ESG Validation

Amazon Web Services Transit Gateway

Simplifying Global Network Architectures

By Alex Arcilla, Validation Analyst

August 2020

This ESG Validation was commissioned by Amazon Web Services and is distributed under license from ESG.

Contents

ESG Validations

The goal of ESG Validations is to educate IT professionals about information technology solutions for companies of all types and sizes. ESG Validations 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.

Executive Summary

While organizations have adopted cloud services to become more agile and deliver applications and services faster, their IT networks have become more complex and difficult to manage as the volume of cloud applications scaled up quickly. AWS Transit Gateway helps to eliminate that complexity and provide operational efficiency by dramatically simplifying how organizations connect applications spanning both their on-premises locations and the cloud.

By employing a "hub-and-spoke" architecture, AWS Transit Gateway centralizes connectivity between large IT deployments both on-premises and in the AWS Cloud. With additional features such as AWS Transit Gateway Inter-Region Peering and AWS Transit Gateway Network Manager, organizations can build out simplified global enterprise network architectures.

Via customer interviews, ESG validated that AWS Transit Gateway reduces the number of point-to-point network connections to be created, monitored, and managed between multiple Amazon Virtual Private Clouds (VPC), as well as between Amazon VPCs and on-premises IT networks.

Introduction

The report illustrates how Amazon Web Services (AWS) Transit Gateway enables organizations to simplify and scale the connectivity of Amazon Virtual Private Clouds (VPCs) with one another and to their on-premises networks via a central hub. We examine the solution, the benefits delivered, and highlight three customers currently using AWS Transit Gateway.

Background

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]

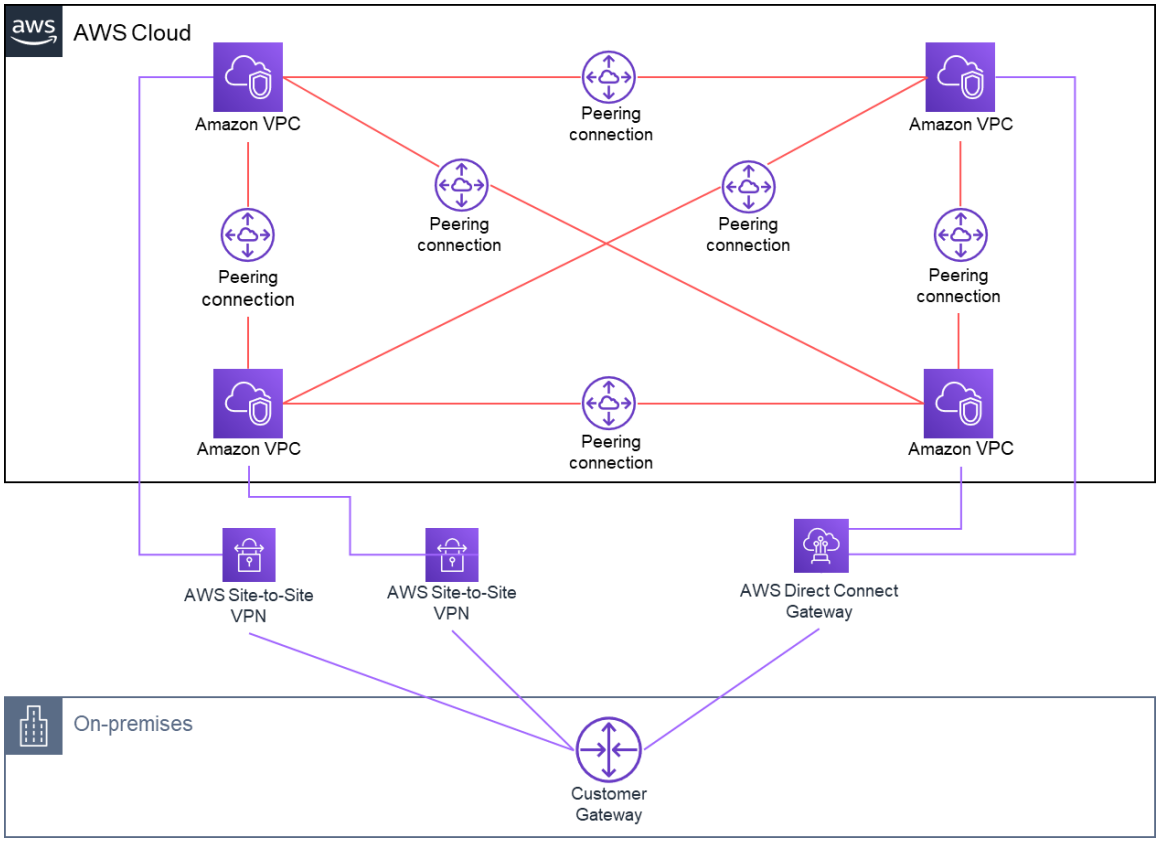
Enterprise cloud adoption continues to increase as organizations want to leverage infrastructure-as-a-service (IaaS) for the ease of application deployment and IT resources scalability. Yet, as the number of organizations planning to run production applications on the cloud grows, they still intend to 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 each other, 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 each other 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

