ASA 8.3(x) PAT حركي مع شبكتين داخليتين ومثال تكوين الإنترنت

المحتويات

المقدمة

يزود هذا وثيقة عينة تشكيل ل ضرب حركي على cisco تعديل أمن أداة (ASA) أن يركض برمجية صيغة 8.3(1). يترجم ضرب حركي عنوان حقيقي يتعدد إلى واحد يخطط عنوان ب يترجم المصدر الحقيقي عنوان ومنفذ مصدر إلى ال يخطط عنوان ومنفذ فريد يخطط. يتطلب كل اتصال جلسة ترجمة منفصلة لأن منفذ المصدر يختلف لكل اتصال.

المتطلبات الأساسية

المتطلبات

تأكد من استيفاء المتطلبات التالية قبل أن تحاول إجراء هذا التكوين:

- تأكد من أن الشبكة الداخلية بها شبكتين موجودتين في داخل ASA:192.168.0.0/24—الشبكة المتصلة مباشرة بالمحول ASA.192.168.1.0/24—الشبكة الموجودة داخل ASA، ولكن خلف جهاز آخر (على سبيل المثال، موجه).
- تأكد من أن المستخدمين الداخليين يحصلون على ضرب كما يلي:تحصل الأجهزة المضيفة الموجودة على الشبكة الفرعية 24/192.168.1.0 على PAT إلى عنوان IP الاحتياطي الذي يقدمه 10.1.5.5) ISP).أي مضيف آخر خلف الداخلي من ال ASA سيجلب ضرب إلى القارن خارجي عنوان من ال 10.1.5.1) ASA).

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- أجهزة الأمان المعدلة (Cisco Adaptive Security Appliance (ASA مع الإصدار 8.3(1)
- ASDM الإصدار 6.3(1)

ملاحظة: ارجع إلى السماح بوصول HTTPS إلى ASDM للسماح بتكوين ASA بواسطة ASDM.

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.

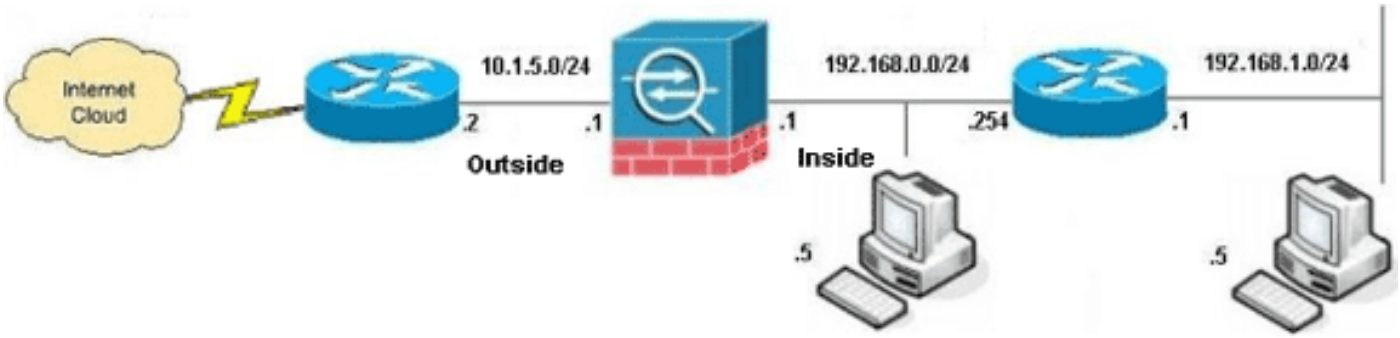
الاصطلاحات

أحلت ال cisco فني طرف إتفاق لمعلومة على وثيقة إتفاق.

التكوين

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



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

- تكوين ASA CLI
- تكوين ASDM

تكوين ASA CLI

يستخدم هذا المستند التكوينات الموضحة أدناه.

تكوين ASA الديناميكي PAT
ASA#**configure terminal** Enter configuration commands, one per line. End with .CNTL/Z *Creates an object called OBJ_GENERIC_ALL. !--- Any ---! host IP not already matching another configured !--- object will get PAT to the outside interface IP !--- on the ASA (or 10.1.5.1), for internet bound traffic.* ASA(config)#**object network OBJ_GENERIC_ALL** ASA(config-obj)#**subnet 0.0.0.0 0.0.0.0**

```
ASA(config-obj)#exit
ASA(config)#nat (inside,outside) source dynamic
OBJ_GENERIC_ALL interface

The above statements are the equivalent of the !--- ---!
nat/global combination (as shown below) in v7.0(x), !---
v7.1(x), v7.2(x), v8.0(x), v8.1(x) and v8.2(x) ASA code:
nat (inside) 1 0.0.0.0 0.0.0.0
global (outside) 1 interface


Creates an object called OBJ_SPECIFIC_192-168-1-0. ---!
!--- Any host IP facing the the 'inside' interface of
the ASA !--- with an address in the 192.168.1.0/24
subnet will get PAT !--- to the 10.1.5.5 address, for
internet bound traffic. ASA(config)#object network
OBJ_SPECIFIC_192-168-1-0
ASA(config-obj)#subnet 192.168.1.0 255.255.255.0
ASA(config-obj)#exit
ASA(config)#nat (inside,outside) source dynamic
OBJ_SPECIFIC_192-168-1-0 10.1.5.5

The above statements are the equivalent of the ---!
nat/global !--- combination (as shown below) in v7.0(x),
v7.1(x), v7.2(x), v8.0(x), !--- v8.1(x) and v8.2(x) ASA
code: nat (inside) 2 192.168.1.0 255.255.255.0
global (outside) 2 10.1.5.5
```

ASA 8.3(1) جار التكوين

```
ASA#show run
Saved :
:
(ASA Version 8.3(1
!
hostname ASA
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
Configure the outside interface. ! interface ---!
GigabitEthernet0/0 nameif outside security-level 0 ip
address 10.1.5.1 255.255.255.0 !--- Configure the inside
interface. ! interface GigabitEthernet0/1 nameif inside
security-level 100 ip address 192.168.0.1 255.255.255.0
! interface GigabitEthernet0/2 shutdown no nameif no
security-level no ip address ! interface
GigabitEthernet0/3 shutdown no nameif no security-level
no ip address ! interface Management0/0 shutdown no
nameif no security-level no ip address management-only !
boot system disk0:/asa831-k8.bin ftp mode passive object
network OBJ_SPECIFIC_192-168-1-0
subnet 192.168.1.0 255.255.255.0
object network OBJ_GENERIC_ALL
subnet 0.0.0.0 0.0.0.0

pager lines 24
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-631.bin
no asdm history enable
arp timeout 14400
```

```
     nat (inside,outside) source dynamic OBJ_GENERIC_ALL
                                                interface
   nat (inside,outside) source dynamic OBJ_SPECIFIC_192-
                                        168-1-0 10.1.5.5

  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 10.1.5.2
                                     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 :
```

تكوين ASDM

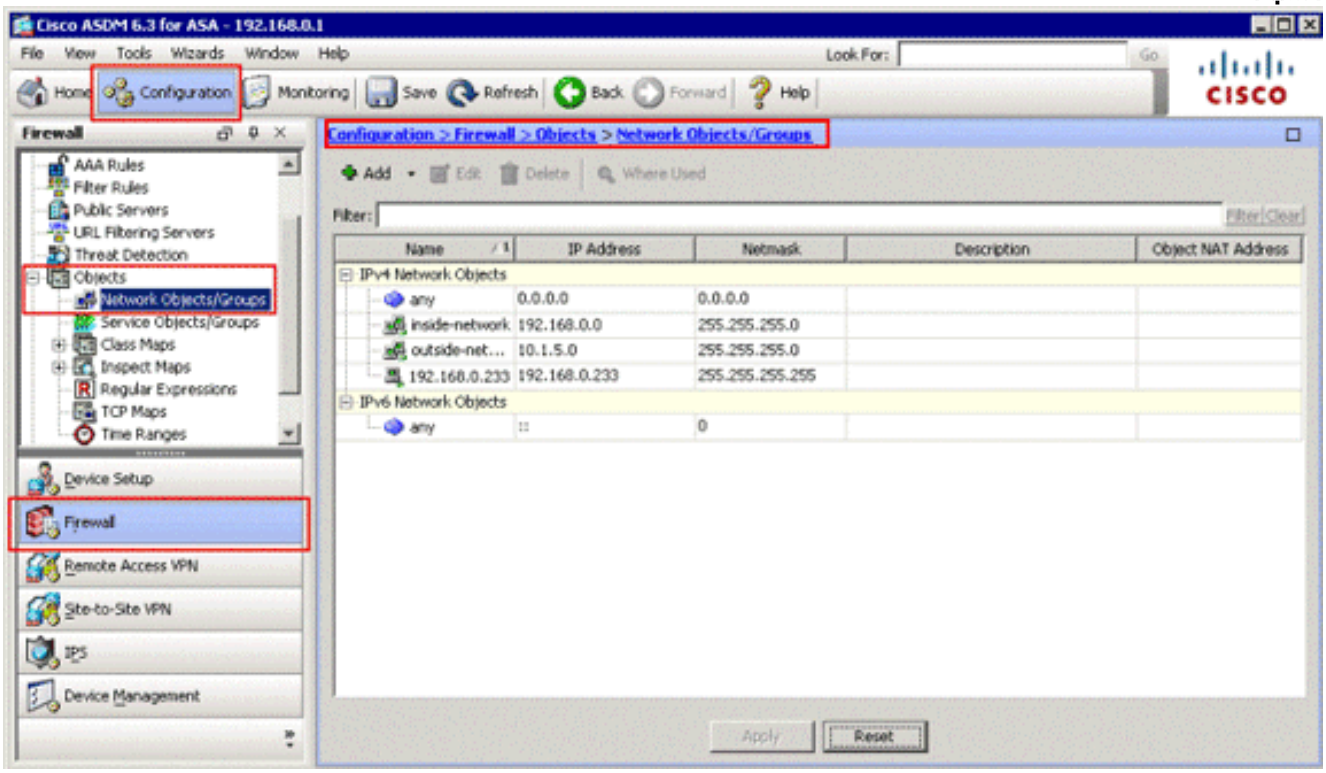
لإكمال هذا التكوين من خلال واجهة ASDM، يجب عليك:

1. إضافة ثلاثة كائنات على الشبكة؛ تضيف هذه الأمثلة كائنات الشبكة التالية:OBJ_GENERIC_ALLOBJ_SPECIFIC_192-168-1-010.1.5.5
2. خلقت إثنان nat/ضرب قاعدة؛ هذا مثال يخلق nat قاعدة ل هذا شبكة كائن:OBJ_GENERIC_ALLOBJ_SPECIFIC_192-168-1-0

