

Problemen met toegang tot SWG-website oplossen

Inhoud

[Inleiding](#)

[Achtergrondinformatie](#)

[Fout "Toegang geweigerd 403" door upstream-blokkering](#)

[Fout "Toegang geweigerd 403" door Java-probleem](#)

[Oorzaak van probleem op hoog niveau](#)

[Wat is Java-gerelateerd probleem met MPS?](#)

[resolutie](#)

[Wat is een 502 Bad Gateway?](#)

[Algemene factoren voor 502 Bad Gateway](#)

[Niet-ondersteunde SWG-coderingssuites](#)

[resolutie](#)

[Aanvraag voor verificatie clientcertificaat](#)

[Headers toegevoegd door Proxy](#)

[resolutie](#)

Inleiding

In dit document wordt beschreven hoe u problemen met de toegang tot websites kunt oplossen die worden gezien met de Umbrella Secure Web Gateway (SWG) Proxy.

Achtergrondinformatie

Laten we aannemen dat de website www.xyz.com niet toegankelijk is via SWG-proxy en wanneer gebruikers direct toegang proberen te krijgen tot internet (zonder dat Umbrella SWG in beeld is), werkt het prima. Laten we verschillende symptomen en verschillende soorten foutmeldingen bekijken die worden gemeld wanneer de website niet toegankelijk is via SWG. De meest voorkomende zijn 502 slechte gateway, 502 kon geen upstream-fout doorgeven, upstream-certificaat ingetrokken, toegang geweigerd 403 verboden, upstream-cijfers mismatch, website net getimed na het draaien voor enige tijd of vergelijkbaar.

Fout "Toegang geweigerd 403" door upstream-blokkering

Webserver of upstream-zijde blokkeert of verstikt onze SWG-proxy IP-bereik. Bijvoorbeeld, Akamai WAF blok heeft een aantal SWG uitgang IP bereiken vermeld. Om dit probleem op te lossen, is de enige optie dat we contact opnemen met websitebeheerders en hen onze IP-bereiken laten deblokken. Tot die tijd kunt u SWG omzeilen met behulp van de externe domeinbeheerlijst voor AnyConnect SWG- en PAC-bestandsimplementaties. Kortom, dit soort

problemen is niet vanwege de proxy zelf, maar vanwege de incompatibiliteit tussen proxy en webserver. Hier is de link om de KB specifiek te verwijzen voor "Toegang geweigerd 403" -fout als gevolg van het blok van Egress IP.

Daarnaast is hier de [link](#) die enkele mogelijke redenen behandelt waarom Akamai IP-adressen heeft geblokkeerd.

Fout "Toegang geweigerd 403" door Java-probleem

De website is niet toegankelijk en gooit "Toegang geweigerd of 403 Verboden - Umbrella cloud security gateway error" wanneer het verzoek wordt verzonden via SWG MPS-proxy met de bestandsinspectie-instelling ingeschakeld. Maar als Bestandsinspectie is uitgeschakeld, worden websites met succes geladen. Of als we de website in bypass-decodering plaatsen, worden websites met succes geladen.

Oorzaak van probleem op hoog niveau

Wat is Java-gerelateerd probleem met MPS?

De site of webserver in kwestie retourneert een TLS-waarschuwing met betrekking tot SNI of SSL-waarschuwing terug naar de proxy nadat de proxy probeert verbinding te maken met de server. Dit gebeurt nadat de klant hello is gestuurd. MPS-proxy (die is gebaseerd op Java en als zodanig) behandelt elke TLS-waarschuwing met "Niet-herkende naam" in het beschrijvingsveld als een fout tijdens SNI-parsing en beëindigt de transactie. Meer details vind je [hier](#)

Houd er rekening mee dat dit geen SWG- of MPS-proxyprobleem is. Dit is een van de onverenigbaarheden met SWG of andere proxy's als gevolg van een verkeerde configuratie aan de serverzijde. Browsers negeren deze waarschuwing meestal, maar SWG of een ander inhoudsbeveiligingsfilter behandelt de SSL-waarschuwing als een fatale fout en beëindigt de sessie, wat resulteert in 403 verboden foutpagina's voor de gebruikers. Het kan ook 502 Bad Gateway-fout melden, maar met de meeste voorbeelden hebben we 403 verboden fout gezien, zoals te zien is in deze afbeelding.

