Silver Peak Best Practice Guidelines: AWS Transit Gateway

This document provides design guidance and best practices for extending the Silver Peak Unity EdgeConnect SD-WAN fabric into a multi-region AWS network using AWS Transit Gateways.

Overview

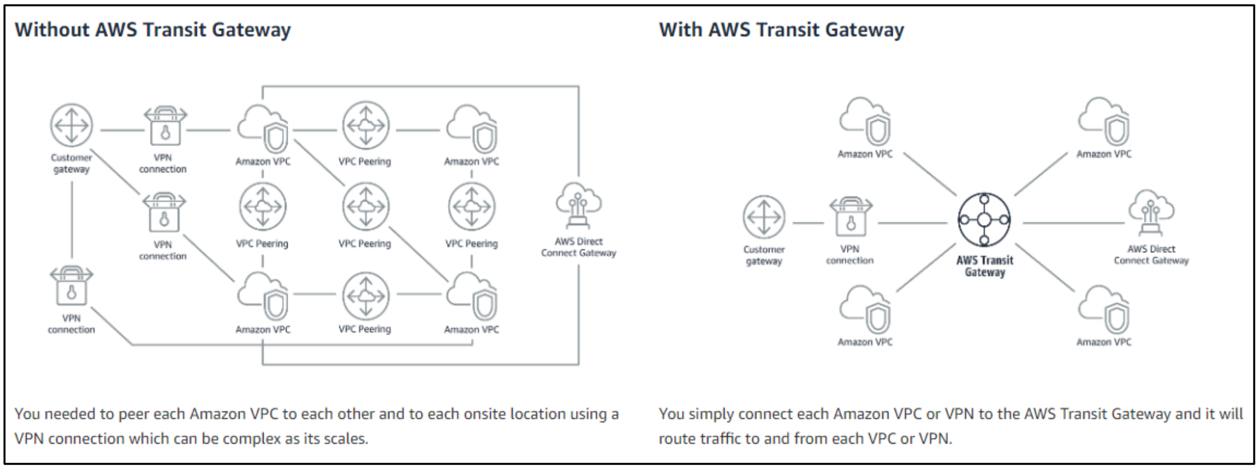
Silver Peak Unity EdgeConnect is available as a Bring your own License (BYOL) AMI in the AWS marketplace. For additional information about requirements and EdgeConnect Virtual (EC-V) deployments, see the following:

- Supported Instance Types and Host Requirements
- EdgeConnect Virtual (EC-V) in AWS Deployment Guide

Introduction to AWS Transit Gateway

The AWS Transit Gateway service lets customers connect their Amazon Virtual Private Clouds (VPCs) and on-premises networks to a single gateway. Prior to AWS Transit Gateway, inter VPC connectivity between AWS regions/accounts required managing point-to-point VPC peering relationships, often in a full-mesh. For on-premises connectivity, you would have needed to attach your AWS VPN to each individual Amazon VPC.

AWS Transit Gateway acts as a hub that controls how traffic is routed among all the connected networks, which act like spokes. An AWS Transit Gateway spoke can be a VPC in any region/account, VPN connection from a customer gateway, or Direct Connect. Transit gateways eliminate the need for VPN gateways, DX gateways, and transit VPC architectures. Transit gateways support static routing and Border Gateway Protocol (BGP) for learning and advertising network layer reachability information.



