راسملل MTU فاشتكا ىلع WSA كولس WCCP مادختساب

المحتويات

المقدمة

يصف هذا المستند مشكلة تتم مواجهتها عندما يقوم الموجه بإسقاط الحزم عندما يتضمن التكوين الخاص بك كلا من اكتشاف كل من بروتوكول إتصالات ذاكرة التخزين المؤقت للويب (WCCP) ووحدة الإرسال القصوى للمسار (MTU)، ويقدم حلا للمشكلة.

معلومات أساسية

مرحلة ما قبل

عندما ينظر إلى العديد من الخصائص بشكل منفصل، فإنها تكون ممتازة للتعامل مع مشكلة معينة. ومع ذلك أحيانا، إذا قمت بدمج تقنيتين أو ثلاث طرق، فإنه ينتج عنه بعض السلوك المحرج ويجب عليك تقديم ميزة أخرى أو حل بديل لجعله يعمل بشكل صحيح. على سبيل المثال، يستغرق إستخدام تقارب الشجرة المتفرعة وفتح أقصر مسار أولا (OSPF) والطبقة 2 (L2) وقتا أطول (20) من 1s) OSPF إذا تم إستخدام أدنى فاصل زمني غير متوقع)، ولكن إستبدال الشجرة المتفرعة بعدة شجرة متفرعة (MST) وتعمل بشكل صحيح مرة أخرى.

تم ملاحظة نفس سلوك قابلية التشغيل البيني بين اكتشاف WCCP و MTU للمسار؛ يعتقد الكثيرون أنها مشكلة رأس تضمين التوجيه العام (GRE). ومع ذلك، يشرح هذا المستند السبب الحقيقي.

كيف يعمل فك تشفير وحدة الحد الأقصى للنقل (MTU) و WCCP بشكل منفصل

اكتشاف مسار وحدة الحد الأقصى للنقل (MTU)

يحتوي كل سطر على الحد الذي يمكن أن تكون عنده الحزمة كبيرة. إذا قمت بإرسال حزمة أكبر من الدعم، يتم

إسقاطها. أحد أدوار أجهزة L3 (الموجهات) في الطريق هو توخي الحذر وتقسيم الحزم الكبيرة من أحد الأسطر إلى الآخر للتأكد من أن الاتصال من نهاية إلى نهاية شفاف لقدرات كل سطر.

على الرغم من ذلك في بعض الأحيان، يتم تكوين المضيفين النهائيين بطريقة لا يمكن بها قص الحزم (على سبيل المثال، الملفات المشفرة والمكالمات الصوتية). يتم توصيل هذه المعلومات من خلال وحدة بت عدم التجزئة (DF) داخل رأس IP. تقوم الموجهات بإسقاط الحزم كهذه، ولكن الموجه يحاول الإبلاغ للمضيف النهائي عبر رسالة بروتوكول رسائل التحكم في الإنترنت (ICMP) (النوع 3-Destination unreachable، الرمز 4 - التجزئة المطلوبة، ولكن مجموعة بت DF). بهذه الطريقة، يعرف المضيف أن يرسل حزم أصغر في المستقبل.

