身份验证后银行站点的安全访问502错误

目录

问题

用户报告在成功向FCBanking进行身份验证后收到502个错误网关HTTP错误代码。身份验证过程已成功完成，允许用户输入其登录凭证，但是，浏览器在身份验证后立即显示502错误网关错误。

FCBanking域及其相关类别免除SSL和IPS解密，此配置更改无法解决502 HTTP错误。此问题间歇性发生，仅在完全绕过FCBanking域的安全访问之后才得到解决。HAR文件分析显示“my.fcbanking.com”的目的地址存在502个错误，活动搜索日志未显示HAR文件中捕获的502个错误，这表明这些错误发生在中间设备级别。

环境

- 思科安全接入 — 互联网接入（漫游模块、VA、DNS、SWG、PAC、IPS、证书）
- 网络拓扑:用户PC >交换机> Catalyst SD-WAN路由器>本地互联网或CSA隧道
- 使用应用策略规则配置的Catalyst SD-WAN边缘通过直接互联网接入(DIA)绕过网络隧道组(NTG)发送端口80和443上的所有流量
- Cisco安全客户端依靠旁路列表来确定到安全访问的流量路由
- 银行业务域：fcbanking.com和相关子域(my.fcbanking.com、treasury.fcbanking.com)

分辨率

主要解决方法涉及添加银行域以完全绕过安全访问，允许流量直接流到互联网，同时维护DNS层安全。

步骤 1：将主域添加到旁路列表

- 将fcbanking.com添加到Secure Access配置中的仅旁路代理列表。这可以确保Web流量绕过安全访问代理，同时保持DNS层安全并记录到活动搜索中。

步骤 2：标识和添加域别名

- 银行站点通常使用多个别名，这些别名也必须添加到旁路列表中。使用缓存检查标识银行域的所有别名。
- 对于fcbanking.com，已标识这些别名并将其添加到旁路列表中：
  - treasury.fcbanking.com(别名：treasuryvanity.jackhenry.com)
  - my.fcbanking.com(别名：banno-online.jackhenry.bank)
  - treasuryvanity.jackhenry.com
  - banno-online.jackhenry.bank

步骤 3：使用IP地址进行替代解析

- 作为基于域的旁路的替代方案，可以将银行站点的已解析IP地址添加到旁路列表中。思科安全客户端将旁路列表中的FQDN转换为IP地址，并将网络流量直接路由到互联网。

步骤 4：启用调试日志记录以进行故障排除

- 要捕获详细日志以供进一步分析，请启用最大调试日志记录：
- 使用以下内容创建名为“SWGConfigOverride.json”的文件：

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

将SWGConfigOverride.json文件放在SWG文件夹中：

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

重新启动SWG或Umbrella服务，或重新启动系统以应用调试日志记录配置。

注意：调试日志记录不会影响系统性能，但可以增加日志文件大小。获取DART捆绑包后，删

除SWGConfigOverride.json文件以返回正常日志记录级别。

步骤 5：确认

- 实施旁路配置后，用户在访问银行站点时不再报告502个错误。当Web流量直接流向Internet时，DNS流量继续记录在活动搜索中。

原因

银行站点通常实施安全措施，检测并阻止源自代理服务器或共享IP地址范围的流量。Cisco安全访问使用共享IP范围（151.186.144.0/20和151.186.176.0/20）作为代理流量，银行站点可以检测这些流量，并以静默方式丢弃或响应HTTP 502错误。

当域放置在do not decrypt列表中时，源IP似乎仍来自Secure Access共享IP范围，从而触发银行站点的安全机制。此外，未正确排除的银行流量和域别名的IPS检测会导致连接故障。此问题的间歇性性质以及HAR文件中出现但不在活动搜索日志中的502个错误都表明这些错误是由中间代理处理而不是目标银行服务器生成的。

相关内容

- 排除SWG网站访问问题
- 禁用QUIC协议以确保正确的网络流量检测
- Cisco安全访问IP范围文档
- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。