Without AWS Transit Gateway

With AWS Transit Gateway

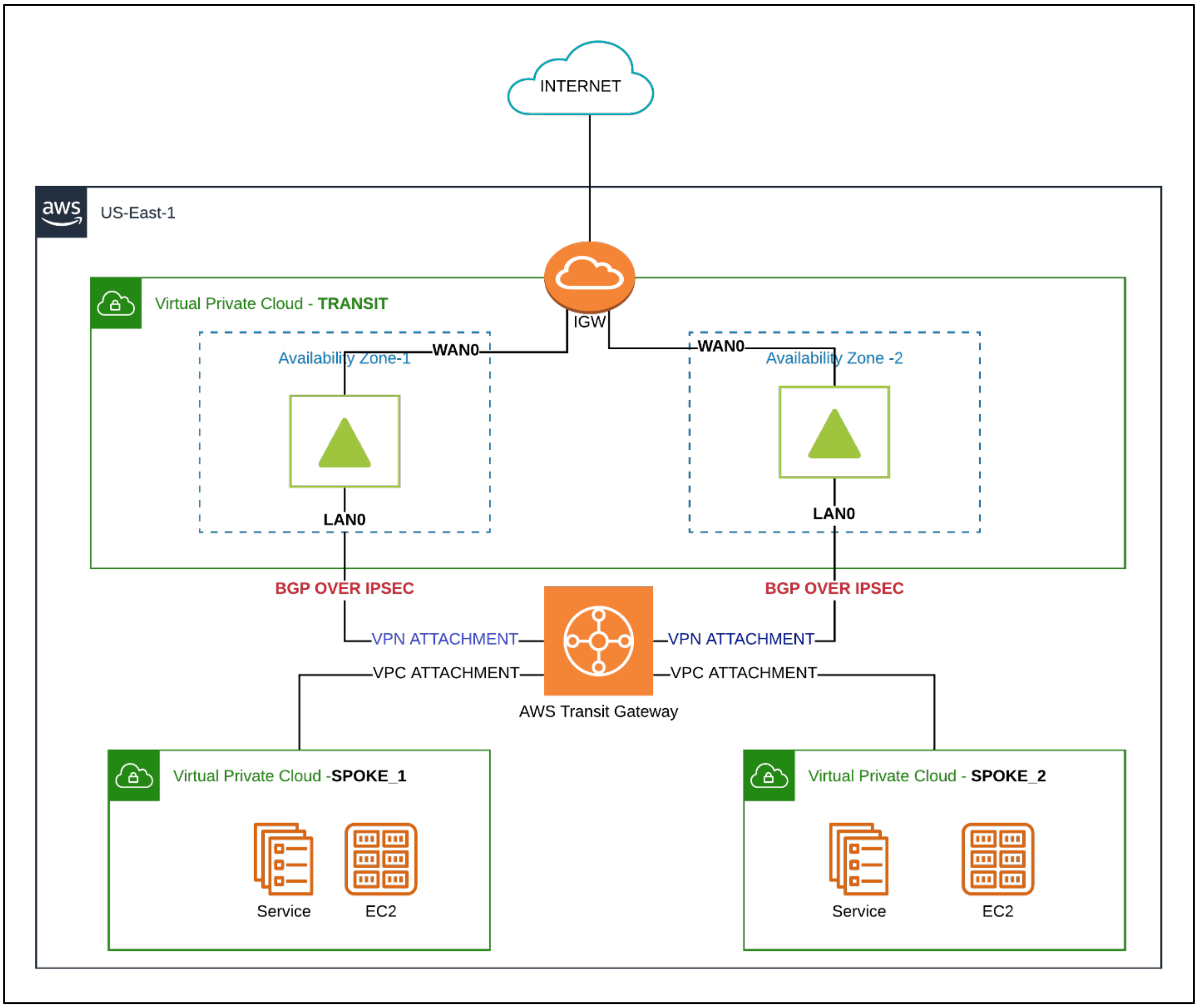
You needed to peer each Amazon VPC to each other and to each onsite location using a VPN connection which can be complex as its scales.

You simply connect each Amazon VPC or VPN to the AWS Transit Gateway and it will route traffic to and from each VPC or VPN.

EdgeConnect High Availability with Transit Gateways

EdgeConnect IaaS deployments in AWS can be scaled horizontally for the purpose of high availability and fault tolerance in addition to accommodating high throughput requirements.

The diagram below depicts EdgeConnect appliances configured as an HA pair in two different availability zones (AZs). The EdgeConnect appliances in the Transit VPC are added to the Transit Gateway as a VPN attachment. Redundant third-party VPN tunnels (two per VPN attachment) are established between the EdgeConnect LAN interface on both appliances to the Transit Gateway public IP addresses. Routes can be propagated between the Transit Gateway and the EdgeConnect (VPN attachment) via static routing, or BGP dynamic routing can be run over the IPSec tunnel. The spoke VPCs where cloud workloads are present are added to the Transit Gateway as VPC attachments.



NOTE: The design illustrated above uses a dedicated LAN interface with an elastic public IP address to build and terminate VPN connections to the Transit Gateway. Optionally, the VPN connection to the Transit Gateway can be established on the WAN interface leveraging the existing public IP on that interface. The EdgeConnect would then hairpin (WAN to WAN) the traffic from the SD-WAN tunnels to the third party IPSec tunnel to the Transit Gateway.

Design Considerations

It is important to keep in mind the following limitations when architecting your SD-WAN solution to integrate with AWS Transit Gateways.

