Cons:

- This is a point connectivity solution which does not scale across an entire cloud network

- While the deployment of the IPsec tunnel is automated, the IPsec tunnels are per-WAN Edge, and cloud connectivity is not consolidated to a Cloud Gateway. This requires more monitoring and telemetry.
- Commonly, this deployment uses Internet transport rather than one with SLA such as a service provider, middle mile or private circuit. This type of connectivity tends to be simple and cheap but lacks service level agreements, making it best used for non-critical application connectivity.

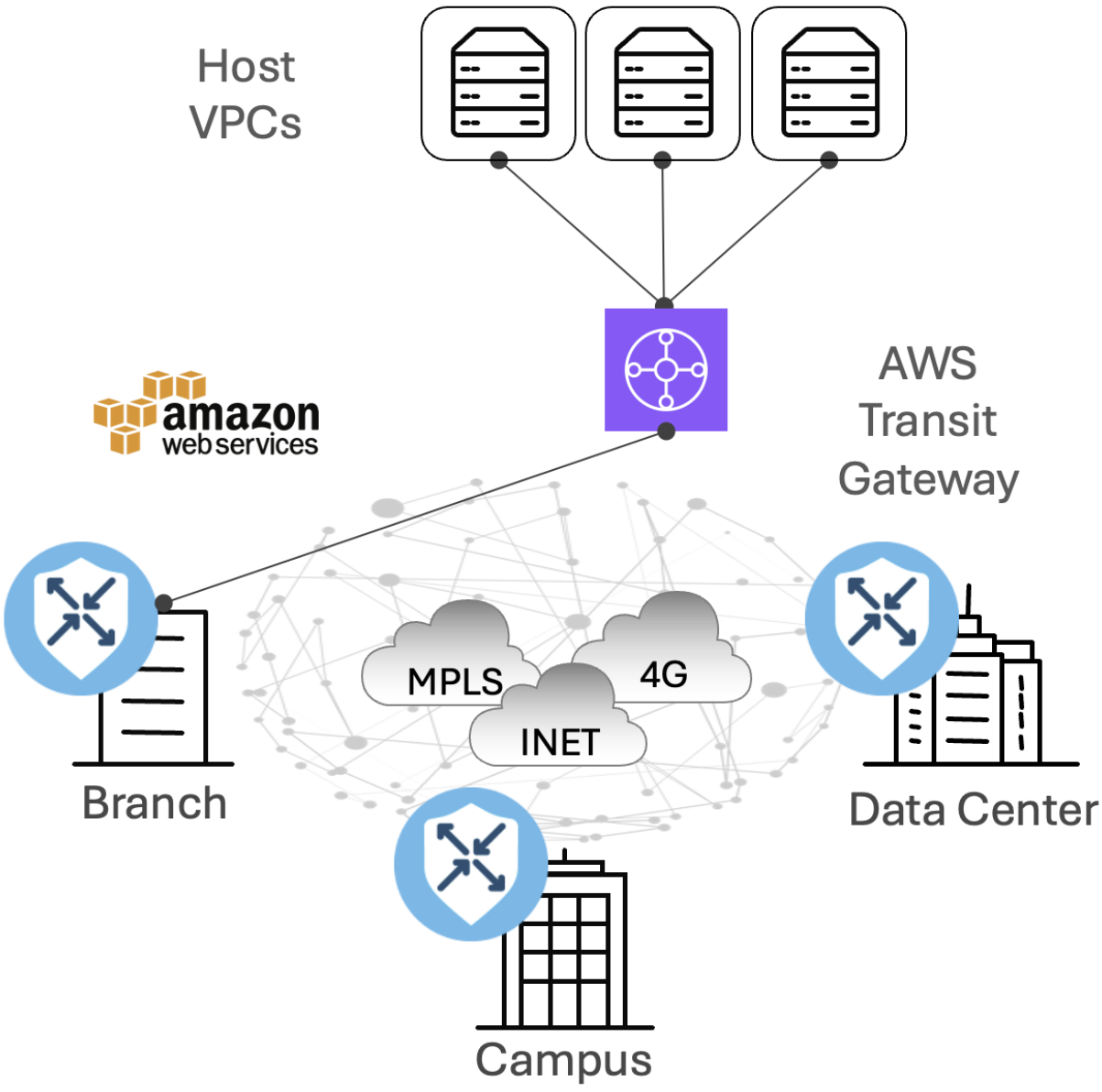

Figure 2. SD-WAN Cloud OnRamp for Multicloud Deployed with Branch Connect

Option 3: SD-WAN Site-to-Site Connectivity Over Cloud Provider's Backbone

With this type of deployment, SD-WAN sites leverage the Cloud Gateway as a geographical routing point, connecting different regions over the cloud service provider's (CSP's) backbone instead of using a

traditional WAN or Internet. This option can co-exist, and is not mutually exclusive, with the site-to-cloud connectivity (option 1) since the same cloud gateway is used for both.

Pros:

- The path over the CSP backbone could be faster and more reliable than internet, yet potentially cheaper than MPLS. This depends heavily on the data transferred between regions, however.
- SD-WAN fabrics deployed over a CSP backbone benefit from path visibility and health monitoring using SD-WAN's built-in BFD and SLA probes

Cons:

- Potentially more expensive depending on traffic flows and data transfer
- Increases lifecycle complexity due to necessity of orchestrating upgrades to minimize impact

What organizations will benefit most from SD-WAN Cloud OnRamp for Multicloud?

The SD-WAN Cloud OnRamp for Multicloud solution provides a complete solution to integrate hybrid cloud networks, whether it be connected over the Internet, a service provider's private circuits, or through a colocation provider such as Equinix or Megaport. This means that the solution covers many deployment options and solutions and so should be able to meet most organizational objectives. However, there are organizations who would align more closely with the benefits and strengths of this solution, such as organizations that:

- Use a Cisco Catalyst SD-WAN deployment that incorporates WAN transports that are to be used for hybrid cloud connectivity to one or more clouds (i.e. Internet, cloud service provider circuit, middle mile colocation provider circuit)
- Have resources in one or more public clouds that requires connectivity to or from users and applications connected to a Cisco Catalyst SD-WAN deployment
- Wish to extend or involve SD-WAN policy and security to resources located in one or more public clouds
- Have a need for simple, efficient, and self-contained automation solution for hybrid connectivity that is not already managed by another IaC solution

Organizations that have complex hybrid cloud connectivity options such as a mixture of private circuits and Internet connectivity stand to gain the most from a Cloud Gateway deployment. Such a deployment leverages the greatest strengths of an SD-WAN deployment to steer traffic intelligently and automatically react to changing conditions. As of Cisco Catalyst SD-WAN version 20.18, the ability to seamlessly segment SD-WAN VPNs and cloud-attached resources using CSP Tags can be automatically deployed and enforced.

Which types of organizations will see smaller benefits from using SD-WAN Cloud OnRamp for Multicloud?

SD-WAN Onramp for Multicloud is a self-contained solution that orchestrates and automates connectivity from an SD-WAN fabric to cloud resources over a variety of transports. This allows organizations that do not have a fully Infrastructure-as-Code workflow to capture the most value.

Because SD-WAN Manager and the orchestration/automation of hybrid cloud connectivity in this workflow is contained within the SD-WAN Manager only, , organizations that have a mature IaC solution (such as

cloud-native IaC or 3rd party IaC solutions such as Terraform) for the deployment and management of infrastructure state must exercise caution when including SD-WAN Cloud OnRamp for Multicloud as part of an overall IaC solution to ensure that the IaC management solutions do not interfere with each other.

Organizations that will encounter challenges adopting the SD-WAN Cloud OnRamp for Multicloud include organizations that:

- Utilize cloud-native or 3rd-party IaC solutions for all network connectivity management
- Have a cloud team that manages all network connectivity and does not have access or expertise with Cisco Catalyst SD-WAN

Both challenges are minimized when using the Branch Connectivity workflow due to the lack of SD-WAN deployment into the cloud. Despite this, the main concern continues to be ensuring that state tracking of network connectivity is not shared between multiple orchestration platforms. If this happens, the two platforms often detect changes caused by the other and roll out their own changes to restore the perceived correct state.

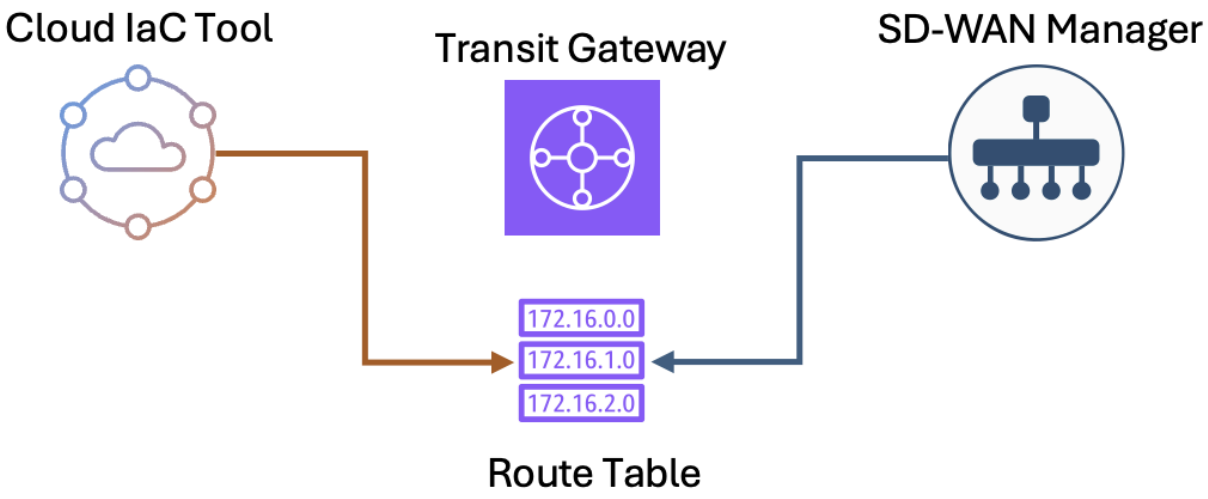

Figure 3. Cloud Native Construct Configuration Change Loop

The second concern is administrative: the team responsible for hybrid networking should understand how to use Cisco SD-WAN Manager to deploy and manage the solution.

These challenges are minor and can be solved with proper planning and an understanding of what each IaC solution will be responsible for deploying and managing to ensure there is no overlap.

Cisco SD-WAN Cloud OnRamp for Multicloud: Business and Technical Value

Before adopting any new solution, it is important for organizations to understand their own current and future deployment plans and the value any proposed solution will deliver. In this next section, the strengths and value will be explained for each type of deployment. Some deployment types may be combined, such as a Multicloud deployment including Cloud Interconnect options through middle mile providers. Many of these benefits are also additive; that is, benefits realized in a single cloud deployment are also observed in a multicloud deployment, in addition to simplifying the connectivity between clouds. For this reason, this section will focus on the specific benefits available in each, but the total benefits are additive throughout.

This section will focus on Cloud Gateway; Branch Connectivity is a simple, fast way to connect resources together in AWS, involves the least amount of routing complexity, and requires no network virtual appliances in the cloud. The drawback for Branch Connectivity is its lower level of control and its lack of visibility or policy in the cloud, as discussed in the Overview section.

SD-WAN Cloud Onramp for Multicloud: Single Cloud Deployment

Organizations that utilize a single cloud may be considering whether a solution that explicitly says, “for Multicloud”, can provide value and would fit their business requirements. This section seeks to explain the business and technical value that the solution provides for organizations that are currently utilizing only one cloud.

