Q-Balancer®

your trusted SD-WAN partner

Solution Brief: Q-Balancer Hybrid WAN

Augmenting Connectivity | Reducing Costs | Simplifying Network

Highlights

> Uninterrupted public and private cloud connectivity with WAN resiliency

> Faster application delivery with efficient utilization of WAN bandwidth

> High flexibility and scalability to avoid overprovision

> Assured delivery for business-critical applications as best path is always selected

> Lower CAPEX and OPEX

> Uncompromised data security

Overview

To gain more agility and faster response times, enterprises are rapidly moving many of their applications to the cloud. This means workers in branch offices will be accessing more distributed and cloud-based services that may be hosted in one or more locations via public and private clouds. Internet access play an important role as SaaS and IaaS are becoming part of the enterprise networks.

It is estimated by industry experts that as many as 2/3 of workloads will be moved to the cloud by 2021. To support this transition, enterprises increasingly are looking to leverage a hybrid WAN approach where lower cost, higher bandwidth broadband services are used in addition to MPLS services. This hybrid WAN approach helps in increasing WAN capacity and availability, leveraging existing WAN infrastructure, reducing total WAN cost, and improving application performance.

In this solution guide we'll take a look at the increasing challenges to legacy WAN, introduce the top benefits of Q-Balancer Hybrid-WAN, and brief how they are applied to WAN management and control. We will also discuss how Q-Balancer Hybrid-WAN ensures continuous availability and predictable application performance to keep productivity moving at optimal speed.

Challenges

In the past, legacy point-to-point WAN technologies were massively used for connections from branch offices to corporate networks, or to data centers separated by distance; these WAN technologies often required proprietary hardware or fixed circuits. However, enterprises today are demanding flexible, open, and cloud-based WAN technologies, rather than installing proprietary or specialized WAN technologies that often involve fixed circuits or proprietary hardware.

Unlike the point-to-point WAN technology, MPLS services are implemented without the requirements of adding proprietary hardware at your corporate network. MPLS uses communications via a cloud based network with each node connecting to the provider's cloud. This overlay technology makes the remote locations appear to

be directly connected to the corporate network or data center.

WAN outages occur for hours or even days per year despite MPLS service comes with very high SLAs. MPLS might be able to provide virtually unlimited bandwidth for enterprise's needs, yet that might be cost-prohibitive. Some locations might not be able to apply MPLS service as they are not within the MPLS provider's cloud. This means these locations have to find the alternatives.

MPLS redundancy can be done by adding a second MPLS connection as a backup. The secondary line takes over only when the primary MPLS line fails. However it's typically not instantaneous and it's almost never able to have a third party option. The followings are the challenges faced by enterprises using MPLS services:

Inefficient bandwidth utilization

In order to increase WAN reliability, some enterprises apply multiple Internet connections, yet the additional WAN link are often provisioned and deployed as separate links. This means that one may be an active link while the other stay idle as a backup. This might be good for redundancy, yet there is always a live link only for backup, resulting in inefficient utilization of bandwidth resources.

Unpredictable application performance

With legacy WAN, users may experience unreliable application performance due to network congestion and changing network conditions causing disruption and low productivity. Thus, enterprises need an intelligent solution that is able to identify, classify, and prioritize critical applications, and dynamically direct traffic across the WAN transport services. All cloud applications will then be sent down the best-possible path to the clouds, delivering high availability and total application performance.

Need for application-aware network

In a legacy distributed network, the corporate WAN backhauls all traffic from branch offices to headquarters or data centers. This imposes significant performance penalties to cloud-based application while directing traffic from branches to the cloud via data centers or headquarters. Real-time applications such as VoIP and video conferencing between branches and corporate network might also be

affected because the cloud traffic might saturate backhaul pipe and cause congestion. Some enterprises might consider to upgrade their MPLS bandwidth or apply for a second line; however the upgrade could overprovision expensive MPLS infrastructure just to accommodate the casual and unpredictable traffic spikes.

