Technical Review

Simplifying Branch-to-cloud Connectivity with Amazon Web Services Transit Gateway and Aruba SD-Branch

Date: September 2020 **Author:** Alex Arcilla, Validation Analyst

Abstract

The report highlights the benefits delivered by Amazon Web Services (AWS) Transit Gateway in conjunction with Aruba SD-Branch. We illustrate how AWS Transit Gateway can help organizations to scale the interconnection of multiple Amazon Virtual Private Clouds (VPCs) with one another and their on-premises networks. We also describe the benefits that organizations can derive from the integration of AWS Transit Gateway capabilities with those of Aruba SD-Branch. A case study features the benefits derived from using this combined solution.

The Challenges

The percentage of organizations that use or plan to use infrastructure-as-a-service (IaaS).[1]

The percentage of organizations that expect to **maintain a measurable on-premises environment** in the next three years.[2]

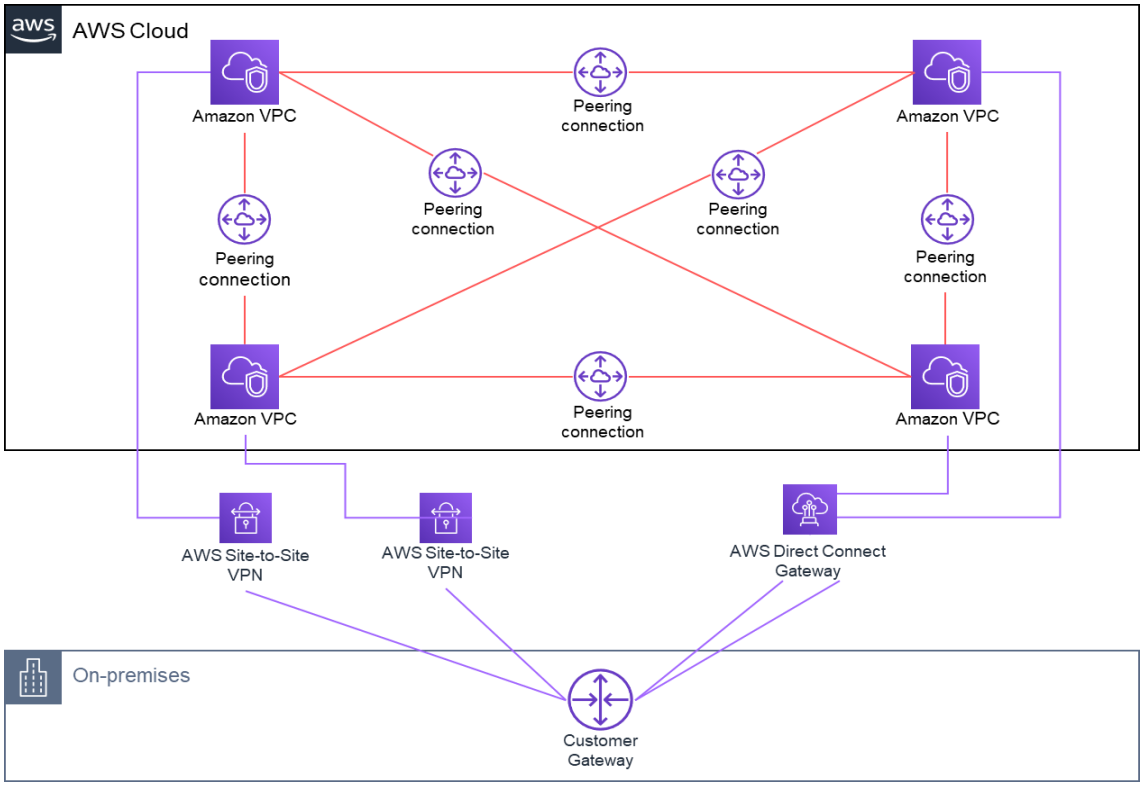
The percentage of organizations that view their IT environments as **equally or more complex** than two years ago.[3]

Enterprise cloud adoption continues to increase as organizations want to leverage infrastructure-as-a-service (IaaS) for the ease of application deployment and IT resources scalability. Yet, as the number of organizations planning to run production applications on the cloud grows, they still intend to maintain a measurable on-premises IT environment—data centers and remote offices/branch offices (ROBOs)—for the foreseeable future. Furthermore, the increasingly distributed nature of organizations and their applications make IT environments more complex and difficult to manage. These organizations need to ensure that their cloud-based resources are networked to their on-premises environments, and to one another, without incurring additional IT network complexity and associated costs.

Typically, connecting on-premises offices and data centers to the cloud requires the use of point-to-point connections, such as IPsec Virtual Private network (VPN) tunnels or private network fiber connections. Connecting virtual networks (groups of networked cloud resources) with one another also requires point-to-point connections. However, as the number of on-premises offices and virtual networks increases, the number of point-to-point connections grows, resulting in a large mesh network that can be difficult, cumbersome, and costly to manage. Organizations using AWS have typically used AWS Direct Connect[4] and AWS Site-to-Site Virtual Private Network (VPN) connections[5] for connecting their on-premises environment to individual Amazon VPCs, and VPC peering for connecting their Amazon VPCs with one another (see Figure 1).

[1] Source: ESG Master Survey Results, *2020 Technology Spending Intentions Survey*, January 2020.
[2] Source: ESG Master Survey Results, *Hybrid Cloud Trends*, May 2019.
[3] Source: ESG Master Survey Results, *2020 Technology Spending Intentions Survey*, January 2020.
[4] AWS Direct Connect is a cloud service solution for establishing a dedicated network connection from on-premises locations to AWS.
[5] An AWS Site-to-Site VPN connection consists of two Internet Protocol Security (IPsec) VPN tunnels, each terminating in two different Availability Zones (AZ) to ensure high availability.

Figure 1. Before AWS Transit Gateway



Source: Enterprise Strategy Group

As organizations deployed more geographically dispersed Amazon VPCs, AWS initially offered a networking construct called a transit VPC to manage their growing AWS environments. The transit VPC served as a central hub for VPC peering connections as well as connections between Amazon VPCs and on-premises locations. While the transit VPC helped to centralize network connectivity, organizations would still need to manually configure redundant third-party virtual routers within the transit VPCs. Should issues arise with the transit VPC, organizations would need to coordinate external support between multiple vendors.

Ideally, organizations should be able to connect their cloud and on-premises resources without adding network complexity and ongoing management and operational effort.

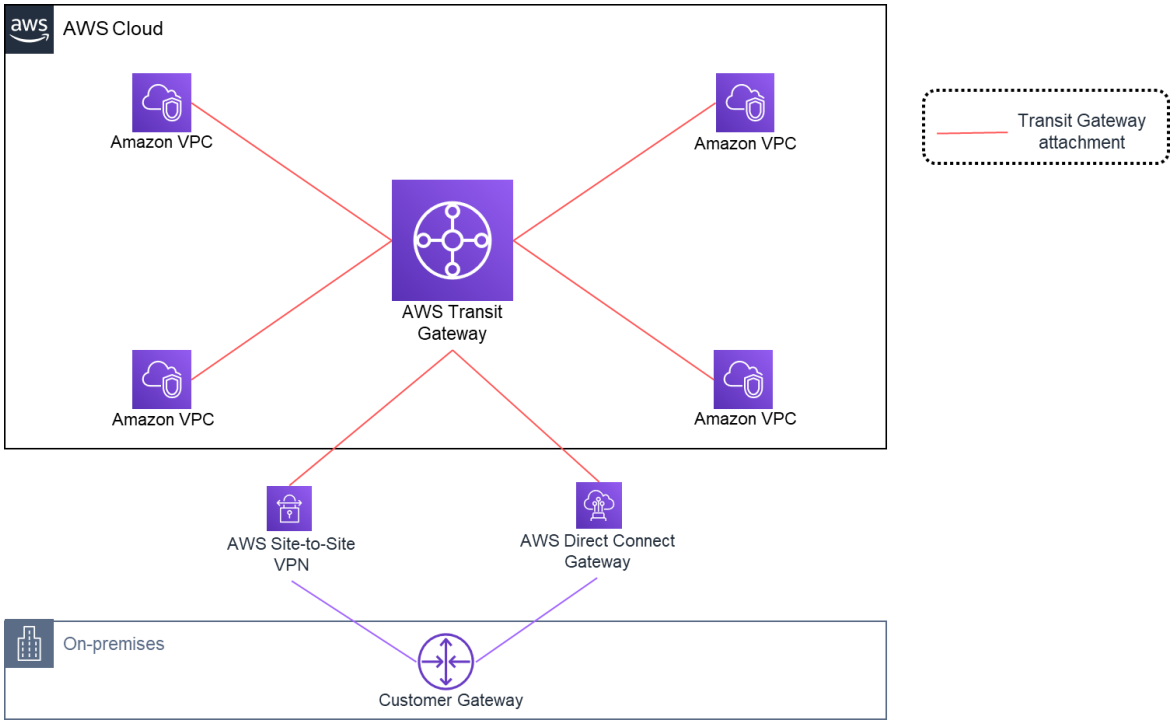
The Solution: Amazon Web Services Transit Gateway

Amazon Web Services (AWS) Transit Gateway is a managed, regional, and scalable service that enables organizations to interconnect a large number of Amazon VPCs and on-premises networks without relying on numerous point-to-point connections or the transit VPC.

AWS Transit Gateway simplifies how organizations connect their Amazon VPCs with one another and to their on-premises networks within a region (see Figure 2) by serving as a central point for Layer 3 network connectivity. By enabling a "hub-and-spoke" topology, the solution can help organizations reduce the number of VPC peering connections and consolidate access to the on-premises network.

Even though the number of VPCs is small and there is only one enterprise location in Figure 1, it is easy to see how the Transit Gateway simplifies the environment. Imagine how much complexity is removed when there are additional enterprise locations and hundreds or thousands of Amazon VPCs. Now, organizations can simply connect their on-premises networks and Amazon VPCs via AWS Transit Gateway.

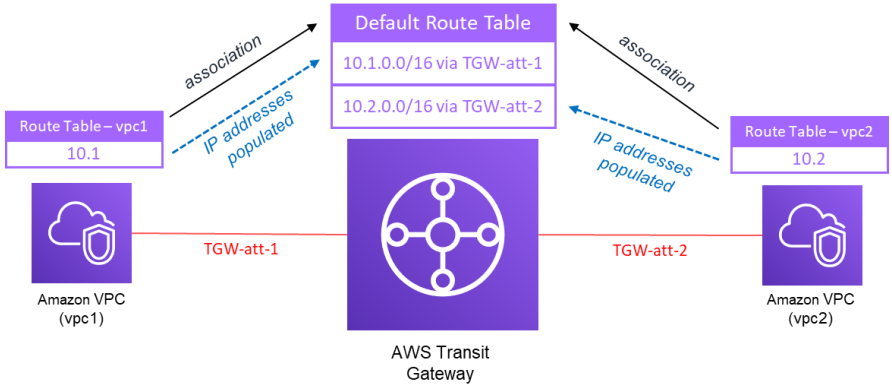
Figure 2. AWS Transit Gateway – Reducing Number of Point-to-point Connections



Source: Enterprise Strategy Group

Routing Traffic with AWS Transit Gateway

Amazon VPCs and on-premises locations connect to AWS Transit Gateway via transit gateway attachments (see Figure 2). These attachments enable AWS Transit Gateway to route traffic to the correct destination either on-premises or in the AWS Cloud.



When connecting an Amazon VPC with AWS Transit Gateway via a transit gateway attachment, AWS Transit Gateway's default route table[6] is automatically populated with the destination IP addresses of the attached Amazon VPC to which AWS Transit Gateway can direct traffic. (Routing outgoing traffic from an Amazon VPC requires that an administrator updates the Amazon VPC route table with the relevant destination IP addresses.) When attaching an on-premises location to AWS Transit Gateway either via a VPN tunnel or AWS Direct Connect, a similar exchange of IP address information occurs.

Organizations can also segment and isolate network traffic by creating multiple route tables within AWS Transit Gateway. Each route table corresponds to a routing domain that directs traffic to specific Amazon VPCs or on-premises locations based on business needs. Because AWS Transit Gateway can support multiple route tables on AWS Transit Gateway in a region, an administrator can control routing on a per-attachment basis.

Reducing the overall number of point-to-point connections to create and configure individually, as well as dynamic routing between AWS Transit Gateway and an organization's on-premises locations and Amazon VPCs, helps to decrease network complexity while increasing operational efficiency. Creating AWS Direct Connect, AWS Site-to-Site VPN, and VPC peering

[6] A route table contains dynamic and static routes that decide how traffic is directed based on the destination IP address of the packet.

connections may require little manual effort (such as navigating multiple interfaces and configuring routers and gateways) for a small number of on-premises locations and Amazon VPCs. However, for enterprises with IT environments spanning hundreds of Amazon VPCs and multiple on-premises offices, that manual effort, along with the associated resources and costs, can very quickly become quite difficult to manage. Ultimately, using AWS Transit Gateway can help to lower operational efforts and costs while increasing business agility.

Building Global Enterprise Network Architectures with AWS Transit Gateway

Organizations can now use AWS Transit Gateway to build out their IT networks without dealing with extensive network architecture planning and upgrades. They can take advantage of other networking and security services offered by AWS or AWS partners to deploy a global enterprise-grade network, as opposed to manually integrating different solutions from multiple vendors. Because AWS Transit Gateway is a managed service, enterprises can also avoid the hardware and software refresh and upgrade cycles typically associated with similar hardware or software-based solutions.

Key AWS Transit Gateway features that can be leveraged to build out a global network architecture while centralizing control, maximizing network and application performance, and ensuring overall network security include:

AWS Transit Gateway Inter-Region Peering

AWS Transit Gateway Inter-Region Peering enables traffic to traverse between AWS Transit Gateways over the AWS global backbone. Deploying a global network becomes easier using inter-region peering as AWS Transit Gateways and their VPC and VPN attachments can be interconnected. Inter-region peering connections also encrypt traffic and route the traffic exclusively on the AWS global backbone, thereby ensuring overall network security. These connections are also designed for high availability, as the AWS backbone is built with redundant 100Gbps network links connecting all AWS Regions globally.

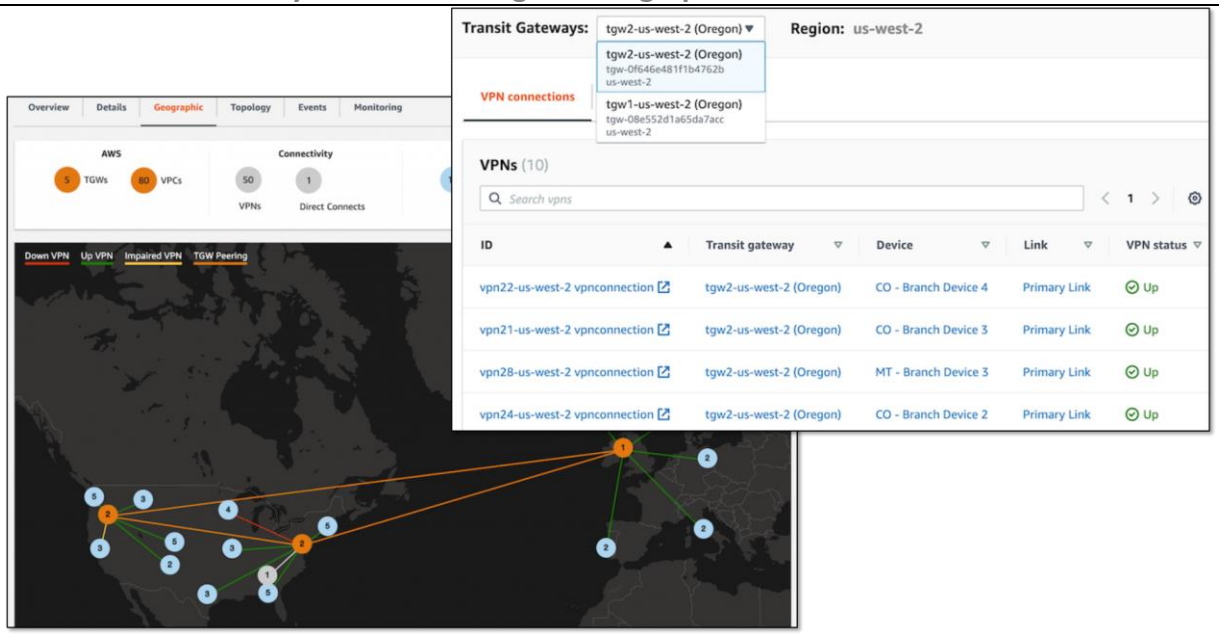
With inter-region peering, organizations can architect a private global network while decreasing the time and resources required to connect an organization's Amazon VPCs and on-premises networks in different regions. Functional groups, such as engineering and development, can collaborate with minimal delay in creating the proper connections to communicate and thus respond to business needs quickly.

AWS Transit Gateway Network Manager

To simplify network operations and administration, the AWS Transit Gateway Network Manager provides a centralized and consistent user experience. With a single interface, global IT networks can be viewed and monitored as the AWS Transit Gateway Network Manager summarizes configuration and performance data from all AWS Transit Gateways and their attachments with other Amazon VPCs and on-premises locations.

Enterprises can view components of their global networks through different visualizations (via lists, logical diagrams, or geographic maps) and alert administrators of unhealthy connections and changes in availability and performance across AWS Regions and on-premises sites. Figure 3 shows the geographic view of a global network. Nodes represent network details such as AWS Regions, AWS Transit Gateways, and on-premises locations. An administrator can click on any nodes to obtain detailed information. For example, by clicking on the US-West-2 node, the AWS Transit Gateway Network Manager reveals its AWS Transit Gateways and connected on-premises offices. Status of the VPN attachments is also displayed.

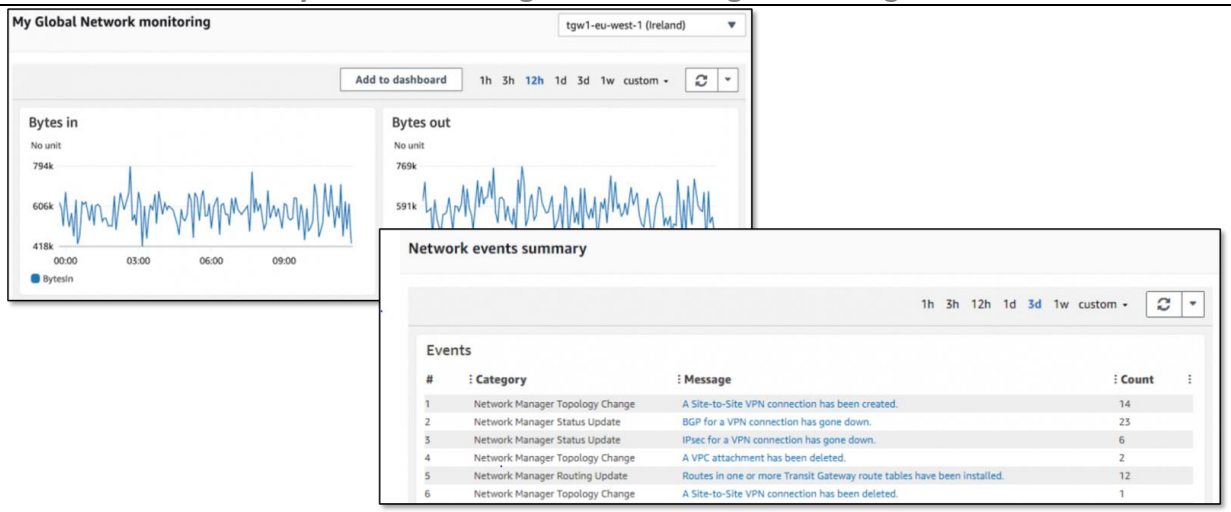
Figure 3. AWS Transit Gateway Network Manager – Geographic and Detailed Views



