Sales FAQ

We've collected answers to frequently asked questions and categorized them as follows:

Broadband Bonding

Broadband Bonding utilizes internet lines without coordination or equipment from any service provider, and enables enterprise networks to create a reliable and high-speed Internet connectivity.

> WAN Load Balancing

The feature of WAN Load Balancing helps business cost-effectively build a reliable and high-speed connectivity by utilizing multiple internet connections and distributing the traffic load across the links.

> WAN Failover

In case the primary line failed, then new request would be transparently routed down the remaining active links; when the primary line recovers from the outage, Q-Balancer again directs new request via the primary line.

> Packet Level Bandwidth Bonding

The technology of Packet-level bandwidth bonding combines bandwidth for site-to-site circuits and makes the bonded circuit work like a virtual leased line. The increased bandwidth theoretically equals to the sum of the separate connections.

> Cellular Bonding

The technology of Cellular Bonding harness multiple 4G LTE connections to provide branch offices a highly resilient and scalable network backhaul.

> Inbound Load Balancing & Failover

Through inbound load balancing, the incoming requests will be directed to the best-performing or least-loaded path, or efficiently distributed across the available paths. This also avoids faulty or congested path(s) when directing incoming requests to the hosted servers, and furthermore highly increases the availability and efficiency of the hosted service to incoming requests.

> Policy-Based Routing (PbR)
Policy-Based Routing can be set to configure preferred paths (WAN & VPN) for different traffic flows based on MAC, IP, Port, FQDN, applications, and schedule.

> Load Balancing based on domain name routing
The technology of domain name routing enables IT to configure PbR policy that explicitly directs outbound traffic destined for certain destinations via the specific path(s) based on business intent.

> Session Persistence
This is to ensure specific traffic will be routed through the same connection persistently based on its source and destination IP addresses. It keeps the outgoing traffic to the particular server(s) on the same path until the session ends.

> Path Monitoring
As a core component, path monitoring constantly monitors the status of all internet circuits, and works in conjunction with dynamic path selection (DPS). DPS is thus able to intelligently failover and distribute traffic across all available links based on the collected information.

> WAN Brownout
In the event of a WAN brownout, the WAN path still has connectivity, but performance is degraded by packet loss, increased latency or jitter.

VPN Bonding
Site-to-site VPN is established based on a single Internet circuit, and VPN is down as soon as the Internet circuit fails. Traditional NAT-based link failover is unable to provide redundancy for VPN connection. In addition, when more bandwidth is needed, it is impossible to increase bandwidth capacity through link load balancing.

> Automated VPN Failover
The devices at both ends increase VPN reliability as they constantly monitor WAN status and automatically divert VPN traffic down to the remaining active paths in case the primary Internet circuit fails.

> Site-to-Site VPN Bonding
Site-to-Site VPN bonding splits a single VPN session into packet level and sends them across multiple Internet circuits; VPN speed and security of data transmission are thus increased.

> Auto-Provisioning VPN Bonding
Q-Balancer XBond is an inbuilt technology of VPN Bonding that enables it overlay network and relevant routing policy to be provisioned automatically.

> IPSec Tunnels Termination

IPSec VPN tunnels can be terminated between Q-Balancer appliances, and between Q-Balancer and third-party IPSec devices.

> Automated IPSec Tunnel Failover

The technology of Automated IPSec tunnel failover automatically divert site-to-site traffic to the remaining active IPSec tunnels in case the primary IPSec tunnel fails. This technology supports the IPSec tunnels terminated between Q-Balancer appliances.

> IPSec Tunnel Load Balancing

The technology of IPSec Tunnel Load Balancing has the ability to distribute traffic sessions across multiple IPSec tunnels, and the speed of data transmission is therefore increased. This technology supports the IPSec tunnels terminated between Q-Balancer appliances.

MPLS Augmentation and Replacement

MPLS no longer meets all the requirements of enterprise networks today. The solution of MPLS Augmentation and Replacement is to overcome some of the issues faced by MPLS customers such as redundancy, lead times, high cost, performance of cloud application, etc.

> Hybrid WAN

Hybrid WAN is commonly used to connect two geographically separate sites with different types of connections. One type of connection is a private MPLS circuit, and the other might be broadband Internet links. In Hybrid WAN network, MPLS line connects to the data center, while the broadband lines can be used as a backup or to connect the public cloud.

> WAN Virtualization

WAN Virtualization combines multiple WAN connections of any type, creating a single virtual pipe. This combines MPLS WAN and low-cost Internet broadband bandwidth, for example, cable, DSL, 4G LTE, to augment or replace individual private WAN connections.

> Overlay Network

Overlay network is a method of using software virtualization to create additional layers of network abstraction (or software-based network overlays) that can be run on top of the physical network, often providing new applications or security benefits.

> Auto-Provisioning Overlay

Overlay network and relevant routing policy can be provisioned automatically in Q-Balancer network. This significantly reduces time and manual overhead for installation because adding new branch network to an enterprise network will take only few minutes.