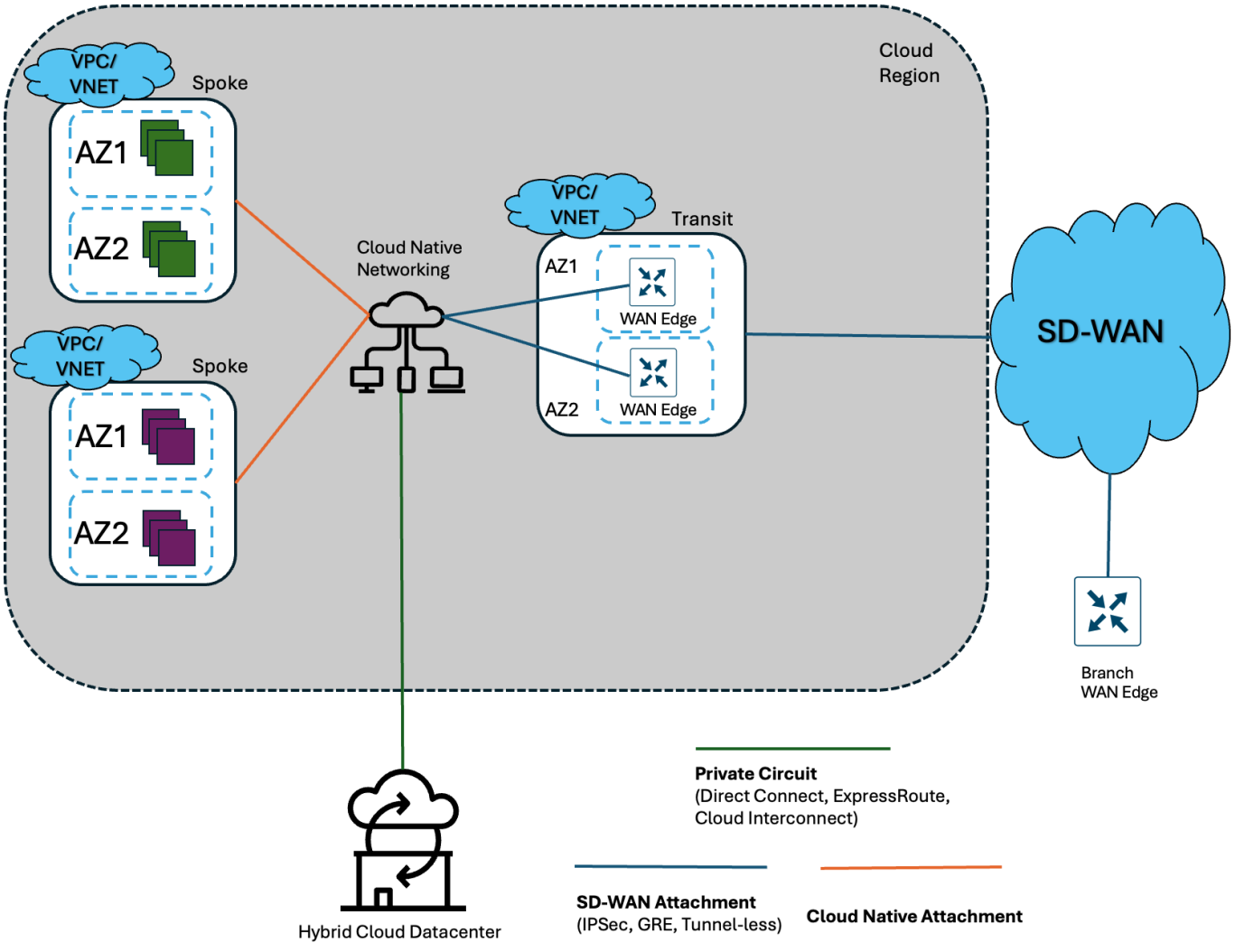

Figure 4. SD-WAN Cloud OnRamp for Multicloud Deployment for Single Cloud

Deploying a Cloud Gateway into a single cloud provides all the benefits of an SD-WAN deployment, allowing SD-WAN policy and security in both north-south and east-west traffic flows.

Benefits:

- Automated deployment of greenfield cloud-native network constructs and connectivity using cloud SD-WAN Edge Routers
- Support for brownfield integration with currently deployed native cloud constructs using cloud SD-WAN Edge Routers
- End to end SD-WAN health and application visibility across any hybrid cloud transport used
- SD-WAN application-aware routing and reactivity to changing WAN conditions regardless of underlying hybrid cloud transport
- Orchestrated segmentation of cloud resources and SD-WAN VPNs based on business intent utilizing a simple segmentation matrix
- Connectivity within and across regions with security and data policy in line with traffic flows

There are many benefits for organizations using the solution even in a single cloud to deploy Cloud Gateways. The largest one is the ability to extend and enforce SD-WAN data and security policy into the cloud itself and between cloud workloads, followed by the ability to orchestrate and enforce segmentation between both cloud resources and SD-WAN VPNs.

SD-WAN Cloud Onramp for Multicloud: Multicloud Deployment

Organizations utilizing multiple clouds will benefit from all the technical and business value previously discussed in every cloud but will also enjoy the added benefit of being able to intelligently connect clouds together if required and can enforce the same SD-WAN data and security policy across multiple clouds irrespective of each cloud's limitations.

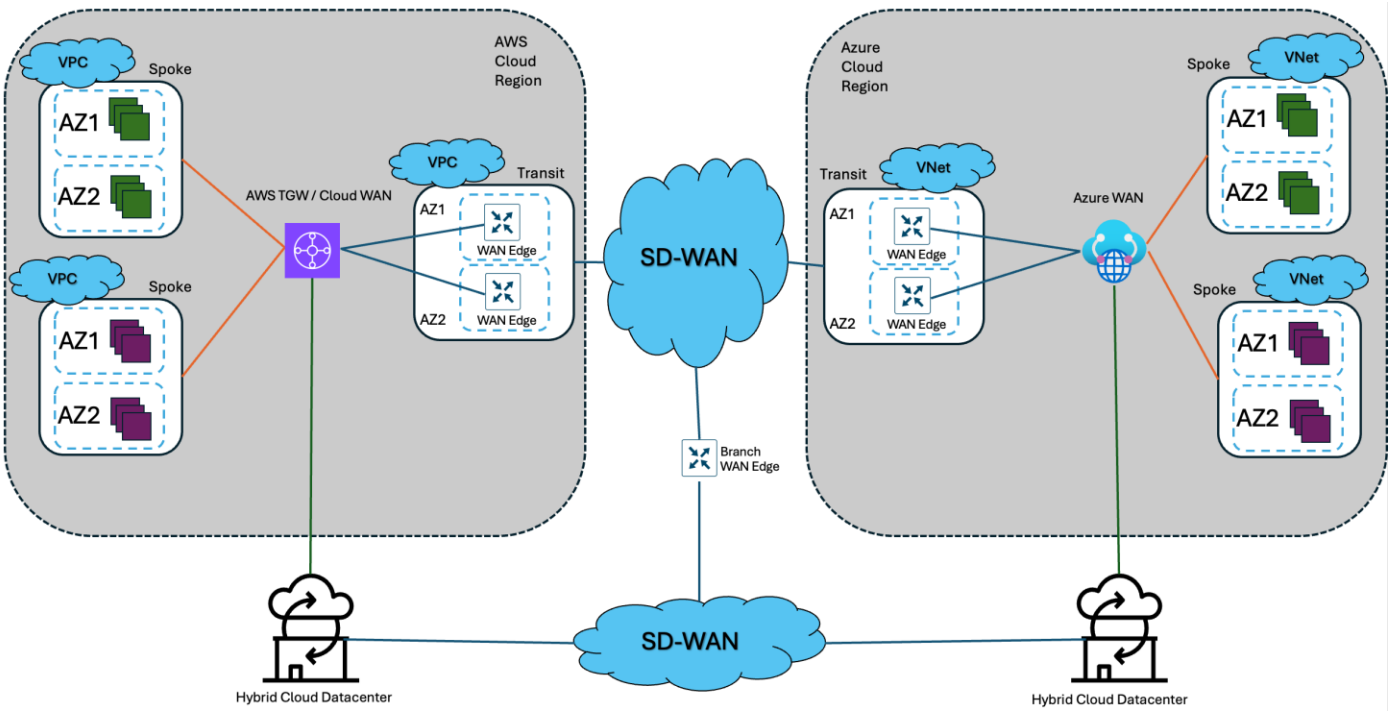

Figure 5. Cisco SD-WAN Cloud OnRamp for Multicloud Deployment in Multiple Clouds

Deploying Cloud Gateways into multiple clouds provides all the benefits of an SD-WAN deployment, allowing SD-WAN policy and security in both north-south and east-west traffic flows within or between any cloud.

Benefits:

- The same SD-WAN data and security policy can be enforced in different cloud environments, overcoming native cloud limitations and differences
- Traffic between clouds can use the best path per application-aware policy or be intelligently steered to lower cost hybrid connectivity however the business intent dictates
- SD-WAN operators and architects do not have to become experts in each cloud to facilitate network deployments that will connect multiple clouds to data centers or each other

In addition to the benefits of a single cloud deployment, a multicloud deployment allows organizations to leverage their SD-WAN to connect workloads in and between different clouds using the best possible transport. Organizations regularly use traffic engineering to engineer traffic between clouds to use private circuits between clouds, taking advantage of the lower costs associated rather than paying Internet egress fees to transfer data between them.

Cisco SD-WAN Cloud Onramp for Multicloud: Cloud Interconnect

Organizations utilizing middle mile colocation providers for connectivity can benefit from adopting the SDCI (Software-Defined Cloud Interconnect) workflow. This workflow allows an organization to utilize cloud provider private circuits from Equinix and Megaport in a fully orchestrated fashion to extend an SD-WAN fabric into the cloud.

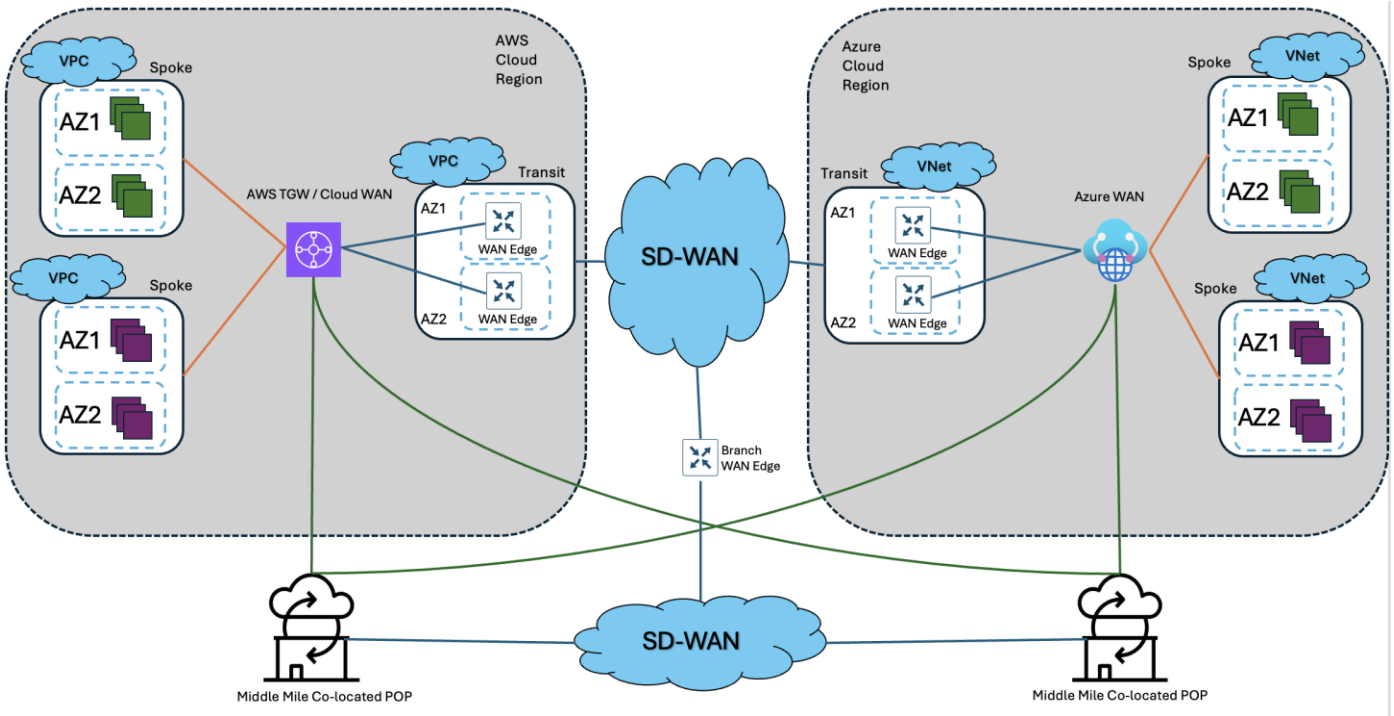

Figure 6. Cisco SD-WAN Cloud OnRamp for Multicloud Cloud Interconnect Deployment

Traditionally, hybrid cloud connectivity has been a mostly manual affair involving multiple vendor workflows and dashboards, stitching together end-to-end connectivity. With SDCI, the entire process can be

automated using SD-WAN Manager, allowing businesses to create seamless, fully encrypted fabrics across transports that are offered by different vendors and crossing different geographical locations.

Benefits:

- Fully automated orchestration of hybrid cloud connectivity across different geographical POPs and vendors as needed
- Middle-mile optimization that is simple and efficient without the need to manage disjointed vendor workflows and interfaces
- Agility to create and destroy these SDCI connections quickly and easily as business requirements change
- SD-WAN path telemetry and health monitoring without needing to correlate other vendor dashboard data

The primary benefit of Cloud Interconnect is the ability to abstract the complexity of building SD-WAN networks across multiple vendor solutions in a way that focuses on outcomes, not inter-operation. Connectivity between geographic locations utilizing middle-mile POP locations allows cost-effective traffic steering between different regions and clouds in an agile way. In minutes, complex networks can be built or destroyed based on the ever-changing needs of the business.

Cisco SD-WAN Cloud OnRamp for Multicloud Deployment Options by Cloud

This section will discuss the details of the architecture in each cloud that SD-WAN Cloud OnRamp for Multicloud deploys based on the business intent. There are many options available to support both new and existing cloud deployments. Many organizations utilize the appropriate workflow to match their overall cloud networking strategy; as always, it is important to understand the business requirements and ensure the deployment selected meets them. Importantly, all AWS use cases support both a site-to-cloud connectivity model between workloads in the cloud and on-prem, and a site-to-site connectivity model that uses the cloud as a backbone to connect users and workloads between sites.

AWS

AWS offers the most options for Cloud Gateway deployment due to the existence of both AWS Transit Gateway and AWS Cloud WAN, an AWS-managed global connectivity service. Organizations using either or both cloud native connectivity solutions will find most connectivity models supported. Integration is architecturally straight forward. This section will cover each integration option, including the strengths and caveats of each.

Tech tip: As of version 20.18, Cisco SD-WAN Cloud OnRamp for Multicloud Gateway can integrate with a brownfield, in-service AWS Transit Gateway or build a new one as part of the workflow. This brownfield integration does not yet extend to AWS Cloud WAN.

