ASA 8.3: إنشاء الاتصال واستكشاف أخطائه وإصلاحها من خلال جهاز الأمان من Cisco

المحتويات

المقدمة

عند تكوين جهاز الأمان القابل للتكيف (ASA) من Cisco في البداية، يكون لديه سياسة أمان افتراضية حيث يمكن لكل شخص موجود من الداخل الخروج، ولا يمكن لأي شخص من الخارج الدخول. إذا كان الموقع الخاص بك يحتاج إلى نهج أمان مختلف، فيمكنك السماح للمستخدمين الخارجيين بالاتصال بخادم الويب الخاص بك من خلال ASA.

بمجرد إنشاء اتصال أساسي من خلال Cisco ASA، يمكنك إجراء تغييرات التكوين على جدار الحماية. تأكد من أن أي تغييرات في التكوين تقوم بها على ASA تتوافق مع نهج أمان الموقع الخاص بك.

ارجع إلى PIX/ASA: إنشاء الاتصال واستكشاف أخطائه وإصلاحها من خلال جهاز الأمان من Cisco للتكوين المتطابق على Cisco ASA مع الإصدارات 8.2 والإصدارات الأقدم.

المتطلبات الأساسية

المتطلبات

يفترض هذا المستند أنه قد تم بالفعل إكمال بعض التكوينات الأساسية على Cisco ASA. ارجع إلى هذه المستندات للحصول على أمثلة لتكوين ASA الأولي:

- ASA 8.3(x): توصيل شبكة داخلية واحدة بالإنترنت
- تكوين عميل PPPoE على جهاز الأمان القابل للتكيف (ASA) من Cisco

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى جهاز الأمان القابل للتكيف (ASA) من Cisco الذي يشغل الإصدار 8.3 والإصدارات الأحدث.

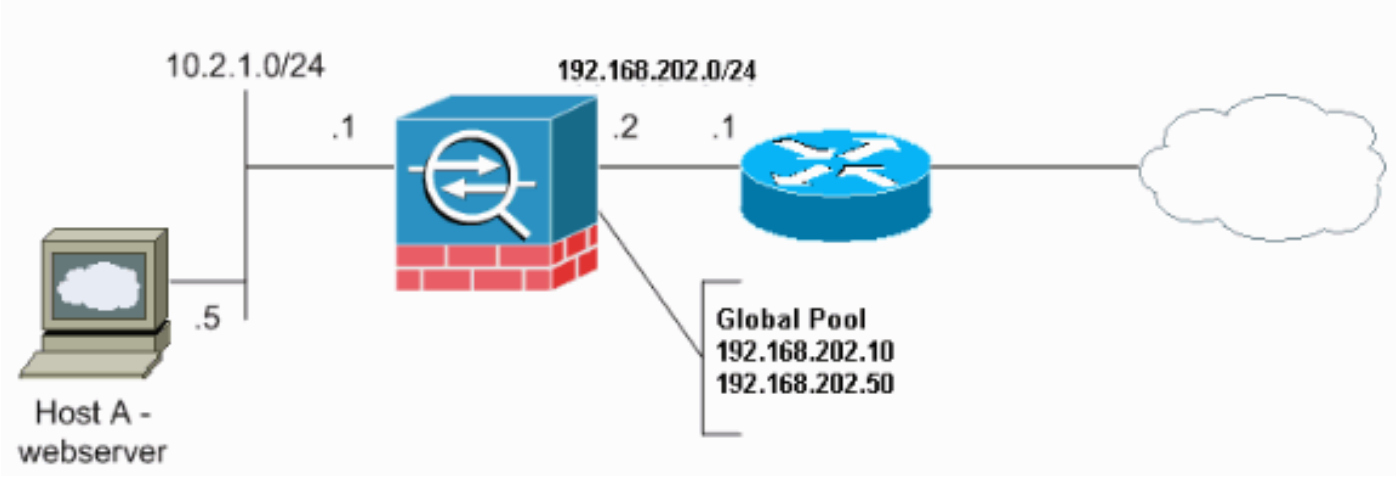
تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

كيفية عمل الاتصال من خلال ASA

في هذه الشبكة، المضيف A هو خادم ويب بعنوان داخلي 10.2.1.5. تم تعيين عنوان خارجي (مترجم) لخادم الويب بقيمة 192.168.202.5. يجب أن يشير مستخدمو الإنترنت إلى 192.168.202.5 للوصول إلى خادم الويب. يجب أن يكون إدخال DNS لخادم ويب هذا العنوان. لا يسمح بأي إتصالات أخرى من الإنترنت.



