

Risoluzione dei problemi di connessione agli hotspot tramite Captive Portal con AnyConnect SWG Module abilitato

Sommario

[Introduzione](#)

[Problema](#)

[Correzioni e suggerimenti per un'ulteriore risoluzione dei problemi](#)

[Configurazione delle applicazioni antivirus per AnyConnect](#)

[Dettagli](#)

[Versioni precedenti alla 4.10.05095](#)

Introduzione

Questo documento descrive la risoluzione dei problemi di connessione agli hotspot tramite Captive Portal con il modulo AnyConnect SWG abilitato.

Problema

Gli utenti che usano il modulo AnyConnect Secure Web Gateway (SWG) potrebbero avere problemi ad accedere in alcune postazioni pubbliche.

Correzioni e suggerimenti per un'ulteriore risoluzione dei problemi

Verificare di usare AnyConnect versione 4.10.05095(4.10MR5). I problemi relativi al portale vincolato sono trattati nella presente versione.

Tuttavia, se il problema persiste anche dopo l'aggiornamento a 4.10.05095, contattare il Supporto Umbrella.

Per velocizzare il processo di assistenza, chiediamo ai clienti di completare questi passaggi e raccogliere i log richiesti prima di contattare l'assistenza Umbrella.

1. I clienti devono configurare tutti gli agenti di sicurezza installati sui loro endpoint in modo da escludere i file binari e le connessioni AnyConnect, in modo da evitare conflitti di criteri. Pertanto, TrendMicro e/o qualsiasi altro agente di sicurezza deve essere configurato di conseguenza.
Fare riferimento allo snippet di codice pertinente delle [note sulla versione di AnyConnect](#) e verificare che le eccezioni relative a AnyConnect siano inserite correttamente.

2. Visitare gli URL HTTP (ad esempio, <http://www.portquiz.net>) e HTTPS (<https://www.google.com>) nel browser e verificare se si verifica il reindirizzamento al portale vincolato.
3. Se il problema persiste, raccogliere un bundle DART (max debug enabled), un file PCAP (incluso il loopback) e una registrazione dello schermo (opzionale) per approfondire l'analisi.

Configurazione delle applicazioni antivirus per AnyConnect

Applicazioni come antivirus, antimalware e Intrusion Prevention System (IPS) possono interpretare erroneamente il comportamento delle applicazioni AnyConnect Secure Mobility Client come dannoso. È possibile configurare le eccezioni in modo da evitare tali errori di interpretazione. Dopo aver installato i moduli o i pacchetti AnyConnect, configurare il software antivirus in modo da consentire l'uso della cartella di installazione di AnyConnect o creare eccezioni di sicurezza per le applicazioni AnyConnect. Le directory comuni da escludere sono elencate, anche se l'elenco potrebbe non essere completo:

- C:\Users<user>\AppData\Local\Cisco
- C:\ProgramData\Cisco
- C:\Program (x86)\Cisco

Dettagli

I problemi relativi a Captive Portal possono essere causati da [CSCwb39828](#) "La pagina Captive Portal non è stata aperta quando SWG è abilitato per entrambe le operazioni di apertura/chiusura non riuscita". Dopo aver eseguito l'aggiornamento a AnyConnect 4.10.05095 in un secondo momento, non è necessario eseguire altre operazioni di configurazione o interazione con l'utente.

Alcuni hotspot wireless e altre reti guest interrompono l'accesso a Internet e reindirizzano il traffico Web a un portale in cattività (talvolta denominato giardino recintato). Le versioni AnyConnect SWG precedenti alla 4.10.05095 potrebbero tentare di inviare il traffico Web alla Umbrella cloud anche se l'accesso a Internet non è disponibile, il che impedisce al sistema di interagire localmente con il portale in cattività. Questa interazione locale potrebbe essere necessaria per concedere l'accesso tramite autenticazione, pagamento o una pagina dell'accordo di accesso.

Versioni precedenti alla 4.10.05095

Quando si usa SWG, il supporto per portali vincolati è limitato alle versioni precedenti di AnyConnect. Queste azioni di un portale vincolato probabilmente lo rendono irraggiungibile per un client SWG:

- Reindirizzamento o caricamento di asset da una destinazione esterna allo spazio di indirizzi IP privato RFC-1918.
- Accettare un handshake TCP per i proxy Umbrella sulla porta 80 o 443 e quindi chiudere la connessione o fornire una risposta imprevista.

Per risolvere il problema, aggiungere le eccezioni nella sezione Distribuzioni → Gestione dominio

—> Domini esterni e IP del dashboard ombrello, per ogni destinazione che non riesce a caricare. Il comportamento del portale vincolato è specifico dell'implementazione, pertanto i domini o gli indirizzi IP di reindirizzamento richiesti variano a seconda dell'hotspot.

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).