

# Domande frequenti di Cisco Umbrella sul geoblocking basato su IP

## Sommario

---

### [Introduzione](#)

[Cosa succede se i miei utenti nelle regioni interessate si connettono a una VPN aziendale al di fuori delle regioni interessate, che a sua volta si connette a Umbrella?](#)

[Perché Cisco sta facendo questo?](#)

[Cosa succede se gli utenti vengono bloccati ma non si trovano in una delle regioni colpite?](#)

[Quanto sono accurati i vostri dati geobloccanti?](#)

[Cosa fare se la posizione associata all'indirizzo IP è errata?](#)

---

## Introduzione

Questo documento descrive i cambiamenti di comportamento mostrati ai clienti di Cisco Umbrella e OpenDNS in Russia e Bielorussia a partire dal 1 agosto. Questi cambiamenti di comportamento si applicano anche ad altre regioni per cui Cisco Umbrella implementa il geoblocking basato su IP. Questo documento è stato aggiornato l'ultima volta il 28 luglio 2022.

### Clienti DNS:

- Il servizio DNS per le query provenienti da indirizzi IP identificati come provenienti da Russia, Bielorussia, Crimea, Luhansk, Donetsk, Siria, Cuba, Iran, Corea del Nord e altre regioni sanzionate con geobloccaggio non deve applicare politiche di sicurezza o di filtraggio dei contenuti. Le query DNS ricevono ancora una risposta valida e vengono gestite con lo stesso livello di servizio del traffico proveniente dal resto del mondo.
- Quando utilizzato per il DNS, il modulo di sicurezza in roaming Umbrella e il modulo di roaming AnyConnect Umbrella continuano a risolvere il traffico DNS.
- La sincronizzazione dei client mobili e gli elenchi dei domini interni possono continuare a essere sincronizzati con il dashboard e fornire il comportamento previsto (invio dei domini interni al server DNS interno). Questo può cambiare in futuro.

### Clienti SIG:

- I server gateway Web sicuri Umbrella non accettano il traffico in cui l'IP originale proviene da Russia, Bielorussia, Crimea, Luhansk, Donetsk, Siria, Cuba, Iran, Corea del Nord e altre regioni sanzionate con geo-blocco. L'implementazione di questa funzionalità consente alle connessioni provenienti da queste aree di visualizzare i server Cisco Umbrella come non in linea o non disponibili. Traffico non accettato o elaborato.
- La configurazione predefinita del modulo AnyConnect Umbrella fa in modo che si connetta direttamente a Internet quando Umbrella non è disponibile. Alcune configurazioni specifiche dei clienti possono funzionare in modalità "fail-closed", che causerebbe la perdita

dell'accesso a Internet da parte degli utenti.

- Per il momento, l'elenco dei domini esterni continua a essere sincronizzato per ottenere gli aggiornamenti da Umbrella. Questo può cambiare in futuro.
- Il file PAC predefinito Umbrella fa sì che si connetta direttamente a Internet quando Umbrella non è disponibile. Alcune configurazioni specifiche del cliente (ad esempio, quelle senza un percorso predefinito) possono "non essere chiuse", causando la perdita dell'accesso a Internet da parte degli utenti.
- I tunnel IPsec vengono disconnessi tramite il blocco IP o la revoca delle credenziali IKE. Il comportamento e l'esperienza dell'utente dipendono dalla configurazione specifica del cliente. Alcune configurazioni possono tornare alla connessione diretta a Internet, altre possono tornare a MPLS e altre possono causare la perdita dell'accesso a Internet da parte degli utenti.

Tutti i clienti:

- Una volta implementato il geoblocking basato su IP per un determinato paese, vengono bloccati anche l'accesso alle API e ai dashboard Umbrella.

## Cosa succede se i miei utenti nelle regioni interessate si connettono a una VPN aziendale al di fuori delle regioni interessate, che a sua volta si connette a Umbrella?

Il nostro geoblocking è basato su IP, basato sull'indirizzo IP di origine visto dal servizio Umbrella.

## Perché Cisco sta facendo questo?

Vi invitiamo a visitare [la pagina The War in Ukraine: Per](#) ulteriori informazioni, [contattare i clienti, i partner e](#) le [comunità](#).

## Cosa succede se gli utenti vengono bloccati ma non si trovano in una delle regioni colpite?

Per [ottenere](#) informazioni sull'emissione, [contattare](#) l'[assistenza](#).

## Quanto sono accurati i vostri dati geobloccanti?

Utilizziamo i servizi di geolocalizzazione leader del settore per determinare il paese per un determinato indirizzo IP.

## Cosa fare se la posizione associata all'indirizzo IP è errata?

È consigliabile inviare una richiesta di correzione a questi servizi:

- <https://www.maxmind.com/en/geoip-location-correction> (servizio principale utilizzato per Umbrella)
- <https://support.google.com/websearch/contact/ip/>
- <https://ipinfo.io/corrections>
- <https://www.ip2location.com/contact/>
- <http://www.ipligence.com/contact/>

## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).