Problemen met het intrekken van browsercertificaten oplossen tijdens het gebruik van Umbrella Filtering

Inhoud

Inleiding

In dit document wordt beschreven hoe u fouten bij het intrekken van browsercertificaten kunt oplossen tijdens het gebruik van Umbrella-filtering.

uitgeven

Bij het gebruik van de modus Alleen toestaan of restrictieve categorie-instellingen moet u vaak meerdere domeinen toevoegen aan de lijst om een site goed te kunnen laden.

Een specifiek probleem is dat Certificate Revocation Lists (CRL's) voor HTTPS / SSL-websites kunnen worden geblokkeerd, wat op zijn beurt fouten genereert in sommige browsers. Soms zorgt het blokkeren van deze CRL's ook voor latentie terwijl de browser probeert zijn validatie uit te voeren.

Oorzaak

CRL's (Certificate Revocation Lists) en nieuwere OCSP (Online Certificate Status Protocol) worden gebruikt om een certificaatautoriteit te vragen of een SSL-certificaat om welke reden dan ook is ingetrokken. Dit gebeurt meestal transparant op de achtergrond wanneer u verbinding maakt met een HTTPS-website.

Het idee is dat de browser stopt met de gebruiker naar de website te gaan als het certificaat is ingetrokken in het geval dat het certificaat / CA in gevaar is gebracht. Het is een goed idee om toegang tot CRL's toe te staan.

In de modus Alleen toestaan worden de meeste CRL's geblokkeerd, tenzij u ze specifiek hebt gedeblokkeerd. De impact hiervan hangt af van welke webbrowser wordt gebruikt...

- Internet Explorer 7 toont een pop-upwaarschuwing met een fout zoals hieronder. De intrekkingsgegevens voor het beveiligingscertificaat voor deze site zijn niet beschikbaar.

- Latere versies van Internet Explorer vertonen geen fouten tenzij een specifieke registersleutelvlag is ingesteld.
- Google Chrome toont een waarschuwing naast de adresbalk. Als u op de waarschuwing klikt, wordt deze fout weergegeven: Kan niet controleren of het certificaat is ingetrokken
- Firefox vertoont geen fouten, tenzij security.OCSP.require instelling is ingesteld in about:config

resolutie

1. Zoek de CRL voor het certificaat door het certificaat in uw webbrowser te bekijken (stappen variëren afhankelijk van de browser).
2. Gebruik het tabblad 'Details' en zoek naar deze informatie:
    - CRL-distributiepunten
    - toegangsgegevens van de autoriteit
3. Noteer de URL-informatie (voorbeeld hieronder) en voeg deze toe aan de lijst met toegestane URL's op uw Umbrella-dashboard:

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.