Q-Balancer®

Your trusted IT partner

Solution Brief: Broadband Bonding for Enterprise Networks

Unbreakable Continuity via Intelligent WAN Load Balancing

Connectivity Augmentation | Cost Reduction | Application Delivery | Network Simplification

Highlights

> Increased network performance through WAN bonding

> Minimal network downtime with network redundancy

> Augmented site-to-site VPN connectivity and performance with VPN bonding

> Improved reliability and response for corporate-hosted applications

> Improved productivity through granular bandwidth control

> Cost saving by leveraging low-cost broadband WANs

> Increased WAN scalability

> Reliable Internet connectivity anywhere

> Service provider independence

Internet plays an important role in today's business operation, and the number of businesses relying on Internet has been growing quickly. Businesses enjoy the convenience and advantage of harnessing internet today. However, poor Internet connectivity can cause less productivity and loss of business opportunity, and even damage the business reputation.

A multi-WAN strategy, using two or more WAN services, is getting applicable and common to enterprises. Initially, many organizations pursued a multi-WAN strategy because they were uncertain about WAN reliability. Multi-WAN was, and still is, seen as a way to prevent downtime caused by a single point of failure on WAN. Multi-WAN deployments were initially being driven by network redundancy, but now they are also driven by the growing demand for high-speed Internet connectivity. Below are the major challenges to enterprise Internet connectivity:

Challenges

> Downtime caused by WAN outages

A network with single WAN link or multiple WAN links from a single service provider will limit the WAN reliability and performance due to single source. Some businesses may apply a secondary WAN link from the other provider to achieve WAN redundancy with manual intervention when/if primary link goes down, yet this cannot be easily managed as WAN outage is so unpredictable.

Some firewalls offer an all-or-nothing failover mechanism, in which when/if primary WAN link goes down, and then all traffic is automatically routed down the remaining active paths. This is great for redundancy, however there are always live links only for backup.

> Corporate-hosted applications

In an enterprise network, a DNS server hosts and serves data for single or multiple domains; when the DNS server receives DNS requests for domain name resolution, it then resolves and returns IP addresses to the requests. However, DNS does not check the possible outages or the status on WAN when replying DNS requests. It always

returns the same IP set for domain name resolution to the DNS requests despite the primary WAN is already down or slow.

Corporate-hosted application servers like Mail or Web servers, which sit on LAN, serve numerous incoming requests via DNS mechanism. These servers are definitely important to enterprises operations, but they can be sometimes unavailable to external requests due to either link failure or congestion.

> Not enough bandwidth

Business-critical applications are sometimes negatively impacted by the limited bandwidth. Adding a WAN connection, which comes with high performance and reliability at a reasonable price, is always welcomed and needed by enterprises. However, increasing bandwidth utilization efficiency for maximum investment becomes another issue after having added more bandwidth.

> Inefficient bandwidth utilization

Enterprise network today must be able to efficiently utilize bandwidth resources as more online applications have emerged. Critical applications like voice or video may be granted priority so that the quality of these applications will be assured, while the non-business related applications will be limited in order to prevent them from over consuming the bandwidth resource.

> Unpredictable application performance

Business may experience unreliable application performance when using broadband lines due to congestion and changing network conditions, causing disruption and low productivity. Today, enterprise WAN solutions must be able to monitor WAN link status, dynamically direct critical applications to best path, and divert traffic from the congested or faulty path(s).

> Lack of business-oriented scalability

As business grows, more bandwidth and branch offices will be added to meet the increasing demand. While planning on WAN infrastructure, enterprise needs a WAN solution that enables them to flexibly add WAN links without limiting the future growth or over

provisioning for the short term.

> Site-to-site network connectivity

Virtual Private Network (VPN) is a widely deployed technology for business to build a secure communication over an IP network between two geographically separate sites. Data security and integrity will be enhanced when VPN solution is in place. It has become one of the most common tools for data security as there is a greater need for encrypting communication than ever before.

IPSec VPN tunnels destined for the same remote network can only be established over a single interface. Should the circuit fails, there is no way to keep the continuity for the LAN-to-LAN connectivity.

