Comment vont-ils le whitelist I manuellement une page Web sur l'appliance de sécurité Web de Cisco (exécutant 5.2.0 et ci-dessus) de sorte que la lecture WBRS, de Webroot ou de McAfee soit sautée ?

Contenu

Question :

Comment vont-ils le whitelist I manuellement une page Web sur l'appliance de sécurité Web de Cisco (exécutant 5.2.0 et ci-dessus) de sorte que la lecture WBRS, de Webroot ou de McAfee soit sautée ?

Symptômes :

L'utilisateur essaye d'accéder à un site légitime, mais est dû à un score du bas WBRS (infection par un virus du web server, du Spam étant envoyés par l'IP etc. de web server) ou dû bloqué à une des engines d'anti-malware déclenchant à cette page.

Si l'utilisateur est dû bloqué à un bas WBRS l'utilisateur voit un message de bloc MALWARE_GENERAL. L'exposition d'accesslogs un WBRS au-dessous du seuil de blocage (le par défaut est -6.0).

Pour une solution permanente, contactez s'il vous plaît Cisco TAC de sorte que la page puisse être passée en revue afin d'ajuster le WBRS ou signaler des faux positifs aux constructeurs d'antivirus et d'anti-malware.

Vous pouvez également contacter Cisco TAC pour recueillir plus d'informations sur pourquoi le site est bloqué de sorte que le contact ou l'administrateur technique du site Web puisse être annoncé et puisse prendre les mesures nécessaires.
Veillez à fournir les codes de blocage et les lignes appropriés d'accesslog en contactant Cisco TAC

Pour sauter WBRS :

4. Cliquez sur en fonction le lien dans la colonne « de filtrage » de réputation et d'Anti-malware de Web de votre stratégie de création récente d'accès au Web (elle devrait lire « la stratégie

globale » jusqu'ici).

5. Choisi « définissez les paramètres personnalisés de réputation et d'Anti-malware de Web

Remarque: Si vous placez l'action « autorisez » dans la catégorie URL, ceci aurait en sautant la lecture d'Anti-malware/virus.

Pour sauter la lecture WBRS et d'anti-malware :

Remarque: Désactiver la lecture d'anti-malware (Webroot et/ou McAfee) pourrait être un risque de sécurité potentielle. Ceci devrait seulement être fait pour les sites qui peuvent sont de confiance de ne pas contenir le malware.