
TECHNICAL DOCUMENT

ORCHESTRATING VIRTUAL GATEWAYS IN PUBLIC CLOUD INFRASTRUCTURE

MAXIMIZING THE BENEFITS OF PUBLIC
CLOUD INFRASTRUCTURE WITH ARUBA
CENTRAL ORCHESTRATION



TABLE OF CONTENTS

KEY BENEFITS	3
--------------	---

INTRODUCTION	3
--------------	---

ARUBA VIRTUAL GATEWAYS IN THE PUBLIC CLOUD	3
--	---

ARUBA'S VIRTUAL GATEWAY APPLICATION	4
-------------------------------------	---

ARUBA IN THE AMAZON AWS ENVIRONMENT	5
-------------------------------------	---

MULTIPLE VPCS AND TRANSIT GATEWAYS	8
------------------------------------	---

CONCLUSION	9
------------	---

KEY BENEFITS

- Easily connect sites to public clouds
- Add resiliency and routing capabilities to VPC environments
- Public cloud environment simply becomes another node in the SD-WAN infrastructure
- Enhance application delivery and optimize traffic to and from public cloud deployments
- Manage entire lifecycle of public cloud gateways
- Deploy higher scale and higher performance SD-WAN nodes in public clouds
- Save money on native VPN subscriptions with cloud providers¹

INTRODUCTION

Many application workloads are housed in public clouds such as those offered by Amazon Web Services (AWS), Microsoft Azure or Google Cloud. Aruba SD-WAN greatly enhances the use of these public clouds by making it easy to connect to virtual private cloud instances, thus optimizing the networking of the hosted workloads by providing complete lifecycle management and orchestration of connectivity policies.

In order to do this, Aruba's SD-WAN solution makes use of the Aruba Virtual Gateway, which serves as an entry point into the Virtual Private Cloud (VPC) environments that a given customer may have within a public cloud provider such as AWS. Aruba provides a simple automated way to spin up and manage Aruba Virtual Gateways, thus making it easy for branch locations to easily connect to VPCs and access workloads in the cloud while benefiting from SD-WAN functionality to improve application performance.²

ARUBA VIRTUAL GATEWAYS IN THE PUBLIC CLOUD

The manual process of managing connectivity to public clouds is time consuming and error prone. It involves a number of steps to spin up virtual machines, configure routing tables, assign certificates, and manage and monitor the gateways. And it is labor intensive to ensure that the administrator has the proper configuration with the right tunnels and routes.

Aruba SD-WAN simplifies this process and provides complete lifecycle management for Aruba Virtual Gateways. These gateways are far more scalable than the native VPN gateways provided by public cloud providers. An Aruba Virtual Gateway managed by Aruba Central significantly improves traffic management and application delivery by:

- Orchestrating VPN tunnels to automate the establishment of IPsec tunnels from branch and data center locations
- Automating the exchange of routes to and from the VPC across the SD-WAN fabric
- Extending SD-WAN policies to the cloud, by load balancing traffic from branch locations and performing Dynamic Path Steering (DPS) to maintain application Service Level Agreements (SLA)
- Providing end-to-end visibility of the entire SD-WAN network from Aruba Central
- Offering multiple Aruba Virtual Gateway form factors from 500Mbps to 4Gbps to meet bandwidth needs
- Scaling to terminate tens of thousands of IPsec VPN tunnels on a single Aruba Virtual Gateway
- Delivering a highly resilient gateway solution to span Availability Zones³ with automatic failover

¹ Subscriptions can be as low as one-tenth non-integrated costs, especially on high-bandwidth gateways and in high-cost cloud regions.

² While this document focuses on integration with AWS, and thus frequently uses AWS terminology (such as VPC), Aruba also supports other public cloud providers such as Microsoft Azure.

³ Amazon locations support multiple regions, and there are multiple Availability Zones within each region. Customers define the resources they need within each Availability Zone.

Effectively, the use of an Aruba Virtual Gateway to connect the SD-WAN environment to the public cloud environment simplifies cloud access: the cloud becomes another node in the SD-WAN network (Figure 1).

The cloud environment is accessible from any branch regardless of the transport medium of choice, and you can use different types of transport based on your policies.

ARUBA'S VIRTUAL GATEWAY APPLICATION

The public cloud environment introduces a very different workflow from typical edge IT networking. Services are established and managed relying on APIs provided by the cloud provider; these APIs are quite different from the tools used in managing enterprise or data center networks.

For this reason, simply offering a virtual machine (VM) from a marketplace is an inadequate way for enterprise IT to utilize the public cloud—users need the ability to treat public cloud endpoints as another node in the network to make the best use of cloud resources.

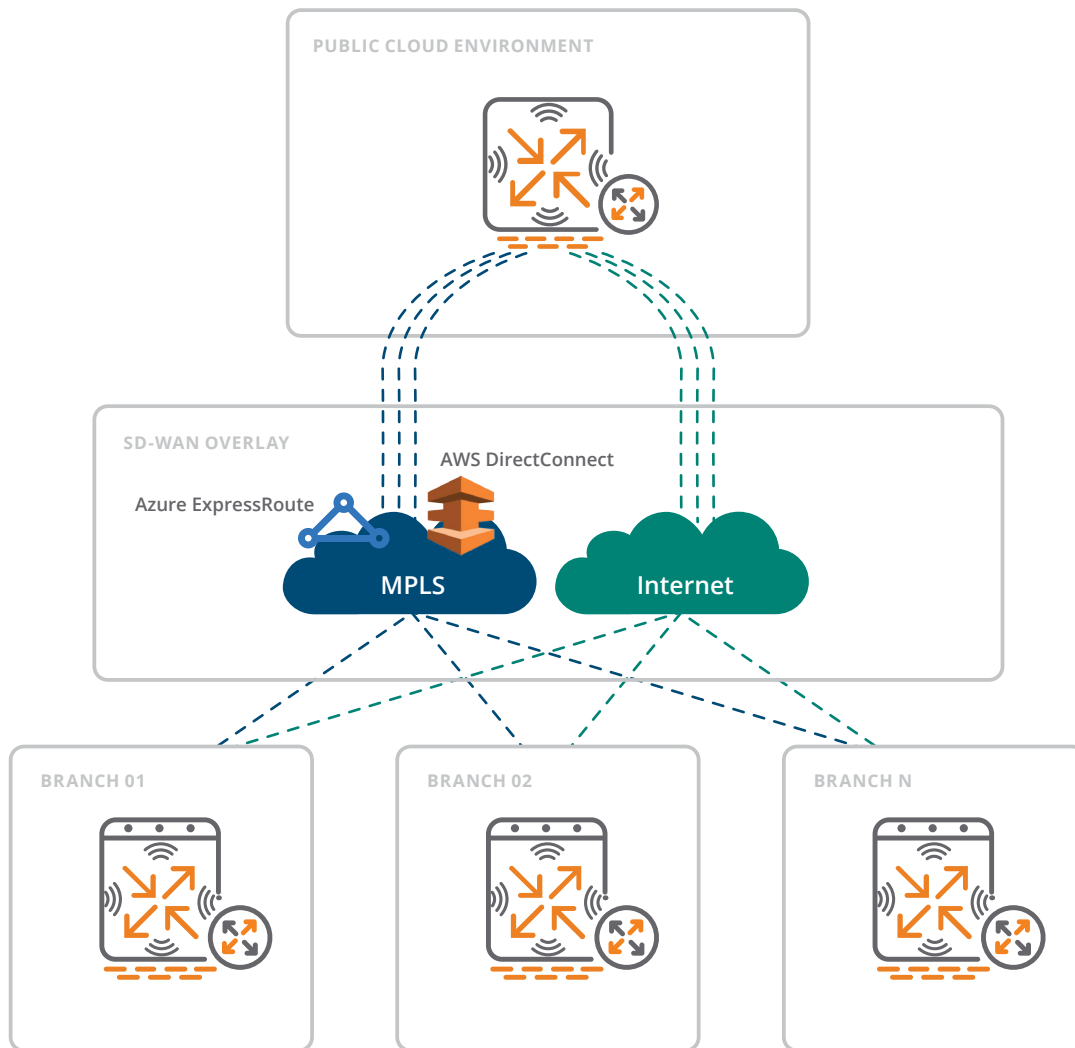


Figure 1: Public Cloud as an SD-WAN Node

The Aruba SD-WAN solution provides a virtual gateway orchestration application with Aruba Central to handle the full life-cycle of the Aruba Virtual Gateway. Although manual bring-up using the public cloud’s console (or native APIs) is supported, the preferred mechanism is to use the automated workflow shown in Figure 2.

Aruba Central handles the entire lifecycle of the Aruba Virtual Gateway, from the initial bring-up and provisioning through all levels of management. From Aruba Central’s perspective, the Aruba Virtual Gateway is just another gateway in the network.

ARUBA IN THE AMAZON AWS ENVIRONMENT

Aruba’s Virtual Gateway application connects with a customer’s public cloud account based on the credentials provided by the customer. The right level of access (including Identity and Access Management—IAM—credentials) to the customer’s VPC is required to gain visibility of the environment and automate the deployment of the Aruba Virtual Gateway. The gateway application provisions the virtual gateway instances, together with the necessary interfaces, subnets, IP mappings, etc. Figure 3 shows this application accessing AWS infrastructure.

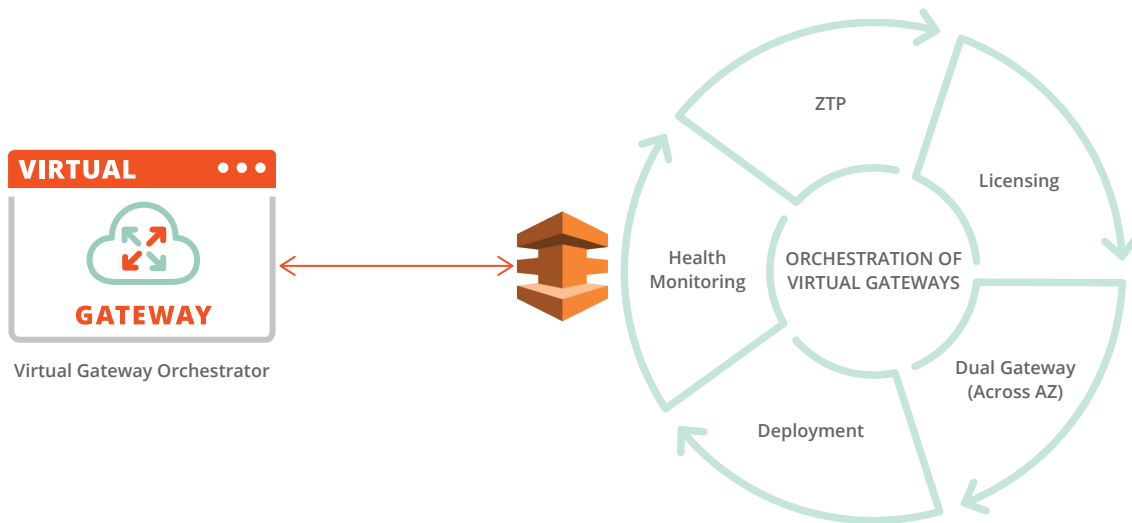


Figure 2: Lifecycle Management for Aruba Virtual Gateway

ORCHESTRATED CLOUD PROVIDER								
SUMMARY OF DEPLOYED VIRTUAL GATEWAYS								
CLOUD PROVIDER	ACCOUNT	REGION	VGW SERIAL	VGW PUBLIC IP	HIGH AVAILABILITY	ORCHESTRATION	VM STATUS	VGW STATUS
Azure	Tropical-Azure	West US 2	VG1910158236	40.90.196.141	ACTIVE	DONE	UP	TIMEOUT
AWS	tropicalsdwan	Asia Pacific (Sydney)	VG1910161288	3.106.11.197	ACTIVE	DONE	UP	TIMEOUT
AWS	tropicalsdwan	EU (Frankfurt)	VG1910126271	18.197.213.29	ACTIVE	DONE	UP	TIMEOUT

Figure 3: Aruba Central’s Virtual Gateway Application (Summary View)

The first step to integrate the gateway is to add a cloud provider account; the Accounts view enables this (Figure 4).

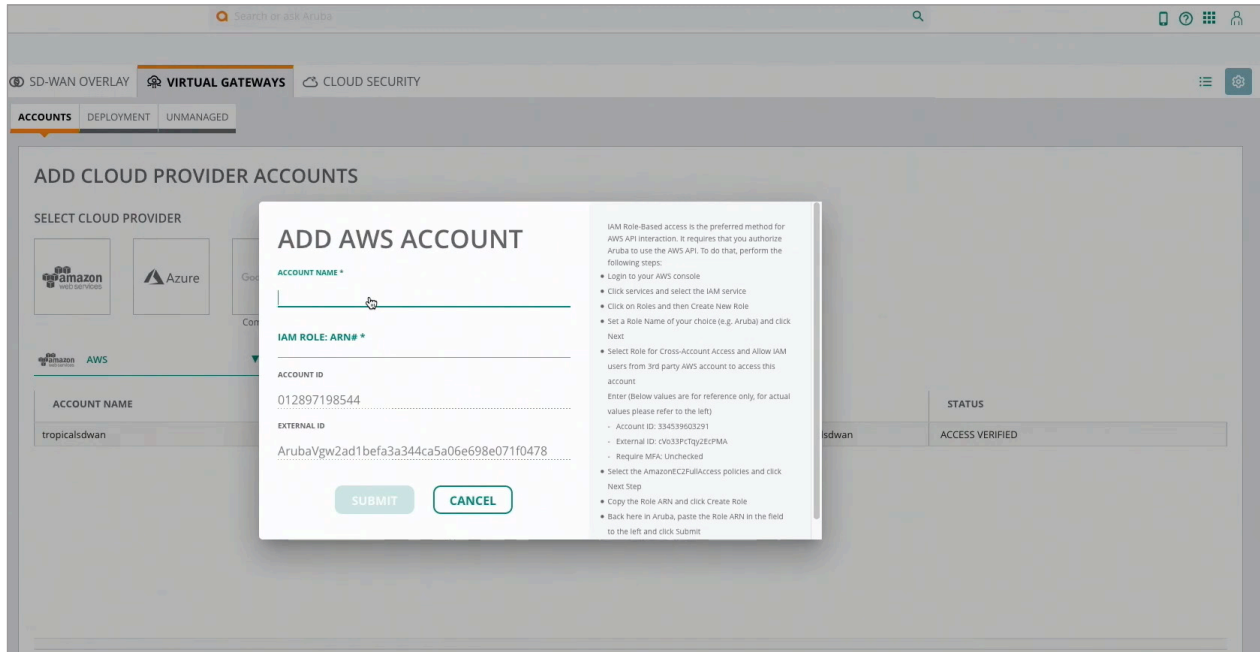


Figure 4: Add a Cloud Provider (AWS) Account

The administrator adds the account name as well as the IAM credentials. The account shows up in the account list (Figure 5).