High cost

High MPLS bandwidth is costly and harder to achieve, and you'll need routers and circuits that cost a significant portion of your IT budget. Also, relying on incumbent vendors will usually mean paying a premium price to deliver the required services. To fix the issues, enterprises must have a right-sized branch solution that is able to deliver the required subset of service components at a budget friendly price, and to leverage public broadband transport other than costly WAN services.

VPN

As an alternative, many enterprises have successfully deployed site-to-site VPN over public cloud because it is a less expensive solution compared with MPLS. Enterprises will have to take the necessary steps to configure VPN on the terminating equipment. VPN can become complex to manage as business grows despite it is quick and easy to deploy. Data security is also one of the concerns as internal network and data could be exposed to the world if this is not configured correctly.

Site-to-site VPN tunnel will be disrupted should the primary WAN link fails, resulting in costly downtime because there is no backup route for it; traditional WAN failover cannot help with VPN resiliency. As business demand grows, enterprises will soon realize that it can be challenging to adding additional bandwidth to an existing platform. Businesses increasingly connect their branch networks for rapid deployment such as temporary sites and pop-up stores, all of which require to stay connected like a regular branch office on landlines. However, in most cases, there is no MPLS or even broadband services available for the deployments, not to mention link failover.

Requirements

An enterprise WAN composed of multiple transports is increasingly common today. Perhaps this WAN configuration already helped leverage both MPLS and broadband circuits at all business locations, and gave increased application performance by defining the usage for WAN transports based on the sources or types of traffic. However, it comes with some downsides, for example, possible inefficient use of bandwidth and session drop on failover. And the need to provide a secure WAN with high performance to enterprises still remains unresolved. To come up with a proper WAN solution to enterprises, the following need to be considered:

> Ability of identifying and classifying application
> Steering traffic across public and private clouds according to business intent policy
> Allowing user to enjoy transport-agnostic WAN connectivity among sites
> High WAN availability for remote offices
> Cost benefits of deploying broadband Internet and/or eliminating expensive MPLS services
> Fully utilizing all available bandwidth while delivering highly available and reliable application performance
> Security to protect the branch offices that use private and public WAN at the same time
> Real-time and historical visibility into issues impacting network or application performance.

Q-Balancer Hybrid-WAN

Q-Balancer Hybrid WAN enables shared use of both private and Internet circuits at all business locations. In Q-Balancer Hybrid WAN, an edge appliance is deployed at branch office, while a network controller appliance is deployed at head office. Both appliances is then connected with a single virtual leased line, which is made up of multiple overlay tunnels between them across both public and private WAN networks. Both head and branch office networks can send and receive traffic at the same time. Through the Q-Balancer Hybrid, enterprises enjoy the following benefits:

Flexible and Scalable – All WAN can be set active based on policy routing. Enterprise can flexibly employ broadband technologies to expand network capacity, while reserving the expensive private backhaul bandwidth for critical applications. Also, the capability of combining hybrid WAN networks enables the branches to access headquarters at a greater speeds than via a single link, and to increase bandwidth capacity by adding broadband lines when needed.

Best Path Is Always Selected – With Q-Balancer Hybrid WAN, business is able to direct business-critical applications to MPLS networks, while sending general traffic across the VPN overlay tunnels. Policies can be put in place to have latency-sensitive applications such as VoIP to get highest priority and be transmitted over the paths with the lowest packet loss and latency. The mechanism makes the critical applications run over the best possible paths with the highest quality.

MPLS Offload – Cloud applications can be sent to the public cloud via the aggregated broadband circuits, delivering the maximum possible capacity, while reserving the expensive private backhaul bandwidth for latency-sensitive or critical applications such as VoIP and Video.

Lower Upfront Investment – Money can be wasted on expensive MPLS bandwidth in order to cope with the unexpected and uncertain traffic spikes in a traditional hybrid network, where a MPLS line works as primary circuit and the other lines work as backup. With Q-Balancer Hybrid WAN, traffic can be sent over the combined capacity of WAN links. Besides, later on, bandwidth can be upgraded quickly by flexibly adding more private or public WAN links. This lowers capital expense for IT departments.

