Problemen met HSTS en fouten in pincertificaten oplossen

Inhoud

Inleiding

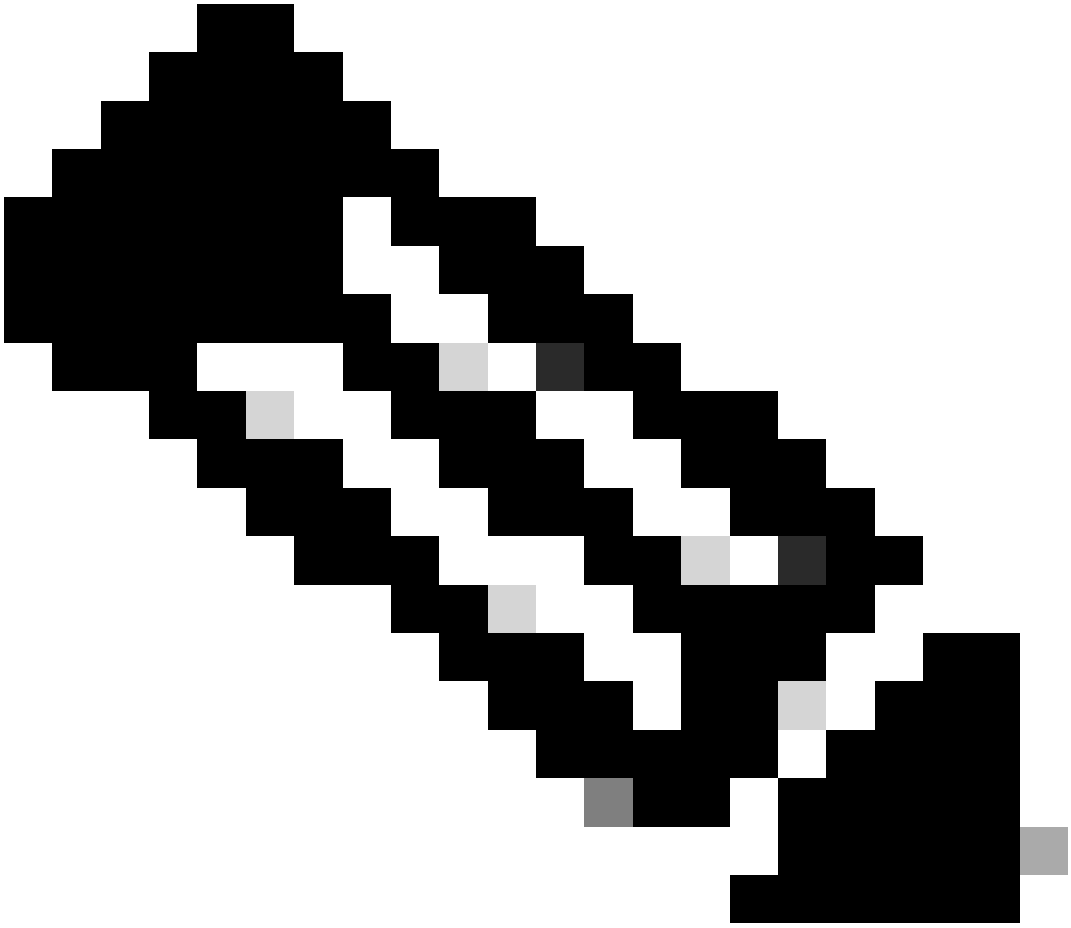
In dit document wordt beschreven hoe u een certificeringsfout "Your Connection is Untrusted/Not Private" (Uw verbinding is niet vertrouwd/niet privé) kunt wissen die niet kan worden omzeild.

Certificaatfout

Wanneer een certificaatfout voor `*.opendns.com` of `*.cisco.com` wordt weergegeven, maar niet kan worden omzeild door een certificaatuitzondering toe te voegen zoals beschreven in de Cisco Umbrella-documentatie Beheer het Cisco Umbrella Root Certificate, gebruikt u deze stappen om de certificaatfout te laten verwijderen.

Wanneer u de certificaatfout niet kunt omzeilen door een uitzondering toe te voegen, is dit vanwege de implementatie van HTTP Strict Transport Security (HSTS) of vooraf geladen Certificate Pinning in moderne browsers. Communicatie tussen bepaalde browsers en bepaalde websites gebeurt op een manier die de vereiste omvat om HTTPS te gebruiken en er is geen bypass of uitzondering mogelijk. Deze extra beveiliging voor HTTPS-pagina's voorkomt dat de Umbrella Block Page en het Bypass Block Page-mechanisme werken wanneer HSTS actief is voor een website.

