Q-Balancer®

SOLUTION
BRIEF FOR
SMEs

Cost-Effective Hybrid Multi-WAN Solution for SMEs

Internet plays an important role in business operation today, and there is an increasing number of companies that rely on Internet. 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 connections, 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.

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 that case, when/if primary WAN link goes down, 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 a typical DNS deployment, a DNS server hosts and serves data for the domain(s); when an incoming DNS request for, e.g. web services appears, DNS server then replies it with IP resolution for the hosted server. This mechanism is designed for translating domain name into IP address, while it does not check if there are any network outages or congestion when replying. Thus, in case the primary WAN link fails, incoming requests might not be able to access hosted service(s) with the IP address resolved by DNS.

> Insufficient Bandwidth Resources

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

> Landline is not viable in some areas

Construction Site or pop-up stores may find landline service is not always available, or takes long time for installation or cost-prohibitive. With many major enterprises operating numerous branch locations across the globe and expanding into new territories, those limits are unacceptable and should be overcome in business world today.

> 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.

> Impact of Packet Loss

Transmission Control Protocol (TCP) is a reliable transport protocol that has been tuned to perform well in networks where packet losses occur mostly because of congestion. In the event of packet loss, TCP resends any segments that have not been acknowledged. TCP can help networks recover from packet loss, however, retransmitting missing packets causes a noticeable decrease in throughput across the networks.

Packet loss will also cause TCP to assume that the network is suffering from congestion, which will trigger its built-in congestion avoidance algorithms. The end stations then exponentially back off the rate of their transmissions, and then slowly increase their rate of transmissions over time. While this helps retain the data integrity, it also reduces the rate of transmissions.

> Unpredictable Application Performance

Business may sometimes experience unreliable application performance due to congestion or latency, causing service disruption and low productivity. WAN solutions for enterprises today must be able to cope with the changing network conditions and dynamically direct critical applications to best path.

> 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 their networks for the short term.

> Site-to-Site VPN Connectivity

Virtual Private Network (VPN) is a widely deployed technology for business to build a secure connection between two geographically separate sites. Critical applications such as VoIP or video conferencing or VDI are frequently transmitted in site-to-site networks. VPN is established based on a single Internet circuit; should the circuit fails, there is no way to keep the connectivity. When/if more bandwidth is required to accommodate growing demand, this is possibly difficult to achieve.

Solutions

As an intelligent multi-WAN load balancing solution for enterprise, Q-Balancer is incorporated with comprehensive 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 Internet.

> WAN Failover

Network downtime means user frustration, lost productivity and decreased revenue. Even a short interruption can have significant impacts such as dropped VoIP calls or disrupted application sessions. The major tasks for WAN failover is to help enterprise build a network that never fails. WAN failover ensures enterprise an unbreakable connectivity in almost every situation.

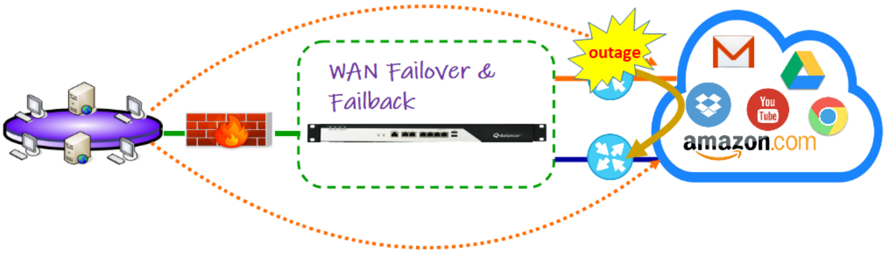

Figure 1: WAN Failover

> Outbound Load Balancing

Outbound load balancing helps business build a high-speed Internet connectivity in a cost-effective way by utilizing multiple Internet links from multiple providers. Outbound load balancing works in conjunction with the inbuilt path-monitoring, which constantly gauges the status of all WAN links. Based on the measured result and the selected algorithm, outbound load balancing efficiently distributes traffic across multiple paths. A variety of algorithms provided will help find the best-performing or responsive Internet connections when new requests arise. Q-Balancer outbound load balancing enables business to enjoy enterprise-grade WAN without paying for expensive network services.