Data Security – Q-Balancer VPN includes 128- or 256-bit AES encryption to prevent data on public cloud from being read or modified. Plus, Q-Balancer is able to chop a VPN session into the packet level, and then sends them over multiple paths, and reassemble them at the receiving end. This makes hackers or intruders impossible to trap data and decrypt confidential information.

Model Recommendation

As an enterprise WAN solution, Q-Balancer is incorporated with WAN failover/ restoration, WAN load balancing, VPN resiliency/ bonding, and many enterprise-grade features such as Firewall, DHCP, routing protocols of OSPF & RIP, and end-to-end WAN QoS, all of which help enterprises take full advantage of hybrid WAN networks at corporate networks, data centers, branch offices, pop-up stores, temporary sites, and vehicle networks. All Q-Balancer models can perform as a network controller or an edge appliance as they all come with all-in-one feature set. The following is the recommendation for model selection:

Models	Targets	SD-WAN Placement
QB-2000	Enterprises / Data Center/ Campus	Controller
QB-500	Medium and Large-sized Enterprises	Controller
QB-300	Small and Medium-sized Enterprises	Controller / Edge
QB-150 / Mesh	Small/ Branch Offices/ Remote Offices	Edge
QB-Vehicle Routers	Vehicles/ Rolling Stock	Edge

Table 1: Model Recommendation

Use Cases

In this section we'll cover the common use cases for Q-Balancer Hybrid-WAN as follows:

> MPLS Bridging Improves Legacy WAN

> Hybrid WAN Assures Cloud Availability and Application Performance

Use Case #1: MPLS Bridging Improves Legacy WAN

Challenges:

> Wasting money as one of links is set standby

> Inefficient bandwidth utilization

> Possible overprovisioning

As illustrated in Figure 1 below, a multi-site enterprise has three locations that are connected with MPLS lines, and deployed Q-Balancer appliances at all three locations respectively. The enterprise then added a second MPLS line from different carriers at each location, and now tries to bridge the services for higher WAN reliability and capacity.

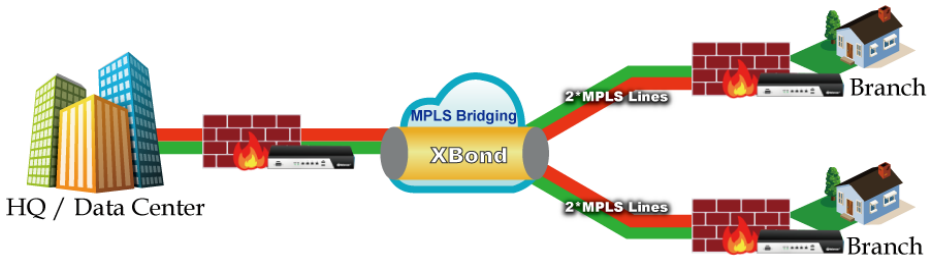

Figure 1: MPLS Bridging Improves Legacy WAN

In this configuration, in case one of MPLS lines fails, saying red line, traffic will be seamlessly routed down the remaining active path (green line) without complex configuration on routing protocols or manual intervention. Furthermore, through Q-Balancer bonding technology, these two MPLS lines (red and green) will be aggregated into a virtual big pipe, which provide higher speed of backhaul. Based on this principle, for higher WAN reliability and capacity, enterprise can flexibly add more MPLS lines from any other providers. The ability of bridging MPLS lines enables enterprises to benefit from:

Full use of bandwidth

Q-Balancer Hybrid-WAN helps fully utilize all available bandwidth, and delivers the highest network performance by setting MPLS lines to run active-active rather than active-standby.

WAN reliability

With Q-Balancer Hybrid-WAN, enterprise is no longer dependent on single network provider. In case a failure or quality issue occurs on the primary line, traffic will automatically be diverted to the remaining active path; link failover switching is done instantly without a session drop out.

