# Risoluzione dei problemi di accesso al sito Web SWG

## Sommario


Introduzione

Premesse

Errore "Accesso negato 403" a causa di un blocco a monte

Errore "Accesso negato 403" a causa di un problema Java

Root cause del problema di alto livello

- Qual è il problema relativo a Java con MPS?
  - Risoluzione

Che cos'è 502 Bad Gateway?

Fattori comuni per 502 Bad Gateway

- Suite di crittografia SWG non supportate
  - Risoluzione
- Richiesta di autenticazione certificato client
- Intestazioni aggiunte dal proxy
  - Risoluzione


## Introduzione

In questo documento viene descritto come risolvere i problemi relativi all'accesso al sito Web rilevati con il proxy Umbrella Secure Web gateway (SWG).

## Premesse

Supponiamo che il sito Web www.xyz.com non sia accessibile tramite proxy SWG e che quando gli utenti provano ad accedere direttamente a Internet (senza che Umbrella SWG sia nella foto), funziona bene.  Esaminiamo vari sintomi e diversi tipi di messaggi di errore segnalati quando il sito Web è inaccessibile tramite SWG. I più comuni sono 502 gateway errato, 502 impossibile inoltrare messaggio errore a monte, certificato a monte revocato, accesso negato 403 vietato, cifratura a monte non corrispondente, sito web appena scaduto dopo la rotazione per un tempo o simili.

## Errore "Accesso negato 403" a causa di un blocco a monte

Il server Web o il lato upstream blocca o limita gli intervalli IP in uscita del proxy SWG. Ad esempio, Akamai WAF ha bloccato un paio di intervalli IP in uscita SWG. Per risolvere questo problema, l'unica opzione è quella di raggiungere gli amministratori del sito Web e farli sbloccare i nostri intervalli IP. Fino ad allora, ignorare SWG usando l'elenco di gestione dei domini esterni per le distribuzioni di file SWG e PAC di Anyconnect. In breve, questo tipo di problema non è dovuto al proxy in sé, bensì all'incompatibilità tra il proxy e i server Web. Di seguito è riportato il

collegamento per fare riferimento alla Knowledge Base in modo specifico per l'errore "Accesso negato 403" a causa del blocco IP in uscita.

Inoltre, questo link tratta alcune possibili ragioni per cui Akamai ha bloccato gli indirizzi IP elencati.

# Errore "Accesso negato 403" a causa di un problema Java

Il sito Web non è accessibile e viene generato "Accesso negato o 403 non consentito - Errore del gateway di sicurezza del cloud Umbrella" quando la richiesta viene inviata tramite il proxy SWG MPS con l'impostazione di ispezione dei file abilitata. Se invece l'opzione Controllo file è disattivata, i siti Web vengono caricati correttamente. Oppure, se mettiamo il sito in bypass decrittografia, i siti Web si caricano con successo.

# Root cause del problema di alto livello

## Qual è il problema relativo a Java con MPS?

Il sito o il server Web in questione restituisce un avviso TLS relativo a un avviso SNI o SSL al proxy dopo che il proxy ha tentato di connettersi al server. In pratica, questo succede dopo che il cliente saluta. Proxy MPS (basato su Java e come tale) per progettazione, tratta qualsiasi alert TLS con "Nome non riconosciuto" nel campo descrizione come un errore durante l'analisi SNI e termina la transazione. Ulteriori informazioni sono disponibili qui

Tenere presente che non si tratta di un problema di proxy SWG o MPS. Questa è una delle incompatibilità con SWG o qualsiasi altro proxy a causa di una configurazione errata sul lato server. I browser in genere ignorano questo avviso, ma SWG o un altro filtro di protezione del contenuto considera l'avviso SSL come un errore irreversibile e termina la sessione, causando 403 pagine di errore vietate agli utenti. Può anche segnalare un errore 502 di Bad Gateway, ma con la maggior parte degli esempi ne è stato rilevato uno 403 vietato, come mostrato in questa immagine.


Poiché MPS opera a livello di applicazione, non ha quasi alcun controllo su come il livello TLS gestisce la transazione in base agli allarmi prodotti nel protocollo TLS. È responsabilità del server verificare che gli endpoint/certificati TLS siano configurati correttamente. Fare riferimento a questo collegamento.