> Overlay Routing

With the ability to understand (and participate in) popular dynamic routing protocols, for example, OSPF and BGP, Q-Balancer is able to establish and maintain existing routing tables. Thus, in the event of an interface or link outage, traffic for the route will be directed to the defined virtual path.

> Virtual Appliance
The virtual Q-Balancer is a software platform that brings benefits of increased capacity, high reliability, cost saving, and better application delivery to enterprise WAN.

> Branch Network Simplification
With its consolidated features, Q-Balancer lowers WAN complexity for branch networks. Network services integrated within the Q-Balancer SD-WAN products help enterprises with branch simplification efforts.

> WAN Transport Agnostic
Overlay network in Q-Balancer is transport agnostic. Therefore, when it comes to overlay network building, the appliance does not care about whether the WAN transport is, for example, ADSL or 4G LTE lines.

> Network Controller
Network controller maintains connections to all edge appliances and monitor the operational state of overlay tunnels across different WANs, helping enterprise networks become dynamic and intelligent from end to end.

> Edge Appliance
An edge appliance connects MPLS and broadband networks in a multi-office network, and dynamically directs traffic to the specific destinations via the best path or distribute traffic across WAN links of types.

> Dynamic Path Selection
Dynamic Path Selection (DPS) works in conjunction with path-monitoring and allows administrator to configure performance criteria for different types of traffic. It directs packets to an optimal route or distribute traffic across multiple paths based on load balancing policy and collected information.

> Application-Aware Routing
Application-Aware Routing has the ability to identify and selectively directs/distribute traffic flows to the destinations by applications.

> Granular Internet Breakout
Edge appliance locally breaks out internet-bound traffic and intelligently directs business-critical traffic via the designated path(s) respectively to the correct destinations.

> Forward Error Correction
The technology of Forward error correction (FEC) controls data transmission errors over unreliable or noisy communication channels.

Enterprise Features
The advanced features incorporated makes enterprise deployments easier, meets a variety of

requirements, and enables you to fully control your network.

> QoS

QoS enables organizations to proactively manage bandwidth based on business intent policies; therefore, key applications have the required bandwidth and business-unrelated applications are limited from consuming critical bandwidth. Q-Balancer QoS enables admins to control the maximum and/or guaranteed throughput for any load balancing policies specified, and to manage bandwidth based on MAC, IP, Port, DNS routing, applications, and schedule.

> Bandwidth Reduction

Bandwidth reduction is a process of taking a file or multiple files and making them smaller as they pass through the WAN. The size of data can be drastically reduced by compression techniques, which enables senders to send fewer data packets for a single file transmission.

> Server Load Balancing

Q-Balancer sits between the clients and the server farm, distributing incoming requests across multiple servers; the appliance removes the faulty servers from server pool and re-distributes traffic to the remaining active servers when a server outage is detected.

> Global Site Load Balancing (GSLB) & Failover

In GSLB deployment each Q-Balancer tracks the status of the other appliances at different locations; in case one of the sites fails, for example, power outage, GSLB then redirects requests to the remaining active one. This ensures business continuity and buys time for IT team to solve the issues. By business-intent policies or availability and status of data centers, client requests are generally directed to closer servers to ensure minimal latency and better performance.

> High Availability (HA) VRRP

HA VRRP ensures enterprises networks to stay connected with its ability of fault tolerance for unexpected hardware failure. For the planned downtime like system maintenance, the impact will also be reduced without extra effort.

> Multiple Transparent Bridges

With transparent bridge, the appliance acts as a layer 2 bridge between network devices (core switch, router, or firewall), and thus is transparent to the legacy network devices. This means that the configuration on the legacy firewall does not need to be changed for the installation. The deployment works as if the appliance were sitting transparently between the router and firewall. Multiple bridge subnets are supported on Q-Balancer to meet the requirement, where multiple subnets are transparently connected.

> Road Warrior VPN

Client-to-site VPN such as PPTP, L2TP/IPSec, and IPSec are supported on Q-Balancer. This enables remote and mobile devices to access enterprise resources as if they were on the office LAN.

> Link Aggregation Control Protocol (LACP) NIC Binding

LACP is a layer 2 protocol that provides functionality when aggregating one or more Ethernet interfaces to form a single logical link (link aggregation groups). The bond interface share the load among many interfaces, which gives fault tolerance and increases throughput.

Network Security

The appliances protect enterprise networks against unauthorized access with its inbuilt security mechanisms including ARP Spoofing Attack Protection, Stateful Firewall, DNS Firewall, and DDoS Prevention.

> Address Resolution Protocol (ARP) Spoofing Attack Protection

ARP spoofing is a technique by which an attacker sends (spoofed) ARP messages onto a local area network. This results in the linking of an attacker's MAC address with the IP address of a legitimate computer or server or gateway on the network, causing any traffic meant for that IP address to be sent to the attacker instead. The solution uses static IP-MAC binding to protect enterprise network against ARP spoofing attack.

