Problemen met 516-fouten oplossen op Umbrella Secure Web Gateway

Inhoud

Inleiding

In dit document wordt beschreven hoe u een toename van 516 fouten op Umbrella Secure Web Gateway kunt oplossen.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op Umbrella Secure Web Gateway (SWG).

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 zorgen dat u de potentiële impact van elke opdracht begrijpt.

Overzicht

Gebruikers die door de Umbrella Secure Web Gateway (SWG) proxy met HTTPS Inspection bladeren, kunnen frequentere 516 Upstream Certificate CN Mismatch-foutpagina's ontvangen vanaf de tweede helft van oktober 2023.

De 516-foutpagina treedt op wanneer het certificaat van een website niet overeenkomt met de domeinnaam die door de client wordt gebruikt om toegang te krijgen tot de site.

De toename van foutpagina's is te wijten aan een verandering in de afhandeling van verzoeken van de Chrome-browser voor URL's die het HTTP-schema (niet-versleuteld) gebruiken. Chrome probeert nu eerst de bron te laden met het HTTPS-schema (versleuteld). Wanneer SWG is geconfigureerd voor HTTPS-inspectie, controleert het certificaat van een website en retourneert het een webpagina met een foutcode zoals 516 als het certificaat niet wordt geaccepteerd.

Om dit probleem te omzeilen, kunnen klanten hun webbeleid configureren om HTTPS-inspectie te omzeilen voor verzoeken die anders leiden tot 516 fouten.

516 Achtergrond fout

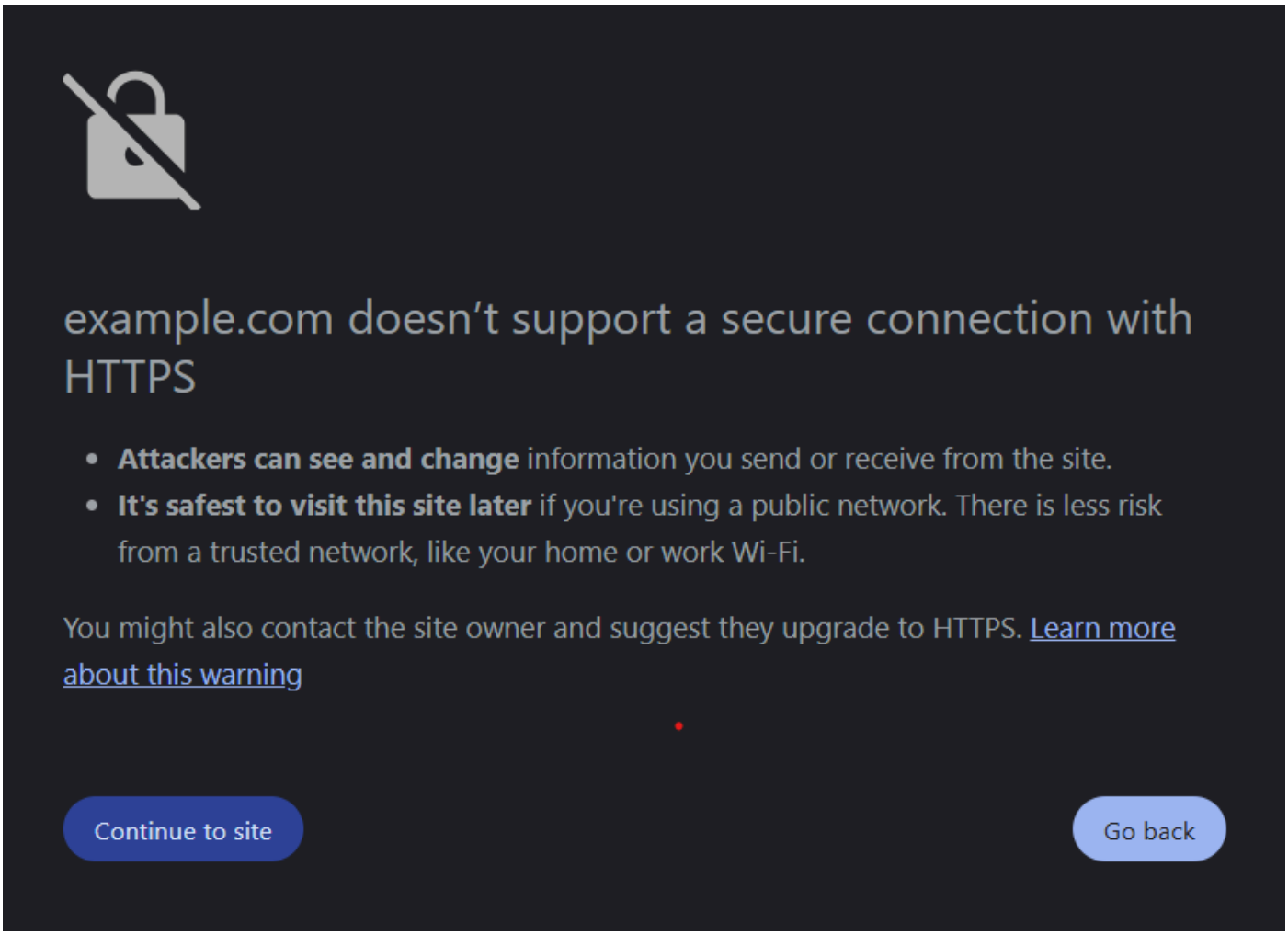
De Umbrella Secure Web Gateway retourneert een 516-foutpagina wanneer de domeinnaam die wordt gebruikt om toegang te krijgen tot een website via HTTPS niet wordt weergegeven in het digitale certificaat van de server. Voor meer informatie over de reden waarom Secure Web Gateway een 516-foutpagina retourneert, raadpleegt u het artikel "516 Upstream Certificate CN Mismatch" van de Umbrella Knowledge Base.