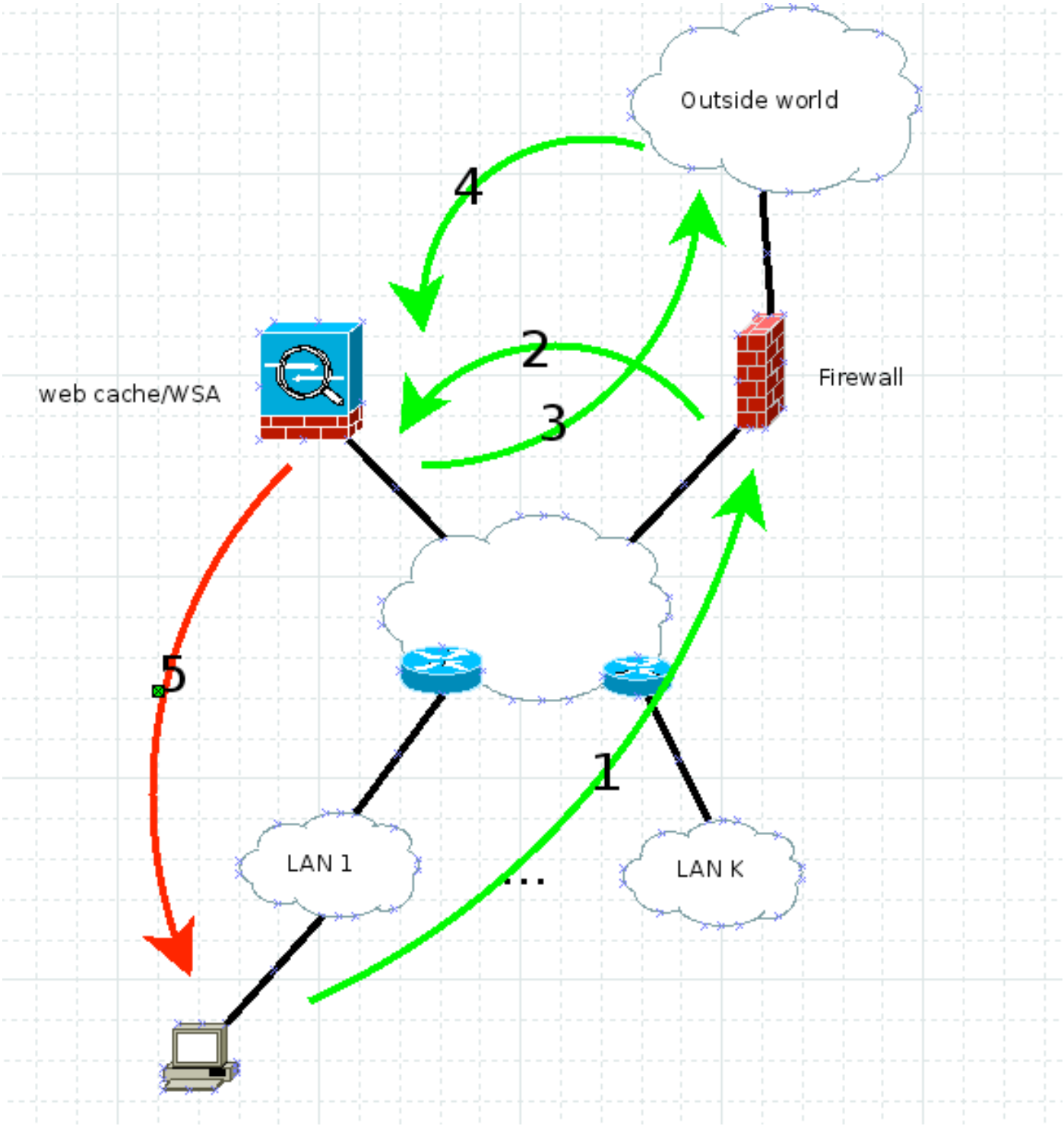
هذا هو مركز اكتشاف MTU للمسار. يمكنك إرسال حزم كبيرة مع مجموعة بت DF لمعرفة ما إذا كانوا يقومون به نحو النهاية أو إذا كنت تتلقى تقرير ICMP كما هو موضح مسبقا. بمجرد تحديد الحد الأقصى لحجم الحزمة القابلة للعمل، استخدمه لأي إتصالات أخرى. راجع RFC 1191 للحصول على مزيد من المعلومات.

يوظف جهاز أمان الويب (WSA) اكتشاف وحدة الحد الأقصى للنقل (MTU) للمسار بشكل افتراضي. وبالتالي، فإن كل الحزم التي تم إنشاؤها لها البت DF مضبوطة بالتكوين الافتراضي.

WCCP

إذا كنت بحاجة إلى فرض الأمان على شبكتك على حركة مرور الويب دون معرفة الآخرين، فأنك تقوم بتشغيل حركة مرور البيانات الخاصة بهم عبر وكيل غير مرئي. WCCP هو البروتوكول الذي يتم إستخدامه للاتصال بين الجهاز الذي يعترض (الموجه/جدار الحماية) ومحرك/وكيل ذاكرة التخزين المؤقت للويب، وهو WSA في هذه الحالة.

