تكوين ASA للشبكات الداخلية المزدوجة

المحتويات

المقدمة

يصف هذا المستند كيفية تكوين جهاز الأمان القابل للتكيف (ASA) من Cisco الذي يشغل الإصدار x.9 من البرنامج لاستخدام شبكتين داخليتين.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

أسست المعلومة في هذا وثيقة على ال cisco ASA أن يركض برمجية صيغة x.9.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة

المُستخدمة 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.

معلومات أساسية

عند إضافة شبكة داخلية ثانية خلف جدار حماية ASA، ضع في الاعتبار هذه المعلومات المهمة:

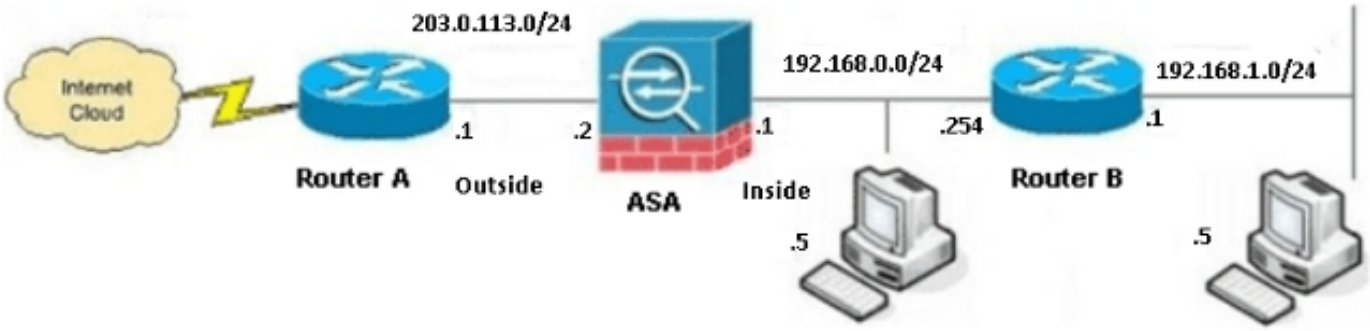
- لا يدعم ASA العنونة الثانوية.
- يجب إستخدام موجه خلف ASA لتحقيق التوجيه بين الشبكة الحالية والشبكة التي تمت إضافتها حديثا.
- يجب أن تشير العبارة الافتراضية لجميع البيئات المضيفة إلى الموجه الداخلي.
- يجب إضافة مسار افتراضي على الموجه الداخلي الذي يشير إلى ASA.
- يجب مسح ذاكرة التخزين المؤقت لبروتوكول تحليل العنوان (ARP) على الموجه الداخلي.

التكوين

أستخدم المعلومات الموضحة في هذا القسم لتكوين ASA.

الرسم التخطيطي للشبكة

هنا المخطط الذي يتم إستخدامه للأمثلة في هذا المستند:



ملاحظة: ال ip ليس يخاطب خطة أن يكون استعملت في هذا تشكيل قانونيا routable على الإنترنت. هم rfc 1918 عنوان أن يكون استعملت في مختبر بيئة.

تكوين ASA 9.x

إن يتلقى أنت الإنتاج من **write terminal ال** أمر من ك cisco أداة، أنت يستطيع استعملت الإنتاج مترجم أداة (يسجل زبون فقط) in order to عرضت ممكن إصدار ونقطة معينة.

هنا التشكيل ل ال ASA أن يركض برمجية صيغة x.9:

```
(ASA Version 9.3(2
!
hostname ASA
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!

.This is the configuration for the outside interface ---!

!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 203.0.113.2 255.255.255.0

.This is the configuration for the inside interface ---!

!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 192.168.0.1 255.255.255.0
!

boot system disk0:/asa932-smp-k8.bin

.This creates an object called OBJ_GENERIC_ALL ---!
Any host IP address that does not already match another configured ---!
object will get PAT to the outside interface IP address ---!
.on the ASA (or 10.1.5.1), for Internet-bound traffic ---!


object network OBJ_GENERIC_ALL
subnet 0.0.0.0 0.0.0.0
nat (inside,outside) dynamic interface
!
route inside 192.168.1.0 255.255.255.0 192.168.0.254 1
route outside 0.0.0.0 0.0.0.0 203.0.113.1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
dynamic-access-policy-record DfltAccessPolicy
http server enable
http 192.168.0.0 255.255.254.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes 4608000
telnet timeout 5
ssh timeout 5
console timeout 0
```

