Cisco SD-WAN Cloud OnRamp for Infrastructure as a Service (IaaS)

Automate Your SD-WAN Fabric Extension to Public Clouds

Cisco® SD-WAN Cloud OnRamp for Infrastructure as a Service (IaaS) extends enterprise WAN to public clouds. This multicloud solution helps to integrate public cloud infrastructure into SD-WAN fabric. This white paper provides an end-to-end technical overview of the solution and not only covers the standard design with transit VPC, but also describes multicloud integration with AWS Transit Gateway (TGW) and Microsoft Azure Virtual WAN (vWAN). The target audience for the solution includes technical roles with basic understanding of SD-WAN and public cloud concepts.

IaaS is a very common usage of the public cloud. The most basic model consists of providers offering IT infrastructure – virtual machines and other resources – as a service to subscribers. What if subscribers, who also use SD-WAN to interconnect branches and data centers, are looking to integrate public cloud infrastructure into SD-WAN? The key benefits of such an integration include: the usage of full SD-WAN capabilities in the cloud, the common Security and Application Quality of Experience (AppQoE) policy framework managed seamlessly via Cisco SD-WAN vManage for all physical on-premises and virtual cloud-based routers, and the interconnection of multiple clouds. The need for such an integration between on-premises and cloud is obvious, so the main question is not “Why?” but “How?” How can the integration be done with high performance, low cost, and the best resilience, in a short amount of time, and across multiple public clouds?

Cloud OnRamp for IaaS

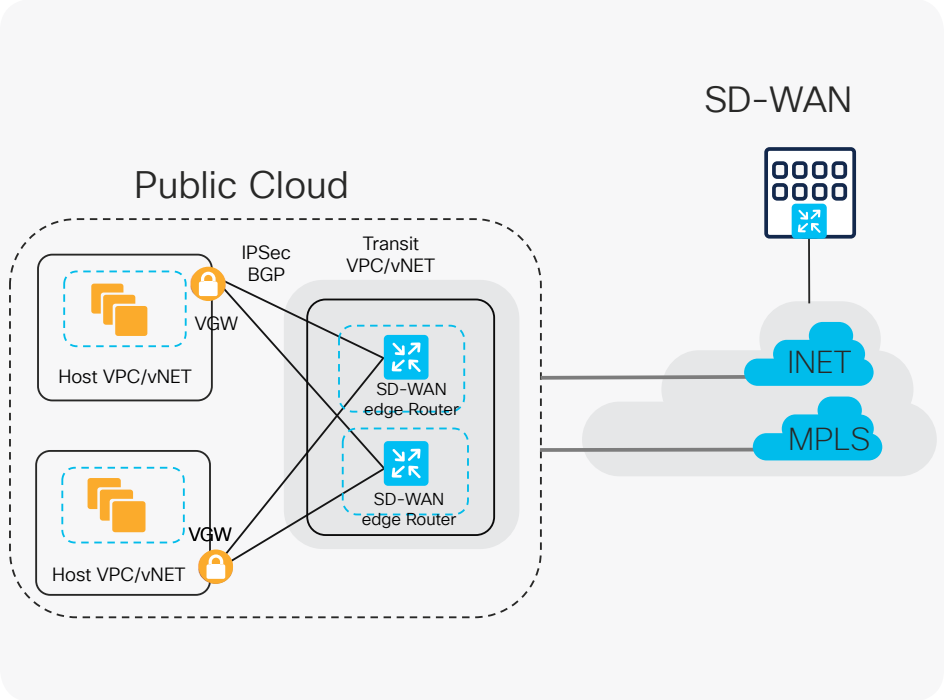
The main goal of this section is to provide a brief overview and describe the key building blocks of the solution. For step-by-step design and configuration steps, please refer to the following design guide “Cisco SD-WAN: Enabling Cisco Cloud OnRamp for IaaS with AWS - April, 2019.” https://www.cisco.com/c/en/us/td/docs/solutions/CVD/SDWAN/Cisco-SD-WAN-Cloud-onRamp-IaaS-AWS-Deployment-2019APR.html.

For online documentation, please refer to https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/Release_18.4/Network_Optimization/Configuring_Cloud_OnRamp_for_IaaS.

