

HTTP 429 Limite di velocità ed errori di connessione durante l'accesso alle applicazioni tramite Secure Access SWG

Sommario

Problema

Gli utenti incontrano errori HTTP 429 relativi al limite di velocità quando tentano di accedere all'applicazione, ad esempio <https://xxxx.com> tramite Cisco Secure Access SWG (Secure Web Gateway). Il problema riguarda i notebook gestiti dall'azienda ed è iniziato circa due settimane prima dell'apertura della richiesta. Questi errori si verificano durante i tentativi di accesso o quando si accede a determinate funzioni dell'applicazione dopo l'autenticazione.

Inoltre, quando il dominio viene aggiunto all'elenco di esclusione dell'accesso sicuro, gli utenti rilevano errori del server HTTP 500 durante la voce OTP (One-Time Password) o errori generali di connessione quando il traffico non continua a scorrere negli intervalli IP SWG (151.186.x.x).

Il proprietario dell'applicazione ha confermato che di recente non è stato modificato alcun limite di velocità sul lato server e il problema sembra essere correlato al traffico proveniente dagli indirizzi IP di uscita SWG di Cisco Secure Access.

Ambiente

- Cisco Secure Access (in precedenza Cisco Umbrella) con SWG abilitato
- Notebook gestiti a livello aziendale con client Cisco SSE (Security Service Edge)
- Intervalli IP in uscita SWG: 151.186,x,x
- Centri dati: AWS Singapore (Asia Pacifico 1) e AWS US West (Oregon)
- Applicazione: <https://sbstransit.aereacommercial.com>

Risoluzione

La risoluzione implica l'implementazione di una configurazione di bypass e il coordinamento con il proprietario dell'applicazione per consentire l'elenco di indirizzi IP specifici.

Seguire i passaggi successivi.

Passaggio 1: Verifica del comportamento SWG corrente

Controllare il criterio corrente e le informazioni sull'indirizzo IP in uscita accedendo a questo URL da un dispositivo interessato:

`https://policy.test.sse.cisco.com/?host=https://sbstransit.aereacommercial.com`

Questo mostra l'IP di uscita SWG corrente in uso (generalmente intervallo 151.186.x.x) e conferma che il traffico viene elaborato tramite Secure Access SWG.

Passaggio 2: Aggiungi dominio all'elenco di esclusione accesso sicuro

Passare a Impostazioni Internet > Ignora accesso sicuro nel dashboard Cisco Secure Access e aggiungere il dominio con problemi per ignorare l'ispezione di DNS e SWG:

`sbstransit.aereacommercial.com`

Passaggio 3: Test di accesso da una rete non aziendale

Verificare l'accesso alle applicazioni da una rete in cui il traffico non arriva tramite Secure Access SWG (intervalli 151.186.x.x). Questa operazione può essere eseguita da un dispositivo personale o disattivando temporaneamente il client SSE.

Per identificare l'indirizzo IP pubblico dell'ISP, visitare:

<https://whatismyip.com>

Passaggio 4: Coordina elenco indirizzi IP consentiti con proprietario applicazione

Fornire l'indirizzo IP dell'ISP pubblico identificato al proprietario dell'applicazione e richiedere che l'IP sia consentito sul lato dell'applicazione. Ciò consente di verificare se l'applicazione sta implementando restrizioni basate su IP che influiscono sugli indirizzi IP in uscita dei file SWG ad accesso sicuro.

Passaggio 5: Verifica risoluzione

Dopo che il proprietario dell'applicazione ha implementato l'elenco di indirizzi IP consentiti, verificare il comportamento dell'accesso per verificare che gli utenti possano accedere all'applicazione senza riscontrare errori HTTP 429 o di connessione.

Causa

L'applicazione sembra implementare limitazioni di velocità o di accesso basate sugli indirizzi IP di origine. Quando più utenti accedono all'applicazione tramite Cisco Secure Access SWG, tutto il traffico sembra provenire da intervalli IP di uscita SWG condivisi (151.186.x.x). In questo modo viene attivato il meccanismo di limitazione della velocità dell'applicazione, che percepisce richieste eccessive provenienti da un singolo indirizzo IP o intervallo IP.

Il problema è aggravato dal fatto che i dispositivi gestiti dall'azienda continuano a instradare il traffico attraverso il client SSE anche quando sono connessi a reti personali, mantenendo lo stesso comportamento IP in uscita che attiva le restrizioni dell'applicazione.

Contenuto correlato

- [Supporto tecnico Cisco e download](#)

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).