Per circoscrivere il problema o risolverlo, è possibile indicarlo facilmente dal laboratorio SSL.


15152060146964

Quando si accede al sito Web senza il proxy SWG al centro o si ignora l'ispezione HTTPS da SWG, il sito Web funziona perché il browser ignora l'avviso di nome SNI non riconosciuto e continua a comunicare con il server Web.

Al momento di scrivere questo articolo, la soluzione consigliata è la migliore mitigazione che possiamo suggerirti. Nel prossimo futuro, grazie alla nuova architettura proxy, saremo in grado di gestire questi problemi in modo più efficiente.

Risoluzione

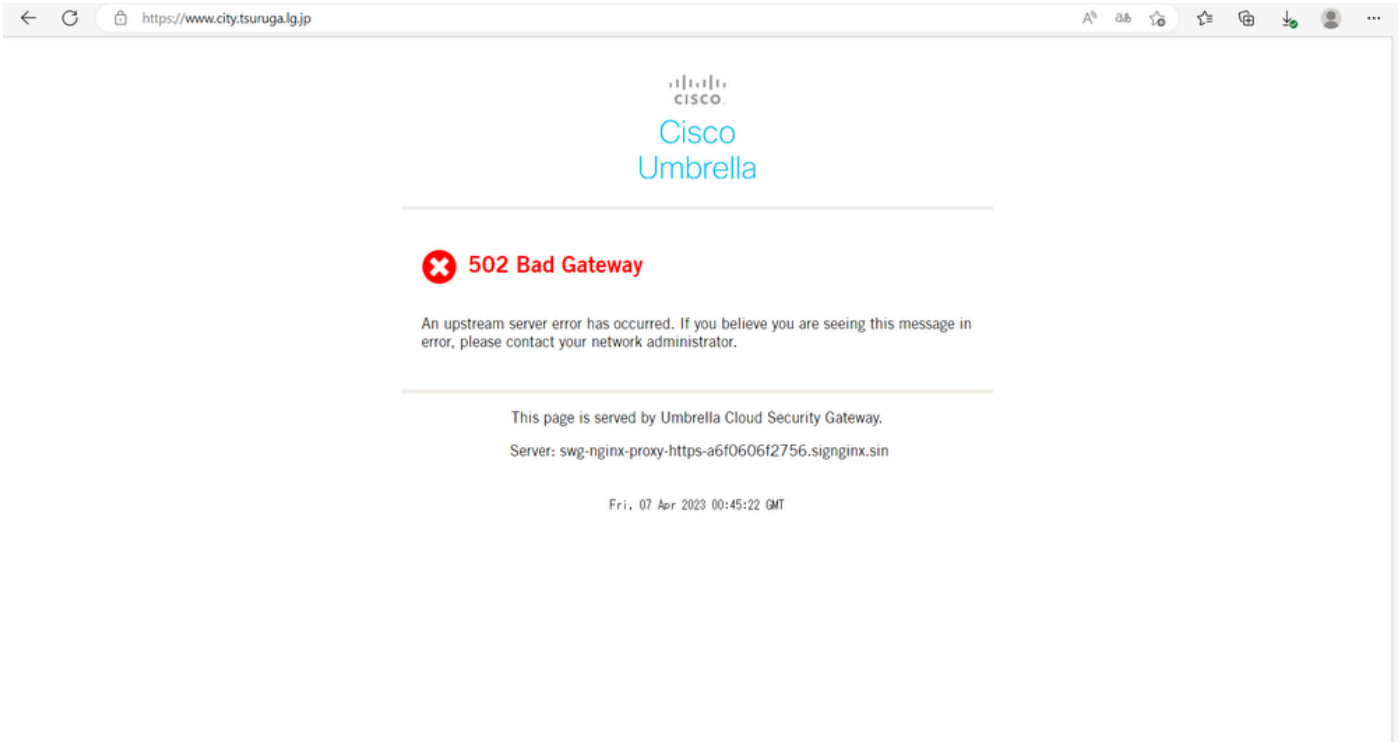
1. Disabilita la decrittografia per i domini interessati - OPPURE
2. Aggiungere il dominio a un elenco di destinazione e associare una regola di autorizzazione (se si considera attendibile il sito)