ملاحظة: ال ip ليس يخاطب خطة يستعمل في هذا تشكيل قانونيا routable على الإنترنت. وهي عناوينRFC 1918 التي تم استخدامها في بيئة مختبرية.

تكوين الاتصال من خلال Cisco ASA

أتمت هذا steps in order to شكلت موصولية من خلال ال ASA:

قم بإنشاء كائن شبكة يحدد الشبكة الفرعية الداخلية وكائن شبكة آخر لنطاق تجمع IP. شكلت ال nat يستعمل. هذا شبكة كائن:

```
object network inside-net
 subnet 0.0.0.0 0.0.0.0
object network outside-pat-pool
range 192.168.202.10 192.168.202.50
nat (inside,outside) source dynamic inside-net  outside-pat-pool
```

2. عينت عنوان ساكن إستاتيكي مترجم للمضيف الداخلي الذي يمكن لمستخدمي الإنترنت الوصول إليه.

```
object network obj-10.2.1.5
 host 10.2.1.5
```

```
nat (inside,outside) static 192.168.202.5
```

3. أستخدم الأمر **access-list** للسماح للمستخدمين الخارجيين من خلال Cisco ASA. أستخدم دائما العنوان المترجم في الأمر **access-list**.

```
access-list 101 permit tcp any host 192.168.202.5 eq www
access-group 101 in interface outside
```

السماح بحركة مرور بث ARP

يقوم جهاز الأمان بتوصيل الشبكة نفسها على الواجهات الداخلية والخارجية الخاصة بها. نظرا لأن جدار الحماية ليس عبارة عن جنجل موجه، فيمكنك بسهولة تقديم جدار حماية شفاف إلى شبكة موجودة. إعادة عنونة IP غير ضرورية. يتم السماح بحركة مرور IPv4 تلقائيا من خلال جدار الحماية الشفاف من واجهة أمان أعلى إلى واجهة أمان أقل، بدون قائمة وصول. يتم السماح ببروتوكولات تحليل العنوان (ARPs) من خلال جدار الحماية الشفاف في كلا الاتجاهين دون قائمة وصول. يمكن التحكم في حركة مرور ARP بواسطة فحص ARP. بالنسبة لحركة مرور الطبقة 3 التي تنتقل من واجهة منخفضة إلى واجهة عالية الأمان، يلزم وجود قائمة وصول موسعة.

ملاحظة: لا يمر جهاز أمان الوضع الشفاف بحزم بروتوكول أستكشاف Cisco (CDP) أو حزم IPv6، أو أي حزم لا تحتوي على EtherType صالح أكبر من أو يساوي 0x600. على سبيل المثال، لا يمكنك تمرير حزم IS-IS. يتم عمل إستثناء لوحدات بيانات بروتوكول الجسر (BPDUs)، والتي يتم دعمها.

عناوين MAC المسموح بها

هذا غاية {upper}mac address سمحت من خلال الشفاف جدار حماية. يتم إسقاط عناوين MAC غير الموجودة في هذه القائمة:

- عنوان MAC لوجهة البث الحقيقية يساوي FFFF.ffff.ffff
- عناوين MAC ذات البث المتعدد ل IPv4 من 0100.5E00.000 إلى 0100.5EFE.FFFF
- عناوين MAC ذات البث المتعدد ل IPv6 من 3333.000.000 إلى ffff.ffff.3333
- عنوان BPDU للبث المتعدد يساوي 0100.0ccc.cccd
- عناوين MAC ذات البث المتعدد من 0900.0700.000 إلى 0900.07FF.FFFF

لا يسمح لحركة المرور بالمرور في وضع الموجه

في وضع الموجه، لا يمكن لبعض أنواع حركة المرور المرور المرور من خلال جهاز الأمان حتى إذا سمحت بها في قائمة الوصول. ومع ذلك، يمكن أن يسمح جدار الحماية الشفاف بأي حركة مرور تقريبا من خلال إستخدام قائمة الوصول الموسعة (لحركة مرور IP) أو قائمة الوصول EtherType (لحركة المرور غير الخاصة ب IP).

