مصادقة ASA إلى ASA في وضع استعادة الاشتراك عندما يكون جهاز AAA موجود من خلال مثال تكوين L2L

المحتويات

المقدمة

يصف هذا المستند كيفية العمل حول سيناريو لا يمكن فيه للمسؤول المصادقة على جهاز أمان قابل للتكيف (ASA) من Cisco في زوج تجاوز الفشل نظرا لحقيقة وجود خادم المصادقة والتفويض والمحاسبة (AAA) على موقع بعيد من خلال شبكة LAN إلى شبكة LAN (L2L).

وعلى الرغم من إمكانية إستخدام الطريقة الاحتياطية للمصادقة المحلية، فيفضل مصادقة RADIUS لكلا الوحدتين.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- تجاوز فشل ASA
- VPN
- ترجمة عنوان الشبكة (NAT)

المكونات المستخدمة

لا يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي

أمر.

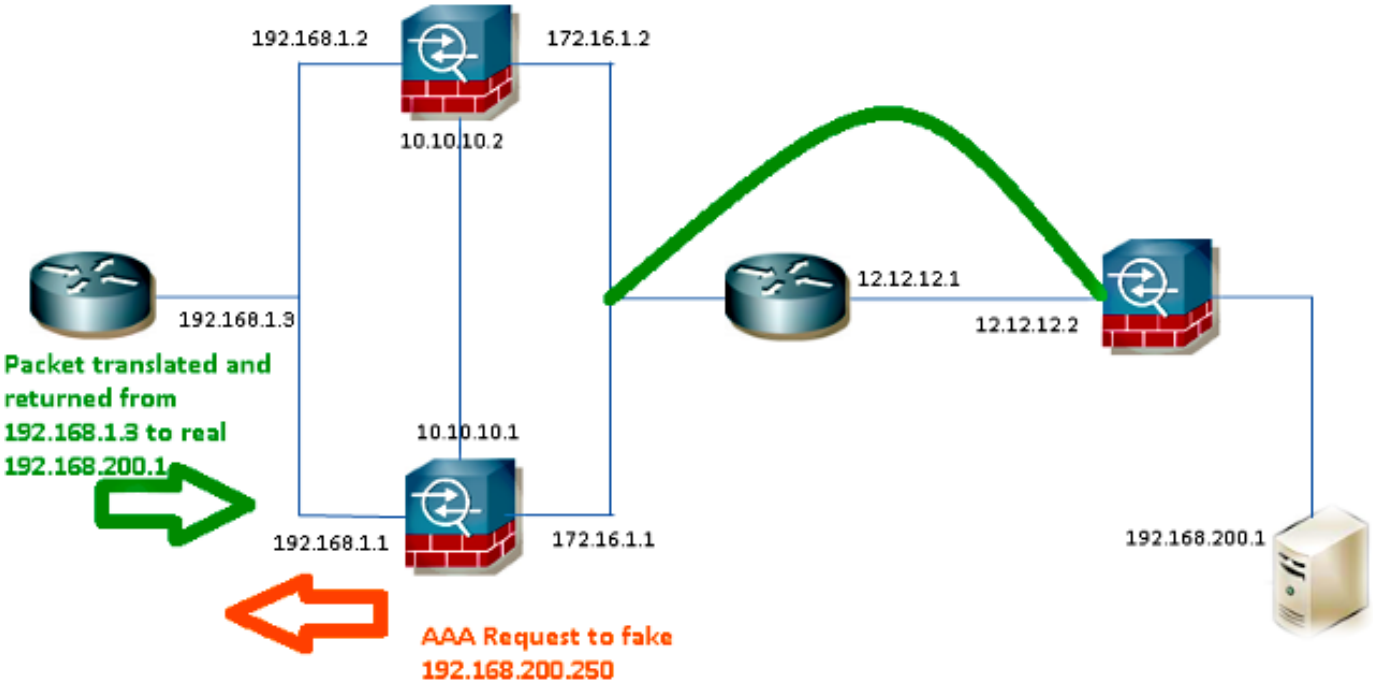
التكوين

ملاحظة: أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

الرسم التخطيطي للشبكة

يوجد خادم RADIUS على الجانب الخارجي لزوج تجاوز الفشل ويمكن الوصول إليه من خلال نفق L2L إلى 12.12.12.2. هذا ما يسبب المشكلة لأن ASA الاحتياطي يحاول الوصول إليها من خلال الواجهة الخارجية الخاصة به ولكن لا يوجد نفق تم إنشاؤه عليه في هذه النقطة؛ ولأنه يعمل، يجب أن يرسل الطلب إلى الواجهة النشطة حتى يمكن للحزمة التدفق عبر الشبكة الخاصة الظاهرية (VPN) ولكن يتم نسخ المسارات من الوحدة النشطة.

أحد الخيارات هو إستخدام عنوان IP مزيف لخادم RADIUS على ASAs وتوجيهه إلى الداخل. لذلك، المصدر والوجهة عنوان من هذا ربط يستطيع كنت ترجمت على أداة داخلي.



الموجه 1

```
interface FastEthernet0/0
ip address 192.168.1.3 255.255.255.0
no ip redirects
no ip unreachables
ip nat enable
duplex auto
speed auto

ip access-list extended NAT
permit ip 192.168.1.0 0.0.0.255 host 192.168.200.250

ip nat source list NAT interface FastEthernet0/0 overload
```

```
ip nat source static 192.168.200.1 192.168.200.250

ip route 0.0.0.0 0.0.0.0 192.168.1.1
```

ASA

```
aaa-server RADIUS protocol radius
aaa-server RADIUS (inside) host 192.168.200.250
timeout 3
***** key
authentication-port 1812
accounting-port 1813

aaa authentication serial console LOCAL
aaa authentication ssh console RADIUS LOCAL
aaa authentication telnet console RADIUS LOCAL
aaa authentication http console RADIUS LOCAL
aaa authentication enable console RADIUS LOCAL

route outside 0.0.0.0 0.0.0.0 172.16.1.3 1
route inside 192.168.200.250 255.255.255.255 192.168.1.3 1
```

ملاحظة: تم إستخدام عنوان 192.168.200.250 IP في المثال، ولكن أي عنوان IP غير مستخدم يعمل.

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر **show**. استخدم "أداة مترجم الإخراج" لعرض تحليل لمُخرَج الأمر **show**.

الموجّه

```
Router#   show ip nat nvi tra
Pro Source global Source local Destin local Destin global
udp 192.168.1.3:1025 192.168.1.1:1025 192.168.200.250:1812 192.168.200.1:1812
--- --- 192.168.2.1 192.168.200.1 ---
--- --- 192.168.200.1 192.168.200.250 ---
```

استكشاف الأخطاء وإصلاحها

لا تتوفر حاليًا معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

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).