تكوين SSE عدم فك تشفير IPS و SWG فك تشفير المرجى الجانبي

المحتويات

مسألة

تستمر حركة مرور HTTPS إلى وجهات فئة التمويل في تقديم شهادة Cisco SSE بدلا من شهادة موقع الويب الأصلية، حتى بعد إضافة فئة "التمويل" أو مجالات محددة إلى قائمة "عدم فك تشفير (DND)" وتطبيق قاعدة الوصول ذات الصلة. ويلاحظ هذا السلوك عند الوصول إلى المواقع عبر Zero Trust Access Client (TIA)، مما يؤثر على وجه التحديد على الوصول إلى مواقع الويب المتعلقة بالتمويل مثل https://onlinesbi.sbi.bank.in/ حيث يلزم رؤية الشهادة من نهاية إلى نهاية.

والسلوك المتوقع هو أنه عند إضافة فئة موقع أو محتوى إلى قائمة DND، يمكن تقديم شهادة موقع الويب الأصلي إلى المستعرض بدلا من شهادة SSE من Cisco. ومع ذلك، يستمر تقديم شهادة Cisco SSE، التي تشير إلى أن فك تشفير حركة المرور لا يزال يحدث على الرغم من تكوين DND.

البيئة

- حافة الخدمة الآمنة (SSE) من Cisco
- اتصال Zero Trust Access Client (TIA)
- تم تمكين فك تشفير IPS العمومي
- نشط على سياسات الوصول IPS
- فئة التمويل التي تم تكوينها في قائمة عدم فك التشفير داخل ملف تعريف الأمان
- قواعد الوصول المطبقة مع ملفات تعريف الأمان المطابقة

قرار

يتضمن الحل فهم أن Cisco SSE ينجز نوعين متميزين من فك الترميز وتشكيل الإعدادات

.المنانسبة عدم فك الترميز لكل نوعي فك الترميز

فهم أنواع فك تشفير SSE

:يقوم Cisco SSE بعمليتي فك تشفير مستقلتين

- فك تشفير SWG (بوابة الويب الآمنة) - فك تشفير وكيل الويب
- فك تشفير IPS - فك تشفير نظام منع الاقتحام

عدم فك تشفير الإدخالات التي تم تكوينها داخل ملف تعريف أمان يطبق فقط على فك تشفير IPS. عند تمكين فك تشفير IPS العام ونشاط IPS وتشفير SWG والسماح بفك تشفير IPS، مما يؤدي إلى تقديم شهادة Cisco SSE إلى أي نهج وصول، يستمر فك تشفير IPS على المستعرض.

خطوات التكوين

الخطوة 1: إضافة مواقع أو فئات محتوى إلى النظام الذي تم توفيره التي تم فك تشفير القائمة.

يتم تطبيق قائمة عدم فك تشفير النظام المتوفرة عبر جميع ملفات تعريف IPS. تؤدي إضافة فئة موقع الويب أو محتوى إلى القائمة التي يوفرها النظام إلى تقديم شهادة موقع الويب الأصلي، مما يؤدي إلى تجاوز عملية فك تشفير IPS بشكل فعال.

الخطوة 2: تحقق من عدم الحاجة إلى تغييرات إضافية في النهج.

تحقق من عدم الحاجة للإشارة إلى عدم فك تشفير قائمة النظام المتوفرة داخل سياسات الوصول. IPS تطبق القائمة تلقائيا على كل توصيفات IPS.

إختبار التحقق من الصحة

:يمكن إستخدام أساليب التحقق من الصحة هذه لتأكيد التكوين الصحيح

الطريقة 1: إضافة مجال إلى النظام الذي تم توفيره ال تقم بفك تشفير القائمة

قد يؤدي إضافة المجال المحدد إلى "قائمة عدم فك التشفير" المقدمة إلى تقديم شهادة SSE من Cisco. موقع الويب الأصلي بدلا من شهادة

الطريقة 2: تعطيل فك تشفير IPS العمومي مؤقتا (للاختبار فقط)

يؤدي تعطيل فك تشفير IPS العمومي بشكل مؤقت أيضا إلى ظهور الشهادة الأصلية SSE من Cisco. للموقع الذي تم إختباره، مما يؤكد أن فك تشفير IPS هو سبب عرض شهادة

النتائج المتوقعة

بعد التهيئة الصحيحة:

- لا تقوم المواقع أو فئات المحتويات التي تمت إضافتها إلى النظام المتوفر بفك تشفير قائمة شهادات مواقع الويب الأصلية الخاصة بها.
- يتم تجاوز كل من فك تشفير SWG و IPS للمواقع أو الفئات المحددة.
- يعرض المستعرض شهادة موقع الويب الفعلية بدلا من شهادة SSE من Cisco.

السبب

عملية: فك تشفير SWG في Cisco SSE يزج إثنان من فصل فك التشفير الإصدار لأن يقع فك تشفير IPS. لا تقوم بفك تشفير الإدخالات التي تم تكوينها داخل ملفات تعريف IPS العمومي ونشاط IPS الأمان فقط تجاوز فك تشفير SWG. عند تمكين فك تشفير IPS في الحدوث بشكل مستقل، مما يتسبب في استمرار فك تشفير IPS على سياسات الوصول، مما يتسبب في DND قوائم المواقع في تضمين المواقع حتى عند المستعرض إلى Cisco SSE تقديم شهادة في الخاصة بملف تعريف الأمان.

لتجاوز الكل النوعين من فك التشفير بشكل كامل، يجب إضافة المواقع أو فئات المحتوى التي تنطبق على جميع ملفات تعريف IPS المقدمة من قبل النظام، والتي تمنع حدوث فك تشفير SWG و IPS.

المحتوى ذي الصلة

- [نمآلا لوصولا ريفشت كم دعل ةمئاق ءاشنإ](#)
- [نمآلا لوصولل ةيساسألا تامولعملا عيمجتو اهالصإو ءاطخألا فاشكتسأ](#)
- [Cisco نم تالينزلتو 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).