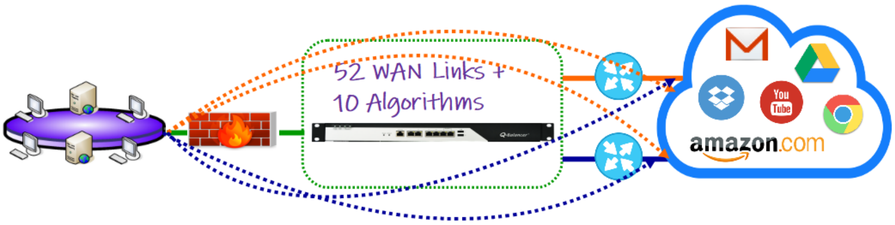

Figure 2: Outbound Load Balancing

> Inbound Failover & Load Balancing

Q-Balancer inbound load balancing works as a DNS server and has the ability to check the link status in realtime whenever replying the incoming DNS requests. Given this ability, content delivery to the incoming requests will be responsive, and overall efficiency of uplink bandwidth will be increased. With Q-Balancer Inbound Load Balancing, the incoming requests will always be directed to the internal servers via the active paths, and be able to avoid WAN outages and congestion.

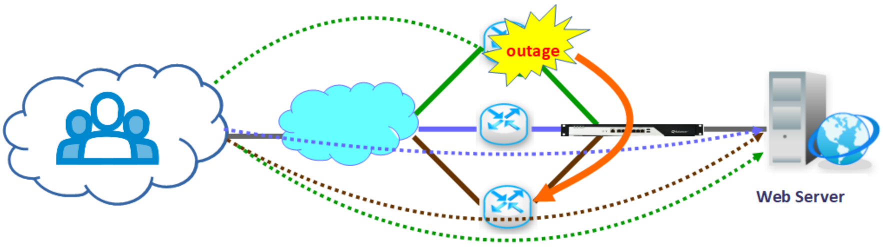

Figure 3: Inbound Load Balancing & Failover

> VPN Failover & Bonding

Q-Balancer has the ability to improve VPN reliability. Once Q-Balancer appliances are in place at both ends and properly configured, they will be able to divert VPN traffic to the remaining active paths in the event of WAN outage, and send VPN traffic through again once the Internet connection failback from outage.

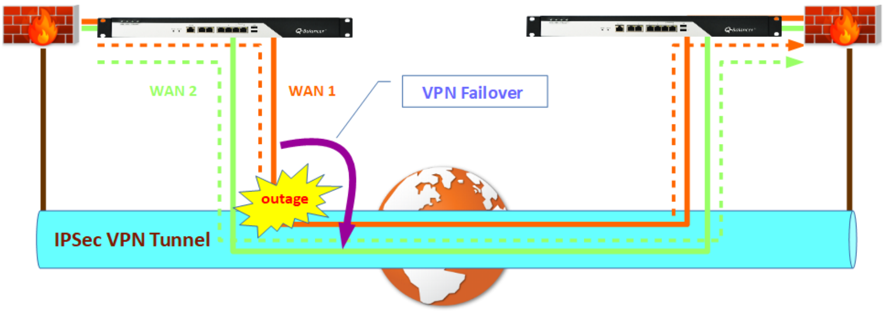

Figure 4: VPN Failover

When bandwidth demand grows, adding Internet connections for VPN, like NAT-based link load balancing does, is technically difficult to achieve. This could mean expensive upgrades or change for legacy WAN infrastructure. The inbuilt XBond (bandwidth bonding technology) is able to deliver maximum performance for VPN connection with its ability to spread the packets of VPN traffic across multiple Internet circuits. This makes VPN bonding go further than session-level load balancing. Q-Balancer VPN Bonding provides a fast, reliable, and secure connectivity for all the online activities, from browsing, video streaming and large file transfer.

The configuration of VPN bonding in Q-Balancer is a time-saving design, and so its provisioning can be done in a minimal effort to reduce operational and overhead costs.

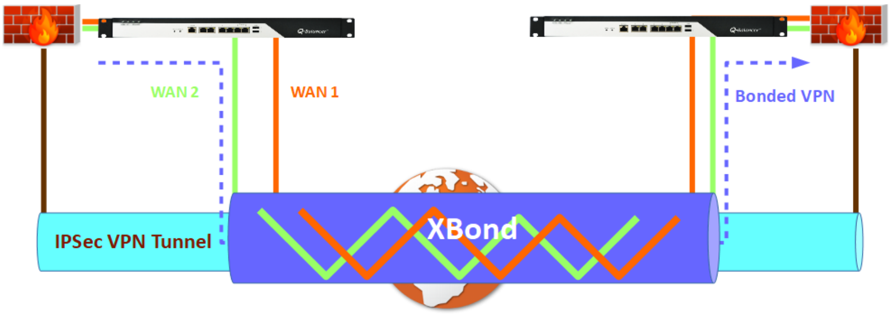

Figure 5: VPN Bonding

> IPSec VPN Tunnels Termination and Failover

Virtual Private Network (VPN) is a widely deployed technology for multi-location enterprises 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.

