يفشل IPsec عبر TCP عند تدفق حركة المرور عبر ASA

المحتويات

المقدمة

قد تتصل عملاء شبكة VPN من Cisco المتصلة بنقطة وصول VPN باستخدام IPsec عبر TCP بغرامة وحدة الاستقبال والبث، ولكن بعد ذلك يفشل الاتصال بعد بعض الوقت. يوضح هذا المستند كيفية التبديل إلى IPsec عبر UDP أو تضمين IPsec ESP الأصلي لحل المشكلة.

قبل البدء

المتطلبات

من أجل مواجهة هذه المشكلة المحددة، يجب تكوين عملاء Cisco VPN للاتصال بجهاز وحدة الاستقبال والبث الخاصة بشبكة VPN باستخدام IPsec عبر TCP. في معظم الحالات، يقوم مسؤولو الشبكة بتكوين ASA لقبول إتصالات عميل Cisco VPN عبر منفذ TCP 10000.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى عميل Cisco VPN.

الاصطلاحات

للحصول على مزيد من المعلومات حول اصطلاحات المستندات، ارجع إلى اصطلاحات تلميحات Cisco التقنية.

المشكلة

عند تكوين عميل VPN ل IPsec عبر TCP (cTCP)، لن يستجيب برنامج عميل شبكة VPN إذا تم تلقي تكرار TCP ACK طالبا من عميل VPN إعادة إرسال البيانات. قد يتم إنشاء مكرر ACK إذا كان هناك فقدان حزمة في مكان ما بين عميل VPN ووحدة الاستقبال والبث الخاصة ب ASA. تعتبر خسارة حزم البيانات المتقطعة حقيقة شائعة إلى حد

ما على الإنترنت. ومع ذلك، نظرا لأن نقاط نهاية الشبكة الخاصة الظاهرية (VPN) لا تستخدم بروتوكول TCP (ارجع إلى أنها تستخدم cTCP)، فستستمر نقاط النهاية في الإرسال وسيستمر الاتصال.

في هذا السيناريو، تحدث مشكلة إذا كان هناك جهاز آخر مثل جدار الحماية يتتبع اتصال TCP بشكل كبير. بما أن بروتوكول cTCP لا يطبق بروتوكول TCP بالكامل ولا تتلقى رسائل ACK المكررة الخاصة بالخادم إستجابة، فإن ذلك قد يتسبب في قيام الأجهزة الأخرى المتوافقة مع تدفق الشبكة هذا بإسقاط حركة مرور TCP. يجب أن يحدث فقد الحزمة على الشبكة مما يتسبب في فقدان مقاطع TCP، وهو ما يؤدي إلى تشغيل المشكلة.

هذا ليس خطأ، ولكن تأثير جانبي لكل من فقدان الحزمة على الشبكة وحقيقة أن cTCP ليس TCP حقيقي. يحاول cTCP محاكاة بروتوكول TCP من خلال التفاف حزم IPsec داخل رأس TCP، ولكن هذا هو مدى البروتوكول.

يحدث هذا الإصدار عادة عندما يقوم مسؤولو الشبكة بتنفيذ ASA باستخدام IPS، أو القيام بنوع من فحص التطبيق على ASA يتسبب في عمل جدار الحماية كوكيل TCP كامل للاتصال. إذا كان هناك فقد للحزم، فسيقوم ASA بتعويض البيانات المفقودة نيابة عن خادم cTCP أو العميل، ولكن لن يستجيب عميل شبكة VPN أبدا. وبما ان ال ASA لا يستلم ابدا البيانات التي يتوقعها، لا يمكن ان يستمر الاتصال. ونتيجة لذلك، يفشل التوصيل.

الحل

لحل هذه المشكلة، قم بتنفيذ أي من هذه الإجراءات:

- قم بالتبديل من IPsec عبر TCP إلى IPsec عبر UDP، أو التضمين الأصلي باستخدام بروتوكول ESP.
- قم بالتبديل إلى عميل AnyConnect لإنهاء الشبكة الخاصة الظاهرية (VPN)، والذي يستخدم مكدس بروتوكول TCP الذي تم تنفيذه بالكامل.
- قم بتكوين ASA لتطبيق تجاوز TCP-state لهذه التدفقات المحددة ل IPsec/TCP. يؤدي هذا بشكل أساسي إلى تعطيل جميع عمليات التحقق من الأمان للاتصالات التي تطابق سياسة تجاوز TCP-State، ولكنه سيسمح للاتصالات بالعمل حتى يمكن تنفيذ حل آخر من هذه القائمة. لمزيد من المعلومات، ارجع إلى إرشادات تجاوز حالة TCP والقيود.
- حدد مصدر فقدان الحزمة، واتخذ الإجراء التصحيحي لمنع حزم IPsec/TCP من السقوط على الشبكة. وعادة ما يكون ذلك أمرا مستحيلا أو صعبا للغاية لأن المشغل لهذه المسألة يكون عادة فقدان حزم البيانات على الإنترنت ولا يمكن منع عمليات السقوط.

معلومات ذات صلة

- الدعم التقني والمستندات - Cisco Systems

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).