## Che cos'è 502 Bad Gateway?

Un errore 502 di gateway non valido indica che il server ha agito come gateway o proxy e ha ricevuto una risposta non valida dal server upstream. Quando l'utente tenta di accedere al sito Web tramite SWG Proxy, si verificano due flussi di comunicazione.

a) Client —> Connessione proxy (downstream)
b) Proxy—> Termina connessione server Web (upstream)

502 Si è verificato un errore di gateway non valido tra il proxy SWG (MPS, Nginx) e la connessione del server finale.




15026978020884

# Fattori comuni per 502 Bad Gateway

1. Suite di crittografia SWG non supportate

2. Richiesta di autenticazione del certificato client

3. Intestazioni aggiunte o rimosse dal proxy SWG

## Suite di crittografia SWG non supportate

Supponiamo che un server Web segnali suite di cifratura SWG non supportate durante la negoziazione TLS. Il proxy SWG MPS (Modular Proxy Service) non supporta la suite di cifratura TLS_CHACHA20_POLY1305_SHA256. Si tenga presente che è presente un articolo separato relativo alle suite di cifratura e TLS supportate dallo SWG. Possiamo facilmente identificare questo problema rivedendo i loro pacchetti acquisiti durante lo scambio di suite di cifratura in ciao client e ciao server. Per risolvere il problema, usare il comando CURL che forza l'uso di cifrari specifici per ridurre il problema e per verificare che sia dovuto alle suite di cifratura, come mostrato negli esempi 1 e 2.

Esempio di comandi Curl:

<#root>

```
curl -vvv "" --ciphers TLS_DHE_DSS_WITH_AES_256_GCM_SHA384 >> /dev/null
curl -vvv "" --ciphers ECDHE-RSA-AES256-GCM-SHA384 >> /dev/null
```

**Testing website With Proxy:**

```
 - curl -x  proxy.sig.umbrella.com:80 -v  xyz.com:80
```

```
curl -x swg-url-proxy-https.sigproxy.qq.opendns.com:443 -vvv -k "https://www.cnn.com" >> null
```

**Testing website without Proxy**

```
: - curl -v www.xyz.com:80
```

**Mac/Linux:**

```
  - curl -vvv -o /dev/null -k -L www.cnn.com
```

**Windows:**

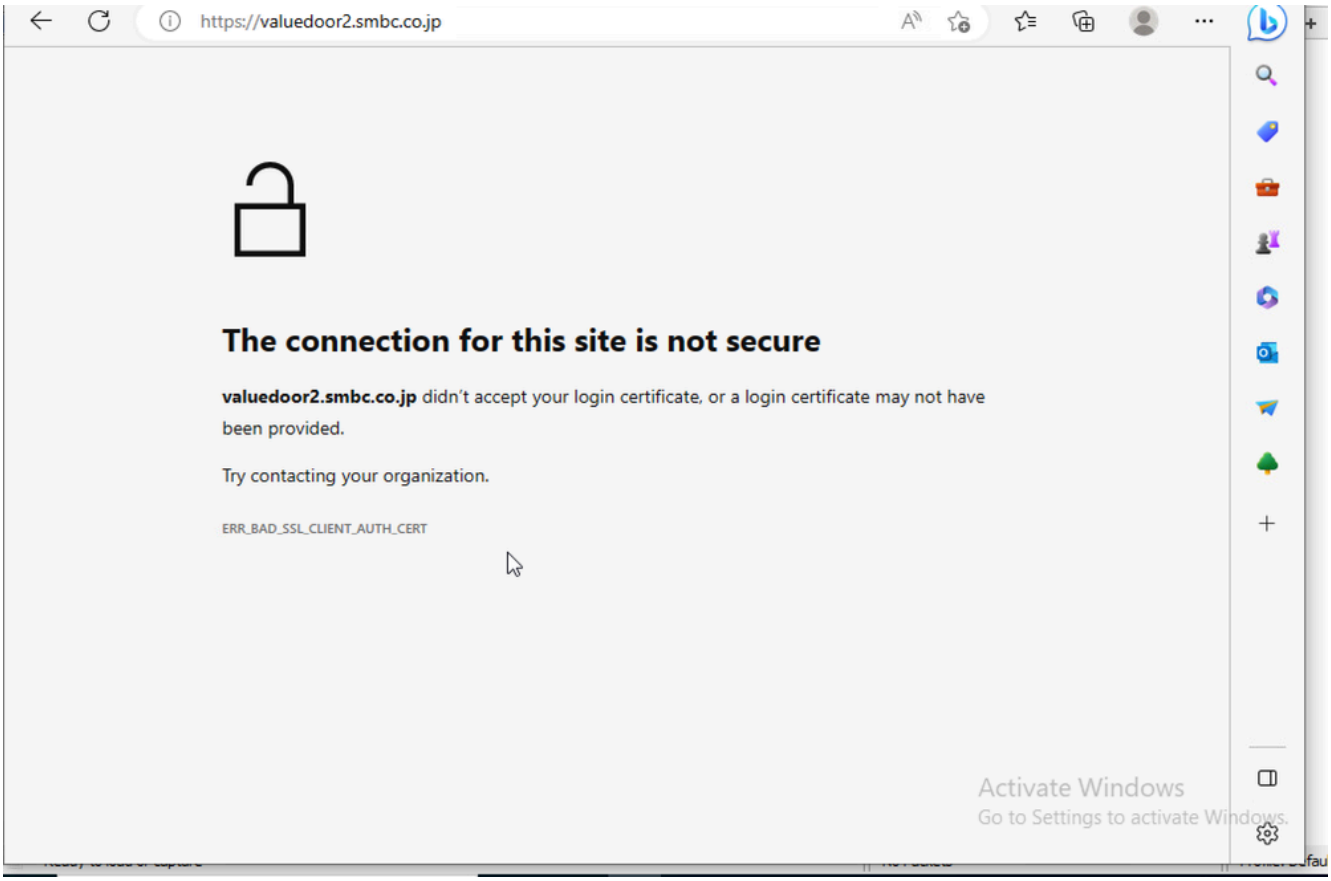
```
 - curl -vvv -o null -k -L www.cnn.com
```