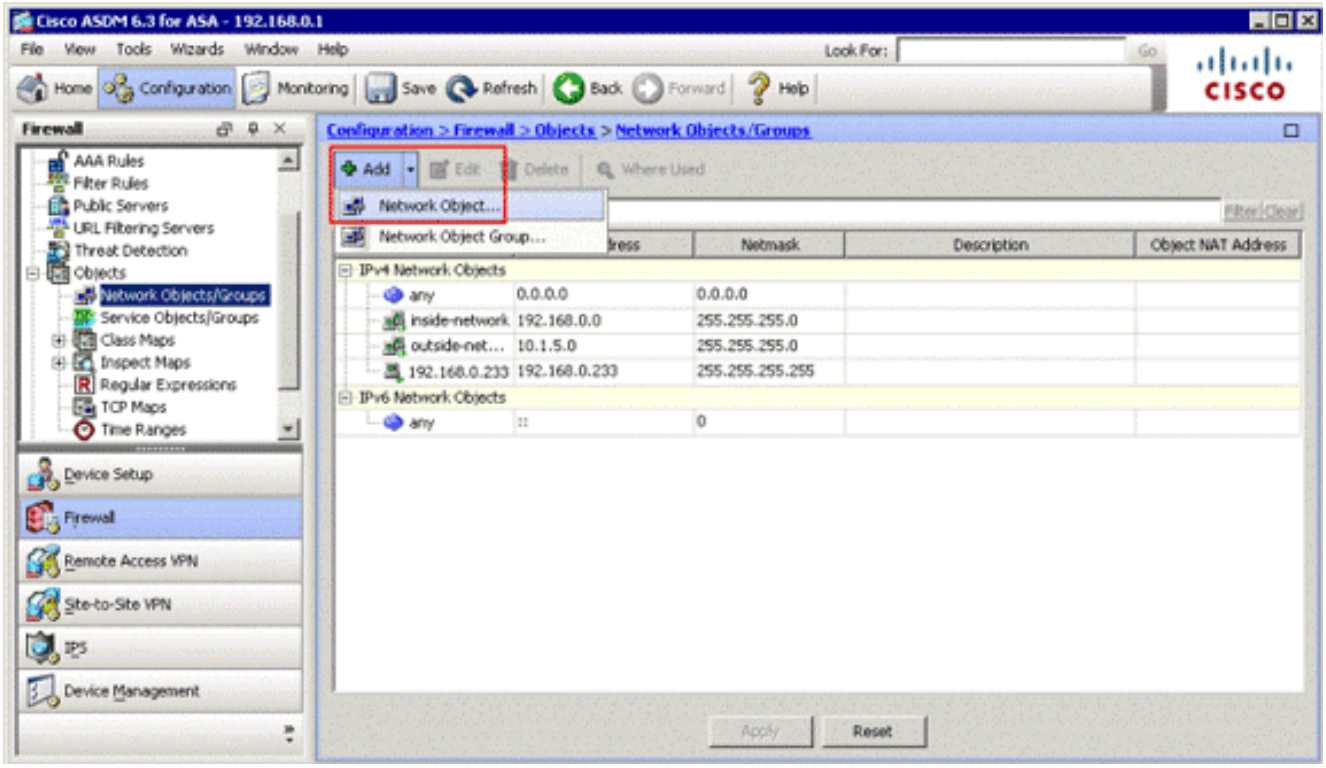
إضافة كائنات شبكة

أتمت هذا steps in order to أضفت شبكة كائن:

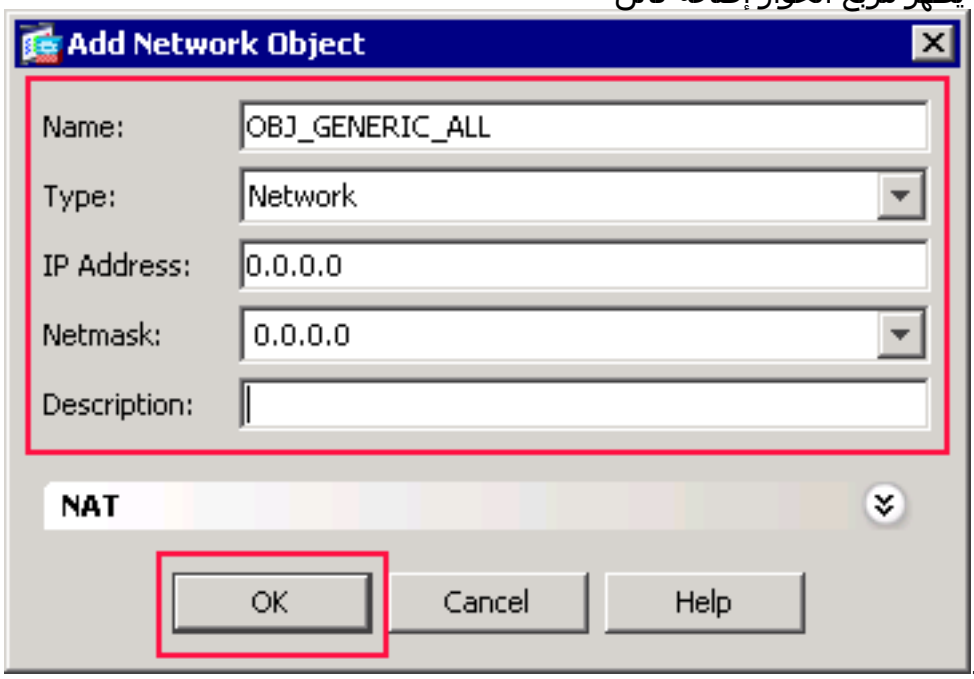
1. قم بتسجيل الدخول إلى ASDM، واختر **التكوين > جدار الحماية > الكائنات > كائنات/مجموعات الشبكة**.



2. أختر **إضافة > كائن الشبكة** لإضافة كائن شبكة.

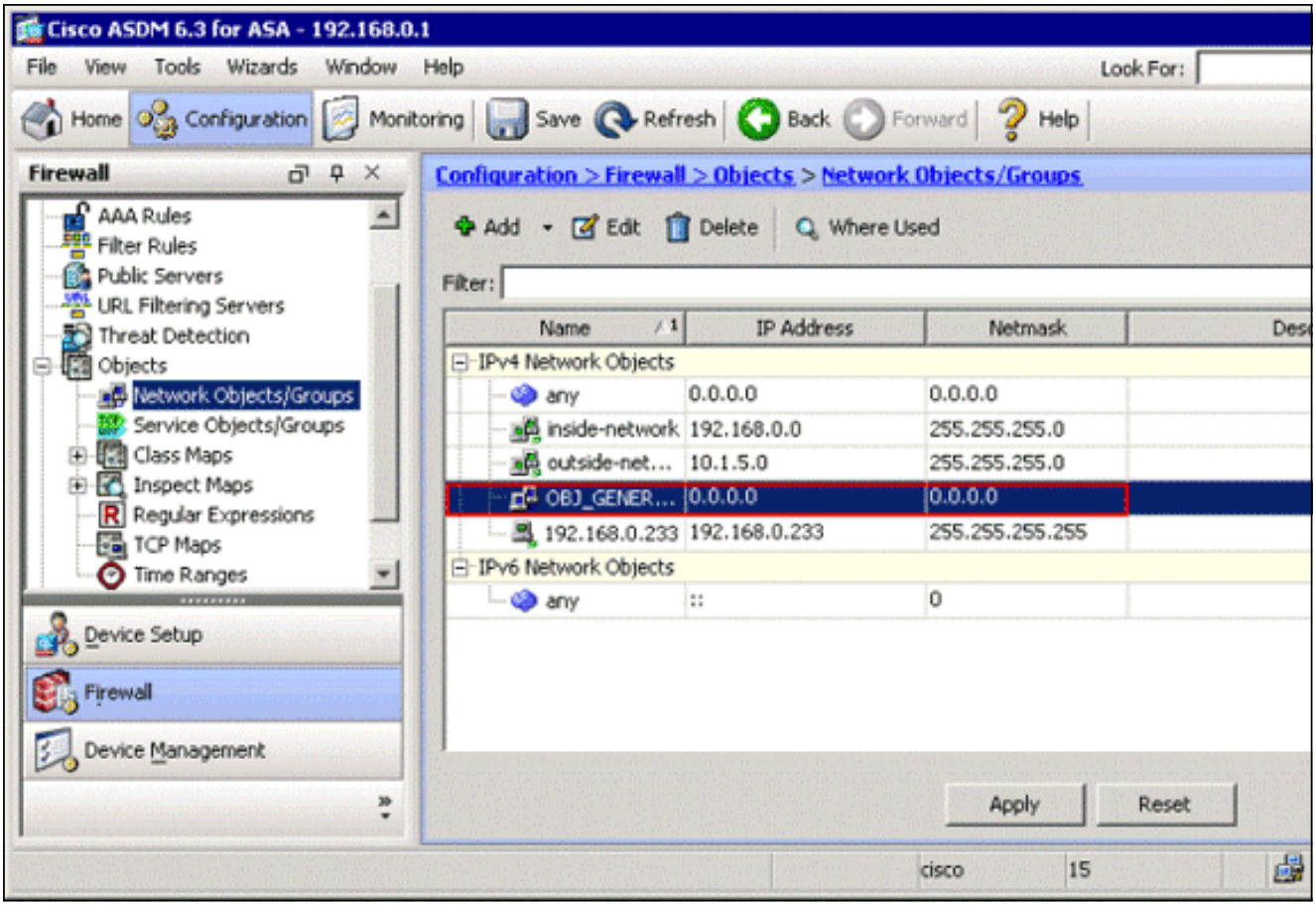


سوف يظهر مربع الحوار إضافة كائن

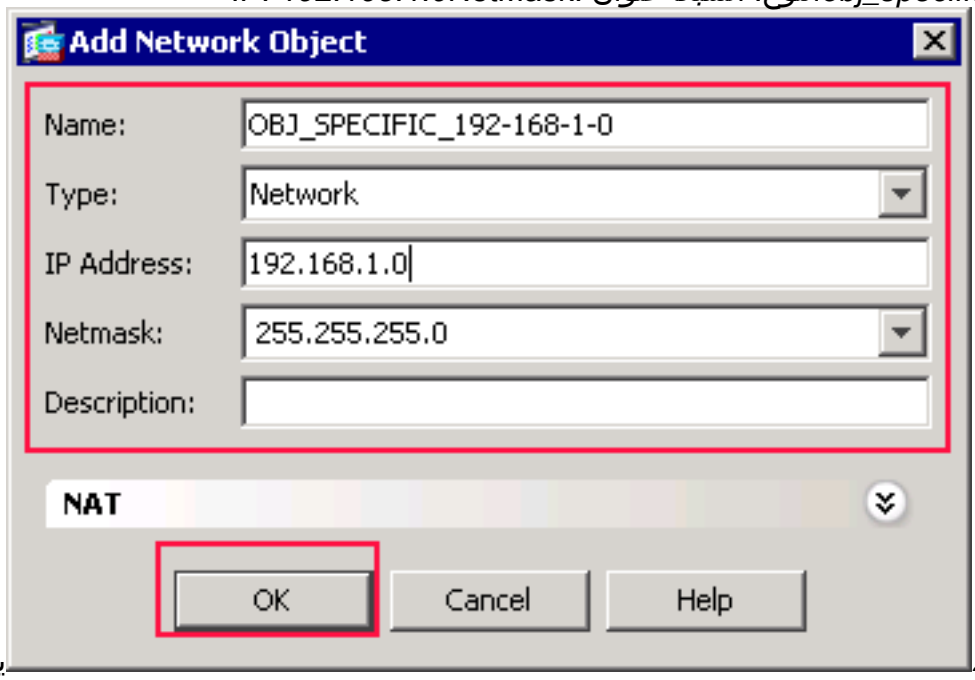


شبكة.

