Risoluzione dei problemi relativi alla licenza 516 su Umbrella Secure Web Gateway

Sommario

Introduzione

In questo documento viene descritto come risolvere un aumento di 516 errori in Umbrella Secure Web Gateway.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano su Umbrella Secure Web Gateway (SWG).

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Panoramica

Gli utenti che navigano attraverso il proxy Umbrella Secure Web Gateway (SWG) con l'ispezione HTTPS possono ricevere più spesso 516 pagine di errore di mancata corrispondenza CN dei certificati upstream a partire dalla seconda metà di ottobre 2023.

La pagina di errore 516 si verifica quando il certificato di un sito Web non corrisponde al nome di dominio utilizzato dal client per accedere al sito.

L'aumento delle pagine di errore è dovuto a una modifica nella gestione da parte del browser Chrome delle richieste di URL che utilizzano lo schema HTTP (non crittografato). Chrome ora tenta di caricare la risorsa prima con lo schema HTTPS (crittografato). Quando è configurato per l'ispezione HTTPS, SWG controlla il certificato di un sito Web e restituisce una pagina Web che visualizza un codice di errore come 516 se il certificato non è accettabile.

Per risolvere il problema, i clienti possono configurare i propri criteri Web in modo da ignorare l'ispezione HTTPS per le richieste che altrimenti generano 516 errori.

516 Sfondo errore

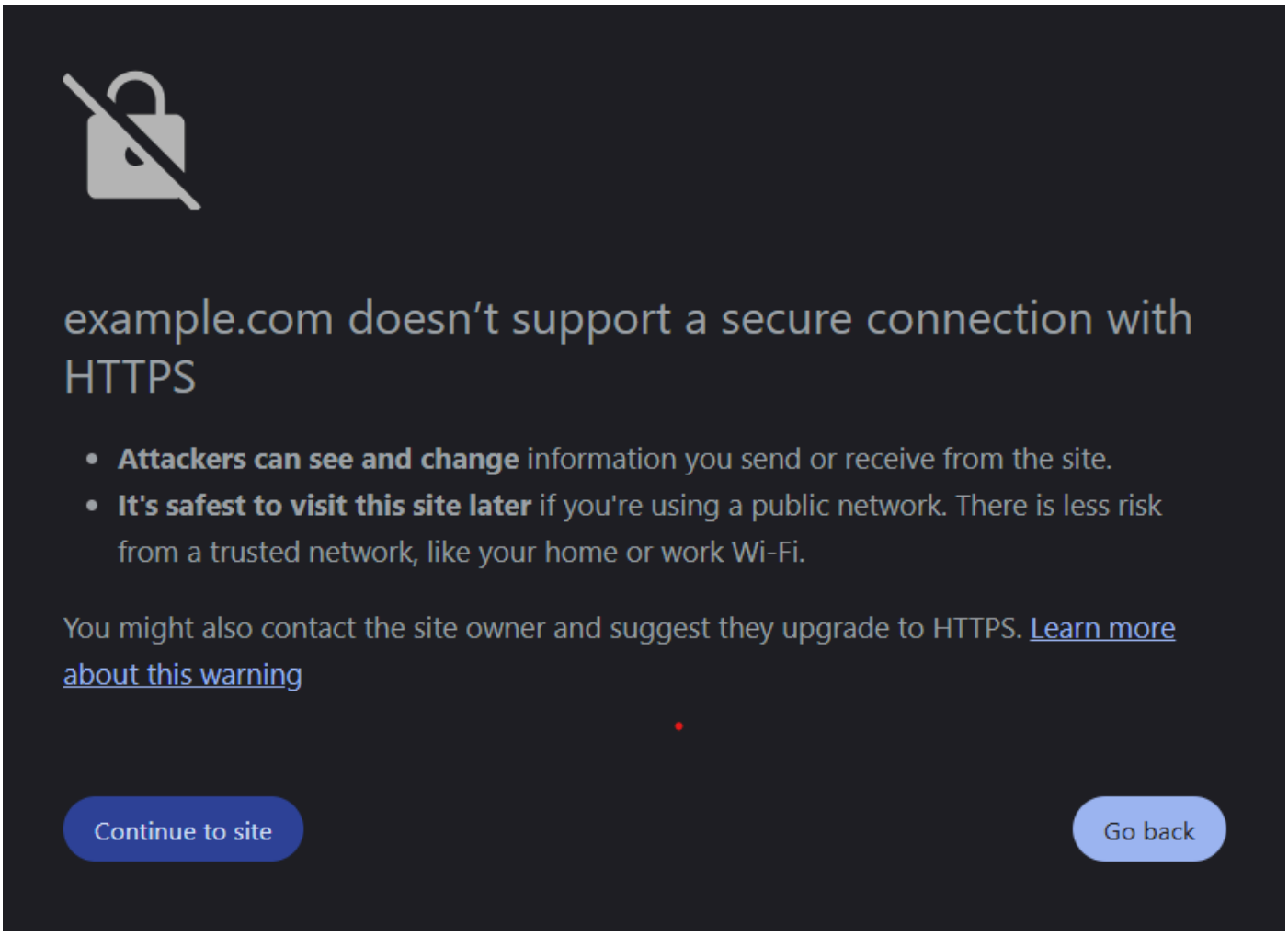
In breve, Umbrella Secure Web Gateway restituisce una pagina di errore 516 quando il nome di dominio utilizzato per accedere a un sito Web tramite HTTPS non viene visualizzato nel certificato digitale del server. Per ulteriori informazioni sul motivo per cui Secure Web Gateway restituisce una pagina di errore 516, consultare l'articolo della Umbrella Knowledge Base "516 Upstream Certificate CN Mismatch" (Mancata corrispondenza CN certificato upstream 516).

