White paper
Cisco public

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

Automate Your SD-WAN Fabric Extension to Public Clouds

Contents

Cisco® Catalyst SD-WAN's 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 Amazon Web Services (AWS) Transit Gateway, Microsoft Azure Virtual WAN (vWAN) and Google Cloud. The target audience for the solution includes technical roles with basic understanding of SD-WAN and public cloud concepts.

Infrastructure as a Service (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 Catalyst SD-WAN Manager 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 guides:

- "Cisco SD-WAN Cloud OnRamp for IAAS using Azure Deployment Guide" https://www.cisco.com/c/en/us/td/docs/solutions/CVD/SDWAN/cisco-sdwan-cloud-onramp-iaas-azure-deploy-guide.html.
- "Interconnecting Cisco SD-WAN and Azure Virtual WAN" https://community.cisco.com/t5/networking-blogs/interconnecting-cisco-sd-wan-and-azure-virtual-wan/ba-p/4077406.

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 Cisco Catalyst SD-WAN Manager 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 Cisco Catalyst SD-WAN Manager.

With Cloud OnRamp for IaaS, Cisco Catalyst SD-WAN Manager will automatically deploy AWS Transit Gateway, two SD-WAN edge virtual routers in a transit SD-WAN VPC, acting as virtual aggregation routers as shown below using AWS as example:

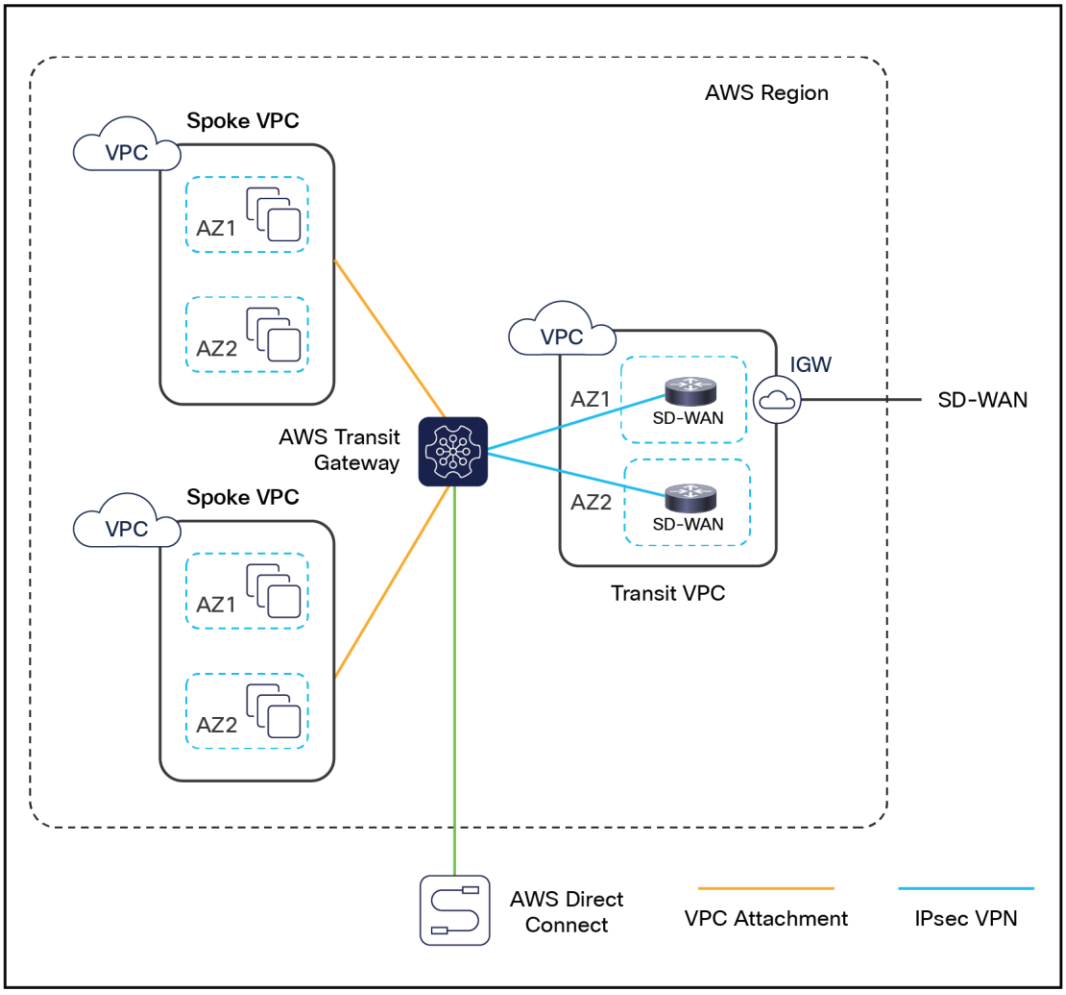

Figure 1.
Cloud OnRamp design with SD-WAN routers and host VPCs connected via AWS Transit Gateway

