Wie kann ich Google Earth dazu bringen, mit der Cisco Web Security Appliance zu arbeiten?

Inhalt

Frage

Wie kann ich Google Earth dazu bringen, mit der Cisco Web Security Appliance zu arbeiten?

Umgebung

Google Earth 4.2

Symptome

Die Anwendung Google Earth funktioniert nicht, wenn der Client mit der Cisco Web Security Appliance (WSA) verbunden ist. Dies kann auf Proxyeinstellungen auf dem Client oder Authentifizierungsanforderungen der WSA zurückzuführen sein.

Fall 1

Wenn Sie Google Earth über die WSA verwenden, wird der Fehlercode 26 oder eine Meldung angezeigt, dass Server nicht erreicht werden können. Wenn die WSA im Netzwerk im expliziten Modus eingerichtet ist, müssen Sie Google Earth so konfigurieren, dass der Proxy verwendet wird.

Nehmen Sie dazu einige Änderungen in Internet Explorer vor:

1. Klicken Sie auf "Start" und wählen Sie "Systemsteuerung" aus.
2. Doppelklicken Sie auf "Internetoptionen".
3. Wählen Sie die Registerkarte "Verbindungen" aus.
4. Klicken Sie auf "LAN-Einstellungen".
5. Wählen Sie unter "Proxy-Server" die Option "Proxy-Server für Ihr LAN verwenden" aus, und

geben Sie die Proxyinformationen ein.
6. Klicken Sie nach dem Speichern auf "OK", um die Änderungen zu speichern.

Fall 2

Google Earth arbeitet nicht über die WSA, und es wird eine Meldung angezeigt, dass eine fehlgeschlagene Authentifizierung/Anmeldeinformationen erforderlich ist. In Fällen, in denen eine Authentifizierung zur Bearbeitung einer Anfrage erforderlich ist, benötigt Google Earth eine Authentifizierungsmethode. Um dieses Problem zu umgehen, müssen wir die Authentifizierung für die Google Earth-Server ausnehmen.

So nehmen Sie Google Earth von der Authentifizierungsfreistellung aus:

Für AsyncOS-Versionen unter 6.x:

1. Navigieren Sie in der WSA-GUI zu "*Web Security Manager*".
2. Wählen Sie *Zielauthentifizierungsausnahmen > Ziele aus.*
3. Fügen Sie die Adressen hinzu: kh.google.com, geo.keyhole.com und 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 und .gstatic.com.
4. Bestätigen Sie die Änderungen.

Für AsyncOS 6.x und höher:

1. Erstellen Sie eine neue benutzerdefinierte URL-Richtlinie mit dem Namen "*Destination Authentication Exemption Destorities"* und fügen Sie 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.com hinzu. und maps.gstatic.com zur Liste.
2. Erstellen Sie eine Identität namens "Application Bypass Identity", und legen Sie sie auf "no authentication required" fest. Wählen Sie im erweiterten Abschnitt die URL-Kategorie mit dem Namen "*Ziel-Authentifizierungsausnahmeziele" aus.*
3. Erstellen Sie eine Zugriffsrichtlinie mit der Bezeichnung "Application Bypass Policy" (Umgehungsrichtlinie für Anwendungen), und weisen Sie ihr die "Application Bypass Identity" zu. Sie umgehen nun die Authentifizierungsanforderungen von Google Earth.

Fall 3

Wenn der Netzwerkverkehr transparent an die WSA umgeleitet wird, ist der Google Earth-Client nicht in der Lage, auf transparente Authentifizierungsanforderungen zu reagieren, und es tritt ein Fehler auf.

In diesen Szenarien kann die WSA so konfiguriert werden, dass Benutzeranmeldeinformationen auf der Grundlage der IP-Adresse des Clients zwischengespeichert werden. In diesem Fall müsste der Google Earth-Client nicht erneut authentifiziert werden, solange der Client zuvor über das Internet kommuniziert hat.

Für AsyncOS 6.x und höher kann dies wie folgt konfiguriert werden: *Netzwerk > Authentifizierung > Surrogattyp: IP-Adresse.*