

Come posso fare in modo che Google Earth lavori con Cisco Web Security Appliance?

Sommario

[Domanda](#)

[Ambiente](#)

[Sintomi](#)

[Caso 1](#)

[Caso 2](#)

[Caso 3](#)

Domanda

Come posso fare in modo che Google Earth lavori con Cisco Web Security Appliance?

Ambiente

Google Earth 4.2

Sintomi

L'applicazione Google Earth non funziona quando il client è collegato a Cisco Web Security Appliance (WSA). Ciò può essere dovuto alle impostazioni proxy sul client o ai requisiti di autenticazione del server WSA.

Caso 1

Quando si utilizza Google Earth tramite WSA, viene visualizzato il codice di errore 26 o un messaggio che indica che non è possibile raggiungere i server. Se WSA è configurato in modalità esplicita nella rete, è necessario configurare Google Earth per l'utilizzo del proxy.

A tale scopo, è possibile apportare alcune modifiche in Internet Explorer:

1. Fare clic su Start e selezionare Pannello di controllo.
2. Fare doppio clic su "Opzioni Internet".
3. Selezionare la scheda "Connessioni".
4. Fare clic su Impostazioni LAN.
5. In "Proxy server", selezionare "Use a proxy server for your LAN" e immettere le informazioni

sul proxy.

6. Al termine, selezionare "OK" per salvare le modifiche.

Caso 2

Google Earth non funziona tramite WSA con un messaggio che indica che l'autenticazione o le credenziali richieste non sono riuscite. Nei casi in cui è richiesta l'autenticazione per elaborare una richiesta, Google Earth avrà bisogno di un modo per autenticarsi. Per risolvere questo problema, sarà necessario esentare l'autenticazione per i server Google Earth.

Per esentare Google Earth dall'esenzione dall'autenticazione:

Per le versioni AsyncOS inferiori a 6.x:

1. Dalla GUI di WSA, selezionare "*Web Security Manager*".
2. Selezionare *Esenzioni autenticazione destinazione > Destinazioni*.
3. Aggiungere gli indirizzi: kh.google.com, geo.keyhole.com e 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 e .gstatic.com.
4. Eseguire il commit delle modifiche.

Per AsyncOS 6.x e versioni successive:

1. Creare un nuovo criterio URL personalizzato denominato "*Destination Authentication Exemption Destinations*" e aggiungere 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 e maps.gstatic.com all'elenco.
2. Creare un'identità denominata "application bypass identity" e impostarla su no authentication required. Nella sezione Advanced (Avanzate), selezionare la categoria URL denominata "*Destination Authentication Exemption Destinations*" (*Destinazioni di esenzione autenticazione destinazione*).
3. Creare un criterio di accesso denominato "criterio di bypass dell'applicazione" e assegnarvi l'identità di bypass dell'applicazione. Le richieste di autenticazione di Google Earth verranno ignorate.

Caso 3

Se il traffico di rete viene reindirizzato in modo trasparente a WSA, il client Google Earth non è in grado di rispondere a richieste di autenticazione trasparenti e si verifica un errore.

In questi scenari, WSA può essere configurato in modo da memorizzare nella cache le credenziali utente in base all'indirizzo IP del client. In questo caso, se il traffico Web proveniente dal client è già passato, il client Google Earth non dovrà essere riautenticato.

Per AsyncOS 6.x e versioni successive, è possibile configurare questa opzione in: *Rete > Autenticazione > Tipo surrogato: Indirizzo IP*.