How do I get Google Earth to work with the Cisco Web Security Appliance?

Document ID: 117943

Contributed by Madhura Kumar and Siddharth Rajpathak, Cisco TAC Engineers.

Jul 15, 2014

Contents

Question

How do I get Google Earth to work with the Cisco Web Security Appliance?

Environment

Google Earth 4.2

Symptoms

The application Google Earth does not work when the client is connected to the Cisco Web Security appliance (WSA). This can be a result of proxy settings on the client or authentication requirements of the WSA.

Case 1

When you are using Google Earth through the WSA, error code 26 or a message indicating that servers can't be reached is seen. If WSA is set up in explicit mode in the network, you will need to configure Google Earth to use the proxy.

This can be done by making some changes in Internet Explorer:

1. Click "Start" and select "Control Panel."
2. Double−click "Internet Options."
3. Select the "Connections" tab.
4. Click "LAN Settings."
5. Under "Proxy server," select "Use a proxy server for your LAN" and enter the proxy information.
6. Once this has been completed, select "OK" to save these changes.

Case 2

Google Earth is not working through the WSA with a message indicating failed authentication/credentials required. In cases where authentication is required to process a request, Google Earth will need a way to authenticate. To work around this issue, we will need to exempt authentication for the Google Earth servers.

To exempt Google Earth from Authentication Exemption:

For AsyncOS versions below 6.x:

1. On WSA GUI, browse to "Web Security Manager".
2. Select Destination Authentication Exemptions > Destinations.
3. Add the addresses − kh.google.com, geo.keyhole.com and auth.keyhole.com, .pack.google.com, pack.google.com, mw1.google.com, clients1.google.com, earth.google.com, maps.google.com, maps.gstatic.com, csi.gstatic.com and .gstatic.com.
4. Commit the changes.

For AsyncOS 6.x and later:

1. Create a new custom URL policy called "Destination Authentication Exemption Destinations" and add kh.google.com, geo.keyhole.com, auth.keyhole.com, .pack.google.com, pack.google.com, mw1.google.com, clients1.google.com, earth.google.com, maps.google.com and maps.gstatic.com to the list.
2. Create an identity called "application bypass identity" and set it to no authentication required. In the advanced section, select the URL category named "Destination Authentication Exemption Destinations".
3. Create an access policy called "application bypass policy" and assign the "application bypass identity" to it. You will now be bypassing Google Earth requests for authentication.

Case 3

If network traffic is being transparently being redirected to WSA, the Google Earth client is unable to respond to transparent authentication requests and failure occurs.

In these scenarios, WSA can be configured to cache user credentials based on the client's IP address. In this case, as long as there has been prior web traffic from the client, the Google Earth client would not need to be re−authenticated.

For AsyncOS 6.x and later, this can be configured under: Network > Authentication > Surrogate Type: IP Address.

Updated: Jul 15, 2014 Document ID: 117943