Best path is always selected

With Q-Balancer, all MPLS lines are constantly monitored and measured for packet loss, latency, jitter, and availability. In case a quality issue occurs on WAN, traffic will be routed down the better-performing or least-loaded paths, preventing any negative impact on critical applications.

No overprovisioning

Enterprises will not overprovision expensive MPLS bandwidth to accommodate unpredictable traffic spikes in this deployment because bandwidth will only be incrementally added when the actual demands is confirmed.

Use Case #2: Hybrid WAN Assures Cloud Availability and Application Performance

Challenges:

> Inefficient bandwidth utilization
> Need for traffic steering
> Unpredictable performance
> Security risk
> Manual provisioning

As depicted in Figure 2, Q-Balancer appliances are respectively deployed at both HQ and branch office. The public WANs (blue and green) in this case are transport agnostic, and private backhaul is with MPLS line (red). Cloud-based applications from branch office are directed to the cloud via public WANs(blue and green) without going

through the private WAN (red). Backhaul bandwidth is reserved for site-to-site applications because Internet-bound communications is offloaded from MPLS line.

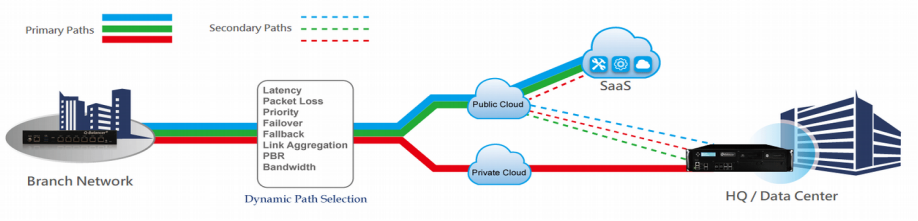

Figure 2: Hybrid WAN Assures Cloud Availability and Application Performance

Q-Balancer Hybrid-WAN enables the distributed enterprises to benefit from:

Higher WAN reliability

In case a failure or quality issue occurs on the MPLS line, site-to-site traffic will automatically be routed down the available broadband lines; link failover for the MPLS backhaul is done instantly without a session drop out.

Assurance of cloud availability and application performance

Q-Balancer harnesses public and private clouds, and packet-based load balancing can still be configured for critical applications across multiple WANs to achieve higher availability and performance.

Increased backhaul availability for critical applications

As illustrated in Figure 2, most SaaS applications will be routed out to the cloud via the public WANs (blue and green) based on predefined policy as Q-Balancer dynamically and intelligently steers traffic based on the applications. This increases the backhaul availability and the performance for site-to-site applications.

Increased control of all applications

With the ability of applications identifying and delivering, Q-Balancer Hybrid-WAN enables policy-based traffic steering for the applications hosted both in the cloud and at enterprise's data center.

More business agility

Q-Balancer Hybrid-WAN enables multi-office enterprises to

incrementally expand WAN bandwidth and flexibly add branch offices, allowing enterprises to respond rapidly and flexibly to the demands.

QoS

QoS rules can be enforced on both private and public WANs, and so business-critical applications receive priority in case conflict occurs.

Reduced cost

With Q-Balancer Hybrid-WAN, enterprises can now augment their WANs or even replace MPLS services with low-cost internet services, and the WAN cost can lowered by up to 90%.

Q-BALANCER CO., LTD.

3F10, No. 5, Sec. 5, Xinyi Road

Taipei, Taiwan 11011

Tel: +886-2-87808518

sales@creek.com.tw | www.creek.com.tw

About Q-BALANCER

Q-BALANCER Company is dedicated to developing the highly innovative Multi-WAN and Hybrid-WAN solutions. Since inception we aim to build a WAN solution for enterprises that is able to deliver higher WAN reliability at lower cost. Through cooperation with our partners, Q-Balancer has been successfully deployed across thousands of enterprises in over 20 countries.