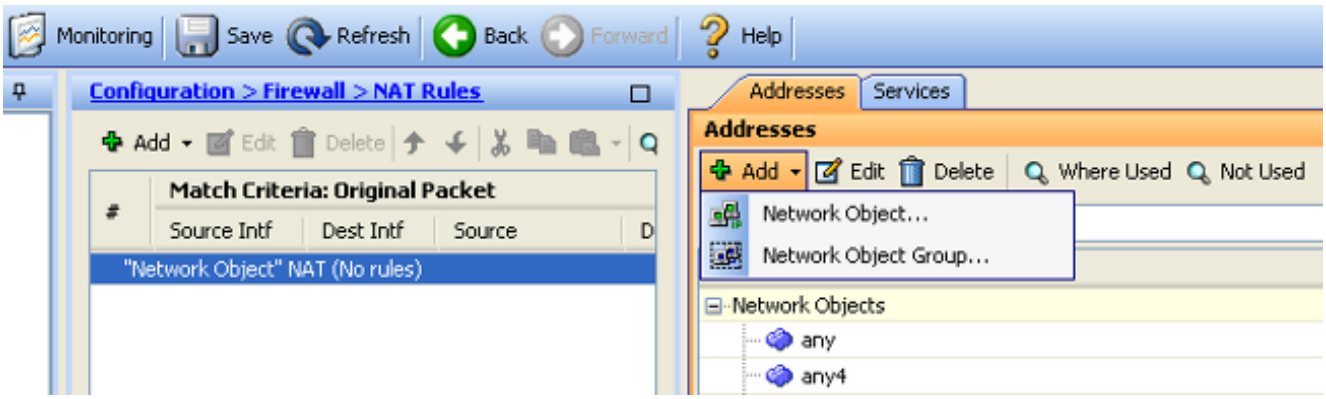
```
                                    threat-detection basic-threat
                                threat-detection statistics access-list
                            no threat-detection statistics tcp-intercept
                                                                    !
                                        class-map inspection_default
                                    match default-inspection-traffic
                                                                    !
                                                                    !
                            policy-map type inspect dns preset_dns_map
                                                                parameters
                                    message-length maximum client auto
                                            message-length maximum 512
                                              policy-map global_policy
                                              class inspection_default
                                            inspect dns preset_dns_map
                                                          inspect ftp
                                                   inspect h323 h225
                                                    inspect h323 ras
                                                         inspect rsh
                                                        inspect rtsp
                                                       inspect esmtp
                                                      inspect sqlnet
                                                      inspect skinny
                                                      inspect sunrpc
                                                       inspect xdmcp
                                                         inspect sip
                                                    inspect netbios
                                                        inspect tftp
                                                  inspect ip-options
                                                                    !
                                        service-policy global_policy global
                                                    prompt hostname context
                                    Cryptochecksum:6fffbd3dc9cb863fd71c71244a0ecc5f
                                                                end :
```