Besides, critical applications such as VoIP or video conferencing are frequently transmitted in site-to-site networks. Besides, when/if more bandwidth is required to accommodate growing demand, this is possibly difficult to achieve through simply adding more WAN links and applying NAT-based WAN load balancing.

> Pop-up stores and temporary sites

Pop-up stores and temporary sites have the need to stay connected to the cloud. However, broadband or MPLS services might be limited or not be available for those deployments, not to mention network redundancy. Thanks to the proliferation of 4G LTE networks, Internet connectivity for those deployments is achievable today without long waiting or paying extra. However providing a secure and reliable WAN connectivity for those deployments still remain challenges due to unpredictable wireless connectivity or harsh environment.

Solutions

As an intelligent multi-WAN load balancing solution for enterprise, Q-Balancer is incorporated with network features such as Out Load Balancing, Inbound Load Balancing, VPN Bonding, IPSec VPN Tunnel Termination & Load Balancing, 4G LTE Bonding, and Multi-Path QoS. The solution is designed to help corporate, data centers, and branch offices take full advantage of WAN connections. Below are the major challenges to enterprise WAN connectivity:

> Outbound Load Balancing

The corporate WAN is an essential part of daily business operations for many organizations. It plays a key role in corporate teamwork and communication, and offers external access to corporate resources. Outbound Load Balancing helps business build a reliable and fast Internet connectivity in a cost-effective way by utilizing multiple Internet links or, in some cases, hybrid links, and it is transport agnostic, either private or public.

Figure 1: Outbound Load Balancing

The solution also helps enterprises achieve higher bandwidth capacity and greater WAN efficiency. A variety of algorithms provided by the Q-Balancer will find the most active and responsive link when new requests arise. The feature intelligently aggregates multiple Internet connections to speed up the application delivery.

The ability to harness legacy and newly added WAN links enables enterprises to incrementally add bandwidth as the business grows. The inbuilt path-monitoring constantly gauges the status of all WAN links. Based on the measured result and the selected algorithm, WAN load balancing efficiently distributes traffic across available paths. Accelerated access and network continuity can be achieved as best performing and least-loaded links are always selected when new requests come up. WAN load balancing enables business customers to enjoy enterprise-grade WAN without expensive network upgrade.

> Inbound Load Balancing

Each host connected to the Internet has a unique IP address, and so other devices can find it via the IP address. In reality, mostly users access online information through human-readable domain names, like google.com or yahoo.com rather than IP address. The Domain Name Systems (DNS) is like the phonebook of the Internet. When a DNS request is received by a DNS server, the DNS server then returns

with the IP address of the domain requested initially. DNS translates domain names to IP addresses, while web browsers interact through IP addresses; therefore, browsers can load the Internet resources.

However, this mechanism might involve some issues. The external requests might not be able to access the server when/if the primary WAN link goes down. Simultaneously using multiple IP address provided by the ISP connections can possibly be a better way. The hosted services then appear as different IP addresses to the external DNS requests. But DNS does not check for WAN outages or status, and so it might return the DNS request with an IP address from the faulty or congested WAN link.

