Cisco Cloud ACI on AWS

Contents

Cisco Cloud Application Centric Infrastructure (Cisco Cloud ACI) overview

In today's world, enterprises are undergoing increasing pressure to innovate rapidly, to keep up with competition and to increase IT agility to meet customer demands. To achieve these goals, businesses are choosing different infrastructure environments for deploying different types of applications. Some applications may be best suited to be hosted on-premises, whereas other applications may be best suited to be hosted in a public cloud, and yet others may benefit from hybrid deployments. In fact, hybrid cloud is becoming the new normal for many businesses.

However, in a hybrid cloud environment it is becoming more and more challenging to maintain a homogeneous enterprise operational model, comply with corporate security policies, and gain visibility across hybrid environments. Cisco Cloud Application Centric Infrastructure (Cisco Cloud ACI) is a comprehensive solution that provides simplified operations, consistent policy management and visibility across multiple on-premises data centers and public clouds or hybrid cloud environments. Cisco Cloud ACI allows customers running Cisco ACI™ in their on-premises data centers to extend their Cisco ACI policies to public clouds.

In an on-premises Cisco ACI data center, Cisco Application Policy Infrastructure Controller (APIC) is the single point of policy configuration and management for all the Cisco ACI switches deployed in the data center. When there is a need to seamlessly interconnect multiple Cisco ACI–powered data centers and selectively extend Cisco ACI constructs and policies across sites, Cisco ACI Multi-Site Orchestrator (MSO) enters the scene. MSO is a software solution that represents a single point of policy orchestration and visibility across multiple geographically dispersed ACI sites.

With the new Cisco Cloud ACI capabilities delivered in Cisco ACI Release 4.1, MSO can manage policies across multiple on-premises Cisco ACI data centers as well as public clouds. The policies configured from MSO can be pushed to different on-premises Cisco ACI sites and cloud sites. Cisco APIC controllers running on premises receive this policy from MSO, then render and enforce it locally. When extending Cisco ACI to the public cloud, a similar model applies. But there is a twist. Public cloud vendors do not speak Cisco ACI natively. Things such as Endpoint Groups (EPGs) or contracts are not familiar concepts there. MSO policies therefore need to be translated into cloud-native policy constructs. For example, contracts between Cisco ACI EPGs need to be translated into security groups on AWS first, then applied to AWS cloud instances. This policy translation and programming of the cloud environment is performed using a new component of the Cisco Cloud ACI solution called Cisco Cloud Application Policy Infrastructure Controller (Cisco Cloud APIC or Cloud APIC).

Cisco Cloud APIC runs natively on supported public clouds[1] to provide automated connectivity, policy translation and enhanced visibility of workloads in the public cloud. Cisco Cloud APIC translates all the policies received from MSO and programs them into cloud-native constructs such as VPCs (Virtual Private Cloud), security groups, security group rules, etc.

This new solution brings a suite of capabilities to extend your on-premises data center into true hybrid cloud architectures, helping drive policy and operational consistency regardless of where your applications reside. It provides a single point of policy orchestration across hybrid environments, operational consistency, and visibility across clouds.

[1] See the data sheet and release notes for public cloud environment support information.

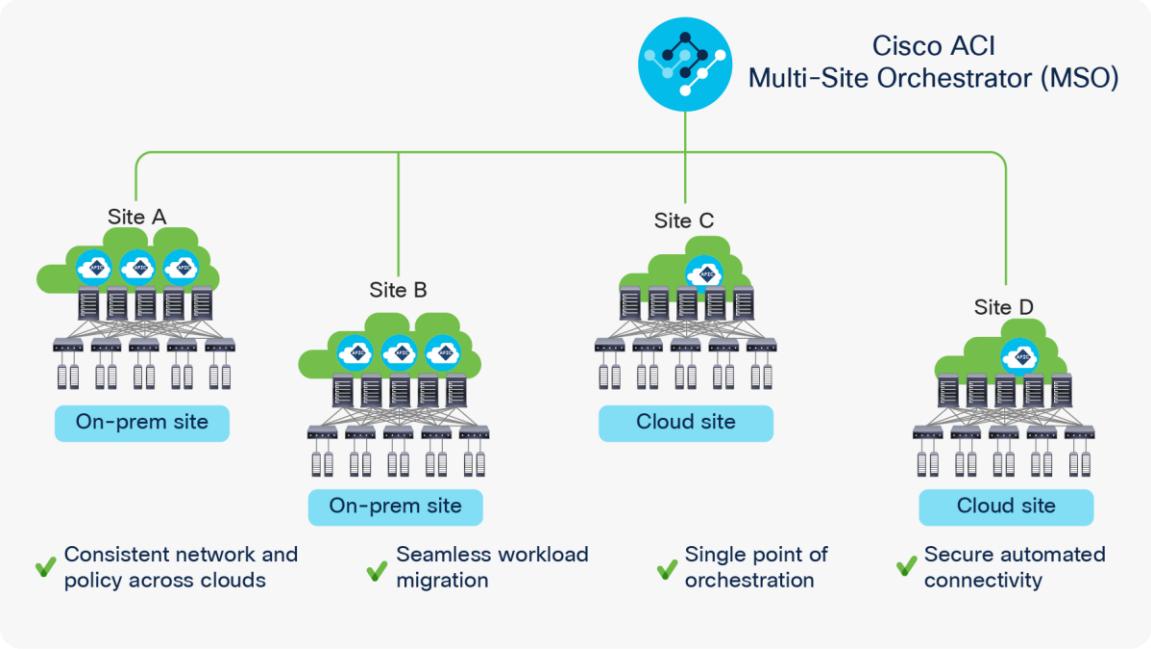


Figure 1.
High-level architecture of Cisco Cloud ACI

Figure 1 shows the overall high-level architecture of Cisco Cloud ACI with Cisco ACI Multi-Site Orchestrator acting as a central policy controller, managing policies across multiple on-premises Cisco ACI data centers as well as hybrid environments, with each cloud site being abstracted by its own Cloud APICs. The rest of this white paper discusses the architecture, benefits, use cases, and deployment of Cisco Cloud ACI on AWS.

Challenges in hybrid cloud environments

As the adoption of hybrid cloud strategies grows, the industry is demanding consistent policy, security, and visibility everywhere with a simplified and consistent operating model. At the same time, the total cost of the solution must be kept under control to benefit from the hybrid cloud advantages.

The main challenges in building and operating a hybrid cloud environment are:

1. Automating the creation of secure interconnects between on-premises and public clouds
2. Dealing with the diverse and disjoint capabilities across on-premises private cloud and public cloud
3. Multiple panes of glass to manage, monitor, and operate hybrid cloud instances
4. Inconsistent security segmentation capabilities between on-premises and public clouds
5. Facing the learning curve associated with operating public cloud environment
6. Inability to leverage a consistent L4–L7 services integration in hybrid cloud deployments

Cisco ACI has delivered on the Software-Defined Networking (SDN) promise of intent-based network configuration and automation and further simplified operations by delivering control and visibility based on network policies that closely mimic your applications. The next phase of Cisco ACI must now address extending this policy-driven automation to hybrid environments. The Cisco Cloud ACI solution offers a coherent hybrid cloud strategy delivering on the key pillars of automation, security, and simplicity.

High-level architecture of Cisco Cloud ACI on AWS

As briefly explained above and further depicted in Figure 2, an instance of MSO orchestrates multiple independent sites using a consistent policy model and provides a single pane of glass for centralized management and visibility. The sites can be on-premises Cisco ACI fabric sites with their own site-local APIC clusters, or cloud sites in AWS with Cloud APIC to manage the cloud site. Just as with a normal Cisco ACI multi-site architecture, all the sites are interconnected via a "plain" IP network. No need for IP multicast or Dynamic Host Configuration Protocol (DHCP) relay here. Just take care of providing IP connectivity, and MSO will be responsible for setting up the intersite overlay connectivity.

For more details on the Cisco ACI multi-site solution, refer to the following white paper: https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-739609.pdf

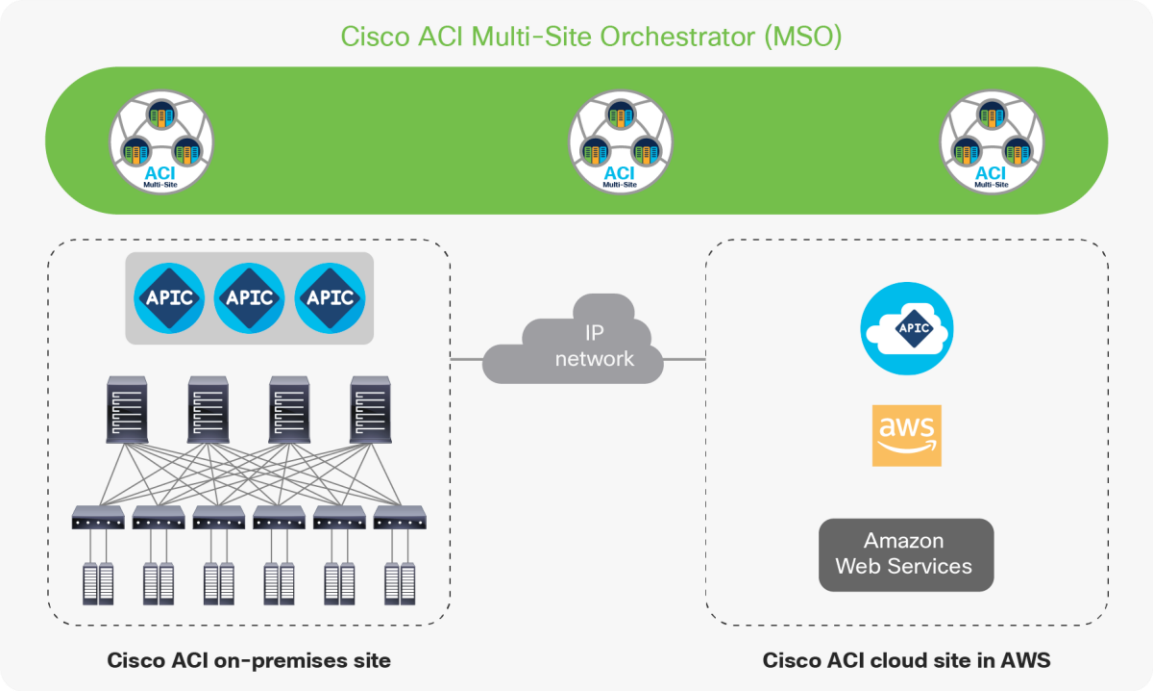


Figure 2.
Cisco Cloud ACI on AWS architecture

The key building blocks of the Cisco Cloud ACI architecture include the following: an on-premises Cisco ACI site running Cisco ACI Release 4.1 software and equipped with at least one second-generation spine model (EX, FX, C or GX), Cisco ACI Multi-Site Orchestrator (MSO), Cisco Cloud APIC, intersite connectivity between the on-premises and cloud sites, and network policy mapping between the Cisco ACI on-premises and cloud sites. Starting from Cisco ACI Release 4.2, on-premises Cisco ACI site is not mandatory, which allows customers to bring the benefits of Cloud ACI, such as single policy management, automation for cloud site provisioning, centralized visibility and correlation, to their cloud-only environments.

Cisco ACI Multi-Site Orchestrator (MSO)

In a Cisco ACI multi-site architecture, the Cisco ACI Multi-Site Orchestrator (MSO) is the single pane of glass for management of all the interconnected sites. It is a centralized place to define all the inter-site policies that can then be published to the individual Cisco ACI sites where the site-local APICs render them on the physical switches that build those fabrics.

With the Cisco Cloud ACI, MSO's orchestration functions expand to the cloud sites. It is responsible for site registration of both on-premises Cisco ACI data center sites and the cloud sites. It automates the creation of overlay connectivity between all the sites (on-premises and cloud). Continuing to be the central orchestrator of intersite policies, MSO now can not only publish policies to on-premises Cisco ACI data center sites, but also push the same policies to cloud site in AWS. It is also capable of instrumenting the policy deployment among different sites by selectively distributing the policies to only the relevant sites. For instance, MSO can deploy the web front tier of an application into the cloud site in AWS while keeping its compute and database tiers in the on-premises site. Through the MSO interface, network administrators can also regulate the communication flow between the on-premises site and AWS as required by applications.

Cisco Cloud APIC on AWS

Cisco Cloud APIC is an important new solution component introduced in the architecture of Cisco Cloud ACI. It plays the equivalent of APIC for a cloud site. Like APIC for on-premises Cisco ACI sites, Cloud APIC manages network policies for the cloud site that it is running on, by using the Cisco ACI network policy model to describe the policy intent. Cloud APIC is a software-only solution that is deployed using cloud-native instruments such as, for example, Cloud Formation templates on AWS. Network and security policies could be locally defined on the Cloud APIC for the cloud site, or globally defined on MSO and then distributed to the Cloud APIC. While the on-premises APIC renders the intended policies onto Cisco ACI switches of the site, Cloud APIC renders the policies onto the AWS cloud network infrastructure. It accomplishes the task by translating the Cisco ACI network policies to the AWS-native network policies and uses the AWS-native policy API to automate the provisioning of the needed AWS-native cloud resources, such as VPCs, cloud routers (Cisco® CSR 1000V Series and AWS Virtual Private Gateway (VGW)), security groups, security group rules, etc. In a nutshell, The key functionalities of Cloud APIC include the following:

1. Provides a north-bound REST interface to configure cloud deployments
2. Accepts Cisco ACI Policy Model and other cloud-specific policies directly or from MSO
3. Performs endpoint discovery in the cloud site
4. Performs Cisco ACI Cloud Policy translation
5. Configures the cloud router's control plane
6. Configures the data-path between Cisco ACI Fabric and the cloud Site

Cisco Cloud APIC is a microservices-based software deployment of APIC controller. Cisco Cloud APIC on AWS is deployed and runs as an Amazon Elastic Compute Cloud (Amazon EC2) instance using persistent block storage volumes in Amazon Elastic Block Store (Amazon EBS). The Amazon Machine for Cisco Cloud APIC are available at AWS marketplace, and use Bring Your Own License (BYOL) model for licensing.

