خطأ في الوصول الآمن إلى 502 للمواقع البنكية بعد المصادقة

المحتويات

مسألة

أبلغ المستخدمون عن تلقي رمز خطأ HTTP لعبارة غير صحيحة 502 بعد المصادقة بنجاح على FCBanking. اكتملت عملية المصادقة بنجاح، مما يسمح للمستخدمين بإدخال بيانات اعتماد تسجيل الدخول الخاصة بهم، ومع ذلك، عرض المستعرض خطأ عبارة غير صحيحة 502 مباشرة بعد المصادقة.

تم إستثناء مجال FCBanking والفئة ذات الصلة به من فك تشفير SSL و IPS ولم يحل تغيير التكوين هذا خطأ 502 HTTP. حدثت المشكلة بشكل متقطع وتم حلها فقط بعد تجاوز الوجهة ل Secure Access بالكامل لمجال FCBanking. كشف تحليل ملف HAR عن 502 خطأ في ملف HAR، ولم تظهر سجلات البحث عن النشاط 502 خطأ تم التقاطها في ملف HAR، 'my.fcbanking.com'. مما يشير إلى أن هذه الأخطاء كانت تحدث على مستوى جهاز متوسط.

البيئة

- الوصول الآمن من Cisco - الوصول إلى الإنترنت (الوحدة النمطية المتجولة، VA، DNS، SWG، PAC، IPS، الشهادات)
- طوبولوجيا الشبكة: كمبيوتر المستخدم > محول > موجه Catalyst SD-WAN > الإنترنت CSA المحلي أو نفق
- تم تكوين Catalyst SD-WAN Edge باستخدام قاعدة سياسة التطبيق لإرسال جميع حركات المرور على المنفذ 80 و 443 عبر الوصول المباشر إلى الإنترنت (DIA) عبر تجاوز مجموعة نفق الشبكة (NTG)
- يعتمد Cisco Secure Client على قائمة تجاوز لتحديد توجيه حركة مرور البيانات للوصول الآمن
- مجال مصرفي: fcbanking.com والمجالات الفرعية المرتبطة (my.fcbanking.com، treasury.fcbanking.com)

رارق

والحل الأساسي ينطوي على إضافة المجال المصرفي إلى تجاوز الوصول الآمن بالكامل، مما يسمح لحركة المرور بالتدفق مباشرة إلى الإنترنت مع الحفاظ على أمان طبقة DNS.

الخطوة 1: إضافة مجال أساسي إلى قائمة التجاوز

- قم بإضافة fcbanking.com إلى قائمة وكيل تجاوز فقط في تكوين الوصول الآمن. وهذا يضمن أن حركة مرور الويب تتجاوز وكيل الوصول الآمن بينما يظل أمان طبقة DNS مفروضا ومسجلا في البحث عن النشاط.

الخطوة 2: تعريف أسماء المجالات المستعارة وإضافتها

- وغالبا ما تستخدم المواقع المصرفية أسماء مستعارة متعددة يجب إضافتها أيضا إلى قائمة التجاوز. أستخدم التحقق من ذاكرة التخزين المؤقت لتحديد كافة الأسماء المستعارة للمجال البنكي.
- بالنسبة إلى fcbanking.com، تم تحديد هذه الأسماء المستعارة وإضافتها إلى قائمة التجاوز:
  - treasury.fcbanking.com (الاسم المستعار: treasuryvanity.jackhenry.com)
  - my.fcbanking.com (الاسم المستعار: بانوأون لاين.جاكهنري بانك)
  - treasuryvanity.jackhenry.com
  - بانوأون لاين.جاكهنري

الخطوة 3: حل بديل باستخدام عناوين IP

- كبديل للتجاوز المستند إلى المجال، يمكن إضافة عناوين IP التي تم حلها للمواقع المصرفية إلى قائمة التجاوز. يترجم ال cisco أمن زبون FQDNs على الالتفافية إلى عنوان ويوجه ويب حركة مرور مباشرة إلى الإنترنت.

الخطوة 4: تمكين تسجيل تصحيح الأخطاء لاستكشاف الأخطاء وإصلاحها

- لالتقاط سجلات تفصيلية لمزيد من التحليل، قم بتمكين الحد الأقصى لتسجيل تصحيح الأخطاء:
  - إنشاء ملف باسم 'SWGConfigOverride.json' مع هذا المحتوى:

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

وضع ملف SWGConfigOverride.json في مجلد SWG:

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

قم بإعادة تشغيل خدمة SWG أو Umbrella، أو إعادة تشغيل النظام لتطبيق تكوين تسجيل الأخطاء.

ملاحظة: قد يؤثر تسجيل التصحيح على أداء النظام ولكن يمكن زيادة حجم ملف السجل. قم بإزالة ملف SWGConfigOverride.json بعد الحصول على حزمة DART للعودة إلى مستويات التسجيل العادية.

الخطوة 5: التحقق

- بعد تنفيذ التكوين الالتفافي، لم يبلغ المستخدمون عن وجود 502 خطأ آخر عند طاش في البحث عن النطاقات في DNS مرور حركة مرور DNS. يستمر تسجيل حركة مرور الوصول إلى الموقع المصرفي. يتم توجيه حركة مرور الإنترنت مباشرة إلى الإنترنت.

السبب

تقوم المواقع المصرفية بشكل عام بتنفيذ تدابير أمنية تعمل على اكتشاف حركة المرور الناشئة من الخوادم العميلة وأنظمة IP المشتركة وحظرها. يستخدم Cisco نطاقات IP مشتركة لحركة مرور الوكيل، Secure Access (151.186.176.0/20 و 151.186.144.0/20) التي يمكن للمواقع المصرفية اكتشافها وإسقاطها أو الاستجابة لها بصمت مع أخطاء HTTP 502.

عندما يتم وضع المجالات في قائمة عدم فك التشفير، يظهر المصدر IP بعد أن ينشأ من الخادم الوكيل السحابي Umbrella. يتم توجيه حركة المرور المشفرة مباشرة إلى الموقع المصرفي، مما يؤدي إلى تشغيل آليات أمان الموقع المصرفي. نطاق IP المشترك للوصول الآمن، يمكن أن يساهم فحص IPS لحركة المرور البنكية أو سماعات المجال غير الإضافة إلى ذلك، المستثناة بشكل صحيح في حالات فشل الاتصال. يشير كل من الطبيعة المتقطعة إلى أن Activity Search سجلات HAR لكن ليس في ملفات أخطاء HTTP 502 و هذه المشكلة تم توليدها عن طريق المعالجة الوسيطة للوكيل بدلا من الخوادم البنكية الوجهة.

المحتوى ذي الصلة

- [استكشاف أخطاء الوصول إلى موقع SWG وإصلاحها](#)
- [تعطيل بروتوكول QUIC لضمان الفحص المناسب لحركة مرور الويب](#)
- [وثائق نطاقات IP للوصول الآمن من Cisco](#)
- [الدعم الفني والتنزيلات من Cisco](#)

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).