Tech tip: It is only possible to deploy one Cloud Gateway per AWS region, at the time of publishing this document

AWS Transit Gateway Connect using IPsec VPN

In this architecture, the Cloud Gateway consists of an AWS Transit Gateway integrated with a Transit VPC using IPsec VPN connectivity. The Transit VPC hosts a pair of WAN edges, each deployed in a different Availability Zone to build resiliency, and each SD-WAN Edge creates two IPsec VPNs to the AWS TGW for resiliency resulting in a total of four VPN connections, shown in Figure 7. below.

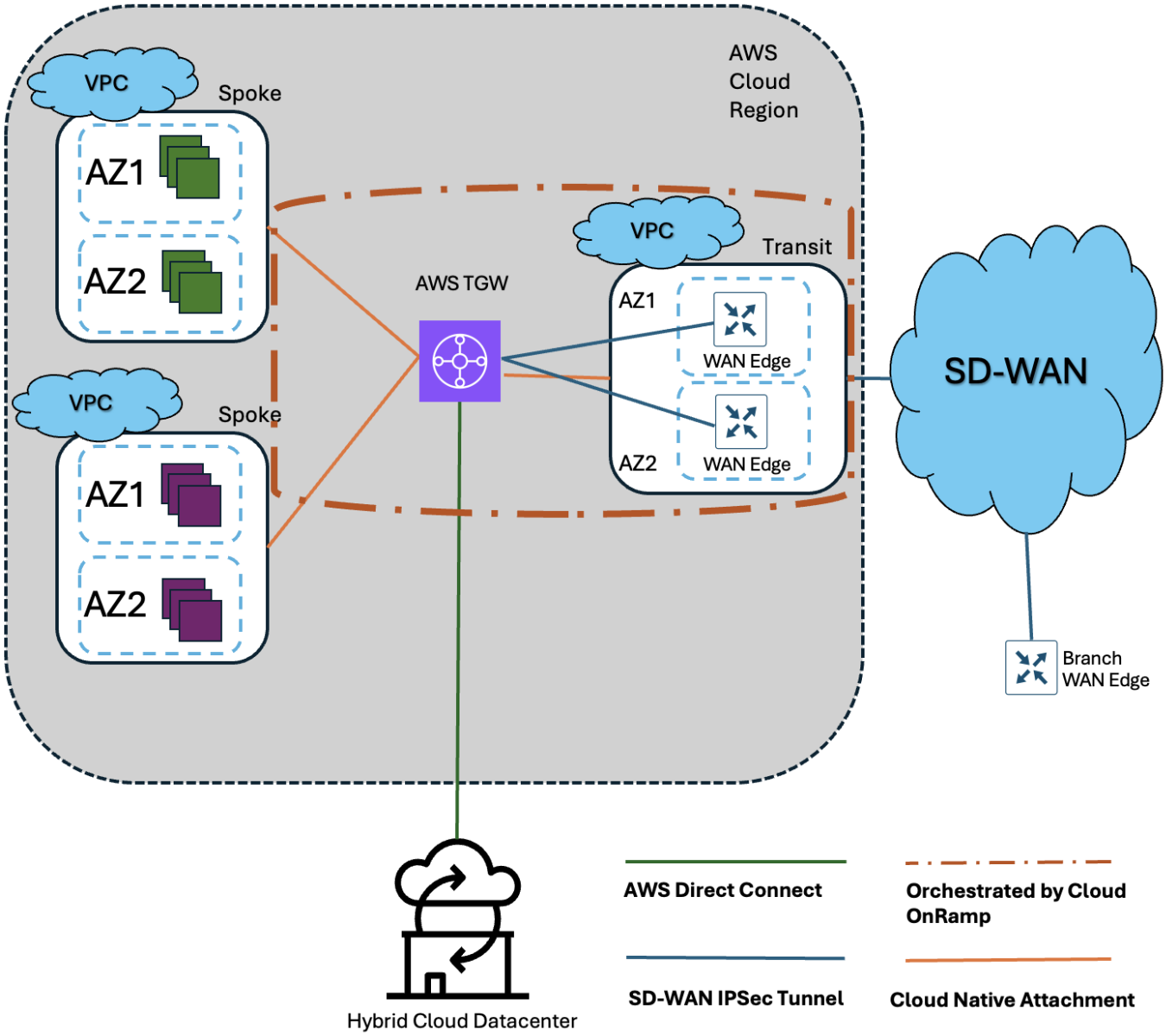

Figure 7. Cisco SD-WAN Cloud OnRamp for Multicloud AWS Transit Gateway IPSec Deployment

The benefit of this kind of integration is that encryption is maintained up to the AWS TGW and the resilient VPN tunnels are automatically orchestrated by SD-WAN Manager as part of the deployment. The drawback to this kind of deployment is the IPsec throughput limitations imposed per-tunnel, but in this deployment model, there are four IPsec tunnels for resiliency and increased throughput.

AWS Transit Gateway Connect using GRE Tunnels

In this architecture, an AWS Transit Gateway integrates with a Cloud Gateway Transit VPC using GRE tunnels, which AWS calls Transit Gateway Connect Peer. The architecture is similar to the IPSec VPN based solution above, with the added option to increase tunnel count up to four tunnels per VPN connection to increase bandwidth and resiliency.

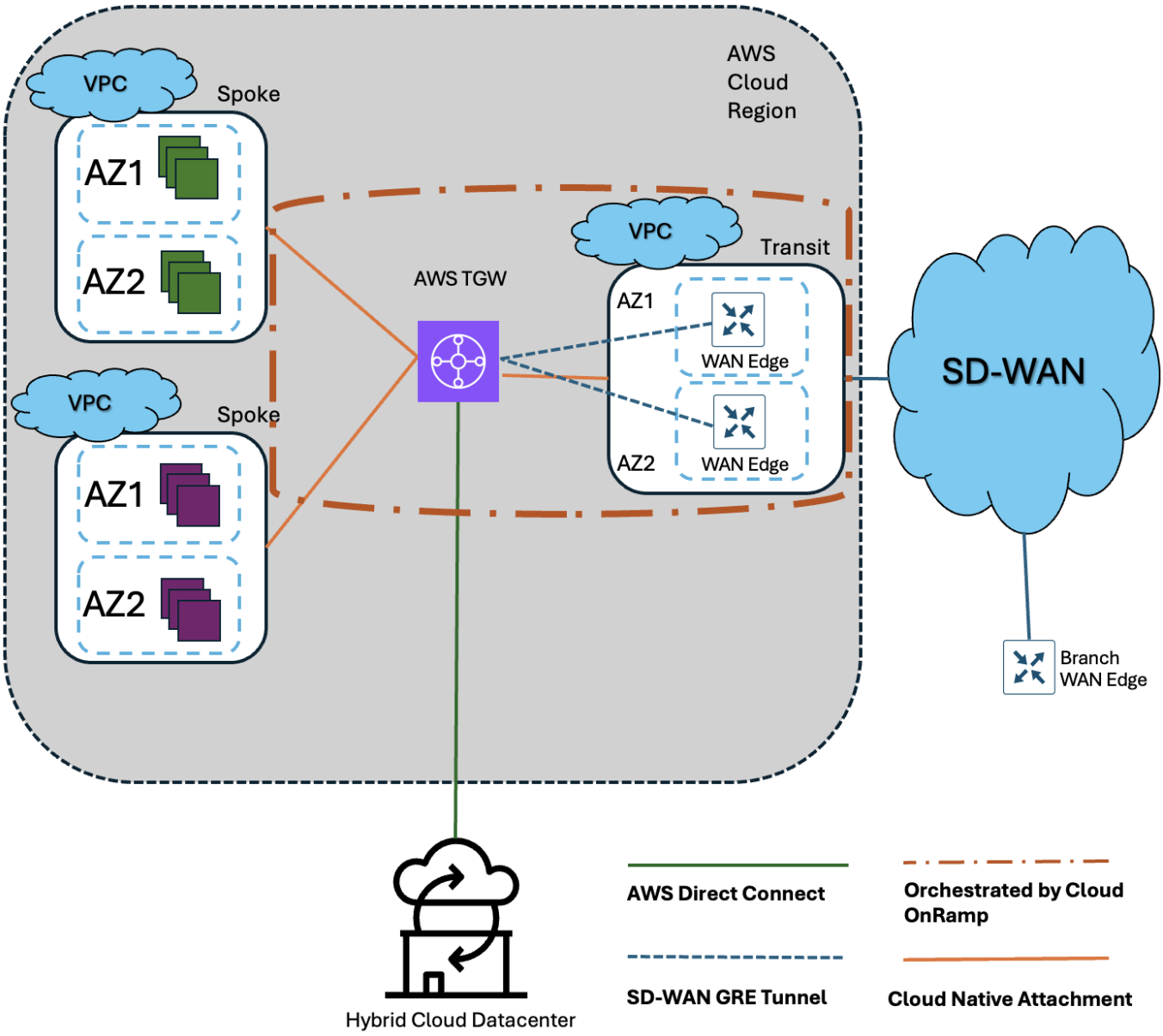

Figure 8. Cisco SD-WAN Cloud OnRamp for Multicloud AWS Transit Gateway Connect Deployment

The benefit of this kind of integration is that traffic throughput is greatly increased to AWS TGW and the resilient GRE tunnels are automatically orchestrated by SD-WAN Manager as part of the deployment. Another benefit is improved security because this option uses private IP addresses, which cannot be attacked from outside. The drawback to this kind of deployment is that the tunnels are not encrypted, which may be against organizational security requirements.

AWS Transit Gateway Connect using Branch Connect

In this architecture, a branch SD-WAN site connects directly with AWS Transit Gateway using IPsec tunnels to access cloud resources without deploying a Cloud Gateway. This connection is simple but is deployed on a per-site basis, which increases the amount of total IPsec tunnels attached to the AWS TGW and does not scale well. This deployment is best for small, single point solution connectivity requirements.

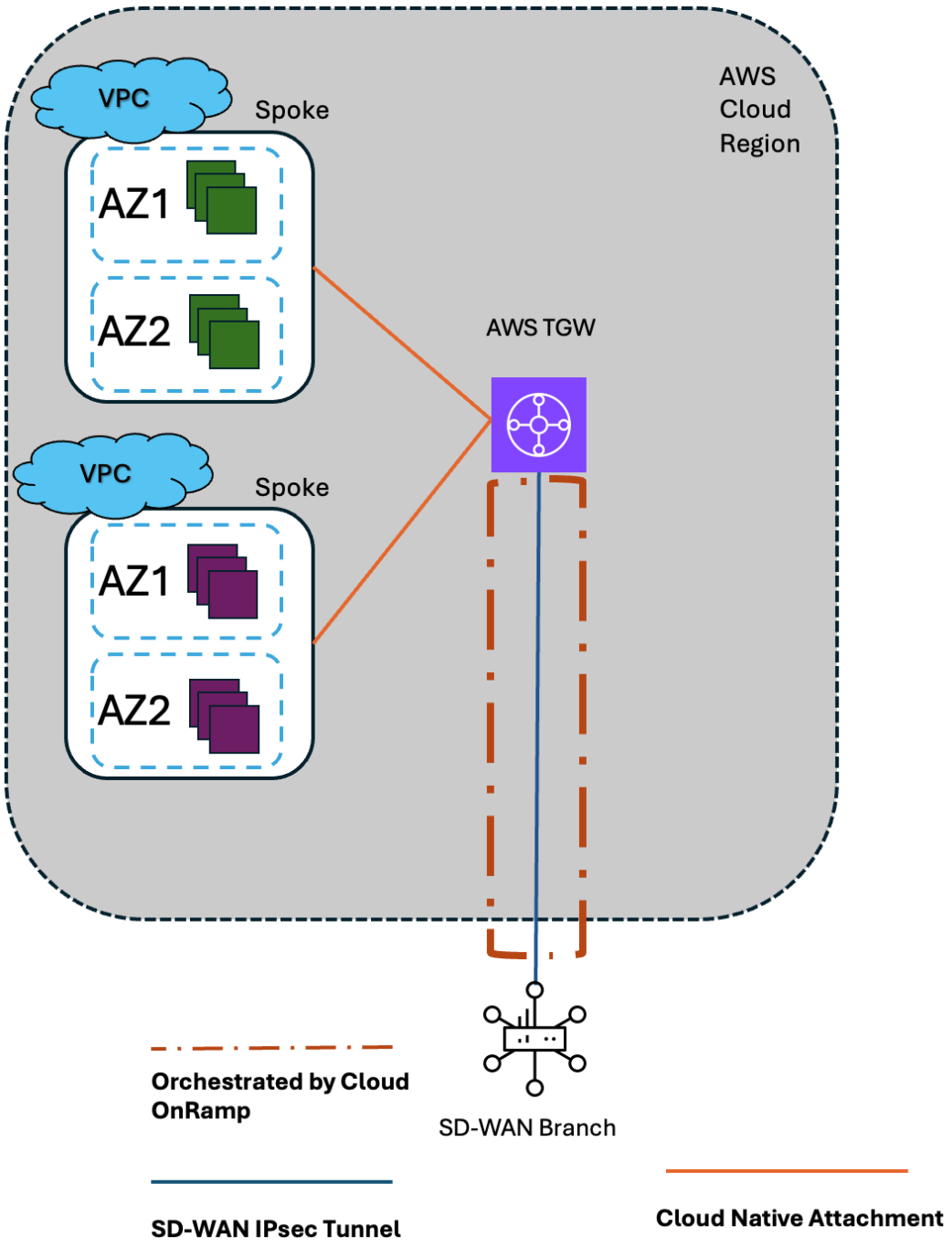

Figure 9. SD-WAN Cloud OnRamp for Multicloud AWS TGW Branch Connect Deployment

AWS Cloud WAN IPsec

In this architecture, AWS Cloud WAN integrates with a Cloud Gateway Transit VPC using IPsec VPN connectivity. Each SD-WAN Edge in the Cloud Gateway creates two IPsec VPN tunnels (one Cloud WAN VPN Attachment) to the AWS Cloud WAN CNE for resiliency resulting in a total of four VPN connections. This design is very similar to how Cloud Gateway does VPN attachments to an AWS Transit Gateway. Under the hood, AWS Cloud WAN is a managed TGW service that uses functionally similar architecture and routing constructs. Figure 10 shows that a native VPC attachment is made between the CNE and the

Transit VPC, and, using AWS Cloud WAN Tunnel-less Connect, the IPsec tunnels are built over the top of this connectivity to the CNE from the SD-WAN Cloud Gateway routers.

