Risolvi errore di mancata corrispondenza CN del certificato upstream 516

Sommario

Introduzione

In questo documento viene descritto come risolvere un errore di mancata corrispondenza CN del certificato upstream 516.

Problema

Quando il proxy Umbrella Secure Web Gateway (SWG) è configurato per eseguire l'ispezione HTTPS, un utente può ricevere una pagina di errore 516 Upstream Certificate CN Mismatch quando naviga verso un sito Web utilizzando un URL HTTPS.

Questo errore non indica un problema con l'attributo Nome comune (CN) nel campo Oggetto del certificato del sito Web. Il problema riguarda invece l'attributo Nome DNS nell'estensione SAN (Subject Alternative Names) di un certificato.

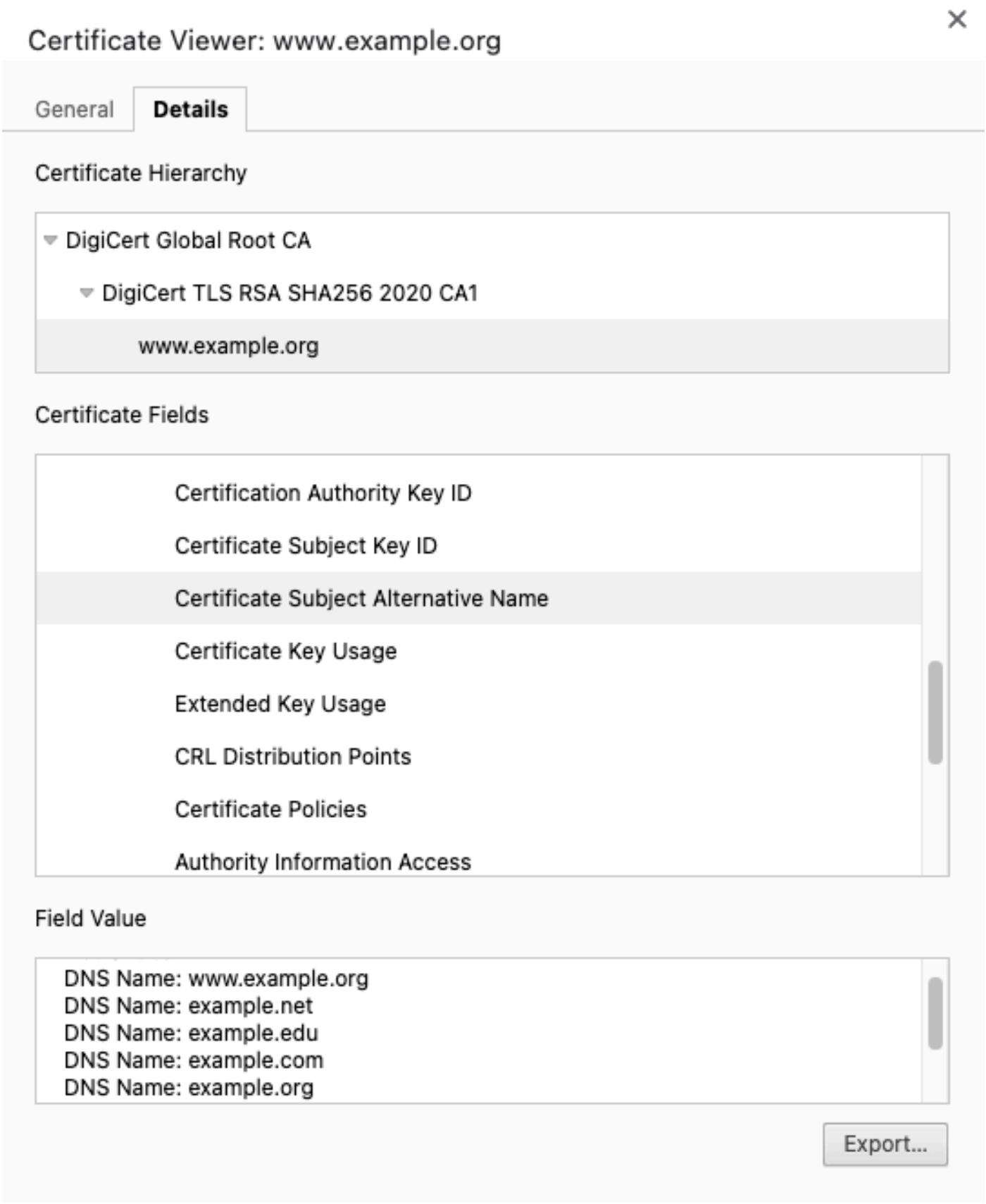
Dopo aver esaminato questo articolo, se non è possibile identificare il motivo per la pagina di errore 516, contattare il supporto tecnico Umbrella e fornirci le informazioni specificate nella sezione Errori di identità del certificato in questo documento.

