透過型プロキシを使用しているユーザは YouTube.com と Google.com を区別するためにトラフィックをアクティブに復号化する必要がある

目次

問題

透過型プロキシを使用しているお客様は、YouTube.com と Google.com を区別するためにトラフィックをアクティブに復号化する必要があります。

環境

透過型プロキシ導入、HTTPS プロキシが有効になっている

症状

これまで、Google は、プライマリ ドメイン名ごとに異なる SSL サーバ証明書を使用していました。 そのため、https://www.google.com と https://www.youtube.com に接続すると、この 2 つのドメインのどちらかに対して有効なことを示す別々のサーバ証明書が表示されました。

最近、Google は、自社のすべての Web プロパティに対して、自社の CA によって署名された単一の SSL サーバ証明書を使用するように切り替えました。 そのため、SSL を使用して上記 2 つのドメインを参照すると、同じ証明書が表示されます。 この証明書では、有効な数十個のドメインを列挙する "SubjectAltName" という名前の X.509 に対する拡張が使用されています。 この新しい証明書に対して有効な Google ドメインの完全なリストを以下に示します。

この拡張はブラウザで正常に動作します。 ブラウザは、それが youtube.com に接続しようとしていることを認識して、youtube.com (およびその他の 10 個ほどのドメイン) に対して有効な証明書を確認し、その接続を警告なしで許可します。

WSA に対する影響

プロキシ サーバでクライアントから要求を受け取ったときにまずやらなければならないことは、クライアントがアクセスしようとしている Web 宛先を特定することです。 単純な HTTP では、極めて簡単です。 HTTP 要求内のホスト ヘッダーを検査するだけです。

SSL では、少し難しくなります。 明確なプロキシ モードでは、ブラウザは CONNECT 要求で指示するだけなので簡単です。 トランスペアレント モードでは複雑になります。 WSA で復号化が有効になっている場合は、実際に接続を復号化する前に、ユーザが参照しようとしている場所を特定する必要があります。

現在、これを行うには、クライアントが接続しようとしている IP アドレスを検査して、その IP に自ら接続し、証明書、特に CN フィールドを検査します。 これは、一意のホスト名に独自の SSL サーバ証明書が割り当てられている場合にうまく機能します。 また、お客様は、何も復号化せずに、つまり、WSA の CA 証明書をクライアントに配布せずに、SSL トラフィックに対して一定量のポリシーを適用することができます。 https://www.google.com は許可するが、https://www.youtube.com はブロックする場合は、復号化ポリシーで前者を "allow, don't decrypt" に設定し、後者を "drop" に設定します。

これで、youtube.com と google.com が同じサーバ証明書を表示します。 これは、2 つのドメインを区別するために、WSA が、クライアントが接続しようとしている IP アドレスで表示される証明書以外の証明書を探す必要があることを意味します。

この問題の解決策は、Cisco Bug ID 74969 として追跡されています。

解決策

設定がこの影響を受ける場合の緊急措置は、SSL トラフィックの復号化を有効にすることです。 WSA から CA 証明書を配布したことがないお客様は、そうすることから始める必要があります。 これが問題に対する最も一般的な解決策です。

付録

Google の新しい証明書が有効になっているドメインのリスト：

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