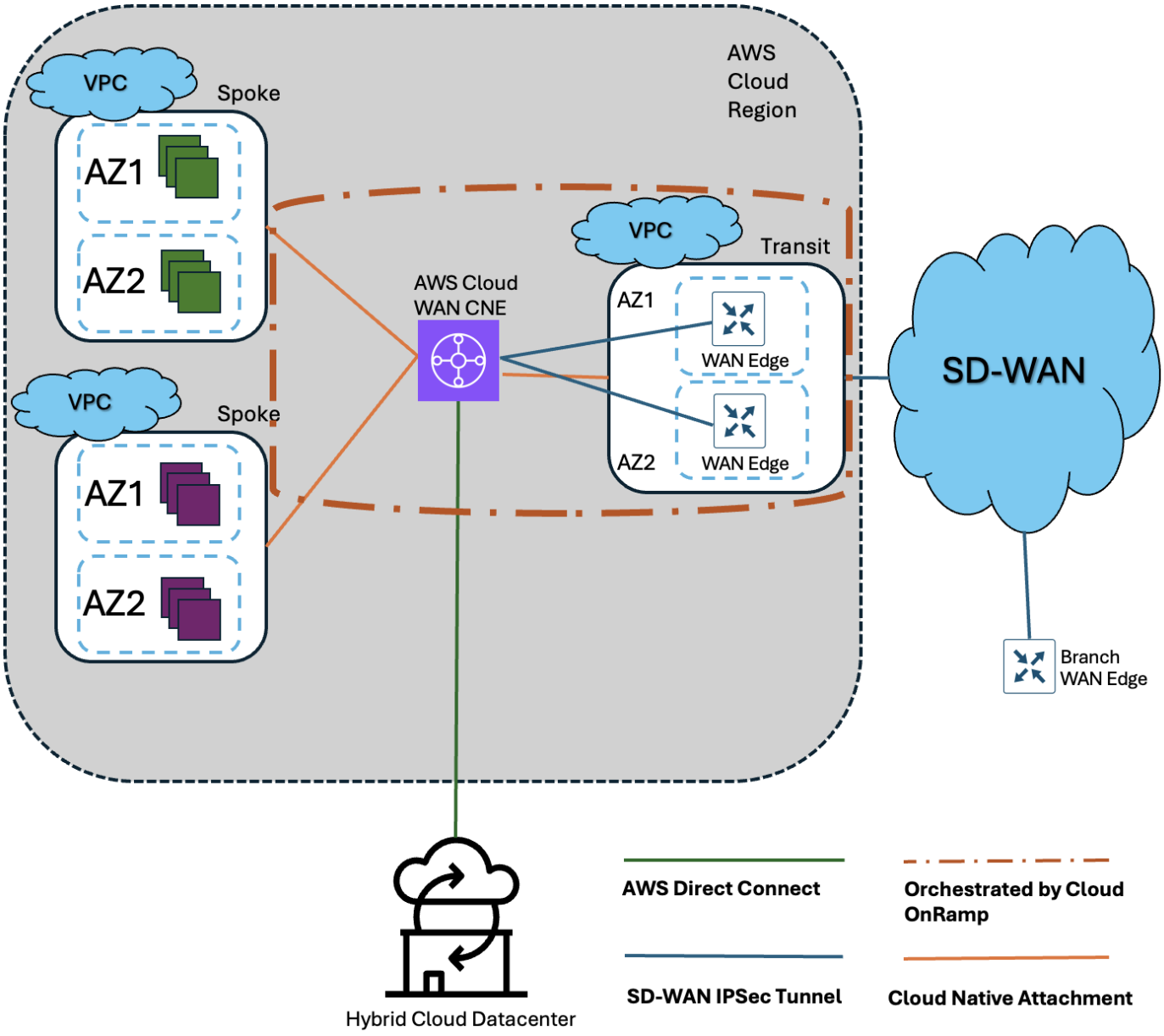

Figure 10. Cisco SD-WAN Cloud OnRamp for Multicloud AWS Cloud WAN IPsec Deployment

The major benefit of this type of Cloud WAN integration is that, as with Transit Gateway integration, encryption is maintained until the CNE. However, the use of IPsec tunnels, as discussed earlier, lowers the total throughput of data between a Cloud Gateway and the attached CNE. Use this option if there is a security mandate for this kind of connectivity and if the data throughput limitations are not a concern.

AWS Cloud WAN Connect

In this architecture, AWS Cloud WAN integrates with a Cloud Gateway Transit VPC using GRE tunnel connectivity. Each SD-WAN Edge in the Cloud Gateway creates between one and four (configurable) GRE tunnels to the AWS Cloud WAN Core Network Edge (CNE) for resiliency and increased throughput. This design is very similar to how Cloud Gateway does TGW Connect attachments to an AWS Transit Gateway.

Under the hood, AWS Cloud WAN is a managed TGW service that uses functionally similar architecture and routing constructs.

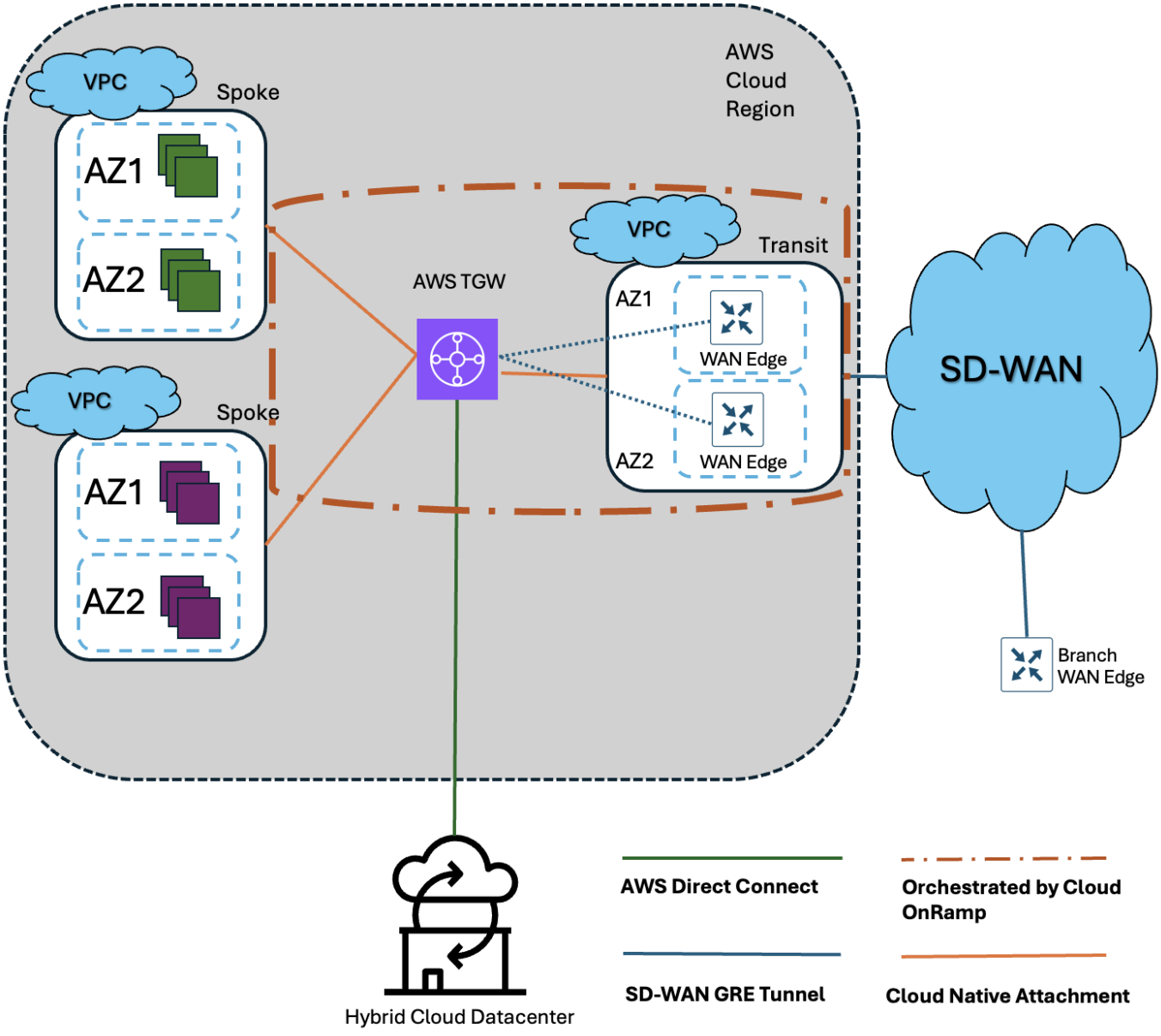

Figure 11. Cisco SD-WAN Cloud OnRamp for Multicloud AWS Cloud WAN GRE Deployment

The major benefit of this type of Cloud WAN integration is that, as with Transit Gateway integration, traffic throughput is maintained to the CNE. However, because GRE is not encrypted, there is a lack of enforced encryption between the SD-WAN Cloud Gateway and CNE. Use this option if there is not a security mandate and if traffic throughput is most important.

AWS Cloud WAN and Transit Gateway - Multi-region / site-to-site connectivity

Cloud OnRamp also supports multi-region / site-to-site deployment with AWS Cloud WAN and Transit Gateway which focuses on using SD-WAN Cloud Gateways configured in different regions of AWS. Transit Gateway-based deployments use full mesh peering of the Transit Gateways, while Cloud WAN-based deployments maximize throughput through the use of AWS Cloud WAN Tunnel-less Connect attachments

Tech tip: AWS Cloud WAN Tunnel-less Connect is only used when the Transit Full Mesh option is selected when deploying the Cloud Gateway. The Tunnel-less Connect connectivity is centered around SD-WAN site-to-site (east-west) connectivity and not connectivity to cloud workloads.

An example multi-region AWS Cloud WAN Site-to-Site deployment is shown in Figure 12:

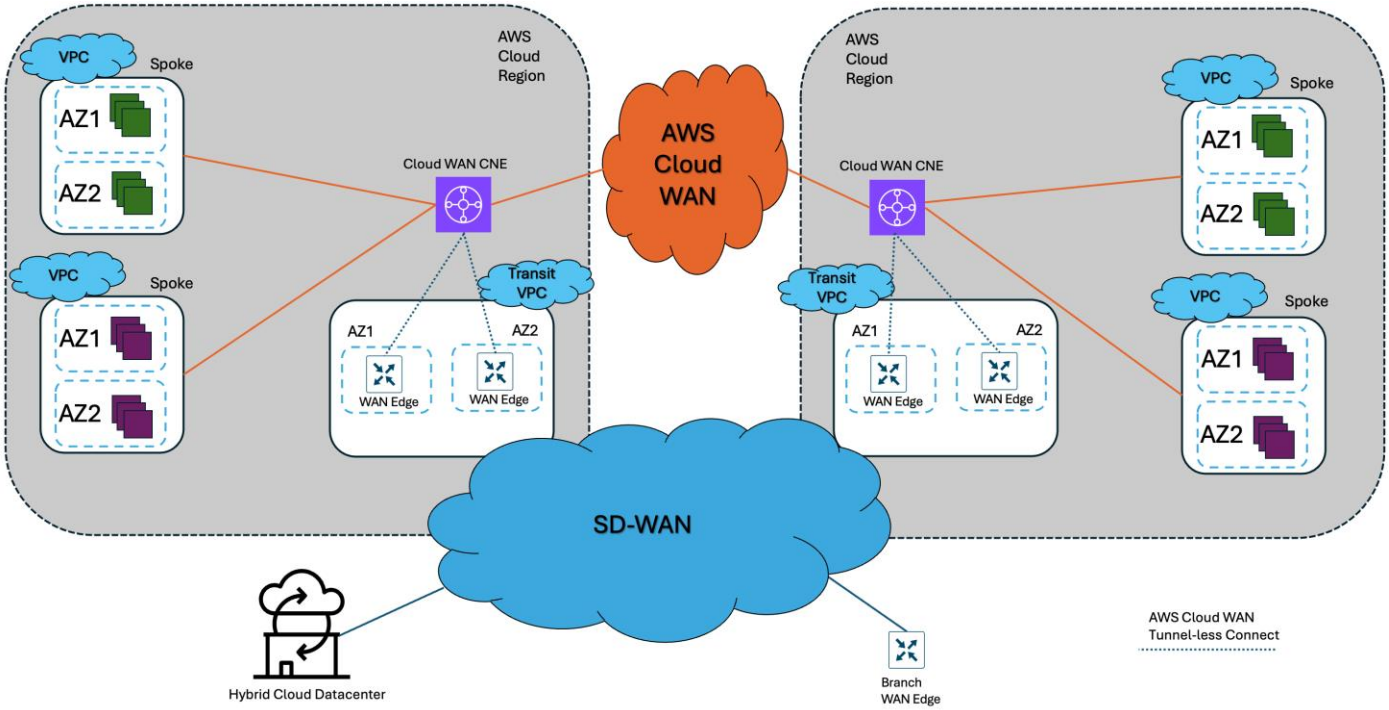

Figure 12. Site-to-Site with AWS Cloud WAN Tunnel-less Connect

Solution	IPsec	GRE	Site-to-cloud connectivity	Site-to-site connectivity	Optimized For:
AWS Transit Gateway	X	X	X	X	Regional Connectivity
AWS Cloud WAN	X	X	X	X	Global Connectivity
AWS Branch Connect	X		X		Point Connectivity

Table 1. AWS Cloud OnRamp for Multicloud Solution Matrix

Tech tip: Once Cloud Gateway has been deployed within AWS, all policy and intent should be configured from SD-WAN Manager to avoid configuration drift and audit alarms. It is not advisable to configure route policy and route tables for attached native constructs such as TGW and Cloud WAN for anything that connects to SD-WAN.