Overweeg bijvoorbeeld een site die inhoud van HTTP-URL's weergeeft in de vorm: http://www.example.com/path_to_content. Als een gebruiker de equivalente HTTPS-URL's aanvraagt, maar de site geen certificaat heeft waarvan de SAN's overeenkomen met www.example.com (misschien komt het SAN alleen overeen met example.com), ontvangt de gebruiker een 516-fout als het verzoek wordt afgehandeld door Umbrella's Secure Web Gateway met een webbeleid dat de HTTPS-inspectiefunctie van SWG gebruikt.

Gedragsverandering in Chrome

In de tweede helft van oktober 2023 voltooide Google de uitrol van een nieuwe functie voor de Chrome-browser. Na die datum wordt een aanvraag voor een HTTP-URL automatisch gedaan met behulp van de HTTPS-versie van die URL. Wanneer een gebruiker bijvoorbeeld een verzoek doet voor http://www.example.com, probeert Chrome eerst aan het verzoek te voldoen met behulp van https://www.example.com.

Als Chrome een HTTPS-gerelateerde fout ontvangt bij het aanvragen van de HTTPS-URL, probeert Chrome vervolgens dezelfde inhoud via HTTP te laden. Als de aanvraag voor de HTTP-URL succesvol is, geeft Chrome een interstitiële pagina weer met tekst die aangeeft dat de site niet veilig is en een link die de gebruiker de optie geeft om verder te gaan, volgens de onderstaande afbeelding.



Dit is het fallback-gedrag in de nieuwe functionaliteit van Chrome.

Als het HTTPS-verzoek echter een HTTPS-gerelateerde fout zoals "ERR_CERT_COMMON_NAME_INVALID" van de site oplevert, onderschept SWG de fout en retourneert een SWG-foutpagina naar Chrome, zoals de 516-foutpagina. Deze SWG-inhoud wordt niet beschouwd als een HTTPS-gerelateerde fout door Chrome, dus produceert het fallback-gedrag niet en wordt de SWG-foutpagina weergegeven in plaats van de pagina in de vorige afbeelding.

Meer informatie over het nieuwe Chrome-gedrag is te vinden in de Chromium-blog en de GitHub-repository van de functie.

De bron van de fout bepalen

Nu Chrome HTTP-URL's automatisch promoot naar HTTPS-URL's, worden websites die 516 fouten genereren vaker gezien door gebruikers.

Om te bevestigen dat een website een HTTPS-gerelateerde fout veroorzaakt, zoals het 516-antwoord, bladert u op de site met Chrome vanaf een desktopsysteem dat geen Umbrella gebruikt. Zorg ervoor dat u handmatig de HTTPS-versie van de URL expliciet invoert in de Omnibox van Chrome (zoals de adresbalk) in plaats van op een HTTP-hyperlink te klikken. Als een hyperlink een 516-fout met SWG heeft veroorzaakt, kan het handmatig aanvragen van de HTTPS-URL in Chrome zonder SWG de foutmelding "ERR_CERT_COMMON_NAME_INVALID"

produceren. Deze foutmelding bevestigt dat het probleem een onjuist certificaat is voor de domeinnaam die is gebruikt om toegang te krijgen tot de website.

U kunt ook een online tool gebruiken, zoals de Qualys SSL Server Test-site, om het probleem met de website te diagnosticeren.