Each Cisco Catalyst SD-WAN edge virtual router in the transit VPC builds IPsec tunnels to the AWS Transit Gateway. Alternatively GRE tunnels can be also used between Cisco Catalyst SD-WAN virtual routers and AWS Transit Gateway. The choice for IPSec or GRE tunnels depends on customer requirements such as required bandwidth, security, use of public or private IP addresses for the tunnel endpoints. Host VPCs are connected to AWS Transit Gateway via VPC Attachments. AWS Direct Connect attachments to AWS Transit Gateway are also possible, but currently not supported in CoR Multicloud Automation. Similar designs are possible with Azure using Virtual WAN (vWAN) and Google Cloud using Network Connectivity Center.

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, AWS Transit Gateway 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: Cisco Catalyst SD-WAN Manager 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. **SETUP:** Identify two unused SD-WAN edge routers in Cisco Catalyst SD-WAN Manager that will be used for Cloud OnRamp for IaaS, configure and attach a basic device template to both routers, enter AWS, Azure or Google Cloud credentials in the Cisco Catalyst SD-WAN Manager Account Configuration section.
2. **DISCOVER:** Cisco Catalyst SD-WAN Manager will discover all host VPCs using defined cloud accounts.
3. **CLOUD GATEWAY:** Cisco Catalyst SD-WAN Manager will create SD-WAN virtual routers and cloud infrastructure (i.e. AWS Transit Gateway) for you.
4. **INTENT MANAGEMENT/CLOUD CONNECTIVITY:** host VPCs will be mapped to SD-WAN networks.

After the five key steps above are completed, Cisco Catalyst SD-WAN Manager 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, Azure and Google Cloud. Multicloud capabilities are one of the strongest benefits of the Cloud OnRamp solution.

The following screen shot demonstrates the end state, where Cisco Catalyst SD-WAN Manager created connectivity to AWS, Azure and Google Cloud. The key four steps are shown at the bottom of the image:

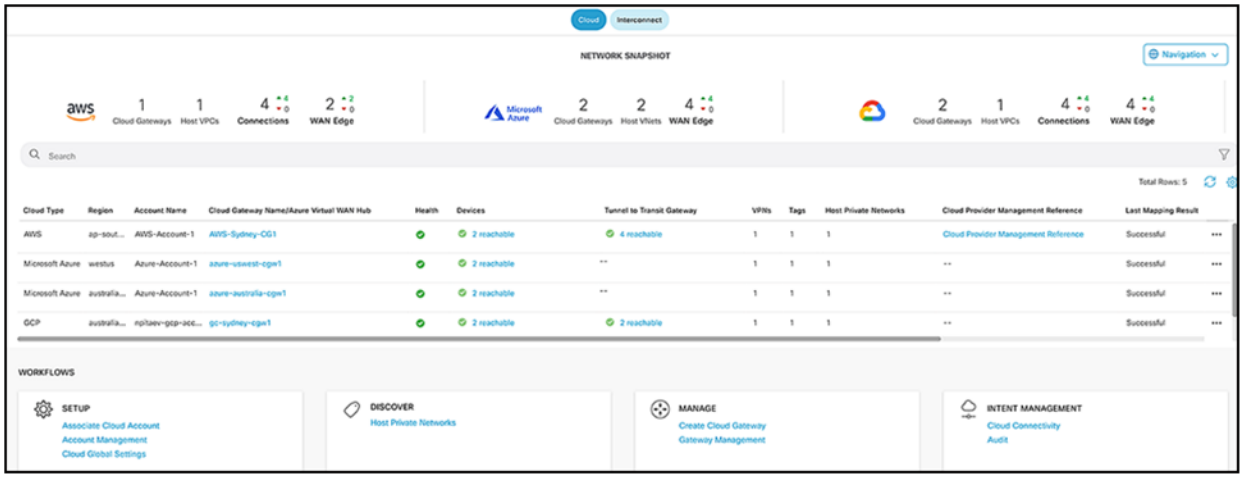

Figure 2.
Cloud OnRamp Dashboard of Cisco Catalyst SD-WAN Manager

Interconnecting Cisco Catalyst SD-WAN with AWS Transit Gateway

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 can be used for SD-WAN integration.

