Enterprise Strategy Group | **Getting to the bigger truth.™**

Technical Review

Automation of Cloud Networking with Amazon Web Services Transit Gateway and Aviatrix Orchestrator

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

Abstract

The report highlights the benefits delivered by AWS Transit Gateway in conjunction with the Aviatrix Transit Gateway Orchestrator. We illustrate how the Amazon Web Services (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 how the Aviatrix Transit Gateway Orchestrator enables organizations to automate the deployment and administration of a hybrid cloud architecture enabled by AWS Transit Gateway. A case study features the benefits derived from using this combined solution.

The Challenges

67% The percentage of organizations that use or plan to use infrastructure-as-a-service (IaaS).[1]

54% The percentage of organizations that expect to **maintain a measurable on-premises environment** in the next three years.[2]

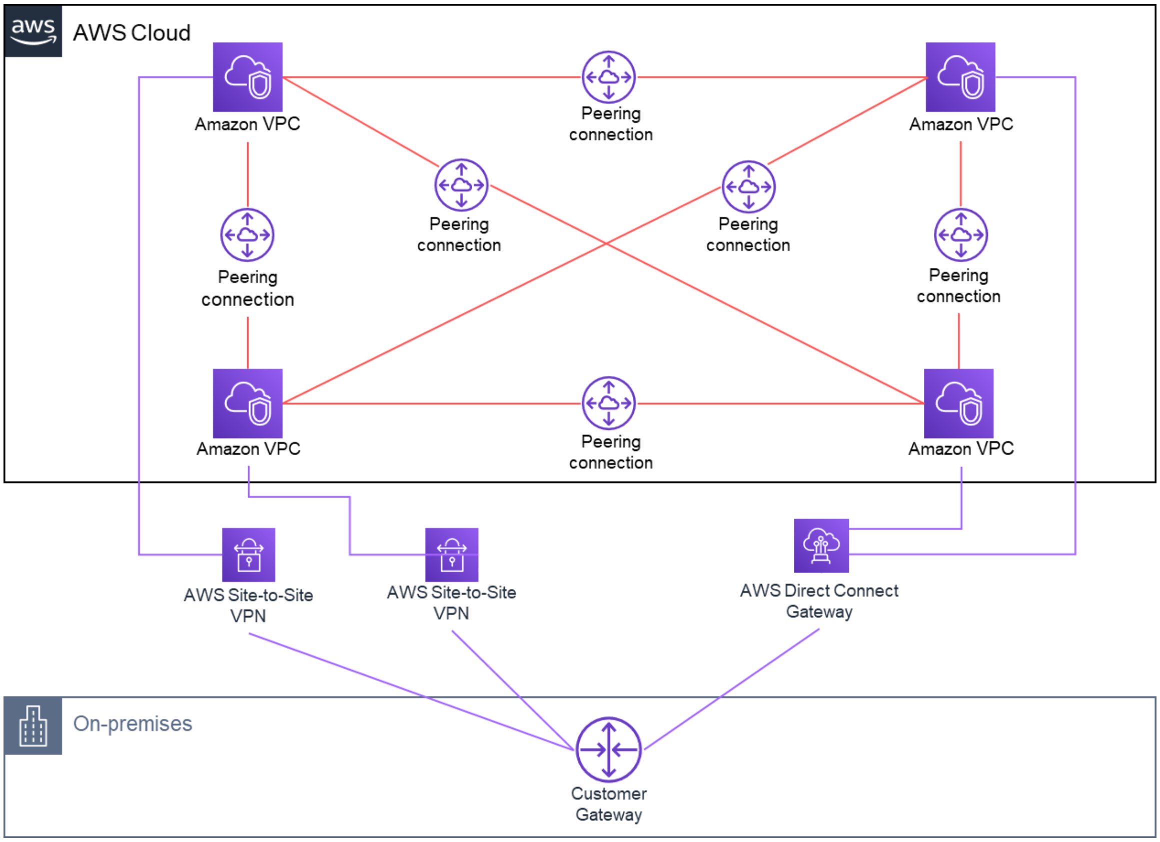
95% The percentage of organizations that view their IT environments as **equally or more complex** than two years ago.[3]

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.

