使用透明代理的客户必须积极地解密流量为了区分在YouTube.com和Google.com之间

目录

问题

使用透明代理的客户必须积极地解密流量为了区分在YouTube.com和Google.com之间。

环境

透明代理部署， HTTPS代理启用

症状

以前，谷歌使用了不同的SSL服务器证书他们的每一个主要的域名。因此，如果连接对https://www.google.com和https://www.youtube.com，您会看到不同的服务器证书，其中每一指定他们是有效在那两个域之一内。

最近，谷歌交换对使用单个SSL服务器证书所有他们的Web属性，签字由他们自己的内部的CA。因此，如果浏览对在使用SSL上列出的两个域，您将获得同一证书。证书使用一分机对X.509呼叫“SubjectAltName”列出一些十二个域如有效为该证书。的谷歌域详尽列表为此新证书是有效下面。

这为浏览器良好工作：您的浏览器知道它尝试连接到youtube.com，看到为youtube.com的证书(和其他几件事)是有效，并且让连接经历，不用任何警告。

这如何影响WSA

任何代理服务器，您需要做的第一件事，当您看到从客户端的一请求是确定客户端尝试去的什么Web目的地。对于无格式HTTP，是相当容易：查看在HTTP请求的主机报头。

对于SSL，这是更加困难。在明确代理模式，浏览器在连接请求告诉我们，因此是容易。困难进来透明模式。当解密启用在WSA，我们需要确定用户哪里尝试浏览到在实际解密连接前。

今天，我们通过查看客户端尝试连接对的IP地址，连接对该IP我们自己和查看证书执行此，特别是，CN字段。当一唯一主机名有其自己的SSL服务器证书时，这工作良好。它也允许客户实现某相当数量SSL流量的策略执行，无需解密任何东西和因而，无需分配WSA的CA cert对他们的客户端。客户能允许https://www.google.com，但是块https://www.youtube.com通过设置第一“准许，不解密”和“丢弃的”第二个在解密策略。

现在， youtube.com和google.com服务同一服务器证书。这意味着为了区分在两个之间， WSA必须寻找某事除证书之外服务在客户端尝试连接的IP地址。

对此问题的解决方案被跟踪作为Cisco Bug ID 74969。

解决方案

如果安排一配置影响受此的，则直接解决方案将打开SSL流量的活动解密。对于以前未分配从WSA的CA证书的客户，他们将需要开始如此执行。这是最好的方案对问题。

附录

谷歌的新证书是有效域的列表：

DNS名：*.google.com
DNS名： google.com
DNS名：*.atggl.com
DNS名：*.youtube.com
DNS名： youtube.com
DNS名：*.ytimg.com
DNS名：* .google.com.br
DNS名：* .google.co.in
DNS名：*.google.es
DNS名：* .google.co.uk
DNS名：*.google.ca
DNS名：*.google.fr
DNS名：*.google.pt
DNS名：*.google.it
DNS名：*.google.de
DNS名：*.google.cl
DNS名：*.google.pl
DNS名：*.google.nl
DNS名：* .google.com.au
DNS名：* .google.co.jp
DNS名：*.google.hu
DNS名：* .google.com.mx
DNS名：* .google.com.ar
DNS名：* .google.com.co
DNS名：* .google.com.vn
DNS名：* .google.com.tr
DNS名：*.android.com
DNS名：*.googlecommerce.com