403 Forbidden

Umbrella Cloud Security Gateway

15151734443924

Omdat MPS op de applicatielaag werkt, heeft het weinig tot geen controle over hoe de TLS-laag de transactie afhandelt op basis van de waarschuwingen die in het TLS-protocol worden geproduceerd. Het is de verantwoordelijkheid van de server om ervoor te zorgen dat hun TLS-eindpunt/certificaten correct zijn geconfigureerd. Raadpleeg deze [link](#).

Om het probleem te beperken of op te lossen, kan het gemakkelijk worden aangegeven vanuit

Java 7u25	Client aborts on SNI unrecognized_name warning RSA 2048 (SHA256) TLS 1.0 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1
Java 8u161	Client aborts on SNI unrecognized_name warning RSA 2048 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 ECDH secp256r1
Java 11.0.3	Client aborts on SNI unrecognized_name warning RSA 2048 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1
Java 12.0.1	Client aborts on SNI unrecognized_name warning RSA 2048 (SHA256) TLS 1.2 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 ECDH secp256r1

15152060146964

Wanneer de website wordt geopend zonder SWG-proxy in het midden of HTTPS-inspectie van SWG omzeilen, werkt de website omdat de browser de SNI Unrecognized name alert negeert en blijft communiceren met de webserver.

Op het moment van schrijven van dit artikel is de aanbevolen oplossing de beste oplossing die we u kunnen voorstellen. In de nabije toekomst, met de nieuwe proxy-architectuur, zijn we in staat om deze problemen sierlijker aan te pakken.

resolutie

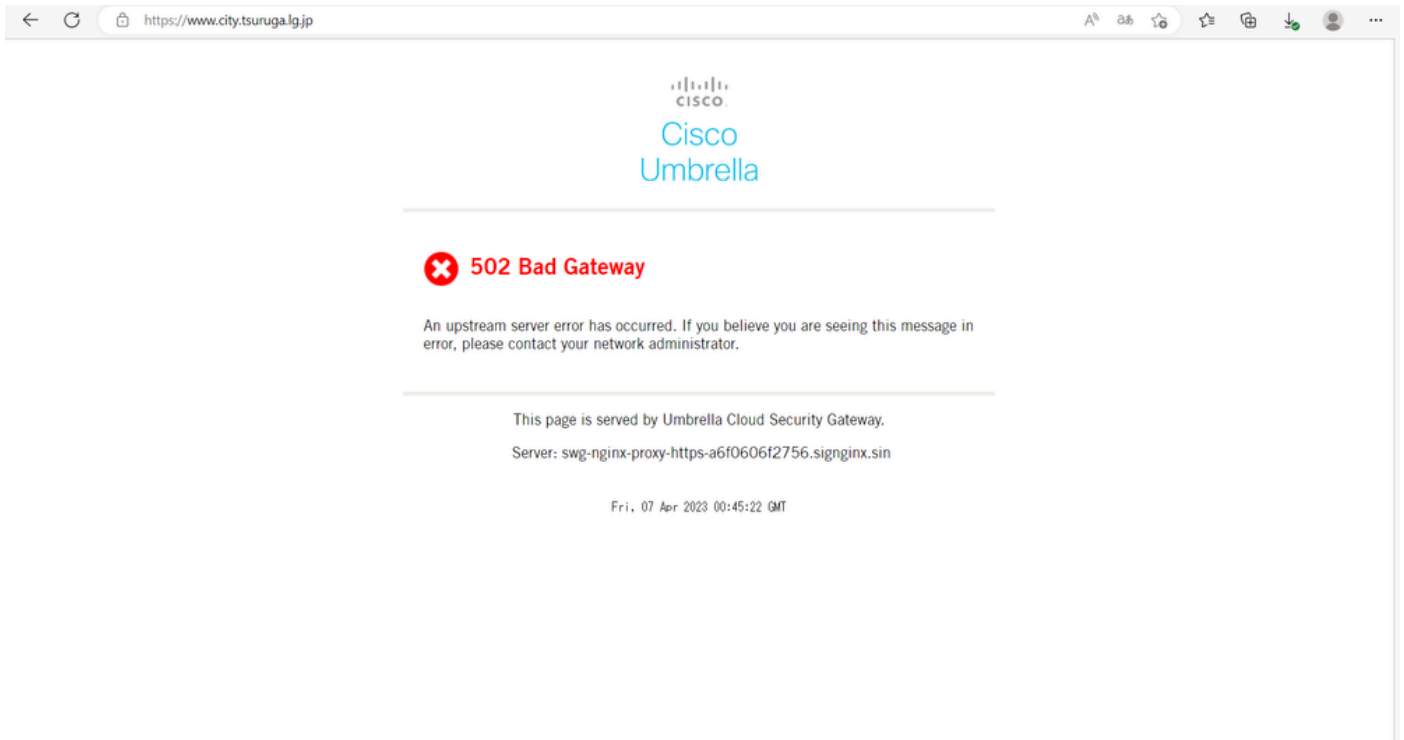
1. Decryptie voor de betreffende domeinen uitschakelen - OF
2. Voeg het domein toe aan een bestemmingslijst en koppel een allow-regel (als u de site vertrouwt)

Wat is een 502 Bad Gateway?

