aruba
a Hewlett Packard Enterprise company

SOLUTION OVERVIEW

SD-WAN Multi-Cloud Connect

WHAT'S DRIVING THE NEED FOR IMPROVING SAAS AND IAAS PERFORMANCE?

COVID-19 has accelerated the investment in cloud-first plans as more enterprises adopt multi-cloud strategies, It is estimated that 92 percent of enterprises already have a multi-cloud strategy (source: Flexera 2021 State of the Cloud Report). This means branch offices will be accessing more distributed and cloud-based applications that may reside in more than one location and may include SaaS, IaaS, public and private cloud.

In this type of environment where SaaS and IaaS is an extension of the enterprise network, it becomes critical for the business to reach these applications by the most efficient and high-performance means.

According to IDC, small and medium size businesses (SMBs) plan to increase their number of IaaS providers from two to eight by 2021, and large enterprises plan to increase their number of IaaS providers from five to nine.

Many service providers offer private cloud connect services that securely connect their managed VPN customers to some of the IaaS and SaaS providers using the service provider's MPLS infrastructure. This address- es part of the cloud-enabled WAN, but it is expensive and operationally challenging for service providers to continue to maintain and support direct private MPLS connectivity to the increasing number of SaaS providers. The private cloud connect services also require that all of the remote branch offices are on-net subscribers to a service provider's MPLS VPN service.

Service providers are challenged to offer a managed service that can also deliver guaranteed application performance and availability to all of the SaaS cloud service providers, regardless of the underlay network.

SERVICE PROVIDER CHALLENGES

Unpredictable response times

Backhauling of SaaS applications to a MPLS PoP introduces undesirable latency limiting the ability to offer SLAs

Limited SaaS application traffic steering

Difficult to offer application-based QoS for off-net connections to SaaS providers

SaaS and IaaS direct connections are complex

Reduce complexity of offering public cloud on-ramp connectivity

Limited security service chains

Using public internet connections to SaaS without integrating security policies introduces risk

Integration into orchestration platforms

Ensuring consistent policies across cloud providers can be complex

SOLUTION

Predictable performance for any cloud-based application

Business intent overlay model enables service providers to manage connectivity policies to multiple SaaS and IaaS cloud providers

Automated connectivity of SD-WAN sites to the 4 major public cloud providers simplifying multi-cloud deployments

Optimize cloud connectivity

Dynamic traffic steering, tunnel bonding, SaaS optimization and First-packet iQ prioritize connectivity resources for SaaS applications

Enhance application availability

Path conditioning and WAN optimization ensure application performance during a brownout or blackout

Application segmentation

Flexibility to service chain SaaS applications with leading cloud-hosted network security service or solution

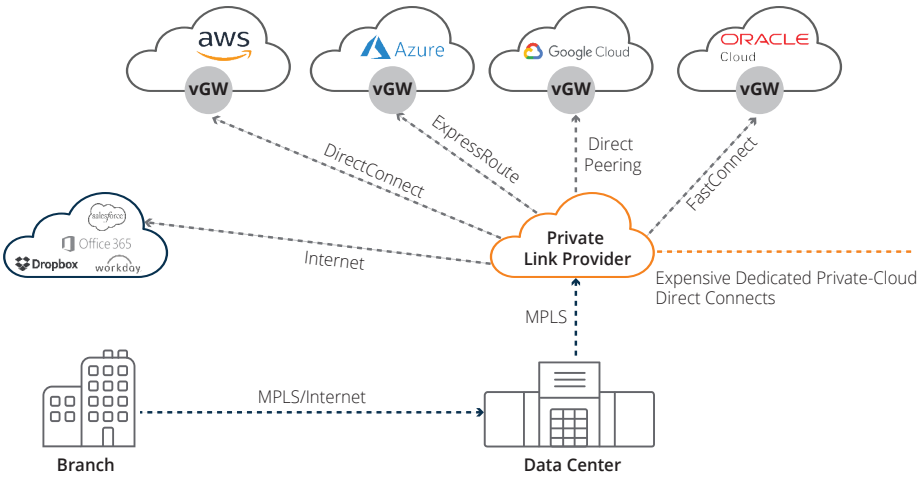

Figure 1. All branch-cloud traffic is backhauled to data center which impacts performance

SERVICE PROVIDER CHALLENGES

Service providers want to offer optimized managed SaaS and IaaS applications at branch offices and must address the following challenges:

- **Unpredictable response times –** Since SaaS and IaaS applications often reside in different locations and may change from time to time for different reasons, the response time in accessing them will vary unpredictably making it difficult to offer service level agreements (SLAs). Service providers that backhaul branch-IaaS traffic to the data center and then use MPLS to connect to cloud providers impacts performance and may introduce undesirable latency for cloud-hosted apps negatively affecting the end-user experience.
- **Limited SaaS application traffic steering –** Service providers typically are unable to classify traffic on an application-basis if the application is using another provider's WAN or broadband service before exiting the branch.
- **SaaS and IaaS direct connections are complex** – Establishing SaaS and IaaS direct connections are expensive and time consuming for service providers. The ability to offer private cloud connect services to new SaaS applications, such as salesforce.com (SFDC), may take as long as 6-12 months, depending on the negotiation to co-locate service provider connectivity to a particular SaaS vendor.
- **Limited security service chains –** Service providers offer separate managed security services that may be independent of their managed MPLS or hybrid WAN solutions. Security vulnerabilities may be exploited when accessing SaaS application services via the public internet.
- **Integration into Orchestration platforms –** Ensuring consistent policies across cloud applications that are hosted in different locations by cloud providers can be complex.

SERVICE PROVIDER REQUIREMENTS

As service providers assess their challenges, they need to evaluate and consider the following requirements for enabling cloud service connectivity:

- Built-in performance enhancement capabilities, especially when using third-party broadband or off-net MPLS services, that enable the ability to eliver SLAs for cloud connect applications
- Intelligent classification of SaaS and IaaS applications enabling dynamic traffic steering across the WAN on an application basis
- Consistent policy and unified management no matter where the application is located, SaaS/IaaS/headquarters-based data centers/ public cloud
- Orchestrated application-driven security policies regardless of application location, for example, an executive mobile laptop user can access a high priority SaaS application like SFDC connected via GuestWiFi, 4G, or MPLS network
- 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.

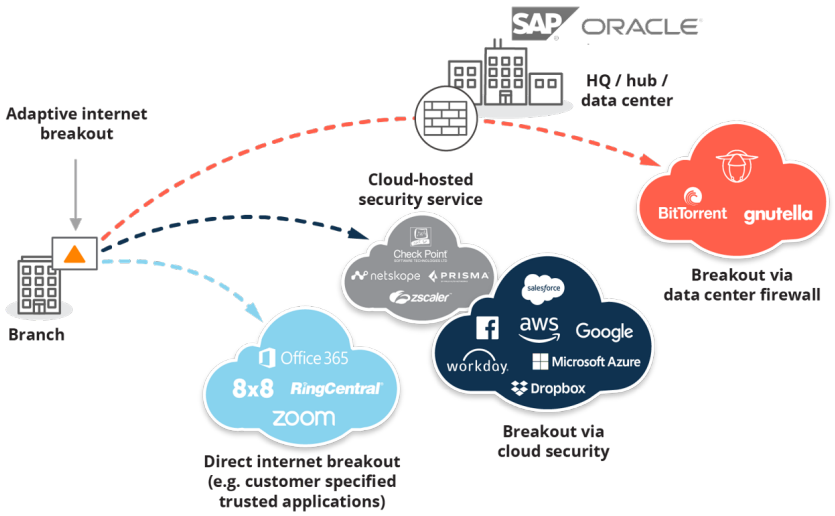

Figure 2. Intelligent Packet Steering

ARUBA EDGECONNECT INCREASES SAAS AND IAAS PERFORMANCE

Predictable Performance – Any Cloud, Any App, Anywhere

- The Aruba business intent overlay model enables service providers to manage connectivity policies to multiple SaaS and IaaS cloud providers, headquarters based data centers and branch offices resulting in consistent, unified policies across applications and predictable application performance.
- EdgeConnect intelligently steers traffic to the best performing path which may be over MPLS, broadband or a bonded overlay tunnel to SaaS and IaaS applications in real-time based on business policies. A managed service provider can optimize cloud application performance by utilizing First-packet iQ™, Local Internet Breakout and SaaS Optimization to support any regional, national or global application presence. This is shown in Figure 2.
- EdgeConnect™ has built-in features that enhance application performance and availability (path conditioning, tunnel bonding, Aruba Boost™ for WAN optimization, SaaS optimization) even during a transport outage or brownout for all applications, no matter where they are hosted.
- EdgeConnect enables service providers to include application segmentation to minimize the attack surface, and AES 256-bit encrypted connectivity between branches, IaaS and headquarters. Service providers that offer their own cloud-host- ed managed security offerings or cloud-hosted secure web gateway and cloud-hosted security solutions such as Zscaler, Checkpoint and Netskope can easily implement service chaining with EdgeConnect or pre-integrated solutions with our eco-system of leading security networking partners.

