

SSL-decoderingscertificaat Fout bij afhandeling van beveiligde toegang

Inhoud

uitgeven

Gebruikers krijgen te maken met certificaatgerelateerde foutpagina's wanneer SSL-decodering is ingeschakeld in Cisco Secure Access. Er zijn meerdere vragen ontvangen met betrekking tot drie specifieke soorten certificaatfouten:

- Fouten in certificaat van oorsprong van server verlopen
- CN/SAN-fouten met betrekking tot certificaten waarbij de algemene naam of alternatieve onderwerpnamen die op het certificaat worden vermeld, niet overeenkomen met het gebruikte domein
- Koppeling Certificate Revocation List (CRL) ingesloten in het certificaat van de oorspronkelijke server waardoor connectiviteitsproblemen ontstaan

Deze certificaatfouten zijn vergelijkbaar met waarschuwingen die normaal in webbrowsers worden weergegeven. De vraag rijst of Cisco Secure Access certificaatgerelateerde fouten kan verwerken door waarschuwingspagina's weer te geven (vergelijkbaar met browsers of inhoudsfilters) en vervolgens toegang toe te staan na het weergeven van de waarschuwing of in alle gevallen toegang toe te staan. Bovendien is het noodzakelijk om het gedrag te begrijpen wanneer SSL-decodering is uitgeschakeld en of het verkeer doorgaat, ongeacht certificaatproblemen.

milieu

- Cisco Secure Access - internettoegang (roamingmodule, VA, DNS, SWG, PAC, IPS, certificaten)
- SSL-decoderingsfunctionaliteit ingeschakeld
- Meerdere domeinen met problemen met certificaatvalidatie

- Origin-servers met verschillende certificaatproblemen, waaronder vervaldatum en domeinmismatch

resolutie

Beperkingen voor afhandeling van fouten in certificaten

Foutafhandeling met betrekking tot certificaten is niet beschikbaar in Cisco Secure Access. Het product ondersteunt niet:

- Browserachtige waarschuwingspagina's voor certificaatproblemen presenteren
- Domeinspecifieke configuratie voor foutafhandeling van certificaten
- Aangepaste foutafhandeling op basis van doeldomeinen
- Waarschuwingspagina's in de stijl van een inhoudsfilter met opties voor overschrijven door de gebruiker

Oplossing voor uitsluiting van SSL-decodering

De aanbevolen aanpak is om problematische domeinen uit te sluiten van SSL-decodering met behulp van de instellingen voor het decoderen van het beveiligingsprofiel. Dit kan worden geconfigureerd via:

Navigeer naar het gedeelte Beveiligingsprofiel > Decryptie-instellingen om specifieke domeinen uit te sluiten van SSL-inspectie.

Wanneer domeinen worden uitgesloten van SSL-decodering, treedt dit gedrag op:

- Verkeer voor uitgesloten domeinen omzeilt SSL-inspectie volledig
- Certificaatvalidatie wordt niet uitgevoerd door Secure Access
- Gebruikers komen geen certificaatfoutpagina's tegen die zijn gegenereerd door Secure Access

- De oorspronkelijke certificaatfouten zijn mogelijk nog steeds zichtbaar in de gebruikersbrowser als de certificaatproblemen blijven bestaan

SSL-decodering uitgeschakeld

Wanneer SSL-decodering is uitgeschakeld voor een domein of wereldwijd, wordt het verkeer door Cisco Secure Access doorgestuurd (doorgestuurd), ongeacht eventuele certificaatproblemen. Het product inspecteert of valideert geen certificaten wanneer decodering niet is ingeschakeld, waardoor al het HTTPS-verkeer op transparante wijze kan passeren.

Oorzaak

De certificaatfouten worden veroorzaakt door legitieme problemen met certificaatvalidatie op de oorspronkelijke servers, waaronder verlopen certificaten, CN/SAN-mismatches en CRL-connectiviteitsproblemen. Cisco Secure Access voert certificaatvalidatie uit als onderdeel van het SSL-decoderingsproces en wanneer deze validatiefouten optreden, genereert het product foutpagina's om mogelijk onveilige verbindingen te voorkomen. Dit is het beoogde beveiligingsgedrag van de SSL-inspectiefunctie.

Verwante inhoud

- [Configuratiedocumentatie voor Cisco Secure Access-decodering](#)
- [Cisco Technical Support en downloads](#)

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.