

Informazioni sugli errori di handshake e certificato SSL in Secure Access

Sommario

Problema

Il traffico HTTP bloccato a causa di errori di certificato e TLS può ora essere visualizzato nella ricerca di attività del dashboard. In questo articolo viene fornito un elenco di messaggi di errore comuni e una breve spiegazione per ognuno di essi.

Ambiente

- Cisco Secure Access - Ispezione SSL Secure Web Gateway

Risoluzione

Certificato upstream scaduto

Il certificato del sito Web è scaduto, quindi Cisco Secure Access non lo considera attendibile. Questa è sul proprietario del sito Web da correggere, quindi contattare il webmaster del sito e informarli.

Certificato upstream autofirmato

Il sito Web sta presentando un certificato firmato da se stesso, anziché uno rilasciato da

un'Autorità di certificazione attendibile. Poiché non esiste un'autorità indipendente che garantisca l'autenticità del certificato, Cisco Secure Access non è in grado di verificarla.

Spesso i certificati autofirmati vengono visualizzati su risorse destinate a un pubblico interno di piccole dimensioni: i portali amministrativi sulle appliance di sicurezza IT sono un classico esempio. Si noti solo che Cisco Secure Access non può essere configurato per considerare attendibili i certificati autofirmati.

Certificato intermedio mancante

Cisco Secure Access non è in grado di raccogliere tutti i certificati intermedi necessari, quindi non è in grado di creare la catena di attendibilità completa per una radice.

Ecco perché è importante: il certificato di un sito web (la "foglia") è firmato da un certificato intermedio, che a sua volta può essere firmato da un altro intermedio e così via fino a una radice attendibile. Affinché questa catena possa effettuare il check-out, il sito Web deve inviare i propri certificati intermedi insieme ai propri. Quando mancano, la convalida si interrompe, quindi informate il webmaster del sito.

Vi è un'eccezione: se il certificato include l'estensione "Authority Information Access" (AIA), Cisco Secure Access può tentare di recuperare i componenti intermedi mancanti. È necessario tenere presente che questa funzionalità è disponibile solo quando sono attivate sia la decrittografia HTTPS che l'ispezione dei file.

Nome soggetto mancante nel certificato upstream

Il certificato non include un nome soggetto (nome distinto) o un nome alternativo soggetto, ovvero non esiste alcun elemento che identifichi chiaramente l'appartenenza del certificato. In caso contrario, Cisco Secure Access non sarà in grado di convalidarlo. Questo è qualcosa che il proprietario del sito deve correggere.

Nome comune mancante nel certificato upstream

Il certificato non ha un nome comune (CN), ovvero il campo che tradizionalmente conteneva il nome host del sito e che ha contribuito a confermare che il certificato appartiene effettivamente al

sito visitato. In questi giorni, il controllo dipende dal nome alternativo del soggetto (SAN) e CN è considerato un campo legacy, ma la sua assenza può comunque causare questo errore. Rivolgersi al webmaster per richiedere l'indirizzamento.

Certificato upstream non attendibile

Cisco Secure Access non considera attendibile questo certificato, in genere perché non riconosce la CA radice che lo ha rilasciato.

Cisco Secure Access SWG tiene un elenco predefinito di Autorità di certificazione radice attendibili, fornito da un provider affidabile e aggiornato. Se il certificato di un sito viene ricondotto a una CA non inclusa in tale elenco, la convalida non riuscirà. Se si è certi che l'autorità di certificazione principale sia affidabile, contattare il supporto tecnico e verificare.

Il nome host nel certificato è diverso da quello previsto

L'indirizzo richiesto non corrisponde al nome del certificato, né al relativo nome comune (CN) né a uno dei relativi nomi alternativi soggetto (SAN). Poiché il certificato non sembra appartenere al sito che si sta raggiungendo, Cisco Secure Access non lo considera attendibile per questa richiesta. Il webmaster deve risolvere il problema.

Certificato upstream revocato

L'autorità di certificazione che ha rilasciato il certificato lo ha successivamente revocato, ovvero non è più considerato valido.

Cisco Secure Access lo conferma utilizzando il protocollo OSCP (Online Certificate Status Protocol), che verifica in tempo reale se un certificato è stato revocato. Informare il webmaster del sito in modo che possa sostituirlo.

Errori handshake TLS

Crittografia Upstream Non Supportata

Impossibile completare l'handshake TLS. Il sito Web non supporta le suite di cifratura utilizzate da Cisco Secure Access SWG. In questo modo si ha la tendenza a mostrare server obsoleti che offrono solo cifrature più deboli. La correzione è sul lato server, quindi passarla al webmaster.

Versione TLS upstream non corrispondente

Handshake non riuscito. Il sito Web non utilizza una versione TLS supportata da Cisco Secure Access SWG. Al momento, il proxy SWG Cisco Secure Access funziona con TLS 1.2 e TLS 1.3, sia per le connessioni in entrata dai client sia per le connessioni in uscita verso i server di destinazione.

Chiave DH a monte inferiore a 1024 bit

Impossibile completare l'handshake. Il sito Web utilizza una chiave Diffie-Hellman troppo debole (inferiore a 1024 bit) per l'accettazione di Cisco Secure Access. Si tratta di una limitazione sul lato server, quindi il webmaster deve rafforzarla.

Soluzioni

Per risolvere questi problemi, è possibile apportare modifiche alla configurazione in Cisco Secure Access.

Questa operazione deve essere eseguita solo se si considera attendibile l'autenticità del server e del certificato.

Per ovviare al problema, è possibile usare una voce "Elenco di decrittografia selettiva" per disabilitare la decrittografia o una voce "Domini esterni" per ignorare completamente il traffico proveniente da Cisco Secure Access. Cisco Secure Access non esegue la convalida del certificato quando la decrittografia è disabilitata.

Tenere presente che nella maggior parte dei casi il browser visualizza ancora un errore o un

avviso quando il traffico viene ignorato da Cisco Secure Access. I browser Web eseguono una convalida del certificato simile.

Causa

Il proxy di ispezione SSL di Cisco Secure Access non è in grado di completare l'handshake TLS, in genere perché la destinazione utilizza il pinning del certificato che rifiuta il certificato rifirmato CSA.

- Associazione certificato: prevista impronta digitale del certificato per i codici hardware del client
- CSA non attendibile sull'endpoint: certificato CA di ispezione non distribuito nell'archivio radice attendibile

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).