# Secure Access 502 Fehler für Bankseiten nach Authentifizierung

## Inhalt

## Problem

Benutzer haben gemeldet, dass sie nach der erfolgreichen Authentifizierung bei FCBanking einen 502 Bad Gateway HTTP-Fehlercode erhalten haben. Der Authentifizierungsprozess wurde erfolgreich abgeschlossen, sodass Benutzer ihre Anmeldeinformationen eingeben konnten. Der Browser zeigte jedoch sofort nach der Authentifizierung einen 502-Fehler wegen eines fehlerhaften Gateways an.

Die Domäne für FCBanking und die zugehörige Kategorie waren von der SSL- und IPS-Entschlüsselung ausgenommen, und durch diese Konfigurationsänderung konnte der 502-HTTP-Fehler nicht behoben werden. Das Problem trat gelegentlich auf und wurde erst behoben, nachdem Secure Access vollständig für die FCBanking-Domäne umgangen wurde. Die HAR-Dateianalyse ergab 502 Fehler am Ziel für "my.fcbanking.com", und die Aktivitätssuchprotokolle zeigten nicht die 502 Fehler an, die in der HAR-Datei erfasst wurden. Dies deutet darauf hin, dass diese Fehler auf einer mittleren Geräteebene aufgetreten sind.

## Umwelt

- Cisco Secure Access - Internetzugang (Roaming-Modul, VA, DNS, SWG, PAC, IPS, Zertifikate)
- Netzwerktopologie: Benutzer-PC > Switch > Catalyst SD-WAN-Router > Lokaler Internet- oder CSA-Tunnel
- Catalyst SD-WAN-Edge mit konfigurierter App-Richtlinienregel zum Senden des gesamten Datenverkehrs auf den Ports 80 und 443 über Direct Internet Access (DIA) unter Umgehung der NTG (Network Tunnel Group)
- Cisco Secure Client anhand einer Umgehungsliste zur Bestimmung der Datenverkehrsweiterleitung zum sicheren Zugriff

- Bankdomäne: fcbanking.com und zugehörige Subdomains (my.fcbanking.com, treasury.fcbanking.com)

## Auflösung

Die primäre Lösung besteht darin, die Banking-Domäne so hinzuzufügen, dass Secure Access vollständig umgangen wird. Dadurch kann der Datenverkehr direkt in das Internet fließen, während die Sicherheit auf der DNS-Ebene erhalten bleibt.

Schritt 1: Primäre Domäne zur Umgehungsliste hinzufügen

- Fügen Sie fcbanking.com der Liste Nur-Proxy-Umgehung in der Konfiguration für sicheren Zugriff hinzu. Dadurch wird sichergestellt, dass der Webdatenverkehr den Secure Access-Proxy umgeht, während die DNS-Layer-Sicherheit weiterhin erzwungen und bei der Aktivitätssuche angemeldet bleibt.

Phase 2: Domänenaliase identifizieren und hinzufügen

- An Bankstandorten werden häufig mehrere Aliase verwendet, die ebenfalls der Umgehungsliste hinzugefügt werden müssen. Verwenden Sie Cache Check, um alle Aliase für die Banking-Domäne zu identifizieren.
- Für fcbanking.com wurden diese Aliase identifiziert und der Umgehungsliste hinzugefügt:
    - treasury.fcbanking.com (Alias: treasuryvanity.jackhenry.com)
    - my.fcbanking.com (Alias: banno-online.jackhenry.bank)
    - treasuryvanity.jackhenry.com
    - banno-online.jackhenry.bank

Schritt 3: Alternative Auflösung mit IP-Adressen

- Als Alternative zur domänenbasierten Umgehung können die aufgelösten IP-Adressen von Banking-Sites der Umgehungsliste hinzugefügt werden. Der Cisco Secure Client übersetzt die in der Umgehungsliste aufgeführten FQDNs in IP-Adressen und leitet den Web-Datenverkehr direkt an das Internet weiter.

Schritt 4: Debug-Protokollierung zur Fehlerbehebung aktivieren

- Um detaillierte Protokolle für weitere Analysen zu erfassen, aktivieren Sie die maximale Debug-Protokollierung:
- Erstellen Sie eine Datei mit dem Namen "SWGConfigOverride.json" und folgendem Inhalt:

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

Legen Sie die Datei SWGConfigOverride.json in den Ordner SWG:

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

Starten Sie die SWG oder den Umbrella-Dienst neu, oder starten Sie das System neu, um die Konfiguration der Debug-Protokollierung anzuwenden.

---

Anmerkung: Die Debug-Protokollierung hat keine Auswirkungen auf die Systemleistung, kann jedoch die Größe der Protokolldatei erhöhen. Entfernen Sie die Datei SWGConfigOverride.json, nachdem Sie das DART-Paket erhalten haben, um zu den normalen Protokollierungsebenen zurückzukehren.

---

Schritt 5: Verifizierung

- Nach der Implementierung der Umgehungskonfiguration meldeten die Benutzer keine weiteren 502 Fehler beim Zugriff auf den Banking-Standort. Der DNS-Datenverkehr wird weiterhin bei der Aktivitätssuche protokolliert, während der Web-Datenverkehr direkt ins Internet fließt.

## Ursache

An Bankstandorten werden in der Regel Sicherheitsmaßnahmen implementiert, die Datenverkehr von Proxyservern oder von gemeinsam genutzten IP-Adressbereichen erkennen und blockieren. Cisco Secure Access nutzt für den Proxy-Datenverkehr gemeinsam genutzte IP-Bereiche (151.186.144.0/20 und 151.186.176.0/20), die Banking-Websites erkennen können, ohne dass sie Fehler im HTTP 502-Format erkennen oder darauf reagieren können.

Wenn Domänen in der Liste "Nicht entschlüsseln" platziert werden, scheint die Quell-IP immer noch aus dem gemeinsamen IP-Bereich von Secure Access zu stammen, was die Sicherheitsmechanismen des Bankstandorts auslöst. Darüber hinaus kann die IPS-Inspektion bei Bankdatenverkehr und nicht ordnungsgemäß freigegebenen Domänenaliasen zu Verbindungsausfällen beitragen. Dieses Problem tritt nur gelegentlich auf, und die 502 Fehler, die in HAR-Dateien, aber nicht in den Aktivitätssuchprotokollen angezeigt werden, weisen darauf hin, dass die Fehler durch eine intermediäre Proxy-Verarbeitung und nicht durch die Ziel-Banking-Server generiert wurden.

## Verwandte Inhalte

- Probleme beim Zugriff auf die SWG-Website beheben
- Deaktivieren Sie das QUIC-Protokoll, um eine ordnungsgemäße Prüfung des Web-Datenverkehrs sicherzustellen.
- Cisco Secure Access IP Ranges-Dokumentation
- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.