As ACI APIC for an on-premises ACI fabric, ACI Cloud APIC contains only policies and is not in the data forwarding path. Any downtime of the Cloud APIC will not impact network forwarding functionality or performance in the cloud site. The Amazon EC2 instance of the Cloud APIC takes advantage of Amazon EBS built-in storage volume redundancy, high availability and durability. Upon a failure in the Amazon EC2 instance, it can always relaunch or restore to the previous state by rebuilding configuration and states from persistent storage and provide seamless Cloud APIC functionalities. Therefore, for simplicity and cost effectiveness, Cloud APIC is deployed as a single Amazon EC2 instance in the initial release of Cisco Cloud ACI on AWS. In the future, clustering of multiple virtual instances will be introduced for Cloud APIC to achieve higher scalability and instance level redundancy.

Key benefits of using Cisco Cloud ACI

The Cisco Cloud ACI solution provides the following key benefits:

Automation of on-premises to cloud interconnect

Cisco Cloud ACI on AWS automates the configuration of end-to-end connectivity between an on-premises Cisco ACI fabric and AWS. This connectivity can take place over the internet using IPsec VPN or through AWS Direct Connect. Cisco Cloud APIC deploys a pair of Cisco CSR 1000V Series routers in AWS and programs them to form an IPsec tunnel to the IPsec terminator that is installed on premises.[2] Once the IPsec tunnel is up, MSO configures the BGP EVPN control plane between the on-premises second-generation Cisco ACI Spines and the Cisco CSR 1000V Series router deployed on AWS. An end-to-end VXLAN tunnel is then established between the on-premises data center and AWS. This end-to-end automation makes hybrid cloud connectivity seamless, reducing the configuration time, risk of errors, and accelerating the pace of deployment and rate of change. Later in the document, more technical details are provided regarding this automated intersite connectivity.

Universal policy model

Both Cisco ACI and AWS use group-based network and security policy models. In a nutshell, the logical network constructs of the Cisco ACI network policy model consist of tenants, Bridge Domains (BDs), bridge-domain subnets, Endpoint Groups (EPGs), and contracts. AWS uses slightly different constructs: user accounts, Virtual Private Cloud (VPC), and security groups, plus security group rules and network access-lists. As shown in Figure 3, Cisco ACI classifies endpoints into EPGs and uses contracts to enforce communication policies between these EPGs. AWS uses Security Groups (SGs) and security group rules for classification and policy enforcement. Figure 4 gives one example of AWS security policy enforcement using security groups and security group rules.

Figure 3.
Cisco ACI EPG-based network model

[2] You are responsible for providing that device. As of Cisco ACI Release 5.1, only the Cisco CSR 1000V is qualified.

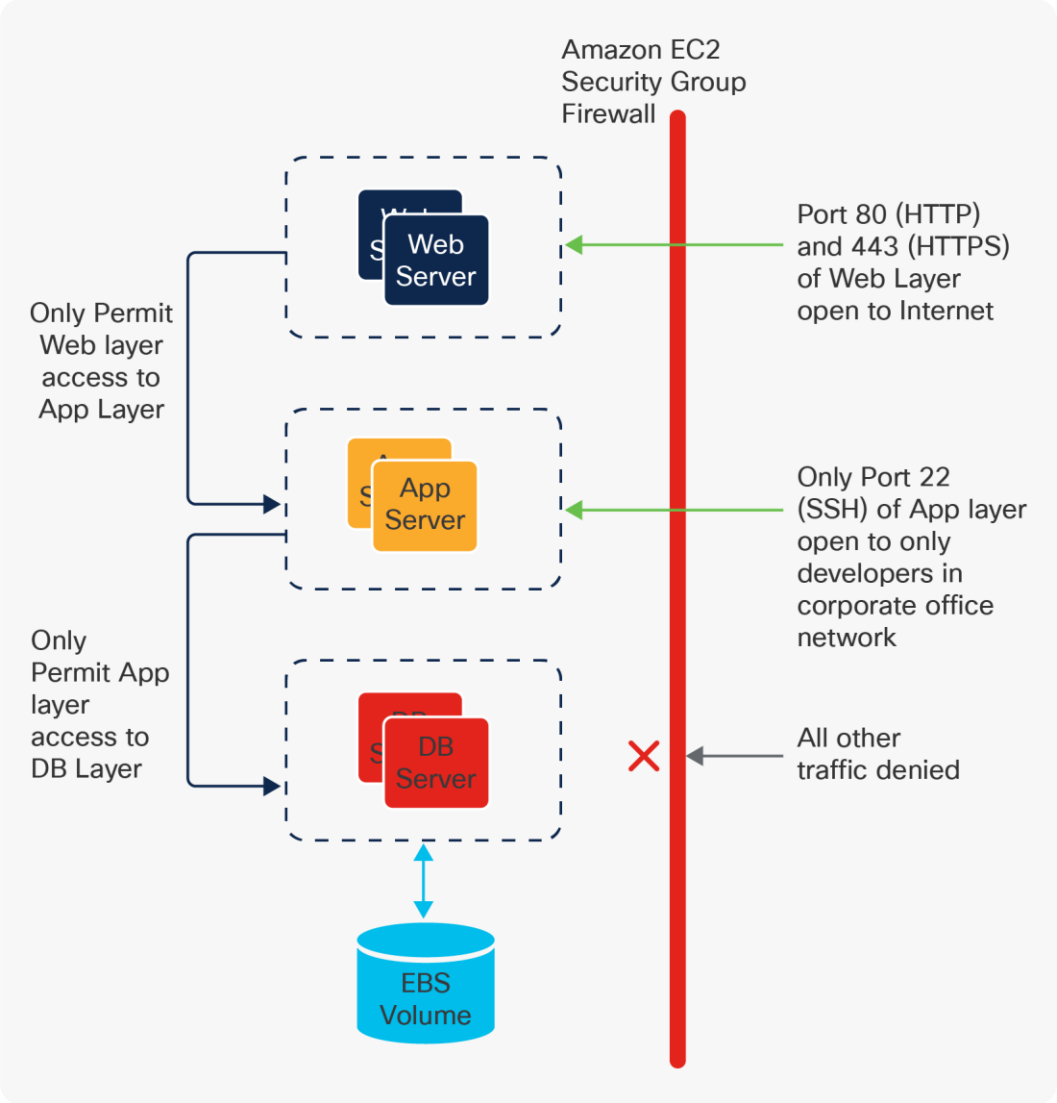


Figure 4.
AWS SG-based network model

*This figure is quoted from the AWS white paper "Web Application Hosting in the AWS Cloud".

Granular and accurate mapping between these two network policy models is crucial to ensure the correct deployment of network policies across Cisco ACI and AWS. Figure 5 shows how Cloud APIC handles this policy mapping.

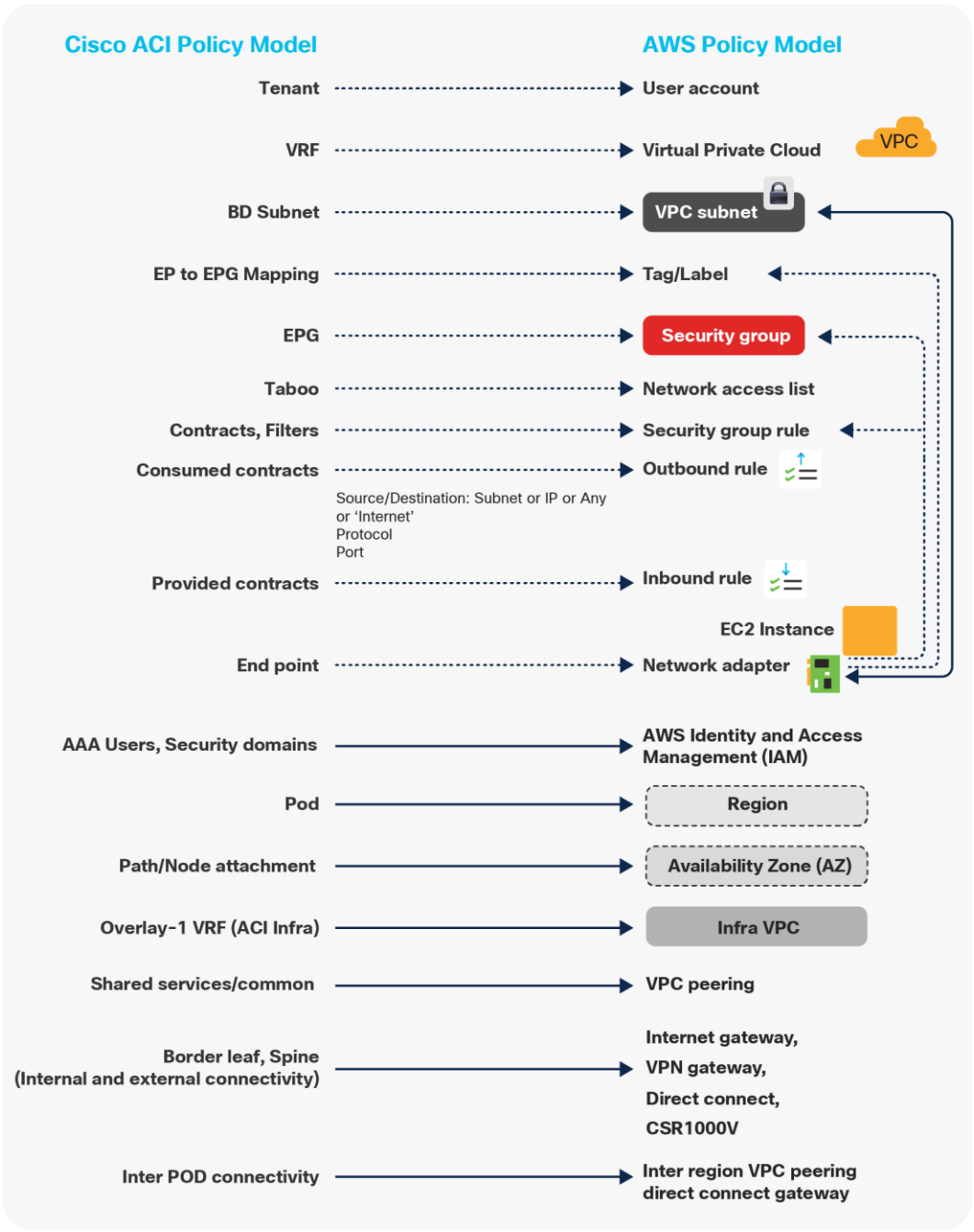


Figure 5.
Cisco ACI policy model to AWS mapping

Unified network management and operations

Cisco ACI Multi-Site Orchestrator (MSO) provides end-to-end visibility and health of all the endpoints managed by it across on-premises and public cloud environments, giving a single place to monitor the health, performance, and operational status of hybrid cloud environments. MSO being the single point of policy configuration and orchestration, this highly reduces the operational complexity of operating across hybrid environments.

Consumption of cloud-native services

Cisco Cloud ACI uses cloud-native constructs for enforcing security and workload segmentation policies. This facilitates the consumption of cloud-native services by workloads managed by Cisco Cloud ACI. Administrators can define policies from MSO regulating which workloads can access which cloud-native services. Inside the AWS environment, these policies then get programmed as security group rules that either allow or deny the workloads to access specific services. To the APIC administrator, whether an application is deployed in part on premises and in part in the cloud does not matter. Familiar EPGs and contracts govern that application's communications. One of the key benefits of this solution is to make Cloud-bursting easy.

Digging further: looking inside an ACI cloud site

Hub-and-spoke topology with an infra VPC

When running Cisco Cloud ACI, a hub-and-spoke Amazon Virtual Private Cloud (VPC) topology is deployed in the AWS-native network infrastructure, based on the translation of Cisco ACI policies into AWS-native policies. The hub is an infra VPC while the spokes are user VPCs where the application endpoints are deployed. Figure 6 shows this concept using IPSec with AWS Virtual Private Gateway(VGW), and Figure 7 shows this concept using AWS Transit Gateway.[3]

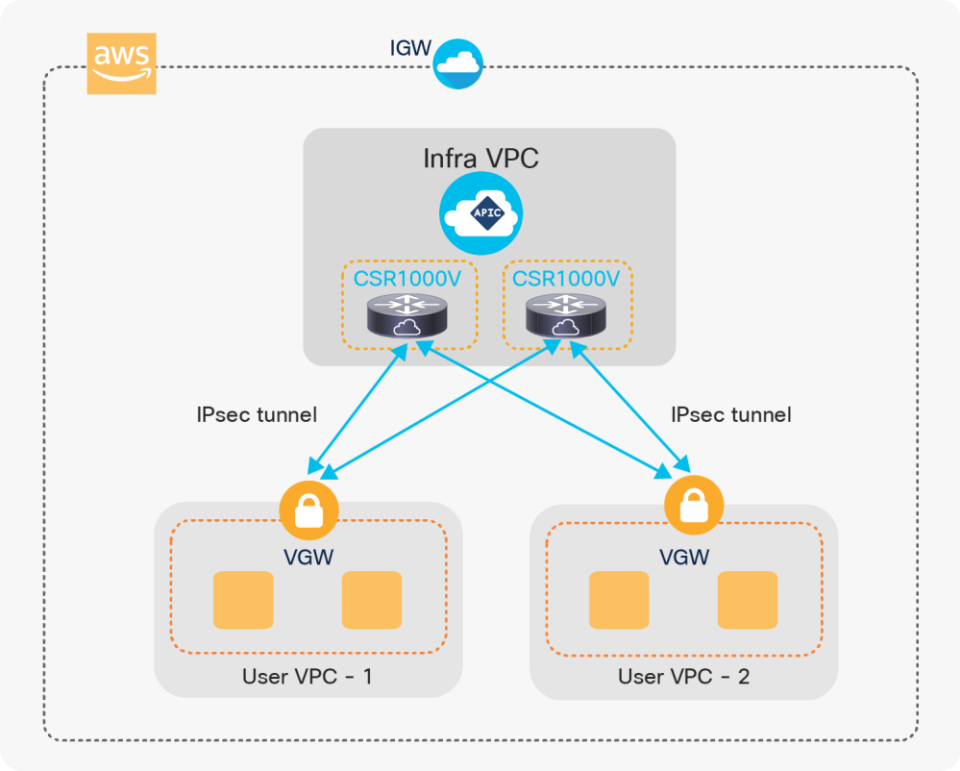


Figure 6.
Inside the cloud using IPsec tunnels with VGW

[3] Starting from Cisco ACI Release 5.0 , AWS Transit Gateway (https://aws.amazon.com/transit-gateway/) is supported.

