Direct Branch Multi-Cloud Connectivity

Background

Geographically distributed enterprises with many branch office locations and multi-cloud instances typically backhaul cloud-destined traffic to the data center at headquarters or to a regional hub site for advanced security inspection. The aggregated traffic is then directed to cloud Infrastructure-as-a-Service (IaaS) or Software-as-a-Service (SaaS) providers using a private high-speed link on the backend such as Microsoft Azure ExpressRoute and Amazon Web Services (AWS) Direct Connect for IaaS services and MPLS or business-grade broadband for SaaS, as shown in figure 1.

Cloud-native development and operations workflows enable enterprises to adopt a multi-cloud strategy. Cloud-native development enables organizations to build a portable software stack that is DevOps driven, free from vendor lock-in and capable of delivering a superior set of capabilities from a single cloud. This allows enterprises to evaluate and select the cloud services that have optimal workflows for certain applications. Often development teams want the freedom to choose an application and not be locked in to an underlying database, for example Oracle, that is specified by IT. The development team then has the freedom of choice to evaluate and select the best database tool that enables managing software development tasks.

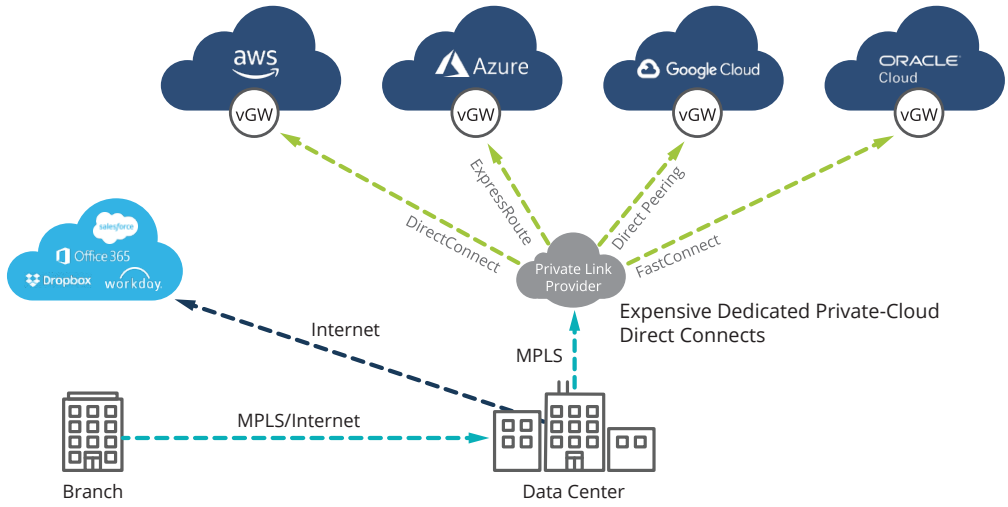

Figure 1: All branch-cloud traffic is backhauled to data center which impacts performance.

Increasingly, enterprises are adopting multi-cloud strategies to leverage multiple cloud platforms to support a range of SaaS and corporate workloads, each with varying software application requirements. A multi-cloud strategy can be implemented with a mix of public, private, hybrid and SaaS clouds to support the specific objectives of an enterprise.

These objectives can range from reducing IT spend on IT infrastructure, to accelerating the on-boarding and delivery of new applications to enterprise users, to improving the end user experience, and shifting spend from capex to opex budgets.

Perhaps the most attractive benefit of a multi-cloud strategy is the ability to avoid vendor lock-in. A multi-cloud strategy shifts the focus from the cloud provider to the enterprise — providing IT organizations with the flexibility to use any combination of cloud (IaaS or SaaS) providers to meet specific workload requirements.

CHALLENGES

Backhauling cloud-destined traffic from branch offices to the data center increases latency and degrades application performance, resulting in a poor quality of experience for users. Backhauling also increases the cost of procuring and managing dedicated high-speed MPLS or Ethernet transport services for traffic that could be sent directly from branch office sites to IaaS and SaaS providers over the internet. As enterprises migrate more workloads to public cloud infrastructure, and also leverage more SaaS, they have to address the complexities associated with managing multi-cloud connectivity requirements for IaaS, SaaS and private cloud-hosted applications. To summarize, key enterprise challenges include:

- Resolving poor end user quality of experience and impaired application performance resulting from increased latency due to backhauling application traffic to a data center for security inspection
- Added costs from relying on expensive, dedicated high bandwidth private MPLS circuits from data centers to virtual private clouds to support application traffic and the transfer of large files between on-premise data centers and IaaS providers
- Increased risk from manually configuring, managing, and optimizing the use of multiple cloud providers for different applications. If one web service host fails, the enterprise continues to operate with other platforms in a multi-cloud environment versus storing all data in one place.
- Exposing the organization to potential security threats by leveraging the internet itself for branch office to cloud connectivity, policing for personal applications (e.g. Facebook, Instagram, Netflix) and any unsanctioned "Shadow IT" cloud environments.