Contents

The key differentiator for Cloud OnRamp for IaaS is automation. The whole solution is completely automated – the end user simply needs to enter public cloud credentials in the related vManage section, discover virtual networks and workloads, and define two routers for interconnection. The whole deployment of the transit VPC, bring-up procedure of virtual routers, and interconnection will be done automatically by vManage.

With Cloud OnRamp for IaaS, vManage will automatically deploy two SD-WAN edge virtual routers in a transit VPC, acting as virtual aggregation routers as shown below:



Each Cisco SD-WAN edge virtual router in the transit VPC builds two site-to-site IPsec tunnels (for redundancy, not for active/active paths) to the virtual private gateway (VGW) in the host VPC. There are two Cisco SD-WAN edge routers in the transit VPC, so the total number of IPsec tunnels in transit VPC is four.

Of course, the same tasks can be done manually. The network administrator can log in to the appropriate public cloud management console, create the transit VPC, spin up two SD-WAN edge virtual routers, and interconnect host VPCs. Even if we assume that the network administrator will not make a single mistake, it might take several hours and will require multiple tasks to be completed in at least two different GUIs: vManage and public cloud management console. With Cisco Cloud OnRamp for IaaS, the same task can be completed in approximately 15 minutes – fully automated – without the chance of human errors.

Here are the key steps for Cloud OnRamp for IaaS:

1. Identify two unused SD-WAN edge routers in vManage that will be used for Cloud OnRamp for IaaS
2. Configure and attach a basic device template to both routers
3. Enter AWS or Azure API credentials (access key and secret key) in the vManage Configuration section
4. Add the transit VPC configuration
5. Discover and map host VPCs to the transit VPC

After the five key steps above are completed, vManage will move forward and deploy the entire solution for you.

The whole process can be repeated for the second public cloud so, at the end, your SD-WAN will be interconnected with AWS and Azure. Multicloud capabilities are one of the strongest benefits of the Cloud OnRamp solution.

Interconnecting Cisco SD-WAN with AWS Transit Gateway (TGW)

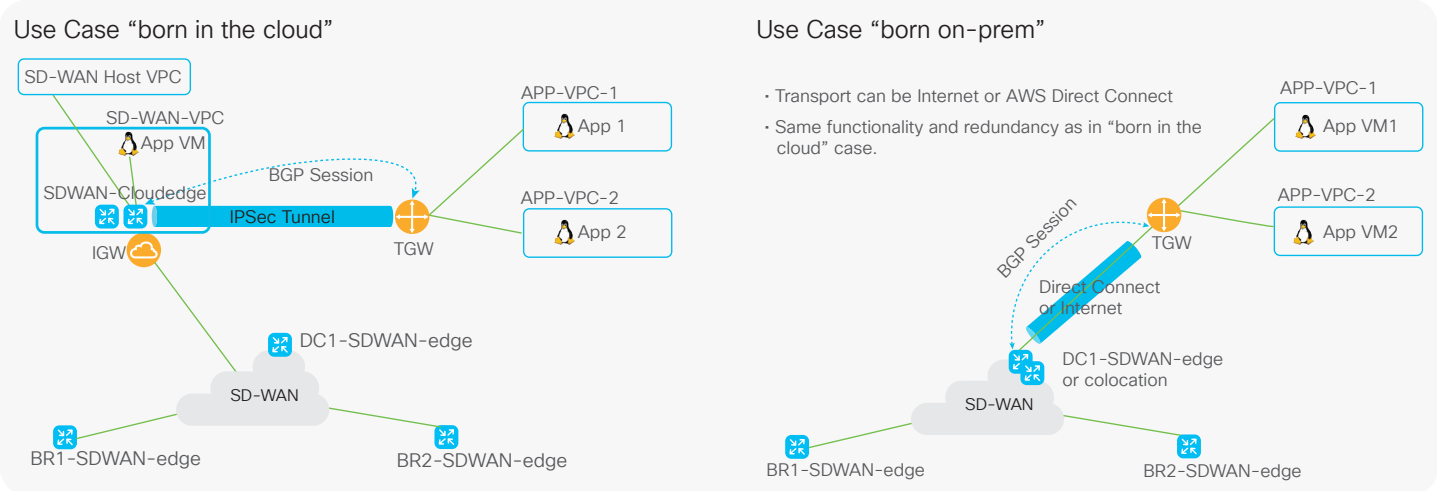
In some cases, the standard Cloud OnRamp solution might be not sufficient. For example, one host VPC is connected to the SD-WAN edge router using an Internet Gateway (IGW). If the IGW bandwidth limit is a bottleneck, then Transit Gateway (TGW) can be used for SD-WAN integration.