Meccanismi di identificazione dei certificati

Quando si richiede un URL HTTPS, un browser o un altro client Web invia il nome di dominio nell'URL al server Web tramite l'estensione Server Name Indication (SNI) nel messaggio Hello del client della negoziazione TLS. Il server utilizza questo valore SNI per selezionare il certificato del server da restituire al client, poiché un server spesso ospita più siti Web e può avere certificati diversi per alcuni o tutti i siti.

Quando il certificato del server viene ricevuto dal client Web, il client verifica che il certificato sia quello corretto per la richiesta confrontando il nome di dominio richiesto con i nomi di dominio negli attributi Nome DNS dell'estensione Nomi alternativi soggetto del certificato. In questa

immagine vengono illustrate queste SAN in un certificato server.



16796247745556

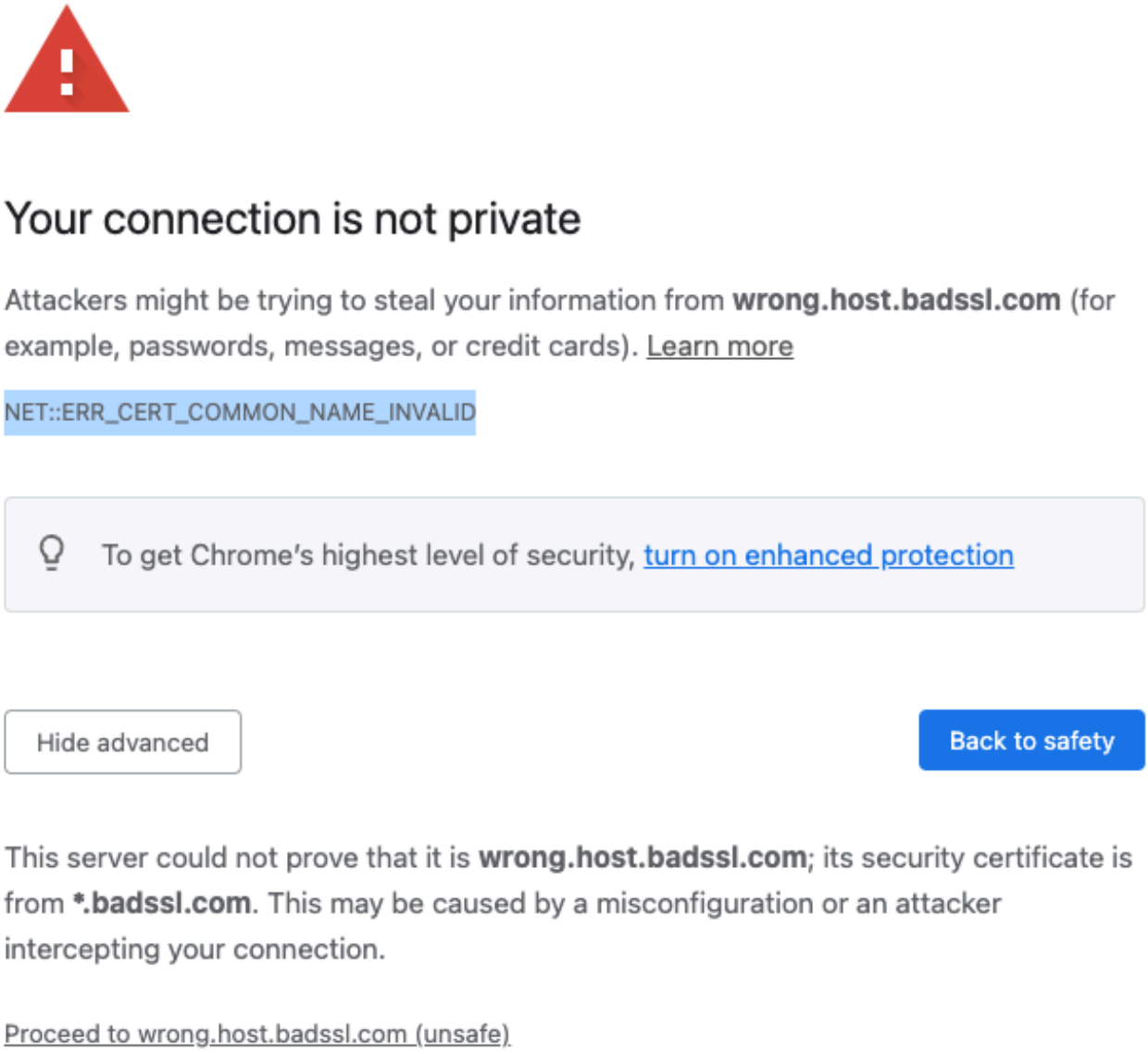
Questo server Web restituisce questo certificato in risposta alle richieste con questi valori SNI, nonché ad altri non visibili nel pannello Valore campo:

- www.example.org
- example.net
- example.edu
- example.com
- example.org

Si noti che il valore SAN "example.com" non corrisponde a un valore SNI di "www.example.com". Tuttavia, un SAN con caratteri jolly "*.example.com" corrisponderebbe a un SNI di "www.example.com" o a qualsiasi altro nome di dominio contenente una singola etichetta (una stringa senza "." carattere) anteposto a example.com, ma non a più etichette. Ad esempio, "www.hr.example.com" non corrisponde a "*.example.com" perché "www.hr" è costituito da due etichette: www e hr. Un singolo carattere jolly può corrispondere solo a una singola etichetta.

Errori di identità del certificato

Quando un client Web riceve un certificato server, se nessuno dei nomi DNS della SAN corrisponde all'SNI del nome di dominio nell'URL richiesto, il client Web in genere visualizza un errore per l'utente. Questa immagine mostra Chrome che visualizza una pagina interstiziale "NET::ERR_CERT_COMMON_NAME_INVALID".



16794294817428

Nell'immagine, il sito richiesto era "https://wrong.host.badssl.com" che non corrisponde ad alcuna delle SAN. Il certificato contiene un nome DNS SAN con caratteri jolly, "*.badssl.com" il cui carattere jolly può corrispondere solo a una singola etichetta, ad esempio "host". Inoltre, il certificato non dispone di un nome DNS SAN con il valore esatto "WRONG.host.badssl.com" o di una SAN con caratteri jolly di "*.host.badssl.com", pertanto viene visualizzato questo errore.

Per identificare il motivo di una mancata corrispondenza dell'identità del certificato, esaminare i nomi DNS SAN del certificato utilizzando la funzione di visualizzazione dei certificati del browser e confrontarli con il nome di dominio nell'URL richiesto. In alternativa, è possibile utilizzare uno strumento quale Qualys SSL Server Test per diagnosticare un problema di identità del certificato.

Se non è possibile identificare la causa dell'errore 516 dopo aver utilizzato le informazioni contenute in questa sezione o se non è possibile utilizzare le risoluzioni e le soluzioni indicate

