Содержание

Проблема

Клиенты, использующие режим прозрачного прокси, должны активно дешифровать трафик для различения YouTube.com и Google.com.

Среда

Развертывания Режима прозрачного прокси, Прокси HTTPS включен

Признаки

Ранее, Google использовал другие сертификаты SSL - сервера для каждого из их названий основного домена. Таким образом, если бы вы соединились с https://www.google.com и https://www.youtube.com, то вы видели бы другие серверные сертификаты, каждый указывающий, что они допустимы для одного из тех двух доменов.

Недавно, Google переключился к использованию одиночного сертификата SSL - сервера для всех их вебов - свойств, подписанных их собственным внутрифирменным CA. Поэтому, если вы перейдете к этим двум доменам, упомянутым выше с помощью SSL, то вы получите тот же сертификат. Тот сертификат использует расширение для X.509 по имени "SubjectAltName" для распечатки нескольких дюжин доменов как допустимых для того сертификата. Полный список доменов Google, которые допустимы для этого нового сертификата, ниже.

Это хорошо работает для браузеров: ваш браузер знает, что пытается соединиться с youtube.com, он видит сертификат, который допустим для youtube.com (и дюжина других вещей), и он позволяет соединению пройти без любых предупреждений.

Как это влияет на WSA

Для любого прокси-сервера первая вещь необходимо сделать, когда вы видите, что запрос от клиента, определяют, какое веб-назначение, к которому клиент пытается перейти. Для простого HTTP это довольно легко: посмотрите на заголовок Хоста в запросе HTTP.

Для SSL это более трудно. В явном режиме proxy браузер говорит нам в Запросе соединения, так, чтобы было легко. Трудность прибывает в прозрачный режим. С расшифровкой, включенной на WSA, мы должны определить, где пользователь пытается перейти к прежде фактически дешифровать соединение.

Сегодня, мы делаем это путем рассмотрения IP-адреса, с которым клиент пытается соединиться, соединяясь с тем IP сами, и смотря на сертификат, в частности в поле CN. Когда уникальное имя хоста имеет свой собственный сертификат SSL - сервера, это работает хорошо. Это также позволяет клиентам внедрять некоторую сумму принудительной политики для трафика SSL, ничего не дешифруя, и таким образом не распределяя свидетельство CA WSA их клиентам. Клиент может позволить https://www.google.com , но заблокироваться , https://www.youtube.com , заставляя первое "позволить, сделать не дешифруют" и второе для "понижений" в политике расшифровки.

Теперь, youtube.com и google.com подают тот же серверный сертификат. Это означает, что для различения эти два, WSA должен искать что-то другое, чем просто сертификат, поданный в IP-адресе, с которым клиент пытается соединиться.

Решение этой проблемы отслеживается как идентификатор ошибки Cisco 74969.

Решение

Если вам влияло на конфигурацию это, то немедленное решение должно включить активную расшифровку трафика SSL. Для клиентов, которые ранее не распределили сертификат CA от WSA, они должны будут начать делать так. Это - лучшее общее решение к проблеме.

Приложение

Список доменов, для которых новый сертификат Google допустим:

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

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