Monitoring and Management

To manage and monitor AWS-based networks, the AWS Transit Gateway Network Manager leverages other AWS services, specifically Amazon CloudWatch and Amazon VPC Flow Logs, to compile and display near real-time metrics such as bandwidth usage on AWS Transit Gateway attachments, packet flow count, packet drop count, and other information related to IP traffic routed through AWS Transit Gateway. For example, Figure 4 shows graphs of metrics tracking traffic bytes routed through AWS Transit Gateway in Ireland. ESG also noted that a summary of events occurring over time can be generated to help an administrator quickly identify possible causes of ongoing network issues.

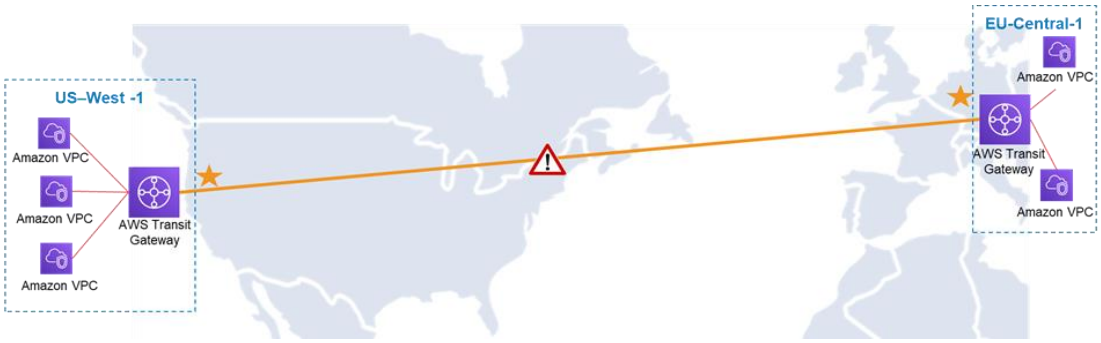
Figure 4. AWS Transit Gateway Network Manager – Monitoring and Management



Route Analyzer

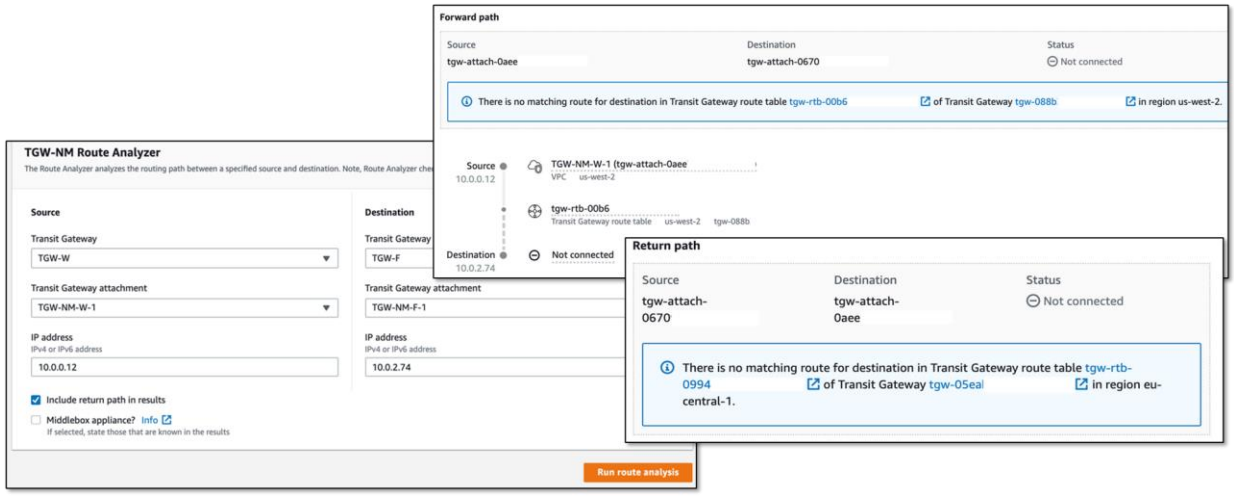
In addition to monitoring near real-time network metrics, organizations can identify potential causes of network disruptions by analyzing how traffic is routed between AWS Transit Gateways and their attached Amazon VPCs and on-premises locations. With Route Analyzer (accessed via the AWS Transit Gateway Network Manager main interface), organizations can identify potential causes of the disruptions.

For example, an administrator has been alerted that AWS resources within Amazon VPCs deployed in the western US (US-East-2) and Germany (EU-Central-1) cannot talk with each other. The Amazon VPCs are attached to AWS Transit Gateways in Oregon and Frankfurt, Germany. To allow communication between Amazon VPCs in the US and Germany, both AWS Transit Gateways should be connected via AWS Transit Gateway Inter-Region Peering.



With Route Analyzer, the administrator can check if the AWS Transit Gateway route tables have been configured correctly (see Figure 5). By inputting the source and destination transit gateway name, transit gateway attachment, and IP addresses, Route Analyzer can check if an EC2 instance in the US-West-2 Region (the source) can communicate with the EC2 instance in the Frankfurt Region (the destination) using peered AWS Transit Gateways. In this case, the Route Analyzer has found that both the forward and return paths do not exist between the AWS Transit Gateways (as indicated in the blue fields). The administrator now knows that correcting this issue requires inputting the correct routes into the AWS Transit Gateway route tables.

Figure 5. Troubleshooting with Route Analyzer



Cross-account Support

An organization can share its AWS Transit Gateway with other AWS accounts so that they are free to attach their own Amazon VPCs or on-premises locations when business needs dictate (e.g., when development and testing groups need to collaborate). Enabling this support eases the process of setting up and tearing down these interconnections without having to configure route tables of multiple Amazon VPCs or on-premises routers and gateways. Management and administration of the AWS Transit Gateway remains with the primary account in order to retain overall centralized control of the network.

Multicast Support

Instead of using on-premises multicast networks, AWS customers can send multicast data straight from AWS-based applications using AWS Transit Gateway Multicast. This is especially applicable for applications such as video or stock ticker information. With AWS Transit Gateway Multicast, organizations eliminate the need for deploying multiple high-bandwidth unicast connections to each client while reducing network congestion and network infrastructure costs.

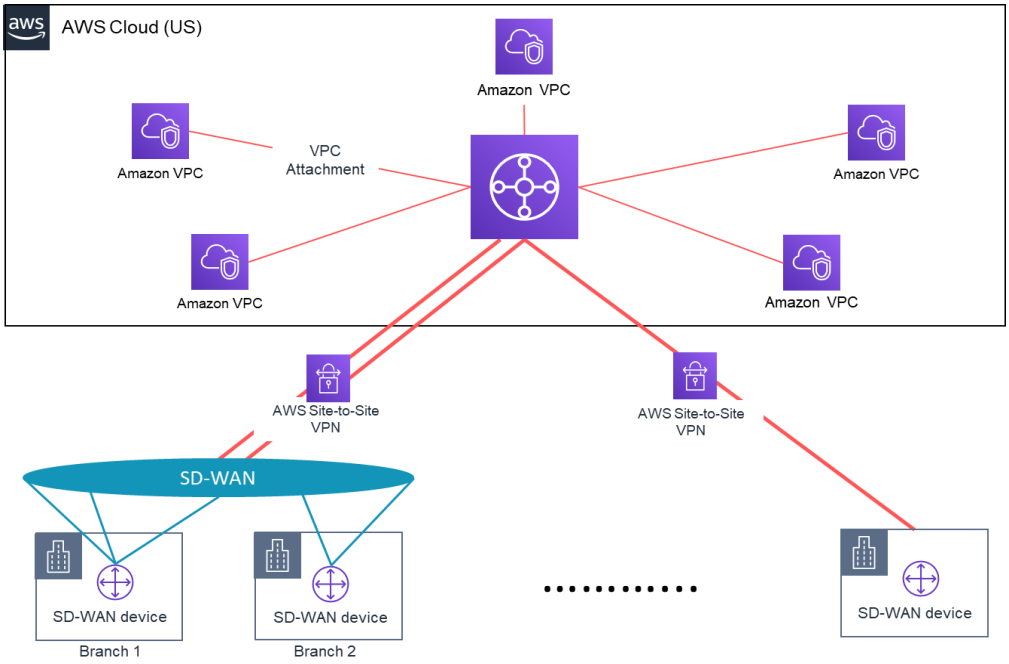
Security

To help in ensuring overall cloud-based network security, AWS Transit Gateway operates on the AWS private network, thus not exposing an enterprise's traffic on the public internet. This helps to decrease threat vectors such as distributed denial of service (DDoS) attacks and common exploits such as SQL injection and cross-site scripting. AWS Transit Gateway also inherits compliance from the Amazon VPCs, meeting the standards for PCI DSS Level 1, ISO 9001, ISO 27001, ISO 27017, ISO 27018, SOC 1, SOC 2, SOC 3, FedRAMP Moderate, FedRAMP High, and HIPAA eligibility.

SD-WAN Integration

Organizations typically use software-defined wide area networking (SD-WAN) solutions to maximize the use of network transport resources by automatically rerouting VPN tunnels over alternative network paths should application or network performance degrade on a designated primary path. With select SD-WAN solutions, organizations also have the option to create AWS Site-to-Site VPN tunnels directly between a branch and AWS Transit Gateway with minimal manual effort using the SD-WAN solution's management interface (see Figure 6). The integration of AWS partner SD-WAN solutions with AWS Transit Gateway Network Manager can also enable organizations to visualize, manage, and monitor IT environments spanning both on-premises and the AWS Cloud.

Figure 6. SD-WAN Integration with AWS Transit Gateway



Source: Enterprise Strategy Group

Why This Matters

Integrating cloud and on-premises IT environments remains a challenge for organizations when pursuing a hybrid cloud strategy. A necessary part of that integration is ensuring that resources both in the cloud and on-premises locations are networked to respond to business needs without the need for extensive architecture planning, management, and administration.

AWS Transit Gateway enables organizations to network their cloud and on-premises environments. With this managed, distributed, and scalable service, large enterprises can develop global private networks connecting on-premises locations to Amazon VPCs in any AWS Region without the need for multiple point-to-point connections. Enterprises can leverage AWS Transit Gateway Network Manager to monitor the performance and availability of their AWS Transit Gateways and corresponding attachments. AWS Transit Gateway also offers other features that help organizations to build out and manage global enterprise-grade networks. With AWS Transit Gateway, organizations can ultimately decrease the time and resources required to deploy and manage a global network architecture with less complexity, decreasing both network infrastructure and operational costs.

Branch-to-cloud Connectivity with AWS Transit Gateway and Aruba SD-Branch

Large organizations with multiple on-premises locations have been adopting software-defined wide area networking (SD-WAN) solutions to simplify branch-to-branch connectivity. As enterprises increase the adoption of IaaS for select workloads, the need arises to scale branch-to-cloud connectivity while retaining the benefits of scalability, orchestration, and cost optimization derived from the use of SD-WAN. With the combination of AWS Transit Gateway and Aruba SD-Branch, large enterprises can simplify, automate, and scale the interconnection of on-premises data centers and ROBOs with multiple Amazon VPCs.

Aruba developed its SD-WAN solution, SD-Branch, to help distributed enterprises in connecting their on-premises data centers and branches using any network transport—5G, LTE, broadband/cable, or public internet—as opposed to relying on traditional multi-protocol label switching (MPLS) networks. The main components of the solution are:

- *Aruba Branch Gateways*: Deployed in data centers and branch offices, the gateways help IT administrators to create and support multiple connections (or IPSec VPN tunnels) between any two locations. These gateways establish the SD-WAN overlay used to create virtual connections between locations in the IT network.
- *Aruba Virtual Gateways*: Deployed in Amazon VPCs, these virtual gateways enable secure connectivity between the branches and data center locations connecting to public clouds. Virtual gateways support public internet and private connections such as AWS Direct Connect.
- *Aruba SD-WAN Orchestrator*: With the web-based orchestrator, organizations can dynamically create IPSec VPN tunnels between Aruba branch gateways to build the SD-WAN overlay. The Orchestrator automatically learns routes between the Aruba branch gateways and distributes all route information within the overlay. Should traffic on one network path in the overlay be unable to support traffic, the Aruba SD-WAN Orchestrator will reroute traffic dynamically to minimize service disruption to end-users. Because the Orchestrator can automate the creation and support of multiple routes, it can scale easily to handle very large networks without adding operational time and complexity.
- *Aruba Central*: This is a cloud-native graphical user interface (GUI) that provides unified management, artificial intelligence support, and security for wired, wireless, and SD-WAN operations across campus, branch, and data center environments.

Aruba has also designed a number of operations to be automated either via out-of-the-box capabilities or programmatically via Aruba applications programming interfaces (APIs). IT staff that manage large and complex distributed enterprises

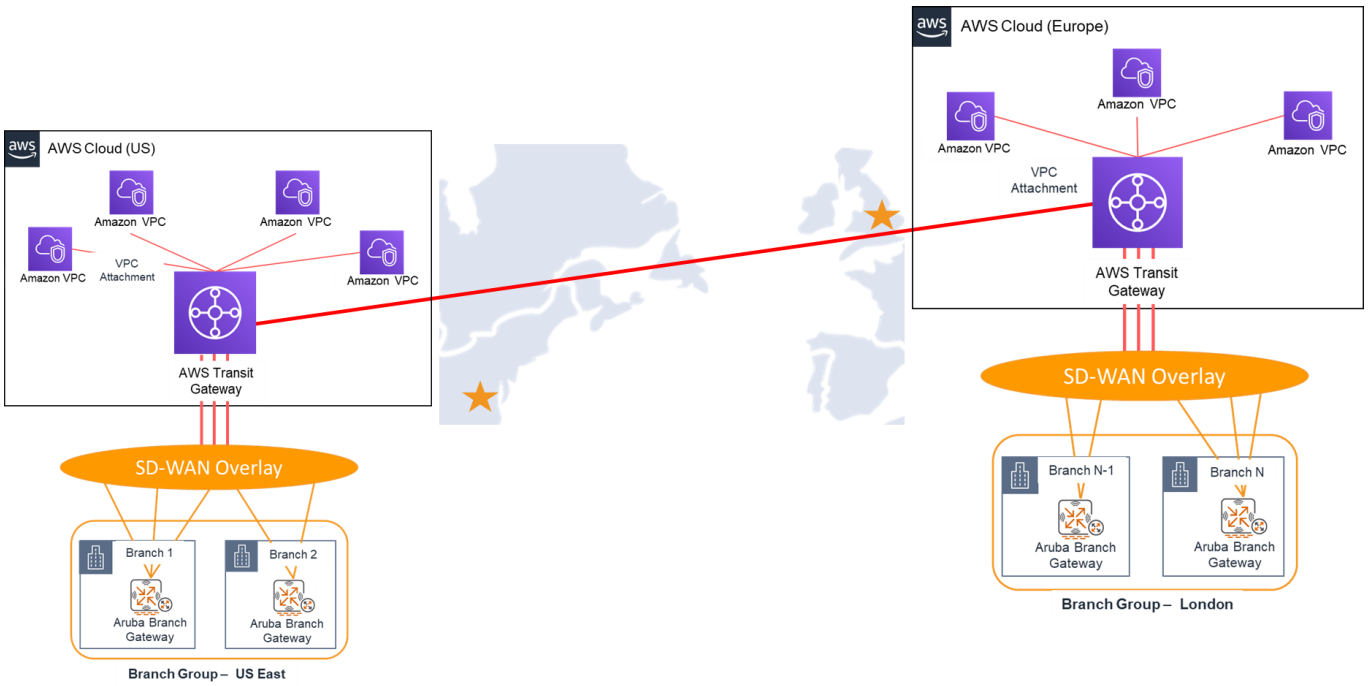
spanning both on-premises and AWS Cloud environments can benefit especially, as the automation can reduce the number of manual steps related to daily network operations. Examples include setting up routes and tunnels between multiple branches and Amazon VPCs, and applying network access control lists (ACLs) to multiple sites.

With Aruba SD-Branch, organizations can reduce the amount of time and resources spent on configuring and managing connections between branches, data centers, cloud service providers, and SaaS providers (e.g., less time spent manually configuring individual network routers and installing at individual locations). They can also maximize the use of existing network bandwidth from a wide range of communication services while decreasing their dependence on costly MPLS resources for establishing available, fault-tolerant connections. To maintain application performance, the Aruba SD-WAN Orchestrator has been designed to reroute traffic dynamically should customer-defined application and/or network thresholds not be met. Capital and operational expenses decrease without sacrificing overall performance and availability.

Aruba SD-Branch customers using AWS Transit Gateway can reap additional benefits with the integration of the two solutions. The integration first simplifies how organizations connect on-premises locations to Amazon VPCs in two ways:

- *Deploy Aruba Virtual Gateways (vGWs) and extend the Aruba SD-WAN fabric into the AWS Cloud via a transit VPC* - By importing an AWS account into Aruba Central, an IT administrator has full visibility into all Amazon VPCs within that account. Aruba vGWs can now be centrally configured and deployed (via Amazon EC2 instances) into any Aruba-based transit VPC. Each transit VPC becomes another "location" that can connect to other on-premises locations included in the SD-WAN overlay. Simultaneously, the transit VPCs connect to AWS Transit Gateway, which connects with the organization's Amazon VPCs.
- *Directly connect on-premises Aruba gateways to AWS Transit Gateway* - Organizations can take advantage of the integration and automation between AWS Transit Gateway Network Manager and Aruba Central. Instead of deploying Aruba vGWs in Amazon Transit VPCs and connecting those vGWs with select branches, an administrator can connect a group of Aruba branch gateways (that share a common configuration and policy within an AWS Region) to an AWS Transit Gateway (see Figure 7).

Figure 7. Using Aruba SD-Branch to Connect to Multiple Amazon VPCs via AWS Transit Gateway



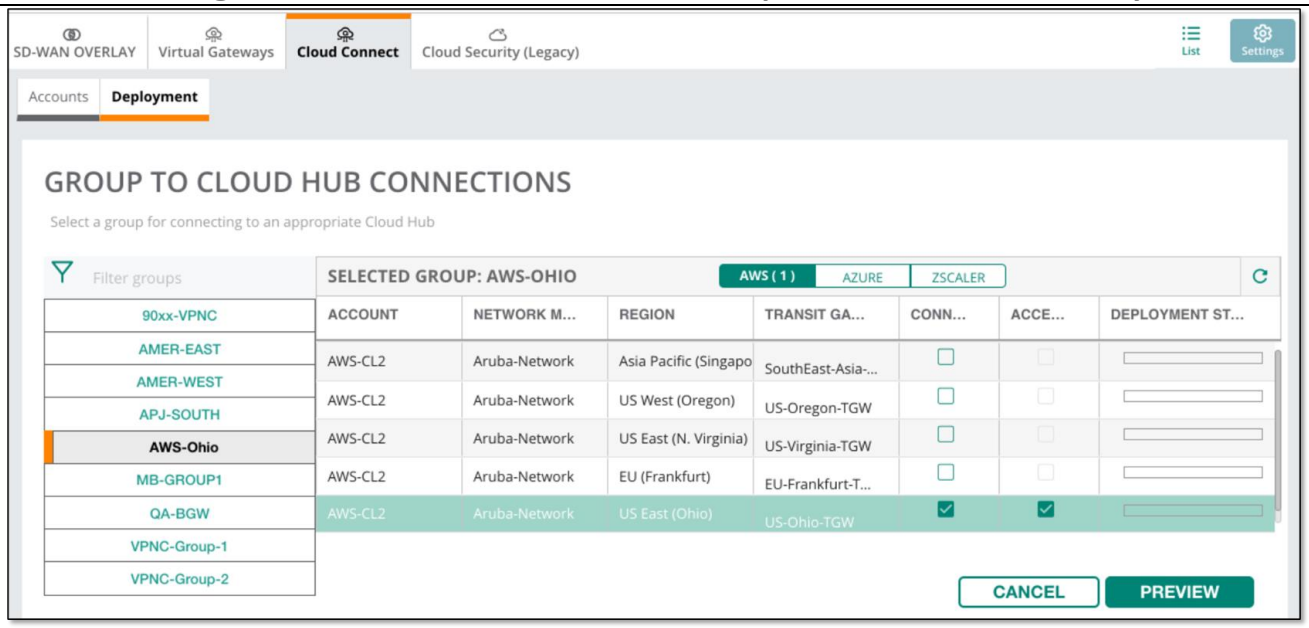
Source: Enterprise Strategy Group

Using the Cloud Connect application of Aruba Central (see Figure 8), an IT administrator imports an AWS account. Aruba Central then detects AWS Transit Gateways (or hubs) accessible to the branch groups. By clicking on the *Connections*

checkbox, the branch groups are automatically connected to the selected hub. Once the connections are established, IP prefixes of allowable addresses are automatically exchanged between AWS Transit Gateway and the Aruba branch gateways in the branch group. Organizations can save time and resources when making connections via groups as opposed to connections with individual branch offices.

Connecting branch groups to AWS Transit Gateway is not limited to an AWS Region. With AWS Transit Gateway Inter-Region Peering, these branch groups can now potentially reach Amazon VPCs deployed in AWS Regions globally (see Figure 7).

Figure 8. Establishing VPN Connections between Branch Groups and AWS Transit Gateway



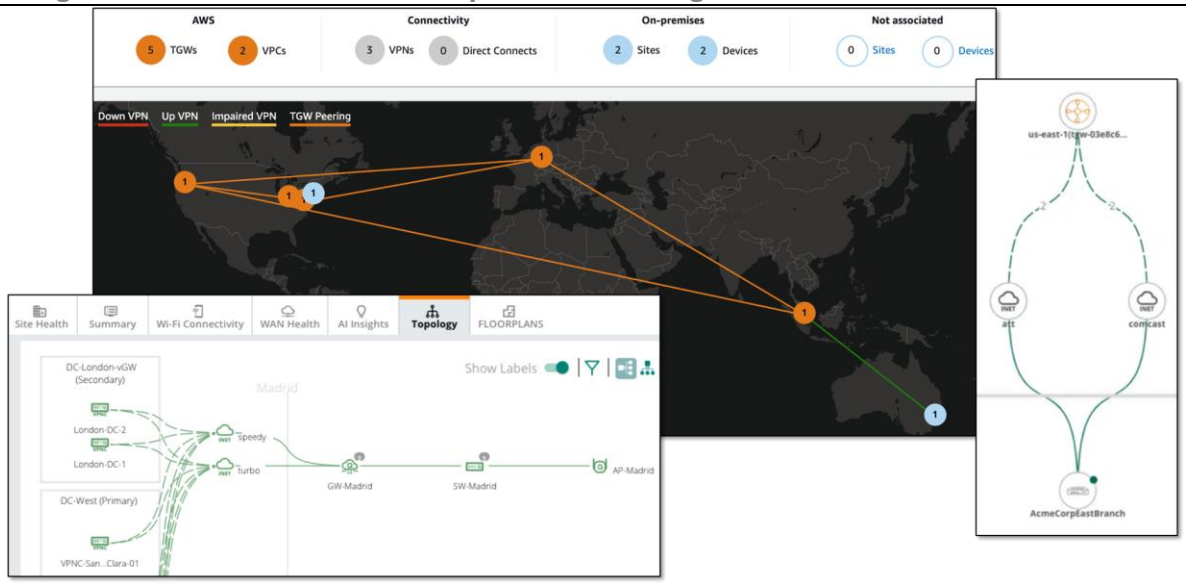
Traffic from any on-premises location can now potentially reach any Amazon VPC connected to the selected AWS Transit Gateway. The number of point-to-point connections between the branch offices and AWS Transit Gateway decreases, as well as the amount of time spent on actually creating these branch-to-cloud connections.

Connections between the branch groups and AWS Transit Gateway can also be managed via policies created by the administrator. If the Aruba Orchestrator detects that thresholds for network and application performance metrics cannot be met for a traffic flow, defined policies will signal the Aruba Orchestrator to dynamically reroute traffic over alternative network transport. Less time is spent on monitoring performance and reconfiguring connections when performance-impacting issues arise, thus increasing service uptime.

With the integration of AWS Transit Gateway Network Manager and Aruba Central, organizations can gain end-to-end visibility of their networks spanning both on-premises and the AWS Cloud (see Figure 9). For example, the IT administrator can view the network's geography as well as a list of the number of AWS resources (hubs and Amazon VPCs), the number and types of connections between the branch groups and hubs, and the number of on-premises locations.

With Aruba Central, an administrator can also view the SD-WAN overlay connecting branch groups and AWS Transit Gateway, along with other relevant information such as originating and terminating IP addresses. The integrated view helps to improve end-to-end visibility of the network while minimizing the number of management interfaces to be used. Time spent on management effort decreases, helping to lower operational costs over time.

Figure 9. Integration of AWS Transit Gateway Network Manager with Aruba Central



Why This Matters

When pursuing a hybrid cloud strategy, connecting IT resources in on-premises data centers and ROBOs to the cloud presents challenges. AWS customers with a large number of Amazon VPCs to be networked with one another and on-premises locations have relied on numerous point-to-point connections, increasing network complexity and time spent on deployment, management, and administration. They need a solution that simplifies the network architecture while decreasing the time spent on network deployment, management, and administration.