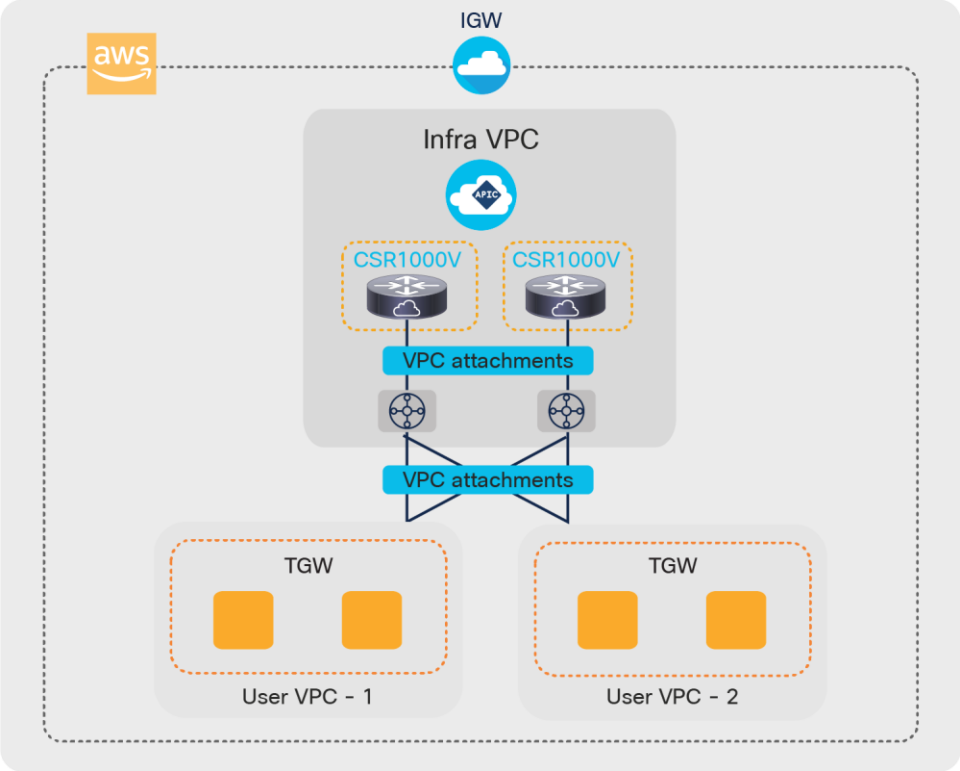


Figure 7.
Inside the cloud using AWS Transit Gateway (after Cisco ACI Release 5.0)

The infra VPC carries the logical role of the on-premises Cisco ACI infra VRF. It is where Cloud APIC is deployed and running. It is automatically created during the deployment of Cloud APIC. Cloud APIC then deploys a pair of Cisco CSR 1000V Series routers in this infra VPC as cloud routers responsible for providing the virtual underlay connectivity, including the internal connectivity within the cloud site and the intersite connectivity to the on-premises Cisco ACI sites. In case of the example described in Figure 7 using AWS Transit Gateways, a pair of AWS Transit Gateways is also automatically created in the infra VPC.

A user VPC is equivalent to a tenant VRF in the Cisco ACI network policy model. Cloud APIC creates a user VPC when an ACI tenant VRF needs to be deployed or extended to the cloud site. Within the user VPC, Cloud APIC provisions an AWS Virtual Private Gateway (VGW) to connect to the infra VPC or configure VPC attachment to the AWS Transit Gateways to connect to the other VPCs to ensure proper end-to-end connectivity.

In case of the example described in Figure 6 using IPsec tunnels with VGWs, IPsec tunnels are automatically provisioned and established between the infra VPC Cisco CSR 1000V Series routers and the user VPC AWS VGWs so that the infra VPC can function as a transit VPC to allow route exchanges between user VPCs through the overlay IPsec tunnels. Endpoint communication between VPCs, and one between a user VPC and the on-premises site goes through VGWs in user VPC and CSR1000Vs in the infra VPC.

In case of the example described in Figure 7 using AWS Transit Gateways, endpoint communication between user VPCs goes through the AWS Transit Gateways and one between the user VPC and the on-premises site goes through the AWS Transit Gateways and the Cisco CSR 1000V Series routers in the infra VPC. This needs each region to have its own local Cisco CSR 1000V in infra VPC. Cloud APIC creates one Transit Gateway route domain per tenant and automatically configures VPC attachments to the AWS Transit Gateway from each VPC, VPC route tables, and Transit Gateway route domains based on VRFs and contracts configuration on the Cloud APIC. If an EPG in a VPC has a contract with an EPG in another VPC, the remote VPC CIDR routes are automatically added to the VPC egress route table by the Cloud APIC, which uses one of the Transit Gateways as the next-hop target, so that inter-VPC traffic within the cloud can be forwarded via the AWS Transit Gateway accordingly.

The use of AWS Transit Gateway is generally recommended because of the following benefits:

- **Higher performance:** AWS Transit Gateway provides significantly more bandwidth than other methods of communication between VPCs. For example, AWS Transit Gateway provides up to 50 Gbps bandwidth for each VPC connection while VPN connections over Internet Protocol Security (IPsec) tunnels are limited to 1.5 Gbps.
- **Simplicity:** AWS Transit Gateway is a network transit hub that interconnects multiple AWS VPCs. Before the introduction of AWS Transit Gateway, interconnectivity among multiple AWS VPCs was achieved by using fully meshed VPC peering or a transit VPC design, both of which add operational complexity. However, AWS Transit Gateway significantly simplifies the inter-VPC connectivity.
- **Potential lower cost:** When using AWS Transit Gateway, you do not need a Cisco Cloud Services Router (CSR) or license if you are connecting VPCs in the same AWS region.

  You still need CSRs for connectivity to the on-premises sites or to other cloud sites. If you need inter-region connectivity between AWS regions that do not support Transit Gateway peering, you still need to use VGWs and CSRs for connectivity.
- **Scalability:** Using VPN tunnels limits the number of BGP routes. However, because AWS Transit Gateway attaches directly to VPCs, it dispenses with using BGP and so supports a greater number of connections.

You can attach 5000 VPCs to each AWS Transit Gateway. Groups of AWS Transit Gateways—called hub networks in the Cisco Cloud APIC solution—support 5000 VPC connections for each region.

An ACI cloud site across multiple AWS regions

An ACI cloud site in AWS can span across multiple AWS regions. While the entire cloud site is managed by the same Cloud APIC, each region can have its own infra VPC with a pair of Cisco CSR 1000V Series routers for networking (as shown in Figure 8 and 9) or share the infra VPC with other regions in case of using IPsec tunnels with VGWs (as shown in Figure 10). User VPCs can be deployed into any of the regions. All of the user VPCs are connected to all the infra VPCs through IPsec tunnels or AWS Transit Gateways.

In case of using IPsec tunnels with VGWs, IPsec tunnels are established between the AWS VGW in each user VPC and all Cisco CSR 1000V routers in the Infra VPC. This provides a full intra-region and inter-region connectivity with virtually a spine-leaf CLOS architecture between infra VPCs and user VPCs. The provisioning of the VPCs, the cloud routers, and the IPsec tunnels is fully automated by Cloud APIC. Meanwhile, MSO automates the provisioning of overlay network connectivity between the on-premises and cloud sites.

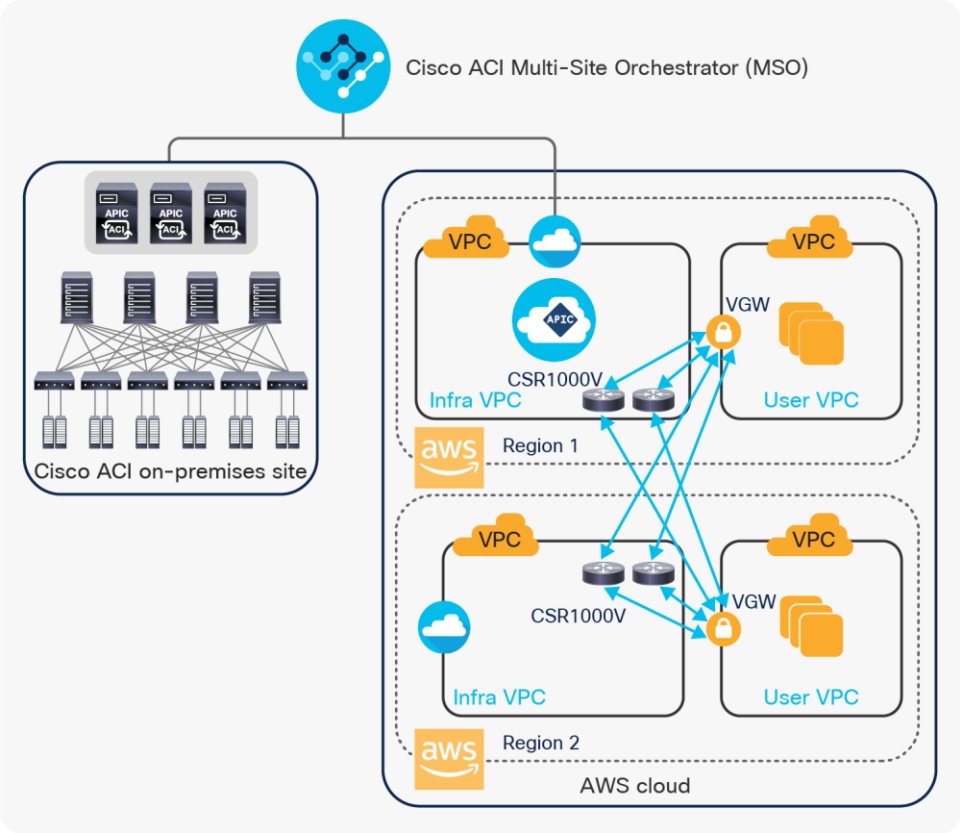


Figure 8.
Cisco Cloud ACI AWS multi-region site with regional dedicated Infra VPC using IPsec tunnels with VGW

In case of using AWS Transit Gateways, in addition to VPC attachments to the AWS Transit Gateways from each user VPC and route-table configurations, inter-region peering between AWS Transit Gateways are also automatically configured by Cloud APIC. This provides intra-region and inter-region connectivity between infra VPCs and user VPCs without full-mesh VPC peering or a transit VPC design. Inter-region connectivity goes through the AWS Transit Gateway peering. Communication between VPCs within the region goes through the local AWS Transit Gateways.

This option needs Cisco CSR 1000V Series routers in each region for traffic between the on-premises and cloud sites, which is via AWS Transit Gateway and CSR 1000V routers in the infra VPC. If an endpoint in a VPC needs to communicate with an endpoint in another cloud or on-premises site, the remote site prefix routes are programmed in the VPC egress route table by the Cloud APIC, and the AWS Transit Gateway is used as the next-hop target. Then the Transit Gateway route domain for the tenant uses the infra VPC attachment as the next-hop target for the 0.0.0.0/0 subnet. The infra VPC route table uses an ENI of a CSR 1000V router in the infra VPC as the next-hop target for the 0.0.0.0/0 subnet. Thus, each region must have CSR 1000V routers in the infra VPC. If that ENI is down, the infra VPC route table will automatically use an ENI of the remaining CSR 1000V router as the next-hop target.