Transit Gateway provides a state of the art way to interconnect VPCs and VPNs. Please refer to AWS Transit Gateway documentation for more details: https://docs.aws.amazon.com/vpc/latest/tgw/what-is-transit-gateway.html.

Cisco Catalyst SD-WAN edge routers will establish a standard IKE-based IPSec tunnel directly to the Transit Gateway instead of the IGW. The Transit Gateway 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 Transit Gateway 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. This use case maps to the Cloud OnRamp Workflow "AWS Transit Gateway with CSR in Transit VPC".
2. **Born on-premises**, where the BGP over IPSec connection to the Transit Gateway is established from an on-premises router. This maps to the Cloud OnRamp workflow "AWS Transit Gateway – Branch Connect".

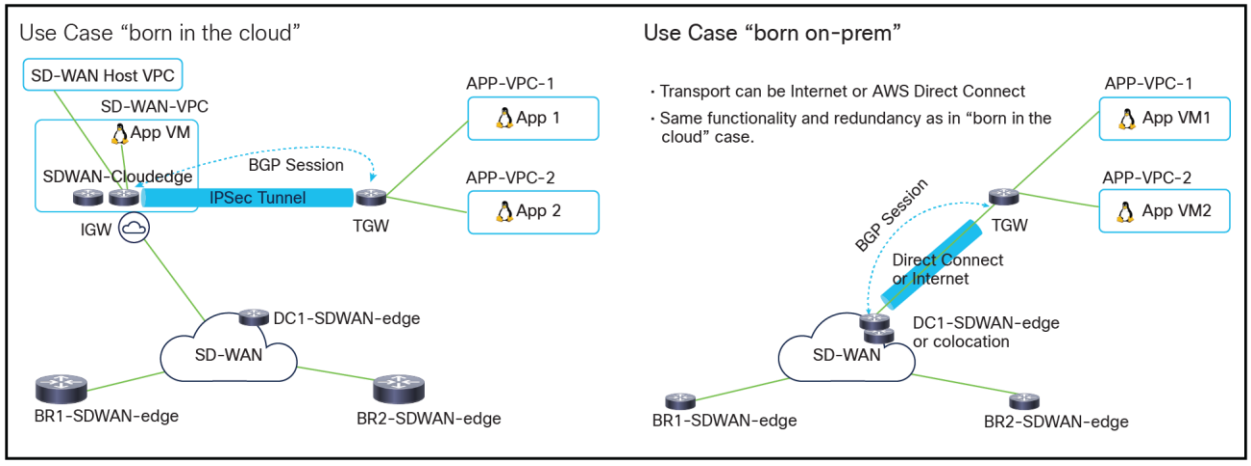

Figure 3.
Two main use cases

The same redundancy principle from Cloud OnRamp is used here: each SD-WAN edge router will establish two IPSec tunnels to Transit Gateway 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 Transit Gateway.

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 Cisco Catalyst SD-WAN Manager. 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-solutionguide-19_1.html.

Customer success story: an American multinational biopharmaceutical company has recently successfully interconnected Cisco Catalyst SD-WAN deployment with AWS Transit Gateway. 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 Transit Gateways and AWS regions via SEN.
- Multicloud architecture support interconnecting AWS Transit Gateways and Azure vWAN today and Google Cloud in the near future.

Another great reference is the following blog: “Cisco Catalyst SD-WAN on AWS Helps ENGIE Become Cloud First”
https://blogs.cisco.com/networking/cisco-sd-wan-on-aws-helps-engie-become-cloud-first.

Interconnecting Cisco Catalyst 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.

Interconnecting Cisco Catalyst SD-WAN with Google Cloud

All concepts described in the previous section are also valid for interconnection with Google Cloud. Cisco SD-WAN Cloud Hub brings automation for the Infrastructure as a Service use case on Google Cloud and helps with the following two use cases starting with 17.5 IOS XE SD-WAN Software:

- **Site-to-cloud:** in this case a branch location needs to access an application running in a VPC on Google Cloud.
- **Site-to-Site:** two branches located in different regions must be connected via Google Cloud global network.

