



Q-global Architecture and Security Reference

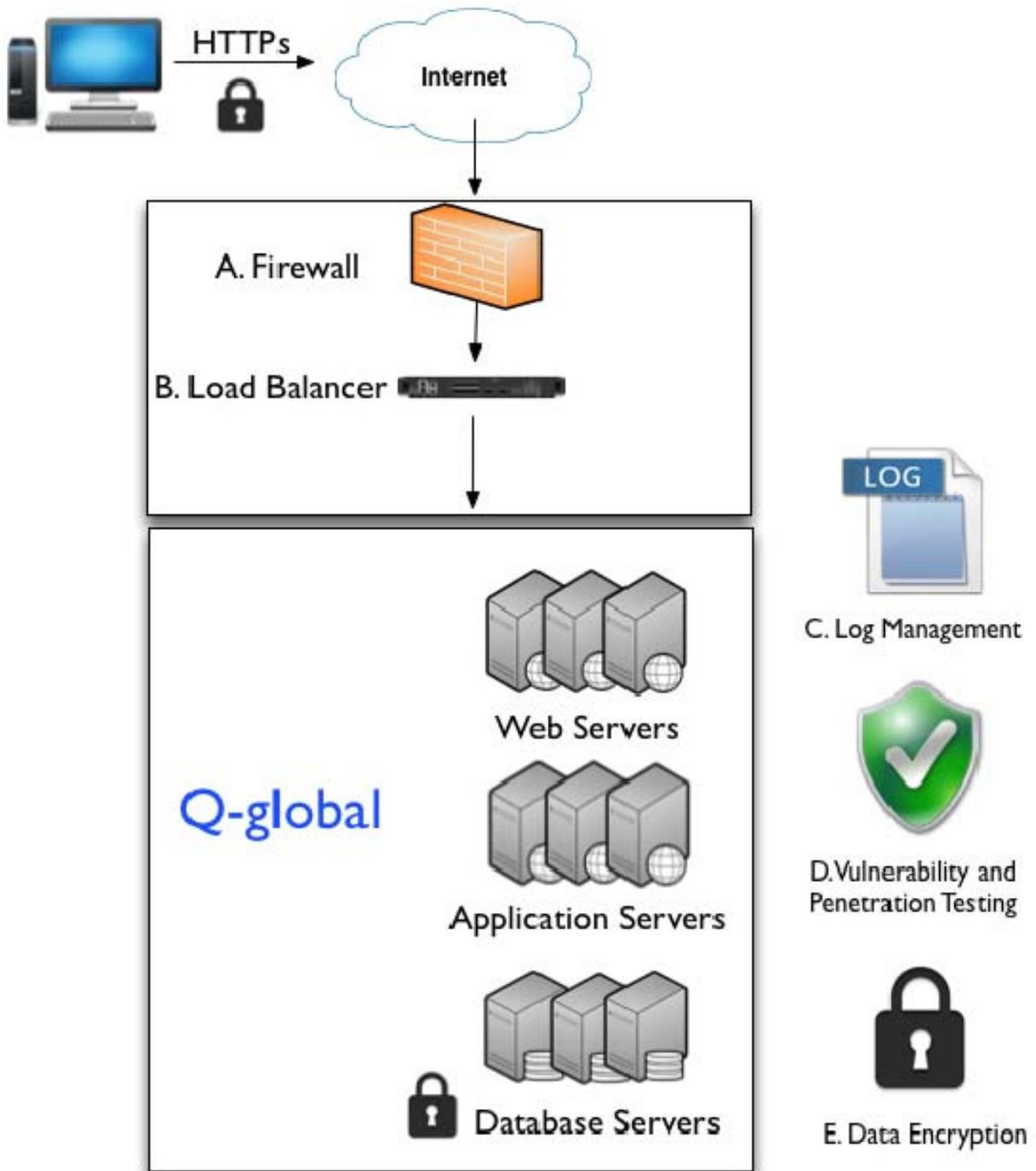
**Version 1.2
September 2016**

1. Introduction

Maintaining a secure infrastructure and environment that safeguards data and personally identifiable information is our highest priority for our customers. This document will focus on the architecture and security that is employed by Q-global to safeguard such data.

II. Architecture

Q-global is a web-based application designed for mental health professionals, educators, and other professionals, who want the ease, reliability, and security for their administration, scoring, and reporting needs.



A. Dedicated Firewall

A dedicated firewall provides the first line of defense and controls traffic between trusted and untrusted networks. It filters and blocks non-essential traffic based on ports and protocols, allowing only wanted and appropriate traffic into the private network.

B. Load Balancer

Load balancers provide redundancy and manage platform load, but they also manage traffic and obfuscate the endpoint to help protect against insertion and evasion network attacks. They enable HTTPs session persistence across servers to ensure data is transferred securely across Q-global.

C. Log Management

Log management helps in detecting unauthorized access attempts. The systems perform specific event logging at the application layer to help identify potential attacks, allowing appropriate monitoring and response.

D. Vulnerability and Penetration Testing

Vulnerability and penetration testing is regularly conducted and allows for the identification of exploitable weaknesses. It can be performed at different intervals to ensure that configuration changes, patches, or functionality enhancements did not introduce exploitable weaknesses. This testing is a proactive, preventative control that enables the finding and addressing of application and infrastructure weaknesses.

E. Data Encryption

1. In Transit

All data that is transferred to the Q-global platform is transmitted using 256-bit TLS connections. The web browser validates the HTTPs certificate and generates an exception if the certificate is not valid.

2. At Rest

Client data on Q-global is encrypted in a database that is hosted in a dedicated, secure environment. This environment is restricted and physical and virtual access is restricted to authorized personnel only. Read and write auditing information is stored for access and modifications to the database.