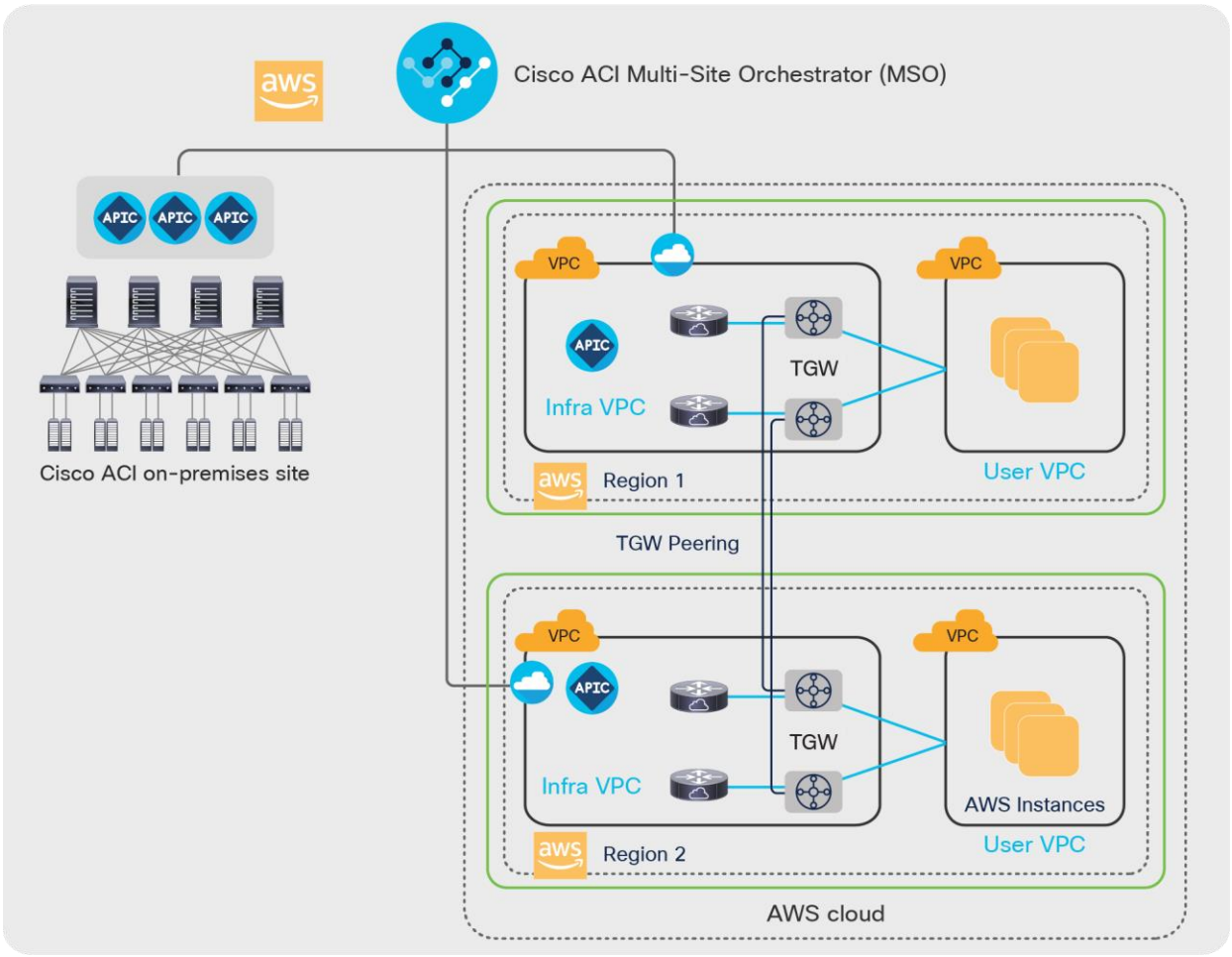


Figure 9.
Cisco Cloud ACI AWS multi-region site with regional dedicated Infra VPC using AWS Transit Gateway

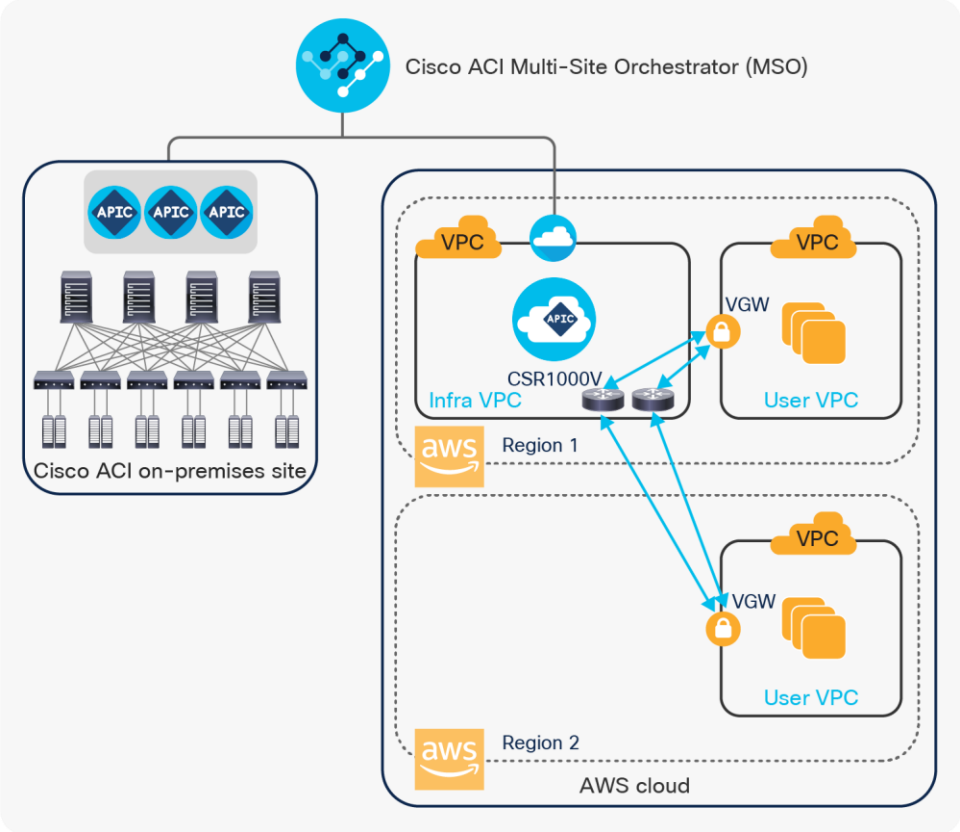


Figure 10.
Cisco Cloud ACI AWS multi-region site with shared Infra VPC using IPsec tunnels with VGW

Traffic flows inside the cloud site

Traffic between two endpoints in the same VPC is routed locally in the VPC. It does not need to go through the infra VPC or hairpin back on premises. Traffic between two endpoints that are in different VPCs needs to be routed through the Cisco CSR 1000V Series router in the infra VPC or AWS Transit Gateway. Traffic between an endpoint in a cloud site and an endpoint on premises needs to be routed through the Cisco CSR 1000V Series router in the infra VPC.

Intersite connectivity

The underlay network between on-premises and cloud sites

The on-premises Cisco ACI sites and the ACI cloud site in AWS are connected through IPsec tunnels over the underlay IP network between the sites. The IPsec tunnels on the ACI cloud site are automatically programmed on the Cloud Cisco CSR 1000V Series routers in the infra VPC. The customer needs to manage the on-premises IPsec devices on which the inter-site IPsec tunnels terminate. The underlay IP network can go through the Internet, or a private path that consists of AWS Direct Connect[4]. This underlay network provides IP reachability for the overlay control plane and data plane between the two sites. This is represented in Figure 11.

[4] As of Cisco ACI Release 5.1, though this solution does not take care of an automatic creation or management of AWS Direct Connect, AWS Direct Connect can be used in conjunction with the solution.

For inter-VPC connectivity, either IPsec tunnels using VGWs in user VPCs or AWS Transit Gateway is supported in conjunction with the intersite connectivity using IPsec VPN over the Internet of AWS Direct Connect, as shown in Figure 11.

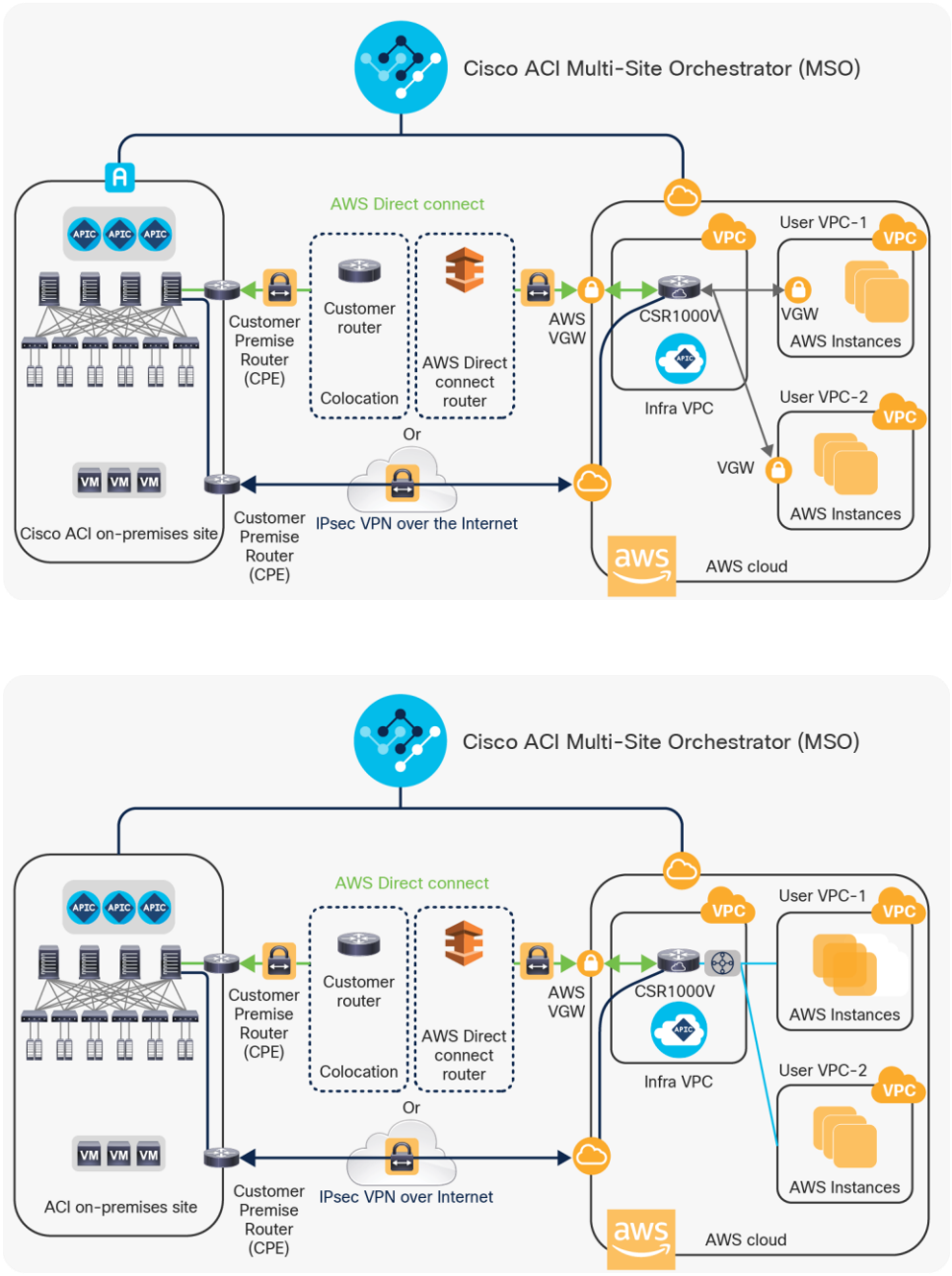


Figure 11.
The underlay network between on-premises and cloud sites

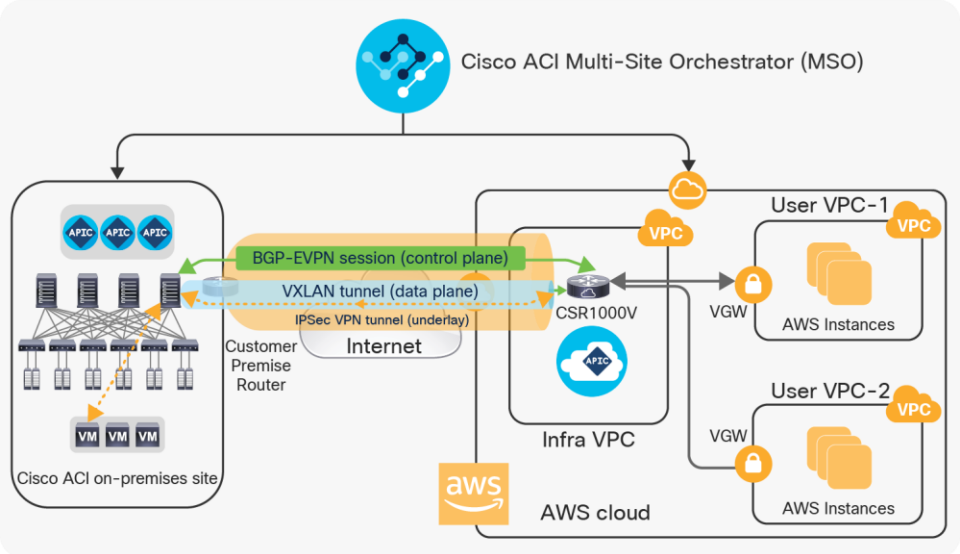
The overlay network between on-premises and cloud sites

The overlay network between the on-premises and cloud sites runs BGP EVPN as its control plane and uses VXLAN encapsulation and tunneling as its data plane. From an architecture perspective, this overlay network uses the Cisco ACI GOLF feature[5] (also known as Layer 3 EVPN Services for Fabric WAN).

BGP EVPN sessions are established between the on-premises Cisco ACI spine switches and the Cisco CSR 1000V Series cloud routers in the Infra VPC of the cloud site. Tenant host routes and prefix routes are exchanged between the two sites as BGP EVPN route type-2 (host) and type-5 (prefix). The provisioning of this overlay network connectivity is automated by MSO.

Figure 12 zooms in on this logical/physical architecture. On-premises spines connect to an intersite network (called ISN or IPN for inter-pod network). That IPN layer then connects to an on-premises IPsec router that initiates IPsec tunnels to the Cisco CSR 1000V Series routers in the AWS Infra VPC. MP-BGP EVPN sessions are established between the ACI spine switches and the Cisco CSR 1000V series routers in the AWS Infra VPC over the IPN network and the IPsec tunnels. For inter-VPC connectivity, either the use of IPsec tunnels using VGSw in user VPCs or AWS Transit Gateway is supported.