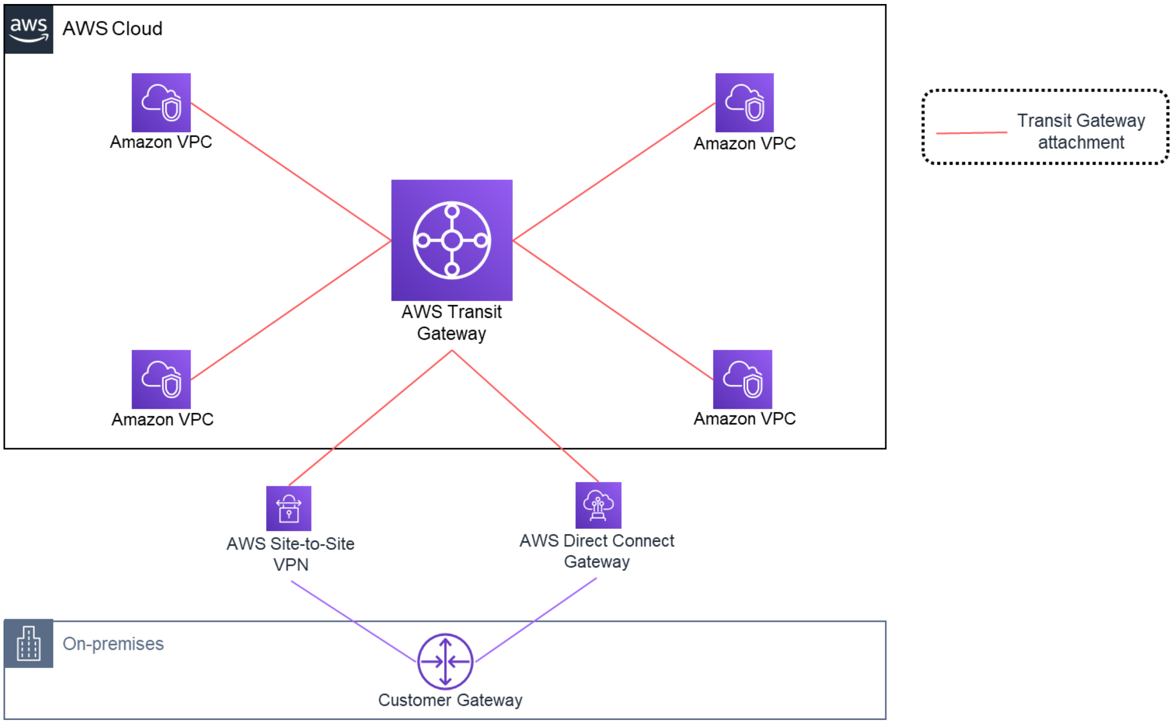
The Solution: Amazon Web Services Transit Gateway

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

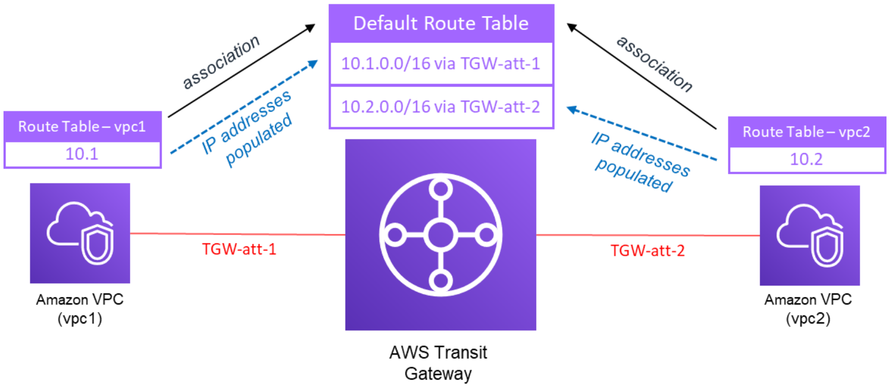


Source: Enterprise Strategy Group

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

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

complexity while increasing operational efficiency. Creating AWS Direct Connect, AWS Site-to-Site VPN, and VPC peering 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 Partner Network (APN) 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 100 Gbps network links connecting all AWS Regions globally.

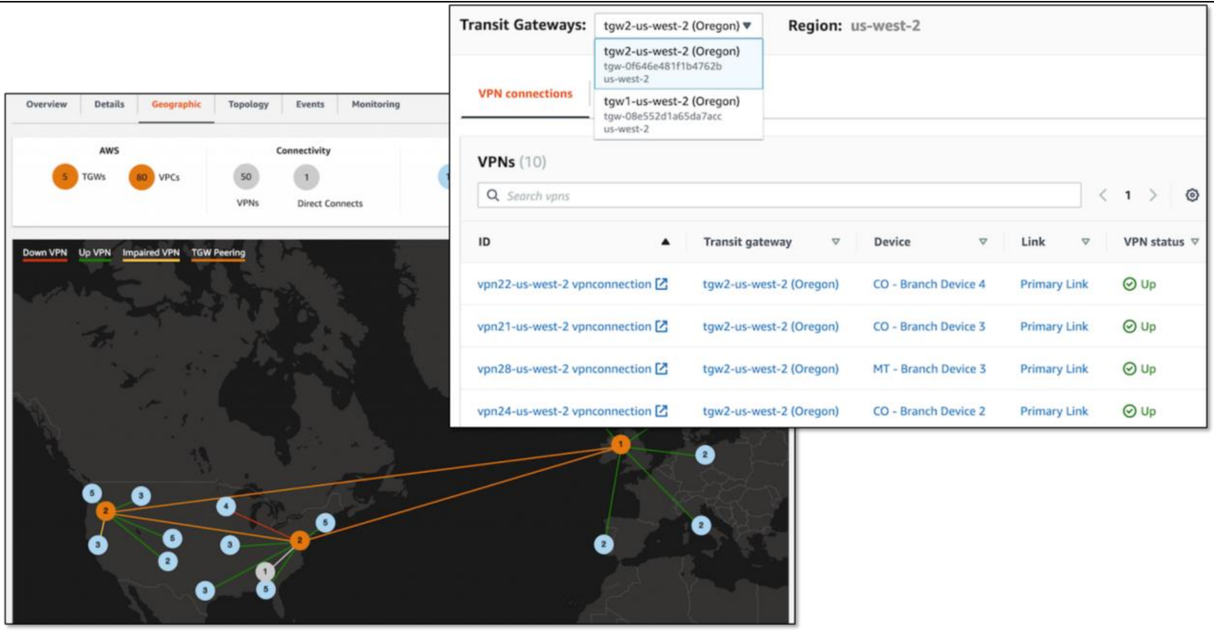
With inter-region peering, organizations can architect a private global network while decreasing the time and resources required to connect an organization’s Amazon VPCs and on-premises networks in different regions. Functional groups, such as engineering and development, can collaborate with minimal 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, 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 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, 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