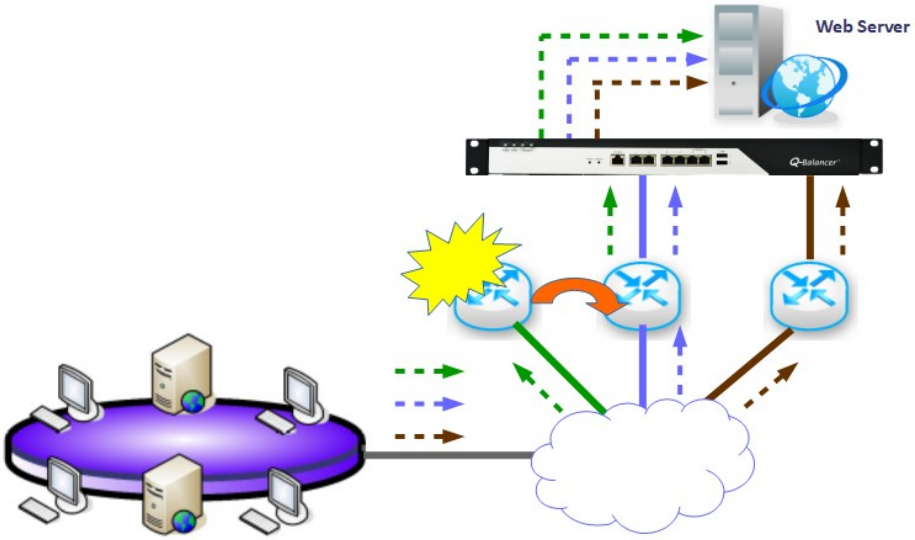

Figure 2: Inbound Load Balancing

With the inbuilt mechanism of Inbound Load Balancing, the incoming requests will always be directed to the internal servers via the available uplinks, and be able to avoid the faulty or congested WAN links. The solution works as a DNS server and has the ability to check the link status whenever replying IP resolution to the DNS requests. Given this ability, content delivery to the incoming requests will be responsive, and total uplink utilization will be increased. The Q-Balancer Inbound Load Balancing is the best-in-class solutions used by heavy-traffic enterprises to deliver their content to their customers quickly, reliably, and securely.

> VPN Bonding & Failover

Critical applications such as VoIP or Video Conferencing are frequently transmitted in site-to-site VPN networks. For multi-office enterprises, site-to-site VPN connectivity with enough bandwidth and high reliability is a key to success. However, VPN network is established based on a single Internet circuit; should the circuit fails, there is no way to keep the connectivity. Besides, when bandwidth demand grows, adding WAN links for more bandwidth is technically difficult to achieve. This could mean expensive upgrades or change for legacy WAN infrastructure.

Site-to-Site VPN Bonding

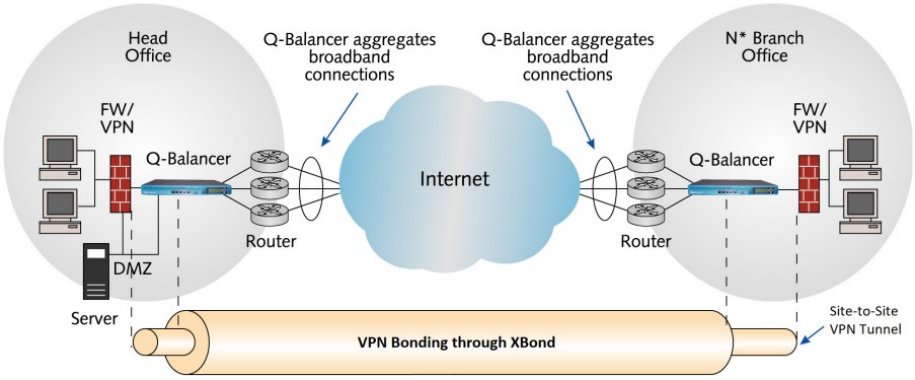

Figure 3: VPN Bonding

The inbuilt XBond (bandwidth bonding technology) is able to deliver maximum performance for VPN connectivity. It has the ability to spread VPN traffic by packet across multiple Internet connections, and this make VPN Bonding goes further than session-level WAN load balancing. The Q-Balancer VPN Bonding provides a faster, more reliable and secure connection for all the online activities, from browsing, video streaming and large file transfers. The Q-Balancer VPN bonding is auto-provisioned, and so can be configured automatically in an effort to reduce operational and overhead costs.

Once the VPN bonding is properly configured on the appliances at both ends, the appliances will automatically keep VPN connectivity up and running. Therefore, the appliances will divert VPN traffic down the remaining active paths in the event of WAN outage, and send VPN traffic through again once the Internet connection restores from outage.

> IPSec VPN Tunnels Termination and Load Balancing

Virtual Private Network (VPN) is a widely deployed technology for multi-office business to build a secure communication over an IP network between the geographically separate sites. It has become one of the most common tools for data security as there is a greater need for encrypting communication than ever before.