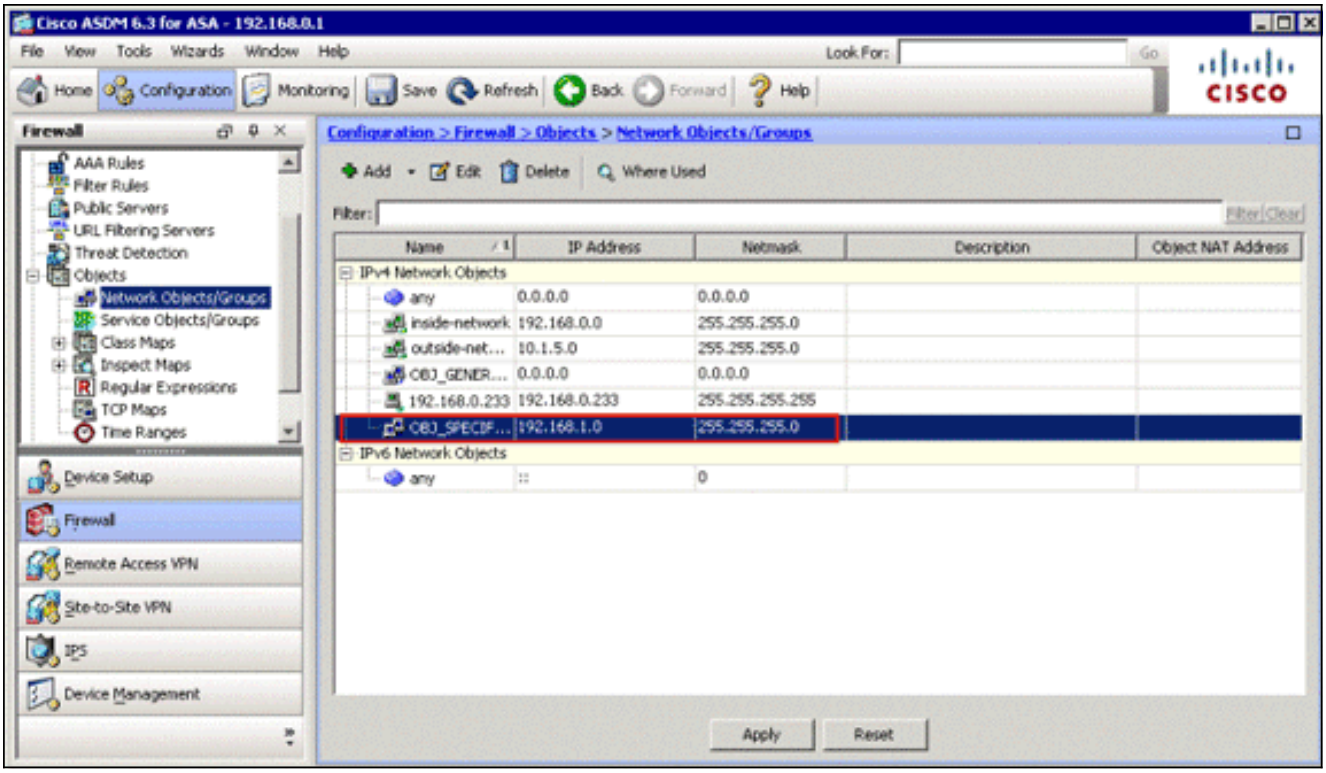
3. أدخل هذه المعلومات في شاشة إضافة كائن شبكة:اسم كائن الشبكة. (يستخدم هذا المثال *OBJ_GENERIC_ALL*.)نوع كائن الشبكة. (يستخدم هذا المثال *الشبكة*.)عنوان IP لكائن الشبكة. (يستخدم هذا المثال *0.0.0.0*.)قناع الشبكة لكائن الشبكة. (يستخدم هذا المثال *0.0.0.0*.)
4. وانقر فوق **OK**.يتم إنشاء كائن الشبكة ويظهر في قائمة كائنات/مجموعات الشبكة، كما هو موضح في هذه الصورة:



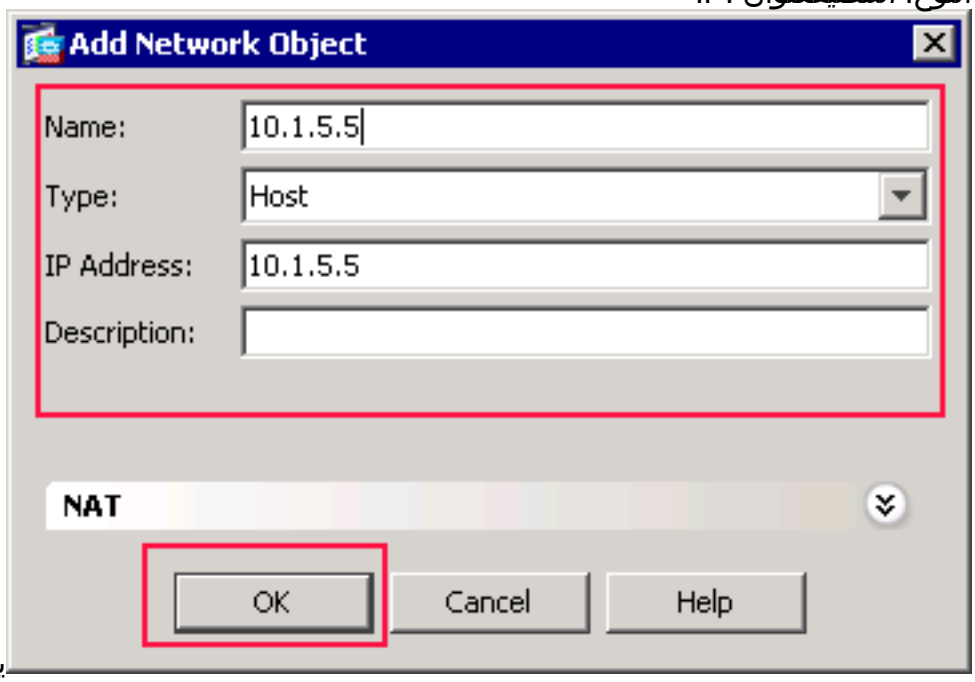
5. كرر الخطوات السابقة لإضافة كائن شبكة ثان، وانقر فوق **موافق**.يستخدم هذا المثال القيم التالية:الاسم: *obj_specific_192-168-1-0*النوع: *الشبكة*عنوان IP: *192.168.1.0*NetMask: *255.255.255.0* يتم إنشاء



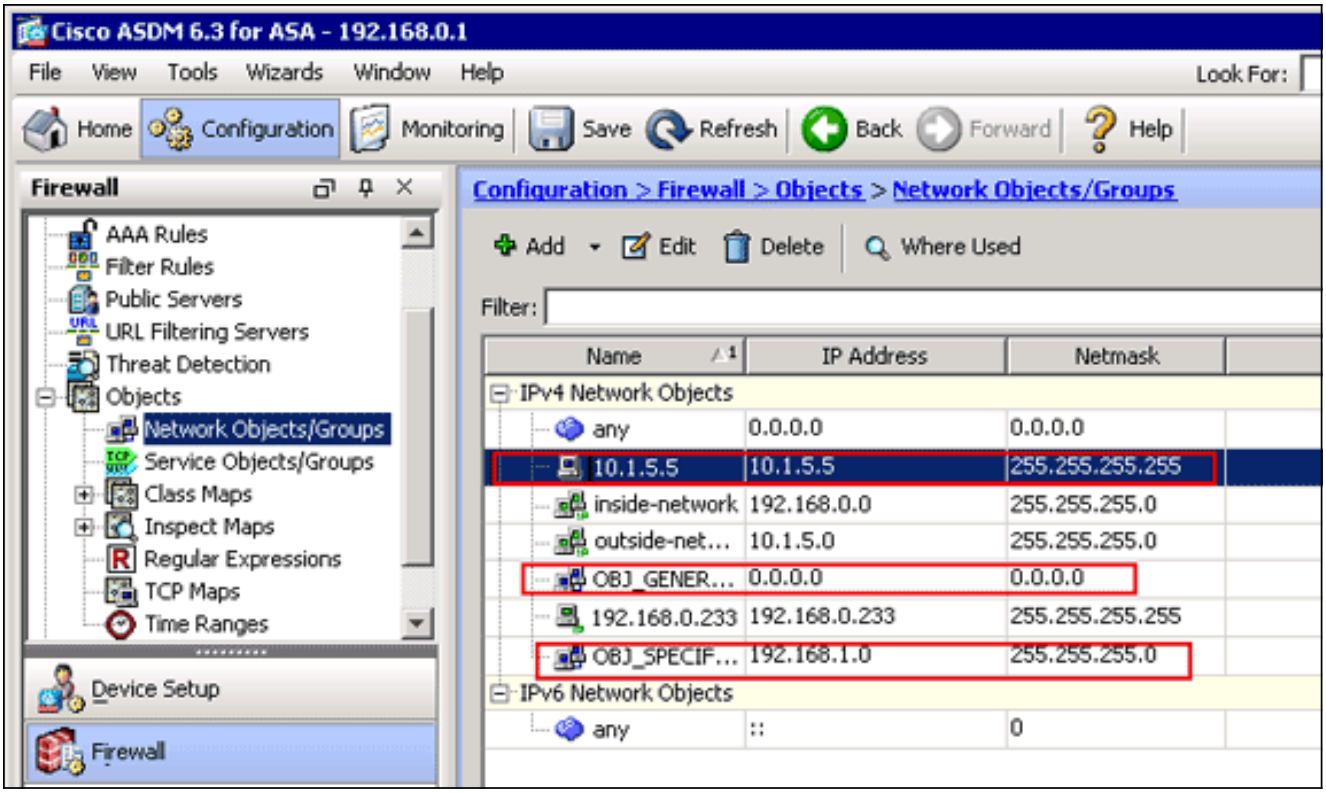
الكائن الثاني ويظهر في قائمة كائنات/مجموعات الشبكة، كما هو موضح في هذه الصورة:



6. كرر الخطوات السابقة لإضافة كائن شبكة ثالث، وانقر فوق **موافق**.يستخدم هذا المثال القيم التالية:الاسم: *10.1.5.5*النوع: *المضيف*عنوان IP:



يتم إنشاء كائنات *10.1.5.5* الشبكة الثالثة وتظهر في قائمة كائنات/مجموعات الشبكة.

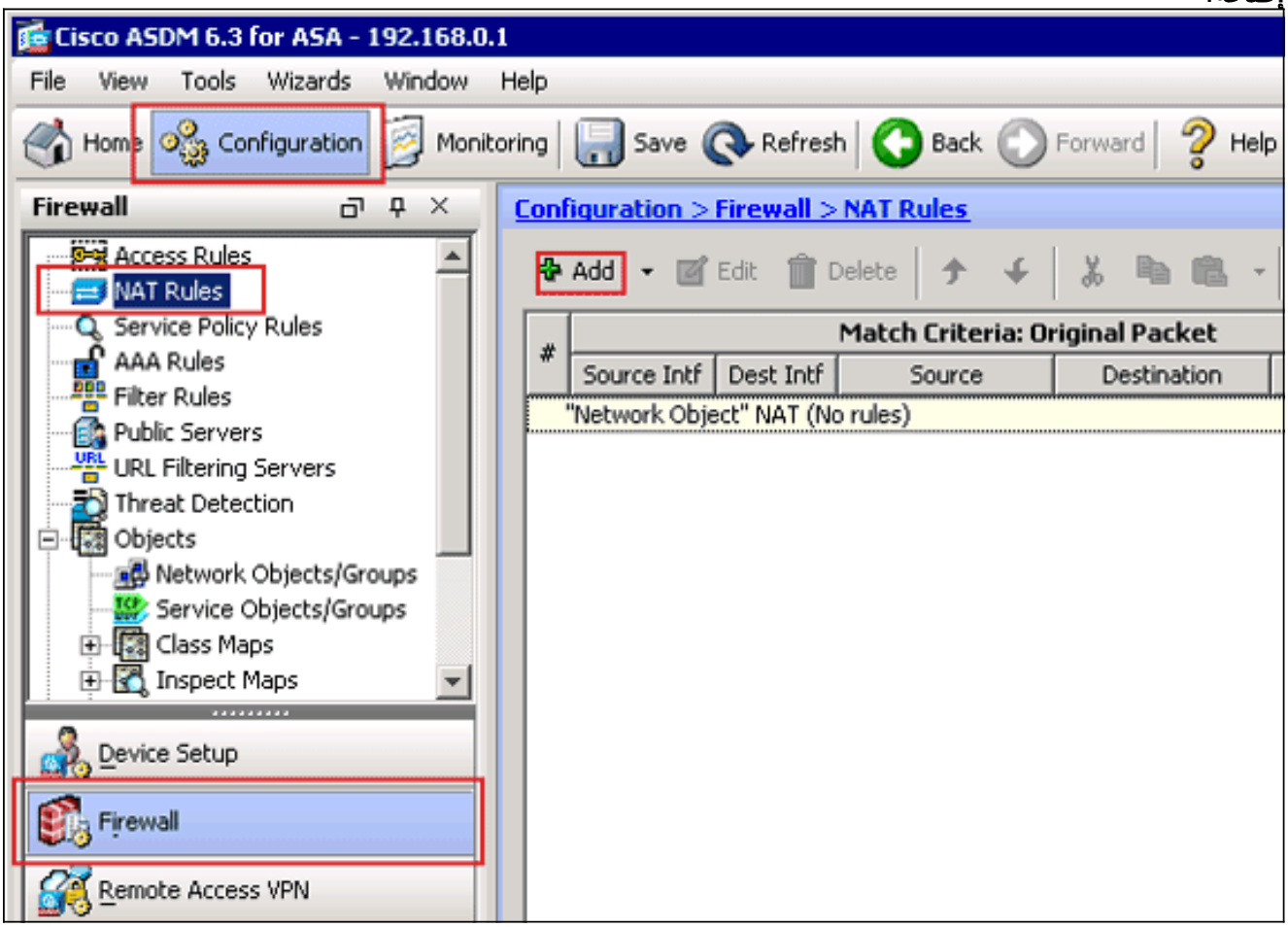


يجب أن تتضمن قائمة كائنات/مجموعات الشبكة الآن الكائنات الثلاثة المطلوبة الضرورية لمرجع قواعد nat.