Een 502 Bad Gateway-fout betekent dat de server als gateway of proxy fungeerde en een ongeldig antwoord van de upstream-server ontving. Wanneer de gebruiker probeert toegang te krijgen tot de website via SWG Proxy, zijn er twee communicatiestromen.

- a) Client --> Proxyverbinding (downstream)
- b) Proxy-> Einde webserververbinding (Upstream)

502 Fout bij slechte gateway treedt op tussen SWG-proxy (MPS, Nginx) en eindserververbinding.



15026978020884

Algemene factoren voor 502 Bad Gateway

1. Niet-ondersteunde SWG-coderingssuites
2. Verzoek om verificatie van clientcertificaat
3. Kopteksten toegevoegd of verwijderd door SWG Proxy

Niet-ondersteunde SWG-coderingssuites

Laten we aannemen dat een webserver niet-ondersteunde SWG-coderingssuites rapporteert tijdens TLS-onderhandelingen. Houd er rekening mee dat SWG MPS (Modular Proxy Service) Proxy de TLS_CHACHA20_POLY1305_SHA256-codeersuite niet ondersteunt. Houd er rekening mee dat er een apart artikel is voor SWG-ondersteunde coderingssuites en TLS. We kunnen dit probleem eenvoudig vaststellen door andere pakketten te bekijken die zijn vastgelegd tijdens de uitwisseling van cijfersuites in hello client en hello server. Als een probleemoplossende stap kunt u de opdracht CURL gebruiken om het gebruik van specifieke cijfers af te dwingen om het probleem te beperken en te bevestigen dat het te wijten is aan coderingssuites zoals weergegeven in voorbeeld 1 en 2.

Voorbeeld van Curl-opdrachten:

<#root>

```
curl -vvv "" --ciphers TLS_DHE_DSS_WITH_AES_256_GCM_SHA384 >> /dev/null
curl -vvv "" --ciphers ECDHE-RSA-AES256-GCM-SHA384 >> /dev/null
```

Testing website With Proxy:

```
- curl -x proxy.sig.umbrella.com:80 -v xyz.com:80  
curl -x swg-url-proxy-https.sigproxy.qq.opendns.com:443 -vvv -k "https://www.cnn.com" >> null
```