You might need to adjust Maximum Transmission Unit (MTU) size on ACI Control Plane MTU policy for BGP EVPN control-plane and on your endpoints for data plane to avoid fragmentation because of IPsec tunnels and VXLAN encapsulation overhead. Otherwise, fragmentation by devices in the network could degrade overall performance. For example, if MTU of the involved endpoints is adjusted to 1300 bytes, this would account for the additional 50 bytes from VXLAN and around 100 bytes for IPsec overhead to go over the Internet where the common value of MTU is 1500 bytes. If adjusting MTU size on your endpoints is not allowed or preferable, you need to configure TCP Maximum Segment Size (MSS) Adjustment on Cisco CSR 1000V Series routers from cAPIC. This configuration option is available starting from Cisco Cloud APIC Release 4.2(4q), 4.2(5n), and 5.0(2i).



[5] https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/2-x/L3_config/b_Cisco_APIC_Layer_3_Configuration_Guide/b_Cisco_APIC_Layer_3_Configuration_Guide_chapter_010010.html

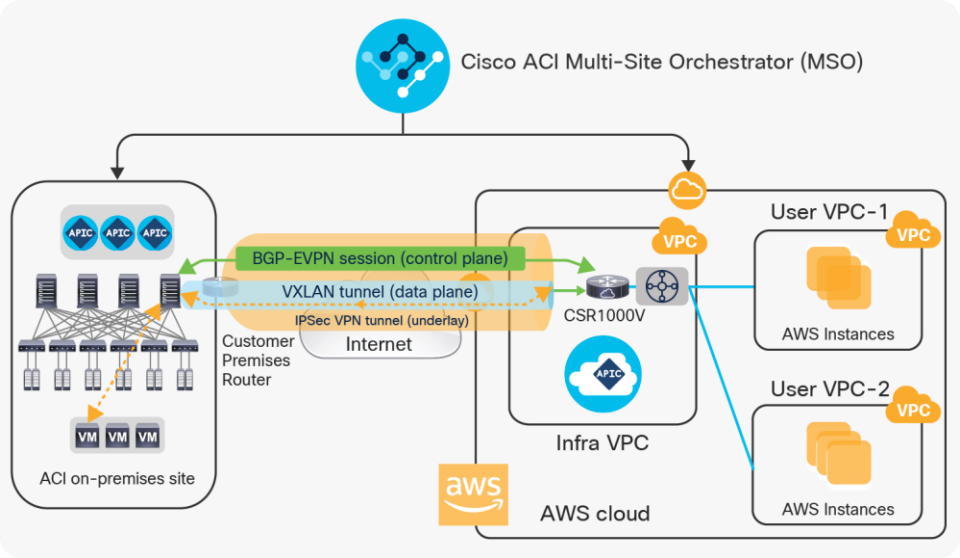


Figure 12.
The overlay network between on-premises and cloud sites

Use-case scenarios

Cisco Cloud ACI enables customers to achieve the following scenarios:

High Availability of applications across on-premises and cloud sites

Cisco Cloud ACI enables customers to deploy an application in High Availability by stretching it across on-premises and cloud sites. This makes it possible to have a multitier application deployed across a hybrid-cloud environment all in the same Virtual Routing and Forwarding domain (VRF).[6]

Customers having application tiers deployed on an on-premises Cisco ACI site can now add new application tiers in an cloud site interacting with the on-premises tiers using consistent policies.

Applications can fail over between the on-premises Cisco ACI site and the ACI cloud site during a disaster recovery, or the application can be deployed in an active/active mode, where both on-premises application tiers and cloud tiers are active. A Global Load Balancer can be configured to distribute traffic between the two sites.

For example, the web and application tiers of an application (two EPGs) in the same VRF running in the on-premises Cisco ACI data center. By stretching the same VRF to the cloud site, we can deploy web and application tiers in the cloud site, and can be configured as an active/active between the on-premises and cloud sites. You can also deploy the on-premises web and application tiers as active, and the cloud tiers can act as standby, and can fail over to a cloud tier in case of a disaster recovery.

All of this can be achieved by using MSO as a single point of orchestration; you can configure contracts between these tiers spread across the hybrid cloud environment. Simply publishing this policy from MSO to both sites programs the end-to-end constructs required to implement the workload segmentation policy. This is shown in Figure 13.

[6] Note: Extending a broadcast domain between an on-premises site and the cloud is not possible. Cloud vendors typically do not run broadcast or multicast and never face unknown unicast situations.

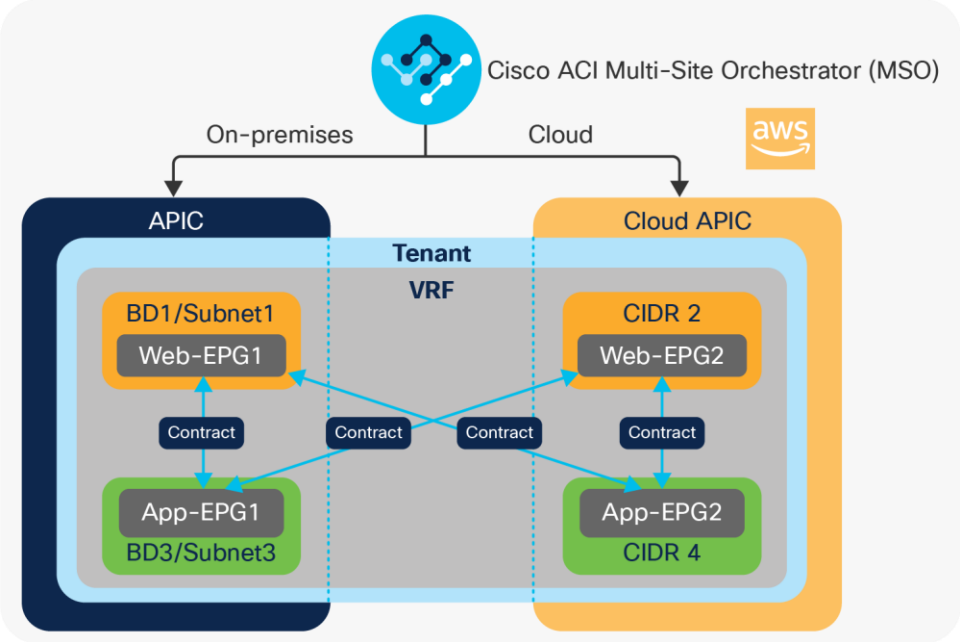


Figure 13.
An example of stretched application between on-premises Cisco ACI and cloud sites

Cloud bursting: stretch an application tier (EPG) to cloud with consistent segmentation

Cisco Cloud ACI enables customers to stretch an application tier across the on-premises and cloud sites in AWS, which means that an ACI EPG can be stretched across the on-premises and AWS sites. This enables customers to burst a tier to AWS Cloud during times of peak load and access other tiers of the application on premises via secure segmentation policies. Even multiple tiers can be burst to the cloud site in AWS and still maintain the same level of policy and consistent segmentation irrespective of where the workloads are deployed.

From MSO, you can either create a new EPG that can then be stretched or import an existing EPG from the on-premises site and stretch it to AWS. This is achieved just as you would with regular Cisco ACI Multi-Site, using templates and schemas. Once that is done, configure the site-local properties that define how the EPG should classify its member endpoints.

When associating an EPG with an on-premises ACI site, you can either associate the EPG to a Virtual Machine Manager (VMM) domain, or to static ports or a VLAN/port combination to classify endpoints on premises. When the same EPG is associated with an cloud site in AWS through MSO, EPG membership classification criteria can then be based on AWS tags, or AWS IP subnets or IP addresses, or AWS regions.

Stretching an EPG does not mean extending a broadcast domain from an on-premises site to the cloud, though; it simply means that you can create an EPG with members on premises and in the cloud, using different subnets. Once two or more endpoints are in the same EPG, communication flows freely inside that EPG.

Example: Let's say you have an application with web and application tiers deployed in an on-premises ACI site. During a peak load time, you burst either web tier or both web and application tiers to the cloud site in AWS. You can do that seamlessly with just a couple of button clicks from Cisco ACI MSO, and stretch the tiers to AWS with the same level of security and segmentation as their on-premises workloads. Now, contracts between stretched Web EPG and on-premises EPGs or Cloud EPGs can be configured as you normally would with an on-premises ACI. Cloud-bursting doesn't get any easier. This is shown in Figures 14.

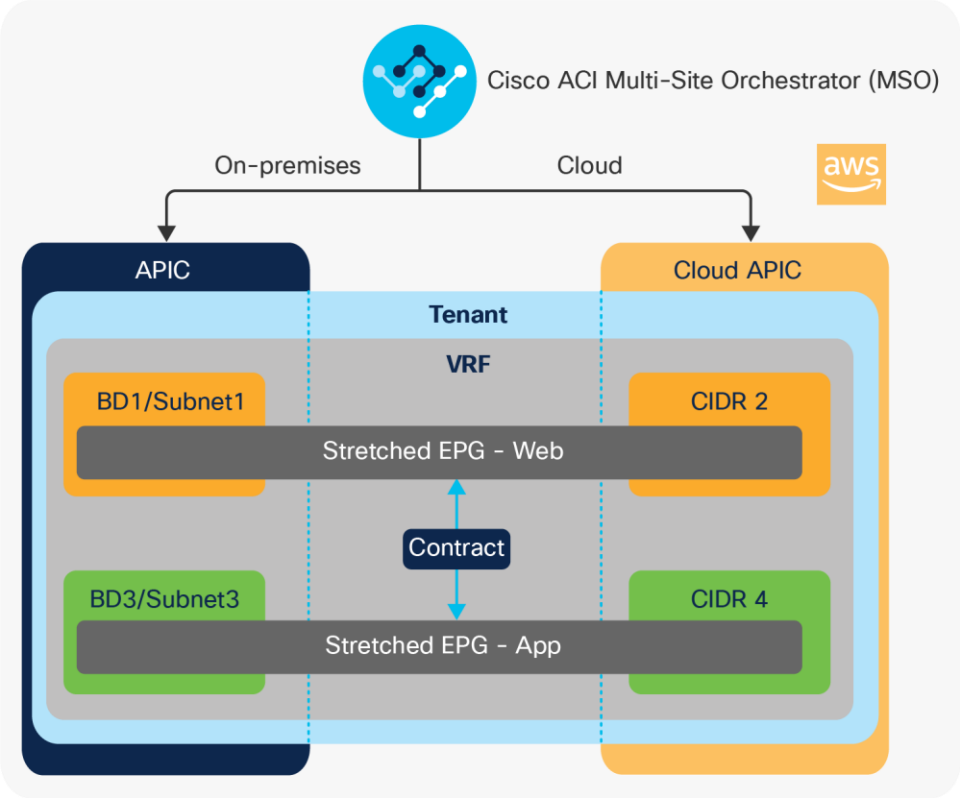


Figure 14.
An example of stretched EPGs across sites

Shared services across hybrid cloud

Shared services such as DNS, Active Directory (AD), or other authentication services deployed in a tenant in an on-premises ACI site can be securely consumed by endpoints in other tenants spread across other Cisco ACI and AWS sites. This enables services from a single on-premises provider tenant to be consumed by multiple consumer tenants spread across the on-premises ACI site and cloud sites in AWS.*

This makes it easier to deploy new applications in the cloud, and consume shared services from the brownfield network on premises, without having to redeploy them for applications hosted in the cloud.

* As of Cisco ACI Release 5.1, inter-tenant shared service is not supported, for example, a contract between a provider EPG in the cloud and a consumer EPG in on-premises is not supported if EPGs are in different tenants.

Example: Let's say there are DNS servers deployed in Tenant-1, an on-premises ACI site. Workloads that are part of the Web-EPG deployed on the cloud site in AWS in Tenant-1 can access these DNS shared services from the on-premises ACI site via an Inter-VRF contract between the DNS-EPG and the Web-EPG. This is shown in Figure 15.

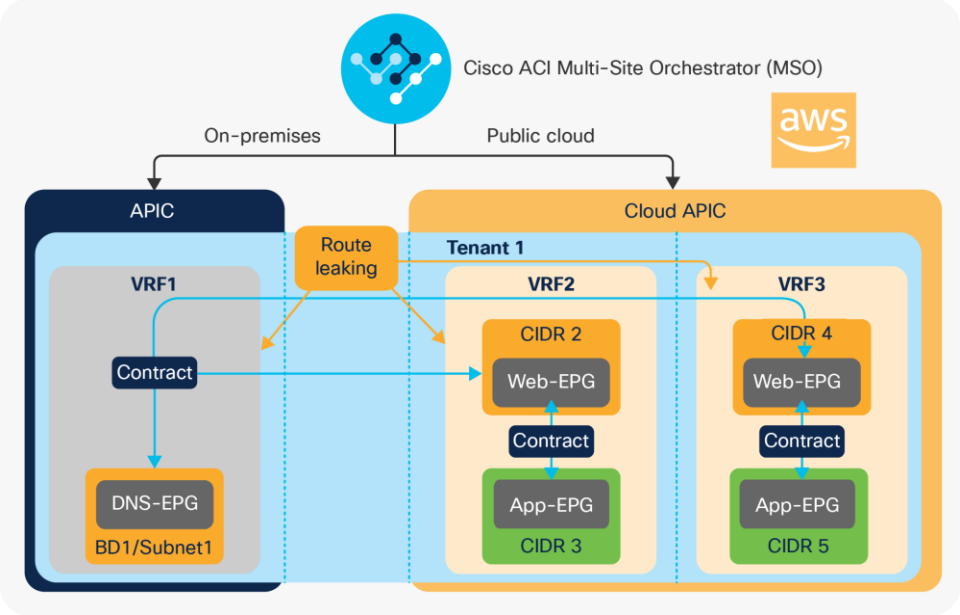


Figure 15.
An example of intersite shared services

External connectivity to the internet via the cloud or on-premises

External connectivity to the Internet for workloads in AWS Cloud can be configured in two ways:

1. Cloud L3Out: A cloud-local Internet connection (also called L3Out in Cisco ACI terminology) can be defined for workloads deployed on AWS. It is achieved by configuring a cloud-External EPG in MSO for the cloud site in AWS. A Cloud-External EPG will create an Internet Gateway (IGW) and attach it to every VPC in the AWS site and appropriate routes will be programmed into the VPC route tables.
2. On-premises L3Out: Some customer environments require all the traffic from a VPC in AWS to transit to an on-premises site and be inspected through an on-premises firewall/IDS/IPS before the traffic exits to, or enters from, the Internet. This can also be achieved by defining an on-premises L3Out as the Internet exit for traffic and associating the cloud endpoints to that EPG via a contract.