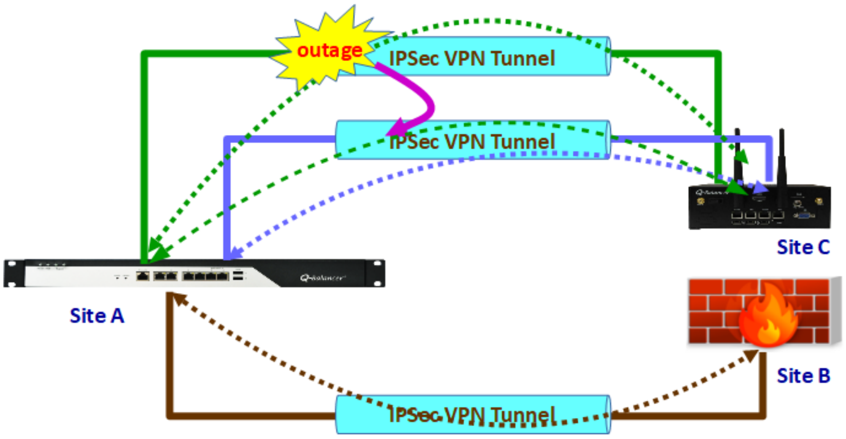

Figure 6: IPSec VPN Tunnels Termination and Failover

IPSec VPN tunnel is established based on a single Internet circuit, for example, an ADSL line. Should the circuit fails, there is no way to keep the connectivity for the LAN-to-LAN access. Q-Balancer is able to form multiple VPN tunnels at both ends, and in the event of WAN outage, LAN-to-LAN traffic will be diverted to the remaining active tunnel(s). This ensures network connectivity between business locations within an enterprise.

> Load Balancing LAN-to-LAN Traffic across IPSec VPN Tunnels

When more bandwidth is required to accommodate the growing demand, it would be possibly difficult to increase bandwidth capacity through traditional NAT-based multiple WAN load balancing technology.

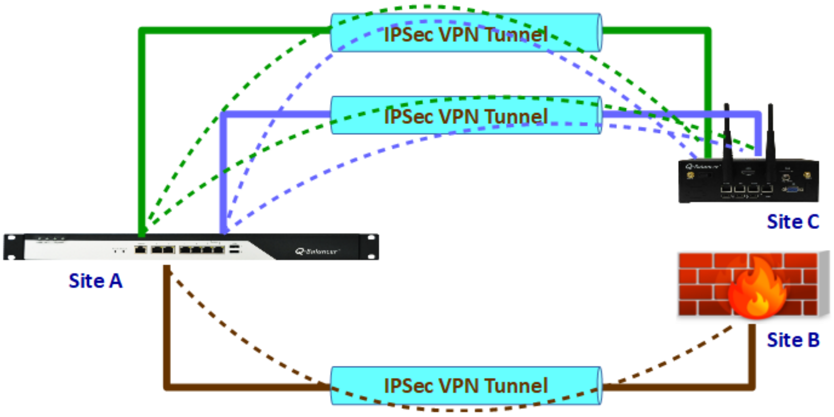

Figure 7: Load Balancing LAN-to-LAN Traffic Across IPSec VPN Tunnels

Multiple IPSec VPN tunnels can be terminated between Q-Balancer and the third-party VPN devices. This allows bandwidth of different links to be concurrently utilized by different networks. The mechanism of link load balancing distributes LAN-to-LAN traffic across multiple IPSec tunnels. As the IPSec tunnel is able to work in conjunction with policy-based load balancing, it increases the flexibility of LAN-to-LAN traffic and routing control.

Any VPN device which supports standard IPSec may terminate IPSec VPN tunnels on Q-Balancer appliance. This enables corporate network to build VPN tunnels whether the branch office has Q-Balancer devices. Bandwidth of all links can thus be highly utilized by configuring multiple IPSec tunnels for different networks.

> Cellular Bandwidth Bonding

With 4G LTE support, pop-up stores and temporary sites now are able to instantly deploy Internet connectivity whenever and wherever needed. By connecting multiple wireless Internet connections from multiple providers to Q-Balancer appliance, those temporary business locations can conduct transactions even if one of Internet connections went down. Customer services will never suffer from any WAN outage.

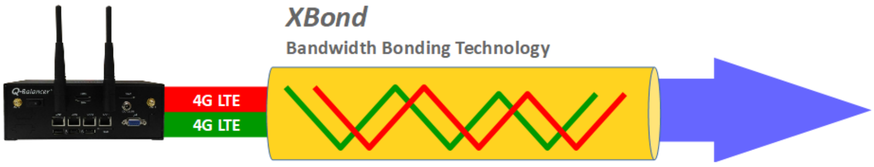

Figure 8: 4G LTE Bonding

> Multi-Path QoS (Quality of Service)

When the transmission of mission-critical applications becomes slow because of limited bandwidth resource, business would be likely to invest more in bandwidth upgrade. however, more bandwidth subscribed means paying more monthly. With Q-Balancer QoS you can flexibly prioritize network traffic based on MAC addresses, IP addresses, ports, services, and applications.