Service Limitations when VPN Peering with a Transit Gateway

Limit	Default
Number of AWS Transit Gateway attachments	5,000
Maximum bandwidth per VPN connection [1]	1.25 Gbps
Maximum bandwidth (burst) per VPC, Direct Connect gateway, or peered Transit Gateway connection	50 Gbps
Number of AWS Transit Gateways per account	5
Number of AWS Transit Gateway attachments per VPC	5
Number of routes	10,000
Number of Direct Connect gateways per AWS Transit Gateway	20

[1] You can use equal-cost multi-path routing (ECMP) to get higher VPN bandwidth by aggregating multiple VPN connections.

The Transit Gateway supports a maximum encrypted throughput of 1.25 Gbps per VPN attachment due to a limitation on software-based VPN solutions in native AWS routing constructs like the TGW. Despite the availability of multiple CPU cores on the VM, a single VPN tunnel can only effectively use one core for site-to-site tunnel connectivity. Silver Peak is actively working on adding Equal Cost Multi-path (ECMP) routing to the EdgeConnect solution. ECMP will allow EdgeConnect to install and leverage multiple BGP next-hops for traffic forwarding and get a higher effective VPN throughput by aggregating multiple VPN attachments to the TGW.

Routing Limitations when BGP Peering with Transit Gateway

The maximum number of routing prefixes (i.e., remote SD-WAN routes) that can be advertised dynamically to a transit gateway is 100. This is a current AWS restriction and may or may not be increased in the future.

Limit	Default
Customer gateways per Region	50
Virtual private gateways per Region – you can attach only one virtual private gateway to a VPC at a time	5
Dynamic routes advertised from a customer gateway device to a Site-to-Site VPN connection (on a transit gateway or virtual private gateway) – this quota cannot be increased	100
Routes advertised from a Site-to-Site VPN connection to a customer gateway device – this quota cannot be increased	1000
Site-to-Site VPN connections per Region	50
Site-to-Site VPN connections per virtual private gateway	10

Silver Peak can address this limitation as follows:

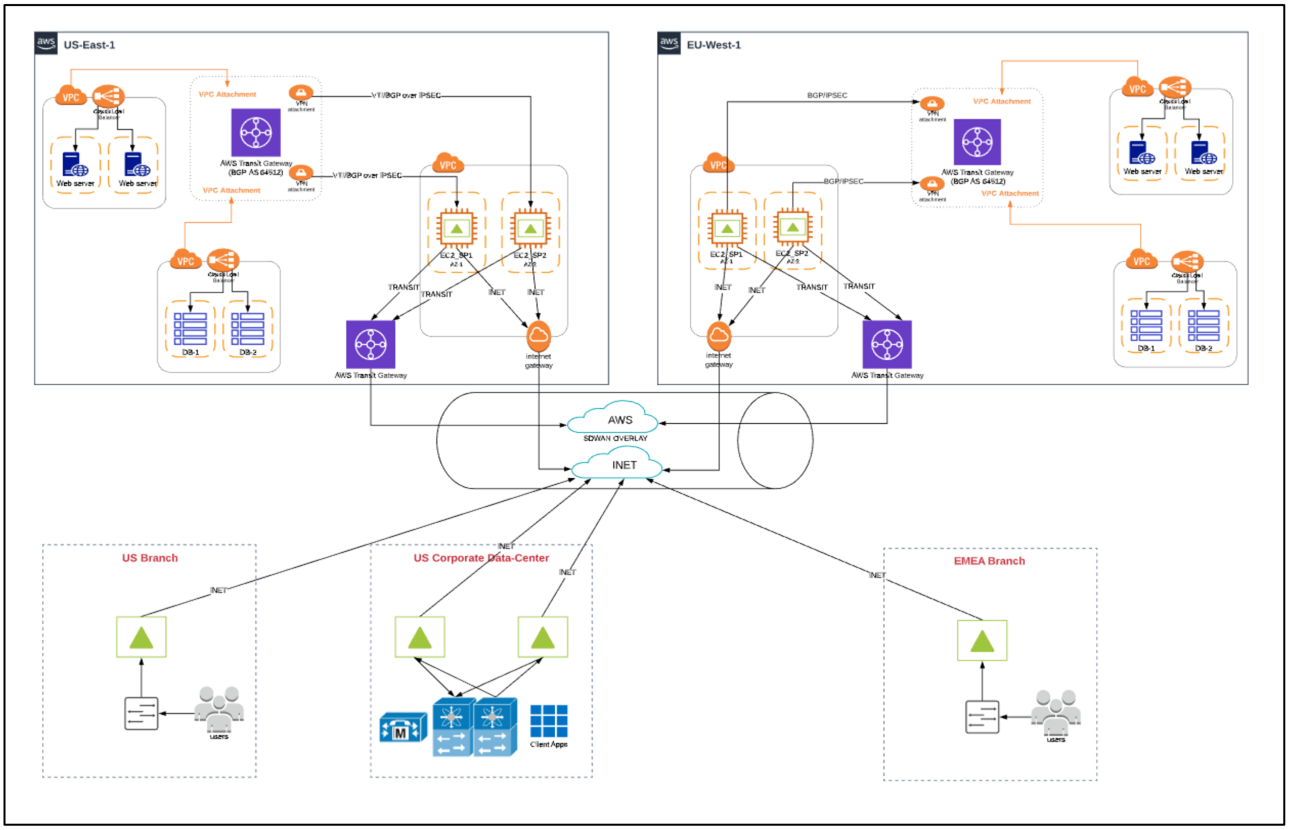
- Summarize or filter routes to reduce the number of remote SD-WAN routes advertised to the TGW.
- Multiple VPN attachments from different ENIs on the EdgeConnect and load share the remote SD-WAN prefixes across them.
- Utilize static routing, if feasible.

