

Le pagine di avviso, conferma e EUN WSA non vengono visualizzate correttamente per le richieste HTTPS esplicite

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Problema](#)

[Soluzione](#)

Introduzione

In questo documento viene descritto un problema riscontrato in Cisco Web Security Appliance (WSA) quando le pagine di avviso, conferma o notifica all'utente finale (EUN) non vengono visualizzate correttamente per le richieste HTTPS esplicite. È inoltre disponibile una soluzione per questo problema.

Prerequisiti

Requisiti

Le informazioni fornite in questo documento presuppongono che:

- Gli indirizzi proxy WSA vengono distribuiti in modalità esplicita.
- Le richieste HTTPS sono bloccate, avviate o richiedono conferma da parte dell'utente.

Componenti usati

Le informazioni fornite in questo documento si basano sul WSA Cisco.

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.

Problema

Le pagine Avviso, Conferma o EUN non vengono visualizzate correttamente per le richieste HTTPS esplicite. Il browser visualizza una pagina di notifica incompleta oppure non visualizza affatto la pagina e visualizza una pagina di errore.

Quando si utilizzano richieste HTTPS esplicite, in queste pagine sono presenti diversi problemi. Quando si configura il browser per l'utilizzo di un proxy, il traffico HTTPS viene indirizzato a WSA su HTTP. La richiesta è formattata come HTTPS su HTTP.

Esistono due problemi noti relativi ai browser che non gestiscono correttamente le risposte HTTP restituite dal server di sicurezza di Windows per le richieste HTTPS esplicite. Quando una richiesta HTTPS esplicita viene bloccata, avvisata o richiede la conferma dell'utente, WSA restituisce un codice di stato 403. All'interno di questa risposta, il WSA include il contenuto della notifica che normalmente dovrebbe essere visualizzato sullo schermo in modo che sia visualizzabile. Tuttavia, in alcuni casi, il browser non è in grado di comprendere la risposta all'interno del contenuto restituito.

Questo è il comportamento del browser osservato:

- Quando si utilizza Internet Explorer versione 6 (IE6) e alcune versioni di IE7, queste richieste non consentono di eseguire il rendering del contenuto completo della risposta HTML. Il browser rispetta solo i primi byte (il contenuto all'interno del primo pacchetto) e ignora il resto. In questi casi, viene visualizzata una pagina incompleta contenente solo pochi caratteri. **Nota:** In questo caso, Cisco consiglia di ridurre la pagina di notifica predefinita dalla risposta WSA. Per ulteriori informazioni su come modificare la pagina EUN, consultare la sezione **Editing IronPort Notification Pages** del manuale **WSA User Guide**.
- Quando si usano IE8 e le versioni più recenti di Mozilla Firefox Release 3, il browser ignora completamente la risposta che il WSA restituisce e la maschera con la propria pagina di errore. Questo comportamento del browser vanifica lo scopo della notifica 403 e causa interruzioni con la funzione.

Soluzione

In questa sezione viene descritto il processo che si verifica quando viene abilitata la decrittografia HTTPS nel server di sicurezza globale. Per risolvere il problema descritto in precedenza, utilizzare le informazioni fornite per verificare che il sistema sia configurato di conseguenza.

Di seguito è riportato un esempio del flusso di traffico quando viene inviata una richiesta HTTPS esplicita:

- Quando la decrittografia HTTPS è abilitata, WSA convalida innanzitutto la richiesta in base ai criteri di decrittografia.
- Se la richiesta è contrassegnata per **PASSTHROUGH**, il traffico viene autorizzato (senza avviso o EUN).
- Se la richiesta è contrassegnata come **DECRITTOGRAFATA**, viene convalidata in base ai criteri di accesso. In questo caso, se il criterio di accesso è configurato per **WARN** o **BLOCK**, la pagina EUN viene visualizzata correttamente. Per Conferma l'utente deve passare alla pagina HTTP e Conferma, che richiede la navigazione attraverso il proxy e quindi al sito HTTPS.

- WSA ricorda l'indirizzo IP del client e non richiede un altro riconoscimento fino alla scadenza del timer.