AWS Transit Gateway enables organizations to network their cloud and on-premises resources simply by centralizing Layer 3 connectivity, decreasing the number of point-to-point connections significantly. When used in conjunction with Aruba SD-Branch, organizations can simplify how they connect their branch offices to the AWS Cloud. Via the SD-WAN overlay supported by the Aruba branch gateways, the Aruba Central SD-WAN Orchestrator can simplify operations by automating and orchestrating connections from the Aruba branch gateways deployed in branch offices directly to AWS Transit Gateway. The combination of AWS Transit Gateway and Aruba SD-Branch ultimately can help organizations to decrease network infrastructure, cloud, and IT operational expenses.

Case Study – Verisk Analytics, Inc.

Verisk Analytics, Inc. (Verisk) is a US-based private company that provides predictive analytics and decision support services in areas such as fraud prevention, actuarial science, and risk assessment. It currently serves clients globally in the insurance, natural resources, financial services, and government sectors.

Challenges

Based in Jersey City, NJ, Verisk has over 10,000 end-users in 171 offices spread across 30 countries. The company is working toward a goal of enabling end-users across all branch offices to access its business applications through a common IT platform. Verisk initially relied on accessing applications via legacy mainframes operating in two data centers located on both the east and west US coasts. Over the past few years, the IT team has been migrating its legacy applications, as well as deploying new applications, into Amazon VPCs that Verisk has deployed in six AWS Regions.

While Verisk transitioned its applications to the AWS Cloud, the company had to ensure that end-users in any branch could continue to access legacy applications that have not yet been migrated from the data centers. Simultaneously, Verisk wanted to simplify how branches connected to any Amazon VPC, as well as how they connected to the data center. Specifically, the team sought to decrease the number of point-to-point connections between branch office Amazon VPCs and between data centers. Verisk also desired to reduce the number of branch connections to data centers to further decrease complexity in its IT network. Finally, the company wanted to simplify how these connections are configured and maintained, especially given the COVID-19 pandemic. As offices remain closed, Verisk can no longer rely on field engineers to manually configure networking equipment onsite.

Solution

With a combination of AWS Transit Gateway and Aruba SD-Branch, Verisk is building out a simpler IT environment that is easier to configure and manage. To decrease the number of connections between branch offices and AWS Transit Gateway in a specific region, Verisk is leveraging AWS Transit Gateway. Specifically, Verisk deploys an Aruba vGW into an Amazon VPC—an edge VPC—that sits between the branches and AWS Transit Gateway. With Aruba branch gateways, the Aruba Orchestrator automates and orchestrates the deployment of VPN tunnels connecting the branches with the edge VPC. A transit gateway attachment then connects the edge VPC with AWS Transit Gateway. Route tables associated with the branch gateways and AWS Transit Gateway are now exchanged so that traffic is accurately directed between the branch offices and the Amazon VPCs. To continue the migration of legacy applications to the AWS Cloud, Verisk connects the data centers to AWS Transit Gateway via AWS Direct Connect. Direct connections from the branch offices to the data centers are eliminated.

Finally, the use of Aruba SD-Branch decreases the need for field engineers to manually configure routers at each office. Using Aruba Central, Verisk can now centrally configure Aruba branch and virtual gateways and simplify how the interconnections are created and maintained.

Benefits

AWS Transit Gateway enabled Verisk to reduce the number of VPN tunnels connecting its branch offices, Amazon VPCs, and data centers, decreasing the overall complexity in its IT architecture. Using Aruba SD-Branch to deploy Aruba branch and virtual gateways and automate how Verisk connects its on-premises environment with the AWS Cloud simplifies IT operations and decreases ongoing management costs.

> "The combination of AWS Transit Gateway and Aruba SD-Branch provides us with a centralized management platform to build a secure, reliable, and cost-effective global hybrid cloud infrastructure that supports our worldwide user community."
>
> - Network Engineering Manager, Verisk, Sophie Wu

The Bigger Truth

Organizations' adoption of cloud infrastructure services continues to increase, yet most plan to maintain some level of on-premises environments. Building and updating the network underlying hybrid clouds can be a complex and time-consuming exercise that decreases business agility. To remove this burden, organizations can benefit from a solution that easily enables a global network architecture connecting cloud and on-premises environments while decreasing overall network complexity.

AWS Transit Gateway can simplify a hybrid cloud network by centralizing Layer 3 connectivity of Amazon VPCs, on-premises data centers, and ROBOs. Beyond this, organizations can use AWS Transit Gateway to address a prominent challenge in implementing a hybrid cloud, particularly in large enterprises: setting up a global, scalable, and manageable network without extensive time dedicated to architecture design, planning, purchasing, and refreshes. Along with AWS Transit Gateway, AWS enables organizations to build out a global enterprise-grade network by offering features such as inter-region AWS Transit Gateway peering and the AWS Transit Gateway Network Manager.

Using Aruba SD-Branch, organizations can simplify how they connect their on-premises locations to their Amazon VPCs without using numerous point-to-point connections. By utilizing branch groups, which contain Aruba branch gateways that share a common configuration and policy within an AWS Region, organizations can directly connect these groups with AWS Transit Gateway. The Aruba SD-WAN Orchestrator automates how branches and Amazon VPCs connect via the AWS Transit Gateway by orchestrating IP source and destination IP addresses exchanged between the branch groups and AWS Transit Gateway. The integration of AWS Transit Gateway Network Manager and Aruba Central provides organizations with centralized configuration and end-to-end visibility of their networks spanning both on-premises and the AWS Cloud.

ESG's case study validated that AWS Transit Gateway has begun to help organizations build out and expand a virtual network architecture connecting large numbers of Amazon VPCs with one another and with on-premises networks. The result was a simplified network architecture in which AWS Transit Gateway acts as the central hub for traffic between branches and Amazon VPCs. Aruba SD-Branch enabled our featured customer to reduce the time in connecting branch offices with Amazon VPCs via AWS Transit Gateway. Effort spent on manually configuring route tables of both Aruba gateways and AWS Transit Gateway decreased when using the Aruba Orchestrator, subsequently decreasing IT operational costs.

ESG was impressed with the benefits that the featured AWS customer derived. We believe that organizations can leverage AWS Transit Gateway to address a wide variety of use cases related to building and managing the network underlying their hybrid clouds. We were also impressed with the capabilities of Aruba SD-Branch and how they further simplify the deployment, management, and administration of hybrid clouds.

For organizations planning large-scale Amazon VPC deployments, ESG strongly believes that you should consider AWS Transit Gateway with Aruba SD-Branch when evaluating solutions for building out a cloud-based global network architecture.