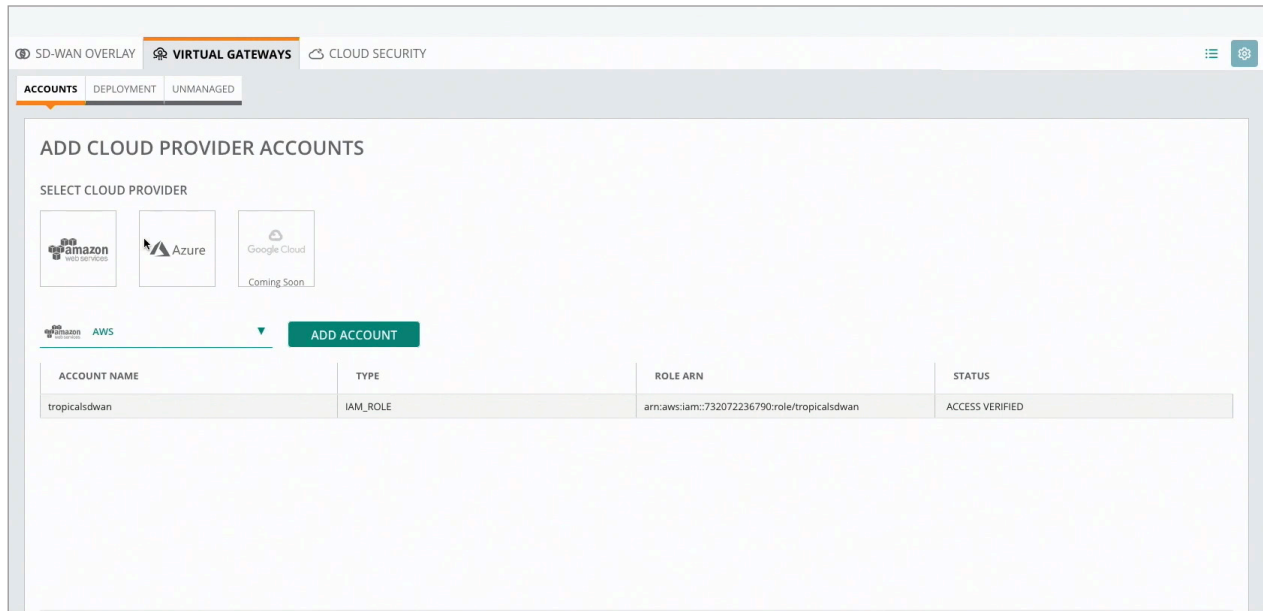


Figure 5: AWS Account (Highlighted) is Added

Using the IAM credentials Aruba Central discovers the VPC topology, which is especially valuable for customers that have a large number of VPCs (Figure 6).

