Quantalytics

Q-WiFi®

The **Q-WiFi**® is an amalgamation of a number of open source software packages running on an extremely small form factor, low-power-consumption network appliance designed to detect and thwart "Evil Twin" Wireless Access Points (WAPs) and decoy WiFi routers. The **Q-WiFi** prevents Evil Twin APs from tricking users while also monitoring network devices and services, and provides intrusion detection and prevention.

The provided WiFi protection includes actively blocking the "Evil Twin" upon its detection by unleashing a Denial of Service ("DoS") attack to prevent users from logging into it. The ultra compact design allows exceptionally flexible and creative deployment options as well as significant electricity and space savings. PoE is available as an option.

Q-WiFi *Hardware Specifications*:

- 108 mm x 64 mm x 26 mm – 170 grams
  (4.25" x 2.50" x 1.125" – 6 oz)
- Power consumption under full load:
  8 watts, 120v-240v
- No fan or any moving parts. Must be installed in a well-ventilated space.
- Operates 0°C–70°C (32°F–158°F)

LED indicators:

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

The **Q-WiFi** network appliance includes:

- **EvilAP_Defender** – **EvilAP_Defender** is the leading open source, enterprise-class tool to discover and prevent Evil Twin Access Points (APs) from attacking wireless users. The **Q-WiFi** can discover and provide an email alert when an Evil Twin is discovered. In addition, it can perform a Denial of Service ("DoS") attack to prevent the legitimate WiFi users from connecting to the Evil Twin AP. This can give network administrators and/or law enforcement time to locate and remove the Evil Twin AP.

- ***Note:*** The DoS feature only works if the Evil Twin and legitimate AP have the same SSID but different BSSID, or is running on a different channel. (The BSSID – Basic Service Set Identifier - is the AP's MAC address.) This prevents accidently crippling a legitimate AP. Whitelisting is done via a wizard during installation in order to recognize and allow legitimate Wireless Access Points (APs).

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

Quantalytics. In-depth network defenses.

- **Aircrack-ng – Aircrack-ng** allows the **Q-WiFi** to capture and monitor WiFi traffic. **Aircrack-ng** feeds this data to **EvilAP_Defender**.

- **Q-Aircrack-ng – Q-Aircrack-ng** is the web-based GUI for **Aircrack-ng**.

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

- **Tiny Honeypot (THP) - THP** helps defend the **Q-WiFi** by fooling attackers, making it appear that the attack is working, while meanwhile logging the attack info. **THP** wastes an attacker's time, and creates an opportunity to detect the network intrusion by offering to the hacker what appears to be thousands of services.

- **HA Proxy – HA Proxy** is the leading open source package for automatic failover and load balancing. Up to 32 **Q-WiFi** network appliances may be linked for automatic failover or load balancing for coverage of extremely large networks. Administration is done through a web gui.

- **ClamAV® – ClamAV®** is the leading open source anti-virus software package.

- **Webmin – Webmin** is the leading open source Web GUI package for server configuration and maintenance. **Webmin** also allows for the linkage of multiple **Q-WiFi** systems for simplified administration.

The **Q-WiFi** is completely administered through a Web GUI. This makes all features easily available even to novice network administrators. No Command Line Interface (CLI) or Linux skill is required.

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

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

Quantalytics. In-depth network defenses.

Quantalytics

Q-WiFi®

The **Q-WiFi** has both a Gigabit (1000 mbps) NIC and 802.11 Dual Band WiFi. (2.4 GHz and 5 GHz.) The **Q-WiFi** is intended to be deployed wherever there is a risk of an Evil Twin attack. **E.G.** Public spaces where free WiFi is offered, in addition to private WiFi networks in order to guard against cyber espionage. PoE (Power over Ethernet) is available as an option.

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-WiFi** network appliance can be integrated with **Nagios** on the **Q-Box**® as another notification route. SMS notification is available as an option. The **Q-WiFi** 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-WiFi@quantalytics.com

Quantalytics. In-depth network defenses.