Q-Proxy®

The **Q-Proxy**® is a Proxy Server built using two open source packages, **Squid** and **SquidGuard**, running on an extremely small form factor, ultra-low power consumption server. **Squid** is the leading open source proxy package. **SquidGuard** is a URL redirector, which enables Squid to use blacklists, including both custom blacklists and blacklists provided by MESD, Shalla's Blacklist, the Université de Toulouse Blacklist Collection, and URLBlacklist.com to block access to web sites. Using **SquidGuard** and a blacklist enables network manages to easily enforce their organization's Internet usage policy.

The **Squid** proxy server software supports caching for HTTP, HTTPS, FTP, as well as other web services. In addition to controlling user access to web sites and web services, the **Q-Proxy** conserves WAN bandwidth by eliminating multiple WAN requests for the same web pages or files. They are accessed instead from the **Q-Proxy**'s cached content. This makes WAN bandwidth available for new content, rather than repeated WAN downloads of the same content by different users.

An example of this would software that has to be installed on multiple PCs, such as Windows Security Patches or an application. By caching the download on the **Q-Proxy**, WAN bandwidth is used only for the original download. The downloads to the network computers from the **Q-Proxy** will also be much faster, occurring at the speed of the LAN, which is typically much, much faster than the WAN connection.

The **Q-Proxy** is especially useful for conserving shared cellular bandwidth, or any metered broadband service. By deploying the **Q-Proxy**, expensive WAN bandwidth is conserved, which helps administrators avoid costly bandwidth upgrades, and for areas where no additional bandwidth can be bought, or bought economically, makes far better use of the existing bandwidth. The **Q-Proxy** comes with 120 GB of storage for cached files.

Q-Proxy Hardware Specifications:

- 126 mm x 70 mm x 28 mm – 170 grams
  (5.0" x 2.8" x 1.1" – 6 oz)
- Power consumption under full load: 8 watts, 120v-240v
- No fan or any moving parts. Must be installed in well-ventilated space.
- Operates 0°C–70°C (32°F–158°F)
- **Capacity:** 120 GBytes for cached files.

LED indicators:

- Power
- Link (physical connection to network)
- Activity (network traffic)
- 1000 mbps (gigabit) NIC connection
- Dual Band WiFi. (2.4 GHz & 5 GHz)

Contact: Richard Avery
646-449-7810
Q-Proxy@quantalytics.com

Quantalytics. In-depth network defenses.

Quantalytics

Q-Proxy®

The **Q-Proxy** includes:

- **Squid** – **Squid** is the leading open source, enterprise-class, proxy server software solution.

- **SquidGuard** – **SquidGuard** is the leading open source URL redirector. It combines custom black lists along with blacklists from either MESD, Shalla's Blacklist, the Université de Toulouse Blacklist Collection, or URLBlacklist.com.

- **Calamaris** – **Calamaris** parses all the log files and generates reports about peak-usage, request methods, status-report of incoming and outgoing requests, second and top level destinations, content-types, and the **Q-Proxy**'s performance.

- **ModSecurity®** – **ModSecurity® (ModSec)** is the leading open source Web Application Firewall (WAF) for cross-scripting attack protection. We have hardened the **Q-Proxy**'s built-in Apache web server to prevent conceivable attacks.

- **ClamAV®** – **ClamAV®** is the leading open source anti-virus package.
- **Tiny Honeypot (THP) - THP** fools attackers by making it appear that the attack is working, while meanwhile logging the attack info. It wastes an attacker's time, and creates an opportunity to detect the network intrusion by offering to the attacker what appears to be thousands of services.

- **Webmin – Webmin** is the leading open source Web GUI package for server configuration and maintenance.

HA Proxy – **HA Proxy** is the leading open source package for automatic failover and load balancing. Up to 32 **Q-Proxy** appliances may be linked for automatic failover or load balancing for coverage of extremely large networks. Administration is done through a Web GUI for monitoring the load balancer and the appliances it has been setup to use.

The **Q-Proxy** has both a Gigabit (1000 mbps) NIC and 802.11 Dual Band WiFi. (2.4 GHz and 5 GHz.)

The **Q-Proxy** is also available as a Virtual Machine (VM).

Contact: Richard Avery
646-449-7810
Q-Proxy@quantalytics.com

Quantalytics. In-depth network defenses.

Quantalytics

Q-Proxy®

The **Q-Proxy** is completely administered through a Web GUI. No Command Line Interface (CLI) or Linux skill is required.

Using the provided **Webmin** module, two-factor authentication can be added using **Google Authenticator** or **Authy**, a commercial service with its own app. **Google Authenticator** runs on Android, IOS, and Blackberry devices, and uses the standard TOTP protocol.

Notifications are provided by e-mail using **SendMail**, which is configured with a module in **Webmin**, and syslog entries. The **Q-Proxy** network appliance can be integrated with **Nagios**® on the **Q-Box**® as another notification route. SMS notification is available as an option. The **Q-Proxy** network appliance can also be integrated with the **Q-Log**® network appliance or any other Syslog or SIEM (Security Information and Event Management) solution.

Contact: Richard Avery
646-449-7810
Q-Proxy@quantalytics.com

Quantalytics. In-depth network defenses.