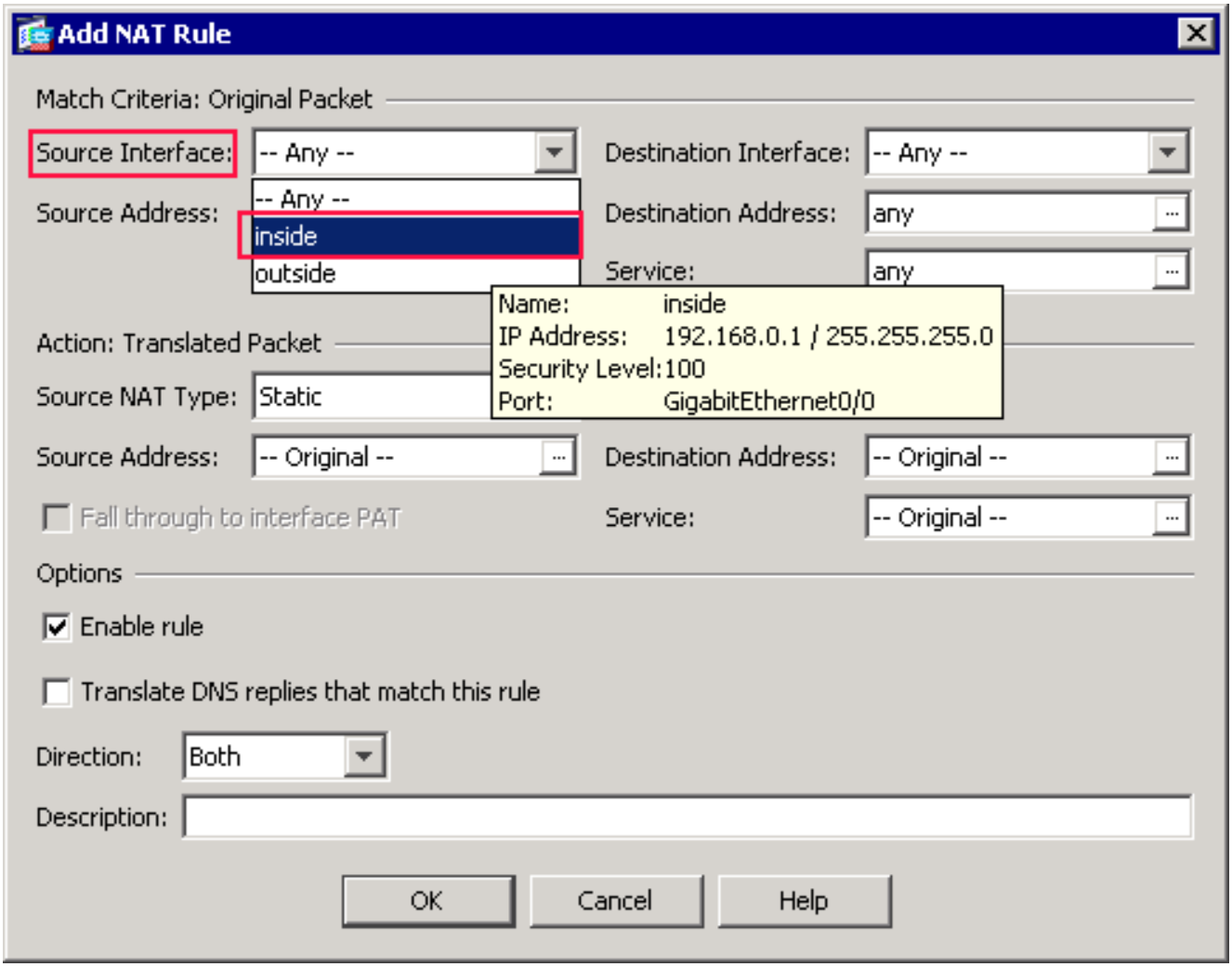
إنشاء قواعد NAT/PAT

أتمت هذا steps in order to خلقت nat/pat قاعدة:

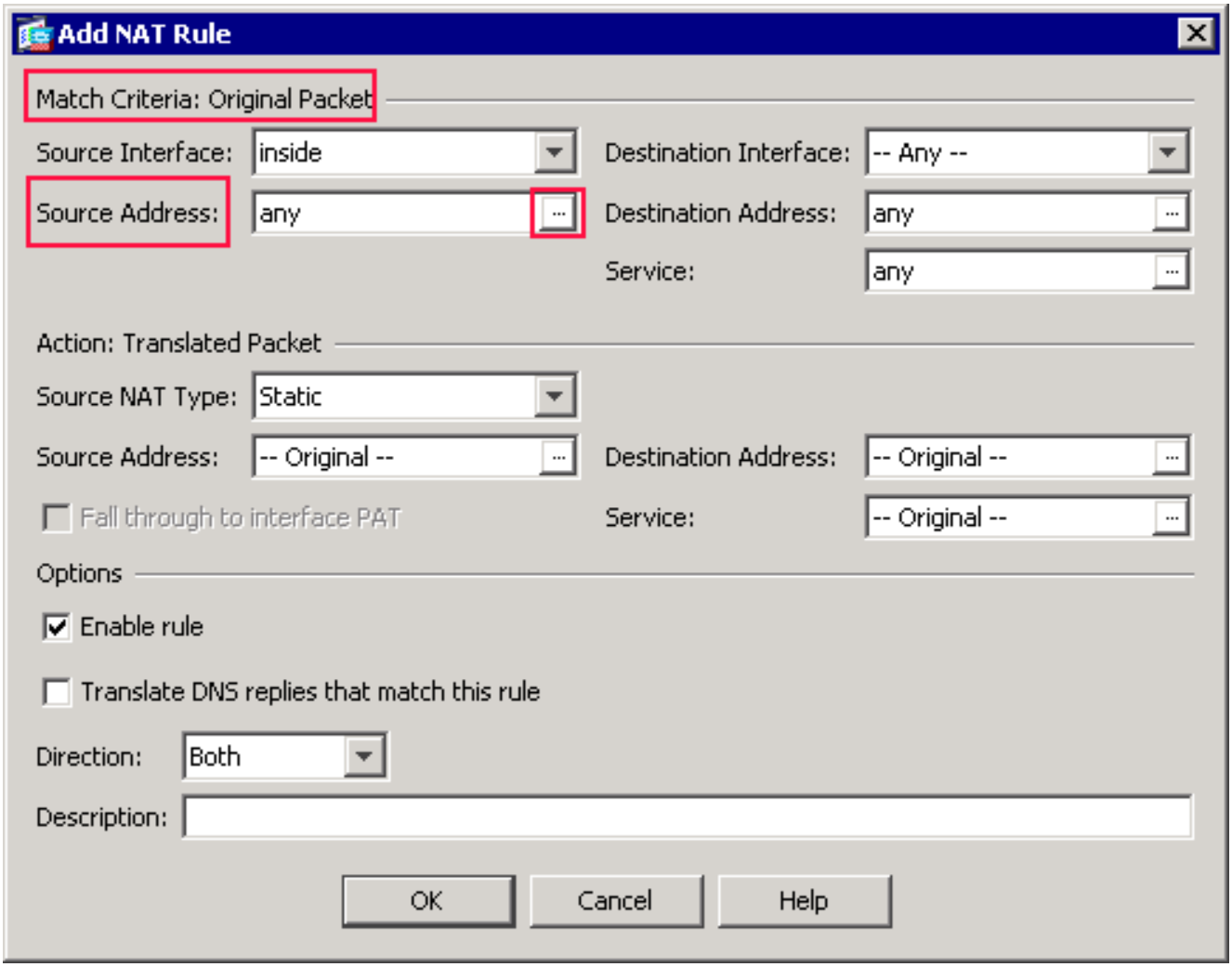
1. خلقت أول nat/pat قاعدة:في ASDM، أختر **تشكيل > جدار حماية > قواعد nat**، وانقر **إضافة**.



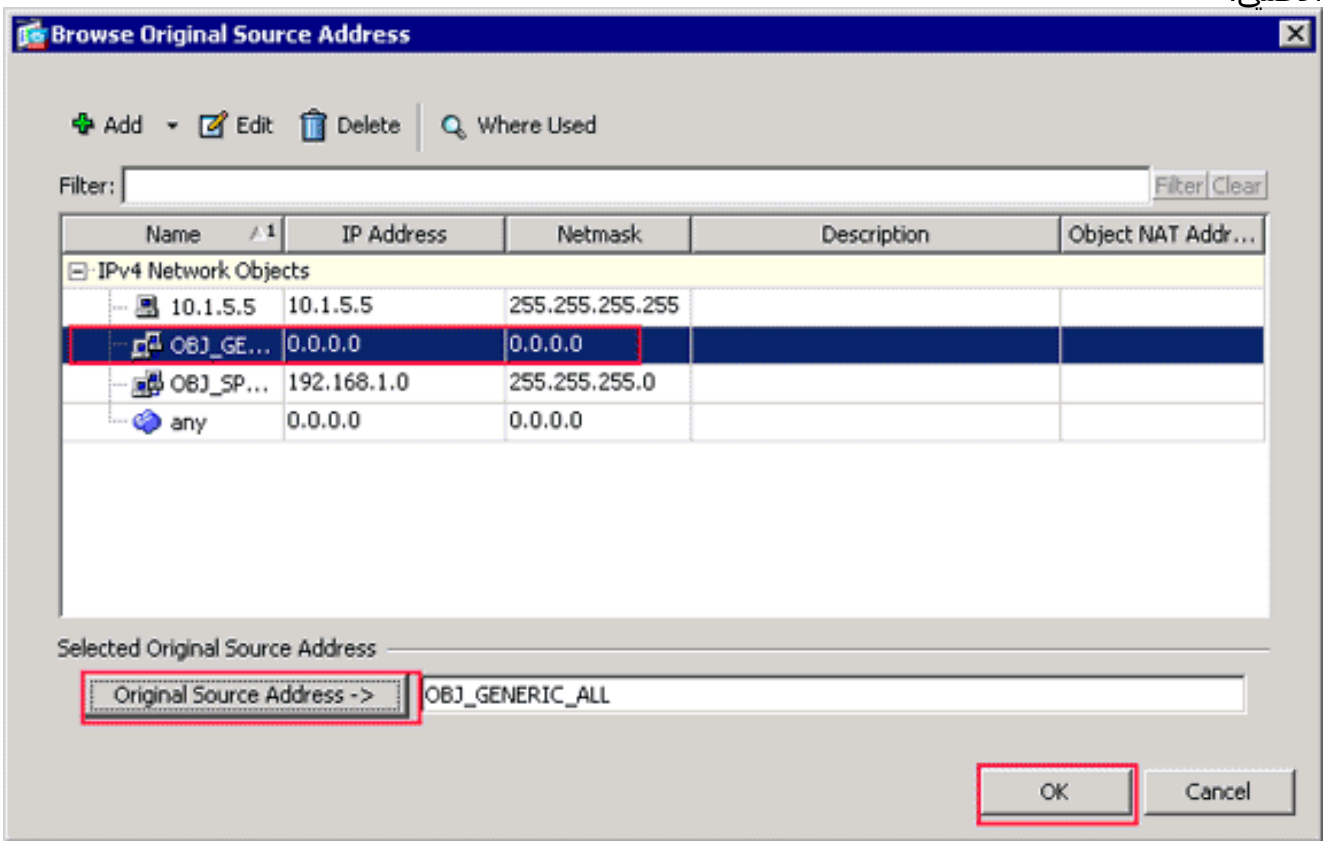
يظهر مربع الحوار إضافة قاعدة
.nat



في مطابقة المعايير: منطقة الحزمة الأصلية من شاشة إضافة قاعدة nat، أختر **داخلي** من القائمة المنسدلة لواجهة
المصدر.