EdgeConnect and AWS Transit Gateway Deployment Examples

This section describes three different deployment examples to illustrate different types of connectivity across regions, remote sites, and branches.

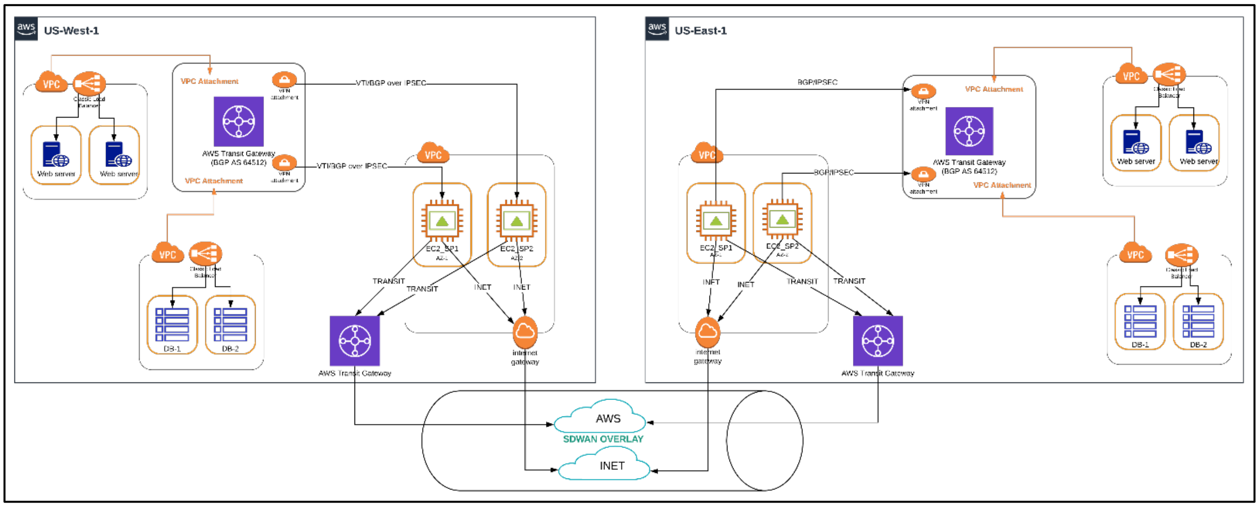
North-South SD-WAN Connectivity Between AWS Regions and Remote SD-WAN Sites

The EdgeConnect appliances deployed in AWS are simply another SD-WAN site and an extension of your on-premises SD-WAN fabric. These IaaS appliances are managed via Orchestrator, providing you with the same visibility, reliability, and automation that you are used to with the on-premises SD-WAN solution.