[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.

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 each other (see Figure 1).

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.

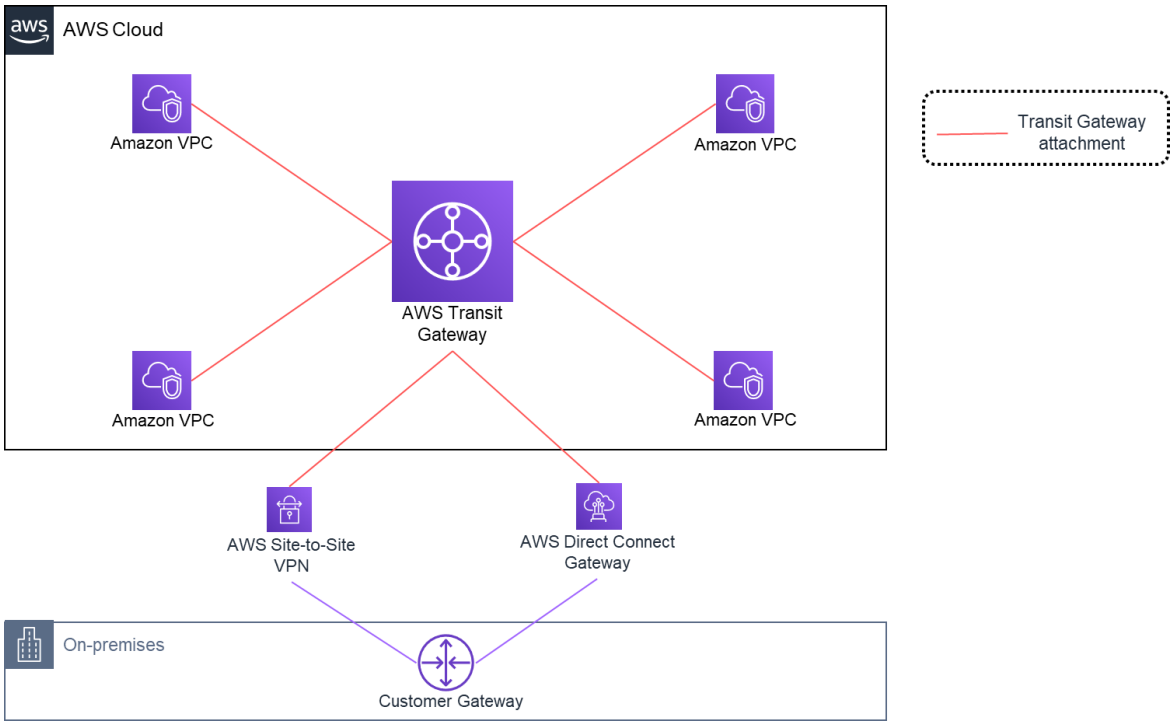
AWS Transit Gateway simplifies how organizations connect their Amazon VPCs with one another and to their on-premises networks within a region (see Figure 2) by serving as a central point for Layer 3 network connectivity. By enabling a "hub-

[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.

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.

