أستكشاف أخطاء APP_UNREACHABLE وإصلاحها للتطبيقات الخاصة في الوصول الآمن

المحتويات

مسألة

عند محاولة الوصول إلى تطبيقات الوصول إلى الشبكة دون ثقة (ZTNA) من خلال Cisco Secure Access، يواجه المستخدمون رسالة خطأ "تطبيق يتعذر الوصول إليه".

- يظهر الموصل صحة/نشاط في لوحة المعلومات، ويتم تأكيد تشغيل التطبيق بواسطة مالكه.
- قد يؤثر الفشل على جميع مستخدمي تطبيق واحد بينما تعمل التطبيقات الأخرى التي يخدمها نفس الموصل بشكل طبيعي.
- في عمليات نشر مجموعة الموصلات، يمكن أن تظهر حالات الفشل بشكل متقطع — تنجح جلسات العمل أو تفشل وفقا للموصل الذي تم تحديده في المجموعة.

البيئة

- نشر الوصول الخاص الآمن من Cisco باستخدام ZTNA
- الموارد الخاصة التي تم تكوينها للوصول إلى ZTNA
- نشر موصل الموارد للوصول إلى الموارد الخاصة

قرار

الخطوة 1. إختبار إمكانية الوصول المباشر من مقطع شبكة Connectors

- موصل الموارد هو جهاز مؤمن ولا يوفر وصول shell إلى أوامر التشغيل مثل curl أو nc مباشرة. بدلا من ذلك، قم بإجراء إختبار قابلية الوصول من مضيف إختبار (أو جهاز VM مؤقت) تم وضعه في نفس الشبكة الفرعية/شبكة VLAN الخاصة بالموصل، وبالتالي فإنه يخضع لنفس قواعد مسار الشبكة والتوجيه وجدار الحماية للتطبيق:

```
curl -v http://APP_IP:PORT/health
nc -zv APP_IP PORT
```

- في حالة فشل هذا الإجراء، يتم تأكيد المشكلة في مسار الشبكة أو على خادم التطبيق — قم بإصلاح هذا أولا قبل مراجعة أي تكوين وصول آمن.

✎ ملاحظة: إن الاختبار من شبكة فرعية مختلفة ليس حاسما — يتم تقييم قواعد جدار الحماية والتوجيه لكل مصدر، حيث يجب أن يعكس مصدر الاختبار وضع IP للموصل عن كثب قدر الإمكان.

الخطوة 2. التحقق من تكوين الموارد الخاصة

- في لوحة معلومات الوصول الآمن، انتقل إلى الموارد > الموارد الخاصة، وافتح المورد الخاص المتأثر، وقارن IP الذي تم تكوينه و FQDN و Port character-for-character مقابل عنوان الربط والمنفذ الفعليين للتطبيق الجاري تشغيله.
- ينتج أي عدم تطابق (IP قديم بعد ترحيل خادم، منفذ خاطئ، HTTP مقابل HTTPS) APP_UNREACHABLE حتى مع مسار شبكة سليم تماما.

الخطوة 3. التحقق من دقة DNS للموصل

- إذا تم تحديد المورد الخاص بواسطة FQDN، فتحقق من إمكانية حل خوادم DNS المعينة للموصل له. من واجهة سطر الأوامر (CLI) لموصل الموارد (توفر عمليات نشر VM واجهة سطر أوامر (CLI) تشخيصية مع أوامر أستكشاف أخطاء Linux القياسية المدعومة)، قم بتشغيل:

```
nslookup app.internal.company.com <internal_DNS_server_IP>
```

- تأكد من إرجاع IP الخاص الصحيح. تأكد من وجود نقاط تكوين شبكة الموصل في خوادم DNS الداخلية التي يمكنها حل شبكات FQDN الخاصة بالتطبيقات؛ يتعذر على "الموصل" المكون بواسطة المحددات العامة حل المناطق الداخلية.

الخطوة 4. مراجعة مسار جدار الحماية

- قم بتأكيد قواعد جدار الحماية (جدران حماية الشبكة وجدار حماية المضيف على خادم التطبيق) للسماح بحركة المرور من عنوان IP الخاص بالموصل إلى IP الخاص بخادم التطبيق على المنفذ المطلوب.

الخطوة 5. التقاط حركة مرور البيانات باستخدام tcpdump على موصل المواد

- قم بتشغيل التقاط حزمة على "موصل المواد" لمراقبة محاولات اتصال المبيل الأخير باتجاه التطبيق. تتوفر الأداة المساعدة tcpdump في موصل المواد—ارجع إلى دليل تشغيل tcpdump في موصلات المواد.

تلميح: لجعل عملية الالتقاط محددة في نشر مجموعة موصلات، احتفظ مؤقتا بموصل مواد واحد ممكن في المجموعة حتى تتمكن جميع جلسات عمل المورد من إجتيازه، ثم قم بتشغيل عملية الالتقاط التي تمت تصفيتها على خادم التطبيق والمنفذ.

- على سبيل المثال:

```
tcpdump 'host x.x.x.x and tcp port 443'
```

(حيث يكون x.x.x.x هو عنوان IP الخاص بخادم التطبيق، بينما يكون 443 هو منفذ التطبيق)

- ترجمة النتائج: تشير SYN الصادرة التي لا تحتوي على SYN-ACK إلى إسقاط جدار حماية أو أن التطبيق لا ينصت؛ يشير RST فوري إلى أن المضيف يمكن الوصول إليه ولكن لا شيء مرتبط بالمنفذ؛ لا توجد حزم على الإطلاق باتجاه التطبيق يشير إلى أن جلسة العمل لا تصل إلى هذا الموصل أو أن DNS قد تم حلها إلى عنوان غير متوقع.

- قم بإعادة تمكين الموصلات المتبقية في المجموعة بمجرد اكتمال عملية الالتقاط.

السبب

- جدار الحماية يمنع حركة مرور الموصلات إلى التطبيقات: يقوم جدار الحماية القائم على الشبكة أو المضيف بحظر المنفذ المطلوب بين IP مضيف الموصل و IP خادم التطبيق.
- عدم تطابق تكوين الموارد الخاصة في Secure Access: ال يتطابق IP أو FQDN أو المنفذ الذي تم تكوينه في تعريف الموارد الخاصة (الموارد > الموارد الخاصة) مع ما يستمع إليه التطبيق بالفعل (على سبيل المثال، تم نقل التطبيق إلى IP جديد، أو استمعت إلى 8443 أثناء تكوين 443).
- فشل تحليل DNS للموصل: يتم تحديد المورد الخاص بواسطة FQDN، ولكن خوادم DNS للموصل ال تحل FQDNs الخاصة بالتطبيق.
- خادم التطبيق معطل أو غير مصغي: يبدو الخادم سليما وفقا لمقاييس أخرى ولكنه غير مرتبط بالمنفذ المتوقع أو أن الخدمة قد تحطمت بينما ظل المضيف قيد التشغيل.
- إمكانية الوصول الجزئي في تجمع موصل: يوجد موصل واحد أو أكثر في التجمع في مقطع شبكة ال يمكنه الوصول إلى التطبيق، لذلك تفشل جلسات العمل المعينة لتلك الموصلات فقط.

المحتوى ذي الصلة

- أستكشاف الأخطاء وإصلاحها وتجميع المعلومات الأساسية ل Cisco Secure Access
- الدعم الفني والتنزيلات من Cisco

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).