Les clients utilisant le proxy transparent doivent activement déchiffrer le trafic afin de distinguer YouTube.com et Google.com

Contenu

Problème

Les clients utilisant le proxy transparent doivent activement déchiffrer le trafic afin de distinguer YouTube.com et Google.com.

Environnement

Déploiement transparent de proxy, proxy HTTPS activé

Symptômes

Précédemment, Google a utilisé différents Certificats de serveur SSL pour chacun de leurs noms de domaine primaires. Ainsi si vous vous connectiez à https://www.google.com et à https://www.youtube.com, vous verriez différents Certificats de serveur, que chacun spécifier ce ils sont valables un de ces deux domaines.

Récemment, Google a commuté à utiliser un certificat de serveur simple SSL pour toutes leurs propriétés de Web, signé par leur propre CA interne. Ainsi si vous parcourez aux deux domaines répertoriés au-dessus d'utiliser le SSL, vous obtiendrez le même certificat. Que le certificat emploie une extension à « SubjectAltName » appelé par X.509 pour répertorier quelques douzaine domaines comme valides pour ce certificat. Une liste complète de domaines de Google qui sont valides pour ce nouveau certificat est ci-dessous.

Ceci fonctionne bien pour des navigateurs : votre navigateur sait qu'il essaye de se connecter à youtube.com, il voit un certificat qui est valide pour youtube.com (et une douzaine d'autres choses), et il permet la connexion de n'intervenir sans aucun avertissement.

Comment ceci affecte le WSA

Pour tout serveur proxy, la première chose que vous devez faire quand vous voyez qu'une demande d'un client est déterminent quelle destination de Web à la laquelle le client essaye d'aller. Pour le HTTP ordinaire, il est assez facile : regardez l'en-tête d'hôte dans la demande de HTTP.

Pour le SSL, c'est plus difficile. Dans le mode proxy explicite, le navigateur nous dit dans la requête de connexion, de sorte que soit facile. La difficulté est livré en mode transparent. Le déchiffrement étant activé sur le WSA, nous devons déterminer où l'utilisateur essaye de parcourir à avant déchiffrer réellement la connexion.

Aujourd'hui, nous faisons ceci en regardant l'adresse IP que le client essaye de se connecter à, en se connectant à cet IP nous-mêmes, et en regardant le certificat, en particulier, au champ NC. Ceci fonctionne bien quand une seule adresse Internet a son propre certificat de serveur SSL. Il permet également à des clients pour implémenter une certaine quantité d'application de stratégie pour le trafic SSL sans déchiffrer n'importe quoi, et ainsi sans distribuer le CERT CA du WSA à leurs clients. Un client peut permettre https://www.google.com mais le bloc https://www.youtube.com en plaçant le premier « laissent, ne déchiffrent pas » et le deuxième « à relâcher » dans la stratégie de déchiffrement.

Maintenant, youtube.com et google.com servent le même certificat de serveur. Ceci signifie qu'afin de distinguer les deux, WSA doit rechercher quelque chose autre que juste le certificat servi à l'adresse IP à laquelle le client essaye de se connecter.

La solution à cette question est dépistée comme ID de bogue Cisco 74969.

Solution

Si vous faites affecter une configuration par ceci, alors la solution immédiate est d'activer le déchiffrement actif du trafic SSL. Pour les clients qui n'ont pas précédemment distribué le certificat de CA du WSA, ils devront commencer faire ainsi. C'est la meilleure solution générale au problème.

Annexe

Liste de domaines pour lesquels le nouveau certificat de Google est valide :

Nom DNS : *.google.com
Nom DNS : google.com
Nom DNS : *.atggl.com
Nom DNS : *.youtube.com
Nom DNS : youtube.com
Nom DNS : *.ytimg.com
Nom DNS : * .google.com.br
Nom DNS : * .google.co.in
Nom DNS : *.google.es
Nom DNS : * .google.co.uk
Nom DNS : *.google.ca

Nom DNS : *.google.fr
Nom DNS : *.google.pt
Nom DNS : *.google.it
Nom DNS : *.google.de
Nom DNS : *.google.cl
Nom DNS : *.google.pl
Nom DNS : *.google.nl
Nom DNS : * .google.com.au
Nom DNS : * .google.co.jp
Nom DNS : *.google.hu
Nom DNS : * .google.com.mx
Nom DNS : * .google.com.ar
Nom DNS : * .google.com.co
Nom DNS : * .google.com.vn
Nom DNS : * .google.com.tr
Nom DNS : *.android.com
Nom DNS : *.googlecommerce.com