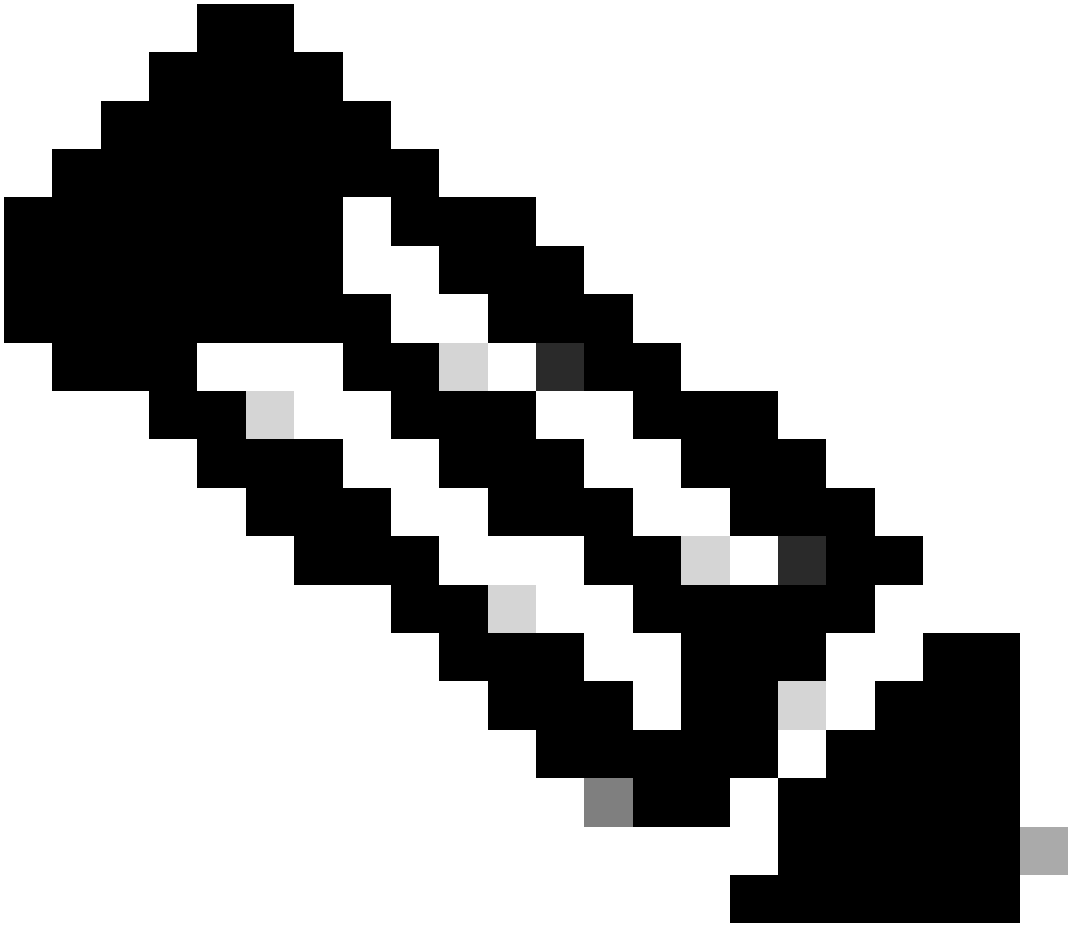
nella sezione successiva, aprire una richiesta di assistenza con il supporto tecnico Umbrella e fornire:

1. uno screenshot che cattura
    - la barra degli indirizzi del browser che mostra l'URL richiesto
    - l'intera pagina di errore 516 (vedere l'immagine nella sezione successiva)
2. il testo dell'URL copiato dalla barra degli indirizzi

Risoluzione

Per risolvere il problema, accedere al server con un nome di dominio corrispondente a uno dei nomi DNS SAN nel certificato. Per questo motivo può essere necessario che l'amministratore del sito Web aggiunga un nome di dominio corrispondente nel DNS per la zona. In alternativa, l'amministratore può emettere nuovamente il certificato per includere il nome di dominio dell'URL in uno dei nomi DNS della SAN.

Per ovviare al problema, il nome di dominio dell'URL può essere aggiunto a un elenco di decrittografia selettiva per il proxy Secure Web Gateway o a un elenco di destinazione nel proxy intelligente. Applicare l'elenco all'impostazione appropriata del set di regole per i criteri Web (Secure Web Gateway) o all'elenco di indirizzi consentiti per i criteri DNS (proxy intelligente). In questo modo si impedisce che la richiesta al sito Web venga decrittografata dal proxy, che impedisce al proxy di visualizzare una pagina di errore 516.



Nota: L'uso del proxy Secure Web Gateway e del proxy intelligente non è supportato. È possibile utilizzare una sola tecnologia proxy per organizzazione. È consigliabile che le organizzazioni che dispongono di sottoscrizioni per Secure Web Gateway utilizzino SWG e non utilizzino il proxy intelligente.

Il nome comune è deprecato

I client Web in origine corrispondevano al nome di dominio nell'URL richiesto con l'attributo Nome comune (CN) nel campo Oggetto del certificato. Questo meccanismo è stato deprecato nei moderni client web; i domini vengono ora confrontati con i nomi DNS dell'estensione del nome alternativo del soggetto. Tuttavia, il testo dei messaggi di errore spesso continua a fare riferimento al meccanismo deprecato, ad esempio "NET::ERR_CERT_COMMON_NAME_INVALID" in Chrome.

Analogamente, Umbrella SWG visualizza una pagina di errore 516 con questo testo quando il proxy SWG richiede un URL da un server Web e si verifica una mancata corrispondenza del nome DNS della SAN:

16794325789332

Cisco Umbrella prevede di aggiornare questo testo in futuro per riflettere meglio il comportamento corrente.

Ulteriori informazioni

Vedere la RFC 5280: Profilo CRL (Certificate and Certificate Revocation List) dell'infrastruttura a chiave pubblica Internet X.509, sezione 4.1.2.6 per informazioni sull'oggetto del certificato e sezione 4.2.1.6 per informazioni sul nome alternativo dell'oggetto.

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).