Tech tip: If something changes with Cloud WAN policy outside of the Cloud OnRamp workflow, it is possible to re-push the intent from SD-WAN Manager under the Multicloud section In Gateway Management. This will reset the policy to match the declared intent.

Microsoft Azure

The Cisco SD-WAN Cloud OnRamp for Multicloud design extends the Cisco Catalyst SD-WAN fabric to Microsoft Azure through integration with Azure Virtual WAN (vWAN). A vWAN is a global construct within Azure, representing the overall network deployment. Within the vWAN, there can be multiple virtual hubs (vHubs) per Azure region. A vHub is a special transit virtual network (vNet) managed by Azure. Since the vHub is completely managed by Azure, IP addresses are dynamically assigned by Azure based upon the address space specified when the vHub is instantiated. Azure automatically partitions the vHub IP address space for each of the subnets needed within the vHub itself.

Host vNets connect via vNet peering connections to a vHub within their Azure region. Host vNet connectivity between Azure regions can be provided through a combination of vHubs with vNet peering within each region, along with vHub-to-vHub peering between regions within the overall vWAN. The Azure vWAN design therefore provides scalable connectivity between host vNets within an Azure region and between regions.

Azure Virtual WAN is architecturally different from the AWS Transit Gateway. Where AWS uses Transit Gateway as a point of connectivity aggregation in which management of each TGW is disaggregated (unless using AWS Cloud WAN), Azure vWAN takes an approach of providing point connectivity into an aggregated fabric of cloud native route propagation.

Functionally, this does not significantly impact how Cisco Catalyst SD-WAN integrates with Azure vWAN, but it is important to understand the different philosophy to appreciate how traffic flows may differ and what connectivity options exist in Azure. Integration is architecturally straight forward; it can be done by deploying Cloud Gateway with NVA (SD-WAN Routers) or via IPsec VPN directly, like AWS Branch Connect. This section will cover both integration options, including the strengths and caveats of each.

Tech tip: Not all Azure regions support vHubs. A full list can be found here by searching for “Virtual WAN” in the Product Availability table: https://azure.microsoft.com/en-us/explore/global-infrastructure/products-by-region/table

Azure vHub with Cloud Gateway NVA

In this architecture, Azure vWAN integrates with a Cloud Gateway using IPsec tunnel connectivity. The vWAN Hub in each region serves as a cloud native connection point into the Azure networking fabric. The Cloud Gateway SD-WAN routers are deployed as network virtual appliances (NVAs) inside the vHubsand use BGP to exchange routes. The architecture is depicted in Figure 13:

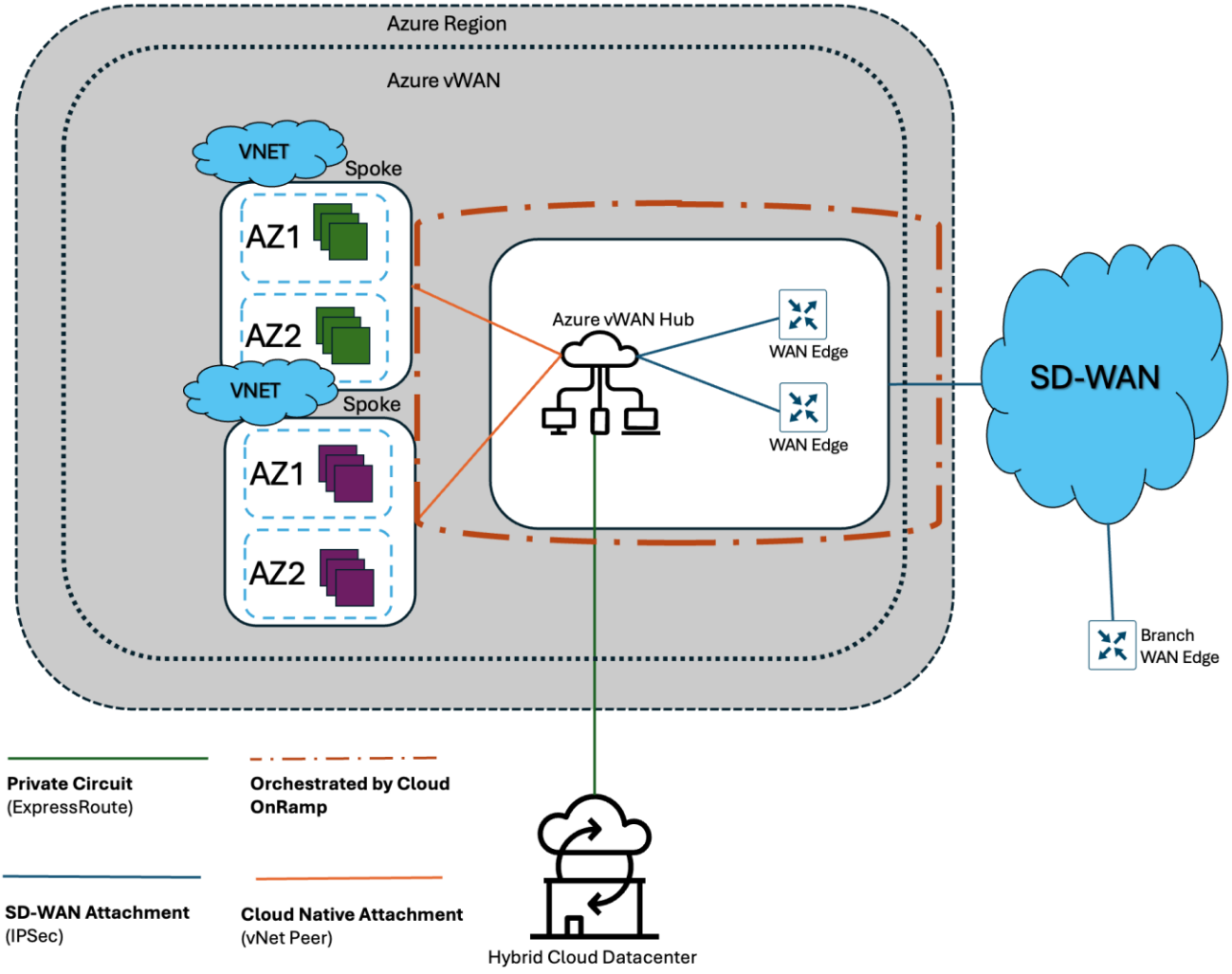

Figure 13. Cisco SD-WAN Cloud OnRamp for Multicloud Azure vWAN with NVA Deployment

The major benefit of this type of vWAN integration is that routing intent and route exchange can be aggregated from the SD-WAN into Azure instead of building ad-hoc routing connectivity on a per-site basis. This is most useful if the organization has a lot of users and sites that require connectivity to Azure workloads, but there may be a requirement to more effectively exchange routes from and to Azure's cloud network fabric. By deploying SD-WAN routers as NVA into Azure's cloud and peering with the vHub, route exchange and traffic control is much easier to aggregate and control from a central management plane.

Azure vHub with Cloud Gateway NVA - Multi-region / site-to-site connectivity

One of the benefits of using Azure vWAN with Cisco SD-WAN Cloud OnRamp for Multicloud is how simple it is to connect multiple Azure regions together and leverage the Azure cloud backbone for multi-region / site-to-site connectivity when desired. An example multi-region deployment is shown in Figure 14 below:

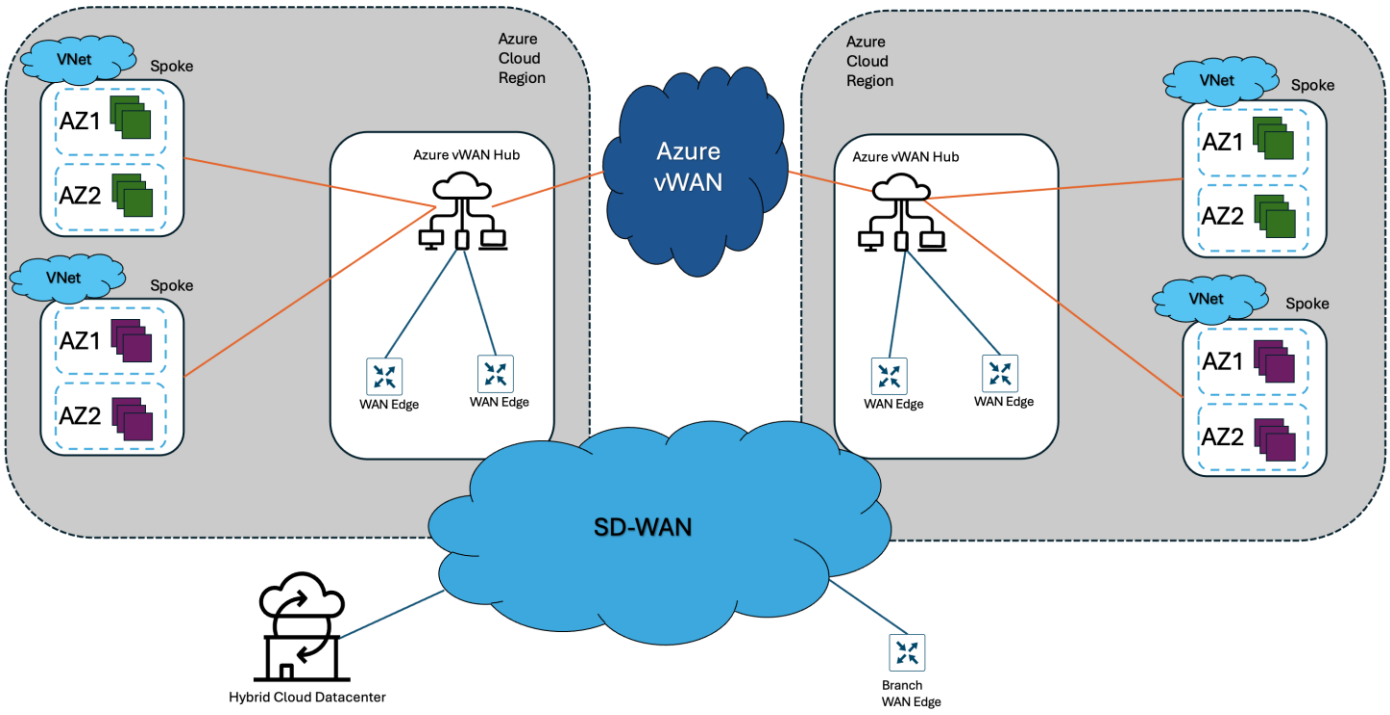

Figure 14. Azure vWAN Multi-region Deployment with Cisco SD-WAN Cloud Gateway

Tech tip: Catalyst 8000V routers functioning as NVAs within the Azure vHub support only one service-side interface (GigabitEthernet2). This service-side interface must be assigned to a single service VPN. eBGP peering is established from the service-side interface of each of the Catalyst 8000v SD-WAN routers to the internal router/route server within the vHub. Routes learned via the eBGP peering are automatically mapped to the default route table of the Azure vHub. Hence, for connectivity, all host vNets mapped to the Cloud Gateway are also assigned to the default route table of the Azure vHub. Please note that this is a cloud-side limitation and not a limitation of Catalyst 8000V.