Transit Gateway was launched in December 2018 and provides a new way to interconnect VPCs and VPNs. Please refer to AWS TGW documentation for more details: https://docs.aws.amazon.com/vpc/latest/tgw/tgw-transit-gateways.html.

Cisco SD-WAN edge routers will establish a standard IKE-based IPSec tunnel directly to the TGW instead of the IGW. The TGW has better scale and the ability to easily attach host VPCs and VPNs via IPSec and AWS Direct Connect. Over secure IPSec tunnels, SD-WAN edge routers establish BGP connectivity to the TGW and exchange BGP (Border Gateway Protocol) routes. WAN edge routers will learn VPC networks over BGP and redistribute routes into Overlay Management Protocol (OMP). Standard redistribution filtering mechanisms can be used for more granular and flexible redistribution. Other SD-WAN locations will learn these public cloud routes via OMP.

There are two use cases:

1. Born in the cloud, where SD-WAN edge virtual routers run in a transit VPC
2. Born on-premises, where the BGP over IPSec connection to the TGW is established from an on-premises router



The same redundancy principle from Cloud OnRamp is used here: each SD-WAN edge router will establish two IPSec tunnels to TGW and run one BGP session per IPSec tunnel. So, there will be four IPSec tunnels and four BGP sessions in total between two WAN edges and TGW.

The born on-premises use case can be implemented with the Cloud OnRamp for Colocation solution, which allows one to create virtual routers and service chains using vManage. This functionality is achieved by using Cloud Services Platform 5000 (CSP 5444) as the base Network Function Virtualization (NFV) platform. By deploying this solution in colocation centers, customers can virtualize network services and other applications and consolidate them into a single platform. Please refer to the following solution guide for more details: https://www.cisco.com/c/en/us/td/docs/routers/sdwan-cloud-onramp-for-colocation/solution-user-guide/cisco-sdwan-cloud-onramp-colocation-solution-guide-19_1.html.

The main difference – the TGW SD-WAN integration is not yet automated and requires a few simple manual steps to be performed:

1. Create standard IKE-based IPSec tunnel on the service side of Cisco SD-WAN edge routers
2. Configure BGP between TGW and WAN edge routers

Customer success story: an American multinational biopharmaceutical company has recently successfully interconnected Cisco SD-WAN deployment with AWS TGW. The customer had the following key benefits:

- Automated and easy connectivity provisioning to the most optimal AWS entry point for all of their data center and hub locations.
- Application and data telemetry in and out of AWS for reporting/chargeback.
- Dynamic routing, multipathing, and deterministic failover behavior through the use of OMP and SD-WAN Secure Extensible Network (SEN) policies.
- Regional hubs interconnecting multiple AWS TGWs and AWS regions via SEN.
- Multicloud architecture support interconnecting AWS TGWs and Azure vWAN today and Google Cloud Platform in the near future.

Interconnecting Cisco SD-WAN with Azure Virtual WAN

All concepts described in the previous section are also valid for interconnection with Azure Virtual WAN (vWAN). WAN edge routers will establish standard IKE-based IPSec tunnels to the virtual hub and then run BGP over IPSec. WAN edge routers will exchange routes via BGP and redistribute into OMP.

Same use cases (born in the cloud and born on-premises), integration steps, and benefits as described above are applicable to vWAN integration as well.

