502 / 504 أخطاء gateway_timeout عند الاستعراض إلى مواقع معينة

المحتويات

سؤال:

لماذا نرى أخطاء GATEWAY_TIMEOUT في 504/502 عند الاستعراض إلى مواقع معينة؟

الأعراض: يستلم المستخدمون أخطاء مهلة العبارة 502 أو 504 من Cisco WSA عند الاستعراض إلى مواقع معينة

يتلقى المستخدمون أخطاء مهلة العبارة 502 أو 504 عند الاستعراض إلى مواقع الويب. تظهر سجلات الوصول 'NONE/504' أو 'NONE/502'

نموذج سطر سجل الوصول:

1233658928.496 153185 10.10.70.50 **none/504** 1729 الحصول على - http://www.example.com/ ..... - DIRECT/www.example.com

هناك العديد من الأسباب التي قد ترجع WSA خطأ انتهاء مهلة العبارة 502 أو 504. على الرغم من أن ردود الأفعال الخاطئة تلك متشابهة، إلا أنه من المهم فهم الاختلافات الطفيفة بينها.

وفيما يلي بعض الأمثلة لأنواع السيناريوهات التي قد تحدث:

- **502**: حاول WSA إنشاء اتصال TCP بخادم الويب، ولكنه لم يتلقى SYN/ACK.
- **504**: يتلقى WSA إعادة تعيين TCP (RST) ينهي الاتصال بخادم الويب.
- **504**: لا يحصل WSA على إستجابة من الخدمة المطلوبة قبل الاتصال بخادم الويب، مثل DNS في حالة فشل.
- **504**: أنشأ WSA اتصال TCP بخادم الويب وأرسل طلب GET، ولكن WSA لم يستلم إستجابة HTTP أبدا.

وفيما يلي أمثلة لكل سيناريو وتفاصيل أكثر بشأن المسائل المحتملة:

502: حاول WSA إنشاء اتصال TCP بخادم الويب، ولكنه لم يتلقى SYN/ACK.
إذا لم يستجب خادم الويب لحزم SYN الخاصة ب WSA، بعد عدد معين من المحاولات، سيتم إرسال العميل خطأ مهلة العبارة 502. الأسباب النموذجية لذلك: 1. توجد مشاكل في خادم ويب أو شبكة خادم ويب. 2. تمنع مشكلة في الشبكة على شبكة WSA وصول حزم SYN إلى الإنترنت. 3. يقوم جدار حماية أو جهاز مشابه بإسقاط حزم WSA SYN أو SYN/ACK لخادم الويب 4. تم تمكين انتحال IP على WSA، ولكنه لم يتم تكوينه بشكل صحيح (لا إعادة توجيه مسار الإرجاع)

خطوات أستكشاف الأخطاء وإصلاحها:

تتمثل الخطوة الأولى في التحقق مما إذا كان بإمكان WSA إختبار اتصال ICMP بخادم الويب. يمكن القيام بذلك باستخدام أمر CLI التالي:
WSA> *ping* www.example.com
إذا فشل إختبار الاتصال، فهذا لا يعني أن الخادم معطل. وقد يعني ذلك أن حزم ICMP يتم حظرها في مكان ما في المسار. إذا نجح إختبار الاتصال، فحينئذ يمكننا التأكد من أن WSA لديها مستوى اتصال أساسي من الطبقة 3 بخادم الويب.
سيقوم إختبار برنامج Telnet بالتحقق من أن WSA لديه القدرة على إنشاء اتصال TCP على المنفذ 80 إلى خادم الويب. انظر التعليمات الموجودة في هذه المقالة حول إجراء إختبار برنامج Telnet.

مشاكل الشبكة أو كتلة جدار الحماية
إذا نجح إختبار الاتصال، ولكن فشل برنامج Telnet، فهناك إمكانية جيدة أن يمنع جهاز التصفية، مثل جدار الحماية، حركة المرور هذه من الوصول عبر الشبكة. يوصى بتحليل سجلات جدار الحماية و/أو التقاط الحزم من جدار الحماية للحصول على مزيد من التفاصيل.
تمكين انتحال عناوين IP، ولكن لم يتم تكوينه بشكل صحيح
إذا نجح الوكيل الصريح من خلال WSA أو إختبار Telnet، فهذا يوضح أن WSA يمكن أن يتصل مباشرة بخادم الويب، ولكن عندما يقوم وكيل عميل من خلال WSA باستخدام انتحال IP، تكون هناك مشكلة.

دون انتحال عناوين IP الخاصة بالعميل:
- يرسل WSA SYN إلى خادم الويب باستخدام عنوان IP الخاص به كمصدر. عندما تعود الحزمة، فإنها تنتقل مباشرة إلى WSA.

باستخدام انتحال عناوين IP الخاصة بالعميل:
- يرسل WSA SYN، ولكن بدلا من ذلك، يستخدم IP الخاص بالعميل كمصدر. بدون إعداد شبكة خاص، سيتم إرسال حزمة الإرجاع إلى العميل بدلا من WSA.
- لاستخدام انتحال عنوان IP للعميل، يجب تكوين الشبكة بطريقة محددة للغاية لتسهيل إعادة توجيه الحزم بشكل صحيح. إذا تم إرسال حزم مسار إرجاع خادم الويب إلى العميل بدلا من WSA، فلن ترى WSA الخوادم SYN/ACK وسترسل خطأ انتهاء مهلة عبارة 502 مرة أخرى إلى العميل.

504: يتلقى WSA إعادة تعيين TCP (RST) ينهي الاتصال بخادم الويب.