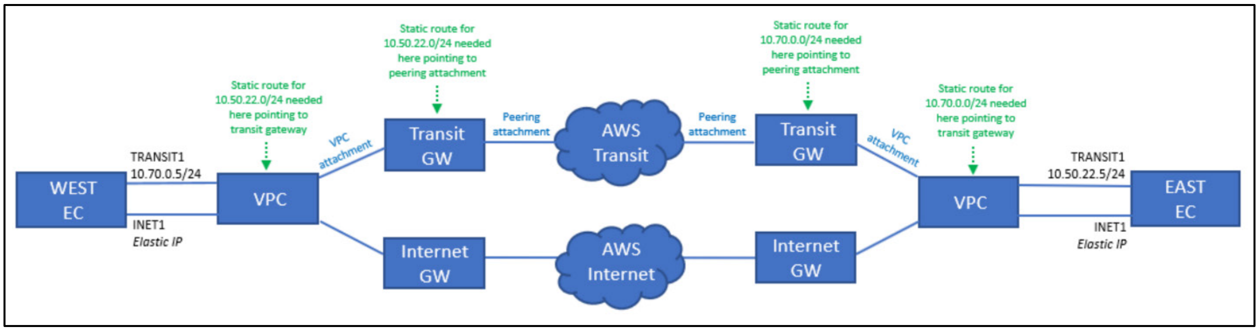


East-West SD-WAN Connectivity Between AWS Regions

SD-WAN overlay tunnel connectivity can be established between EdgeConnect appliances in different AWS regions via inter-region Transit Gateway peering, in addition to the public internet. The image below is a high-level design of inter-region AWS connectivity leveraging internet and AWS backbone (via Transit Gateway peering). Silver Peak's Business Intent Overlays logically bind the two underlay tunnels and employs path conditioning technology to make a best path determination on a per packet basis based on real-time loss, latency, and jitter metrics.

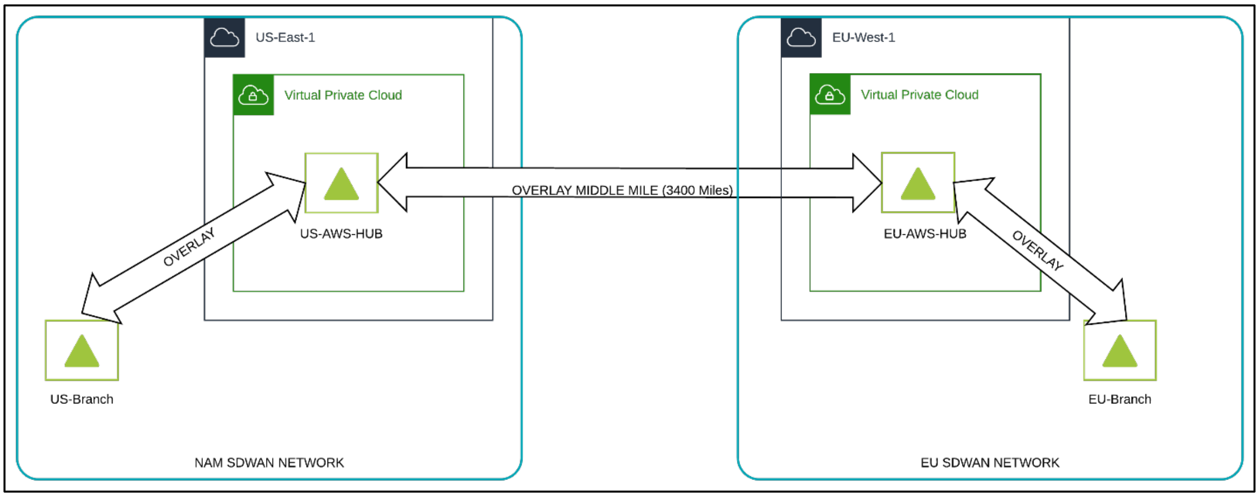


The image below illustrates logical (IP routing) underlay connectivity between EdgeConnect appliances in different regions over internet and Transit Gateways.


WEST EC
TRANSIT1 10.70.0.5/24
INET1 Elastic IP
Static route for 10.50.22.0/24 needed here pointing to transit gateway
VPC
VPC attachment
Static route for 10.50.22.0/24 needed here pointing to peering attachment
Transit GW
Peering attachment
AWS Transit
Peering attachment
Static route for 10.70.0.0/24 needed here pointing to peering attachment
Transit GW
VPC attachment
Static route for 10.70.0.0/24 needed here pointing to transit gateway
VPC
TRANSIT1 10.50.22.5/24
INET1 Elastic IP
EAST EC
Internet GW
AWS Internet
Internet GW

Branch-to-Branch SD-WAN Connectivity with AWS as Middle Mile

In a large enterprise network spanning multiple geographic regions, SD-WAN connectivity between branch offices in different continents can be enabled seamlessly while leveraging the AWS backbone as a middle mile.



In the diagram above, EdgeConnect IaaS appliances in EU-West-1 and US-East-1 regions are configured as regional hubs that act as route reflectors and redistribute learned spoke prefixes to hubs in other regions. The branch office in US and EMEA regions only establish SD-WAN tunnel connectivity to the nearest hub appliances in EU and US regions, leveraging the low latency AWS backbone connectivity between hub appliances for intercontinental traffic.