Deploying Cisco SD-WAN on AWS

Introduction: Why use an SD-WAN solution for the cloud?

Organizations leveraging branch office locations, IoT devices, and distributed network devices face a unique set of considerations as they migrate to the cloud. Many legacy wide area network (WAN) solutions rely on backhauling branch office traffic to the data center, which consumes network bandwidth, takes a circuitous route to the cloud and frequently results in poor application performance. Further, these solutions are generally rigid, complex to configure, and expensive to maintain requiring significant manual network configuration to properly integrate them with cloud environments.

Traditional enterprise WAN architecture

Modern SD-WAN architecture
If you’re looking to migrate on premise workloads to Amazon Web Services (AWS), Cisco SD-WAN can significantly simplify this process. Because it’s transport-independent, it gives you the flexibility to use any WAN transport including Internet broadband, MPLS, 4G and LTE while maintaining strong performance and security. If you’re already using Cisco SD-WAN, you can easily extend this deployment to AWS to minimize manual network configuration and maintain the enterprise functionality that you’ve come to expect from Cisco SD-WAN.

In this guide, we will walk you through the steps required to deploy and manage a Cisco SD-WAN solution on AWS.

**Step 1: Assess your readiness for cloud-based SD-WAN**

Before you start, you should ask yourself a few questions:

1. **Do you have branch offices that you want to connect to the cloud, or that are already connected to the cloud inefficiently?**

   A key driver for SD-WAN adoption is the aggregation of disparate WAN connections plus the management and migration of network changes much quicker and smoother, greatly reducing operational costs (OPEX). Cisco SD-WAN enables enterprise DIA (direct internet access) sending traffic directly from the branch office to the AWS cloud. The network is managed and viewed via the Cisco SD-WAN vManage, which is hosted in a cloud, most frequently the AWS cloud.

2. **Are you relying on expensive MPLS to deliver adequate application performance?**

   Enterprises have traditionally used MPLS for WAN connectivity via their data center, which is very expensive and takes months to deploy. Therefore the bandwidth is often constrained, impacting application performance. Cisco SD-WAN enables migrating WAN connections to increase bandwidth and DIA.

3. **How do you provision connections to AWS?**

   Cisco SD-WAN Cloud OnRamp for IaaS, “Cloud OnRamp” for short, is a Cisco SD-WAN feature that automates provisioning of a Cisco SD-WAN virtual appliance routers (either vEdge Cloud or CSR (Cloud Services Router)) in the AWS cloud, after providing your AWS credentials, the Cloud OnRamp dashboard discovers VPCs in your AWS environment then you can map VPN segments to the appropriate VPC workloads.

4. **Are you already using SD-WAN?**

   Establishing Cloud OnRamp requires Cisco SD-WAN virtual appliances, we recommend two for redundancy, for each branch connection. If you’re already using SD-WAN to support your branch offices, but not in conjunction with a cloud environment, you can use your existing SD-WAN license to deploy SD-WAN on AWS through AWS Marketplace here. Contact your Cisco account team member to purchase the appropriate license if you don’t already have one.
Step 2: Choose network policies that fit your needs

Using Cloud onRamp, you can select a location to discover host VPCs, and map the host VPCs to the gateway VPC(s) of your choice.

Once you have selected the vEdge routers and AWS VPCs that you want to connect, you need to make several policy choices:

1. What mixture of connectivity options do you want to leverage?

AWS Direct Connect has been the de-facto standard hard, dedicated connection for most enterprises connecting to the AWS cloud. While it generally comes with SLAs and offers good performance, it is very costly and takes weeks to months to provision. Cisco SD-WAN’s transport-independence will enable you to more efficiently and affordably connect to your AWS cloud.

2. What applications will get bandwidth priority?

When configuring your AWS network, you will want to think about which applications are the most critical and time-sensitive. In situations where bandwidth is limited, you can give these time-sensitive applications priority over something less time-sensitive by configuring Application Aware Routing (AAR) policies. Cisco SD-WAN is cloud-aware, and gives you the ability to specifically prioritize bandwidth in alignment with each application’s SLA.

3. Which VPCs will act as your gateway and host VPCs?

An SD-WAN architecture contains three primary components. The gateway VPC hosts two virtual router instances and connects the SD-WAN overlay to your applications. The host VPC(s) are where your AWS applications reside. Because the gateway VPC acts as a point of access, you will generally want it more centrally located, whereas host VPCs should generally be selected based on security and access. Multiple host VPCs can be mapped to each gateway VPC, which can in turn be leveraged to set up connections between branch offices and host VPCs. This allows you to use the gateway VPC to scale up host VPCs as needed, keeping workloads segmenting for simpler management and security.

These are only a few of the policy choices you need to make, but taking the time to choose the ones that best align to your business requirements is key to maximizing the value of your SD-WAN investment.
Step 3: Leverage policies to automate the configuration of your AWS network

After selecting the branch offices that you want to connect to AWS, the AWS environment that they will connect to, and policies that align to your needs, you can use Cisco SD-WAN vManage to automate the configuration of your AWS network. If you’ve already got an AWS environment, you can use Cloud OnRamp to connect to vManage. Since you’re likely migrating to the cloud app by app, using Cisco SD-WAN will give you granular control over all apps deployed on AWS.

Step 4: Adjust your policies to improve performance, simplify management, and strengthen security

Once your SD-WAN solution has been running for some time, you can make adjustments to your policies that will often yield significant improvements. A few examples include:

Using application-aware routing (AAR) to choose the best route for each application

Application-aware routing tracks network and path characteristics of the data plane tunnels between vEdge routers and uses the collected information to compute optimal paths for data traffic.

Prioritizing different workloads based on their criticality/SLAs

When the best optimal path for multiple applications is the same, you can use vManage to select which application(s) will receive priority. This enables you to give first priority to applications with the most stringent SLAs. For example, an SAP-based enterprise resource planning (ERP) system is mission critical and user access needs to be real-time. Most enterprises want to give it priority over something like an internal instant messaging application, which is less time-sensitive.

Extending SD-WAN segmentation to VPCs for consistent security posture across AWS and on-prem

If you’re already using SD-WAN on-premises, you may be leveraging its network segmentation functionality for security purposes, such as keeping authenticated users separate from guest users.
Summary

By making it easy to extend your network to AWS, Cisco SD-WAN makes cloud migration simple. It also gives you granular control over network policies through a simple management interface, helping you meet organizational needs.

If you’re ready to get started with Cisco SD-WAN on AWS, contact us or download and launch the Cisco SD-WAN virtual appliances from AWS Marketplace.