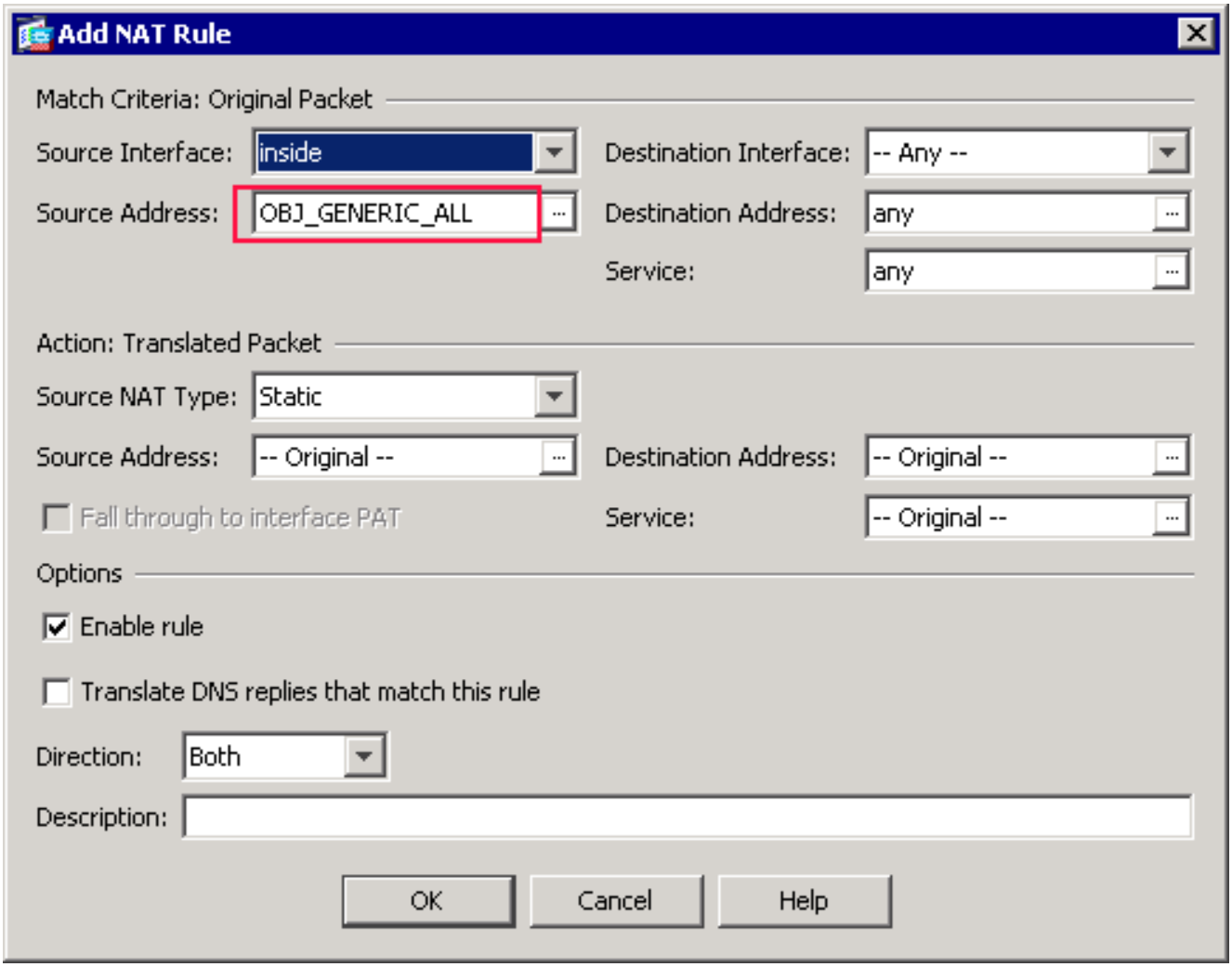


انقر زر تصفح (..) الموجود على يمين حقل نص عنوان المصدر.يظهر مربع الحوار إستعراض عنوان المصدر الأصلي.

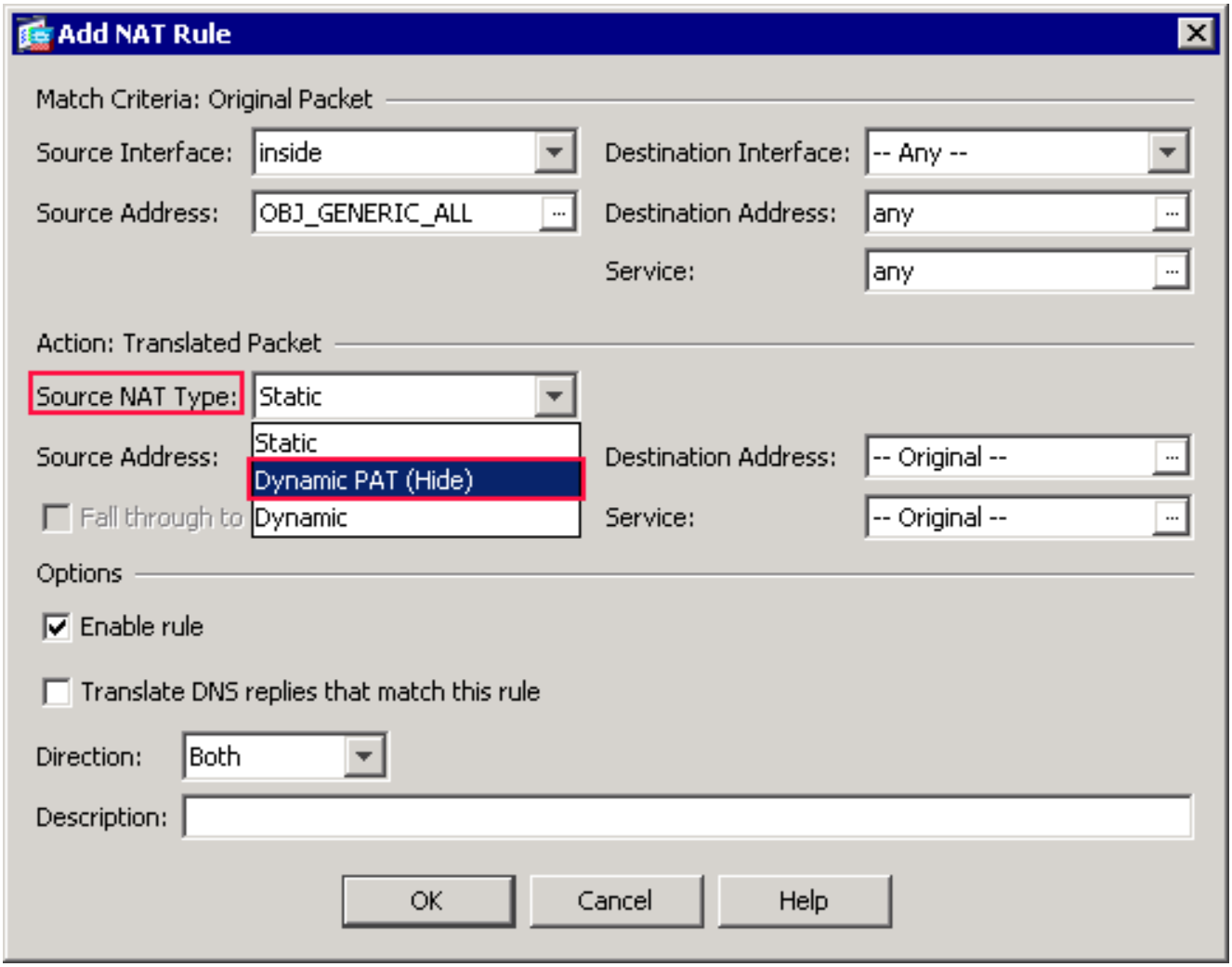


في شاشة تصفح عنوان المصدر الأصلي، أختر أول كائن شبكة قمت بإنشائه. (لهذا المثال، أختر OBJ_GENERIC_ALL.)انقر **عنوان المصدر الأصلي**، وانقر **موافق**.يظهر الآن كائن شبكة

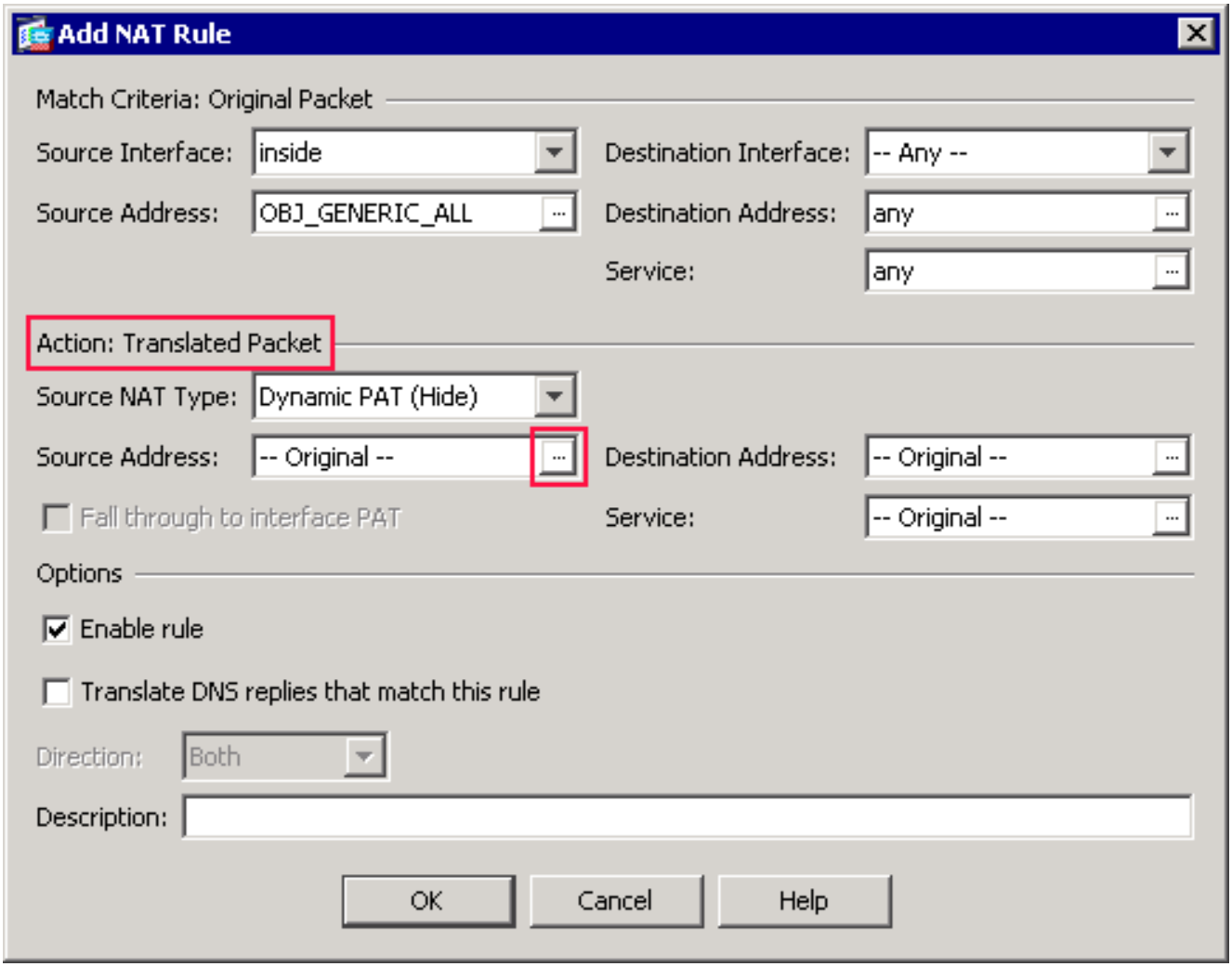
OBJ_GENERIC_ALL في حقل عنوان المصدر في حقل مطابقة المعايير: مساحة الحزمة الأصلية من مربع الحوار إضافة قاعدة
.nat