على سبيل المثال، يمكنك إنشاء عمليات تجاور بروتوكول التوجيه من خلال جدار حماية شفاف. يمكنك السماح بفتح أقصر مسار أولا (OSPF) أو بروتوكول معلومات التوجيه (RIP) أو حركة مرور بروتوكول توجيه العبارة الداخلي المحسن (EIGRP) أو بروتوكول العبارة الحدودية (BGP) من خلال الاعتماد على قائمة الوصول الموسعة. وبالمثل، يمكن لبروتوكولات مثل بروتوكول الموجه الاحتياطي الفعال (HSRP) أو بروتوكول تكرار الموجه الظاهري (VRRP) المرور عبر جهاز الأمان.

يمكن تكوين حركة مرور غير خاصة ب IP (على سبيل المثال، AppleTalk و IPX و BPDUs و MPLS) للمرور باستخدام قائمة الوصول من EtherType.

بالنسبة للميزات التي لا يتم دعمها مباشرة على جدار الحماية الشفاف، يمكنك السماح لحركة مرور البيانات بالمرور حتى تدعم موجهات الخادم والنزل الوظيفة. على سبيل المثال، باستخدام قائمة الوصول الموسعة، يمكنك السماح بحركة مرور بروتوكول التكوين الديناميكي للمضيف (DHCP) (بدلا من ميزة ترحيل DHCP غير المدعومة) أو حركة مرور

البث المتعدد مثل التي تم إنشاؤها بواسطة IP/TV.

أستكشاف أخطاء الاتصال وإصلاحها

إذا تعذر على مستخدمي الإنترنت الوصول إلى موقعك على الويب، أكمل الخطوات التالية:

1. تأكد من إدخال عناوين التكوين بشكل صحيح:عنوان خارجي صالحتصحيح العنوان الداخليقام DNS الخارجي بترجمة العنوان
2. تحقق من الواجهة الخارجية بحثا عن أخطاء.تم تكوين جهاز الأمان من Cisco مسبقا للكشف التلقائي عن السرعة وإعدادات الإرسال ثنائي الإتجاه على الواجهة. ومع ذلك، توجد العديد من الحالات التي يمكن أن تتسبب في فشل عملية التفاوض التلقائي. وهذا يؤدي إلى عدم تطابق السرعة أو الإرسال ثنائي الإتجاه (ومشكلات الأداء). بالنسبة للبنية الأساسية للشبكة الحيوية للمهام، تعمل Cisco يدويا على ترميز السرعة ووضع الإرسال ثنائي الإتجاه على كل واجهة حتى لا تكون هناك فرصة للخطأ. لا تتحرك هذه الأجهزة بشكل عام. لذلك، إذا قمت بتكوينها بشكل صحيح، فلن تحتاج إلى تغييرها.**مثال:**

```
asa(config)#interface ethernet 0/0
asa(config-if)#duplex full
asa(config-if)#speed 100
asa(config-if)#exit
```

في بعض الحالات، يؤدي الترميز الثابت للسرعة وإعدادات الإرسال ثنائي الإتجاه إلى إنشاء أخطاء. لذلك، يلزمك تكوين الواجهة إلى الإعداد الافتراضي لوضع الكشف التلقائي كما يوضح هذا المثال:**مثال:**

```
asa(config)#interface ethernet 0/0
asa(config-if)#duplex auto
asa(config-if)#speed auto
asa(config-if)#exit
```

3. إذا لم ترسل حركة المرور أو تستلم من خلال واجهة ASA أو موجه وحدة الاستقبال والبث، فحاول مسح إحصائيات ARP.

```
asa#clear arp
```

4. أستخدم الأوامر **show run object** و**show run static** للتأكد من تمكين الترجمة الثابتة.**مثال:**

```
object service www
service tcp source eq www
object network 192.168.202.2
host 192.168.202.2
object network 10.2.1.5
host 10.2.1.5
object service 1025
service tcp source eq 1025
nat (inside,outside) source static 10.2.1.5 192.168.202.2 service 1025 www
```

في هذا السيناريو، يتم إستخدام عنوان IP الخارجي كعنوان IP معين لخادم الويب.

```
nat (inside,outside) source dynamic 10.2.1.5 interface service 1025 www
```

5. تحقق لمعرفة أن المسار الافتراضي على خادم الويب يشير إلى الواجهة الداخلية ل ASA.
6. تحقق من جدول الترجمة باستخدام الأمر show xlate لمعرفة ما إذا تم إنشاء الترجمة.
7. أستخدم الأمر logging buffered للتحقق من ملفات السجل لمعرفة ما إذا كان الرفض يحدث. (ابحث عن العنوان المترجم وانظر ما إذا كنت ترى أي رفض.)
8. أستخدم الأمر capture:

```
access-list webtraffic permit tcp any host 192.168.202.5

capture capture1 access-list webtraffic interface outside
```

ملاحظة: يقوم هذا الأمر بإنشاء كمية كبيرة من الإخراج. وقد تتسبب في تعليق الموجه أو إعادة تحميله تحت أحمال حركة المرور الثقيلة.

