Contenu

Question

Comment est-ce que j'obtiens Google Earth pour travailler avec l'appliance de sécurité Web de Cisco ?

Environnement

Google Earth 4.2

Symptômes

L'application Google Earth ne fonctionne pas quand le client est connecté à l'appliance de sécurité Web de Cisco (WSA). Ceci peut être un résultat des paramètres de proxy sur les exigences de client ou d'authentification du WSA.

Affaire 1

Quand vous utilisez Google Earth par le WSA, code d'erreur 26 ou un message indiquant que des serveurs ne peuvent pas être atteints est vu. Si WSA est installé en mode explicite dans le réseau, vous devrez configurer Google Earth pour utiliser le proxy.

Ceci peut être fait en apportant quelques modifications en Internet Explorer :

1. Cliquez sur le « début » et sélectionnez le « panneau de configuration. »
2. Double clic « options Internet. »
3. Sélectionnez l'onglet de « connexions ».
4. Clic « configurations de RÉSEAU LOCAL. »
5. Sous le « serveur proxy, utilisation » choisie la « un serveur proxy pour votre RÉSEAU LOCAL » et écrivent les informations de proxy.
6. Une fois que ceci a été terminé, sélectionnez « CORRECT » pour sauvegarder ces modifications.

Affaire 2

Google Earth ne fonctionne pas par le WSA avec un message indiquant l'authentification défaillante/qualifications exigées. Dans les cas où l'authentification est exigée pour traiter une demande, Google Earth aura besoin d'une manière d'authentifier. Pour fonctionner autour de cette question, nous devrons exempter l'authentification pour les serveurs de Google Earth.

Pour exempter Google Earth d'exemption d'authentification :

Pour des versions d'AsyncOS au-dessous de 6.x :

1. Sur le GUI WSA, parcourez au « *gestionnaire de sécurité Web* ».
2. *Exemptions* choisies *> destinations d'authentification de destination.*
3. Ajoutez les adresses - kh.google.com, geo.keyhole.com et 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 et .gstatic.com.
4. Commettez les modifications.

Pour AsyncOS 6.x et plus tard :

1. Créez nouvelle *destinations d'une exemption d'authentification de destination »* appelées URL de coutume les « par stratégie et ajoutez 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 et maps.gstatic.com à la liste.
2. Créez une identité appelée « l'identité de contournement d'application » et placez-la à aucune authentification requise. Dans la section avancée, sélectionnez la catégorie URL nommée « des *destinations d'exemption d'authentification de destination ».*
3. Créez une stratégie d'accès appelée « la stratégie de contournement d'application » et assignez-« l'identité de contournement d'application » elle. Vous sauterez maintenant des demandes de Google Earth de l'authentification.

Affaire 3

Si le trafic réseau d'une manière transparente est réorienté à WSA, le client de Google Earth ne peut pas répondre aux demandes d'authentification transparentes et la panne se produit.

Dans ces scénarios, WSA peut être configuré pour cacher des identifiants utilisateurs basés sur l'adresse IP du client. Dans ce cas, tant que il y a eu du trafic web antérieur du client, le client de Google Earth n'aurait pas besoin d'être authentifié à nouveau.

Pour AsyncOS 6.x et plus tard, ceci peut être configuré dessous : *Réseau > authentification > type de substitut : Adresse IP.*