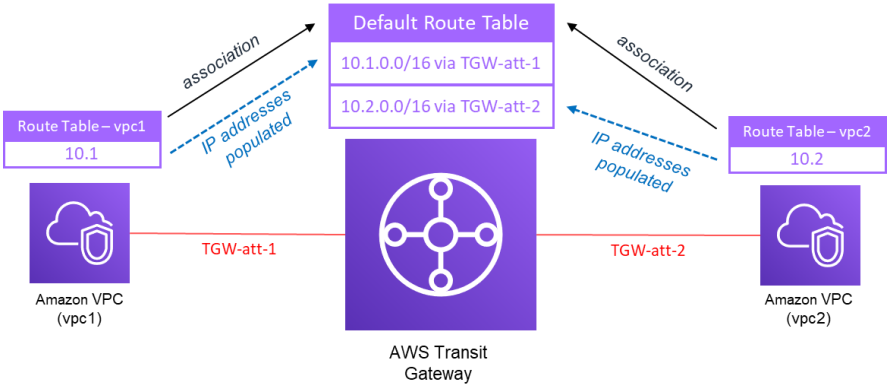
Figure 2. AWS Transit Gateway – Reducing Number of Point-to-Point Connections



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 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

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

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 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.

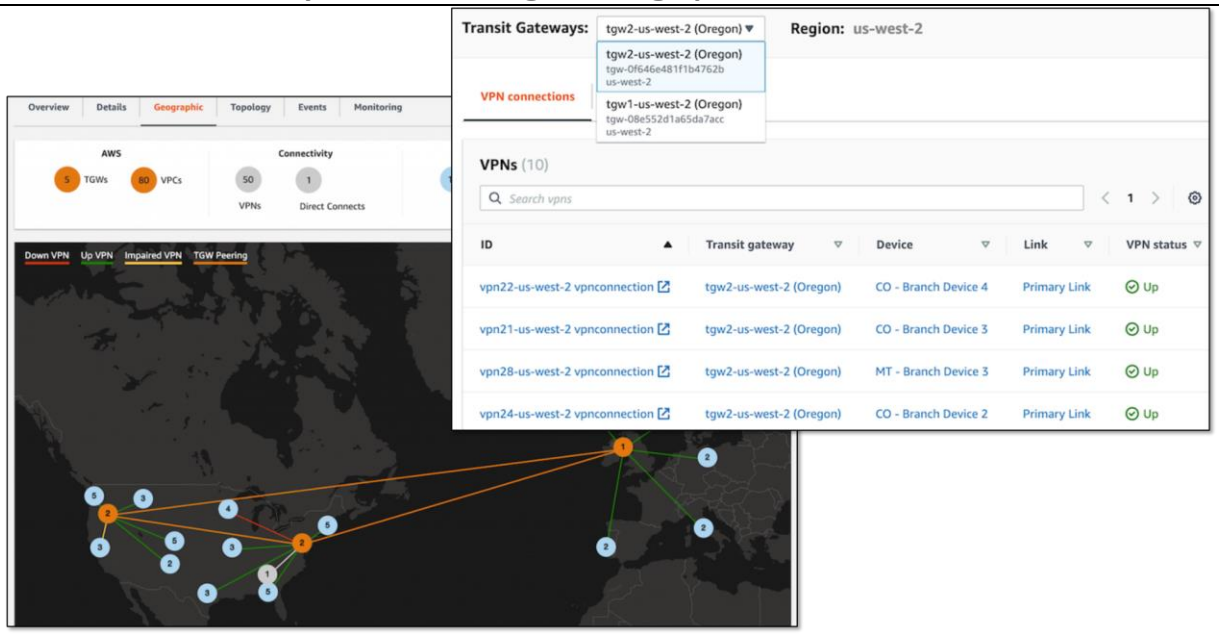
With inter-region peering, organizations can architect a private global network while decreasing the time and resources required to connect an organization's Amazon VPCs and on-premises networks in different regions. Functional groups, such as engineering and development, can collaborate with minimal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