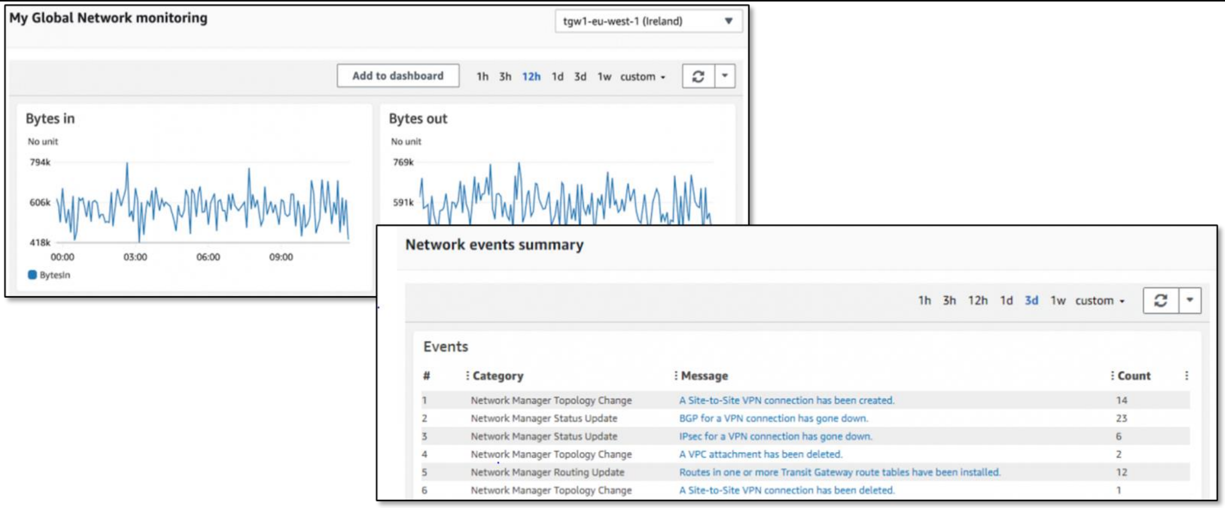


ID	Transit gateway	Device	Link	VPN status
vpn22-us-west-2 vpnconnection	tgw2-us-west-2 (Oregon)	CO - Branch Device 4	Primary Link	✓ Up
vpn21-us-west-2 vpnconnection	tgw2-us-west-2 (Oregon)	CO - Branch Device 3	Primary Link	✓ Up
vpn28-us-west-2 vpnconnection	tgw2-us-west-2 (Oregon)	MT - Branch Device 3	Primary Link	✓ Up
vpn24-us-west-2 vpnconnection	tgw2-us-west-2 (Oregon)	CO - Branch Device 2	Primary Link	✓ Up

Monitoring and Management

To manage and monitor AWS-based networks, 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

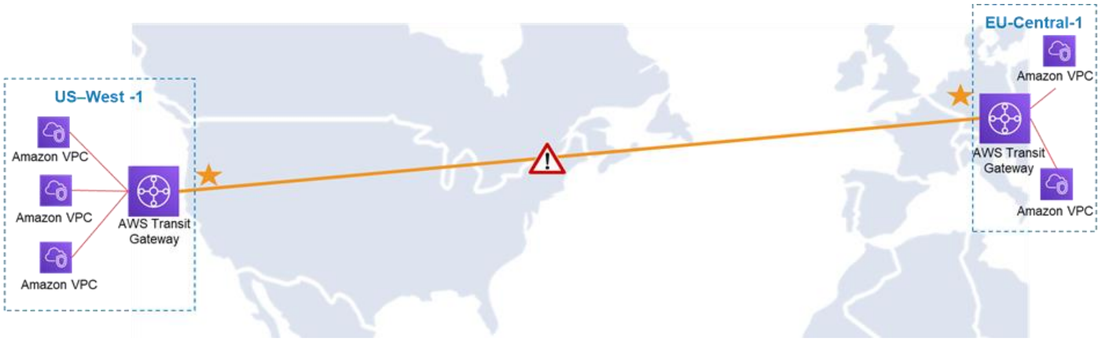


#	Category	Message	Count
1	Network Manager Topology Change	A Site-to-Site VPN connection has been created.	14
2	Network Manager Status Update	BGP for a VPN connection has gone down.	23
3	Network Manager Status Update	IPsec for a VPN connection has gone down.	6
4	Network Manager Topology Change	A VPC attachment has been deleted.	2
5	Network Manager Routing Update	Routes in one or more Transit Gateway route tables have been installed.	12
6	Network Manager Topology Change	A Site-to-Site VPN connection has been deleted.	1