Si consideri, ad esempio, un sito che fornisce contenuto da URL HTTP nel formato: http://www.example.com/path_to_content. Se un utente richiede gli URL HTTPS equivalenti, ma il sito non dispone di un certificato le cui SAN corrispondono a www.example.com (probabilmente la SAN corrisponde solo a example.com), l'utente riceve un errore 516 se la richiesta viene gestita da Umbrella Secure Web Gateway con un criterio Web che utilizza la funzione di ispezione HTTPS di SWG.

Modifica comportamento riquadro

Nella seconda metà di ottobre 2023, Google ha completato l'introduzione di una nuova funzionalità per il browser Chrome. Dopo tale data, viene automaticamente inoltrata una richiesta per un URL HTTP utilizzando la versione HTTPS di tale URL. Ad esempio, quando un utente fa una richiesta per http://www.example.com, Chrome prima tenta di soddisfare la richiesta utilizzando https://www.example.com.

Se Chrome riceve un errore relativo a HTTPS quando richiede l'URL HTTPS, Chrome tenta di caricare lo stesso contenuto su HTTP. Se la richiesta per l'URL HTTP è riuscita, Chrome visualizza una pagina interstiziale con testo che indica che il sito non è sicuro e un collegamento che dà all'utente l'opzione di procedere, come l'immagine seguente.



Questo è il comportamento fallback nella nuova funzionalità di Chrome.

Tuttavia, quando si naviga tramite SWG con Ispezione HTTPS, se la richiesta HTTPS produce un errore relativo a HTTPS come "ERR_CERT_COMMON_NAME_INVALID" dal sito, SWG intercetta l'errore e restituisce una pagina di errore SWG a Chrome, come la pagina di errore 516. Questo contenuto SWG non è considerato da Chrome un errore relativo a HTTPS, quindi non produce il comportamento di fallback e viene visualizzata la pagina di errore SWG, piuttosto che la pagina nell'immagine precedente.

Ulteriori informazioni sul nuovo comportamento di Chrome sono disponibili sul blog Chromium e sul repository GitHub della funzione.

Determinazione dell'origine dell'errore

Ora che Chrome promuove automaticamente gli URL HTTP agli URL HTTPS, i siti web che generano 516 errori sono visti più frequentemente dagli utenti.

Per confermare che un sito web sta causando un errore relativo HTTPS come la risposta 516, esplorare il sito con Chrome da un sistema desktop che non utilizza Umbrella. Assicurarsi di immettere manualmente la versione HTTPS dell'URL esplicitamente in Omnibox di Chrome (come la barra degli indirizzi), piuttosto che fare clic su un collegamento ipertestuale HTTP. Se un collegamento ipertestuale ha generato un errore 516 con SWG, la richiesta manuale dell'URL HTTPS in Chrome senza SWG può generare il messaggio di errore

"ERR_CERT_COMMON_NAME_INVALID". Questo messaggio di errore conferma che il problema è un certificato non corretto per il nome di dominio utilizzato per accedere al sito Web.

In alternativa, utilizzare uno strumento online come il sito di test del server Qualys SSL per diagnosticare il problema con il sito Web.