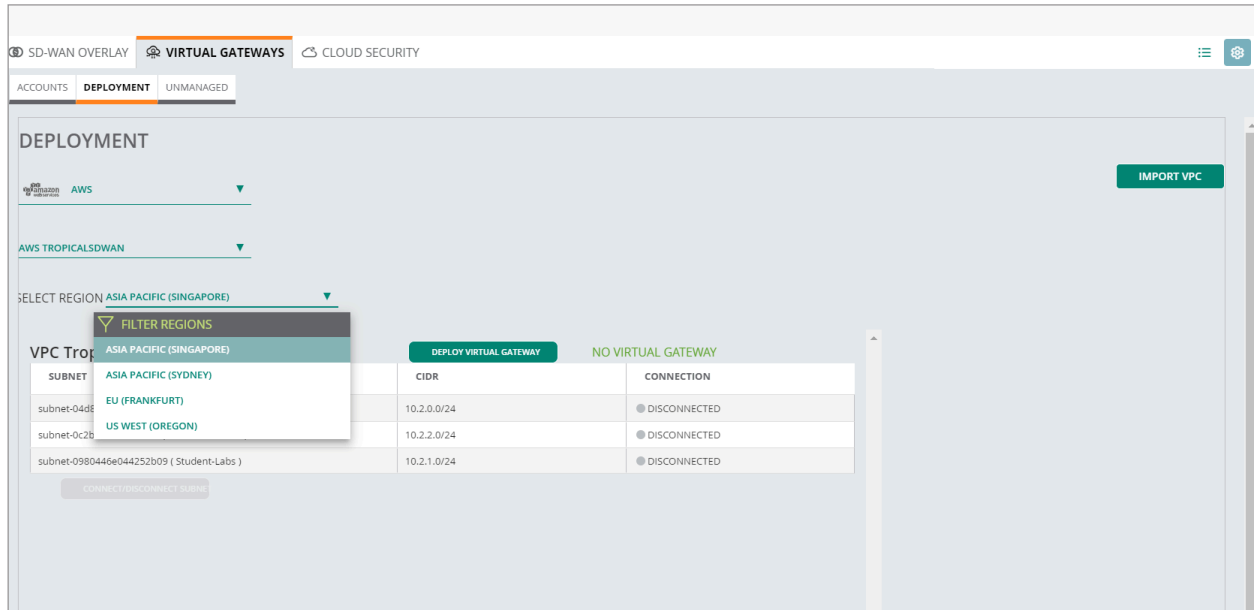


Figure 6: VPC Topology (Regions and Subnets Highlighted)

For any region, we can see the VPCs within that region, along with the subnets for that VPC. We can also import new VPCs as they are added.

Once the VPC topology is discovered in each region using IAM credentials, the user simply selects a VPC created to act as transit VPC and deploys Aruba Virtual Gateways. Figure 7 shows an example of deploying the Aruba Virtual Gateway.

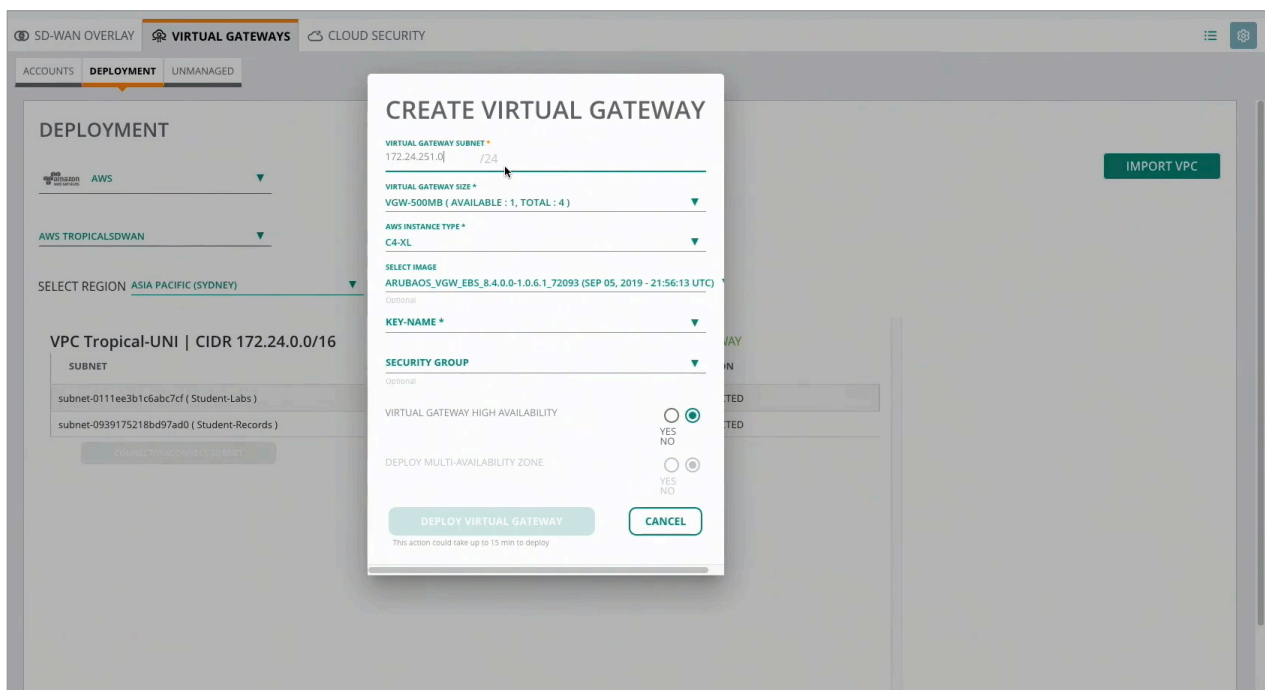


Figure 7: Creating the Virtual Gateway

To take advantage of resiliency features available and follow public cloud best practices (such as using multiple availability zones), the High Availability (HA) pair of Aruba VGs should be deployed in Availability Zones (AZs). This is a straightforward process, achieved by selecting the HA option and multiple AZ as shown in Figure 7 above.