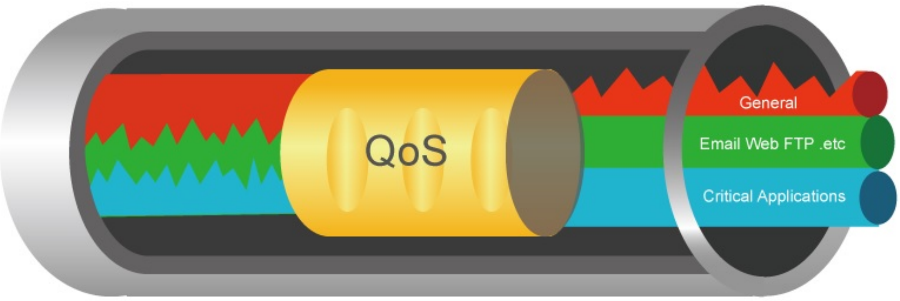

Figure 9: Multi-Path QoS

Q-Balancer QoS provides enterprises with granular control over the bandwidth utilization. The issues of network performance can be sorted or mitigated by allocating enough bandwidth to business-critical applications and limiting the bandwidth usage of business-unrelated traffic. It enables enterprises to throttle traffic flows on multiple paths, and so general or non-critical traffic will not overuse the bandwidth resources.

> Forward Error Correction (FEC)

Forward error correction (FEC) controls data transmission errors over unreliable or noisy communication channels. The technology adds error correction data to the outbound traffic, allowing the receiving end to recover from packet loss and other errors that occur during transmission, improving the quality of real-time applications. This enables network-layer equipment to reconstitute lost packets at the far end of a WAN link, before the packets are delivered to TCP or other transport layers.

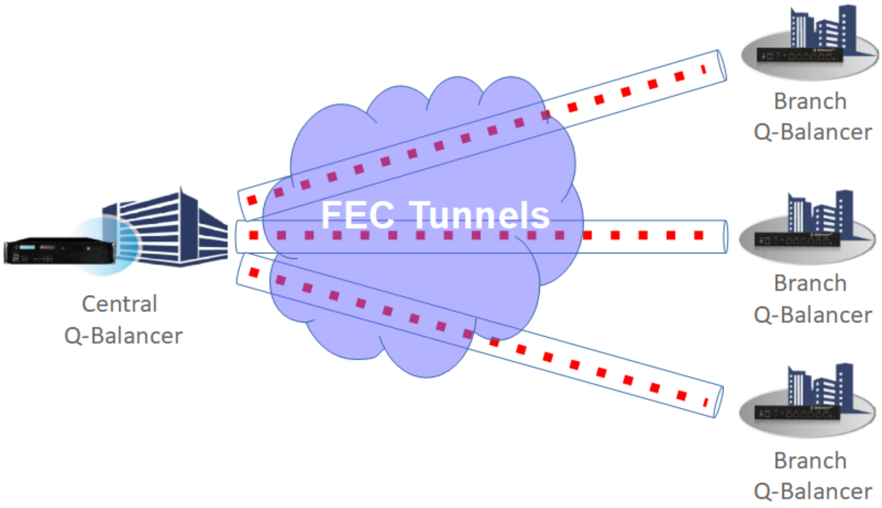

Figure 10: Forward Error Correction

FEC is particularly suitable for networks that leverage packet-level bandwidth bonding when transferring traffic across a WAN. For the network leveraging packet-level bandwidth bonding, Q-Balancer appliance distributes the load into the specified number of equal packets (source packets), and adds the specified number of redundant packets to the outbound traffic. With adaptive FEC, the appliance adjusts these numbers as it measures the link error rate. This enhances data reliability, increases transmission speed, and delivers a better user experience for applications. Enterprises therefore enjoy the significant improvements in application performance through FEC.

Benefits and Business Outcomes

> Improving WAN reliability and performance
> Optimal application delivery
> Increasing VPN reliability and performance
> Increasing WAN scalability
> Ensuring accessibility to internal server for external requests
> Lowering WAN OpEx and CapEx

> Mitigating potential security threats
> Reliable Internet connectivity for branch offices anywhere
> Minimizing effort for branch devices installation
> Simplifying branch network infrastructure

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. 3F10, No. 5, Sec. 5, Xinyi Road, Taipei, Taiwan 11011 | Tel+886-2-87808518 | sales@creek.com.tw | www.creek.com.tw.