إذا تلقت WSA حزمة إعادة تعيين TCP على اتصال الخادم العلوي الخاص بها بخادم الويب، فسيقوم WSA بإرسال خطأ مهلة العبارة 504 إلى العميل.

الأسباب النموذجية لذلك:
1. يقوم Cisco Layer 4 Traffic Monitor (L4TM) بحظر وكيل WSA من توصيل خادم الويب.
2. يمنع جدار الحماية أو المعرفات أو IPS أو جهاز فحص الحزم الآخر WSA.

خطوات أستكشاف الأخطاء وإصلاحها:
حدد أولا ما إذا كان TCP RST يأتي من L4TM أو من جهاز آخر.
إذا كان L4TM يمنع حركة المرور هذه، ستظهر حركة المرور في تقارير واجهة المستخدم الرسومية تحت ***Monitor -> L4 مراقبة حركة المرور***". وإلا، فسيأتي RST من جهاز مختلف.
حظر L4TM:
من المستحسن عدم حظر المنافذ التي يعمل عليها وكيل WSA أيضا إذا كان L4TM قيد الحظر. هناك أسباب متعددة لذلك:
1. يوفر وكيل WSA رسالة خطأ مألوفة في حالة المشكلة، بدلا من مجرد TCP الذي يقوم بإعادة تعيين الاتصال. سيساعد ذلك في الحد من التشويش من قبل المستخدمين النهائيين عند منعهم.
2. يتمتع وكيل WSA بالقدرة على مسح محتوى محدد وحظره، في حين أن L4TM يمنع جميع حركة المرور المطابقة لعنوان IP المدرج في القائمة السوداء.
لتكوين L4TM لعدم الحظر على منافذ الوكيل، انتقل إلى ***GUI -> خدمات الأمان -> L4 Traffic Monitor***".

إذا كان الموقع هو موقع ويب معروف بأنه سيئ، ولكن هناك أسباب للسماح بحركة المرور، يمكن إدراج الموقع باللون الأبيض في:
"*GUI -> Web Security Manager -> L4 Traffic Monitor <- قائمة السماح*"

حظر جدار الحماية / المعرفات / IPS:
إذا كان هناك جهاز آخر على الشبكة يمنع WSA من الاتصال بخادم الويب، فمن المستحسن تحليل ما يلي:
1. سجلات كتل الجدار الناري
2. تلتقط حزمة الدخول / الخروج أثناء المشكلة

قد تؤكد سجلات الحظر بسرعة ما إذا كان الجهاز يقوم بحظر WSA. في بعض الأحيان، يقوم جدار الحماية أو عناوين IPS أو معرفات بحظر حركة المرور وعدم تسجيلها بشكل صحيح. إذا كان هذا هو الحال، فإن الطريقة الوحيدة لإثبات من أين يأتي TCP RST، هي الحصول على لقطات الدخول والخروج من الجهاز. إذا تم إرسال RST من واجهة الدخول ولم يتم نقل حزم من خلال جانب المخرج، فإن جهاز الأمان هو السبب بالتأكيد.

504: أنشأ WSA اتصال TCP بخادم الويب وأرسل طلب GET، ولكن WSA لم يستلم إستجابة HTTP أبدا.
إذا قام WSA بإرسال HTTP GET، ولكنه لا يستلم إستجابة أبدا، فسيرسل خطأ مهلة عبارة 504 إلى العميل.

الأسباب النموذجية لذلك:
- يسمح جدار الحماية أو المعرفات أو IPS أو جهاز فحص الحزم الآخر باتصال TCP، ولكن يمنع محتوى HTTP من الوصول إلى خادم الويب. في هذه الحالة، قد يساعد إختبار telnet في عزل أي نوع من بيانات HTTP يتم حظره.

قد تؤكد سجلات حظر جدار الحماية بسرعة ما إذا / لماذا يقوم الجهاز بحظر WSA. في بعض الأحيان، يقوم جدار الحماية أو عناوين IPS أو معرفات بحظر حركة المرور وعدم تسجيلها بشكل صحيح. إذا كان هذا هو الحال، فإن الطريقة الوحيدة لإثبات من أين يأتي TCP RST، هي الحصول على لقطات الدخول والخروج من الجهاز. إذا تم إرسال RST من واجهة الدخول ولم يتم نقل حزم من خلال جانب المخرج، فإن جهاز الأمان هو السبب بالتأكيد.

إختبار الاتصال بخادم ويب باستخدام برنامج Telnet
من واجهة سطر أوامر (CLI) WSA، قم بتشغيل الأمر **telnet**:

WSA> **telnet**
الرجاء تحديد الواجهة التي تريد برنامج Telnet منها.
1. تلقائي
2 - الإدارة (wsa.hostname.com :24/192.168.15.200)
3 - البرنامج 1 (data.com :24/192.168.113.199)
[1]> **3**

أدخل اسم المضيف أو عنوان IP البعيد.
[]> www.example.com

أدخل المنفذ البعيد.
[25]> **80**

جار محاولة 10.3.2.99...
متصل ب www.example.com.
حرف الهروب هو '^]'.

ملاحظة: تشير الرسالة "المتصلة" باللون الأحمر إلى أن بروتوكول TCP قد تم إنشاؤه بنجاح بين WSA وخادم الويب.

يمكن إرسال طلب HTTP يدويا من خلال جلسة عمل برنامج telnet هذه أيضا. فيما يلي نموذج طلب يمكن كتابته بعد الرسالة "المتصلة":

—

الحصول على HTTP/1.1 http://www.example.com

المضيف: www.example.com

{Enter}

—

ملاحظة: تأكد من إضافة إرجاع النقل الإضافي في النهاية، وإلا فلن يستجيب الخادم للطلب.

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).