Contenu

Question :

Comment pousser un certificat racine auto-signé avec la stratégie de groupe ou le GPO ?

Remarque: Cet article de la base de connaissances met en référence le logiciel qui n'est pas mis à jour ou est pris en charge par Cisco. Les informations sont données comme courtoisie pour votre commodité. Pour davantage d'assistance, contactez s'il vous plaît le fournisseur de logiciels.

Avec la version 5.5.x et ultérieures d'AsyncOS, l'appliance de sécurité Web de Cisco fournit la capacité de déchiffrer le trafic HTTPS en activant le proxy HTTPS sous GUI > Services de sécurité > proxy HTTPS. Le déchiffrement HTTPS étant activé, les clients devraient faire confiance au certificat téléchargé ou généré sous la section de proxy HTTPS afin d'éviter de voir des erreurs de certificat sur des machines cliente.

des Certificats Auto-signés ou générés sur WSA ne seraient pas en soi faits confiance par les machines cliente et sinon ont été faits confiance, puis les clients devraient manuellement recevoir l'avertissement de certificat. Si nous ne voulons pas que tous les utilisateurs passent par les étapes de recevoir le certificat auto-signé non approuvé de Cisco WSA manuellement, alors nous pouvons pousser le certificat aux machines cliente par l'intermédiaire de la stratégie de groupe (GPO).

Veuillez se référer aux articles ci-dessous qui prévoient des détails sur la façon dont accomplir ceci :

Lien : http://www.unixwiz.net/techtips/deploy-webcert-gp.html

Lien : http://technet.microsoft.com/en-us/library/cc738131(v=ws.10).aspx

Lien : http://technet.microsoft.com/en-us/library/cc770315(v=ws.10).aspx