Route Analyzer

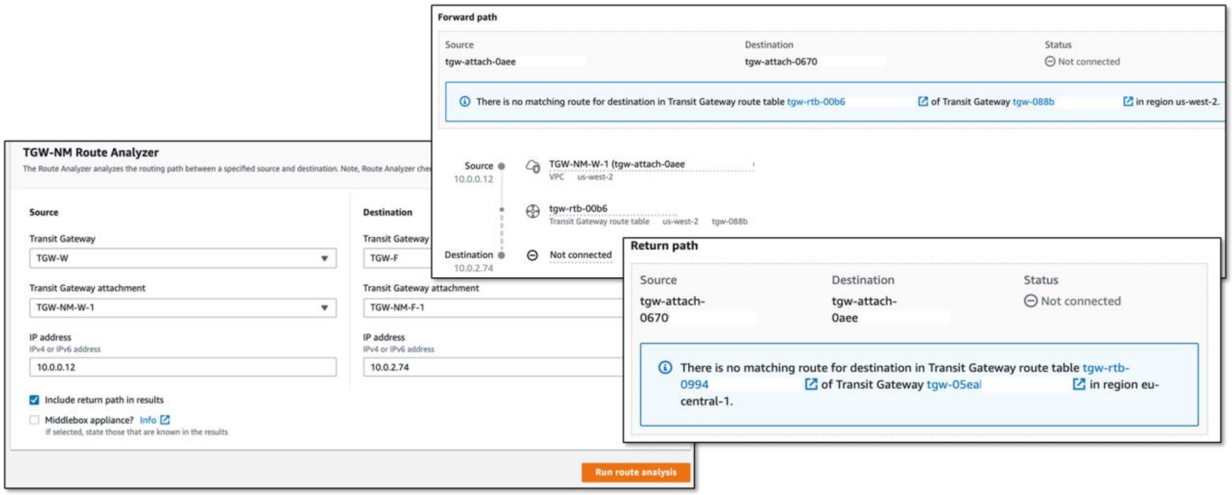
In addition to monitoring near real-time network metrics, organizations can identify potential causes of network disruptions by analyzing how traffic is routed between AWS Transit Gateways and their attached Amazon VPCs and on-premises locations. With Route Analyzer (accessed via AWS Transit Gateway 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 AWS Transit Gateway's 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 AWS Transit Gateways (as indicated in the blue fields). The administrator now knows that correcting this issue requires inputting the correct routes into AWS Transit Gateway's route tables.

Figure 5. Troubleshooting with Route Analyzer



Forward path

Source	Destination	Status
tgw-attach-0aee	tgw-attach-0670	⊖ Not connected

ⓘ There is no matching route for destination in Transit Gateway route table tgw-rtb-00b6 of Transit Gateway tgw-088b in region us-west-2.

Source 10.0.0.12 — TGW-NM-W-1 (tgw-attach-0aee VPC us-west-2

tgw-rtb-00b6 Transit Gateway route table us-west-2 tgw-088b

Destination 10.0.2.74 — ⊖ Not connected

TGW-NM Route Analyzer

The Route Analyzer analyzes the routing path between a specified source and destination. Note, Route Analyzer che

Source	Destination
Transit Gateway: TGW-W	Transit Gateway: TGW-F
Transit Gateway attachment: TGW-NM-W-1	Transit Gateway attachment: TGW-NM-F-1
IP address (IPv4 or IPv6 address): 10.0.0.12	IP address (IPv4 or IPv6 address): 10.0.2.74

☑ Include return path in results

□ Middlebox appliance? Info
If selected, state those that are known in the results

Return path

Source	Destination	Status
tgw-attach-0670	tgw-attach-0aee	⊖ Not connected

ⓘ There is no matching route for destination in Transit Gateway route table tgw-rtb-0994 of Transit Gateway tgw-05eal in region eu-central-1.

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 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.