Customers have full control over external network connectivity options for workloads deployed in the cloud and can choose to redirect the traffic for inspection by various services deployed on premises by using Cisco ACI service graphs. All this can be done through a single policy, and end-to-end connectivity can be automated and orchestrated by Cisco ACI Multi-Site Orchestrator, greatly simplifying the operational workflows.

Example: When an administrator configures a cloud L3Out in the AWS environment (as shown in Figure 16), each AWS VPC will have an AWS Internet Gateway (IGW) attached to it, and the Amazon EC2 instances in the VPC can directly communicate with the Internet based on the policies defined.

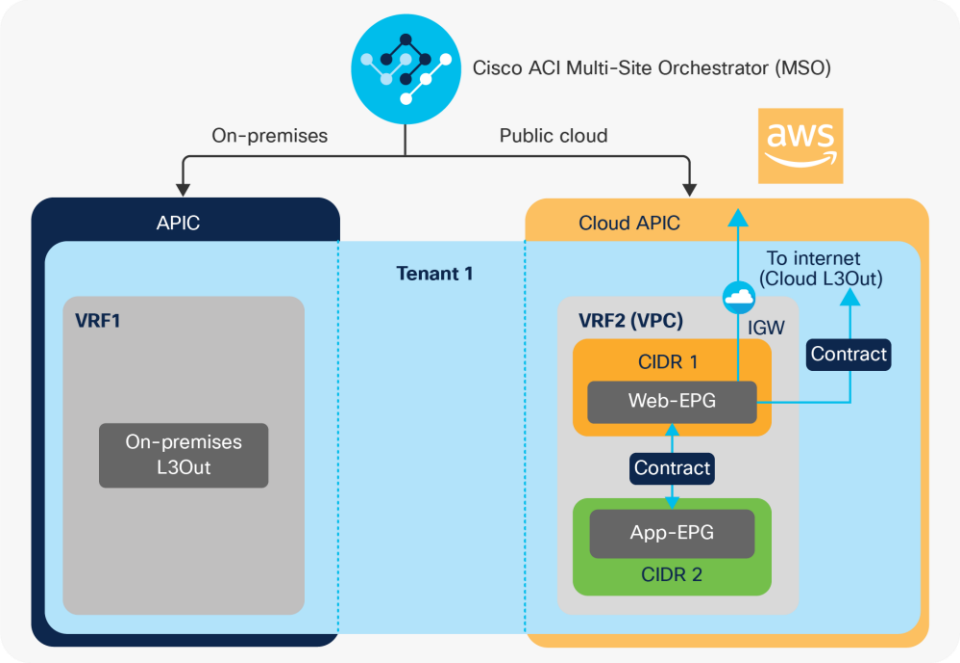


Figure 16.
An example of Cloud L3Out

If the administrator defines an on-premises Cisco ACI L3Out (as shown in Figure 17) and forces cloud instances to use that L3Out, then all traffic from Amazon EC2 instances reaches the Cisco CSR 1000V Series router via the VPN tunnels, and will be sent on premises over the VXLAN tunnel running over the IPsec tunnel. Traffic can then exit via the on-premises Cisco ACI L3Out instead of using the AWS Internet gateway directly.

Once traffic reaches the on-premises Cisco ACI site, the administrator may choose to subject this traffic to various inspections using the service chain options in Cisco ACI and then let the traffic exit to the Internet.

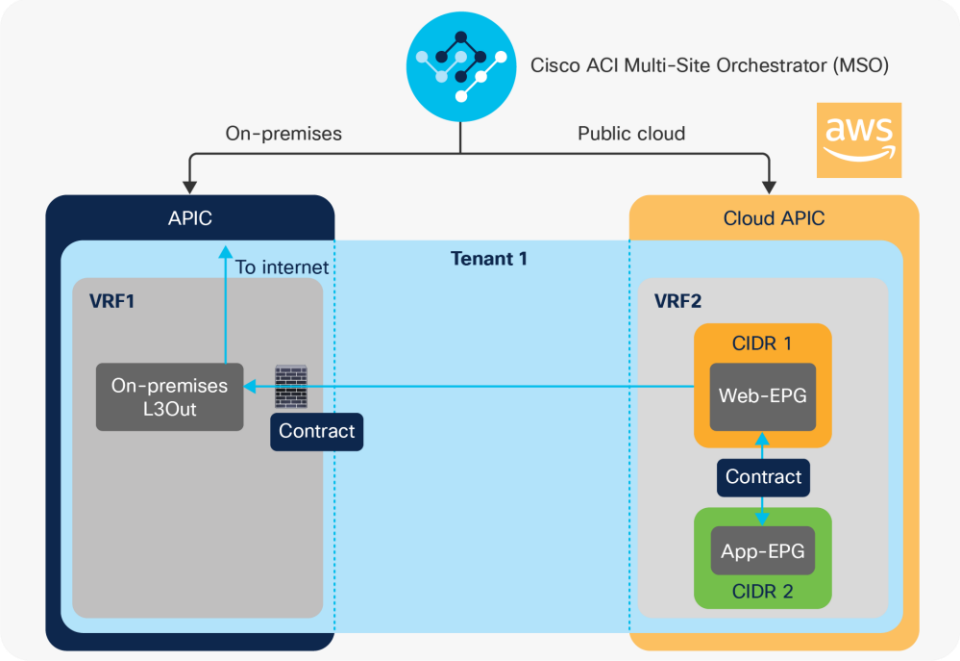


Figure 17.
An example of On-Premises L3Out for cloud endpoints

Cloud-native and on-premises services

Cisco Cloud ACI makes it easy to securely consume services that are either cloud-native in AWS or on premises.

1. AWS Application Load Balancer: Using service graph concepts similar to those for on-premises ACI, you can seamlessly integrate cloud-native services such as AWS Application Load Balancer (ALB) with your application stack. This can be fully configured from MSO, and the Cloud APIC will automate end-to-end deployment and configuration of ALB in the VPC and associate it with endpoints in a given endpoint group.
2. On-premises services: For application tiers that are split across on-premises and AWS sites, you can seamlessly insert on-premises services (such as load balancer or firewall). This can be achieved by configuring ACI service graphs from MSO.

Example: Let's say we need an east-west firewall between the database tier deployed on premises and a web tier that is stretched across the hybrid cloud environment. As shown in Figure 18, this can be configured with much ease using ACI Service graphs from MSO, and the traffic between the database and web tiers always passes through this firewall irrespective of where the endpoints of the web tier are located across the hybrid cloud.

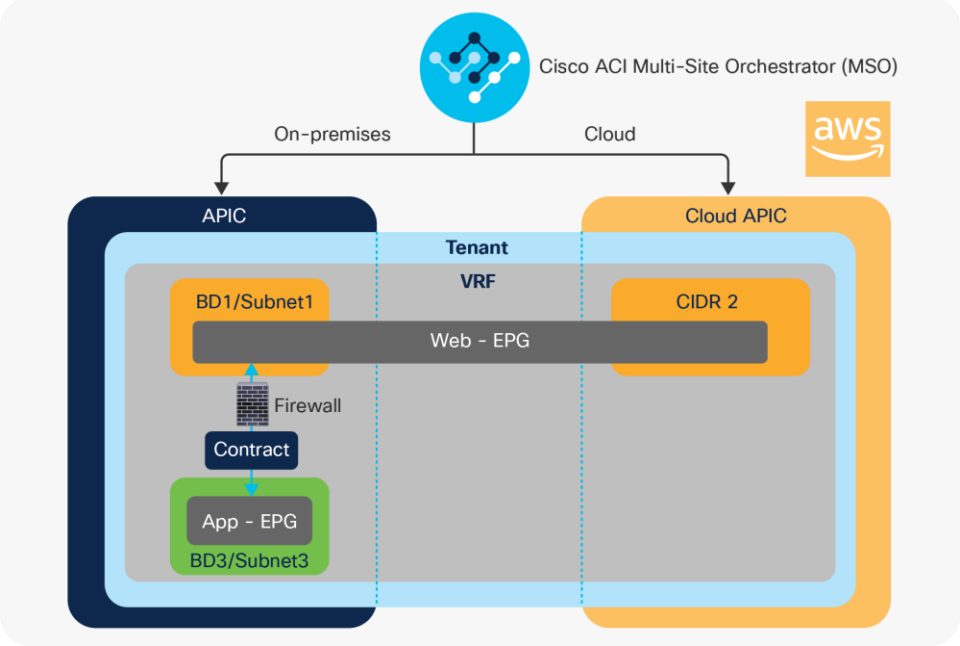


Figure 18.
On-premises service chaining for a stretched application tier

How to deploy the solution

Deploying Cisco Cloud APIC and the Infra VPC

The AWS AMI images for Cisco Cloud APIC are available at AWS marketplace, and uses the BYOL model for licensing at the time of the writing of this white paper. Readers are encouraged to refer to the ordering guide for any other options.

The first step to deploy Cisco Cloud ACI is to configure the Infra VPC and to launch Cisco Cloud APIC in AWS. Those steps are all performed by using a Cisco-provided AWS CloudFormation template, which allows you to create automation workflows called stacks that will execute a series of steps on your behalf.

CloudFormation uses a JSON or YAML template to describe the automation workflows. Cisco provides a CloudFormation template to execute the necessary steps to configure Cisco Cloud ACI integration. The CloudFormation template is available in AWS marketplace and can be executed from there. Alternatively, it can be downloaded from Cisco public website and used to initiate a CloudFormation stack as shown in Figure 19. This stack will prompt the user for the required parameters defined in the template and will run the tasks defined in the workflow. A walkthrough of deploying Cisco Cloud APIC in AWS is available at https://www.cisco.com/c/m/en_us/products/data-center/software-demos/aci/cloud-apic-deployment-walkthrough.html.

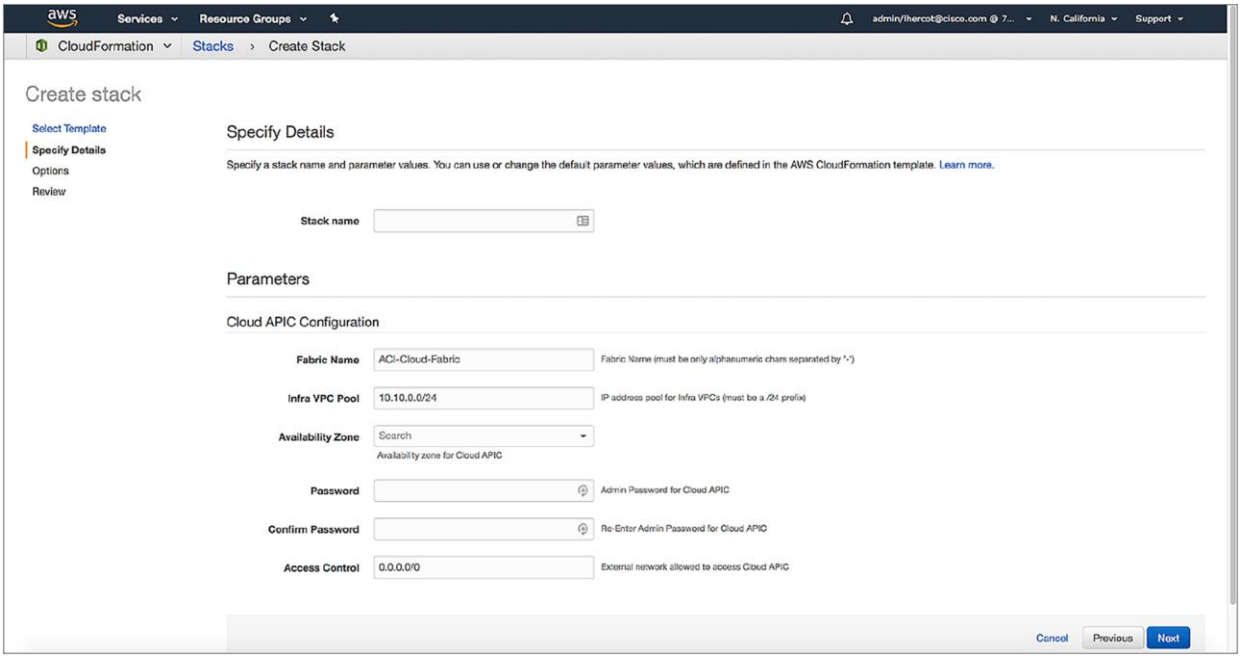


Figure 19.
Create CloudFormation stack to launch Cisco Cloud APIC on AWS

Once the CloudFormation template is deployed successfully, your Cisco Cloud APIC becomes accessible via its Web UI and API. As shown in Figure 18, you can find the public IP address of Cisco Cloud APIC by viewing the CloudFormation template outputs or by consulting the elastic IP address assigned to the Cloud APIC Amazon EC2 instance. Connect to the Cisco Cloud APIC UI to complete the installation through the getting-started wizard.

