Q-WiFi®

Le **Q-WiFi**® est une amalgame d'un certain nombre de progiciels logiciels open source fonctionnant sur un appareil de réseau à faible consommation de faible consommation, conçue pour détecter les points d'accès sans fil (WAP) et les routeurs WiFi appelés «Evil Twin» et les contrecarrer. Le **Q-WiFi** empêche les Jumeaux Maléfiques («Evil Twin») APs de tromper les utilisateurs tout en surveillant les périphériques et les services réseau, et fournit une détection et une prévention des intrusions. La protection WiFi fournie comprend le blocage actif du «Evil Twin» lors de sa détection en déclenchant une attaque de Déni de Service («DoS») pour empêcher les utilisateurs de se connecter à elle. Le design ultra compact permet des options de déploiement exceptionnellement flexibles et créatives, ainsi que d'importantes économies d'électricité et d'espace.

- Spécifications matérielles du **Q-WiFi**:
- 108 mm x 64 mm x 26 mm – 170 grammes (4.25" x 2.50" x 1.125" – 6 oz)
- Consommation électrique à pleine charge: 8 watts, 120v-240v
- Pas de ventilateur ou de pièces mobiles. Doit être installé dans un espace bien ventilé.
- Fonctionne à partir 0°C à 70°C (32°F–158°F)

Indicateurs LED:

- Pouvoir électrique
- Lien (connexion physique au réseau)
- Activité (trafic réseau)
- 1000 mbps (gigabit) NIC connexion
- WiFi Bi-Bande. (2.4 GHz et 5 GHz)

L'appliance réseau **Q-WiFi** comprend:

- **EvilAP_Defender – EvilAP_Defender** est le principal outil open source, de classe entreprise, pour découvrir et empêcher «Evil Twin» Point d'Accès (AP) d'attaquer les utilisateurs sans fil. Le **Q-WiFi** peut découvrir et fournir une alerte par courrier électronique lorsqu'un «Evil Twin» est découvert. En outre, il peut effectuer une attaque de Déni de **Service** («DoS») pour empêcher les utilisateurs légitimes de WiFi de se connecter à l'AP «Evil Twin». Cela peut donner aux administrateurs du réseau et / ou au temps d'application de la loi pour localiser et supprimer l'AP «Evil Twin». **N.B**. La fonction DoS ne fonctionne que si le «Evil Twin» léger et l'AP légitime ont le même SSID mais différents BSSID, ou s'exécutent sur un canal différent. (Le BSSID - Basic Service Set Identifier - est l'adresse MAC de l'AP). Cela empêche de paralyser accidentellement un AP légitime. La liste blanche est effectuée via un assistant lors de l'installation afin de reconnaître et autoriser les points d'accès sans fil (AP) légitimes.
- **Aircrack-ng – Aircrack-ng** permet à **Q-WiFi** de capturer et de surveiller le trafic WiFi. Aircrack-ng alimente ces données à **EvilAP_Defender**.
- **qAircrack-ng – qAircrack-ng** est l'interface graphique Web pour **Aircrack-ng**.
- **Webmin - Webmin** est utilisé pour l'entretien ménager des réseaux et la configuration du réseau.
- **HA Proxy – HA Proxy** est le premier fournisseur open source pour le basculement

Contact: Richard Avery
+1 646-449-7810
Q-WiFi@quantalytics.com

Quantalytics. Défenses de réseau en profondeur.

automatique et l'équilibrage de charge. Jusqu'à 32 appareils de réseau **Q-WiFi** peuvent être liés pour le basculement automatique ou l'équilibrage de charge pour la couverture de réseaux extrêmement grands. L'administration se fait via un web gui.

- **ModSecurity® – ModSecurity®** («**ModSec**») est le premier package de protection contre les attaques du serveur Web Apache. **ModSec** est utilisé pour endurer le serveur web Apache intégré de l'appliance **Q-WiFi** et éviter les attaques imaginables.
- **Tiny Honeypot («THP») - THP** trompe les attaquants en faisant apparaître que l'attaque fonctionne, tout en enregistrant les informations d'attaque. **THP** gaspille le temps d'un attaquant et crée l'opportunité de détecter l'intrusion du réseau en offrant à l'attaquant ce qui semble être des milliers de services.
- **ClamAV®** – **ClamAv®** est le premier package antivirus open source.

L'appliance de réseau **Q-WiFi** dispose à la fois d'une NIC 10/100 MB et d'un WiFi 802.11 b / g / n. Il est destiné à être déployé partout où il y a un risque d'une attaque Evil Twin. **PAR EXEMPLE**. Les espaces publics où WiFi gratuit est offert, en plus des réseaux WiFi privés.

L'appliance réseau **Q-WiFi** possède possède à la fois un NIC Gigabit (1000 mbps) et un WiFi Bi-Bande 802.11 (2.4 GHz & 5 GHz).

PoE (Alimentation par Ethernet - Power over Ethernet) est disponible en option.

L'appliance réseau **Q-WiFi** est complètement administrée via une interface graphique Web. L'utilisation de tous les packages se fait via des interfaces Web, ouvrant ainsi une détection d'intrusion sophistiquée, une analyse légale en réseau et une surveillance de réseau même aux administrateurs réseau novateurs. Aucune interface de ligne de commande («CLI») ou Linux n'est requise.

En utilisant le module **Webmin** fourni, l'authentification à deux facteurs peut être ajoutée à l'aide de **Google Authenticator** ou **Authy**, un service commercial avec sa propre application. **Google Authenticator** s'exécute sur les appareils Android, IOS et Blackberry, et utilise le protocole standard de TOTP.

Les notifications sont fournies par e-mail à l'aide de **SendMail**, qui est configuré avec un module dans **Webmin** et les entrées syslog. L'appliance réseau **Q-WiFi** peut être intégrée à **Nagios®** sur le **Q-Box®** comme autre voie de notification. La notification par SMS est disponible en option. L'appliance réseau **Q-WiFi** peut également être intégrée à l'appliance réseau **Q-Log®** ou à toute autre solution Syslog ou SIEM. (Security Information and Event Management).

Contact: Richard Avery
+1 646-449-7810
Q-WiFi@quantalytics.com