

Sécurité Web de nuage : Redirection régionale avec Google

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Informations générales](#)

[Problème](#)

[Solution](#)

[Informations connexes](#)

Introduction

Ce document décrit comment résoudre le problème de réorienter des demandes de Google à une région inattendue, tout en utilisant le service de la sécurité Web de nuage de Cisco (CWS).

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

[Composants utilisés](#)

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

[Informations générales](#)

Cisco opacifiant la sécurité Web (CWS) est une solution de sécurité basée par nuage qui utilise des serveurs proxys situés dans les centres de traitement des données autour du monde. Des utilisateurs provisionnés sur un proxy près de leur situation géographique pour assurer la meilleure représentation, aussi bien que la livraison du contenu régional approprié.

Quand un utilisateur parcourt à un site Web par l'intermédiaire du service CWS, des insertions CWS X-Expédier-pour les en-têtes (XFF) dans chaque demande de HTTP. Ceci permet à Google pour identifier l'adresse IP source de la demande (votre IP réel de sortie) plutôt que l'adresse IP du proxy CWS. C'est particulièrement important pour les utilisateurs qui sont dans une région

différente au proxy CWS le plus étroit. Par exemple, des utilisateurs en Espagne typiquement provisionnés sur un proxy au R-U ; le centre de traitement des données le plus étroit à leur situation géographique. Sans ajout de l'en-tête XFF, Google réorienterait des demandes à google.co.uk au lieu de google.es.

En 2013, Google a mis à jour le comportement par défaut de page de recherche qui a réorienté toutes les demandes de HTTP à HTTPS. Ceci empêche CWS d'insérer l'en-tête XFF parce que la connexion est maintenant chiffrée. Afin d'insérer l'en-tête XFF sur une connexion cryptée, la caractéristique d'inspection HTTPS doit être activée dans le portail CWS. Autrement, la décision régionale de la redirection de Google sera basée sur l'IP de sortie du proxy CWS.

Problème

Quand un utilisateur parcourt à Google par l'intermédiaire du service CWS, ils sont réorientés à une région inattendue. Par exemple, un utilisateur à Miami parcourt à Google.com, mais est réorienté à Google Mexique (Google.com.mx), qui fait être la page retournée de recherche dans l'Espagnol.

Solution

Cisco a fonctionné avec Google pour développer un whitelist des adresses IP de sortie de proxy CWS. Au cas où CWS ne fournirait pas l'en-tête XFF (pour des demandes non-examinées HTTPS), la demande sera réorientée au domaine régional de Google, basé sur le whitelist.

Avec cette solution en place, si CWS ne peut pas ajouter l'en-tête XFF, ou si Google n'identifie pas l'adresse IP de sortie CWS, l'utilisateur peut encore être réorienté à une région inattendue. À ces occasions, le seul contournement disponible du côté CWS est d'activer l'inspection HTTPS. Cependant, ce problème pourrait également se poser quand Google reçoit l'en-tête XFF, mais met en référence des données incorrectes de Geo-emplacement pour l'adresse IP de sortie de l'utilisateur. À ces occasions, la question ne peut pas être résolue par CWS.

- Si Google assigne un Geo-emplacement incorrect à votre IP de sortie, vous pouvez signaler la question à Google. Référez-vous à <https://support.google.com/websearch/answer/873?hl=en> pour plus de détails.
- Si vous souhaitez sauter la redirection régionale pour visiter Google.com au lieu du site local de Google, utilisez <http://www.google.com/ncr>

Informations connexes

- [Support et documentation techniques - Cisco Systems](#)