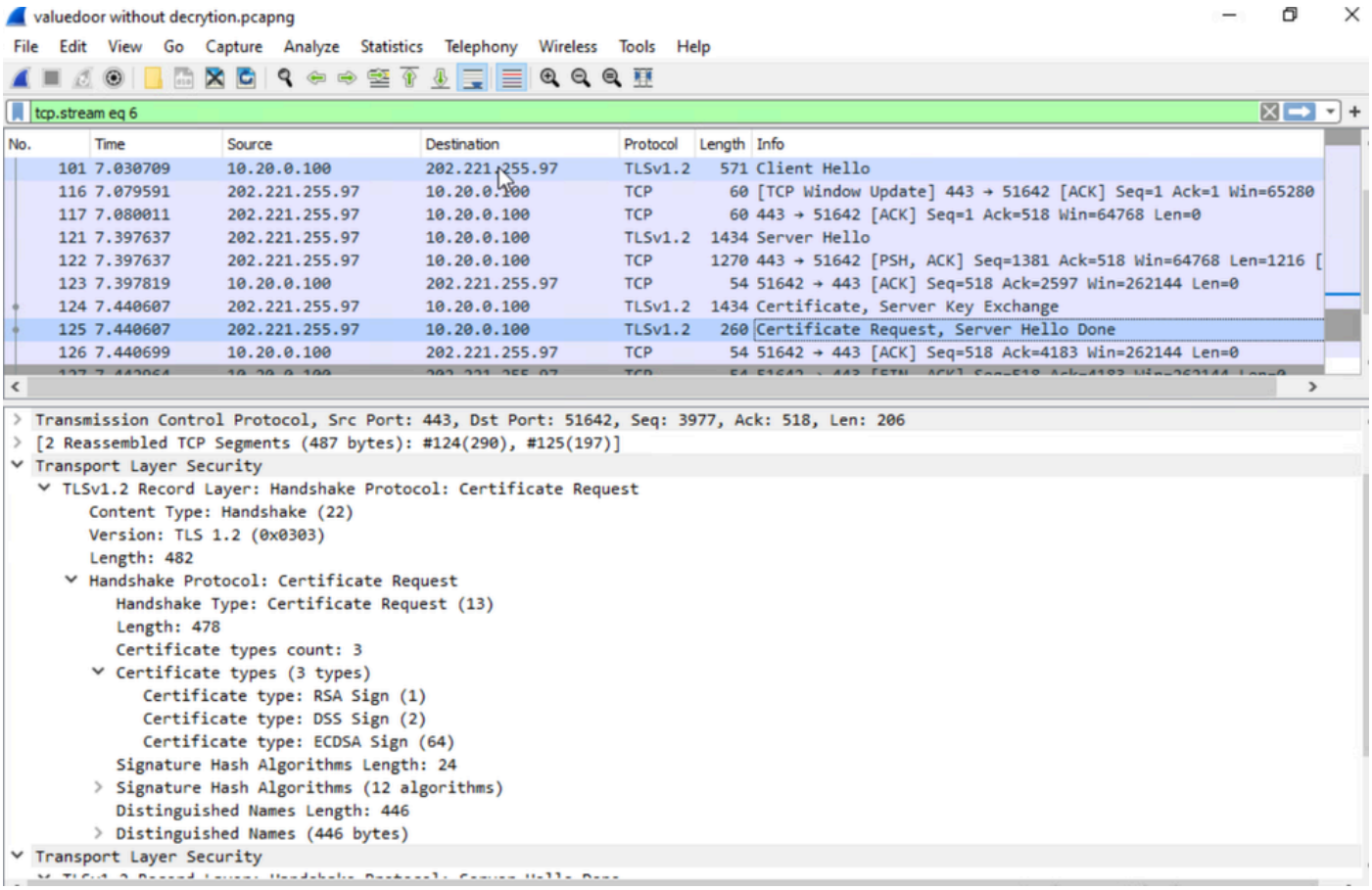
### Risoluzione

Per risolvere il problema, ignorare l'ispezione per il sito Web con problemi utilizzando l'elenco di decrittografia selettiva.

## Richiesta di autenticazione certificato client

Durante l'handshake TLS tra il proxy SWG e il server Web upstream, il server Web upstream si aspetta l'autenticazione del certificato client. Poiché l'autenticazione dei certificati client non è supportata, è necessario ignorare tali domini dal proxy utilizzando l'elenco di gestione dei domini esterni e ignorare solo l'ispezione https non è sufficiente. Ad esempio: https://valuedoor2.smbc.co.jp.

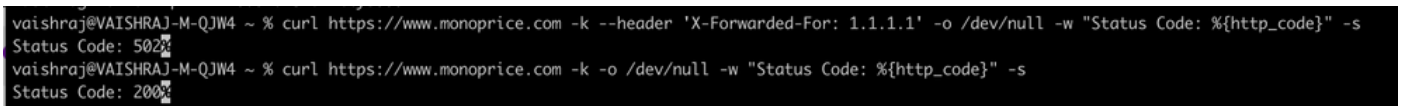





15027192992276

## Intestazioni aggiunte dal proxy

Il server Web segnala un errore gateway 502 non valido a causa dell'intestazione X-Forward-For (XFF) aggiunta dal proxy SWG quando l'ispezione https è abilitata. Possiamo facilmente ridurre la maggior parte dei 502 problemi di gateway errati risolvendo prima il problema con o senza ispezione https, e con o senza ispezione file per escludere problemi di scansione file con proxy MPS.




15123666760340

```
curl https://www.xyz.com -k --header 'X-Forwarded-For: 1.1.1.1' -o /dev/null -w "Status Code: %{http_co
Status Code: 502
curl https://www.xyz.com -k -o /dev/null -w "Status Code: %{http_code}" -s
Status Code: 200
```

L'intestazione XFF viene utilizzata quando l'ispezione HTTPS è attivata, in modo che il server upstream possa fornire un contenuto di geolocalizzazione ottimale basato sull'indirizzo IP del client (che fornisce la posizione fisica dell'utente).

Quando l'ispezione HTTPS non è abilitata, l'intestazione non viene aggiunta dal proxy, quindi non si verifica un errore 502 Bad Gateway. Questo non è un problema di proxy SWG . Questo errore è dovuto al server Web upstream non configurato correttamente per non supportare l'intestazione XFF standard.

Risoluzione

Per risolvere il problema, ignorare l'ispezione HTTPS per uno o più domini specifici utilizzando elenchi di decrittografia selettivi.

- Certificato upstream 517 revocato
- Errori del certificato e del protocollo TLS
- Selezione manuale del controller di dominio SWG per test interni

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).