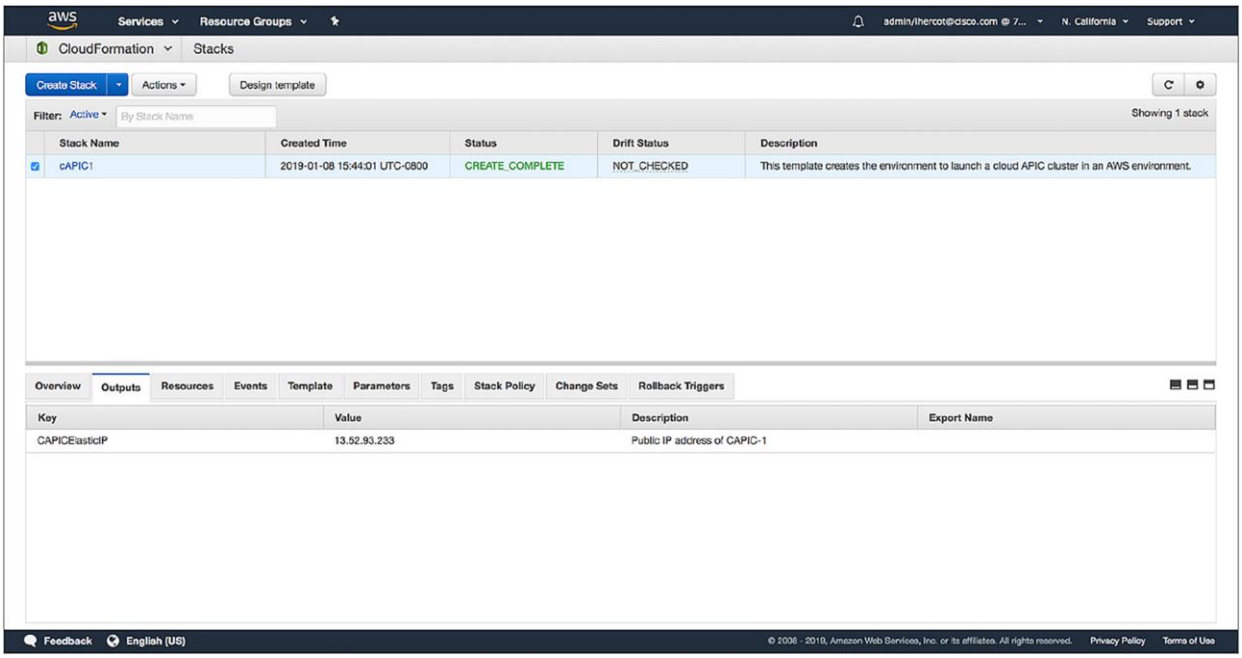


Figure 20.
CloudFormation template output with Cisco Cloud APIC Public IP address

Cisco Cloud APIC's First Time Setup wizard

The first time you connect to Cisco Cloud APIC UI, the First Time Setup wizard (shown in Figure 21) automatically kicks off. This wizard helps you configure some of the Cisco Cloud APIC required settings, such as DNS, the TEP pool, the regions to be managed, and IPsec connectivity options. At the end of the First Time Setup wizard, Cisco Cloud APIC configures the AWS infrastructure needed to become fully operational, such as the pair of Cisco CSR 1000V Series routers. The provisioning of the AWS infrastructure is fully automated and carried out by Cisco Cloud APIC. After this step, you will be able to start deploying your Cisco ACI policy on AWS.

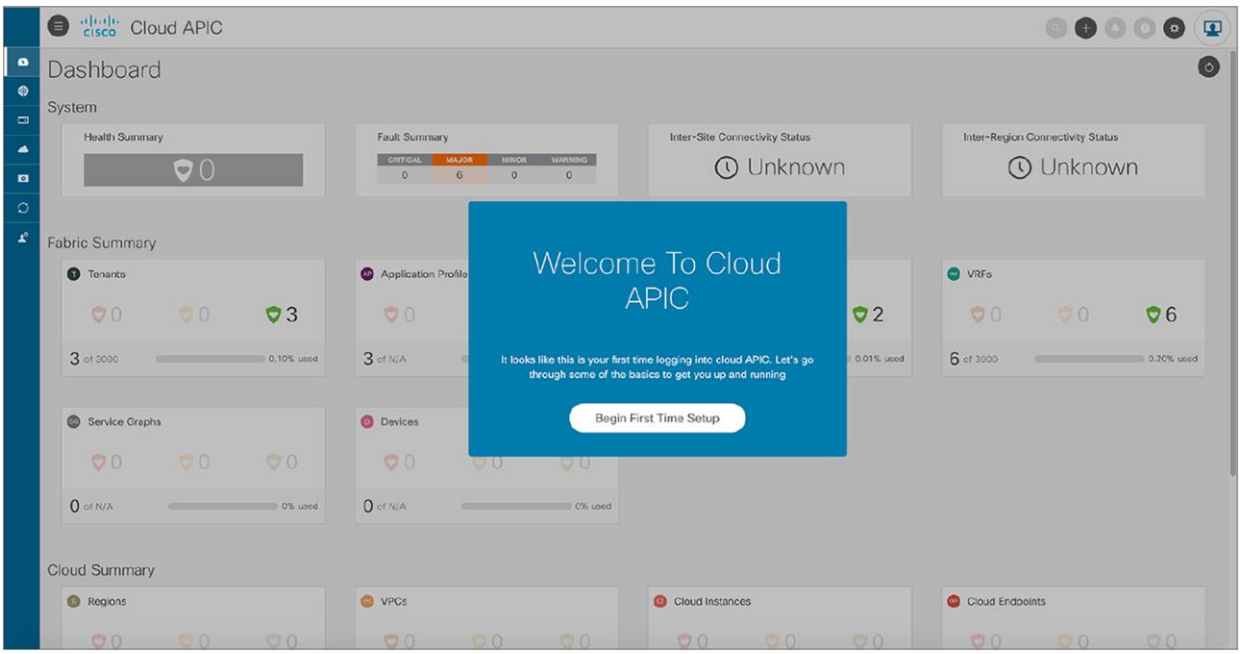


Figure 21.
First time setup wizard of Cisco Cloud APIC

Registering a Cisco ACI cloud site in MSO

Each Cisco Cloud APIC represents a Cisco ACI site. To extend policy across sites, Cisco ACI uses the Cisco ACI Multi-Site Orchestrator (MSO). As shown in Figure 22, when you register a Cisco Cloud APIC in MSO, it will appear as a new site and will allow you to deploy existing or new schemas to AWS. MSO ensures that you specify the required site-specific options, such as subnets and EPG membership classification criteria, which are different for each site.

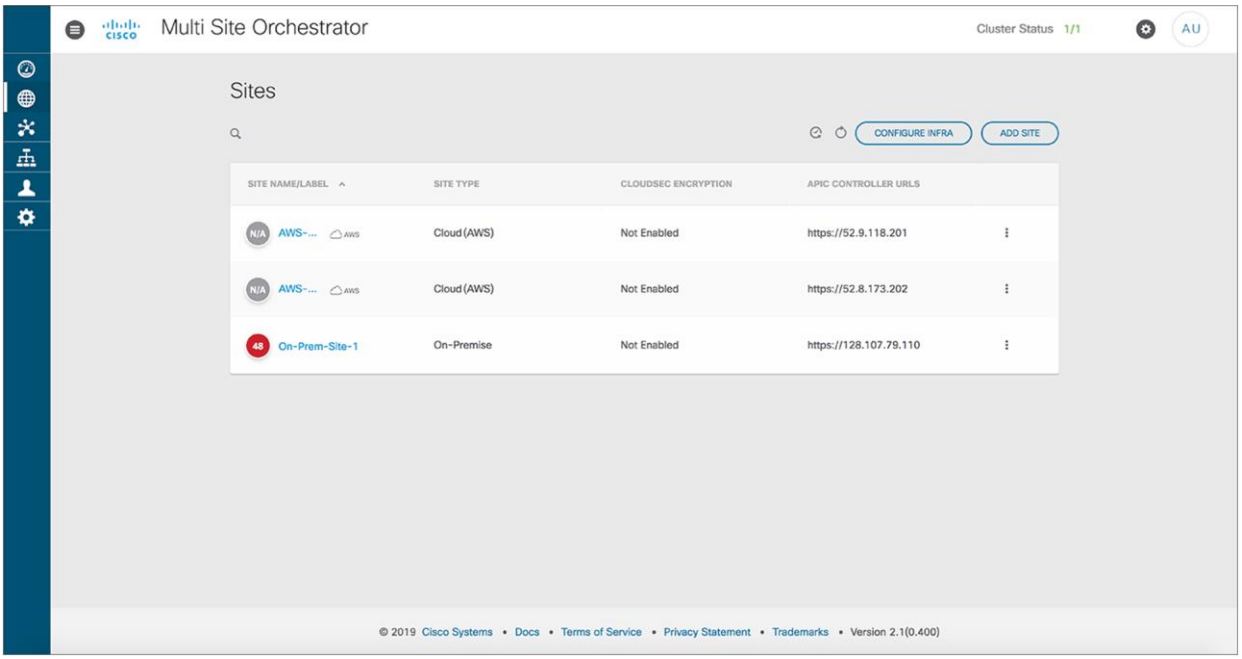


Figure 22.
Register a Cisco ACI cloud site in MSO

Cisco Cloud APIC lets you create networks on AWS using the Cisco ACI object model representation. In the backend, Cisco Cloud APIC translates Cisco ACI objects into AWS-native constructs. This means that Cisco Cloud ACI adheres to AWS networking specifications. As those differ slightly from what you might be used to with Cisco ACI, they are detailed below.

As shown in Figure 23, In AWS, a subnet is bound to an Availability Zone (AZ) of a VPC, which itself is bound to a region.

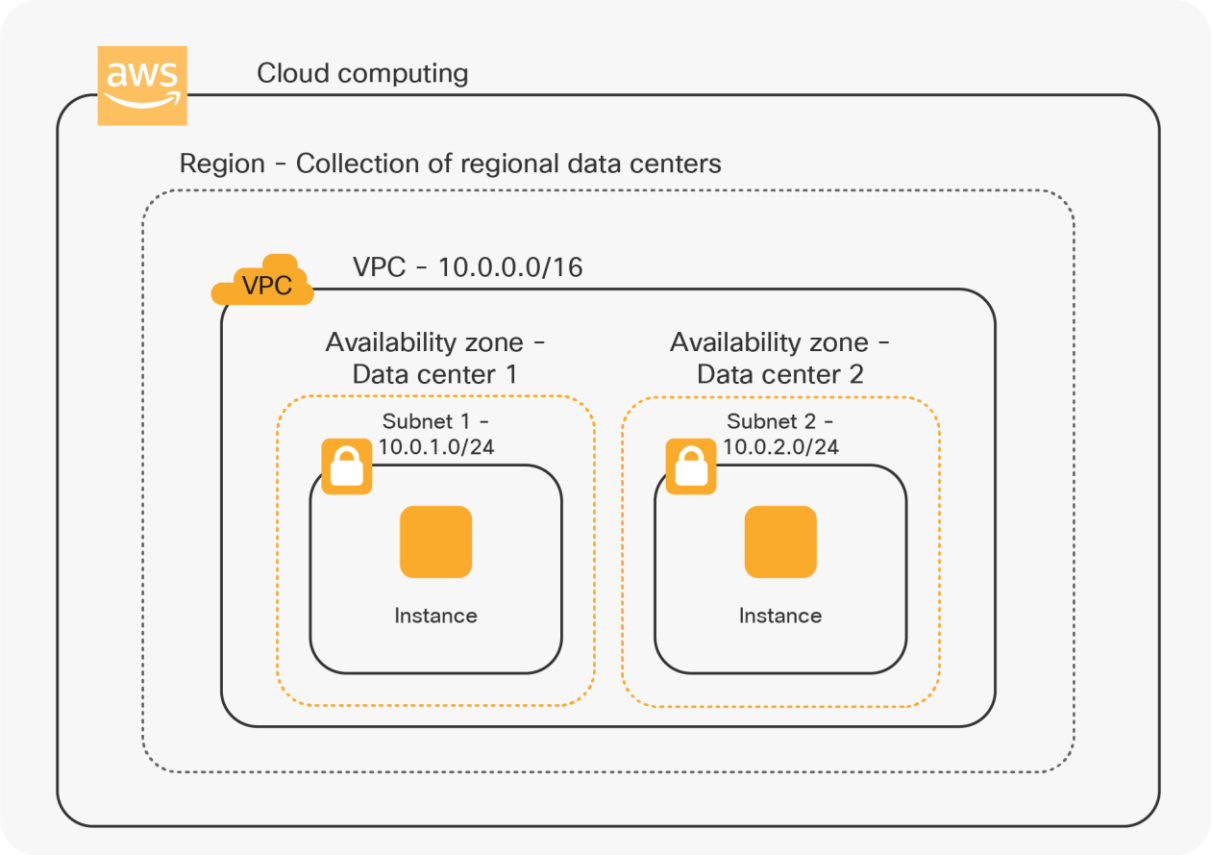


Figure 23.
AWS-native network construct

This means that, between AZs, VPCs, or regions, the traffic is routed. There is no concept of extending L2 from one VPC to another VPC or from the on-premises site to a VPC in AWS. To respect this design philosophy, Cisco Cloud ACI extends on-premises networks using L3 only.

Cisco Cloud APIC also provides a view of the AWS-native constructs used to represent the Cisco ACI policy. This allows network administrators to gradually familiarize themselves with AWS networking constructs. Figure 24 below demonstrates the native cloud resources view on the Cloud APIC UI. As an example, it shows the display of the provisioned AWS VPCs in a cloud site.

