Secure Access 502 Error For Banking Sites After Authentication

Contents

Issue

Users reported receiving a 502 Bad Gateway HTTP Error code after successfully authenticating to FCBanking. The authentication process completed successfully, allowing users to enter their login credentials, however, the browser displayed a 502 bad gateway error immediately after authentication.

The domain for FCBanking and its relevant category were exempt from SSL and IPS decryption and this configuration change did not resolve the 502 HTTP error. The issue occurred intermittently and was only resolved after bypassing Secure Access entirely for the FCBanking domain. HAR file analysis revealed 502 errors on the destination for 'my.fcbanking.com', and Activity Search logs did not show the 502 errors that were captured in the HAR file, indicating these errors were occurring at an intermediate device level.

Environment

- Cisco Secure Access - Internet Access (Roaming Module, VA, DNS, SWG, PAC, IPS, Certificates)
- Network Topology: User PC > Switch > Catalyst SD-WAN Router > Local internet or CSA tunnel
- Catalyst SD-WAN edge configured with app policy rule to send all traffic on port 80 & 443 via Direct Internet Access (DIA) bypassing Network Tunnel Group (NTG)
- Cisco Secure Client relying on a bypass list to determine traffic routing to Secure Access
- Banking Domain: fcbanking.com and associated subdomains (my.fcbanking.com, treasury.fcbanking.com)

Resolution

The primary resolution involves adding the banking domain to bypass Secure Access entirely, allowing traffic to flow directly to the internet while maintaining the DNS layer security.

Step 1: Add Primary Domain to Bypass List

- Add fcbanking.com to the **bypass proxy only** list in Secure Access configuration. This ensures web traffic bypasses the Secure Access proxy while the DNS layer security remains enforced and logged in the Activity Search.

Step 2: Identify and Add Domain Aliases

- Banking sites often use multiple aliases that must also be added to the bypass list. Use Cache Check to identify all aliases for the banking domain.
- For fcbanking.com, these aliases were identified and added to the bypass list:
  - treasury.fcbanking.com (alias: treasuryvanity.jackhenry.com)
  - my.fcbanking.com (alias: banno-online.jackhenry.bank)
  - treasuryvanity.jackhenry.com
  - banno-online.jackhenry.bank

Step 3: Alternative Resolution Using IP Addresses

- As an alternative to domain-based bypass, the resolved IP addresses of banking sites can be added to the bypass list. The Cisco Secure Client translates FQDNs found on the bypass list to IP addresses and routes web traffic directly to the internet.

Step 4: Enable Debug Logging for Troubleshooting

- To capture detailed logs for further analysis, enable maximum debug logging:
- Create a file named 'SWGConfigOverride.json' with this content:

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

Place the SWGConfigOverride.json file in the SWG folder:

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

Restart the SWG or Umbrella service, or restart the system to apply the debug logging configuration.

Note: Debug logging does not affect system performance but can increase log file size. Remove the SWGConfigOverride.json file after obtaining the DART bundle to return to normal logging levels.

Step 5: Verification

- After implementing the bypass configuration, users reported no further 502 errors when accessing the banking site. DNS traffic continues to be logged in Activity Search while web traffic flows directly to the internet.

Cause

Banking sites commonly implement security measures that detect and block traffic originating from proxy servers or shared IP address ranges. Cisco Secure Access uses shared IP ranges (151.186.144.0/20 and 151.186.176.0/20) for proxy traffic, which banking sites can detect and silently drop or respond to with HTTP 502 errors.

When domains are placed in the do not decrypt list, the source IP still appears to originate from the Secure Access shared IP range, triggering the banking site's security mechanisms. Additionally, IPS inspection on banking traffic and domain aliases not being properly exempt can contribute to connection failures. The intermittent nature of this issue and the 502 errors appearing in HAR files but not in the Activity Search logs indicate the errors were generated by intermediate proxy processing rather than the destination banking servers.

Related Content

- Troubleshoot SWG Website Access Issues
- Disable QUIC Protocol to Ensure Proper Web Traffic Inspection
- Cisco Secure Access IP Ranges Documentation
- Cisco Technical Support & Downloads