REQUIREMENTS

There are three requirements for Multi-cloud support that include:

1. Simplifying cloud connectivity: Connecting to each of the major public clouds can be complex and time consuming and the process to onboard applications for each provider is proprietary.
2. Policing of business applications: Supporting granular QoS and security policies can often be complicated for IT staff since different business units or groups may have differing policies.
3. Automating multi-cloud connectivity: Incorporating automation to provide the flexibility to easily scale applications horizontally across multiple cloud providers and selecting the best cloud provider for the right application.

SILVER PEAK SOLUTION AND BENEFITS

The Silver Peak Unity EdgeConnect™ SD-WAN edge platform addresses the challenges associated with backhauling cloud-destined traffic to the data center, thereby reducing the cost of bandwidth connectivity from the data center to cloud providers and reducing latency by enabling direct branch-cloud connectivity. The platform automates connectivity to cloud providers, greatly simplifying multi-cloud deployments.

There are several important capabilities of the EdgeConnect platform that enhance multi-cloud support:

- Business Intent Overlays: Intent-based application security, connectivity and control that easily supports simultaneous use of multiple cloud platforms, enabling IT to optimize the best cloud provider for a particular application (Fig 2.)
- Centralized orchestration of any IaaS and SaaS connectivity policies and services via Unity Orchestrator™ : A single intuitive graphical user interface (GUI) for orchestrating, changing and maintaining policies for multi-cloud hosted applications, ensuring consistent policies are enforced across the enterprise
- End-to-end micro-segmentation unified with a zone-based firewall ensures data is protected and complies with industry security regulations such as Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI DSS), Sarbanes-Oxley Act (SOX), the European Union GDPR, and the Federal Information Processing Standards (FIPS 140-2),
- Automate connectivity and increase application performance to Microsoft Azure
- Automate and simplify connectivity between AWS and branch locations via AWS Transit Gateway Network Manager (TGNM)
- Deliver the highest quality of user experience for Microsoft Office 365

Figure 2 highlights how an enterprise might leverage an EdgeConnect SD-WAN to enable direct connectivity to multiple cloud providers using the internet in place of dedicated private connections. Business Intent Overlays specify unique application policies that map the specific capabilities or economics of a cloud service to a given application.

For example, an IT organization prefers to use Google Cloud to host a real-time, mission-critical data analytics application with a QoS policy that's optimized for high quality, and that leverages WAN optimization. In contrast, the same company may host a widely used transaction processing application in AWS for economies of scale with a best-effort QoS policy but a stringent security policy for PCI compliance. Enterprises can also move application workloads across public cloud providers with EdgeConnect virtual appliance deployments in public cloud providers as shown in Figure 2, without disrupting the end users accessing cloud services from the branch.

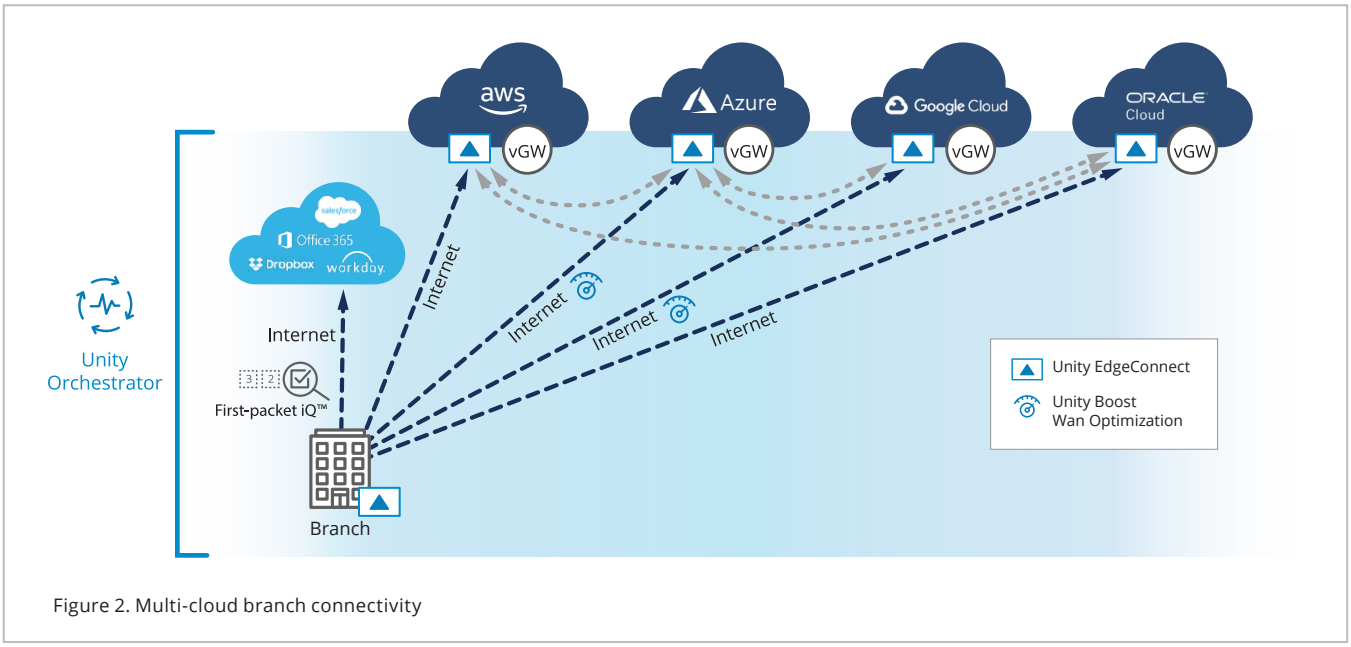

Figure 2. Multi-cloud branch connectivity

	Azure	aws	Google Cloud	ORACLE Cloud
Private Line	Express Route	Direct Connect	Cloud Interconnect	Fast Connect
IPSec VPN	VPN Gateway	TGW – Transit Gateway	Cloud VPN	DRG – Dynamic Routing Gateway
Automated IPSec VPN	Virtual WAN	Transit Gateway Network Manager	N/A	N/A
EdgeConnect "Bookended"	Yes	Yes	Yes	Yes

Figure 3. Public cloud access options

The following deployment examples listed in Figure 3 highlight the flexibility of connecting in one of four ways to each of the major public cloud providers.

EdgeConnect virtual instances (EC-V) can be easily deployed within any combination of four of the major public cloud providers, Amazon AWS, Google Cloud, Microsoft Azure and Oracle Cloud Infrastructure, via their respective marketplaces. The Orchestrator supports automated IPsec VPN tunnels between EdgeConnect sites and to each of the four major public cloud providers via the cloud provider's VPN gateway.

An EdgeConnect appliance deployed at each branch office enables seamless end-to-end connectivity to any of the public cloud providers by extending the SD-WAN fabric and deploying a virtual instance of EdgeConnect in any or all of the four public cloud providers. This "bookended" solution, row four in Figure 3, provides predictable application performance and the highest end user quality of experience.

In the bookended solution, enterprises can leverage the true benefits delivered by an EdgeConnect SD-WAN multi-cloud fabric. Enterprises can easily move workloads from one cloud provider to another, for example AWS to Azure using business intent overlays.

Some enterprises may be using additional Microsoft Azure and AWS services. Silver Peak has certified and automated IPsec VPN integrations with Microsoft's Azure vWAN network service offering and Amazon's AWS Transit Gateway Network Manager (AWS TGNM).

Microsoft Azure Virtual WAN (vWAN) simplifies branch connectivity across the global Microsoft network and the EdgeConnect SD-WAN edge platform enables automated and secure branch connectivity to Azure Virtual WAN; optimally routing traffic and minimizing latency when connecting to Azure-hosted workloads.

AWS customers that are planning to use AWS TGNM which is a network hub that enables customers to scale and manage connectivity between Amazon Virtual Private Clouds (VPCs) and their on-premise data centers can utilize EdgeConnect to integrate branch offices onto the AWS backbone. The AWS TGNM integration allows enterprises to centrally monitor, manage and automate connectivity between EdgeConnect branch deployments and AWS.

The new Microsoft Azure and AWS services can help existing Azure or AWS customers simplify and automate the branch network connectivity to their nearest Azure or AWS network edge or PoP.

MULTI-CLOUD FLEXIBILITY

Enterprises have many options for leveraging cloud-hosted applications and managing the diversity of public cloud provider choices. Silver Peak provides the most flexible multi-cloud options for enterprises to leverage SD-WAN connectivity while delivering the highest quality of experience for end users and IT. Silver Peak EdgeConnect:

- Supports diverse deployment options for SD-WAN in the four major public cloud providers, Amazon AWS, Google Cloud, Microsoft Azure and Oracle Cloud Infrastructure
- Certified support for Microsoft Azure vWAN, Microsoft Office 365 and AWS Transit Gateway Network Manager
- Enables cloud connectivity service flexibility with either MPLS or broadband underlay
- Flexibility to move application workloads from one cloud provider to another cloud provider without impacting branch-cloud connectivity

Secure, direct branch-multi-cloud connectivity is available today with the Silver Peak Unity EdgeConnect SD-WAN edge platform, enabling organizations to securely connect users directly from branch offices to multi-cloud services, enabling a better user experience and cost savings for the business.

Company Address

Silver Peak Systems, Inc
2860 De La Cruz Blvd.
Santa Clara, CA 95050

Phone & Fax

Phone: +1 888 598 7325
Local: +1 408 935 1800

Online

Email: info@silver-peak.com
Website: www.silver-peak.com

SP-UC-MULTI-CLOUD-CONNECTIVITY-041420