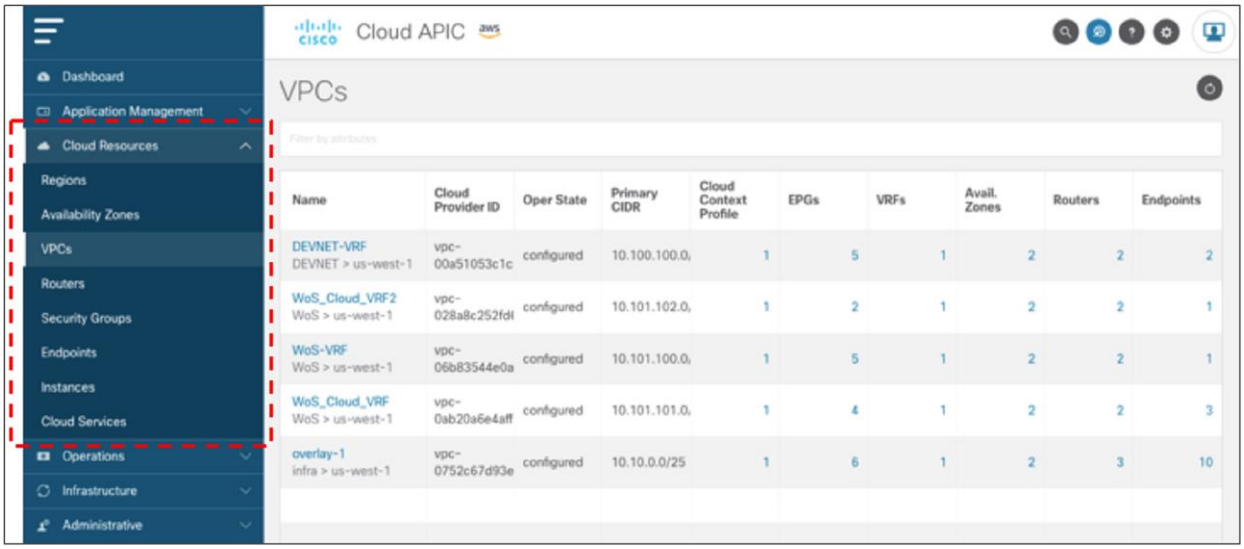


Figure 24.
Native cloud resources view on the Cloud APIC UI

Deploying a multi-tier application in a hybrid scenario

We use a classic three-tier application as an example in this session. The application consists of a Database (DB), App, and Web tier. To deploy it across an on-premises data center and the AWS cloud using Cisco Cloud ACI integration, you will need to configure a schema on MSO that represents this policy. As shown in Figure 25, it should contain at least one VRF, one Application Profile, and three EPGs (one EPG for each tier of the application) as well as contracts between the tiers. For example, the App and DB tiers can be deployed on premises and the Web tier in AWS. Or you can use any permutation of this set as you see fit, including (as explained previously) the option to stretch one or more EPGs between the on-premises data center and the cloud.

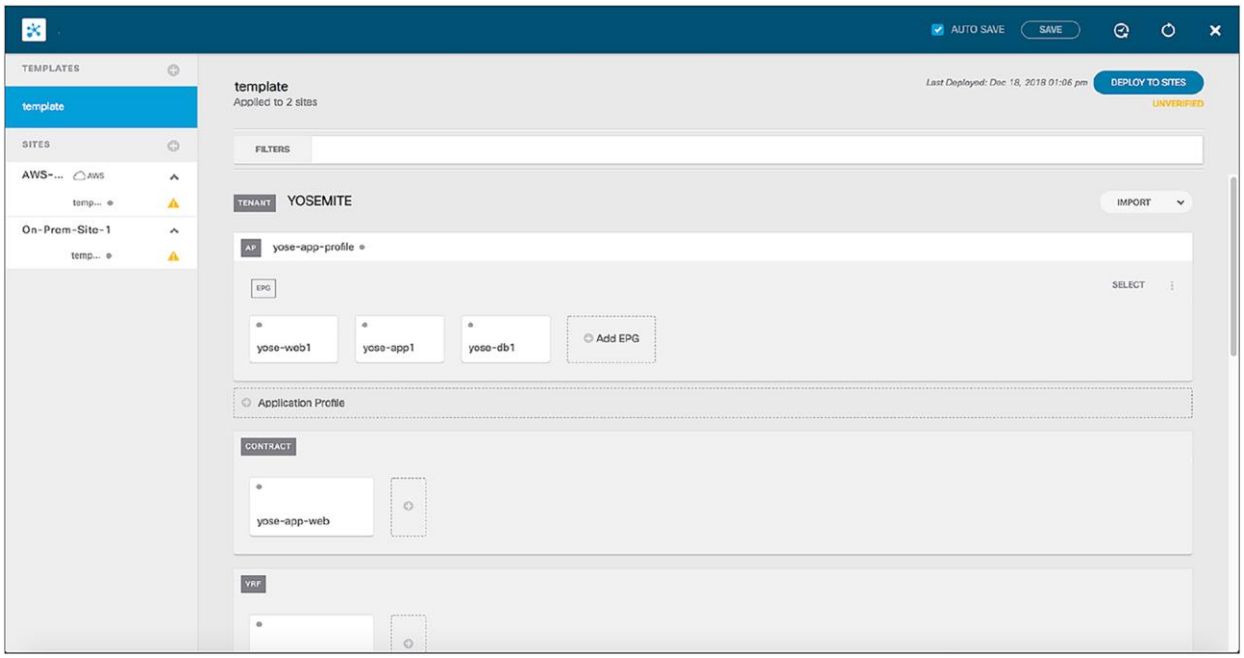


Figure 25.
Three-tier application schema on MSO

The schema can then be associated with the on-premises site and the Cisco Cloud ACI site. Once the association is made, you then define the subnets to be used for the VRF on AWS. Cisco Cloud APIC model associates subnets to VRF because, in AWS, VRFs are mapped to VPCs and subnets are mapped to an Availability Zone (AZ) inside a VPC. This means that you need to define a separate subnet for the Web EPG that only exists in the AWS cloud. You will also define the membership criteria for cloud instances to join the Web EPG. As shown in Figure 26, once you are satisfied with the MSO schema and you have completed the required site-specific configuration steps, you can deploy the configuration to both Cisco ACI sites using the MSO one-click deployment button.

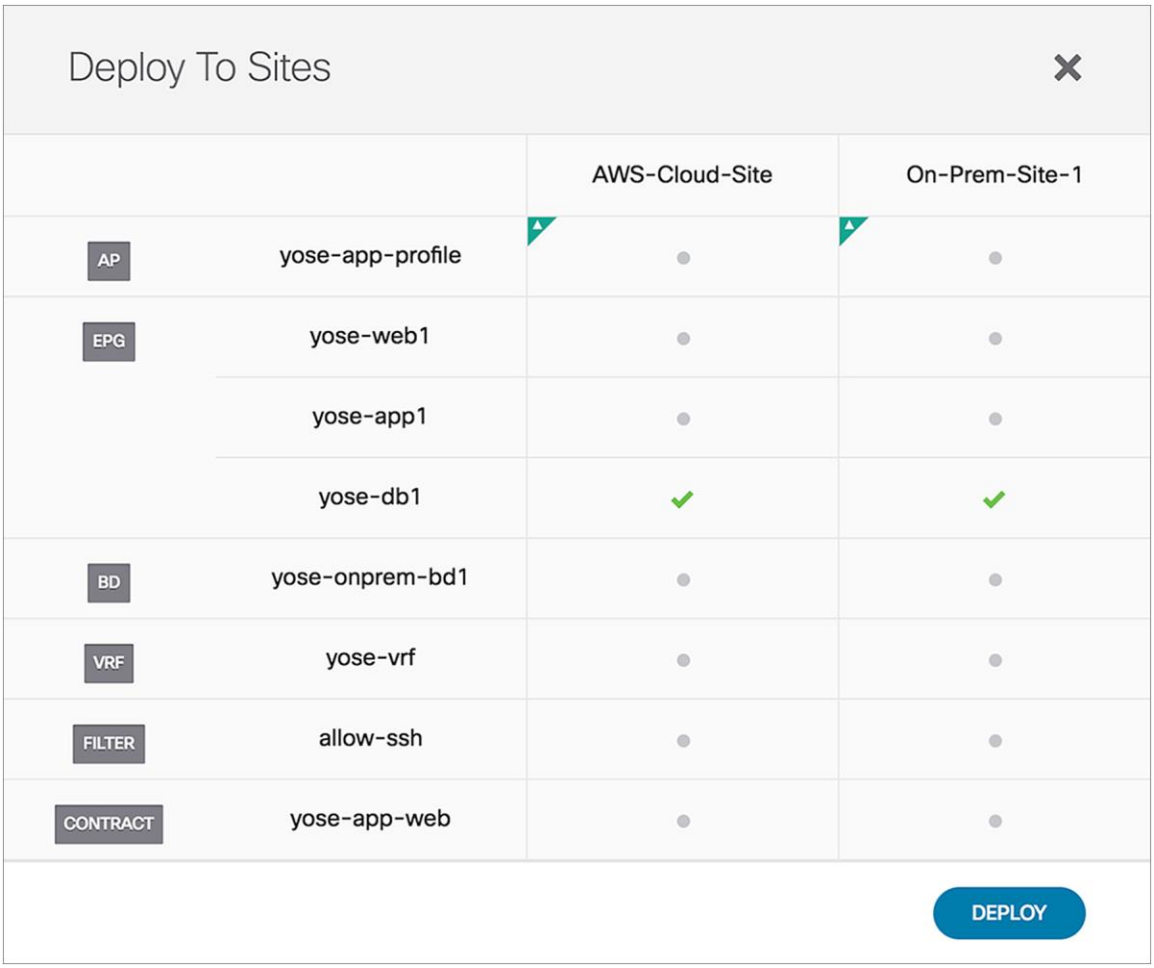


Figure 26.
Deploy application to on-premises and cloud sites in AWS

Cisco Cloud ACI ensures that the AWS cloud and on-premises ACI are configured appropriately to allow communication between the App EPG and the Web EPG residing on AWS, as shown in Figure 27.

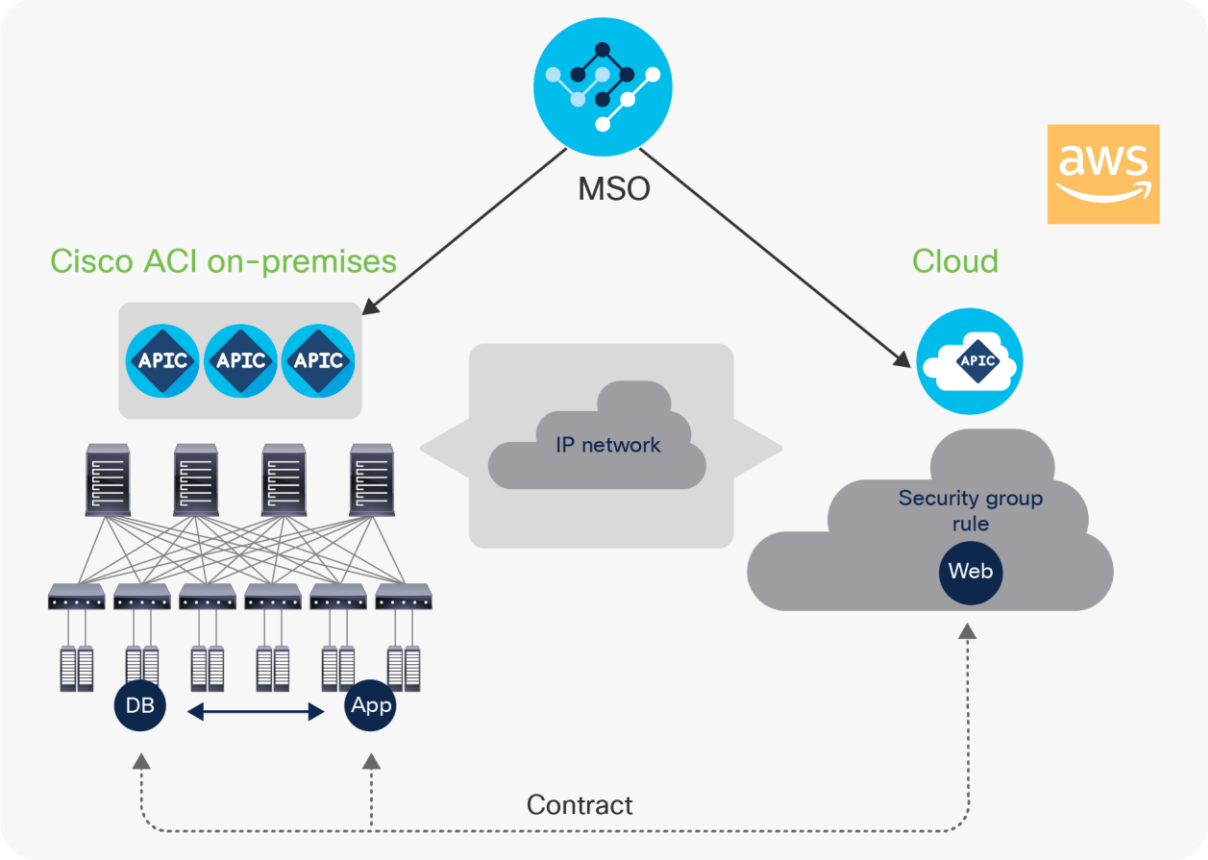


Figure 27.
Three-tier application deployed across on-premises and cloud sites in AWS

You can now deploy new Web instances on AWS to accommodate your needs.

Summary

The new Cisco Cloud ACI capabilities delivered in Cisco ACI Release 4.1 make it easy for network administrators to quickly tailor the infrastructure to adapt to constantly evolving business requirements. The solution provides ultimate IT agility by greatly facilitating the configuration and day-2 operation of hybrid cloud environments. Cisco Cloud ACI lets you architect complex network topologies and security policies that encompass on-premises locations and public cloud sites. Cross-site orchestration of network connectivity and workload segmentation policies is achieved by Cisco ACI Multi-Site Orchestrator working in tandem with Cisco Cloud APIC and on-premises APIC.

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 C11-741998-04 10/20