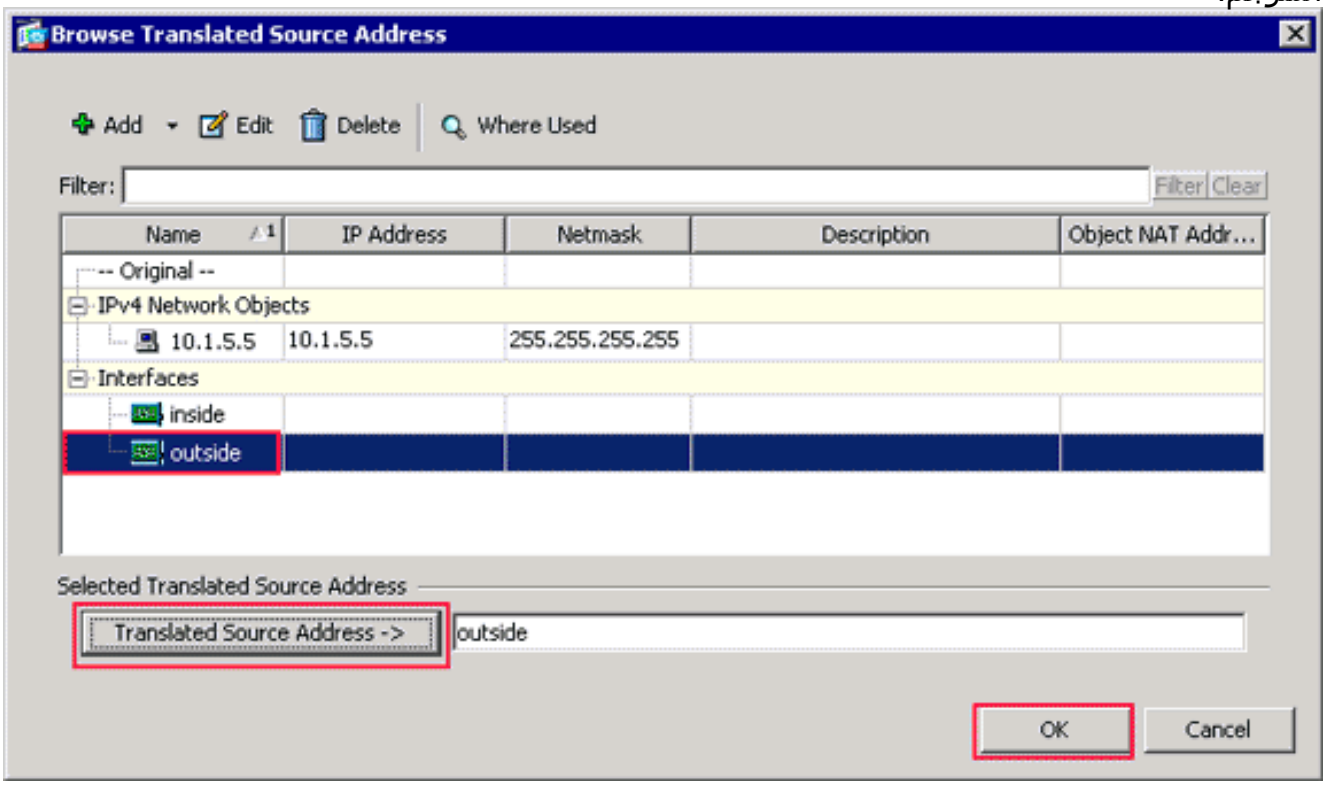
في العملية: ترجمة مساحة الحزمة من شاشة إضافة قاعدة nat، أختر **ضرب ديناميكي (إخفاء)** من شاشة نوع NAT
للمصدر.



انقر فوق زر إستعراض (..) الموجود على يمين حقل عنوان المصدر.

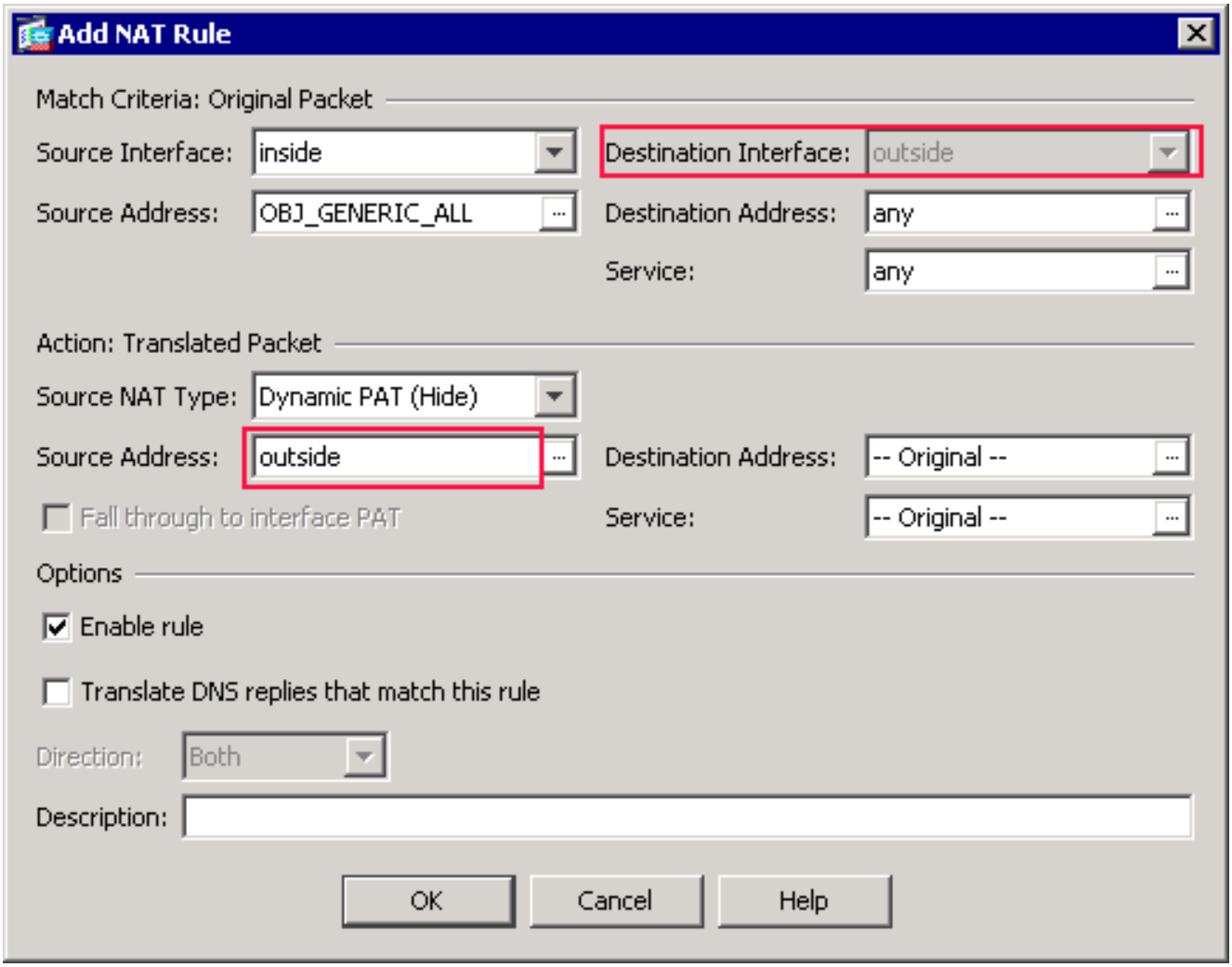


يظهر مربع الحوار إستعراض عنوان المصدر المترجم.

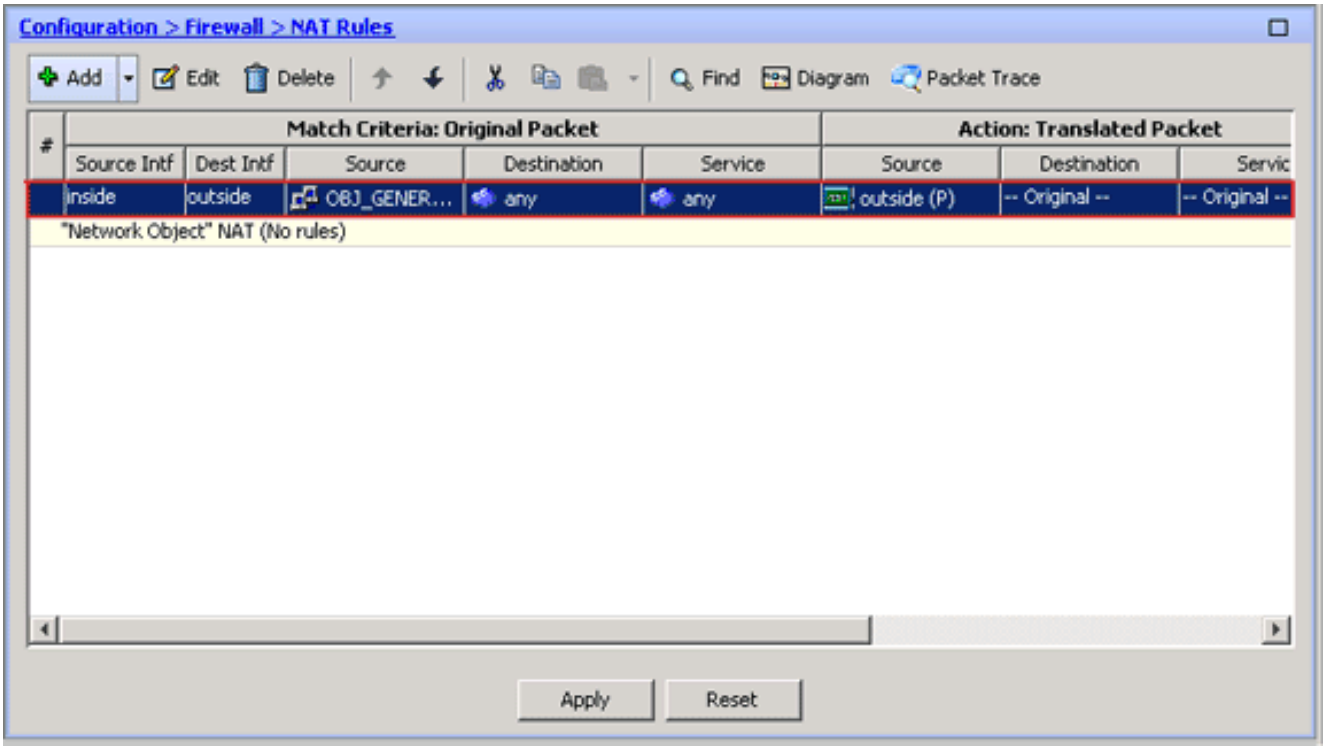


في شاشة تصفح عنوان المصدر المترجم، أختر كائن الواجهة **الخارجية**. (تم إنشاء هذه الواجهة بالفعل لأنها جزء من التكوين الأصلي.)طقطقة **يترجم مصدر عنوان**، وطقطقة **ok**.يظهر القارن خارجي الآن في المصدر عنوان مجال في الإجراء: يترجم منطقة ربط على ال إضافة nat قاعدة