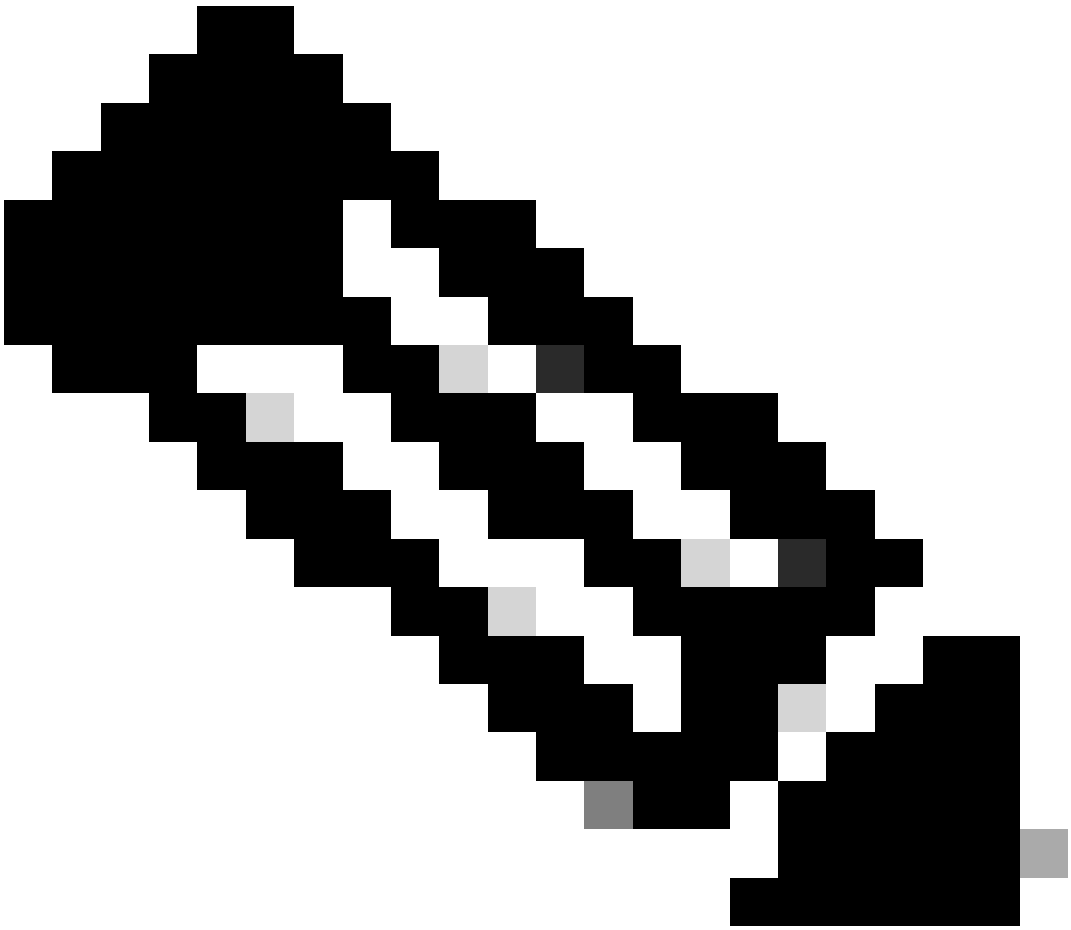
Soluzioni

Gli amministratori Umbrella possono risolvere il problema con una delle seguenti opzioni:

1. Creare un elenco di destinazione specifico per questi siti e aggiungere l'elenco a un criterio Web senza ispezione HTTPS.

2. Creare un elenco di decrittografia selettiva di siti che generano 516 pagine di errore e aggiungere l'elenco di decrittografia selettiva a tutti i criteri Web pertinenti

---



Nota: Fattori quali i reindirizzamenti HTTP o i sistemi di sicurezza e-mail che sostituiscono gli URL HTTPS del servizio agli URL HTTP originali possono oscurare il nome di dominio necessario. L'identificazione del nome di dominio corretto per un elenco di destinazione o

