خطأ في مزامنة تكوين ZTNA للوصول الآمن إلى الشبكة مع فك تشفير SSL وأنفاق

المحتويات

مسألة

تم بنجاح تسجيل الوصول الآمن إلى Cisco Secure Client Zero Trust Access (ZTA)، ولكن يفشل أثناء مزامنة التكوين مع استجابات HTTP 502 وحالة اتصال الخادم "BadResponse". تظهر سجلات DART من نقطة نهاية Windows 11 التسجيل الناجح ولكن مرات فشل مزامنة التكوين المتكررة. تحدث المشكلة فقط عندما تكون نقطة النهاية متصلة بمسار الامن Meraki AutoVPN، بينما شبكة الشركة باستخدام وكيل Secure Access/Umbrella مع أنفاق مزامنة التكوين على شبكة محلية بدون بنية تقوم نقطة النهاية نفسها بنجاح بإكمال النفق الأساسي للوكيل وأ.

البيئة

- Cisco Secure Client ZTA، الإصدار 5.1.16.4434
- نقطة نهاية Windows 11 Enterprise
- أجهزة Meraki MX مع دمج AutoVPN
- الوصول الآمن (SSE) باستخدام عبارة أنفاق الشبكة (NTG)
- نظام أسماء المجال للوصول الآمن أو Umbrella DNS
- تم تمكين فك تشفير SSL وفحص HTTPS على مسار شبكة الشركة
- تم تكوين قائمة عدم فك التشفير (DND) التي تم توفيرها بواسطة النظام لم يتم بشكل مبدئي

رارق

تم حل فشل مزامنة التكوين من خلال تنفيذ عمليات تجاوز فك تشفير SSL المناسبة عند إستخدام أنفاق الشبكة مع الوصول الآمن ZTA للمجالات ذات الصلة.

الخطوة 1: تحديد تأثير فك تشفير SSL

تحقق من أن فك تشفير SSL يتسبب في فشل مزامنة التكوين عن طريق مراجعة سجلات البحث عن النشاط في "الوصول الآمن" لأحداث فك التشفير المتعلقة بمجالات ZTA.

الخطوة 2: تكوين قائمة DND التي يوفرها النظام

عند إستخدام عبارة أنفاق الشبكة (NTG) مع الوصول الآمن، يجب تمكين النظام الذي تم توفيره DND لاجتياز حركة المرور المتعلقة ZTA بشكل صحيح من فحص SSL.

انتقل إلى لوحة معلومات الوصول الآمن > Secure (تأمين) > عدم فك تشفير القوائم القائمة وتعديل النظام المتوفر لا تقم بفك تشفير القائمة.

الخطوة 3: إنشاء ملف تعريف أمان لمجالات ZTA

قم بإضافة المجالات المرتبطة ب ZTA المطلوبة إلى ملف تعريف أمان جديد باستخدام قائمة DND التي يوفرها النظام:

- zpc.sse.cisco.com
- *.zpc.sse.cisco.com
- ztna.sse.cisco.com
- acme.sse.cisco.com
- devices.api.umbrella.com

الخطوة 4: تطبيق ملف تعريف الأمان على قاعدة الاختبار

قم بتعيين ملف تعريف الأمان الذي تم إنشاؤه حديثا والذي يحتوي على مجال ZTA الذي يتجاوز قاعدة إختبار للتحقق من التكوين.

الخطوة 5: التحقق من صحة مزامنة التكوين

إختبار مزامنة تسجيل ZTA والتكوين من شبكة الشركة. يمكن الآن إكمال المزامنة بنجاح بدون أخطاء HTTP 502.

الخطوة 6: التنسيق مع فريق Meraki

للحصول على تغطية شاملة، قم بالتنسيق مع دعم Meraki للتحقق من صحة عناوين URL الرسمية ذات الصلة ب ZTA والنطاقات التي يمكن تجاوزها من فحص الوصول الآمن. الإشارة إلى وثائق Meraki هذه:

- قواعد جدار الحماية للتدفق لاتصال السحابة
- تحديث URL لوحة معلومات Meraki - التوافق مع PCI

السبب

نتج فشل مزامنة التكوين عن فك تشفير SSL وتوكيل حركة مرور Zero Trust Access على شبكة الشركة. عند إستخدام عبارة أنفاق الشبكة (NTG) مع الوصول الآمن، يجب تجاوز المجالات ذات الصلة ب ZTA باستخدام قائمة عدم فك تشفير (DND) المقدمة من النظام. بدون تكوين الالتفاف هذا، يقوم فحص SSL بتعديل سلاسل الشهادات ويدخل في اتصال مستوى التحكم ZTA، مما يتسبب في تلقي العميل استجابات HTTP 502 أثناء محاولات مزامنة التكوين.

المحتوى ذي الصلة

- أستكشاف أخطاء فك تشفير الوصول الآمن و SSL وإصلاحها
- خدمات التسجيل المستندة إلى العميل لـ Secure Access Zero Trust

- نمآلا لوصولل ZTA لاجم تابلطتم
- اهحالصإو نمآلا لوصولا أطخ لجيست لكاشم فاشكتسأ
- اهحالصإو لماعلا نيوكت ةنمازم ءاطخأ فاشكتسأ
- اهحالصإو ءاطخألا فاشكتسالا ةيلصفتلا ZTNA تالجس عيمجت
- Cisco نم تانزيلتلاو ينفلا معدلا

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).