السماح للمضيفين الداخليين بالوصول إلى الشبكات الخارجية باستخدام PAT

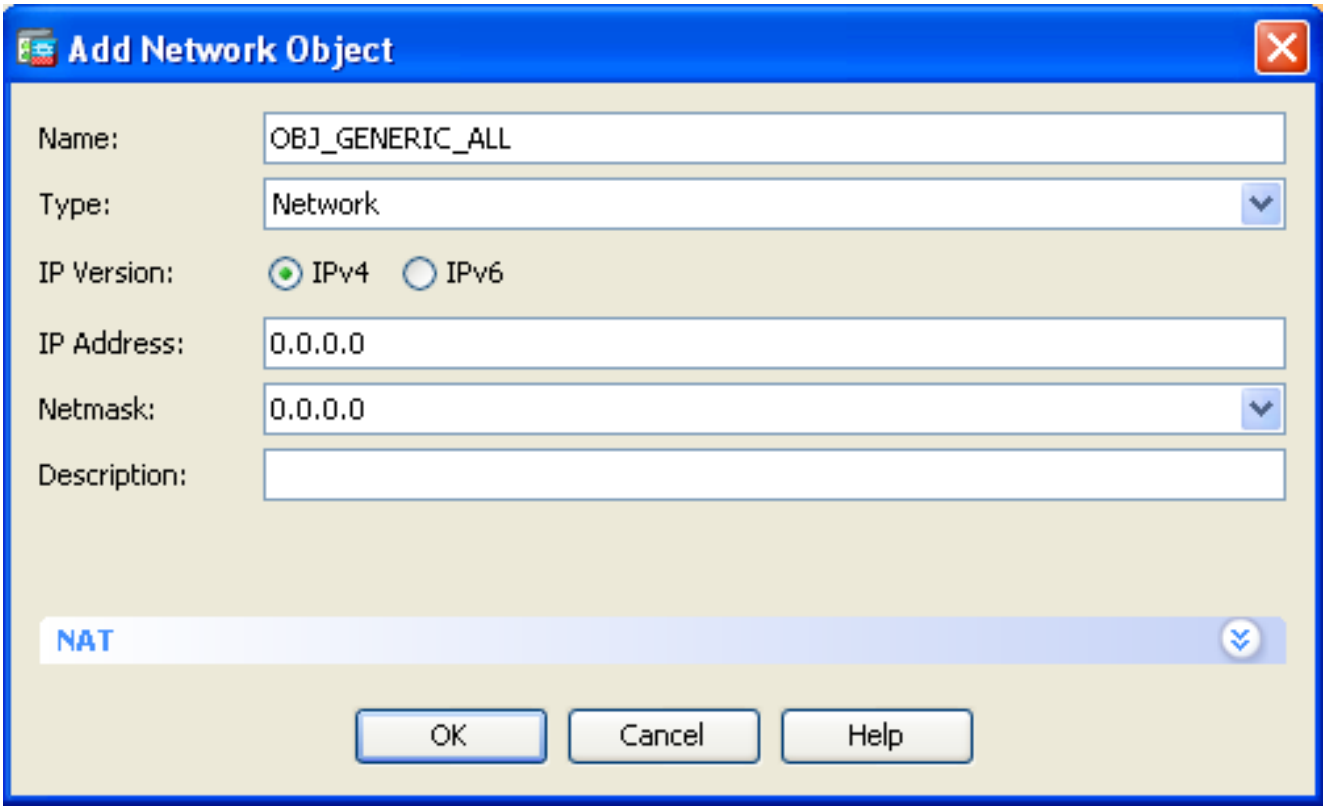
إن ينوي أنت أن يتلقى الداخل مضيف يشارك عنوان عام وحيد للترجمة، استعملت أيسر عنوان ترجمة (ضرب). يتضمن أحد أبسط تكوينات PAT ترجمة جميع البيئات المضيفة الداخلية بحيث تظهر على أنها هي عنوان IP للواجهة الخارجية. هذا ال ضرب تشكيل نموذجي أن يكون استعملت عندما الرقم من مسحاج تخديد عنوان أن يكون يتوفر من ال isp مقصر إلى قليل، أو فقط واحد.

أتمت هذا steps in order to سمحت الداخل مضيف منفذ إلى الشبكة الخارجية مع ضرب:

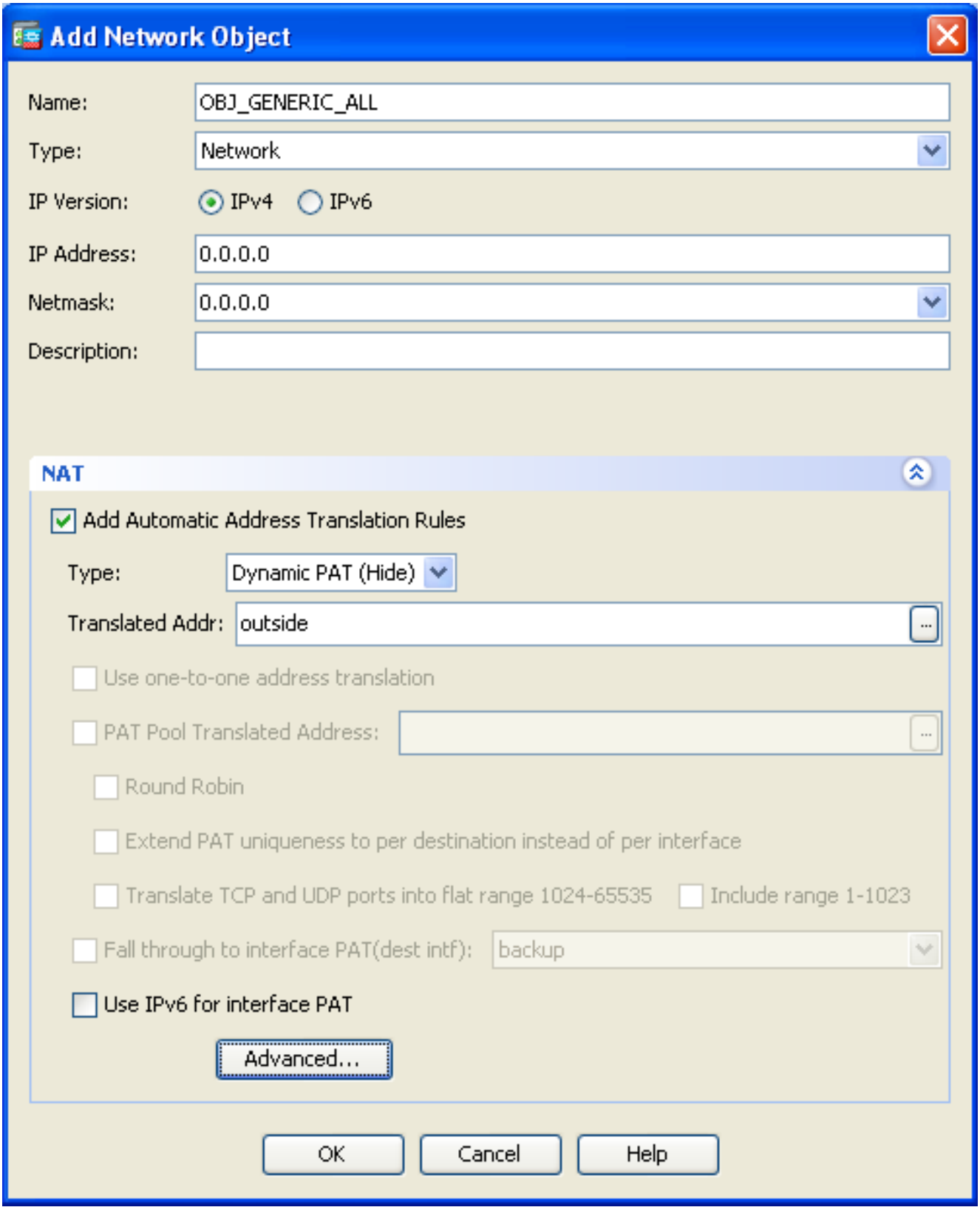
1. انتقل إلى التكوين > **جدار الحماية>قواعد NAT**، ثم انقر فوق **إضافة**، واختر كائن الشبكة لتكوين قاعدة NAT الديناميكية:



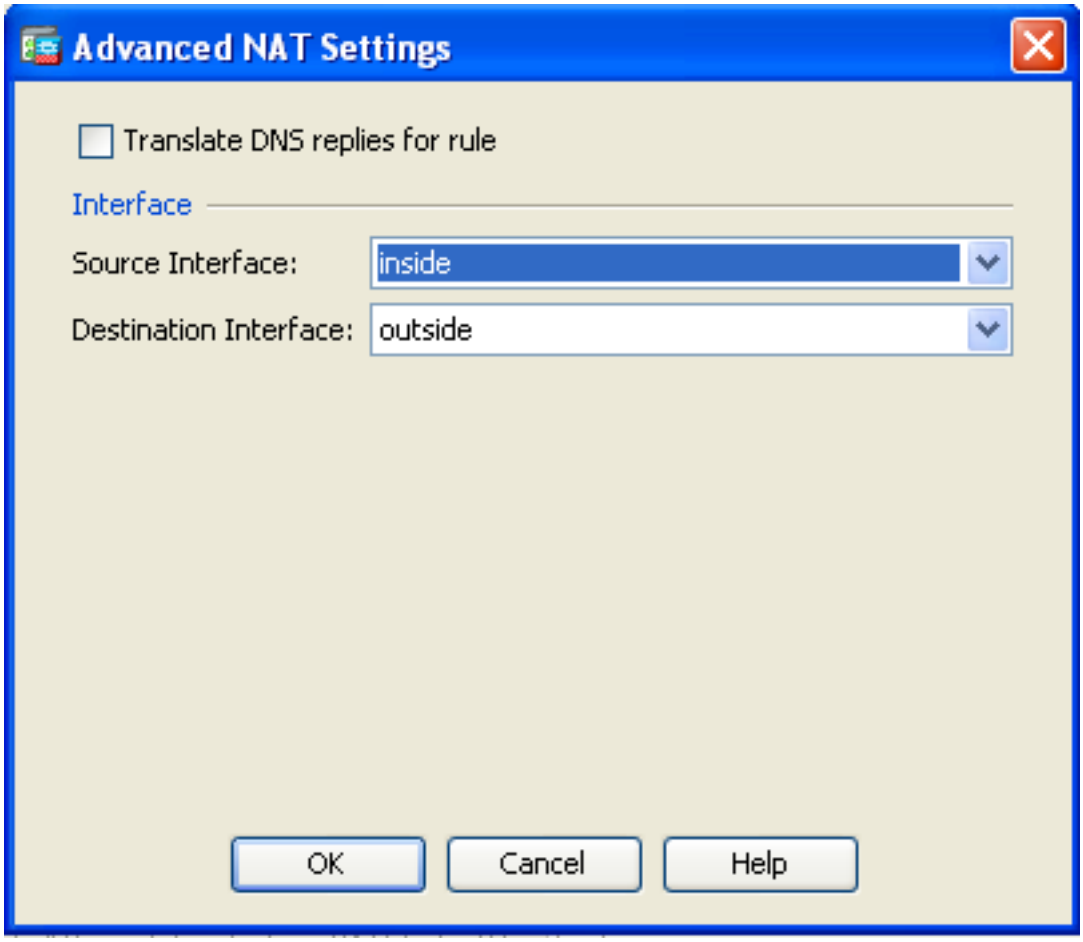
2. قم بتكوين الشبكة/المضيف/النطاق الذي يلزم وجود PAT الديناميكي له. في هذا المثال، تم تحديد جميع الشبكات الفرعية الداخلية. يجب تكرار هذه العملية للشبكات الفرعية المحددة التي ترغب في ترجمتها بهذه الطريقة:



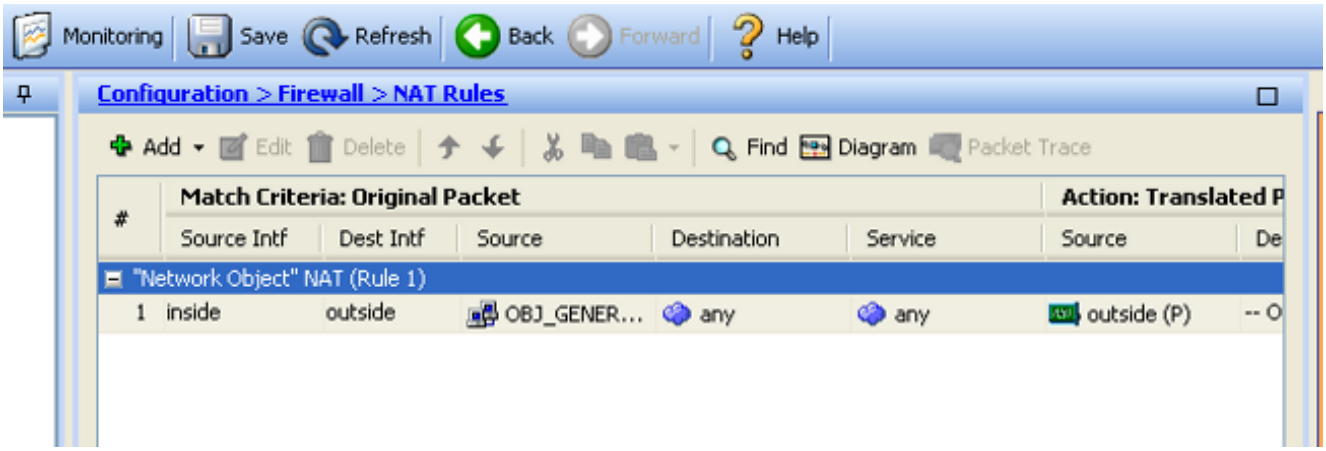
3. طقطقت **nat**، فحصت ال **يضيف آلي عنوان قاعدة** تدقيق، دخلت حركي، **وعينت ال** يترجم عنوان **خيار لذلك هو يعكس القارن خارجي.** إذا قمت بنقر زر البيضاوي، فإنه يساعدك في إختيار كائن تم تكوينه مسبقا، مثل الواجهة الخارجية:



4. طقطقة **متقدم** in order to حددت مصدر وغاية قارن:



5. انقر فوق **موافق**، ثم انقر فوق **تطبيق** لتطبيق التغييرات. وبمجرد اكتماله، يعرض مدير أجهزة الأمان المعدلة (ASDM) قاعدة NAT:



تكوين الموجه B

هنا تكوين الموجه B:

```
...Building configuration

:Current configuration
!
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
```

```
!
hostname Router B
!
!
username cisco password 0 cisco
!
!
!
!
ip subnet-zero
ip domain-name cisco.com
!
isdn voice-call-failure 0
!

!
interface Ethernet0/0
ip address 192.168.1.1 255.255.255.0
no ip directed-broadcast
!
interface Ethernet0/1

!This assigns an IP address to the ASA-facing Ethernet interface ---.

ip address 192.168.0.254 255.255.255.0
no ip directed-broadcast

ip classless

!This route instructs the inside router to forward all of the ---
.non-local packets to the ASA ---!

ip route 0.0.0.0 0.0.0.0 192.168.0.1
no ip http server
!
!
line con 0
exec-timeout 0 0
length 0
transport input none
line aux 0
line vty 0 4
password ww
login
!
end
```

التحقق من الصحة

قم بالوصول إلى موقع ويب عبر HTTP من خلال مستعرض ويب للتحقق من أن التكوين لديك يعمل بشكل صحيح.

يستخدم هذا المثال موقعا يتم إستضافته في عنوان IP *198.51.100.100*. إذا نجح الاتصال، يمكن رؤية المخرجات التي يتم توفيرها في الأقسام التالية على واجهة سطر الأوامر (CLI) الخاصة بوحدة ASA.

الاتصال

أدخل الأمر **show connection address** للتحقق من الاتصال:

```
ASA(config)# show connection address 172.16.11.5
in use, 98 most used 6
,TCP outside 198.51.100.100:80 inside 192.168.1.5:58799, idle 0:00:06, bytes 937
flags UIO
```

ASA هو جدار حماية ذو حالة، ويتم السماح بحركة المرور العائدة من خادم الويب مرة أخرى من خلال جدار الحماية لأنه يطابق ***اتصالا*** في جدول اتصال جدار الحماية. يتم السماح بحركة المرور التي تطابق اتصال موجود مسبقا من خلال جدار الحماية دون منعها بواسطة قائمة التحكم في الوصول إلى الواجهة (ACL).

في الإخراج السابق، قام العميل الموجود على الواجهة الداخلية بإنشاء اتصال بالمضيف 198.51.100.100 الموجود خارج الواجهة. يتم إجراء هذا الاتصال باستخدام بروتوكول TCP وقد كان خاملا لمدة ست ثوان. تشير علامات الاتصال إلى الحالة الحالية لهذا الاتصال.