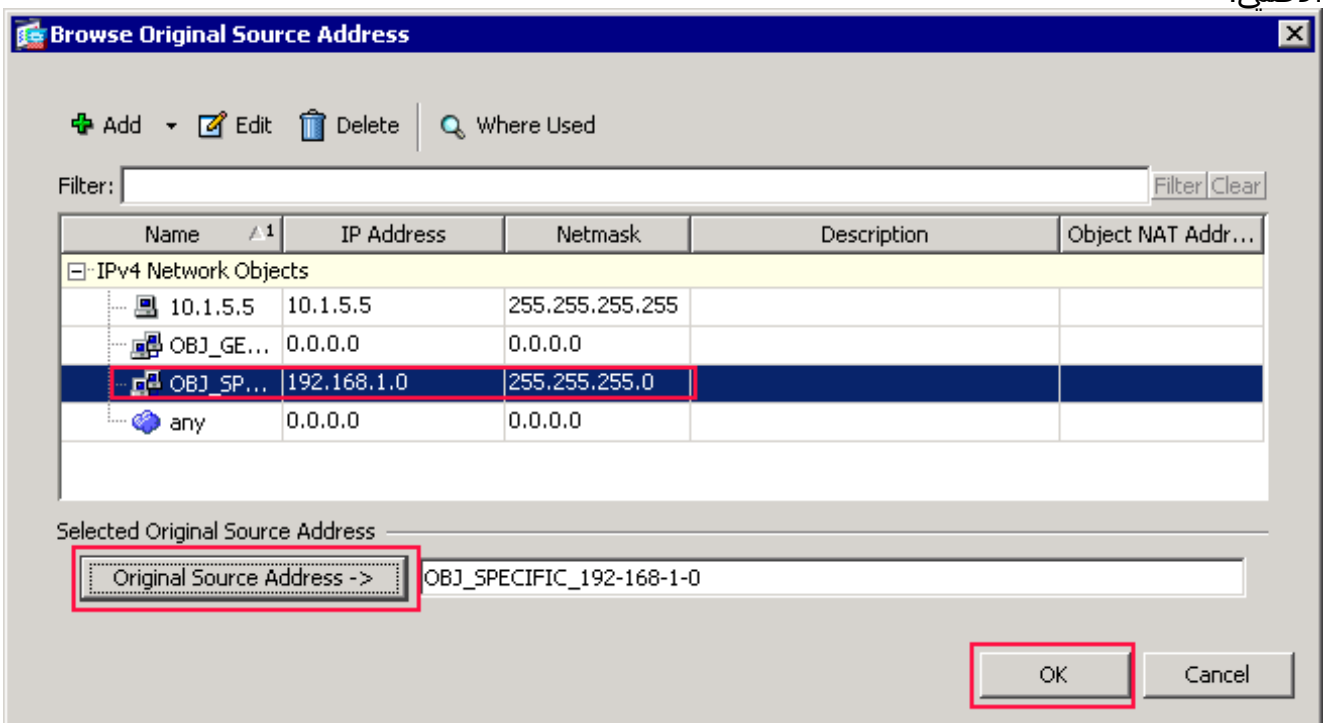
شاشة.



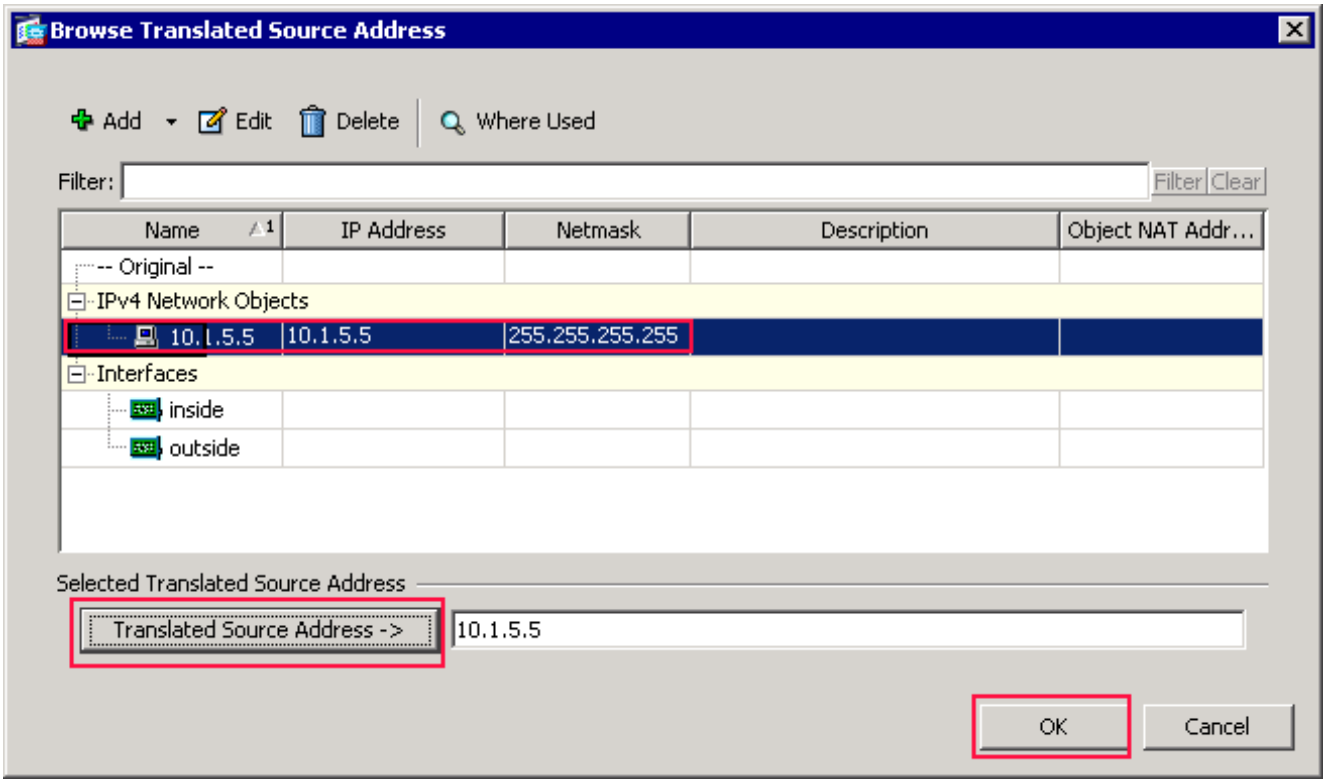
ملاحظة: يتغير حقل *الواجهة الوجهة* أيضا إلى الواجهة الخارجية.دققت أن يظهر أول عملية ضرب قاعدة كما يلي:في معايير المطابقة: مساحة الحزمة الأصلية، تحقق من القيم التالية:واجهة المصدر = داخليعنوان المصدر = OBJ_GENERIC_ALLغاية عنوان = أيالخدمة = أيفي العملية: يترجم منطقة ربط، دققت هذا قيمة:نوع NAT المصدر = ضرب ديناميكي (إخفاء)عنوان المصدر = خارجيغاية عنوان = أصليالخدمة = الأصلوانقر فوق **OK**.تظهر قاعدة NAT الأولى في ASDM، كما هو موضح في هذه الصورة:



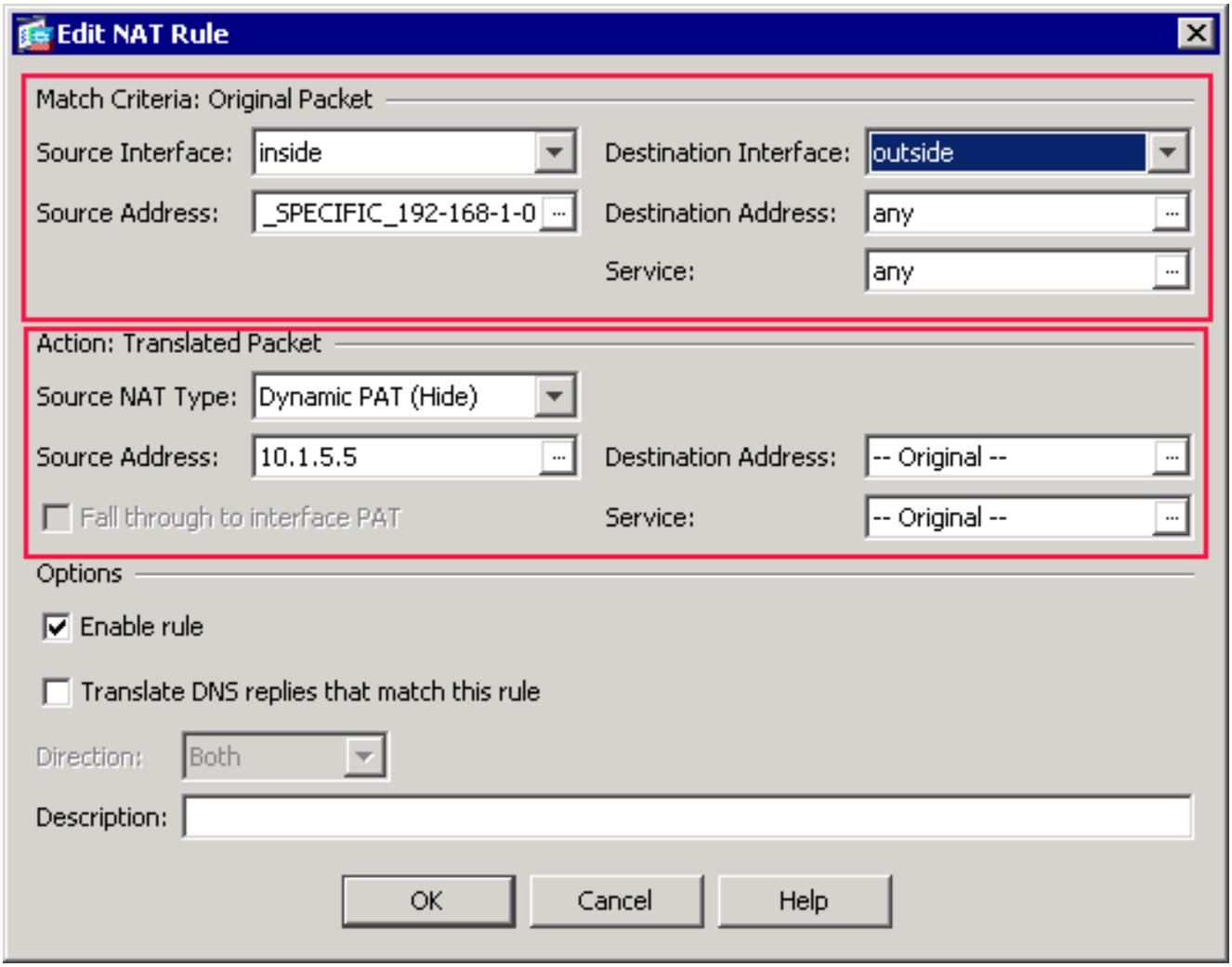
2. خلقت الثاني nat/ضرب قاعدة:في ASDM، أختر **تشكيل > جدار حماية > قواعد nat**، وانقر **إضافة**.في مطابقة المعايير: منطقة الحزمة الأصلية من شاشة إضافة قاعدة nat، أختر **داخلي** من القائمة المنسدلة لواجهة المصدر.انقر فوق زر إستعراض (..) الموجود على يمين حقل عنوان المصدر.يظهر مربع الحوار إستعراض عنوان المصدر
الأصلي.



