Contenido

Problema

Los clientes que usan el proxy transparente deben desencriptar activamente el tráfico para distinguir entre YouTube.com y Google.com.

Entorno

Despliegue del proxy transparente, proxy HTTPS habilitado

Síntomas

Previamente, Google utilizó diversos Certificados de servidor SSL para cada uno de sus Domain Name primarios. Tan si usted conectara con https://www.google.com y https://www.youtube.com, usted vería diversos certificados de servidor, cada uno especificando que son válidos para uno de esos dos dominios.

Recientemente, Google ha conmutado a usar un solo certificado de servidor SSL para todas sus propiedades Web, firmado por su propio CA interno. Tan si usted hojea a los dos dominios enumerados sobre usar el SSL, usted conseguirá el mismo certificado. Que el certificado utiliza una extensión al X.509 llamó “SubjectAltName” para enumerar algunos docena dominios como válidos para ese certificado. Una lista completa de dominios de Google que sean válidos para este nuevo certificado está abajo.

Esto trabaja muy bien para los navegadores: su navegador sabe que está intentando conectar con youtube.com, ve un certificado que sea válido para youtube.com (y otra docena de cosas), y deja la conexión ir a través sin ningunas advertencias.

Cómo esto afecta el WSA

Para cualquier servidor proxy, la primera cosa que usted necesita hacer cuando usted ve que es una petición de un cliente determina qué destino de la red al cual el cliente está intentando ir. Para el HTTP llano, es bastante fácil: mire la encabezado del host en el pedido de HTTP.

Para el SSL, es más difícil. En el modo de representación explícito, el navegador nos dice en el pedido de conexión, de modo que sea fácil. La dificultad viene en el modo transparente. Con el desciframiento habilitado en el WSA, necesitamos determinar donde el usuario está intentando hojear antes realmente a desencriptar la conexión.

Hoy, hacemos esto mirando la dirección IP que el cliente está intentando conectar con, conectando con ese IP nosotros mismos, y mirando el certificado, particularmente, el campo CN. Esto trabaja bien cuando un nombre de host único tiene su propio certificado de servidor SSL. También permite que los clientes implementen una cierta cantidad de aplicación de políticas para el tráfico SSL sin desencriptar cualquier cosa, y así sin la distribución del CERT CA WSA a sus clientes. Un cliente puede permitir https://www.google.com pero el bloque https://www.youtube.com fijando el primer “permite, no desencripta” y el segundo “a caer” en la política de descifrado.

Ahora, youtube.com y google.com sirven para arriba el mismo certificado de servidor. Esto significa que para distinguir entre los dos, WSA tiene que buscar algo con excepción apenas del certificado servido para arriba en la dirección IP con la cual el cliente está intentando conectar.

La solución a este problema se está siguiendo como Id. de bug Cisco 74969.

Solución

Si usted hace una configuración afectar por esto, después la solución inmediata es girar el desciframiento activo del tráfico SSL. Para los clientes que no han distribuido previamente el certificado de CA del WSA, necesitarán comenzar a hacer tan. Ésta es la mejor solución general al problema.

Apéndice

Lista de dominios para los cuales el nuevo certificado de Google es válido:

Nombre DNS: *.google.com
Nombre DNS: google.com
Nombre DNS: *.atggl.com
Nombre DNS: *.youtube.com
Nombre DNS: youtube.com
Nombre DNS: *.ytimg.com
Nombre DNS: * .google.com.br
Nombre DNS: * .google.co.in
Nombre DNS: *.google.es
Nombre DNS: * .google.co.uk
Nombre DNS: *.google.ca
Nombre DNS: *.google.fr
Nombre DNS: *.google.pt
Nombre DNS: *.google.it
Nombre DNS: *.google.de
Nombre DNS: *.google.cl
Nombre DNS: *.google.pl
Nombre DNS: *.google.nl

Nombre DNS: * .google.com.au
Nombre DNS: * .google.co.jp
Nombre DNS: *.google.hu
Nombre DNS: * .google.com.mx
Nombre DNS: * .google.com.ar
Nombre DNS: * .google.com.co
Nombre DNS: * .google.com.vn
Nombre DNS: * .google.com.tr
Nombre DNS: *.android.com
Nombre DNS: *.googlecommerce.com