Manage Cloud-Connect Branches

- The Aruba Edge- Connect SD-WAN solution enables service providers to offer enterprises higher application and network performance as well as real-time visibility and analytics of SaaS applications as they migrate key business applications from on-premises infrastructure to IaaS and/or SaaS for increased business agility.
- Service providers can enable enterprise application workloads to easily move across public cloud providers with EdgeConnect virtual appliance deployments in public cloud providers as shown in Figure 3, without disrupting the end users accessing cloud services from the branch The following deployment examples listed in Figure 4 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.

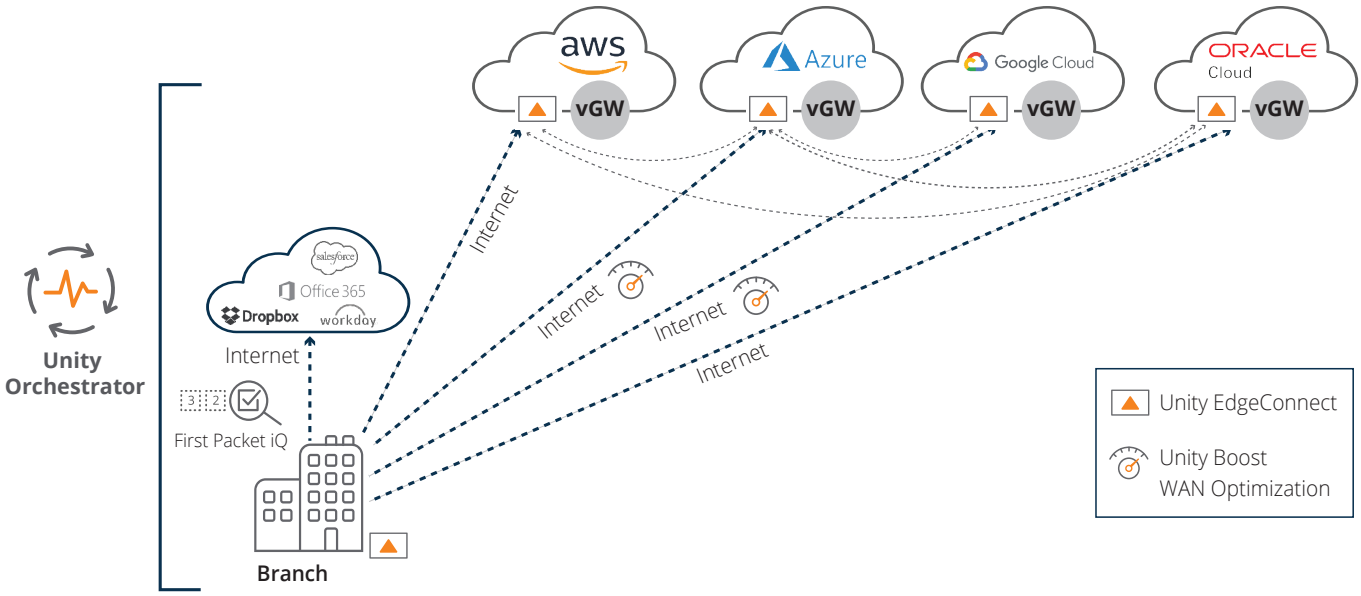

Figure 3. Multi-cloud branch connectivity

- 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 4, provides predictable application performance and the highest end user quality of experience.

	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 4. Public cloud access options

BENEFITS AND BUSINESS OUTCOMES

A managed Aruba EdgeConnect^{SP} SD-WAN solution provides enterprises and service providers with tangible benefits:

FOR ENTERPRISES, EDGECONNECT^{SP}:

- Assurance of SaaS and IaaS application performance and availability
- Enables secure cloud connectivity from any on-net or off-net branch location to IaaS and SaaS applications
- Supports diverse deployment options for SD-WAN in the four major public cloud providers, Amazon AWS, Google Cloud, Microsoft Azure and Oracle Cloud Infrastructure
- 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
- Reduces security risks dramatically with a multi-dimensional approach to keep IaaS and SaaS applications safe from vulnerabilities and threats

FOR SERVICE PROVIDERS, EDGECONNECT^{SP}:

- Increases the potential for MPLS cloud connect revenues for new SaaS applications, without requiring direct connect agreements, therefore improving time-to-service for branch-cloud connectivity
- Service providers can partner to offer integration services to additional Microsoft Azure and AWS services. Aruba 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), and Equinix Cloud Exchange (ECX) Fabric

SO_SD-WANCloudConnect_SK_120721 a00119357enw