Als gevolg hiervan kan de pagina in kwestie niet worden geopend via Block Page Bypass (BPB) (in feite wordt het Bypass-scherm mogelijk niet eens weergegeven). Deze methoden kunnen toegang tot de BPB-login toestaan, maar na de aanmelding verschijnt de certificaatfout opnieuw en wordt de toegang geweigerd. Bekijk de rest van dit artikel als u een certificaatfout ziet in Google Chrome, Mozilla Firefox, Safari die niet kan worden omzeild en u probeert toegang te krijgen tot de bypass-aanmelding.



Opmerking: er is nu een oplossing voor dit probleem beschikbaar die gemakkelijker te beheren en voor alle sites permanent is.

Hierdoor is deze informatie nog steeds toepasbaar maar kan er nu met een permanente oplossing worden omheen gewerkt. Probeer de Cisco Root CA te installeren via de Cisco Umbrella-documentatie: Het Cisco Umbrella Root Certificate beheren

---

BELANGRIJK: Als het domein op de vastgezette lijst van HSTS staat, kan een uitzondering niet worden toegevoegd omdat de lijst effectief niet kan worden omzeild als u Chrome, Safari of Firefox uitvoert (Internet Explorer (IE) wordt niet beïnvloed). Blokpagina-bypass werkt niet voor sites als deze. Voor een volledige lijst met services die HSTS gebruiken door deze drie browsers, raadpleegt u de Google Chromium Code Search. Bekende services in deze lijst zijn:

- Google (en Google-bronnen, zoals Gmail, YouTube of Google Docs)
- Dropbox
- tjilpen
- Facebook

Als dit een probleem veroorzaakt voor u of uw gebruikers en u wijzigingen wilt zien in de Blokkeer pagina omzeilen om dit probleem te verhelpen, kunt u een e-mail sturen naar umbrella-support@cisco.com of uw accountmanager om een aanvraag voor een functie in te dienen. Onze productmanagement- en engineeringteams zijn zich bewust van problemen met certificaten en het omzeilen van blokpagina's en testen alternatieve herontwerpen van deze functie.