Azure vHub with IPsec VPN

In this architecture, Azure vWAN integrates directly with SD-WAN sites using IPsec tunnels as a site-to-site VPN connection. The vWAN Hub in each region serves as a cloud native connection point into the Azure networking fabric. This approach is more disaggregated and ad-hoc, like the AWS Branch Connect option. The architecture is depicted in Figure 15:

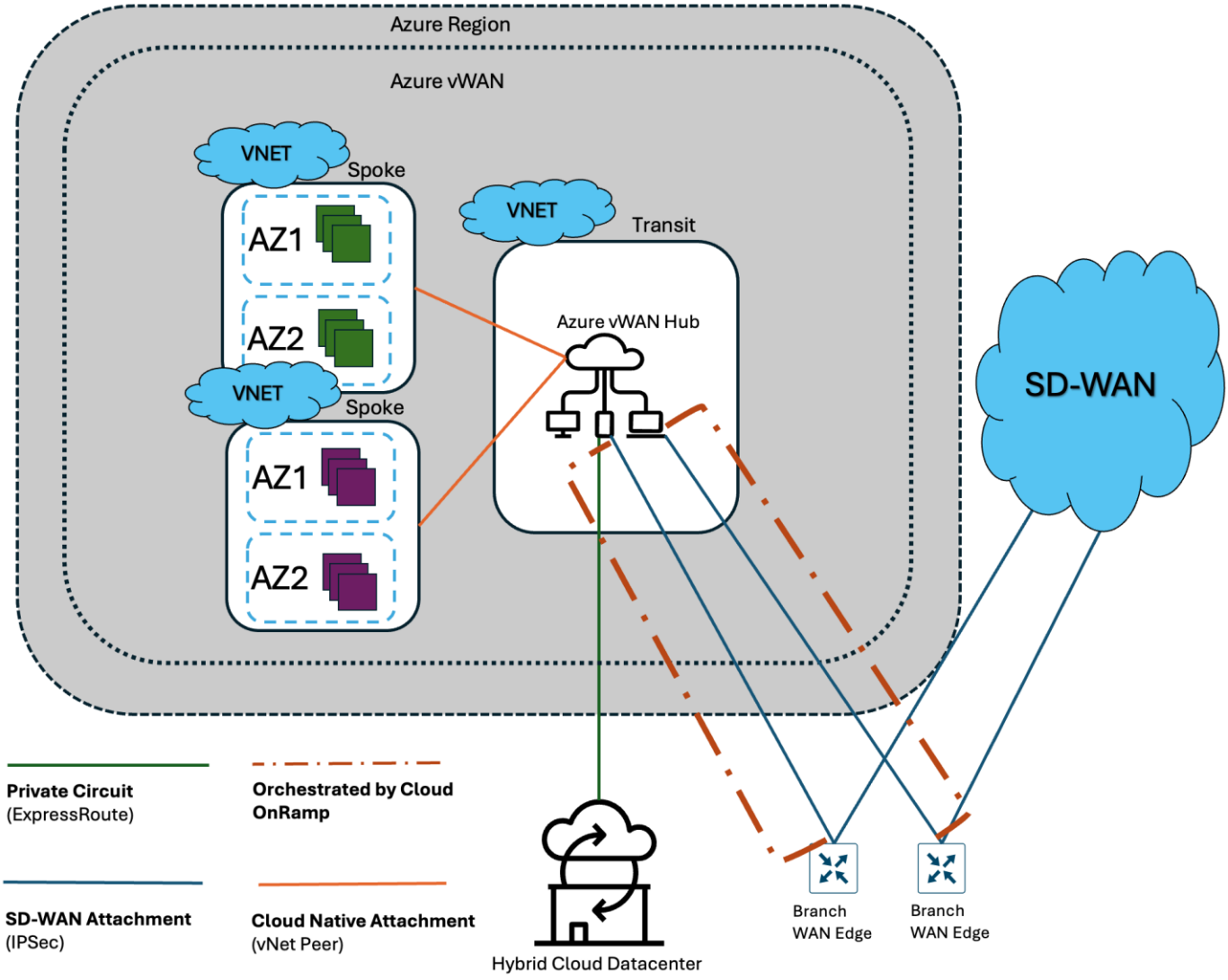

Figure 15. Cisco SD-WAN Cloud OnRamp for Multicloud Azure vWAN with IPsec Deployment

The major benefit of this type of vWAN integration is that connectivity is ad-hoc and disaggregated, which is advantageous if the organization requires only specific sites to access Azure workloads. It is simple to instantiate due to it being a simple site-to-site IPsec VPN solution that includes BGP for route exchange. This solution would not be preferred if there are many sites that need connectivity to Azure workloads as it increases operational overhead in deployment and management of each connection.

Google Cloud

Google Cloud integration with Cisco Catalyst SD-WAN focuses on two potential outcomes: Connecting organizations to Google Cloud resources or using Google Cloud to provide a cloud-based backbone to connect sites together. Integration is architecturally straight forward. This section will cover both integration options, including the strengths and caveats of each.

Tech tip: The diagrams below show a simplified deployment for Google Cloud for ease of understanding. Google Cloud requires that each NVA interface be connected to a different VPC, so each SD-WAN router interface is in a different VPC; what is displayed is the logical, effective result of this.

Google Cloud WAN with Site-to-Cloud Deployment

In this architecture, Google Cloud WAN integrates with a Cloud Gateway Transit VPC using IPsec tunnel connectivity. The SD-WAN routers are deployed in a global VPC in selected regions, serving as a connection point into Google Cloud. The Cloud Gateway SD-WAN routers build redundant IPsec tunnels to Google Cloud Router and use BGP to exchange routes. The architecture is depicted in Figure 16:

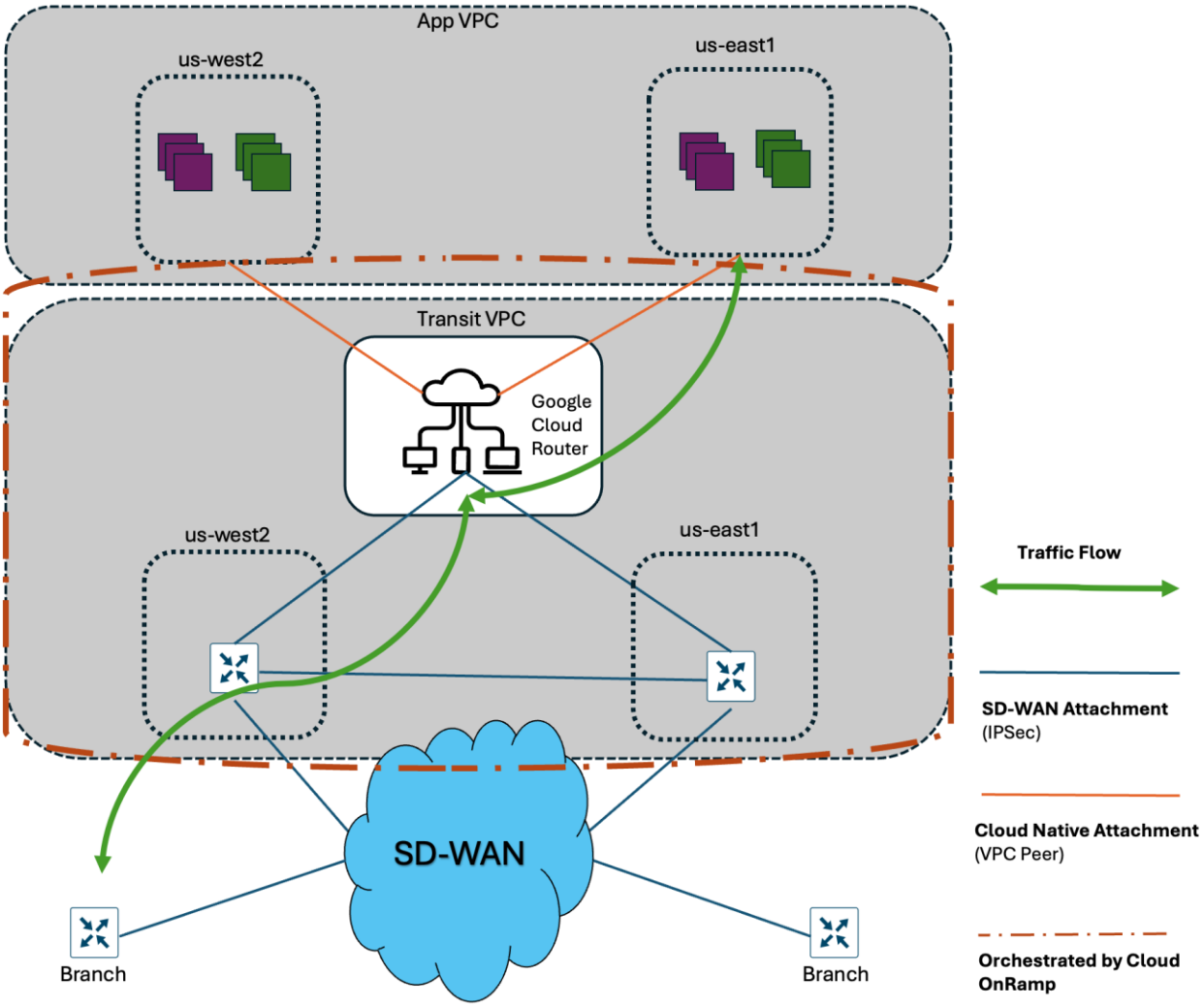

Figure 16. Cisco SD-WAN Cloud OnRamp for Multicloud Google Cloud S2C Deployment

In this use case, SD-WAN routers are being used to integrate with NCC in a manner similar to the AWS and Azure deployments. Users access cloud applications and data over the SD-WAN, and native cloud constructs are integrated on the back end with the SD-WAN fabric. The SD-WAN Cloud OnRamp for Multicloud workflows allow seamless and automated deployment for this purpose.

Google Cloud WAN with Site-to-Site Deployment

In this architecture, Google Cloud WAN integrates with a Cloud Gateway Transit VPC using IPsec tunnel connectivity. The SD-WAN routers are deployed in a global VPC in each region, serving as a connection point into Google Cloud. The Cloud Gateway SD-WAN routers build redundant IPsec tunnels to Google Cloud Routers and use BGP to exchange routes. The architecture is depicted in Figure 17:

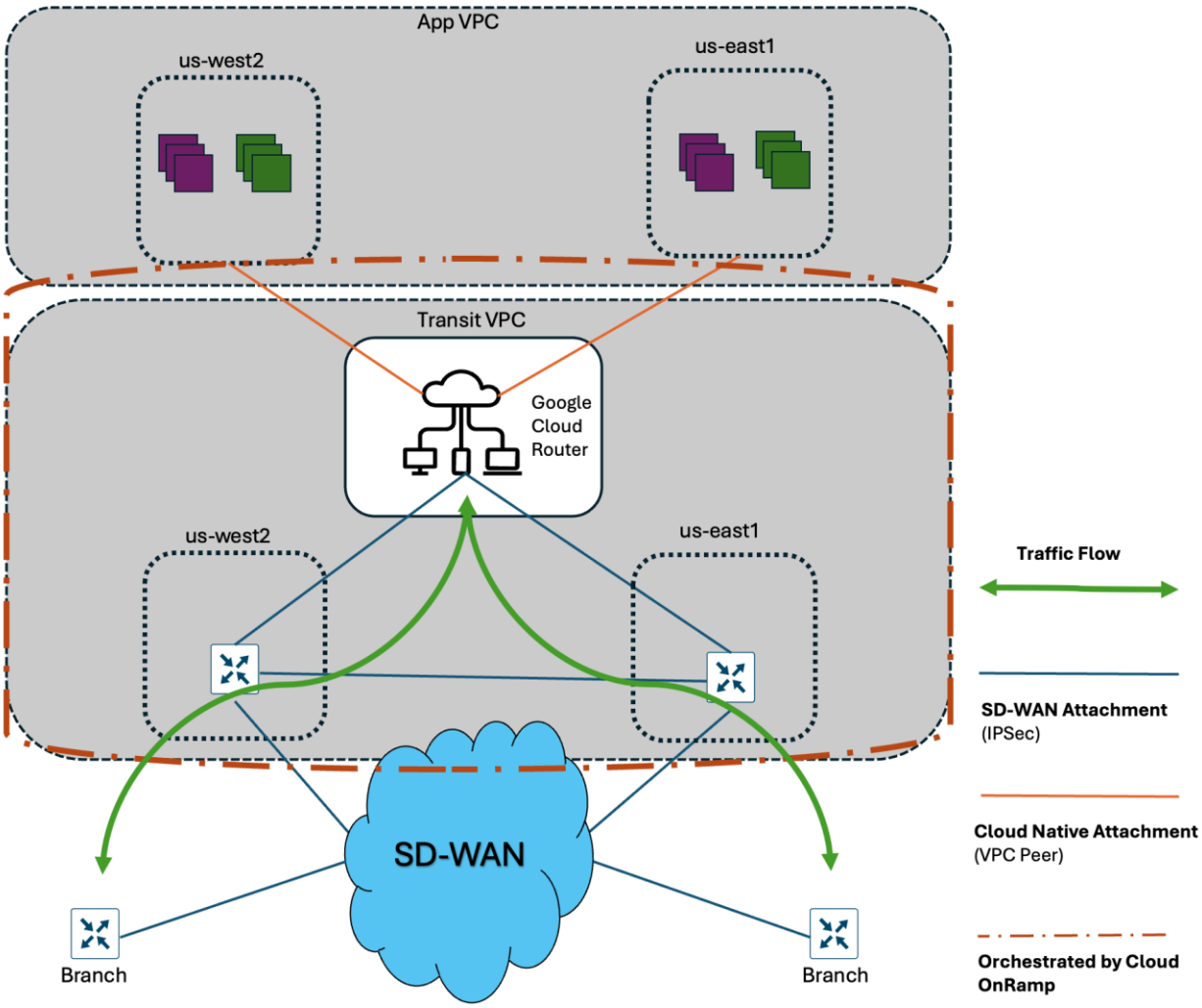

Figure 17. Cisco SD-WAN Cloud OnRamp for Multicloud Google Cloud WAN S2S Deployment

It's not a mistake that these diagrams are the same; the architecture of this use case is the same. The major difference in this type of deployment is that in the previous use case, the main traffic flow was a user-to-cloud application flow, and the integration focused on this. For the site-to-site use case, the main goal is to leverage Google's cloud backbone to connect sites together across geographies. This is made simpler by the Google Cloud Global VPC construct that simplifies connecting regions, but even with this use case, the integration with NCC is preserved, so organizations can also (if desired) connect to cloud workloads as well.