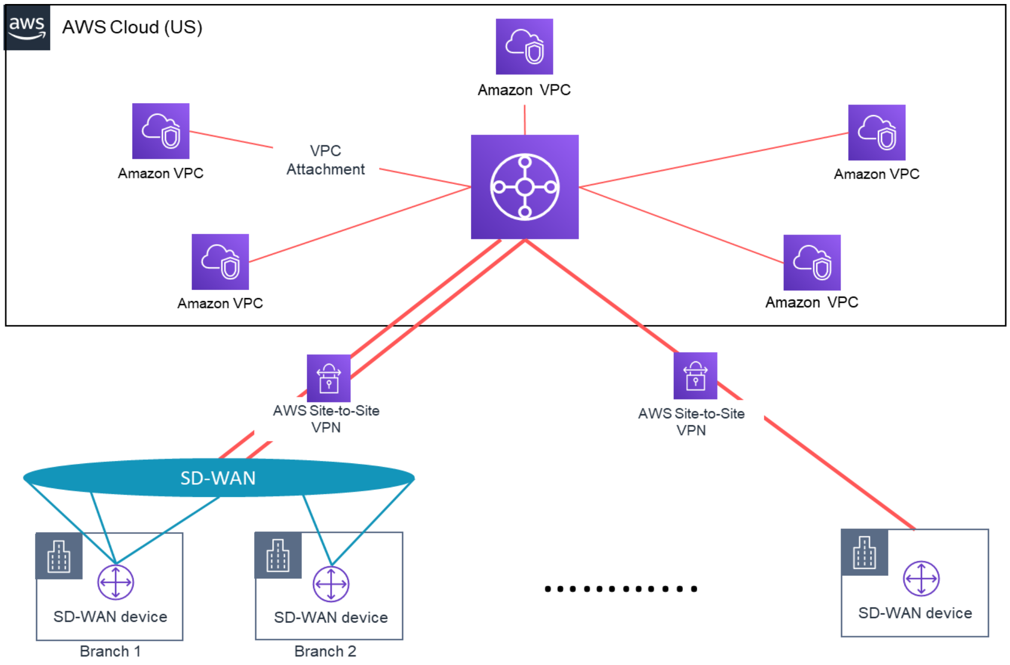
Security

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 APN 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.

Network Orchestration at Scale with the Aviatrix Orchestrator

While AWS Transit Gateway can consolidate a large number of Amazon VPC connections, organizations can still spend excessive time on manually updating the Amazon VPC route tables. When an Amazon VPC attaches to AWS Transit Gateway, its IP address ranges are propagated to the gateway's default route table, defining how traffic flows from the gateway to the Amazon VPC. To route traffic on the Amazon VPC's egress path to other Amazon VPCs or on-premises locations, a network or cloud administrator must manually enter the destination IP addresses in the Amazon VPC route table and designate AWS Transit Gateway as the target. As the number of attached Amazon VPCs increase, so does the time related to Amazon VPC route table administration.

The Aviatrix Transit Gateway Orchestrator is designed to dynamically update the route tables of Amazon VPCs attached to AWS Transit Gateway. Any changes made to route tables of AWS Transit Gateway and attached Amazon VPCs are automatically propagated to one another via the Orchestrator. The Orchestrator can reduce the time and resources spent on route table administration. It also helps in reducing the number of manual errors that can occur when configuring route tables.

The Orchestrator natively supports both Amazon Site-to-Site VPN and AWS Direct Connect, enabling organizations to connect their Amazon VPCs with their on-premises offices and data centers to create a hybrid cloud. Scaling a hybrid cloud environment is easier as the Orchestrator can automatically update route tables of Amazon VPCs within and across AWS Regions as well as across multiple AWS accounts, as well as customer gateways.

Organizations can also segment the Amazon VPC network by creating Aviatrix Security Domains,[7] leveraging the capability to create multiple route tables within AWS Transit Gateway. An administrator can impose policies on Security Domains to direct and isolate traffic via the Orchestrator. Security Domains will not impact network performance as they do not impose any traffic overhead. For example, organizations can use Security Domains to segment and isolate application traffic and resources via network segmentation and isolation.

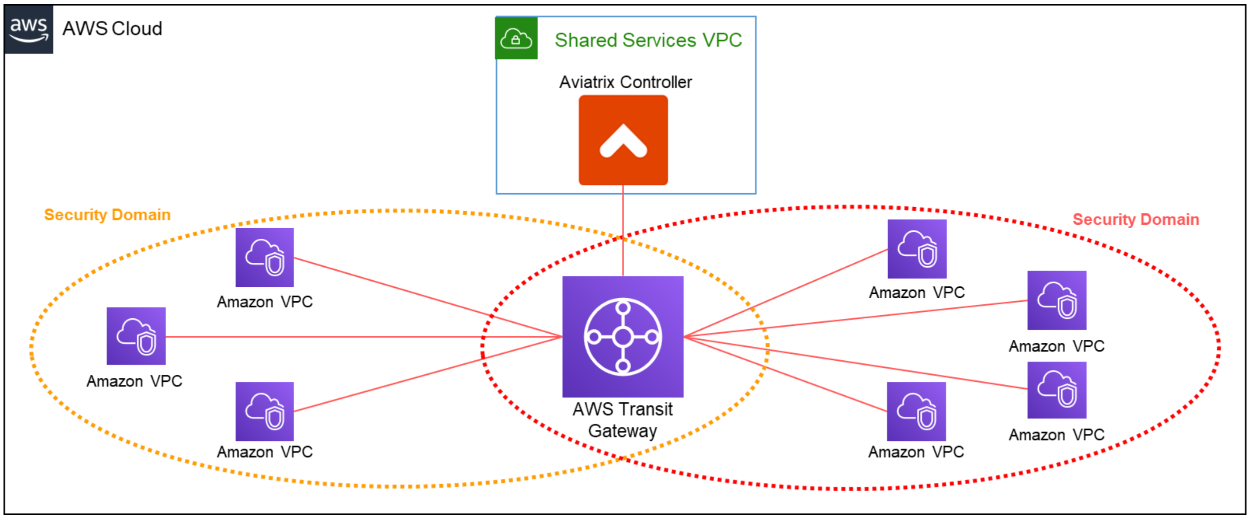
Central to the Orchestrator is the Aviatrix Controller, which creates the abstraction layer, representing the interconnection of an organization's AWS Transit Gateway with its Amazon VPCs and related Security Domains (see Figure 7). Not only does