Testing website without Proxy

```
: - curl -v www.xyz.com:80
```

Mac/Linux:

```
- curl -vvv -o /dev/null -k -L www.cnn.com
```

Windows:

```
- curl -vvv -o null -k -L www.cnn.com
```

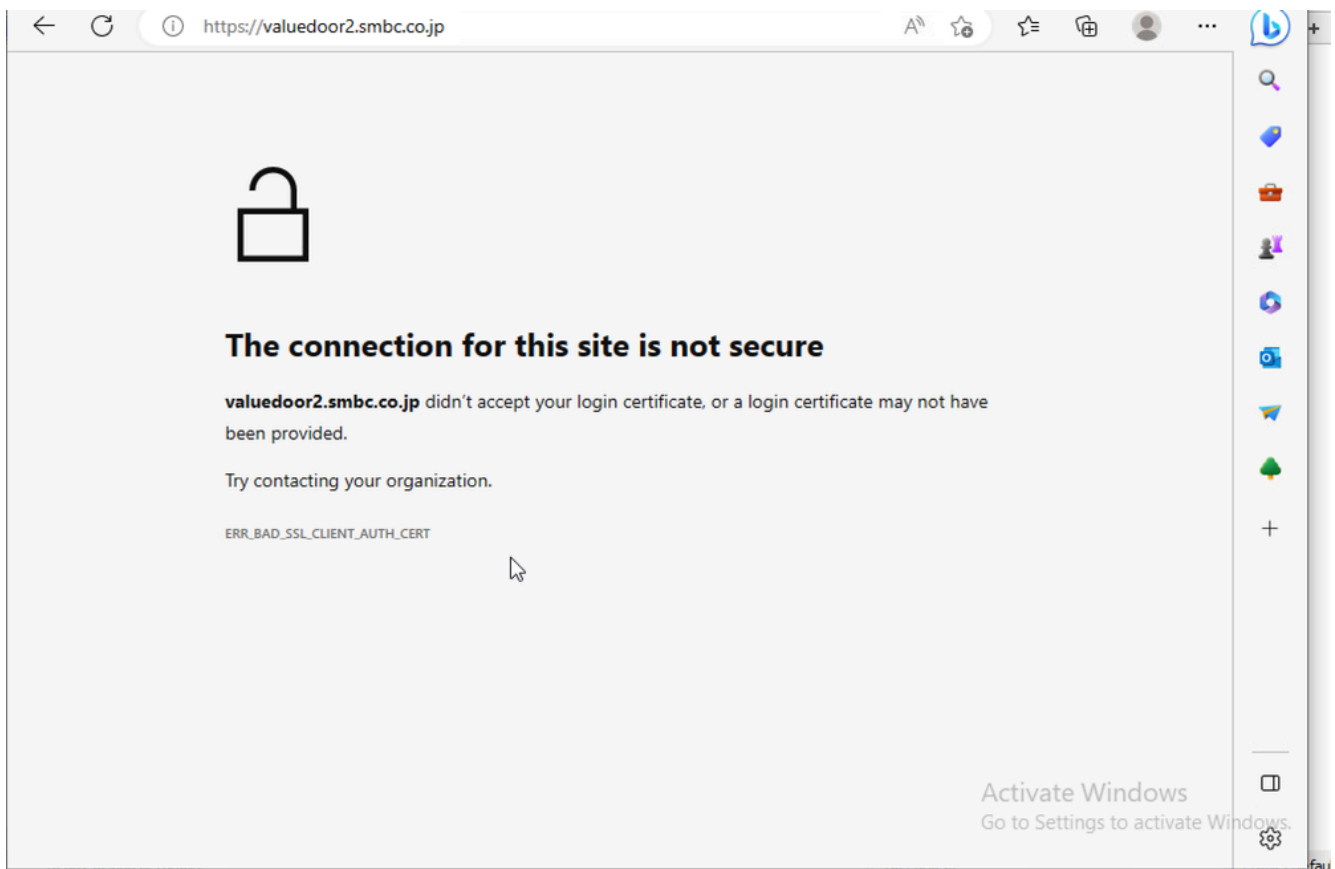
resolutie

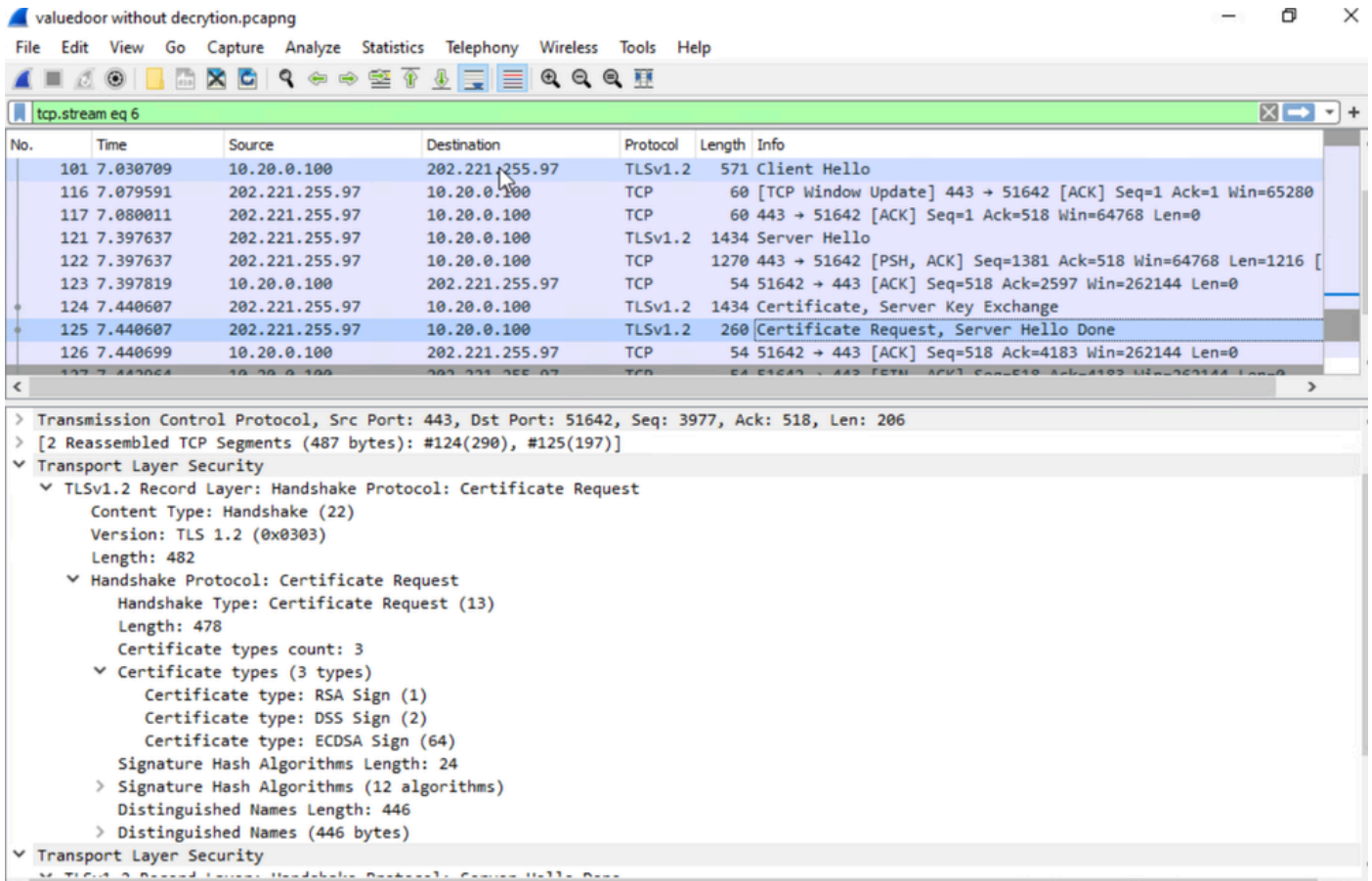
Om het probleem op te lossen, sla de inspectie voor de problematische website met behulp van selectieve decodering lijst.

Aanvraag voor verificatie clientcertificaat

Tijdens de TLS-handshake tussen SWG Proxy en upstream verwacht de upstream webserver verificatie van het clientcertificaat. Aangezien clientcertificaatverificatie niet wordt ondersteund, moeten we deze domeinen omzeilen van proxy met behulp van de externe domeinbeheerlijst en is het niet voldoende om alleen https-inspectie te omzeilen. Bijvoorbeeld:

<https://valuedoor2.smbc.co.jp>.





15027192992276

Headers toegevoegd door Proxy

De webserver rapporteert 502 slechte gateway-fout als gevolg van X-Forward-For-header (XFF) toegevoegd door SWG Proxy wanneer https-inspectie is ingeschakeld. We kunnen de meeste 502 slechte gateway-problemen eenvoudig beperken door eerst het probleem op te lossen met of zonder https-inspectie en met of zonder bestandsinspectie om bestandsscanproblemen met MPS Proxy uit te sluiten.

```
vaishraj@VAISHRAJ-M-QJW4 ~ % curl https://www.monoprice.com -k --header 'X-Forwarded-For: 1.1.1.1' -o /dev/null -w "Status Code: %{http_code}" -s
Status Code: 502
vaishraj@VAISHRAJ-M-QJW4 ~ % curl https://www.monoprice.com -k -o /dev/null -w "Status Code: %{http_code}" -s
Status Code: 200
```

15123666760340

```
curl https://www.xyz.com -k --header 'X-Forwarded-For: 1.1.1.1' -o /dev/null -w "Status Code: %{http_code}" -s
Status Code: 502
curl https://www.xyz.com -k -o /dev/null -w "Status Code: %{http_code}" -s
Status Code: 200
```

We gebruiken de XFF-header wanneer de HTTPS-inspectie is ingeschakeld, zodat de upstream-server optimale geolocatie-inhoud kan bieden op basis van client-IP (die de fysieke locatie van de gebruiker biedt).

Wanneer HTTPS-inspectie niet is ingeschakeld, wordt deze header niet toegevoegd door de proxy, dus er is geen 502 Bad Gateway-fout. Dit is geen probleem met SWG-proxy. Deze fout is te wijten aan de upstream-webserver die niet is geconfigureerd om standaard XFF-header niet te ondersteunen.

resolutie

Om het probleem op te lossen, omzeilen HTTPS-inspectie voor specifieke domein (en) met behulp van selectieve decoderingslijsten.

- 517 Upstream-certificaat ingetrokken
- Fouten in certificaat en TLS-protocol
- SWG DC handmatig selecteren voor interne tests

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.