Cisco SD-WAN Cloud OnRamp for Multicloud: Options for Existing Cloud Networks

AWS

In version 20.18, Cisco SD-WAN Cloud OnRamp for Multicloud added the ability to integrate with existing AWS Transit Gateways as part of the workflow. This was technically possible before, but it has now been added to the UI and API as a workflow item. This capability allows organizations to integrate with a deployed cloud network, utilizing TGW without interrupting or impacting current deployments. The rest of the AWS Cloud Gateway is deployed as normal.

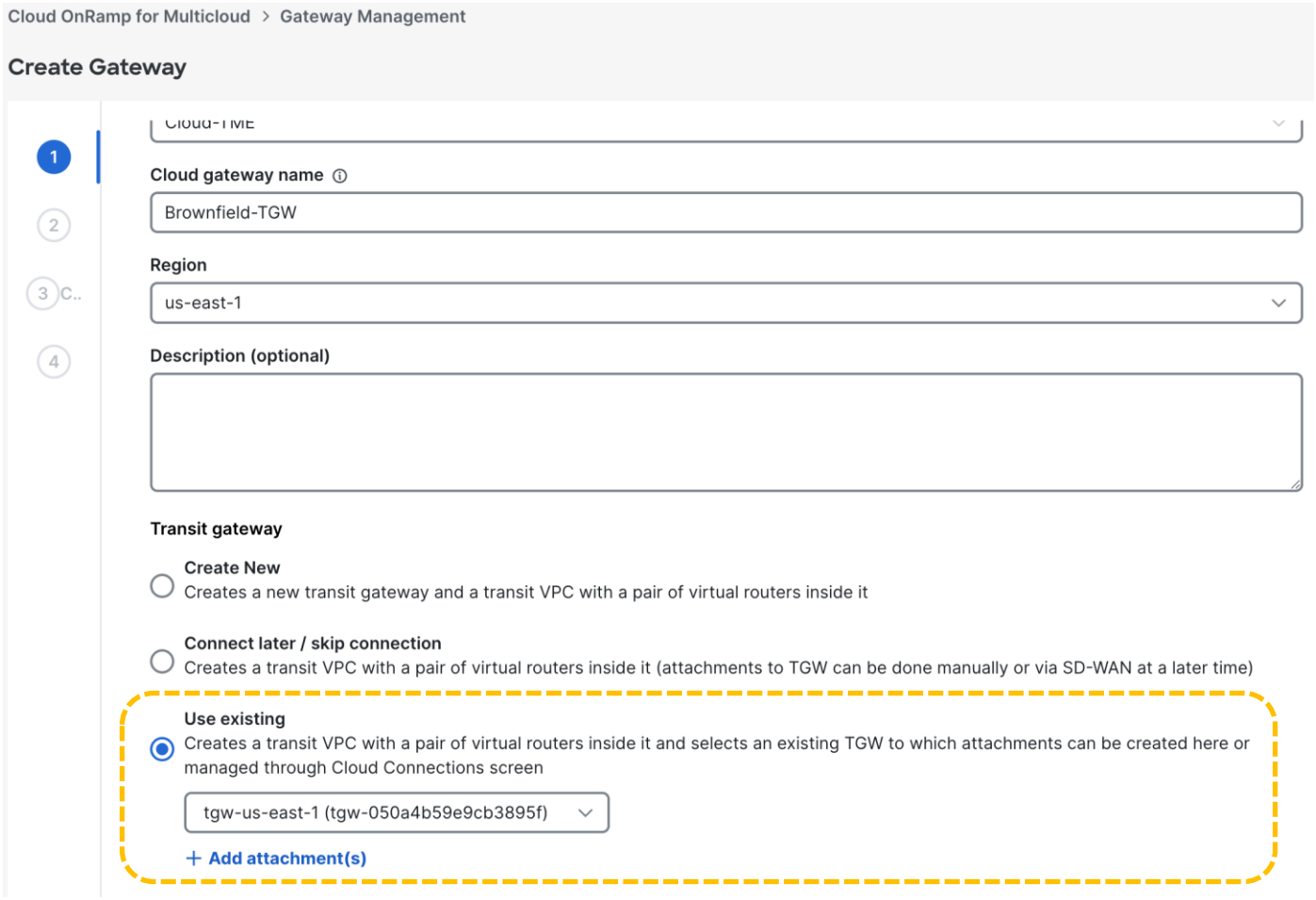

Figure 18. Using existing Transit Gateways when creating a Cloud Gateway in AWS

Tech tip: When the existing Transit Gateway is integrated with Cloud Gateway, future changes should be initiated from the SD-WAN Manager to ensure there is parity and synchronization.

Tech tip: Currently, this existing network integration workflow does not extend to AWS Cloud WAN

Azure

Cloud Gateway can be integrated with an existing Azure vWAN via the normal Cloud Gateway Azure deployment workflow. In this case, instead of providing a new name for an Azure vWAN, organizations can provide the name of a currently deployed vWAN, and the Cloud Gateway workflow will utilize the currently deployed vWAN instead.

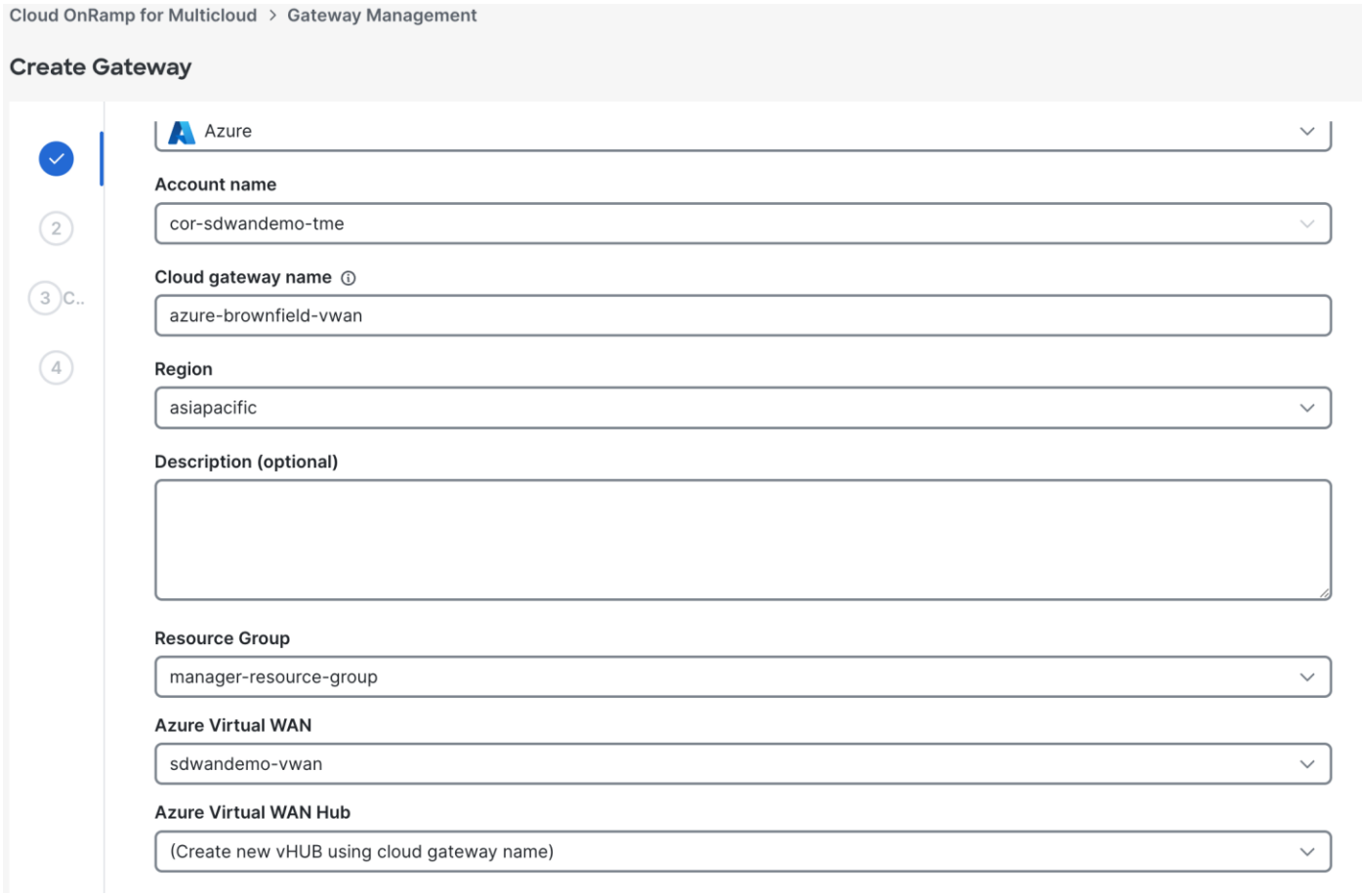

Figure 19. Using existing Virtual WANs when creating a Cloud Gateway in Azure

Google Cloud

There is not currently a GUI or API workflow for integrating Cloud Gateway with a brownfield NCC in Google, however, this can be manually implemented by the UI or API by building manual IPsec tunnels to a brownfield NCC and configuring the NCC according to Google's instructions for integrating with third-party network virtual appliances. Workflow integration with brownfield Google deployments is the subject of investigation for future SD-WAN enhancements.

Cisco SD-WAN Cloud OnRamp for Multicloud Segmentation Options by Cloud

Overview

One of the most powerful capabilities unlocked by using the SD-WAN Cloud OnRamp for Multicloud workflow is in automated orchestration of network segmentation between cloud workloads and SD-WAN VPNs. The process takes three high-level steps:

Step 1. Define Cloud tags for workloads at the VPC/VNet level to be used as segmentation criteria

Step 2. Specify Tag-to-VPN Mappings with business intent

Step 3. Realize intent by pushing policy, which orchestrates route tables and route leaking, providing connectivity to the specified workloads and VPNs

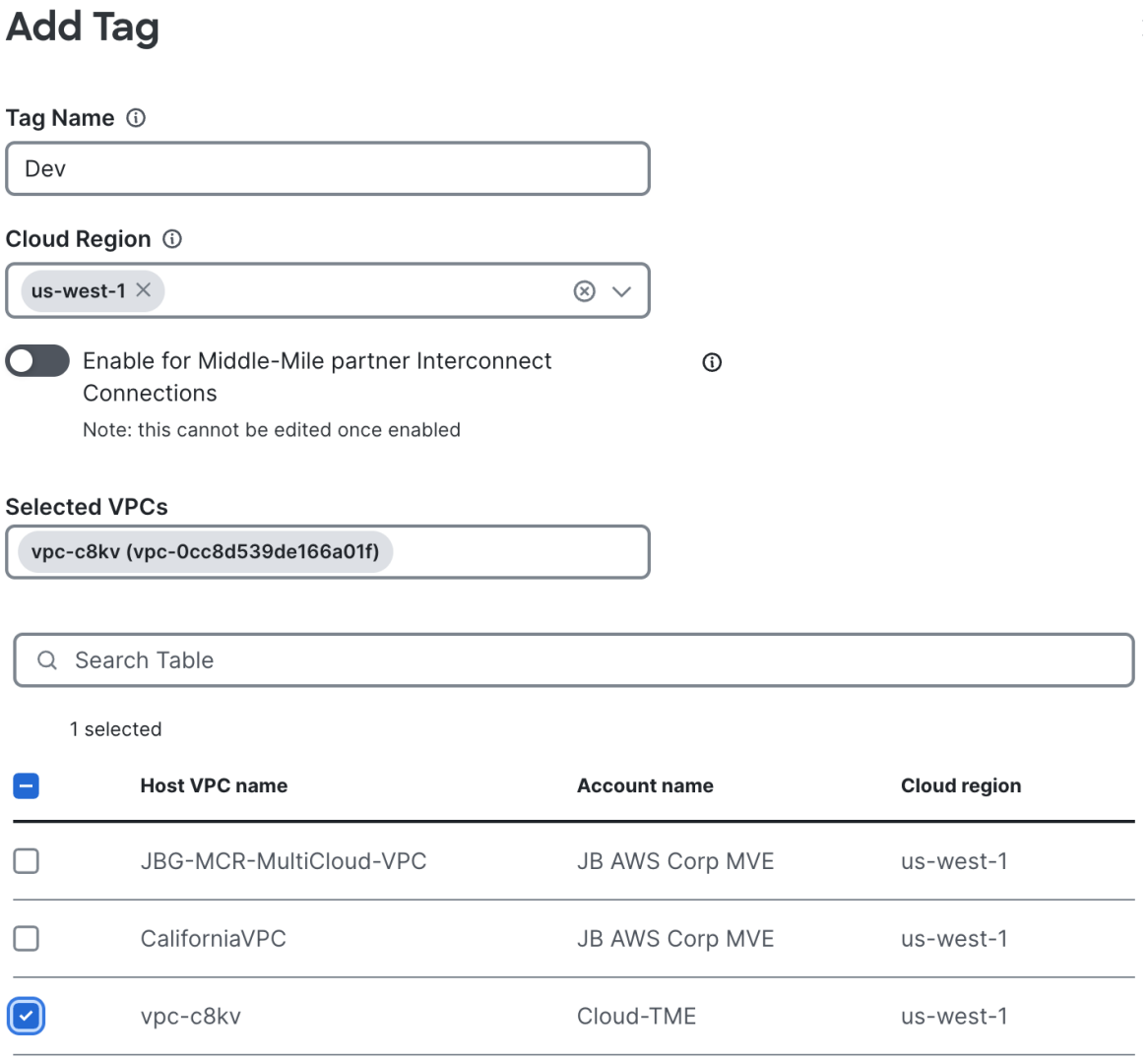

Figure 20. Definition of Cloud Tags for VPCs and VNets in Catalyst SD-WAN Manager