[7] An Aviatrix Security Domain is an enforced network of Amazon VPCs. Amazon VPCs within a Security Domain can communicate with one another, not with Amazon VPCs in separate Security Domains, unless dictated by policy set within the Aviatrix Orchestrator.

the Controller automate route propagation, but it also provides end-to-end network visibility. This visibility includes network performance monitoring, such as latency between any Amazon VPCs.

The Orchestrator can also uncover connectivity issues via FlightPath. This tool reveals connection paths between any Amazon EC2 instances by using information collected by the Aviatrix controller: Amazon EC2 security groups, route table entries, and network access control lists (ACL). FlightPath supports network troubleshooting, reducing time spent on identifying and resolving connectivity issues. Management costs decrease while business uptime increases.

Figure 7. Integration of Aviatrix Orchestrator with AWS Transit Gateway



Source: Enterprise Strategy Group

Why This Matters

When pursuing a hybrid cloud strategy, interconnecting IT resources in both the cloud and on-premises data centers and ROBOs 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. With the Aviatrix Orchestrator, large enterprises can automate route propagation at scale when changes in the route tables of AWS Transit Gateway, Amazon VPCs, and on-premises gateways occur. The Orchestrator can also provide end-to-end network visibility to help in resolving network performance and connectivity issues.

Case Study - Taco Bell

Taco Bell is a global fast-food restaurant brand operated by Yum! Brands, Inc., a Fortune 500 global corporation. As of 2018, Taco Bell has over 7,000 locations in the Americas, Europe, and Asia-Pacific regions.

Challenges

Based in Irvine, CA, Taco Bell's IT operations focus on restaurant support, serving organizations responsible for a variety of functions, such as front of house (e.g., registers, self-serve kiosks, and digital menu boards), back-of-house (e.g., labor scheduling, timekeeping, and inventory management). Taco Bell had been leveraging AWS services and appreciated the speed and flexibility AWS offered for spinning up IT resources when needed. Over time, the company recognized that there was a lack of centralized control in the AWS environment; multiple individuals opened their own accounts unknown to IT operations. Individuals resorted to using personal credit cards to open AWS accounts, and no one person knew which Amazon VPCs peered with one another (i.e., there was little visibility into east-west traffic). Taco Bell also faced challenges in scaling its network, as deploying virtual firewalls in every VPC to secure traffic would not scale in the long run, both from a cost and operational perspective. Firewalls inspecting all traffic between Amazon VPCs could also impact network performance, which would conversely impact end-user experience.

Solution

Taco Bell is better securing its AWS environment by using the AWS Landing Zone to automate the setup of a standard baseline environment across multiple accounts. Taco Bell also began using AWS Transit Gateway so that only an AWS primary account owner could create Amazon VPCs for internal organizations, centralizing connectivity, control, and monitoring.

While Taco Bell looked to build out a cloud-native network, it wanted to preserve the functionality that was used to operate and manage a traditional on-premises network. Taco Bell viewed the Aviatrix Orchestrator as key in providing the capabilities for managing and administering this network. The company leveraged the Orchestrator's automation capabilities to facilitate dynamic routing so as to propagate route changes to all Amazon VPC route tables with minimal manual intervention.

Taco Bell also wanted to route traffic through a "central" firewall, as an organization would traditionally route all traffic through firewalls in a data center. To accomplish this, Taco Bell also implemented a Shared Services VPC to host the network's firewalls. Using Aviatrix's Security Domains, Taco Bell could set policies directing all traffic via AWS Transit Gateway to the Shared Services VPC, ensuring full unified threat management as all east-west and north-south traffic is inspected by the firewalls and firewall logs are collected for monitoring purposes.

