Segurança da Web da nuvem: Reorientação regional com Google

Índice

Introdução

Este documento descreve como resolver o problema de reorientar pedidos de Google a uma região inesperada, ao usar o serviço da Segurança da Web da nuvem de Cisco (CWs).

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Informações de Apoio

Cisco nubla-se a Segurança da Web (CWs) é uma solução baseada nuvem da Segurança que utilize os servidores proxy situados nos centros de dados em todo o mundo. Os usuários são fornecida em um proxy perto de sua localização geográfica assegurar o melhor desempenho, assim como na entrega do índice regional apropriado.

Quando um usuário consultar a um Web site através do serviço CWs, inserções CWs X-Enviar-para os encabeçamentos (XFF) em cada pedido do HTTP. Isto permite que Google identifique o endereço IP de origem do pedido (seu IP real da saída) um pouco do que o endereço IP de Um ou Mais Servidores Cisco ICM NT do proxy CWs. Isto é particularmente importante para os

usuários que estão em uma região diferente ao proxy o mais próximo CWs. Por exemplo, os usuários na Espanha seriam tipicamente fornecida em um proxy no UK; o centro de dados o mais próximo a sua localização geográfica. Sem a adição do encabeçamento XFF, Google reorientaria pedidos a google.co.uk em vez de google.es.

Em 2013, Google atualizou o comportamento da página de pesquisa do padrão que reorientou todos os pedidos do HTTP ao HTTPS. Isto impede que o CWs introduza o encabeçamento XFF porque a conexão é cifrada agora. A fim introduzir o encabeçamento XFF em uma conexão criptografada, a característica da inspeção HTTPS deve ser permitida no portal CWs. Se não, a decisão de redirecionamento regional de Google será baseada no IP da saída do proxy CWs.

Problema

Quando um usuário consulta a Google através do serviço CWs, estão reorientados a uma região inesperada. Por exemplo, um usuário em Miami consulta a Google.com, mas é reorientado a Google México (Google.com.mx), que faz com que a página de pesquisa retornada esteja no espanhol.

Solução

Cisco trabalhou com Google para desenvolver um whitelist de endereços IP de Um ou Mais Servidores Cisco ICM NT da saída do proxy CWs. Caso o CWs não fornecer o encabeçamento XFF (para pedidos NON-inspecionados HTTPS), o pedido estará reorientado ao domínio regional de Google, com base no whitelist.

Com esta solução no lugar, se o CWs é incapaz de adicionar o encabeçamento XFF, ou se Google não identifica o endereço IP de Um ou Mais Servidores Cisco ICM NT da saída CWs, o usuário pode ainda ser reorientado a uma região inesperada. Nestas ocasiões, a única ação alternativa disponível no lado CWs é permitir a inspeção HTTPS. Contudo, este problema pôde igualmente ocorrer quando Google recebe o encabeçamento XFF, mas provê dados incorretos do GEO-lugar para o endereço IP de Um ou Mais Servidores Cisco ICM NT da saída do usuário. Nestas ocasiões, a edição não pode ser resolvida pelo CWs.

- Se Google atribui um GEO-lugar incorreto a seu IP da saída, você pode relatar a edição a Google. Refira https://support.google.com/websearch/answer/873?hl=en para mais detalhes.
- Se você deseja contornear a reorientação regional para visitar Google.com em vez do local local de Google, use http://www.google.com/ncr

Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems