Secure Access 502-fout voor banksites na verificatie

Inhoud

uitgifte

Gebruikers meldden dat ze een 502 Bad Gateway HTTP-foutcode ontvingen nadat ze met succes waren geverifieerd op FCBanking. Het verificatieproces is met succes voltooid, waardoor gebruikers hun inloggegevens kunnen invoeren, maar de browser heeft onmiddellijk na de verificatie een fout van 502 slechte gateway weergegeven.

Het domein voor FCBanking en de desbetreffende categorie waren vrijgesteld van SSL- en IPS-decodering en deze configuratiewijziging heeft de 502 HTTP-fout niet opgelost. Het probleem trad af en toe op en werd pas opgelost nadat Secure Access volledig was omzeild voor het FCBanking-domein. HAR bestandsanalyse onthulde 502 fouten op de bestemming voor 'my.fcbanking.com', en Activity Search logs toonden niet de 502 fouten die werden vastgelegd in het HAR-bestand, wat aangeeft dat deze fouten zich voordeden op een intermediair apparaatniveau.

milieu

- Cisco Secure Access - Internettoegang (roamingmodule, VA, DNS, SWG, PAC, IPS, certificaten)
- Netwerktopologie: gebruikerspc > Switch > Catalyst SD-WAN-router > Lokaal internet of CSA-tunnel
- Catalyst SD-WAN edge geconfigureerd met app policy rule om al het verkeer op poort 80 & 443 via Direct Internet Access (DIA) te versturen zonder Network Tunnel Group (NTG) te omzeilen
- Cisco Secure Client vertrouwt op een bypass-lijst om de routering naar Secure Access te bepalen
- Bankdomein: fcbanking.com en bijbehorende subdomeinen (my.fcbanking.com,

treasury.fcbanking.com)

resolutie

De primaire resolutie omvat het toevoegen van het bankdomein om Secure Access volledig te omzeilen, waardoor verkeer rechtstreeks naar het internet kan stromen terwijl de beveiliging van de DNS-laag wordt gehandhaafd.

Stap 1: Primair domein toevoegen aan bypass lijst

- Voeg fcbanking.com toe aan de lijst met alleen bypass proxy in de configuratie Secure Access. Dit zorgt ervoor dat webverkeer de Secure Access-proxy omzeilt terwijl de beveiliging van de DNS-laag wordt gehandhaafd en wordt aangemeld bij de activiteitenzoekopdracht.

Stap 2: Domeinaliassen identificeren en toevoegen

- Banksites gebruiken vaak meerdere aliassen die ook aan de bypass-lijst moeten worden toegevoegd. Gebruik Cachecheque om alle aliassen voor het bankdomein te identificeren.
- Voor fcbanking.com werden deze aliassen geïdentificeerd en toegevoegd aan de bypass-lijst:
    - treasury.fcbanking.com (alias: treasuryvanity.jackhenry.com)
    - my.fcbanking.com (alias: banno-online.jackhenry.bank)
    - treasuryvanity.jackhenry.com
    - banno-online.jackhenry.bank

Stap 3: Alternatieve resolutie met IP-adressen

- Als alternatief voor een domeingebaseerde bypass kunnen de opgeloste IP-adressen van banksites aan de bypass-lijst worden toegevoegd. De Cisco Secure Client vertaalt FQDN's die in de bypass-lijst staan naar IP-adressen en leidt webverkeer rechtstreeks naar het internet.

Stap 4: Debug-logboekregistratie inschakelen voor probleemoplossing

- Als u gedetailleerde logbestanden wilt vastleggen voor verdere analyse, schakelt u de logboekregistratie voor het maximale aantal foutmeldingen in:
- Maak een bestand met de naam 'SWGConfigOverride.json' met deze inhoud:

```
{"logLevel": "1"}
```

Plaats het bestand SWGConfigOverride.json in de map SWG:

```
C:\ProgramData\Cisco\Cisco Secure Client\Umbrella\SWG\
```

Start de SWG- of Umbrella-service opnieuw op of start het systeem opnieuw op om de foutopsporingslogconfiguratie toe te passen.


Opmerking: foutmelding heeft geen invloed op de systeemprestaties, maar kan de grootte van het logbestand vergroten. Verwijder het bestand SWGConfigOverride.json na het verkrijgen van de DART-bundel om terug te keren naar normale logniveaus.

Stap 5: Verificatie

- Na het implementeren van de bypass-configuratie rapporteerden gebruikers geen verdere 502-fouten bij het openen van de banksite. DNS-verkeer blijft in Activity Search worden aangemeld, terwijl het webverkeer rechtstreeks naar het internet stroomt.

Oorzaak

Banksites implementeren vaak beveiligingsmaatregelen die verkeer afkomstig van proxyservers of gedeelde IP-adresbereiken detecteren en blokkeren. Cisco Secure Access maakt gebruik van gedeelde IP-bereiken (151.186.144.0/20 en 151.186.176.0/20) voor proxyverkeer, die banksites kunnen detecteren en stilletjes kunnen laten vallen of reageren met HTTP 502-fouten.

Wanneer domeinen worden geplaatst in de lijst Niet decoderen, lijkt het bron-IP nog steeds afkomstig te zijn van het gedeelde IP-bereik van Secure Access, waardoor de beveiligingsmechanismen van de banksite worden geactiveerd. Bovendien kan IPS-inspectie van

bankverkeer en domeinaliassen die niet naar behoren zijn vrijgesteld, bijdragen aan verbindingsfouten. De intermitterende aard van dit probleem en de 502-fouten in HAR-bestanden, maar niet in de activiteitenzoeklogboeken, geven aan dat de fouten werden gegenereerd door intermediaire proxyverwerking in plaats van de bestemmingsbankservers.

Gerelateerde inhoud

- Problemen met toegang tot SWG-website oplossen
- QUIC-protocol uitschakelen om een goede controle van het webverkeer te garanderen
- Cisco Secure Access IP Ranges-documentatie
- 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.