ملاحظة: راجع مستند Cisco علامات اتصال ASA TCP (تجميع الاتصال وإنهاؤه) للحصول على مزيد من المعلومات حول علامات الاتصال.

استكشاف الأخطاء وإصلاحها

استعملت المعلومة أن يكون وصفت في هذا قسم in order to تحريت تشكيل إصدار.

Syslogs

دخلت **العرض سجل** أمر in order to شاهدت ال syslogs:

```
ASA(config)# show log | in 192.168.1.5

:Apr 27 2014 11:31:23: %ASA-6-305011: Built dynamic TCP translation from inside
to outside:203.0.113.2/58799 192.168.1.5/58799

:Apr 27 2014 11:31:23: %ASA-6-302013: Built outbound TCP connection 2921 for outside
(to inside:192.168.1.5/58799 (203.0.113.2/58799 (198.51.100.100/80) 198.51.100.100/80
```

يقوم جدار حماية ASA بإنشاء syslog أثناء التشغيل العادي. نطاق syslogs في النطاق الترددي استنادا إلى تكوين التسجيل. يبدي الإنتاج إثنان syslog أن يكون رأيت في مستوى ستة، أو *المعلوماتية* مستوى.

في هذا مثال، هناك إثنان syslog ولدت. الأولى هي رسالة سجل تشير إلى أن جدار الحماية قام بإنشاء ترجمة، وعلى وجه التحديد، ترجمة TCP ديناميكية (PAT). هو يشير المصدر عنوان ومنفذ، as well as ال يترجم عنوان ومنفذ، بما أن الحركة مرور يعبر من الداخل إلى الواجهات الخارجية.

ويشير syslog الثاني إلى أن جدار الحماية قام بإنشاء اتصال في جدول الاتصال الخاص به لحركة المرور المحددة هذه بين العميل والخادم. إذا تم تكوين جدار الحماية لحظر محاولة الاتصال هذه، أو قام عامل آخر بمنع إنشاء هذا الاتصال (قيود الموارد أو احتمال حدوث خطأ في التكوين)، فلن يقوم جدار الحماية بإنشاء سجل للإشارة إلى إنشاء الاتصال. وبدلا من ذلك، فإنه يسجل سببا لرفض الاتصال أو إشارة فيما يتعلق بالعامل الذي منع إنشاء الاتصال.

حزم التتبع

دخلت هذا أمر in order to مكنت الربط tracer وظيفة:

```
ASA(config)# packet-tracer input inside tcp 192.168.1.5 1234 198.51.100.100 80

--Omitted--

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: allow
```

تسمح لك وظيفة تعقب الحزمة على ASA بتحديد حزمة *محاكية* وعرض جميع الخطوات والفحوصات والوظائف المختلفة التي يكملها جدار الحماية عندما يعالج حركة مرور البيانات. باستخدام هذه الأداة، من المفيد أن تقوم بتحديد مثال لحركة المرور التي تعتقد *أنه* يجب السماح لها بالمرور من خلال جدار الحماية، واستخدام تلك الحزمة 5 لمحاكاة حركة المرور. في المثال السابق، يتم إستخدام تعقب الحزمة لمحاكاة محاولة اتصال تطابق هذه المعايير:

- تصل الحزمة المحاكاة إلى الواجهة الداخلية.
- البروتوكول الذي يتم إستخدامه هو TCP.
- عنوان IP الخاص بالعميل المحاكي هو 192.168.1.5.
- يرسل العميل حركة مرور يكون مصدرها من المنفذ 1234.
- يتم توجيه حركة المرور إلى خادم على عنوان IP 198.51.100.100.
- حركة المرور موجهة إلى منفذ 80.

لاحظ أنه لم يتم ذكر الواجهة الخارجية في الأمر. هذا إلى ربط متتبع تصميم. تخبرك الأداة كيفية معالجة جدار الحماية لهذا النوع من محاولات الاتصال، والتي تتضمن كيفية توجيهها، ومن أي واجهة.

تلميح: للحصول على مزيد من المعلومات حول وظيفة تعقب الحزمة، ارجع إلى قسم التتبع للحزم tracer في دليل تكوين *سلسلة Cisco ASA 5500 باستخدام CLI، 8.4 و 8.6*.