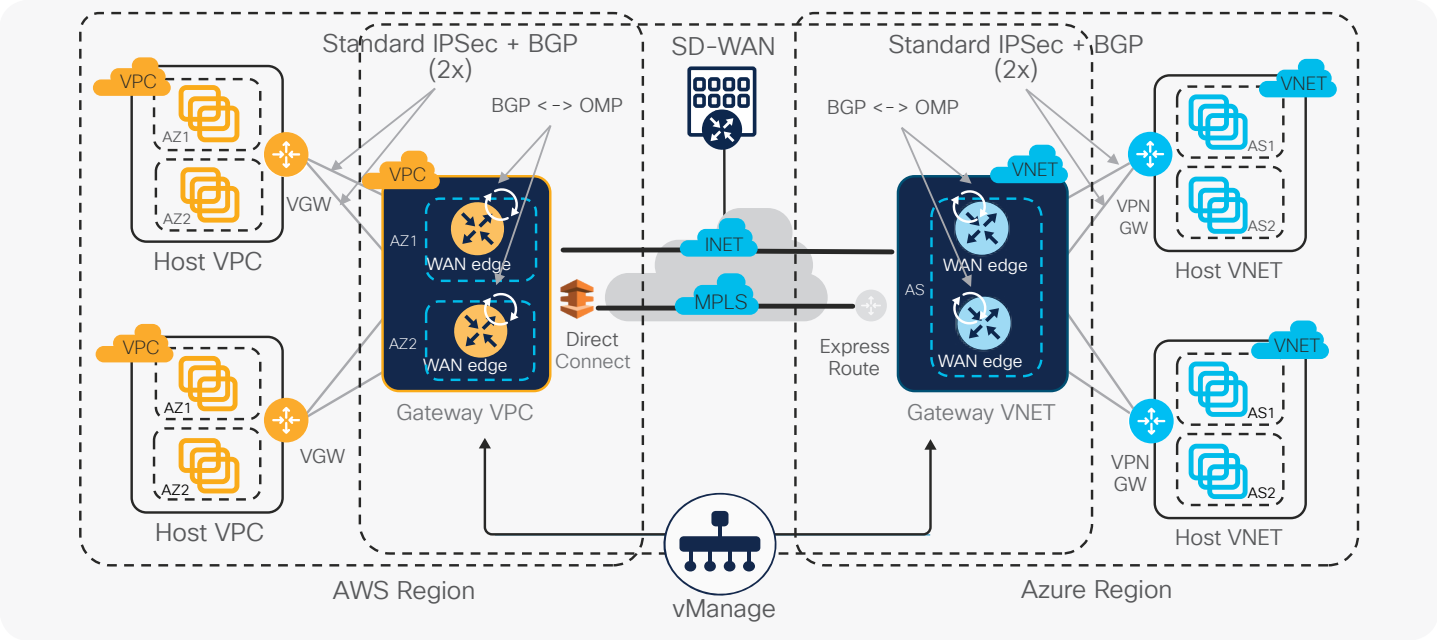
Please refer to the following for more details on Azure vWAN https://docs.microsoft.com/en-us/azure/virtual-wan/virtual-wan-about.

Cloud Infrastructure as Code

For use cases like AWS TGW or Azure vWAN interconnection with Cisco SD-WAN, where Cloud OnRamp for IaaS currently does not provide automation, you can use an Infrastructure as Code (IaC) approach for automation. IaC is the process of setting up, managing, and provisioning infrastructure through machine-readable definition files, rather than interactive configuration tools or GUI. Each public cloud provides several scripting options, which can be used to bring up and configure TGW or vWAN. There are also several multicloud options like Terraform or Ansible that support TGW and vWAN. You can use the tool of your choice to script automatic public cloud integration with SD-WAN.

Multicloud

The key benefit of Cisco SD-WAN public cloud integration is multicloud capability. Customers can apply the same policy, security, and other SD-WAN policies everywhere with vManage as single NMS for all Cisco SD-WAN devices, on-premises and on multiple clouds. Infrastructure on AWS and Azure can be seamlessly integrated into the SD-WAN fabric. Cloud OnRamp for IaaS automates all steps and vManage builds the whole solution within minutes. The picture below shows the final topology with AWS and Azure integrated:



Conclusion

Cisco SD-WAN Cloud OnRamp for IaaS provides an automated way to integrate public cloud infrastructure into the SD-WAN fabric. It has two key use cases: “born in the cloud” and “born on-premises.” Integration with AWS TGW and Azure vWAN is possible today with simple manual bring up, and in the near future it too will be automated. Main benefit: multicloud infrastructure is fully integrated into the SD-WAN with common policy, segmentation, and security.

Get started

Ask your local Cisco sales team for a presentation and demo of Cloud OnRamp for IaaS.

C11-742817-00 11/19