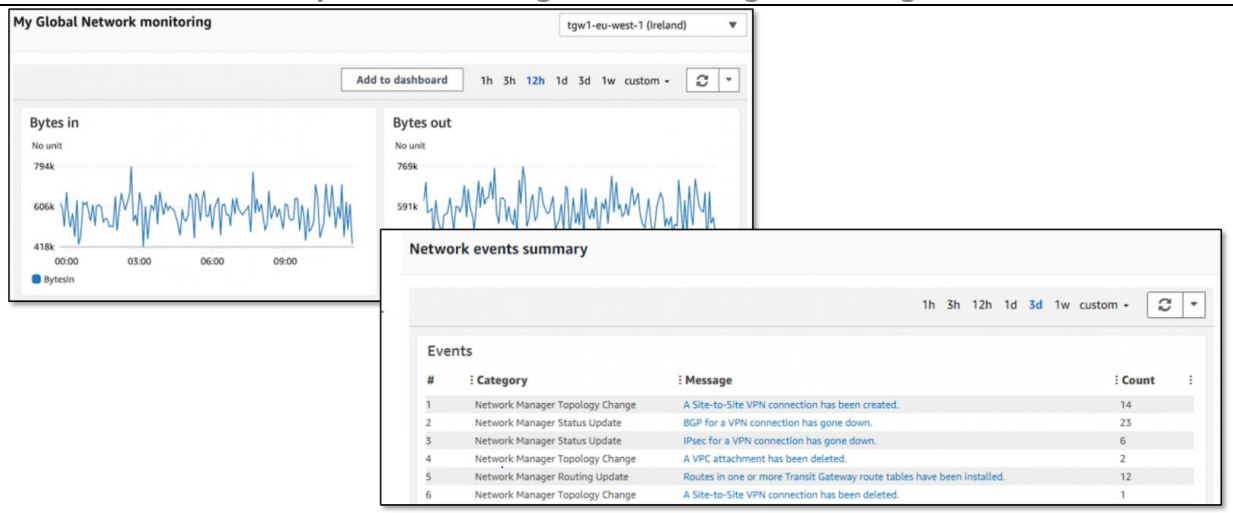
Figure 3. AWS Transit Gateway Network Manager – Geographic and Detailed Views



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



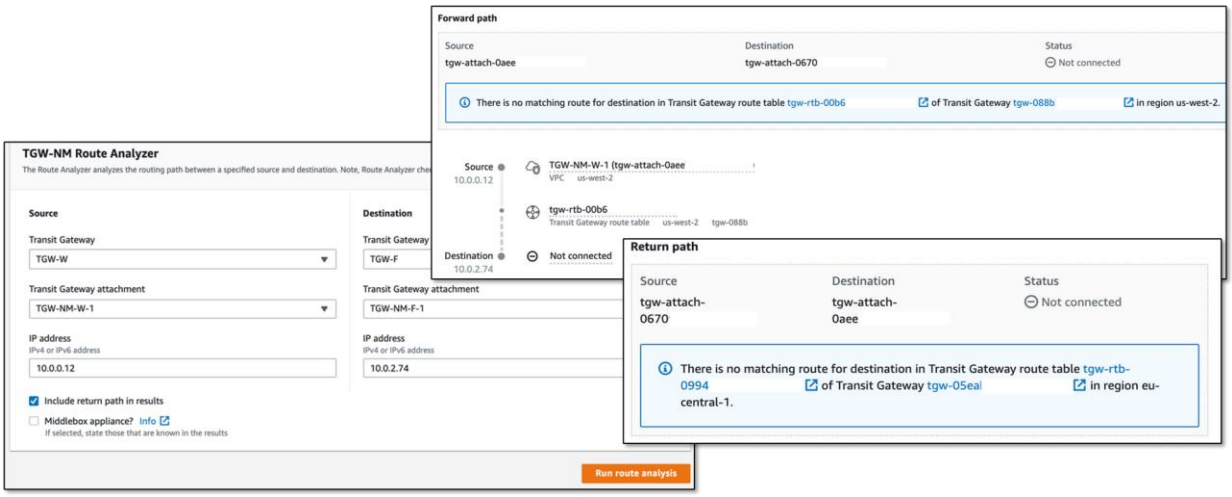
Route Analyzer

In addition to monitoring near real-time network metrics, organizations can also 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 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



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.