يوضح هذا المخطط كيفية تدفق حركة المرور في هذا السيناريو:



تعمل هكذا:

1. يرسل العميل HTTP مع مصدر IP، وعنوان IP الخاص به (عنوان IP للعميل)، وعنوان IP للخادم الوجهة.

2. يعترض جدار الحماية أو الموجه HTTP الحصول على HTTP ويعيد توجيهه عبر WCCP GRE أو L2 الصافي إلى ذاكرة التخزين المؤقت للويب/WSA. المصدر لا يزال عنوان IP العميل والوجهة لا تزال عنوان IP لخادم الويب.

3. تفحص WSA الطلب، وإذا كان شرعيا، فتقوم بعكسه تجاه خادم الويب. هنا الغاية عنوان هو ال web server عنوان والمصدر عنوان أمكن كنت ال WSA أو الزبون، يؤسس على ما إذا أنت مكنت زبون عنوان انتحال. على سبيل المثال، لا يهم أن حركة المرور العائدة في كلا الحالتين يجب أن تضرب WSA.

4. يتم فحص حركة المرور العائدة في WSA.

5. يرسل ال WSA الاستجابة إلى الزبون مع المصدر عنوان، دائما ال web server عنوان (لذلك الزبون لا يشك)، والعنوان.

المشكلة

ماذا يحدث إذا اضطر أحد الموجهات من المخطط إلى تجزئة حركة المرور؟ تضع WSA بت DF على الحزمة رقم 5، لكنها يجب أن تكون مجزأة. يقوم الموجه بإسقاطه ويخبر المرسل بأن التجزئة مطلوبة ولكن تم تعيين بت DF (رمز ICMP النوع 3 4). وعلى أية حال، يجب أن يعمل RFC 1191 الآن ويجب على المرسل تقليل حجم الحزمة الخاصة به.

باستخدام WCCP، يكون عنوان IP المصدر هو عنوان IP لخادم الويب، لذلك لا يذهب ICMP هذا إلى WSA أبدا، بل يحاول الانتقال إلى خادم الويب الحقيقي (تذكر، أن هذا الموجه الموجود في الأسفل لا يعي WCCP). هذه هي الطريقة التي يتم بها أستكشاف WCCP و MTU للمسار معا في بعض الأحيان كسر تصميم الشبكة لديك.

الحل

هناك أربع طرق لحل هذه المشكلة:

- اكتشف وحدة الحد الأقصى للنقل (MTU) الحقيقية ثم أستخدم **etherConfig** على WSA لخفض وحدة الحد الأقصى للنقل (MTU) للواجهة. تذكر أن رأس TCP هو 60، و IP هو 20، وعندما تستخدم ICMP، فإن ذلك يضيف 8 بايت إلى رأس IP.

- تعطيل اكتشاف MTU للمسار (أمر CLI WSA ل **pathMtudiscovery**). ينتج عن ذلك TCP MSS ل 536، والذي قد يسبب مشكلة في الأداء.

- غيرت الشبكة لذلك هناك ما من L3 تجزئة بين WSA والعملاء.

- أستخدم الأمر **ip tcp mss-adjust 1360** (أو رقم محسوب آخر) على كل موجه من Cisco في الطريق على الواجهات ذات الصلة.

ملاحظات إضافية

بينما كانت هذه المشكلة قيد التحقيق، تم اكتشاف أنه إذا قمت بتعيين الوكيل بشكل صريح في العميل لبضع دقائق ثم قم بإزالته، فسيتم حل المشكلة خلال الساعات الأربع إلى الخمس التالية. وذلك نظرا لحقيقة أن آلية اكتشاف وحدة الحد الأقصى للنقل (MTU) للمسار بين WSA والعميل تعمل، في الوضع الصريح. بمجرد أن يكتشف WSA وحدة الحد الأقصى للنقل (MTU) للمسار، فإنه يخزنها مع TCP MSS المكتشفة على الجدول الداخلي للمرجع. يبدو أنه يتم تحديث هذه الطاولة كل أربع إلى خمس ساعات، مما يجعل الحل لا يعمل مرة أخرى بعد مرور الكثير من الوقت.

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).