---

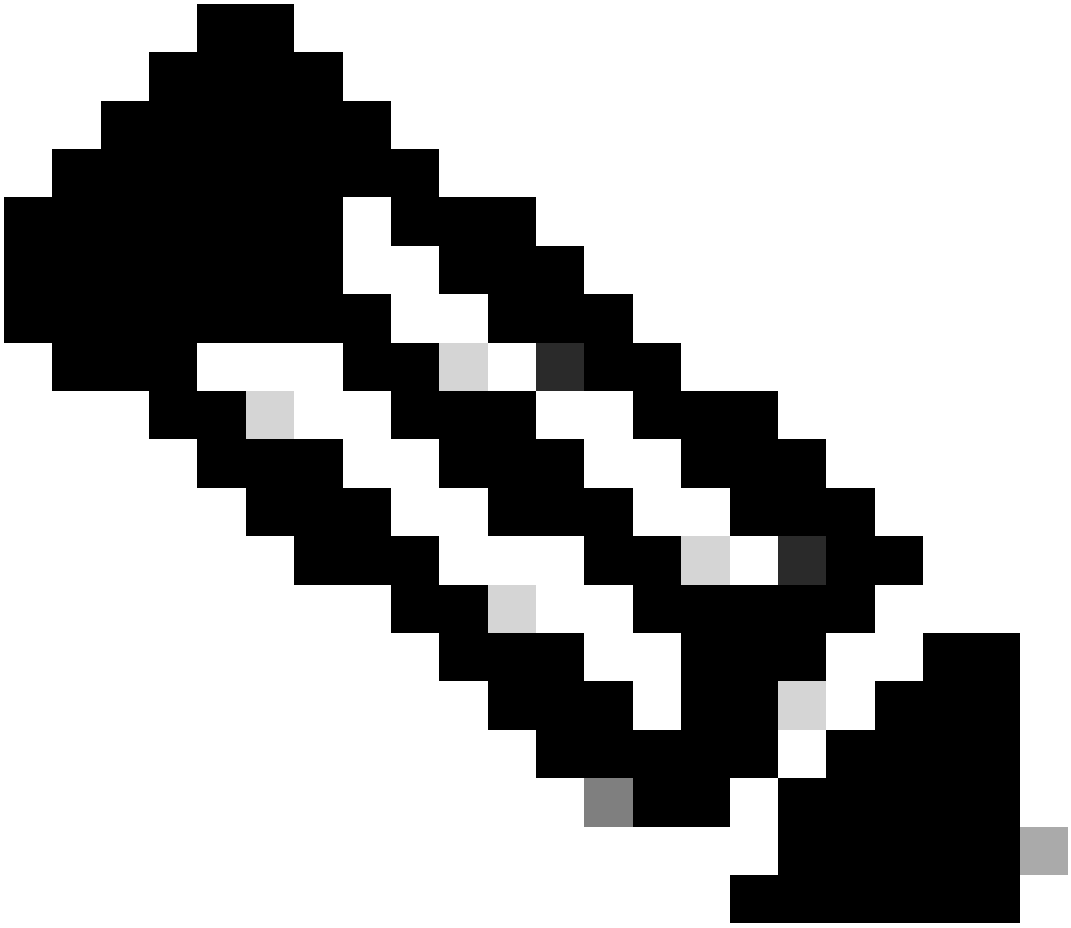
un elenco di decrittografia selettiva può richiedere un'analisi, incluso l'utilizzo di strumenti specifici (curl, Chrome Developer Tools, un registro del fornitore della sicurezza e-mail e così via).

516 Errori e sistemi di posta elettronica

Un aumento della frequenza di errore di 516 può derivare da sistemi e-mail che visualizzano messaggi e-mail in formato HTML e consentono collegamenti ipertestuali nei messaggi. Durante la composizione di un messaggio e-mail, se il mittente digita o incolla un nome di dominio nel corpo del messaggio, molti sistemi e-mail promuovono automaticamente un nome di dominio in testo normale a un collegamento ipertestuale. In genere, quando viene creato il collegamento, lo schema è HTTP anziché HTTPS.

Se ad esempio si digita la stringa `example.com` in un messaggio di posta elettronica, verrà visualizzato un messaggio contenente il codice HTML `<a href="http://www.example.com">` visualizzato come collegamento ipertestuale www.example.com.

Se un destinatario di un messaggio di posta elettronica di questo tipo fa clic sul collegamento ipertestuale HTTP, la richiesta inizialmente utilizza HTTPS se il clic apre Chrome o se Chrome è già utilizzato per visualizzare il messaggio di posta elettronica.



Nota: Anche altri browser possono promuovere HTTP a HTTPS.

Inoltre, un collegamento ipertestuale in un messaggio e-mail che utilizza intenzionalmente lo schema HTTP viene gestito in modo simile.

Alcuni servizi cloud comuni inviano messaggi di posta elettronica dai provider di servizi di posta elettronica transazionale di terze parti con collegamenti ipertestuali HTTP anziché HTTPS. Il sito HTTPS che Chrome tenta automaticamente di caricare può rispondere con un errore di certificato al nome di dominio nel collegamento e-mail come in questo esempio da Seegrid.

Quando queste e-mail hanno elenchi di destinatari di grandi dimensioni, molti utenti i cui clic (o richieste) vengono inviati tramite SWG possono segnalare errori come l'errore 516. Contattare il provider del servizio di posta elettronica o l'organizzazione che ha inviato l'e-mail per richiedere la risoluzione dell'errore del certificato.

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).