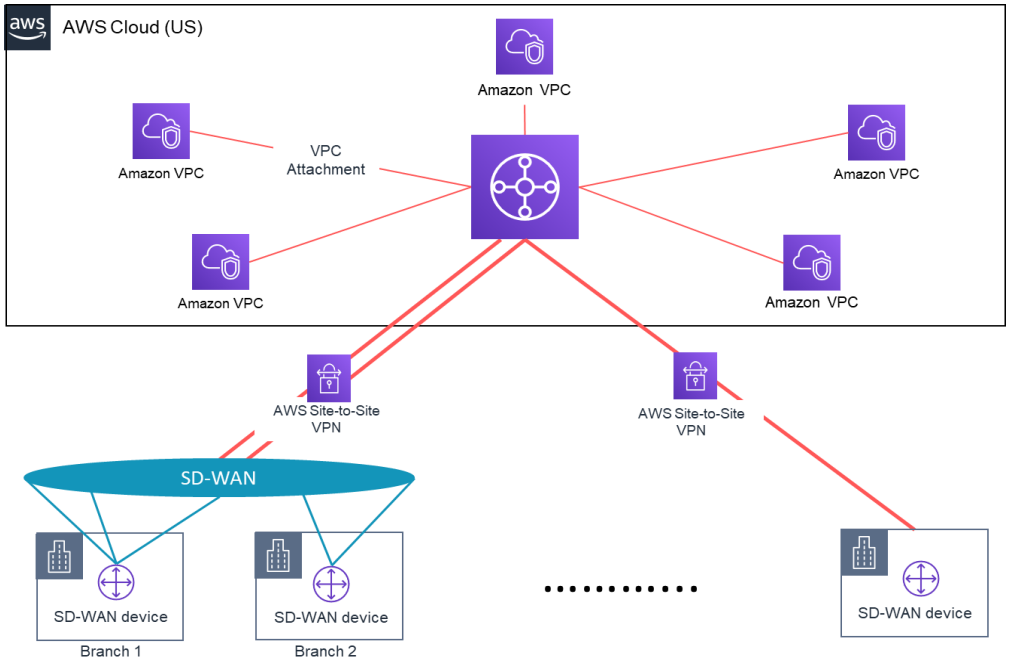
Security

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 re-routing 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.

ESG Customer Validation

ESG interviewed three AWS customers to illustrate how they used AWS Transit Gateway to address their challenges and highlight the benefits they derived.

Fuze

Headquartered in Boston, MA, Fuze is a privately held company that delivers unified communications-as-a-service (UCaaS) to global enterprises. The company's product combines business communications services including business voice, videoconferencing, contact center, instant messaging, content sharing, and collaboration apps.

Challenges

Fuze initially worked with AWS to migrate the majority of its global local compute resources off of regional co-location spaces (co-los) onto AWS infrastructure so that they could reduce the time to deploy infrastructure for delivering its UCaaS to new accounts globally— North America, Latin America, Europe, Asia-Pacific, and Africa.

As Fuze continued to deploy Amazon VPCs, particularly for its production networks, the need to interconnect these Amazon VPCs grew. On a regional level, internal groups, such as Infrastructure, DevOps, and development, needed to collaborate on projects in which AWS resources were distributed. Fuze also had to ensure that Amazon VPCs were interconnected where necessary to ensure smooth service delivery to its customers without sacrificing performance. Fuze still relied on global and strategic points of presence (PoP) for either customers that demanded on-premises private connectivity or carriers with whom Fuze partnered for telecom services. While the company initially leveraged VPC peering and AWS Site-to-Site VPN connections, the number of point-to-point connections increased significantly as Fuze deployed additional VPCs. Its network of cloud and on-premises resources was becoming too complex to grow and manage.