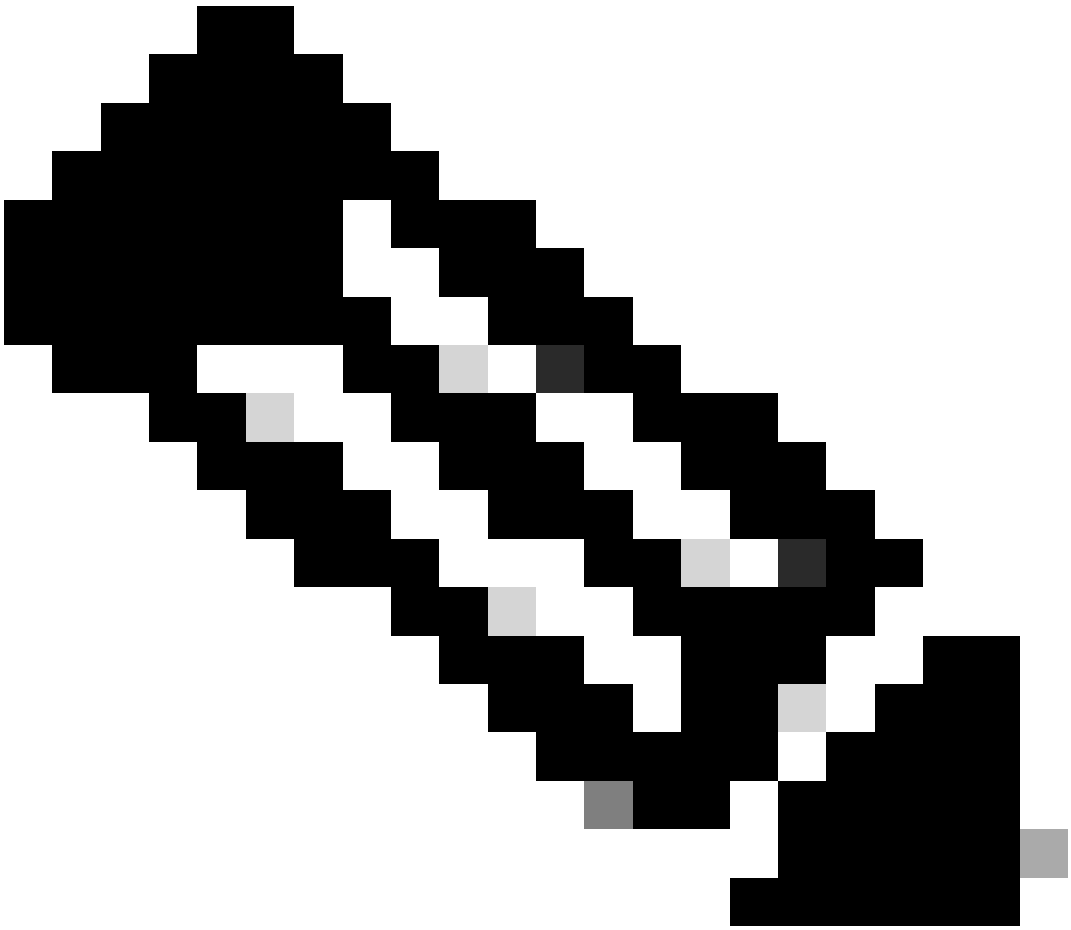
tijdelijke oplossingen

Paraplubeheerders kunnen het probleem oplossen met een van de volgende opties:

1. Maak een bestemmingslijst speciaal voor deze sites en voeg de lijst toe aan een webbeleid zonder HTTPS-inspectie.

2. Maak een selectieve decoderingslijst van sites die 516 foutpagina's produceren en voeg de selectieve decoderingslijst toe aan alle relevante webbeleidsregels

---



Opmerking: factoren zoals HTTP-omleidingen of e-mailbeveiligingssystemen die de HTTPS-URL's van hun service vervangen door de oorspronkelijke HTTP-URL's, kunnen de benodigde domeinnaam verhullen. Het identificeren van de juiste domeinnaam voor