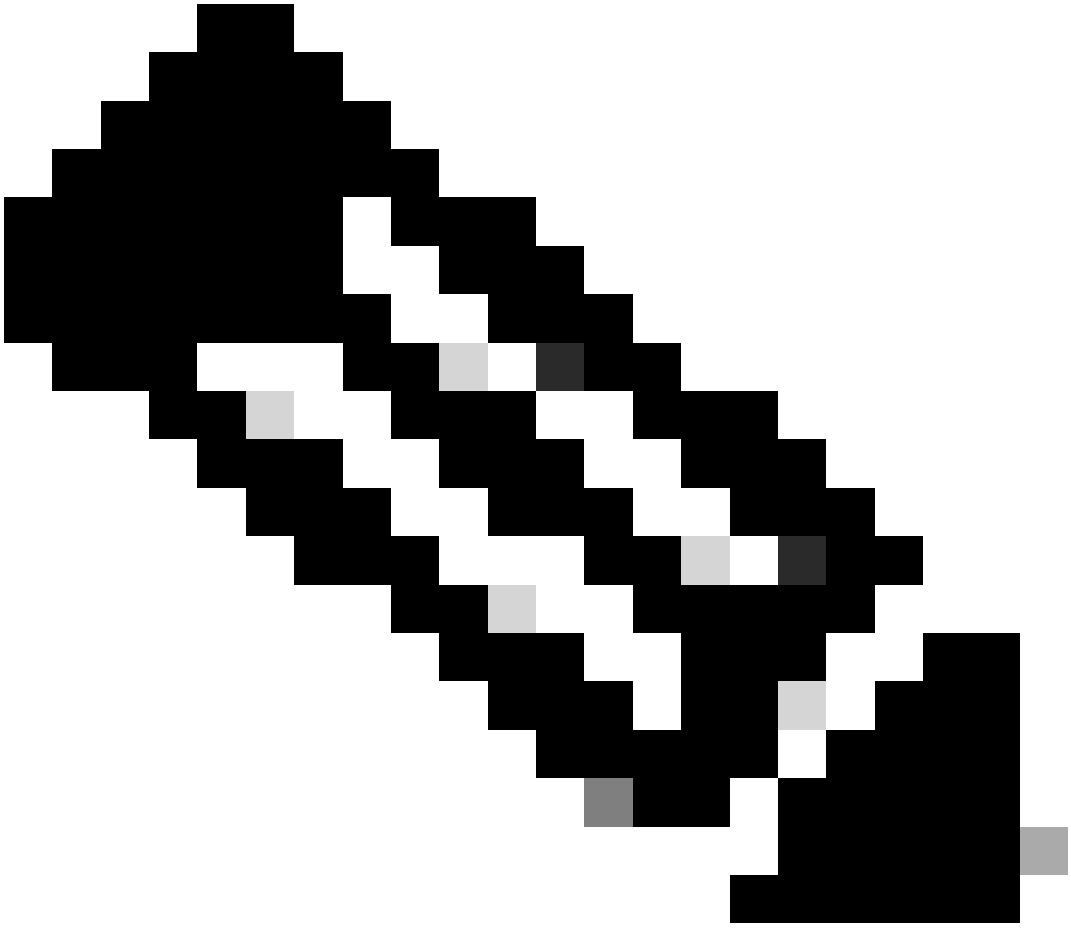
Mogelijke oplossingen

Er zijn een paar manieren om deze problemen op te lossen. Ten eerste laten deze secties zien hoe u gedetailleerder beleid kunt gebruiken om dit probleem te omzeilen. Ten tweede kunt u browserconfiguraties gebruiken, maar deze worden geïsoleerd tot een subset van de browsers die door dit probleem worden beïnvloed.

Beleidsbeheer en de roamingclient

Er kunnen problemen zijn met uw netwerkconfiguratie of het beleid voor aanvaardbaar gebruik (HR) dat deze oplossing voorkomt. Beleidsbeheer is geen effectieve oplossing als gebruikers deze domeinen alleen op bepaalde tijden mogen bezoeken (zoals tijdens hun lunchpauze). Umbrella kan geen op tijd gebaseerde beleidsapplicatie bieden met onze service, dus het zou problematisch kunnen zijn om een gebruiker de hele tijd toegang te geven tot de site. Op een gedeelde computer, zoals een openbare terminal, kan de Umbrella-roamingclient geen onderscheid maken tussen gebruikers en kan hij niet gemakkelijk de juiste domeinen voor de juiste mensen toestaan.

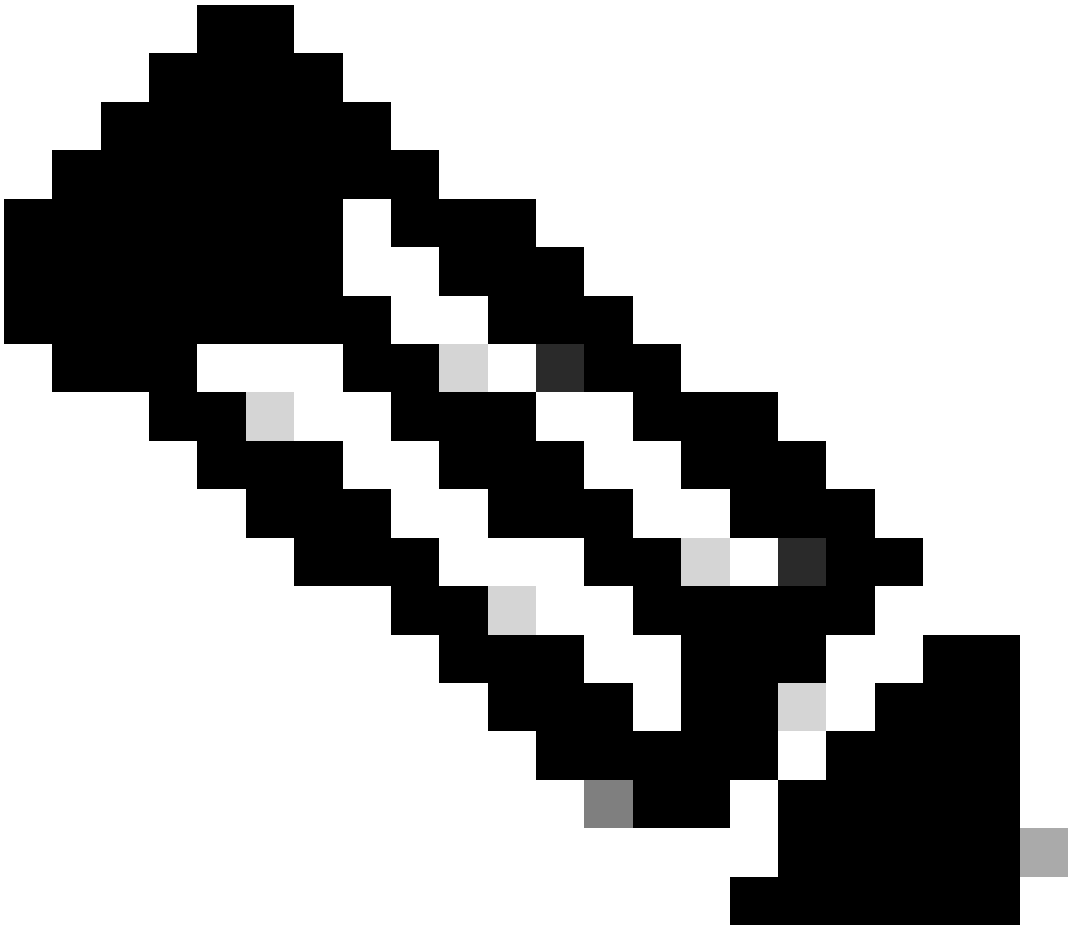
Beleidsbeheer is niet zo effectief bij het overwegen van niet-granulaire identiteiten, zoals Sites of Netwerken, tenzij de beheerder zich op zijn gemak voelt en alle gebruikers van dat netwerk dezelfde toegang geeft. Beleidsbeheer werkt het beste wanneer het wordt toegepast op een subset van gebruikers die toegang hebben tot sites terwijl de rest van het netwerk dat niet kan, en deze gebruikers uitkiezen door de roamingclient op hun machines te installeren en de juiste beleidshiërarchie toe te passen.