Solution

With AWS Transit Gateway, Fuze began to simplify its overall global network architecture, spanning both AWS infrastructure and its remaining co-lo footprint. Fuze interconnected all of its Amazon VPCs by creating attachments to this central hub, instead of creating multiple point-to-point connections with VPC peering. Fuze now relies on one attachment between a co-lo and AWS Transit Gateway to communicate with any attached Amazon VPC. Fuze is currently exploring the use of AWS Transit Gateway peering to not only interconnect Amazon VPCs in different global regions but also to take advantage of the AWS global backbone to add a layer of network availability, in case of failure in its own private network backbone.

Benefits

With AWS Transit Gateway, Fuze simplified the interconnection of AWS resources without creating and managing multiple point-to-point connections. Rather than dealing with the management overhead of VPC peering, Fuze can simply create the desired attachments between select Amazon VPCs and the regional AWS Transit Gateway. Creating new connections between Amazon VPCs and its co-los also became simpler, as the company no longer had to request individual AWS Site-to-Site VPN or AWS Direct Connect connections to interconnect with select regional Amazon VPCs. Internal IT operations no longer has to coordinate with the networking team to create VPN tunnels to the AWS environment.

> "With the simple design of AWS Transit Gateway, Fuze decreased the time and management complexity of interconnecting our AWS based environments and on-premises PoPs. With this fully managed service, we were able to reduce the time to spin up and interconnect resources from weeks to minutes"
>
> **Khoder Shamy - Director of Cloud Services, Fuze**

Trend Micro

Trend Micro is a multinational enterprise cybersecurity and defense company that develops software, cloud, and virtualized security products. Global enterprises use Trend Micro products to secure servers and containers, as well as cloud computing environments, networks, and endpoints.

Challenges

Trend Micro has been leveraging AWS to deliver its cloud-based products to customers globally. The company's current footprint encompasses nine AWS regions, each containing multiple Amazon VPCs, while it still maintains five on-premises, co-located data centers. Within each AWS region, Trend Micro deployed multiple Amazon VPCs that focus on the development and delivery of its cloud-based products. To ensure high service availability and exceptional customer experience, the company has assigned Amazon VPCs to focus on service delivery, while it has deployed other VPCs, in different regions, where DevOps can build and validate new services or service features before deployment.

Once DevOps completed their work, they would need to interconnect their Amazon VPCs with Trend Micro's production Amazon VPCs; both sets of Amazon VPCs would belong to different AWS accounts. While the company would typically use VPC peering to interconnect the DevOps and production Amazon VPCs, it found drawbacks to this approach.

Setting up VPC peering connections between separate accounts became unmanageable and cumbersome. For a VPC peering connection to be established, one account sends the connection request, while the other account must accept it. The account accepting the request must manually configure the Amazon VPC to accommodate the new connection. While this may be a simple process when dealing with a small number of connections, Trend Micro anticipated repeating this process and reconfiguring connections as part of their normal operations. Since DevOps deployed its new services and features via AWS CloudFormation templates, setting up VPC peering connections via infrastructure-as-code would result in repeated code changes as the VPC peering connections would constantly change. Trend Micro faced similar issues when having to connect its data centers with Amazon VPCs using AWS Site-to-Site VPN connections.

Solution

Using AWS Transit Gateway, Trend Micro only had to interconnect both Amazon VPCs and on-premises data centers via transit gateway attachments. The need for two-way coordination, especially between teams with different AWS accounts, to interconnect Amazon VPCs and on-premises data centers was eliminated. DevOps no longer has to modify multiple lines of code in AWS CloudFormation templates to deploy new services validated in the DevOps Amazon VPCs to customers.

> "Without waiting days or weeks to provision new connections between DevOps and Production Amazon VPCs, our DevOps team can now deploy the cloud-based network architecture for delivering new services on-demand by leveraging infrastructure-as-code. Lines of code are minimized and easy to update as all interconnections are facilitated via attachments to AWS Transit Gateway."
>
> Jaffer Li - Senior Project Manager, Trend Micro

Benefits

Trend Micro experienced a significant decrease in overall network deployment effort after migrating to AWS Transit Gateway. The company can now network Amazon VPCs to one another and with its on-premises data centers within a matter of hours as opposed to days. No longer are point-to-point connections required as all traffic is routed via attachments to AWS Transit Gateway. DevOps also reduces the time and effort to update its AWS CloudFormation templates, thus decreasing service delivery time to its customers.

