Errore Secure Access 502 Per I Siti Bancari Dopo L'Autenticazione

Sommario

Problema

Gli utenti hanno segnalato la ricezione di un codice di errore HTTP 502 di gateway non valido dopo la corretta autenticazione a FCBanking. Il processo di autenticazione è stato completato, consentendo agli utenti di immettere le credenziali di accesso. Tuttavia, il browser ha visualizzato un errore di gateway 502 non valido subito dopo l'autenticazione.

Il dominio per FCBanking e la relativa categoria erano esenti dalla decrittografia SSL e IPS e questa modifica di configurazione non ha risolto l'errore HTTP 502. Il problema si è verificato in modo intermittente ed è stato risolto solo dopo aver ignorato completamente Secure Access per il dominio FCBanking. L'analisi del file HAR ha rilevato 502 errori nella destinazione di 'my.fcbanking.com' e nei log di ricerca attività non sono stati rilevati 502 errori nel file HAR. Ciò indica che tali errori si sono verificati a livello di dispositivo intermedio.

Ambiente

- Cisco Secure Access - Accesso a Internet (modulo roaming, VA, DNS, SWG, PAC, IPS, certificati)
- Topologia della rete: Utente PC > Switch > Catalyst SD-WAN Router > Internet locale o tunnel CSA
- Catalyst SD-WAN edge configurato con regola dei criteri dell'applicazione per inviare tutto il traffico sulla porta 80 e 443 tramite Direct Internet Access (DIA) ignorando Network Tunnel Group (NTG)
- Cisco Secure Client che si basa su un elenco di esclusione per determinare il routing del traffico per l'accesso sicuro
- Settore bancario: fcbanking.com e sottodomini associati (my.fcbanking.com, treasury.fcbanking.com)

Risoluzione

La risoluzione principale prevede l'aggiunta del dominio bancario per ignorare completamente Secure Access, consentendo al traffico di fluire direttamente su Internet mantenendo la sicurezza a livello DNS.

Passaggio 1: Aggiungi dominio primario all'elenco di esclusione

- Aggiungere fcbanking.com all'elenco Ignora solo proxy nella configurazione Accesso sicuro. In questo modo il traffico Web ignora il proxy di accesso sicuro mentre la sicurezza a livello DNS rimane applicata e registrata in Ricerca attività.

Passaggio 2: Identificare e aggiungere alias di dominio

- I siti bancari utilizzano spesso più alias che devono essere aggiunti anche all'elenco di esclusione. Utilizzare Cache Check per identificare tutti gli alias per il dominio bancario.
- Per fcbanking.com, questi alias sono stati identificati e aggiunti all'elenco di esclusione:
    - treasury.fcbanking.com (alias: treasuryvanity.jackhenry.com)
    - my.fcbanking.com (alias: banno-online.jackhenry.bank)
    - treasuryvanity.jackhenry.com
    - banno-online.jackhenry.bank

Passaggio 3: Risoluzione alternativa tramite indirizzi IP

- In alternativa al bypass basato su dominio, gli indirizzi IP risolti dei siti bancari possono essere aggiunti all'elenco di bypass. Cisco Secure Client converte gli FQDN trovati nell'elenco di esclusione in indirizzi IP e instrada il traffico Web direttamente su Internet.

Passaggio 4: Abilita registrazione debug per risoluzione problemi

- Per acquisire i log dettagliati per ulteriori analisi, abilitare il log di debug massimo:
- Creare un file denominato 'SWGConfigOverride.json' con il seguente contenuto:

```
{"logLevel": "1"}
```

Posizionate il file SWGConfigOverride.json nella cartella SWG:

```
C:\ProgramData\Cisco\Cisco Secure Client\Umbrella\SWG\
```

Riavviare il servizio SWG o Umbrella oppure riavviare il sistema per applicare la configurazione di registrazione del debug.



Nota: La registrazione del debug non influisce sulle prestazioni del sistema, ma può aumentare le dimensioni del file di registro. Rimuovere il file SWGConfigOverride.json dopo aver ottenuto il bundle DART per tornare ai livelli di registrazione normali.

Passaggio 5: Verifica

- Dopo aver implementato la configurazione di bypass, gli utenti non hanno segnalato altri 502 errori durante l'accesso al sito bancario. Il traffico DNS continua ad essere registrato in Ricerca attività mentre il traffico Web si dirige direttamente a Internet.

Causa

I siti bancari solitamente implementano misure di sicurezza che rilevano e bloccano il traffico proveniente dai server proxy o dagli intervalli di indirizzi IP condivisi. Cisco Secure Access utilizza intervalli IP condivisi (151.186.144.0/20 e 151.186.176.0/20) per il traffico proxy, che i siti bancari possono rilevare e ignorare automaticamente o a cui possono rispondere con errori HTTP 502.

Quando i domini vengono inseriti nell'elenco di non decrittografare, l'IP di origine sembra ancora provenire dall'intervallo IP condiviso di accesso sicuro, attivando i meccanismi di sicurezza del sito bancario. Inoltre, l'ispezione IPS sul traffico bancario e gli alias di dominio non esentati correttamente possono contribuire agli errori di connessione. La natura intermittente di questo problema e i 502 errori presenti nei file HAR ma non nei log di ricerca attività indicano che gli errori sono stati generati dall'elaborazione proxy intermedia anziché dai server bancari di destinazione.

Contenuto correlato

- Risoluzione dei problemi di accesso al sito Web SWG
- Disabilitare il protocollo QUIC per garantire la corretta ispezione del traffico Web
- Documentazione sugli intervalli IP di Cisco Secure Access
- 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).