Q-ModSec®

L'appareil de réseau **Q-ModSec**® (**ModSecurity**®, "**ModSec**") est un Firewall d'Application Web (WAF). Le **Q-ModSec** fournit une surveillance, une journalisation et un contrôle d'accès en temps réel aux applications Web afin de durcir les serveurs Web Apache et Nginx contre les attaques, et surtout, mais pas exclusivement, contre les attaques de scripts croisés. Le script croisé est la forme d'attaque la plus commune et la plus dangereuse utilisée contre les serveurs Web. Apache gère la plupart des serveurs Web d'Internet. Les serveurs Nginx sont également supportés explicitement. Il est également disponible en tant que machine virtuelle (VM).

L'appliance de réseau **Q-ModSec** fonctionne en tant que pare-feu d'application Web (WAF) en effectuant une surveillance de la sécurité des applications en temps réel de tout le trafic HTTP, plus une inspection en temps réel. Ceci est combiné avec un mécanisme de stockage persistant intégré au **Q-ModSec** pour suivre les éléments du système au fil du temps. À son tour, cela crée la possibilité d'effectuer des corrélations au fil du temps afin de rechercher des modèles d'attaque. Le **Q-ModSec** permet le blocage sélectif des éléments afin de couper les chemins d'attaque potentiels. Dans le cadre de sa sécurité améliorée, le **Q-ModSec** effectue des évaluations de sécurité passives continues**. Il s'agit d'une forme de surveillance en temps réel.** Au lieu de se concentrer sur le comportement des acteurs externes (pirates informatiques), un rôle joué par Intrusion Detection Systems (IDS), le **Q-ModSec** se concentre sur le comportement du serveur web lui-même. À la suite de cet objectif interne, **Q-ModSec** peut détecter des anomalies et des faiblesses de sécurité avant que le serveur Web ne soit piraté. Afin de durcir davantage les serveurs Web et les sites Web, le **Q-ModSec** peut réduire considérablement la liste des comportements HTTP autorisés, créant ainsi une surface d'attaque plus petite et, à son tour, augmenter la sécurité. PAR EXEMPLE. Méthodes de demande HTTP. En-têtes de requêtes. Types de contenu. Etc. Le **Q-ModSec** fournit également une application de restriction soit directement, soit par interaction avec d'autres modules Web Apache. En utilisant le **Q-ModSec**, il est possible d'éliminer les vulnérabilités de falsification de requêtes entre sites dans le cadre du durcissement de l'application Web.

En plus du durcissement du serveur web, le **Q-ModSec** peut être utilisé comme un routeur de service Web XML. Le **Q-ModSec** analyse XML et peut appliquer des expressions XPath tout en demandant des demandes de serveur, ce qui se produit comme un routeur XML.

Le **Q-ModSec** comprend également la console de sécurité **WAF-FLE**. L'interface Web **WAF-FLE** permet aux administrateurs de mémoriser, de visualiser et de rechercher des événements à l'aide d'un gui graphique en ligne de tableau de bord. Les événements sont rassemblés par des capteurs. Il n'y a pas de limite sur le nombre de capteurs autorisés, permettant à **WAF-FLE** de desservir un très grand nombre de serveurs Web et / ou de sites Web. L'interface Web **WAF-FLE** élimine la nécessité de toutes les compétences de l'interface de ligne de commande (CLI).

Un bref résumé de chaque colis est ci-dessous. Nous vous encourageons à consulter notre site Web, www.quantalytics.com, pour obtenir une explication plus complète des fonctionnalités de chaque paquet.

*Spécifications matérielles **Q-ModSec**:*

- 108mm x 64mm x 26mm – 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 de 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)

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

Quantalytics. Défenses de réseau en profondeur.

Q-ModSec®

Le système de réseau **Q-ModSec** comprend:

- **ModSecurity® - ModSec** "(**ModSecurity®**) est un firewall d'application Web en temps réel (WAF) pour la surveillance, la journalisation et le contrôle d'accès afin de durcir les serveurs Web Apache et Nginx contre les attaques. **ModSec** peut également être utilisé comme un routeur pour les demandes de service XML via XPath et sa demande intégrée de demandes de serveurs Web. Nous utilisons également **ModSec** pour sécuriser le serveur web Apache intégré de cet appareil.
- **WAF-FLE – WAF-FLE** est une console d'interface Web open source (gui) pour **ModSec**. Il permet aux administrateurs de configurer et de déployer des capteurs **ModSec**, puis de voir et d'analyser les données, en utilisant une variété de filtres intégrés.
- **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 automatique et l'équilibrage de charge. Jusqu'à 32 appareils de réseau **Q-ModSec** 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.
- **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.

Le **Q-ModSec** possède possède à la fois un NIC Gigabit (1000 mbps) et un WiFi Dual Band 802.11 (2.4 GHz & 5 GHz).

Le **Q-ModSec** est également disponible en tant que Machine Virtuelle («VM»).

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 de réseau **Q-ModSec** peut être intégré à **Nagios®** sur le **Q-Box®** comme autre voie de notification. La notification par SMS est disponible en option. L'appliance de réseau **Q-ModSec** peut également être intégré au **Q-Log®** ou à toute autre solution Syslog ou SIEM (Security Information and Event Management).

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

Quantalytics. Défenses de réseau en profondeur.