MULTIPLE VPCS AND TRANSIT GATEWAYS

When bringing SD-WAN into a more common AWS environment with applications running in multiple VPCs in each region, it is more scalable and common to have a “Transit VPC” that would serve as the gateway between the AWS environment and the SD-WAN’s connected sites. A transit VPC connects multiple VPCs within the region. This simplifies network management and minimizes the connections needed to connect multiple VPCs and remote networks (Figure 8).⁴

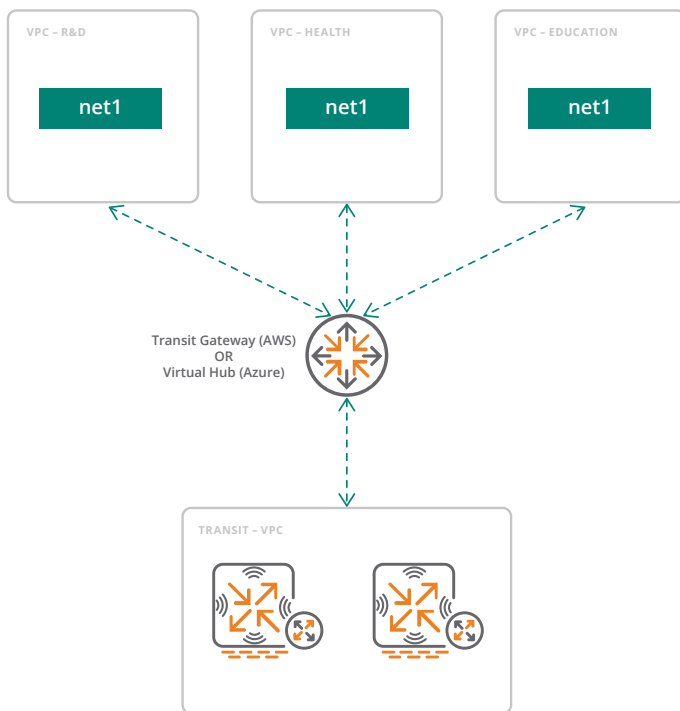


Figure 8: Multiple VPCs Peering with a Transit Gateway

Aruba Virtual Gateways would then peer directly with the AWS Transit Gateway (TGW).⁵

A deployed Virtual Gateway is simply another node managed by Aruba Central. The connectivity is automatically established as defined in the SD-WAN policies, and they are visible in a monitoring dashboard.

A topology diagram (Figure 9) shows the connectivity from a branch to both on-premises headend gateways and to an Aruba Virtual Gateway in the public cloud.

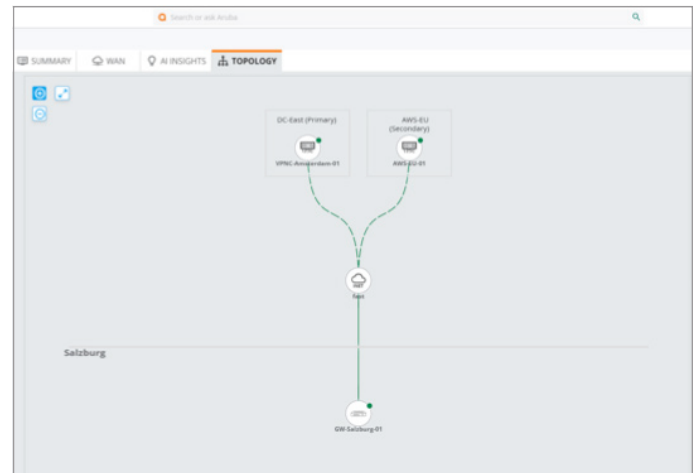


Figure 9: End to End Visualization from Branch to Data Center and Public Cloud

⁴For more information, see Amazon VPC Connectivity Options.