IPSec VPN tunnel are traditionally established based on a single Internet circuit. Should the circuit fails, there is no way to keep the connectivity for the LAN-to-LAN access. In addition, if more bandwidth is required to accommodate the growing demand, this is possibly difficult to achieve through traditional NAT-based link load balancing technology.

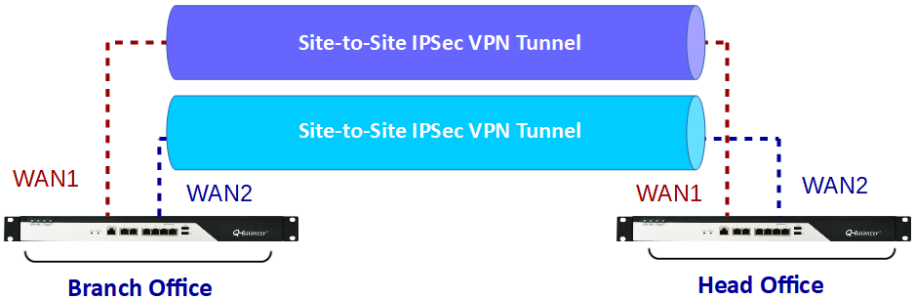

Figure 4: IPSec VPN Tunnels Termination and Load Balancing

The inbuilt feature of multi-path IPSec VPN Termination and Load Balancing enables LAN-to-LAN traffic to be securely distributed across multiple WAN links, and it works in conjunction with policy-based routing. This increases the flexibility of traffic control and routing decisions in site-to-site network deployments.

Through the inbuilt multi-path IPSec VPN Termination and Load Balancing, it is now technically possible to form and send LAN-to-LAN traffic over multiple IPSec VPN tunnels. The IPSec VPN tunnels terminated on the Q-Balancer appliances can be either standard IPSec or the Q-Balancer proprietary IPSec VPN tunnels.

> IPsec VPN Third-Party Compatibility

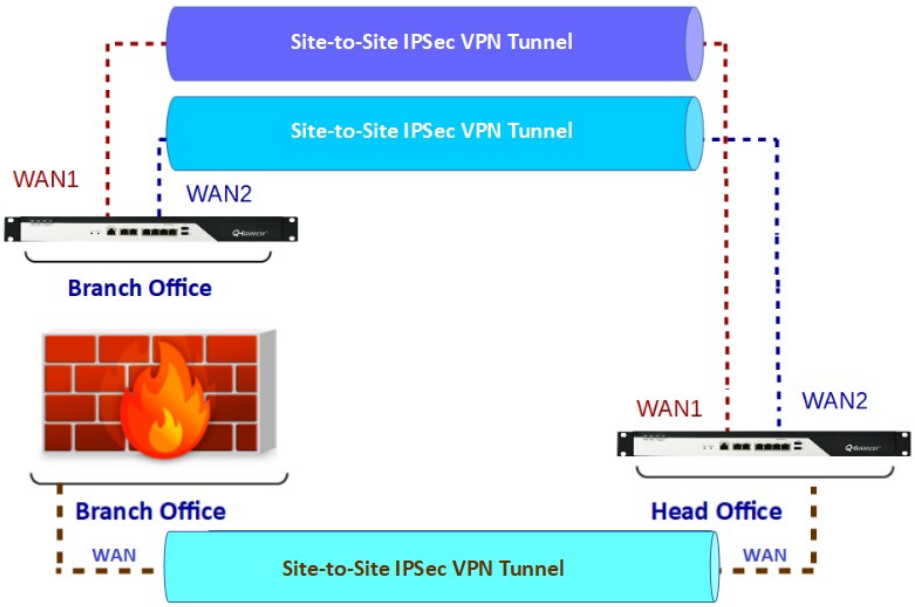

Figure 5: IPSsec VPN Tunnel Termination on Q-Balancer & Firewall

Any VPN device which supports standard IPSec may be connected to a Q-Balancer appliance running IPSec VPN. In addition, multiple IPSec tunnels can be established with third-party VPN devices, and meanwhile multiple IPSec tunnels can be built with other Q-Balancer appliances running IPSec VPN.