---

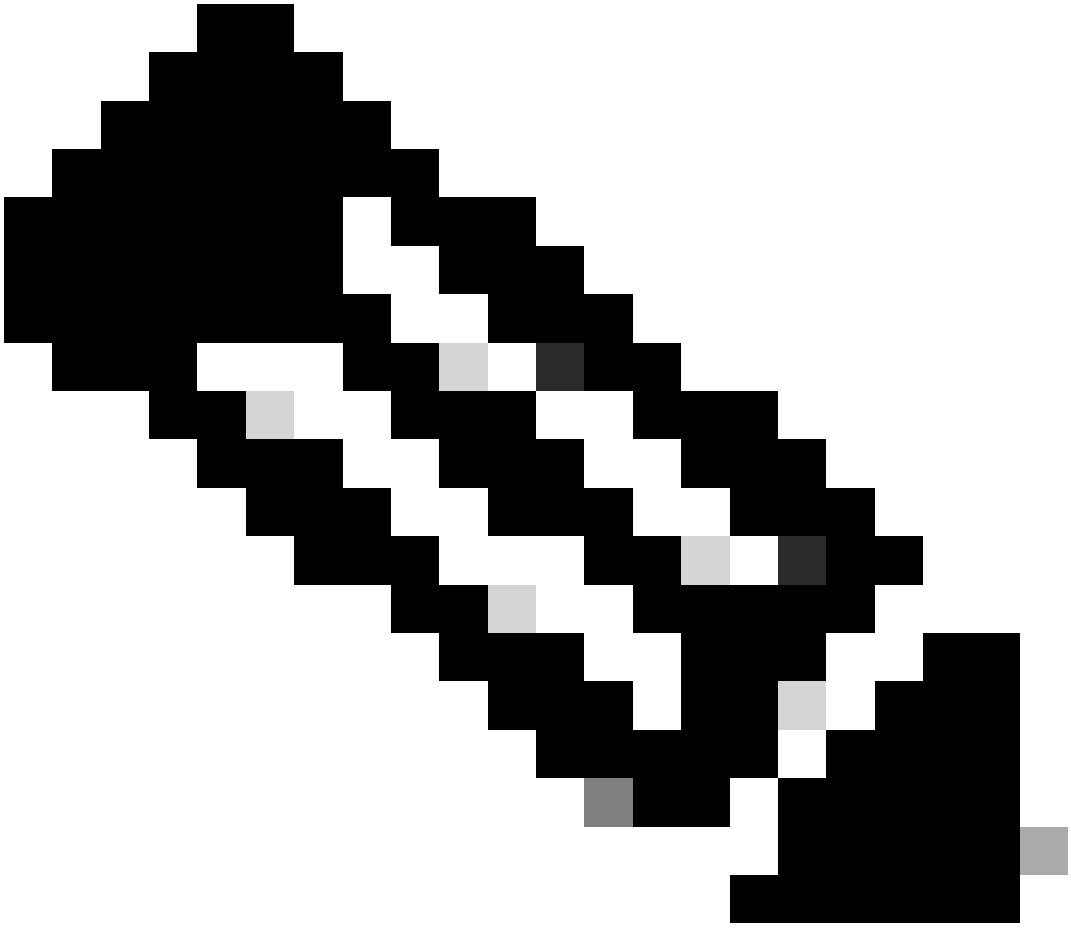
een bestemmingslijst of selectieve decoderingslijst kan onderzoek vereisen, inclusief het gebruik van specifieke tools (curl, Chrome Developer Tools, het logboek van een e-mailbeveiligingsleverancier, enzovoort).

516 Fouten en e-mailsystemen

Een toename van de 516-foutfrequentie kan het gevolg zijn van e-mailsystemen die e-mails in HTML-indeling weergeven en hyperlinks in de e-mails toestaan. Als de afzender bij het opstellen van een e-mail een domeinnaam in de hoofdtekst van de e-mail typt of plakt, wordt in veel e-mailsystemen automatisch een domeinnaam met platte tekst naar een hyperlink gepromoot. Wanneer de koppeling wordt gemaakt, is het schema meestal HTTP in plaats van HTTPS.

Als u bijvoorbeeld de tekenreeks `example.com` in een e-mail typt, wordt een e-mail met de HTML-code `<a href="http://www.example.com">` weergegeven als de hyperlink www.example.com.

Als een ontvanger van een dergelijke e-mail op die HTTP-hyperlink klikt, gebruikt het verzoek aanvankelijk HTTPS als de klik Chrome opent of als Chrome al wordt gebruikt om de e-mail te bekijken.



Opmerking: andere browsers kunnen ook HTTP naar HTTPS promoten.

Bovendien wordt een hyperlink in een e-mail die opzettelijk het HTTP-schema gebruikt, op dezelfde manier behandeld.

Sommige gangbare cloudservices verzenden e-mails van hun derde partij transactionele e-mailserviceproviders met HTTP-hyperlinks in plaats van HTTPS-hyperlinks. De HTTPS-site die Chrome automatisch probeert te laden, kan reageren met een certificaatfout op de domeinnaam in de e-maillink, zoals in dit voorbeeld van Segrid.

Wanneer deze e-mails grote lijsten met ontvangers hebben, kunnen veel gebruikers waarvan de klikken (of verzoeken) via SWG worden verzonden, fouten melden, zoals de 516-fout. Neem contact op met uw e-mailserviceprovider of de organisatie die de e-mail heeft verzonden om de certificaatfout te laten verhelpen.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.