أسر

دخلت هذا أمر in order to طبقت التقاط:

```
ASA# capture capin interface inside match tcp host 192.168.1.5 host 198.51.100.100
ASA# capture capout interface outside match tcp any host 198.51.100.100

ASA#show capture capin

packets captured 3

1: 11:31:23.432655 192.168.1.5.58799 > 198.51.100.100.80 :S 780523448
(0)780523448 <mss 1460,nop,wscale 2,nop,nop,sackOK> win 8192
2: 11:31:23.712518 198.51.100.100.80 > 192.168.1.5.58799 :S 2123396067
(0)2123396067 <mss 1024,nop,nop,sackOK,nop,wscale 8> win 8192
3: 11:31:23.712884 192.168.1.5.58799 > 198.51.100.100.80 . :
ack 2123396068 win 32768
```

```
ASA#show capture capout

packets captured 3

:S 1633080465 :198.51.100.100.80 < 203.0.113.2.58799 11:31:23.432869 :1
        <win 8192 <mss 1380,nop,wscale 2,nop,nop,sackOK (0)1633080465
:S 95714629 :203.0.113.2.58799 < 198.51.100.100.80 11:31:23.712472 :2
<ack 1633080466 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8 (0)95714629
ack 95714630 . :198.51.100.100.80 < 203.0.113.2.58799 11:31:23.712914 :3
<win 32768/pre
```

يمكن أن يلتقط جدار حماية ASA حركة مرور البيانات التي تدخل الواجهات أو تتركها. وظيفة الالتقاط هذه رائعة لأنها يمكن أن تثبت بشكل قاطع ما إذا كانت حركة المرور تصل إلى جدار الحماية أو تغادر منه. يوضح المثال السابق تكوين إلتقطين يسميان **Capin** و**capout** على الواجهات الداخلية والخارجية، على التوالي. تستخدم أوامر **الالتقاط** الكلمة الأساسية **match**، والتي تتيح لك تحديد حركة مرور البيانات التي تريد التقاطها.

بالنسبة لمثال التقاط *الكابين*، يشار إلى أنك تريد مطابقة حركة مرور البيانات التي يتم رؤيتها على الواجهة الداخلية (مدخل أو مخرج) التي تطابق *مضيف 192.168.1.5 TCP المضيف 198.51.100.100*. بمعنى آخر، أنت تريد التقاط أي حركة مرور TCP التي يتم إرسالها من المضيف *192.168.1.5* إلى المضيف *198.51.100.100*، أو العكس. يسمح إستخدام الكلمة الأساسية **مطابقة** جدار الحماية بالتقاط حركة المرور تلك بشكل ثنائي الإتجاه. لا يشير أمر **capture** الذي تم تعريفه للواجهة الخارجية إلى عنوان IP العميل الداخلي لأن جدار الحماية يجري PAT على عنوان IP ذلك العميل. ونتيجة لذلك، لا يمكنك المطابقة مع عنوان IP هذا العميل. بدلا من ذلك، يستخدم هذا المثال **أي** للإشارة إلى أن جميع عناوين IP المحتملة ستطابق هذا الشرط.

بعد تكوين عمليات الالتقاط، يمكنك بعد ذلك محاولة إنشاء اتصال مرة أخرى والمتابعة لعرض عمليات الالتقاط باستخدام الأمر **show capture<*capture_name*>** . في هذا المثال، يمكنك أن ترى أن العميل قادر على الاتصال بالخادم، كما هو موضح من خلال مصافحة TCP ثلاثية الإتجاه التي تظهر في عمليات الالتقاط.

معلومات ذات صلة

- مدير أجهزة حلول الأمان المعدلة من Cisco
- جدران الحماية من الجيل التالي من Cisco ASA 5500-X Series
- طلبات التعليقات (RFC)
- دليل تكوين واجهة سطر الأوامر من السلسلة Cisco ASA Series، الإصدار 9.0a تكوين المسارات الثابتة والافتراضية
- الدعم التقني والمستندات أ.أأ سيسكو سيستمز

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).