VMware Carbon Black

VMware Carbon Black is a public company with more than 5,000 customers. It develops a cloud-native security platform that uses big data and behavioral analytics to provide comprehensive endpoint protection against cyberattacks.

Challenges

VMware Carbon Black uses AWS to deliver the Carbon Black Cloud, a software-as-a-service (SaaS) solution. With its deployment of Amazon VPCs in the US, Europe, and Asia regions, VMware Carbon Black funnels and processes billions of real-time event data to provide security intelligence (such as live incident response) to over 5000 customers through VMware Carbon Black Cloud, a software-as-a-service based (SaaS) solution. Its AWS footprint consists of 400 Amazon VPCs spanning 30 AWS accounts. VMware Carbon Black also has an on-premises data center that holds critical workloads the company requires to be highly secure.

Prior to using AWS Transit Gateway, the company leveraged VPC peering and AWS Direct Connect to connect Amazon VPCs with each other and its on-premises data center with point-to-point connections. However, it not only added to the overall network complexity, but also did not provide a level of visibility and control over the network traffic flow. This was especially a concern for its security operations center (SOC) teams, who are responsible for monitoring all traffic flowing between Amazon VPCs as well as to and from its data center. With these point-to-point connections, the SOC team could not track and monitor all traffic efficiently, as it would need to collect and examine logs from each connection. The team also did not have control over which AWS account would request to connect with Amazon VPCs or the data center owned by other AWS accounts. The effort expended by the SOC team to gain some level of visibility and control ultimately took time and resources away from their primary responsibilities—to secure VMware Carbon Black's IT environment.

Solution

By leveraging AWS Transit Gateway, VMware Carbon Black connected its Amazon VPCs and on-premises data center via a central hub. The company decreased the number of existing point-to-point connections that had been maintained. VMware Carbon Black could also control how traffic flowed throughout its environment, as it leveraged AWS Transit Gateway to centralize how Amazon VPCs from different AWS accounts speak with each other. It could also dictate specific Amazon VPCs that connected with its on-premises data center.

Benefits

VMware Carbon Black can now centralize how it isolated and controlled its network traffic flows. The company can manage how traffic is directed between Amazon VPCs, as one team manages AWS Transit Gateway. The SOC team could now use data collected from AWS Transit Gateway to track and monitor traffic flows. The company also preserved its desired strict security controls over interconnection with its data center, as it houses its intellectual property.

> "As a security-focused company, we wanted to ensure that we had full visibility and control over the traffic traversing our hybrid cloud. AWS Transit Gateway simplified how we managed communications between our Amazon VPCs and with our data center"
>
> **Billy Oreste - Manager, Site Reliability Engineering, VMware Carbon Black**

The Bigger Truth

Organizations' adoption of cloud infrastructure services continues to increase,[7] yet most plan to maintain some level of on-premises environments.[8] 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.

Through our customer interviews, ESG validated that AWS Transit Gateway can help organizations build out and expand a virtual global network architecture interconnecting large numbers of Amazon VPCs with one another and with on-premises networks. Our findings revealed that current AWS customers benefited from reducing the number of point-to-point connections used, thus eliminating the need for a complicated mesh network to be managed and maintained. Across the board, the AWS customers stated that they reduced the time for deploying and managing these network connections within their IT environments.

AWS Transit Gateway has succeeded in introducing a service that immediately addresses the issues of interconnecting multiple VPCs with each other and on-premises networks. As the service remains in its early stages, ESG believes that AWS Transit Gateway has room to grow into a more robust solution, such as incorporating advanced routing capabilities that global enterprises encounter when architecting their networks. With its customer-driven philosophy, ESG sees AWS Transit Gateway gaining more adoption in enterprise IT 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 their global network architecture. ESG strongly believes that you should consider AWS Transit Gateway when evaluating solutions to simplify the creation of a scalable, global network architecture that spans both the AWS cloud and on-premises environments.

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

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

 www.esg-global.com

 contact@esg-global.com

 P. 508.482.0188