

Risoluzione dei problemi relativi all'interazione del portale vincolato con il client Umbrella Roaming

Sommario

[Introduzione](#)

[Panoramica](#)

[Comportamenti e scenari previsti](#)

[Cisco Security Connector \(CSC\)](#)

[DNS di terze parti bloccato](#)

[Reindirizzamento DNS di terze parti](#)

[DNS di terze parti consentito](#)

Introduzione

Questo documento descrive le interazioni tra il portale vincolato e il client di roaming Umbrella.

Panoramica

I portali vincolati sono il nome comune per le connessioni Internet pubbliche o "as-a-service" che richiedono il pagamento, l'autenticazione o l'accettazione delle condizioni di servizio/utilizzo accettabile (TOS/AUP) prima di consentire la connettività a un dispositivo.

I portali in cattività sono generalmente visti in aeroporti, hotel, bar o in qualsiasi luogo che gratuitamente o a pagamento wifi è offerto. È inoltre possibile visualizzarli in reti wifi guest in ambienti aziendali o scolastici.

Un portale vincolato in genere si presenta come un "gate" o popup nel browser in cui l'utente finale deve intervenire per fornire le credenziali, il pagamento o accettare i termini di servizio per raggiungere Internet. Finché il portale vincolato non viene cancellato, l'utente non è in grado di esplorare altre risorse oltre a quelle all'interno della subnet in cui è presente il portale.

Comportamenti e scenari previsti

La maggior parte dei portali vincolati reindirizza tutte le richieste del browser (HTTP/HTTPS) al proprio portale Web locale. Il portale Web locale è in genere basato su IP e non su DNS. Ciò significa che non vi sono problemi di comportamento causati quando si utilizza il client di roaming Umbrella su un computer che si connette a un portale vincolato.

Nel raro caso in cui un portale vincolato utilizzi in qualche modo il DNS per facilitare il proprio servizio, questo comportamento si verifica prima di completare i requisiti del portale vincolato

(pagamento, accettazione TOS/AUP, ecc.).]

I portali vincolati basati su DNS potrebbero essere in grado di reindirizzare le query HTTP solo senza errori. I browser moderni gestiscono automaticamente le richieste conosciute come google.com per essere <https://www.google.com/>, che potrebbero interrompere alcuni portali vincolati. Provare a utilizzare il sito di controllo del portale captive di Apple per accedere alla pagina di accesso del portale captive che è solo http. A tale scopo, visitare il sito <http://captive.apple.com>.

Cisco Security Connector (CSC)

Come per il client in roaming, CSC rimane protetto e crittografato se UDP 443 è consentito dietro un portale in cattività. Di conseguenza, il DNS locale per il portale vincolato non riesce a risolvere il risultato locale. Pertanto, per accedere al portale in cattività, è necessario visitare un dominio presente nell'elenco dei domini interni per questi portali in modalità semi-cattività.

Per consentire il funzionamento del rilevamento automatico di iOS Captive Portal:

- Aggiungi questi elementi all'elenco dei domini interni
 - captive.apple.com
 - www.airport.us
 - www.thinkdifferent.us

DNS di terze parti bloccato

Se il portale vincolato blocca le richieste DNS destinate a Umbrella, la connettività DNS viene bloccata per circa sei secondi dal client di roaming Umbrella. Dopo sei secondi, il client di roaming Umbrella passa allo stato [Non protetto/Non crittografato](#) finché non può nuovamente comunicare con Umbrella.

Reindirizzamento DNS di terze parti

Se il portale vincolato reindirizza le richieste DNS destinate a Umbrella, la connettività DNS viene bloccata per circa due-sei secondi dal client di roaming Umbrella. Dopo questo periodo, il client di roaming Umbrella passa allo stato [Non protetto/Non crittografato](#) finché non può nuovamente comunicare con Umbrella.

DNS di terze parti consentito

Se il portale vincolato non sta manipolando o bloccando le richieste DNS destinate a Umbrella, il client di roaming Umbrella funziona come previsto e potrebbe comportare l'esclusione completa della parte di accesso del portale vincolato.

Soluzione: Visita un dominio nell'elenco dei domini interni. In questo modo è possibile eseguire il reindirizzamento dei portali in modo vincolato anche quando è consentito il DNS di terze parti. Eseguire questa operazione quando il client in roaming rimane in uno stato protetto dietro un portale vincolato.

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).