> 4G LTE WAN Bonding

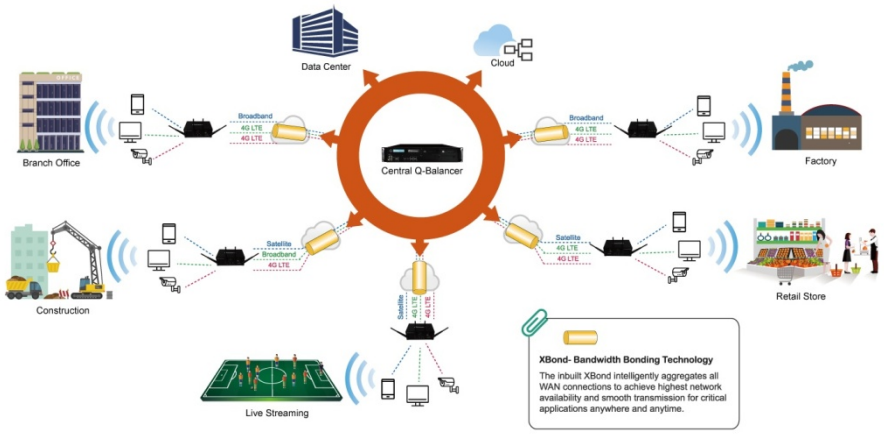

Figure 6: 4G LTE Bonding for pop-up store and temporary sites

By deploying the Q-Balancer appliance with multiple 4G LTE lines, pop-up stores and temporary sites now are able to instantly deploy Internet connectivity whenever needed. By taking on multiple links

from multiple providers, the Q-Balancer solution ensures those temporary deployments to keep on conducting transactions with customers even if one of Internet lines went down, and therefore customer services would not suffer from WAN outage.

> Multi-Path QoS

When the response of mission-critical applications becomes slow because of limited bandwidth resource, businesses would have to invest more in bandwidth upgrade. However, more bandwidth means paying more to service providers monthly. The Q-Balancer Quality of Service (QoS) gives enterprises granular control over the bandwidth utilization. With QoS you can prioritize network traffic based on addresses, ports or services.

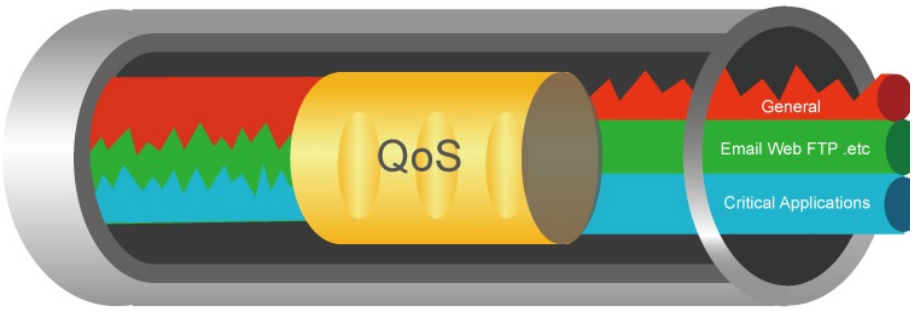

Figure 7: Quality of Service

The Q-Balancer Multi-Path QoS enables enterprises to throttle traffic flows, and so non-critical applications will not overuse the bandwidth allocated. The issues of network performance can be sorted or mitigated by allocating enough bandwidth to business-critical applications. Other than bandwidth allocation, the Multi-Path QoS has the ability to instantly prioritize critical applications. For example, set lower priorities to non-critical applications, while assign higher priorities to critical applications. This enables critical applications to get enough bandwidth they needs to cross the network unhindered by the business-unrelated or non-critical traffic.

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 US

Q-BALANCER Company is a software company that builds specialized and high-performance network appliances for enterprises. Our solutions accelerate digital economy, reduce connectivity costs, augment traditional WAN network, and optimize delivery for next-generation applications. Since inception our solutions have been successfully deployed across thousands of customer networks in over 20 countries through cooperation with the channel partners.