⁵Detailed information about the AWS TGW can be found in the AWS documentation.

The Overlay Tunnel Orchestrator Topology shows the connections from branch locations to any geographical locations where applications are running (Figure 10).

This global view shows all cloud providers and on-premises data centers per branch group.

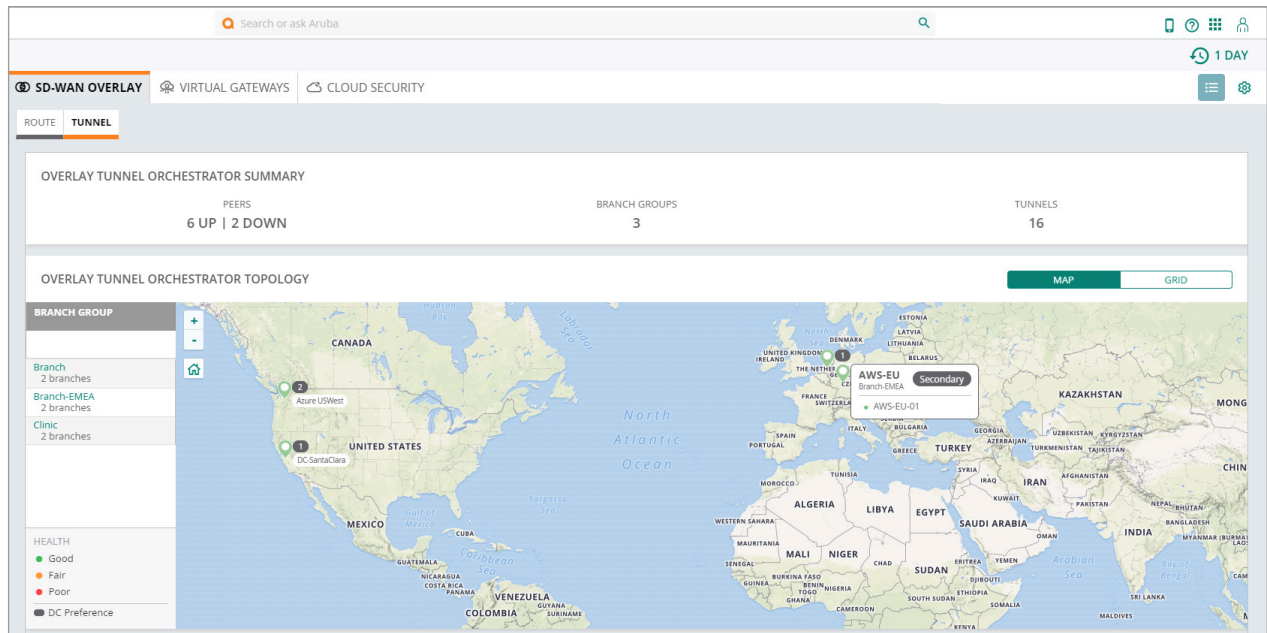


Figure 10: Global SD-WAN Orchestrator View

CONCLUSION

Aruba’s SD-WAN solution greatly enhances the benefits of integrating with public cloud infrastructure, as it essentially makes the public cloud environment into an SD-WAN node. Aruba Virtual Gateways are scalable and can terminate thousands of IPsec VPN tunnels, making it easy for a large number of branch locations to directly access workloads in public clouds. Aruba SD-WAN simplifies the routing and the resiliency capabilities of VPC environments for AWS and Microsoft Azure.

In the AWS case, Aruba Virtual Gateways connect individual customer VPCs with the customer’s enterprise network via Direct Connect or via the Internet Gateway by extending the SD-WAN fabric. For complex cloud environments, Aruba simplifies the process of connecting VPCs.