SD-WAN Cloud Connect

SERVICE PROVIDER CHALLENGES

Unpredictable response times
Backhauling of SaaS applications to a 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 SLAs for both on-net and off-net services

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

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

What's Driving the Need for Improving SaaS and IaaS Performance?

It is estimated that 78 percent of workloads will be processed in cloud data centers by 2018 (source: IDC 2016). 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 2019, 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 addresses 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

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 SaaS traffic to the nearest MPLS point of presence (PoP) may introduce undesirable latency for cloud-hosted voice and video applications, 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.
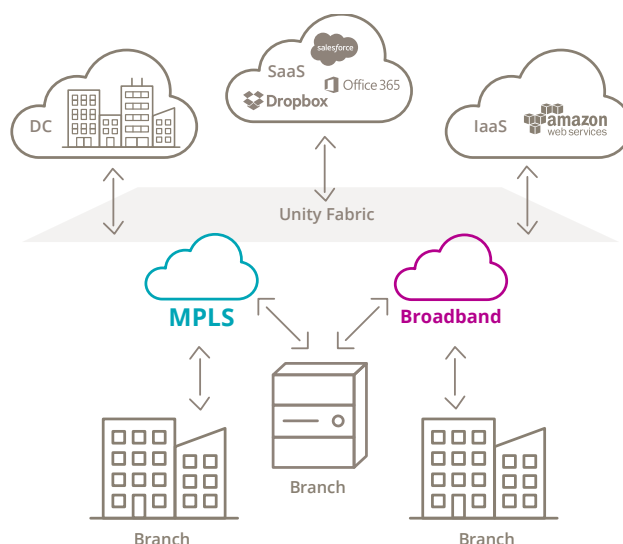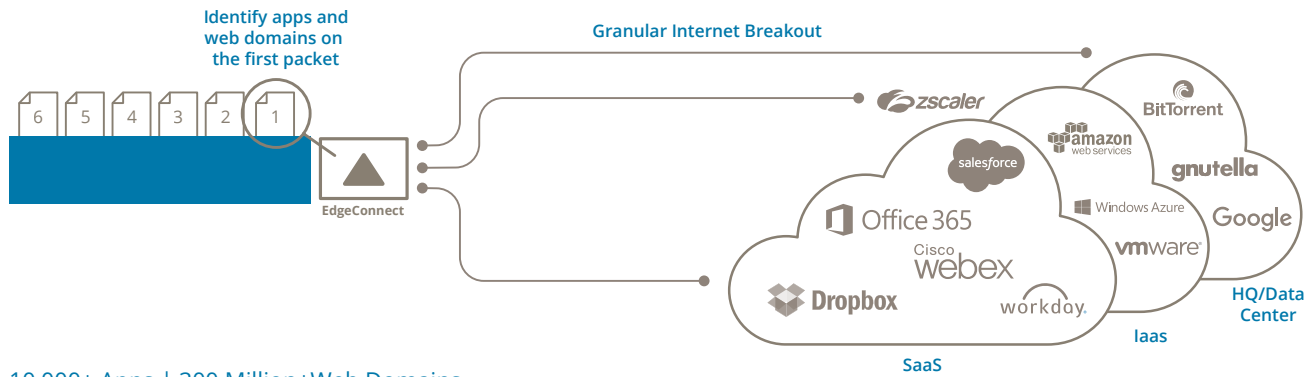

Figure 1: Hybrid Branch Network.

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 deliver 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

Identify apps and web domains on the first packet

Granular Internet Breakout

EdgeConnect

10,000+ Apps | 300 Million+Web Domains

zscaler

salesforce

Office 365

Cisco webex

Dropbox

amazon web services

Windows Azure

vmware

workday

BitTorrent

gnutella

Google

HQ/Data Center

IaaS

SaaS

Figure 2: Intelligent Packet Steering

Silver Peak Unity EdgeConnect^{SP} Solution Increases SaaS and IaaS Performance

Predictable Performance – Any Cloud, Any App, Anywhere

> The Silver Peak 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^{SP} 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™, 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, Unity Boost™ for WAN optimization, SaaS optimization) even during a transport outage or brownout for all applications, no matter where they are hosted as shown in Figure 3.

> 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-hosted managed security offerings or cloud-hosted secure web gateway solutions such as Zscaler can easily implement service chaining with EdgeConnect or pre-integrated solutions with our ecosystem of leading security networking partners.
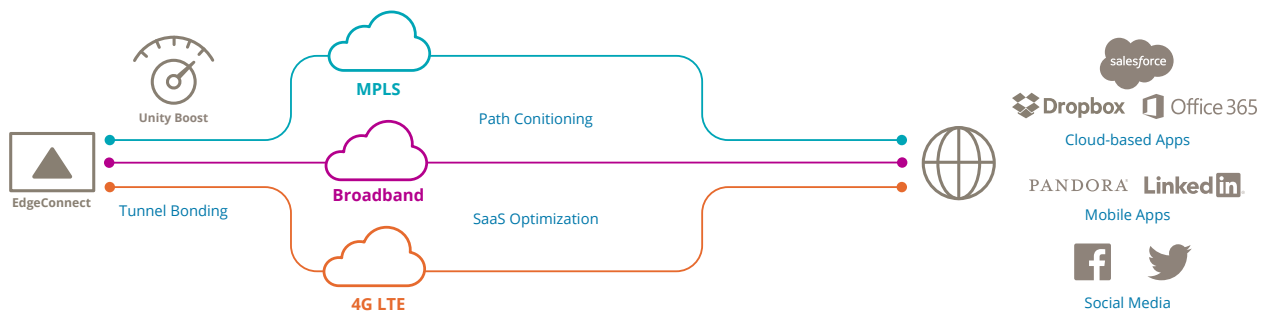

Unity Boost

EdgeConnect

Tunnel Bonding

MPLS

Broadband

4G LTE

Path Conitioning

SaaS Optimization

salesforce

Dropbox   Office 365

Cloud-based Apps

PANDORA   Linked in

Mobile Apps

Social Media

Figure 3: Path Conditioning & Tunnel Bonding
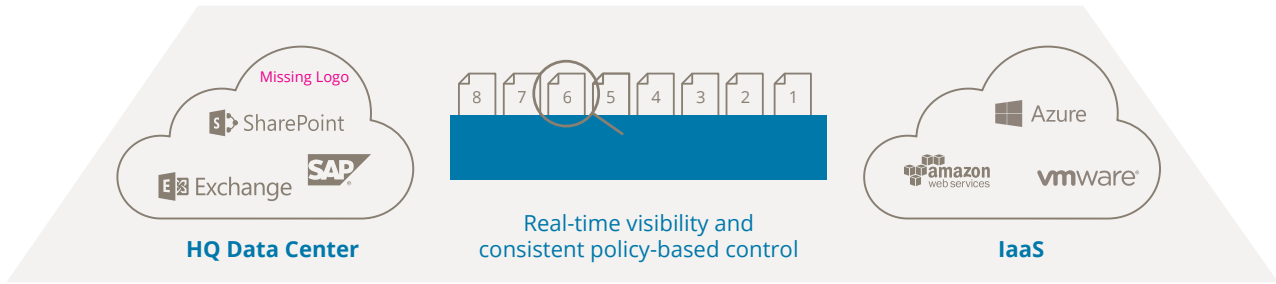
Figure 4: Application Visibility & Control

Manage Cloud-Connect Branches

> As shown in Figure 4, the Silver Peak Unity Edge-Connect^{SP} 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.

Benefits and Business Outcomes

A managed Silver Peak 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

> 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

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-SPUC-SD-WAN-CC-062718