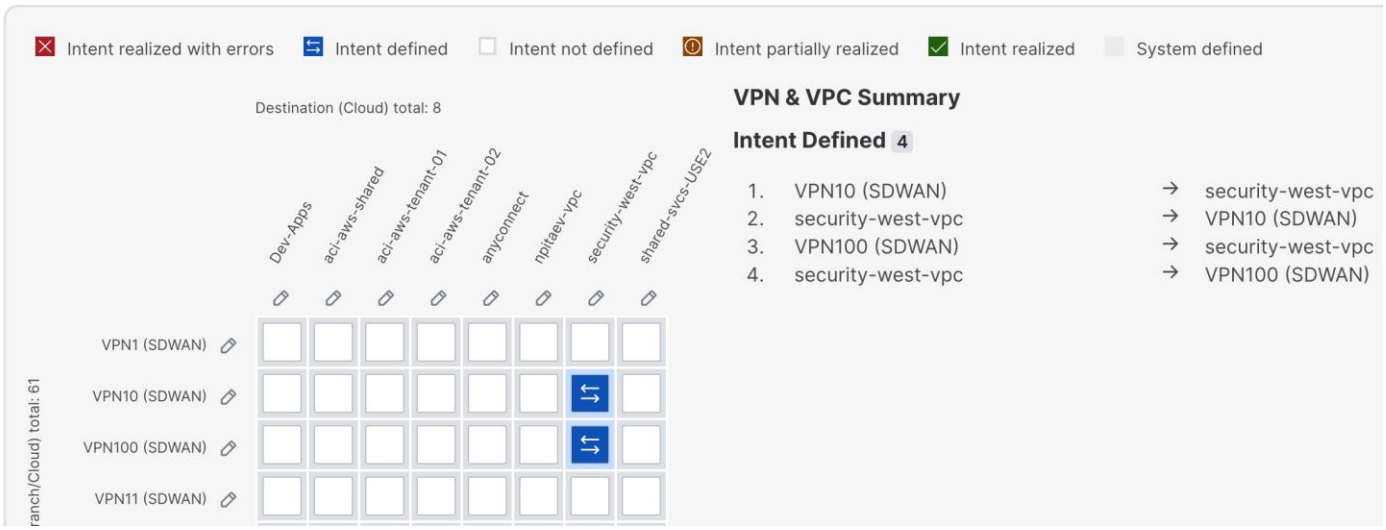

Figure 21. Specifying segmentation intent for Cloud Gateway

AWS

AWS uses a straight-forward orchestration of Transit Gateway (or Cloud WAN) Route Tables for the attachments coming from the integrated SD-WAN routers, or the VPN attachments from Branch Connect routers. This intent matrix determines what VPC attachments are propagated into the SD-WAN fabric and determines what SD-WAN VPNs integrate with the TGW or CNE. This process requires no manual orchestration on the part of the network operator or cloud engineer.

Tech tip: Currently deployed AWS Transit Gateways can be discovered as well and the 'Cloud router connectivity' tab can be used to map VPNs to each cloud gateway. This intent matrix does not orchestrate the route tables in the same manner as AWS TGW deployed via the Cloud OnRamp for Multicloud workflow. Instead, it only brings the attachments up to the existing TGW. Any segmentation intent inside the TGW routing tables is managed by the user outside of SD-WAN Manager

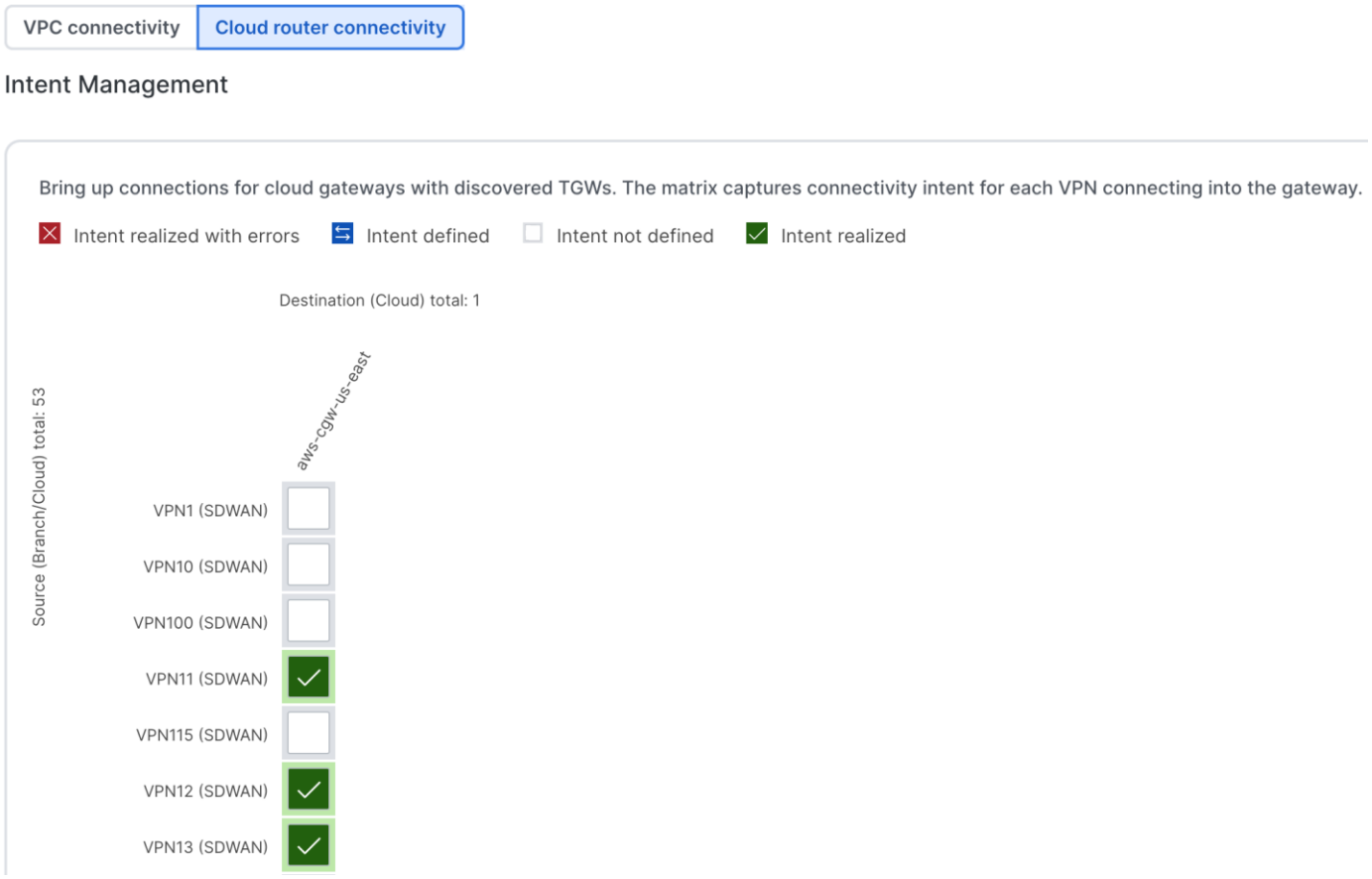

Figure 22. Mapping SD-WAN VPN to discovered Transit Gateways

Azure

Because of the limitations of Azure vWAN, only a single VPN can be connected from the SD-WAN fabric. The cloud tags work the same, but the vWAN connection is limited to a single SD-WAN VPN. In Azure, therefore, it may be more advantageous to set up a specific SD-WAN VPN for peering and do VPN route-leaking on the SD-WAN fabric side if further VPN segmentation is needed.

Google Cloud

Google works the same way as Azure in this case, orchestrating SD-WAN VPN and cloud tag inter-connectivity with route leaking. In the case of Google Cloud, this is done via Network Connectivity Center instead of Azure vWAN, but the methodology is the same.

Cisco SD-WAN Cloud OnRamp for Multicloud Interconnect

A key benefit of Cisco Catalyst SD-WAN public cloud integration is multicloud capability. Customers can apply the same policy, security, and other SD-WAN policies everywhere with Cisco Catalyst SD-WAN Manager as the single NMS for all Cisco Catalyst SD-WAN devices, on-premises and on multiple clouds. Infrastructure on AWS, Azure, and Google Cloud can be seamlessly integrated into the SD-WAN fabric. Cloud OnRamp for Multicloud automates all steps and Cisco Catalyst SD-WAN Manager builds the whole solution within minutes.

For site-to-any-cloud and site-to-site use cases, colocation facilities and Software-Defined Cloud Interconnect (SDCI) providers are often the best solution. Megaport and Equinix have partnered with Cisco to enable both use cases. In the same Cisco Catalyst SD-WAN Manager configuration section for Cloud OnRamp for Multicloud, you will find “Interconnect” tab and be able to configure a middle-mile connection as shown below:

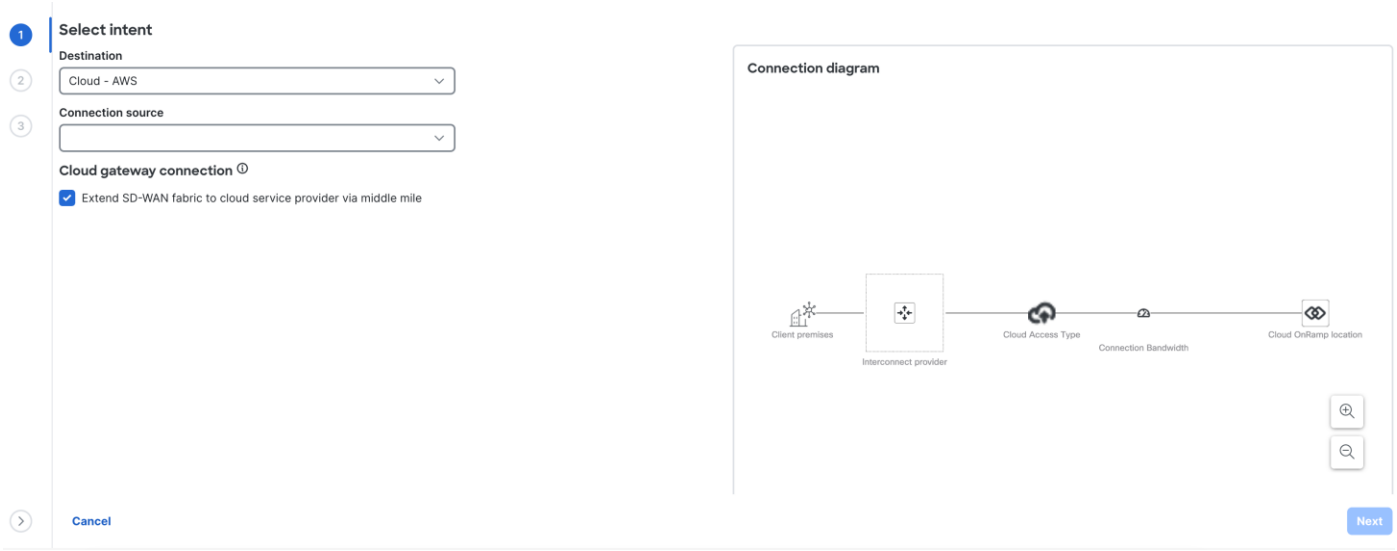

Figure 23. Cisco SD-WAN Cloud OnRamp for Multicloud Interconnect Configuration

With this solution, organizations can quickly and simply orchestrate the entire path, from their own SD-WAN routers to a middle-mile provider, all the way into Cloud Gateways deployed in any of the supported clouds with one simple workflow. This allows Multicloud transit in an easy, automated fashion.

Cisco SD-WAN Cloud OnRamp for Multicloud Failure Detection and Audit Capability

Cisco SD-WAN Manager has the capability to automatically (or on-demand) audit the cloud deployment for which it is responsible, alerting organizations if the intent does not match the current configuration. By default, this audit feature runs every two hours, but it can also be triggered manually to verify the deployment settings. This audit feature can help diagnose and resolve common cloud configuration drift and misconfiguration and should be considered part of an operator's troubleshooting toolkit when investigating potential hybrid cloud issues.

Tech tip: The Audit feature is not in any way intrusive and will not make any configuration corrections. However, the Auto-Correct function could potentially have impact when resolving issues and should be used with caution. In the event of a configuration drift or misconfiguration, SD-WAN Manager will destroy the constructs and rebuild them, which may impact a functioning cloud network. For this reason, the general recommendation is to enable the Audit feature but only use the Auto-Correct feature in testing prior to deploying to a production network.

Learn more about the Audit messages and repair capabilities here: Cisco Catalyst SD-WAN Cloud OnRamp Configuration Guide

Conclusion

Cisco SD-WAN Cloud OnRamp for Multicloud provides an automated way to integrate public cloud infrastructure into the SD-WAN fabric. The center of data gravity, maturity of cloud deployment, and familiarity with SD-WAN are the primary decision drivers on what is the best way to leverage this capability. Integration with AWS Transit Gateway, Azure vWAN, and Google Cloud NCC is possible today with automation that makes it simple and secure. With this solution, multicloud infrastructure is fully integrated into the SD-WAN with common policy, segmentation, and security.

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**.