> Stateful Firewall

The inbuilt stateful firewall is aware of the connections that pass through the appliance. Stateful inspection of Q-Balancer firewall monitors incoming and outgoing packets over time, as well as the state of the connection, and stores the data in dynamic connection tables. This accumulative data is evaluated for filtering, so that filtering decisions would not only be made based on pre-defined rules, but also on context that has been built by previous connections as well as previous packets belonging to the same connection.

> DNS Filtering

DNS Firewall prevents network users and systems from connecting to known malicious Internet locations. DNS Firewall is similar to traditional firewalls as it blocks end-users from accessing malicious sites at a different layer and phase.

> Distributed Denial of Service (DDoS) Prevention

DDoS attacks are the most common type of online attacks as they are an attempt to exhaust network, server or application resources so that they are no longer available to intended users. Q-Balancer detects DDoS traffic and mitigates it rapidly, providing your network infrastructure with the most robust security against such attacks.

> Connection Limit

Connection limit is configured to allow a maximum number of TCP connections for a single IP host or subnet to protect a network. When the number of connections exceeds the maximum, the new connections is dropped and logged.

General

> Who is Q-BALANCER Company?

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.

> What is the solution?

The Q-Balancer solution is designed to provide a reliable and scalable WAN for branch offices, corporate headquarters, large organizations, and data centers. All its features such as broadband bonding, VPN bonding, MPLS augmentation and replacement are located on a single appliance with policies and configurations being managed through an intuitive web interface.

> What are the main benefits of Q-Balancer solution to enterprises?

>> Improving WAN reliability and performance

>> Optimal application delivery

>> Increasing VPN reliability and performance

>> Augmenting MPLS reliability and performance

>> Flexibly 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

>> Enhancing dynamic routing capability

>> Minimizing effort for branch devices installation

>> Simplifying branch network infrastructure

>> Increasing backhaul capacity

> How long does it normally take to deploy a Q-Balancer appliance at a single site?

Other than knowledge of TCP/IP, the engineers installing Q-Balancer appliance for enterprises do not require advanced skill set. The time required to enable an enterprise network to access the internet through the Q-Balancer appliance can be measured in minutes.

> How does the Q-Balancer solution save customers money?

Cost saving is one of the major benefits to the customer. The following are about how Q-Balancer saves cost for customers:

>> Leveraging inexpensive broadband connectivity instead of costly MPLS services helps customers reduce the monthly recurring costs for bandwidth.

>> CapEX saving is achieved as some specific network devices such as routers, firewalls, etc can be eliminated when designing the network for branch offices. Its competitive pricing also

mitigates the upfront investment on branch network. These advantages enable companies to choose the best model for their budget and objectives.

>> OpEX saving is achieved as the solution allows merely a single WAN administrator to centrally manage the connectivity at the branch and enforce business intent policies for hundreds of branch offices. It also eliminates the costs associated with networking engineers that require particular skill set to maintain various hardware appliance at the branch offices.

>> The WAN performance and reliability gains helps reduce costs associated with lost productivity.

> How to select the suitable model of Q-Balancer?

The solution supports a range of customer segment from branch offices, corporate headquarters, large organizations to data centers. The solution can be delivered as either a physical or virtual appliance.

>> Physical Appliances

Q-Balancer 2000 is designed for educations, large enterprises and data centers, and supports up to 52 WAN links and up to 20 Gbps throughput. Large organization can employ Q-Balancer 2000 to work as a link load balancer to ensure network connectivity, while in a distributed network Q-Balancer 2000 can function as a network controller.

Q-Balancer 500 is designed to bring high network reliability and performance to medium and large-sized enterprise and regional data centers. This 1U rack-mountable appliance supports up to 52 WAN links and up to 3 Gbps throughput. Q-Balancer 500 protects business from any potential network failure and disruption.

Q-Balancer 300 is designed for small and medium-sized enterprises and supports up to 25 WAN links and up to 1.5 Gbps throughput. This 1U rack mountable appliance ensures connectivity while providing key features for enterprises including routing, firewall and bandwidth management.

Q-Balancer 300D is a desktop version of Q-Balancer 300. This low-cost desktop appliance ensures connectivity while providing key features for enterprises including routing, firewall and bandwidth management.

Q-Balancer 150 is a compact design appliance for small and branch offices with higher bandwidth demand. The appliance supports up to 10 WAN links and up to 300 Mbps throughput. Q-Balancer 150 comes with all-in-one features, and brings the benefits of low costs and high reliability.

Q-Balancer Mesh is designed to provide secure WAN access for pop-up stores and branch offices wherever they are, particularly for the locations where wired solutions are not available or costly. With its intelligent algorithms and industry-grade 4G LTE connectivity, Q-Balancer Mesh enables branch networks to stay connected as needed.

>> Virtual Appliance

QB-V2000 is a virtual edition of Q-Balancer 2000 running on VMware vSphere virtual server,

and provides same functionality as the physical appliance of QB-2000.

In case you have questions beyond them, kindly contact your resellers or contact us.