

WSA-waarschuwing, bevestiging en EUN-pagina's worden niet correct weergegeven voor expliciete HTTPS-aanvragen

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Probleem](#)

[Oplossing](#)

Inleiding

Dit document beschrijft een probleem dat op de Cisco Web Security Appliance (WSA) wordt aangetroffen wanneer de pagina's Waarschuwing, Bevestiging of Eindgebruikermelding (EUN) niet correct worden weergegeven voor expliciete HTTPS-verzoeken. Er is ook een tijdelijke oplossing voor dit probleem.

Voorwaarden

Vereisten

De informatie in dit document gaat ervan uit dat:

- De WSA proxy-adressen worden in Expliciete modus ingezet.
- De HTTPS-verzoeken zijn geblokkeerd, gewaarschuwd of vereisen erkenning van de gebruiker.

Gebruikte componenten

De informatie in dit document is gebaseerd op de Cisco WSA.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Probleem

De pagina's Waarschuwing, ERKENNING of EUN worden niet correct weergegeven voor expliciete HTTPS-verzoeken. De browser geeft een onvolledige kennisgevingspagina weer of geeft de pagina helemaal niet weer en geeft in plaats daarvan een foutpagina weer.

Er zijn verschillende kwesties rond deze pagina's wanneer je expliciete HTTPS-verzoeken gebruikt. Wanneer u uw browser aanpast om een proxy te gebruiken, wordt HTTPS verkeer naar de WSA over HTTP geleid. Dit verzoek is geformatteerd als een HTTPS over HTTP.

Er zijn twee bekende kwesties met browsers die de HTTP-antwoorden niet correct verwerken die de WSA voor expliciete HTTPS-verzoeken teruggeeft. Wanneer een expliciet HTTPS-verzoek is geblokkeerd, gewaarschuwd of gebruikerserkenning vereist, geeft de WSA een 403 statuscode terug. In dit antwoord bevat de WSA de berichtinhoud die normaal op het scherm moet worden weergegeven, zodat deze zichtbaar is. In sommige gevallen kan de browser het antwoord echter niet begrijpen binnen de geretourneerde inhoud.

Dit is het browser gedrag dat wordt waargenomen:

- Wanneer Internet Explorer versie 6 (IE6) en bepaalde versies van IE7 worden gebruikt, geven deze verzoeken niet de volledige inhoud van het HTML-antwoord weer. De browser eert alleen de eerste paar bytes (de inhoud binnen het eerste pakket) en negeert de rest. In dergelijke gevallen ziet u een onvolledige pagina die slechts een paar tekens weergeeft. Opmerking: Als dit het geval is, raadt Cisco u aan om de standaardberichtpagina van het WSA antwoord te sluiten. Raadpleeg het gedeelte **Meldingspagina's van de WSA-gebruikershandleiding** voor meer informatie over het bewerken van uw EUN-pagina.
- Wanneer IE8 en nieuwere versies van Mozilla Firefox release 3 worden gebruikt, negeert de browser volledig het antwoord dat het WSA teruggeeft en maskeert met zijn eigen foutpagina. Dit browser gedrag is niet geschikt voor het doel van de 403 waarschuwing en veroorzaakt verstoring met de functie.

Oplossing

In deze sectie wordt het proces beschreven dat optreedt wanneer HTTPS-decryptie op de WSA is ingeschakeld. Als tijdelijke oplossing voor het eerder beschreven probleem gebruikt u de informatie die u hebt ontvangen om er zeker van te zijn dat uw systeem correct is geconfigureerd.

Hier is een voorbeeld van de verkeersstroom wanneer een expliciete HTTPS-aanvraag wordt verzonden:

- Wanneer HTTPS-decryptie is ingeschakeld, bevestigt de WSA eerst het verzoek tegen het decryptie beleid.
- Als het verzoek is gemarkeerd voor **PASSTHROUGH**, dan is het verkeer toegestaan door (geen waarschuwing of EUN).
- Als het verzoek is gemarkeerd als **DECRYPTED**, wordt het verzoek gevalideerd in overeenstemming met het toegangsbeleid. Als het toegangsbeleid in dit geval is ingesteld om een **BLOK** te **WAARSCHUWEN** of te **blokkeren**, dan wordt de EUN-pagina correct weergegeven. Helaas, voor bevestiging moet de gebruiker naar de HTTP pagina en de kennis

navigeren, wat navigatie door de proxy en dan naar de HTTPS site vereist.

- WSA herinnert het client IP adres en vereist geen andere bevestiging tot de timer afloopt.