Cisco kondigde het einde van de levensduur voor Umbrella Roaming Client op 2 april 2024. De laatste datum van ondersteuning voor Umbrella Roaming Client is 2 april 2025. Alle functies van Umbrella Roaming Client zijn momenteel beschikbaar in Cisco Secure Client. Cisco biedt alleen toekomstige innovaties in Cisco Secure Client. We raden klanten aan om nu al te beginnen met het plannen en plannen van hun migratie. Raadpleeg dit KB-artikel voor richtlijnen voor het migreren van de Umbrella Roaming Client naar Cisco Secure Client.

Goed beleidsbeheer is de beste oplossing voor dit probleem, omdat de browser in de eerste plaats geen mislukte validatierespons ontvangt. Als sommige van uw gebruikers toegang hebben tot sites die ze normaal gesproken zouden moeten gebruiken om de pagina te blokkeren om toegang te krijgen, kunt u in plaats daarvan een apart beleid voor deze gebruikers configureren en de domeinen toevoegen die ze kunnen gebruiken om de lijst met machtigingen te gebruiken. Aangezien de verzoeken van de gebruikers nooit worden geblokkeerd, ontvangt de browser nooit een verzoek van een domein met een niet-overeenkomend certificaat. U kunt de Umbrella Roaming Client gebruiken om dit specifieke beleid te leveren. Dit betekent dat u bepaalde domeinen op elk moment van de

dag in een lijst met machtigingen plaatst om deze fouten te omzeilen.



Opmerking: de Umbrella-roamingclient is een effectieve manier om bepaalde beleidsregels aan meerdere gebruikers te distribueren, maar als u de Active Directory(AD)-integratie hebt ingeschakeld, kunt u deze toegestane beleidsregels ook op bepaalde AD-gebruikers toepassen.

Fouten met uitzondering van certificaten negeren (alleen Chrome voor Windows)

Alleen Chrome voor Windows kan worden geconfigureerd om fouten in de certificaatuitzondering te negeren, waardoor deze fout wordt beperkt. De browser wordt verteld om de fout te negeren en in plaats daarvan wordt de normale Umbrella-blokpagina weergegeven.

BELANGRIJK: Deze methode is riskanter dan het aanpassen van uw beleidsbeheer, omdat de browser is geconfigureerd om certificaatfouten te negeren. Het is mogelijk dat hierdoor de browser

onderhevig kan zijn aan man-in-the-middle (MiTM) aanvallen. Als gevolg hiervan kunnen we dit niet aanbevelen als een veilige aanpak van deze fout, maar het is een tijdelijke oplossing.

Deze configuratiewijzigingen moeten per computer worden doorgevoerd, wat het moeilijk maakt voor grootschalige omgevingen, maar het werkt wel.

Firefox, Safari en Chrome voor Mac OS X

Firefox, Safari en Chrome voor Mac OS X kunnen niet worden geconfigureerd om certificaatuitzonderingsfouten voor vastgezette domeinen te negeren en altijd de HSTS-lijst te respecteren. Er is geen bekende oplossing voor deze fouten.

Internet Explorer

Internet Explorer (IE) implementeert geen HSTS-beperkingen. Als gevolg hiervan hoeft IE niet te worden geconfigureerd en wordt deze fout niet weergegeven. Dit is onderhevig aan wijzigingen in toekomstige versies van IE als Microsoft ervoor kiest om HSTS in de browser te implementeren.

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.