Benefits

With AWS Transit Gateway, Taco Bell centralized network control, ensuring that all Amazon VPCs were created from one account so that it had visibility into the demand for AWS resources. It could now scale its network easily by leveraging the automation capabilities of the Aviatrix Orchestrator. Taco Bell also gained end-to-end visibility of its cloud-based network from a routing and security perspective with the Orchestrator. Using these solutions jointly, Taco Bell foresees that it can provide an overall better user experience for both its internal organizations and Taco Bell customers.

> "The combination of the AWS Transit Gateway and the Aviatrix Orchestrator provides Taco Bell with a cloud-native network with all the functionality we require for managing and securing an on-premises network. We get the security and visibility that we want from the Aviatrix Orchestrator with the networking, security, and flexibility that we need."
>
> Senior Manager – Network Engineering, Eric Rhoades, Taco Bell

The Bigger Truth

Organizations' adoption of cloud infrastructure services continues to increase,[8] yet most plan to maintain some level of on-premises environments.[9] 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 global network architecture by centralizing Layer 3 connectivity of Amazon VPCs, on-premises data centers, and remote offices. Organizations can use AWS Transit Gateway to quickly set up a global, scalable, and manageable network without extensive time dedicated to architecture design, planning, purchasing, and refreshes. AWS enables organizations to build out such a network by offering features such as AWS Transit Gateway Inter-Region Peering, AWS Transit Gateway Network Manager, and cross-account support.

Using the Aviatrix Orchestrator, organizations can scale out their network easily via its automation capabilities. As changes to route tables occur, the Aviatrix Orchestrator propagates these changes throughout the network based on AWS Transit Gateway, reducing the time and effort typically dedicated to route table administration. Large enterprises building out their hybrid cloud environments with a large number of Amazon VPCs will especially benefit from the automation.

The Aviatrix Orchestrator also helps with improving overall network security. By setting up Security Domains, organizations can deploy policies that direct traffic to specific Security Domains. Specifically, organizations can deploy virtual firewalls within a Shared Services VPC in its own Security Domain, then use the Orchestrator to direct all traffic there for full inspection, without impacting network performance.

ESG's case study validated that AWS Transit Gateway can serve as a platform for building and expanding a virtual network architecture interconnecting large numbers of Amazon VPCs with one another and with on-premises networks. At the same time, AWS Transit Gateway enabled our featured customer to centralize network control without sacrificing flexibility and scalability. The Aviatrix Orchestrator enhances the benefits of segmentation and network visibility that AWS Transit Gateway provides by providing functionality that large enterprises typically require for deploying and managing traditional on-premises networks.

AWS has managed to simplify the deployment of scalable network environments, yet large enterprises want to operate them in ways similar to traditional wired networks. As the AWS-Aviatrix partnership progresses, Aviatrix will need to respond quickly to its customers as AWS Transit Gateway continues to evolve to provide functionality that will help in transitioning from on-premises to hybrid cloud environments.

ESG was impressed with the benefits that AWS customers 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 the Aviatrix Orchestrator and how they further simplify the deployment, management, and administration of hybrid clouds via its automation of route table propagation and end-to-end visibility. For organizations planning large-scale Amazon VPC deployments, ESG strongly believes that you should consider AWS Transit Gateway with the Aviatrix Orchestrator when evaluating solutions for interconnecting your cloud and on-premises environments.

[8] Source: ESG Master Survey Results, *2020 Technology Spending Intentions Survey*, January 2020.
[9] Source: ESG Master Survey Results, *Hybrid Cloud Trends*, May 2019.

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of The Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at 508.482.0188.

The goal of ESG Validation reports is to educate IT professionals about information technology solutions for companies of all types and sizes. ESG Validation reports are not meant to replace the evaluation process that should be conducted before making purchasing decisions, but rather to provide insight into these emerging technologies. Our objectives are to explore some of the more valuable features and functions of IT solutions, show how they can be used to solve real customer problems, and identify any areas needing improvement. The ESG Validation Team's expert third-party perspective is based on our own hands-on testing as well as on interviews with customers who use these products in production environments.