9. إذا كانت الحزم تقوم بذلك إلى ASA، فتأكد من صحة المسار إلى خادم الويب من ASA. (تحقق من أوامر المسار في تكوين ASA الخاص بك.)
10. تحقق لمعرفة ما إذا كان ARP للوكيل معطلا. قم بإصدار الأمر show running-config sysopt في ASA 8.3.هنا، أعجزت ARP للوكيل ب **sysopt noproxy** أمر **خارجي**:

```
ciscoasa#show running-config sysopt
no sysopt connection timewait
sysopt connection tcpmss 1380
sysopt connection tcpmss minimum 0
no sysopt nodnsalias inbound
no sysopt nodnsalias outbound
no sysopt radius ignore-secret
sysopt noproxyarp outside
sysopt connection permit-vpn
```

دخلت in order to reenable ARP وكيل، هذا أمر في شامل تشكيل أسلوب:

```
ciscoasa(config)#no sysopt noproxyarp outside
```

عندما يرسل المضيف حركة مرور IP إلى جهاز آخر على شبكة الإيثرنت نفسها، يحتاج المضيف إلى معرفة عنوان MAC الخاص بالجهاز. ARP هو بروتوكول من الطبقة 2 يعمل على حل عنوان IP إلى عنوان MAC. يرسل المضيف طلب ARP ويسأل "من هو عنوان IP هذا؟ ". الجهاز الذي يملك عنوان الرد، "أنا أمتلك عنوان IP هذا؛ هنا عنوان MAC الخاص بي."يسمح ARP للوكيل لجهاز الأمان بالرد على طلب ARP نيابة عن الأجهزة المضيفة التي وراءه. وهو يقوم بذلك من خلال الرد على طلبات ARP للعناوين الثابتة المعينة لتلك الأجهزة المضيفة. يستجيب جهاز الأمان للطلب باستخدام عنوان MAC الخاص به، ثم يقوم بإعادة توجيه حزم IP إلى المضيف الداخلي المناسب.على سبيل المثال، في الرسم التخطيطي في هذا المستند، عند إجراء طلب ARP لعنوان IP العالمي لخادم الويب، 192.168.202.5، يستجيب جهاز الأمان باستخدام عنوان MAC الخاص به. إذا لم يتم تمكين ARP للوكيل في هذه الحالة، فلن تتمكن الأجهزة المضيفة الموجودة على الشبكة الخارجية لجهاز الأمان من الوصول إلى خادم الويب عن طريق إصدار طلب ARP للعنوان 192.168.202.5. راجع مرجع الأمر للحصول على مزيد من المعلومات حول الأمر sysopt.

11. إذا ظهر كل شيء صحيحا، ولا يزال المستخدمون غير قادرين على الوصول إلى خادم الويب، فافتح حالة باستخدام دعم Cisco الفني.

رسالة خطأ - ASA-4-407001٪:

لا يمكن لعدد قليل من البيئات المضيفة الاتصال بالإنترنت - ASA-4-407001: يتم تلقي رسالة الخطأ interface_name:inside_address في syslog. كيف يتم حل هذا الخطأ؟

يتم تلقي رسالة الخطأ هذه عندما يتجاوز عدد المستخدمين حد المستخدم للترخيص المستخدم. لحل هذا الخطأ، قم بترقية الترخيص إلى عدد أكبر من المستخدمين. يمكن أن يكون هذا الرقم 50 أو 100 أو ترخيص مستخدم غير محدود حسب الطلب.

معلومات ذات صلة

- أجهزة الأمان المعدلة Cisco ASA 5500 Series Adaptive Security Appliances
- الإعلامات الميدانية لمنتج الأمان (بما في ذلك أجهزة الأمان المعدلة (ASA) من Cisco)
- طلبات التعليقات (RFCs)
- 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).