The following example illustrates both use cases:

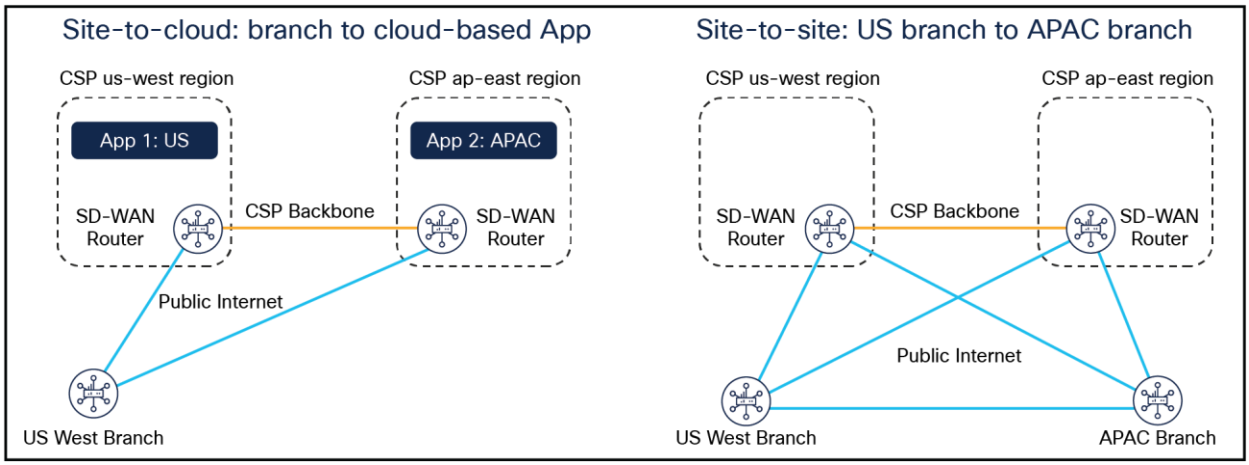

Figure 4.
SD-WAN and Google Cloud Use Cases

The following building blocks are important for the high-level design

- Cisco Catalyst 8000V Edge Software virtual SD-WAN platform
- Google Cloud Network Connectivity Center
- Google Cloud Router and VPC Peering

Cisco Catalyst SD-WAN Manager will use built-in automation to do the following:

1. Create WAN-VPC and spin up two Cisco Catalyst 8000V SD-WAN virtual routers
2. Create Site-to-cloud VPC
3. Create Site-to-Site VPC

The following technical diagram summarizes the design for both use cases:

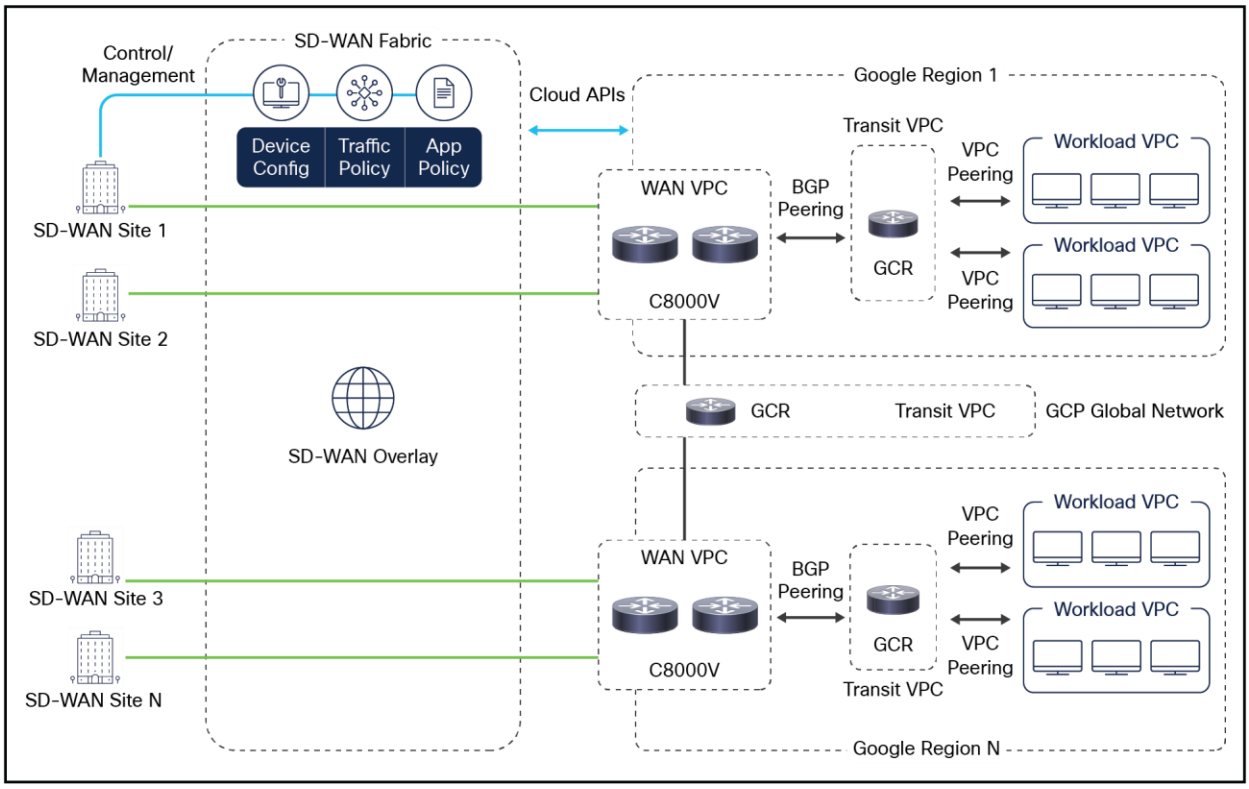

Figure 5.
Technical Cloud OnRamp Design for Google Cloud

Cloud Infrastructure as Code

For use cases like AWS Transit Gateway or Azure vWAN interconnection with Cisco Catalyst 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 Transit Gateway or vWAN. There are also several multicloud options like Terraform or Ansible that support Transit Gateway and vWAN. You can use the tool of your choice to script automatic public cloud integration with SD-WAN.

Cloud Interconnect and Colocation (Megaport and Equinix)

The 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 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 IaaS 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 IaaS you will find "Interconnect" tab as shown in the screen shot below:

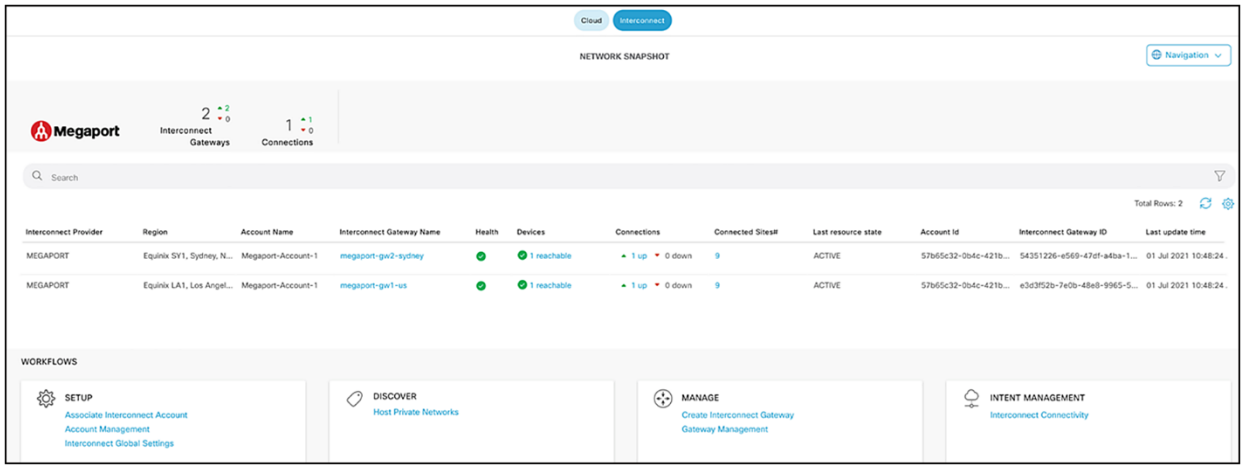

Figure 6.
Cisco Catalyst SD-WAN Manager Cloud OnRamp Dashboard for Cloud Interconnect

Using the same configuration workflow (Setup -> Discover -> Manage -> Interconnect), you can enable both use cases fully automated with Megaport starting with Cisco SW release 20.5/17.5.

Equinix automation will follow in the near feature. Today's Equinix implementation involves executing the following five simple steps:

1. Create, in Cisco Catalyst SD-WAN Manager, a configuration template for virtual SD-WAN routers, which will be running in the Equinix facilities.
2. Export the day-0 configuration from Cisco Catalyst SD-WAN Manager for virtual routers as a.cfg file.
3. In the Equinix Fabric portal, create SD-WAN virtual routers and upload the day-0 configuration in the cfg file. Once booted, the SD-WAN virtual routers will join your SD-WAN fabric automatically.

4. Now, in the Equinix Fabric portal, you can create point-to-point connections between related SD-WAN routers. SD-WAN routers will establish SD-WAN tunnels over Equinix connections automatically.
5. As a last step, in Cisco Catalyst SD-WAN Manager configure an SD-WAN control policy to steer the traffic based on your requirements.

Please refer to the following white paper for more details: https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/sd-wan/white-paper-c11-2373512.html.

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 Transit Gateway 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.

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 C11-742817-02 10/23