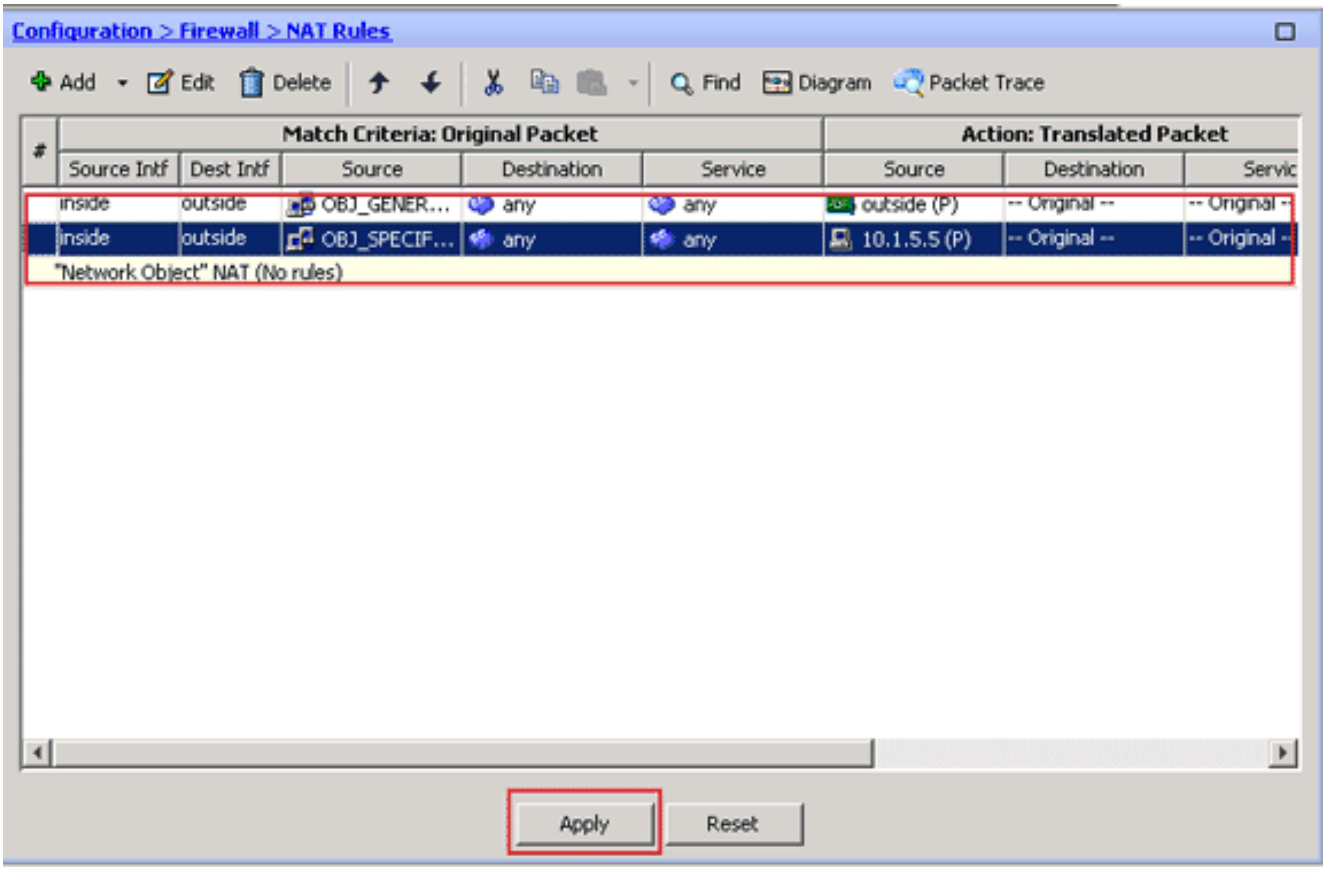
في شاشة تصفح عنوان المصدر الأصلي، أختر الكائن الثاني الذي قمت بإنشائه. (لهذا المثال، أختر **OBJ_SPECIFIC_192-168-1-0**.)انقر **عنوان المصدر الأصلي**، وانقر **موافق**.يظهر كائن الشبكة *OBJ_SPECIFIC_192-168-1-0* في حقل عنوان المصدر في مربع الحوار مطابقة المعايير: مساحة الحزمة الأصلية من مربع الحوار إضافة قاعدة nat.في العملية: ترجمة مساحة الحزمة من شاشة إضافة قاعدة nat، أختر **ضرب ديناميكي (إخفاء)** من شاشة نوع NAT للمصدر.انقر فوق الزر **...** الموجود على يمين حقل عنوان المصدر.يظهر مربع الحوار إستعراض عنوان المصدر
المترجم.



في شاشة تصفح عنوان المصدر المترجم، أختر الكائن **10.1.5.5**. (تم إنشاء هذه الواجهة بالفعل لأنها جزء من التكوين الأصلي).انقر فوق **عنوان المصدر المترجم**، ثم انقر فوق **موافق**.يظهر كائن الشبكة **10.1.5.5** في حقل العنوان المصدر في الإجراء: تتم ترجمة منطقة الحزمة من شاشة إضافة قاعدة nat.في مطابقة المعايير: منطقة الحزمة الأصلية، أختر **خارج** القائمة المنسدلة لواجهة الوجهة.**ملاحظة:** إذا لم تقم باختيار *خارجي* لهذا الخيار، فستشير واجهة الوجهة إلى *أي*.



دققت أن الثاني أتمت nat/pat قاعدة يظهر كما يلي:في معايير المطابقة: مساحة الحزمة الأصلية، تحقق من القيم التالية:واجهة المصدر = داخليعنوان المصدر = 0-1-168-192_SPECIFIC_OBJغاية عنوان = خارجالخدمة = أيفي العملية: يترجم منطقة ربط، دققت هذا قيمة:نوع NAT المصدر = ضرب ديناميكي (إخفاء)عنوان المصدر = 10.1.5.5غاية عنوان = أصليالخدمة = الأصلوانقر فوق **OK**.يظهر التكوين المكتمل nat في ASDM، كما هو موضح في هذه الصورة:



3. انقر فوق الزر **تطبيق** لتطبيق التغييرات على التكوين الجاري تشغيله.
هذا يتم التشكيل من ضرب حركي على cisco تعديل أمن أداة (ASA).

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

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

التحقق من قاعدة PAT العامة

- show local-host — يعرض حالات الشبكة للمضيفين المحليين.

```
ASA#show local-host

Interface outside: 1 active, 2 maximum active, 0 denied
                                    ,<local host: <125.252.196.170
                                  TCP flow count/limit = 2/unlimited
                                     TCP embryonic count to host = 0
                                  TCP intercept watermark = unlimited
                                   UDP flow count/limit = 0/unlimited
The TCP connection outside address corresponds !--- to the actual destination of ---!
,125.255.196.170:80 Conn: TCP outside 125.252.196.170:80 inside 192.168.0.5:1051
                                          idle 0:00:03, bytes 13758, flags UIO
                  ,TCP outside 125.252.196.170:80 inside 192.168.0.5:1050, idle 0:00:04
                                                bytes 11896, flags UIO
                               Interface inside: 1 active, 1 maximum active, 0 denied
                                                    ,<local host: <192.168.0.5
                                  TCP flow count/limit = 2/unlimited
                                     TCP embryonic count to host = 0
                                  TCP intercept watermark = unlimited
                                   UDP flow count/limit = 0/unlimited
```

```
The TCP PAT outside address corresponds to the !--- outside IP address of the ASA – ---!
    10.1.5.1. Xlate: TCP PAT from inside:192.168.0.5/1051 to outside:10.1.5.1/32988 flags
                                        ri idle 0:00:17 timeout 0:00:30
              TCP PAT from inside:192.168.0.5/1050 to outside:10.1.5.1/17058 flags
                                        ri idle 0:00:17 timeout 0:00:30

                                                                        :Conn
            ,TCP outside 125.252.196.170:80 inside 192.168.0.5:1051, idle 0:00:03
                                                bytes 13758, flags UIO
            ,TCP outside 125.252.196.170:80 inside 192.168.0.5:1050, idle 0:00:04
                                                bytes 11896, flags UIO
```

- show conn — يعرض حالة الاتصال لنوع الاتصال المعين.

```
                                                        ASA#show conn
                                                    in use, 3 most used 2
        ,TCP outside 125.252.196.170:80 inside 192.168.0.5:1051, idle 0:00:06
                                                bytes 13758, flags UIO
        ,TCP outside 125.252.196.170:80 inside 192.168.0.5:1050, idle 0:00:01
                                                bytes 13526, flags UIO
```

- show xlate — يعرض المعلومات المتعلقة بفتحات الترجمة.

```
                                                        ASA#show xlate
                                                    in use, 7 most used 4
          ,Flags: D - DNS, I - dynamic, r - portmap, s - static, I - identity
                                                                T - twice
              TCP PAT from inside:192.168.0.5/1051 to outside:10.1.5.1/32988 flags
                                        ri idle 0:00:23 timeout 0:00:30
              TCP PAT from inside:192.168.0.5/1050 to outside:10.1.5.1/17058 flags
                                        ri idle 0:00:23 timeout 0:00:30
```

التحقق من قاعدة PAT معينة

- show local-host — يعرض حالات الشبكة للمضيفين المحليين.

```
                                                        ASA#show local-host
                                    Interface outside: 1 active, 2 maximum active, 0 denied
                                                          ,<local host: <125.252.196.170
                                                TCP flow count/limit = 2/unlimited
                                                   TCP embryonic count to host = 0
                                                TCP intercept watermark = unlimited
                                                 UDP flow count/limit = 0/unlimited
  The TCP connection outside address corresponds to !--- the actual destination of ---!
       ,125.255.196.170:80. Conn: TCP outside 125.252.196.170:80 inside 192.168.1.5:1067
                                        idle 0:00:07, bytes 13758, flags UIO
                                    ,TCP outside 125.252.196.170:80 inside 192.168.1.5:1066
                                        idle 0:00:03, bytes 11896, flags UIO
                                    Interface inside: 1 active, 1 maximum active, 0 denied
                                                          ,<local host: <192.168.0.5
                                                TCP flow count/limit = 2/unlimited
                                                   TCP embryonic count to host = 0
                                                TCP intercept watermark = unlimited
                                                 UDP flow count/limit = 0/unlimited


  The TCP PAT outside address corresponds to an !--- outside IP address of 10.1.5.5. ---!
                Xlate: TCP PAT from inside:192.168.1.5/1067 to outside:10.1.5.5/35961 flags
                                        ri idle 0:00:17 timeout 0:00:30
              TCP PAT from inside:192.168.1.5/1066 to outside:10.1.5.5/23673 flags
                                        ri idle 0:00:17 timeout 0:00:30

                                                                        :Conn
            ,TCP outside 125.252.196.170:80 inside 192.168.1.5:1067, idle 0:00:07
                                                bytes 13758, flags UIO
            ,TCP outside 125.252.196.170:80 inside 192.168.1.5:1066, idle 0:00:03
```

```
bytes 11896, flags UIO
```

- show conn — يعرض حالة الاتصال لنوع الاتصال المعين.

```
ASA#show conn
in use, 3 most used 2
,TCP outside 125.252.196.170:80 inside 192.168.1.5:1067, idle 0:00:07
bytes 13653, flags UIO
,TCP outside 125.252.196.170:80 inside 192.168.1.5:1066, idle 0:00:03
bytes 13349, flags UIO
```

- show xlate — يعرض المعلومات المتعلقة بفتحات الترجمة.

```
ASA#show xlate
in use, 9 most used 3
,Flags: D - DNS, I - dynamic, r - portmap, s - static, I - identity
T - twice
TCP PAT from inside:192.168.1.5/1067 to outside:10.1.5.5/35961 flags
ri idle 0:00:23 timeout 0:00:30
TCP PAT from inside:192.168.1.5/1066 to outside:10.1.5.5/29673 flags
ri idle 0:00:23 timeout 0:00:30
```

استكشاف الأخطاء وإصلاحها

لا تتوفر حاليًا معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

معلومات ذات صلة

- مدير أجهزة حلول الأمان المعدلة من Cisco
- أجهزة الأمان المعدلة Cisco ASA 5500 Series Adaptive Security Appliances
- 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).