PALMADITA dinámica ASA 8.3(x) con dos redes internas y ejemplos de configuración de Internet

Contenido

Introducción

Este documento proporciona una configuración de muestra para la PALMADITA dinámica en un dispositivo de seguridad adaptante de Cisco (ASA) esa versión de software de los funcionamientos 8.3(1). La PALMADITA dinámica traduce a las direcciones reales múltiples a una sola dirección IP asociada traduciendo el direccionamiento y el puerto de origen de verdadero origen al direccionamiento asociado y al puerto asociado único. Cada conexión requiere una sesión de traducción independiente porque el puerto de origen es diferente para cada conexión.

prerrequisitos

Requisitos

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Aseegurese la red interna tiene dos redes situadas en el interior del ASA:192.168.0.0/24 — Red conectada directamente con el ASA.192.168.1.0/24 — Red en el interior del ASA, pero detrás de otro dispositivo (por ejemplo, un router).
- Aseegurese a los usuarios internos conseguir la PALMADITA como sigue:Los host en la subred 192.168.1.0/24 conseguirán la PALMADITA a una dirección IP de repuesto dada por el ISP (10.1.5.5).Cualquier otro host detrás del interior del ASA conseguirá la PALMADITA a la dirección IP de la interfaz exterior del ASA (10.1.5.1).

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Dispositivo de seguridad adaptante de Cisco (ASA) con la versión 8.3(1)
- Versión 6.3(1) del ASDM

Note: Consulte Cómo Permitir el Acceso HTTPS para el ASDM para que el ASA sea configurado por el ASDM.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

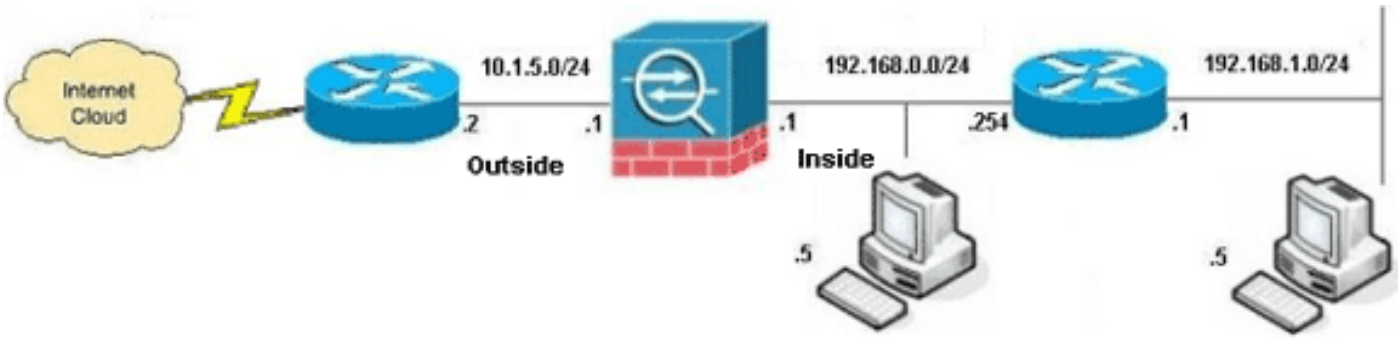
Convenciones

Refiera a los convenios de los consejos técnicos de Cisco para la información sobre las convenciones sobre documentos.

Configuración

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Note: Los esquemas de direccionamiento IP usados en esta configuración no son legalmente enrutables en Internet. Son los direccionamientos del RFC 1918, que se han utilizado en un ambiente de laboratorio.

- Configuración CLI ASA
- Configuración de ASDM

Configuración CLI ASA

Este documento usa las configuraciones detalladas a continuación.

Configuración dinámica de la PALMADITA ASA
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
```

Config que se ejecutan ASA 8.3(1)

```
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
```

Configuración de ASDM

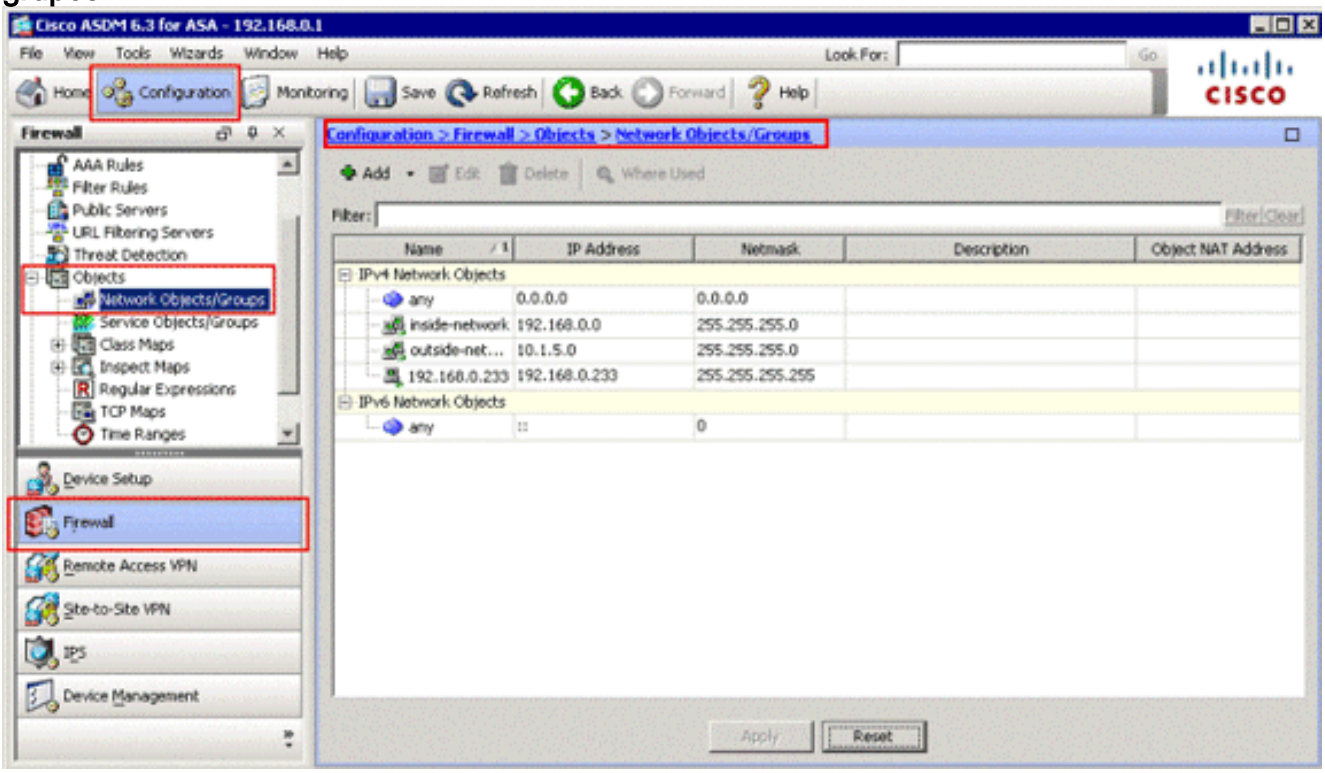
Para completar esta configuración a través de la interfaz del ASDM, usted debe:

1. Agregue tres objetos de red; este los ejemplos agregan estos objetos de red:OBJ_GENERIC_ALLOBJ_SPECIFIC_192-168-1-010.1.5.5
2. Cree dos reglas NAT/PAT; este los ejemplos crean las reglas NAT para estos objetos de red:OBJ_GENERIC_ALLOBJ_SPECIFIC_192-168-1-0

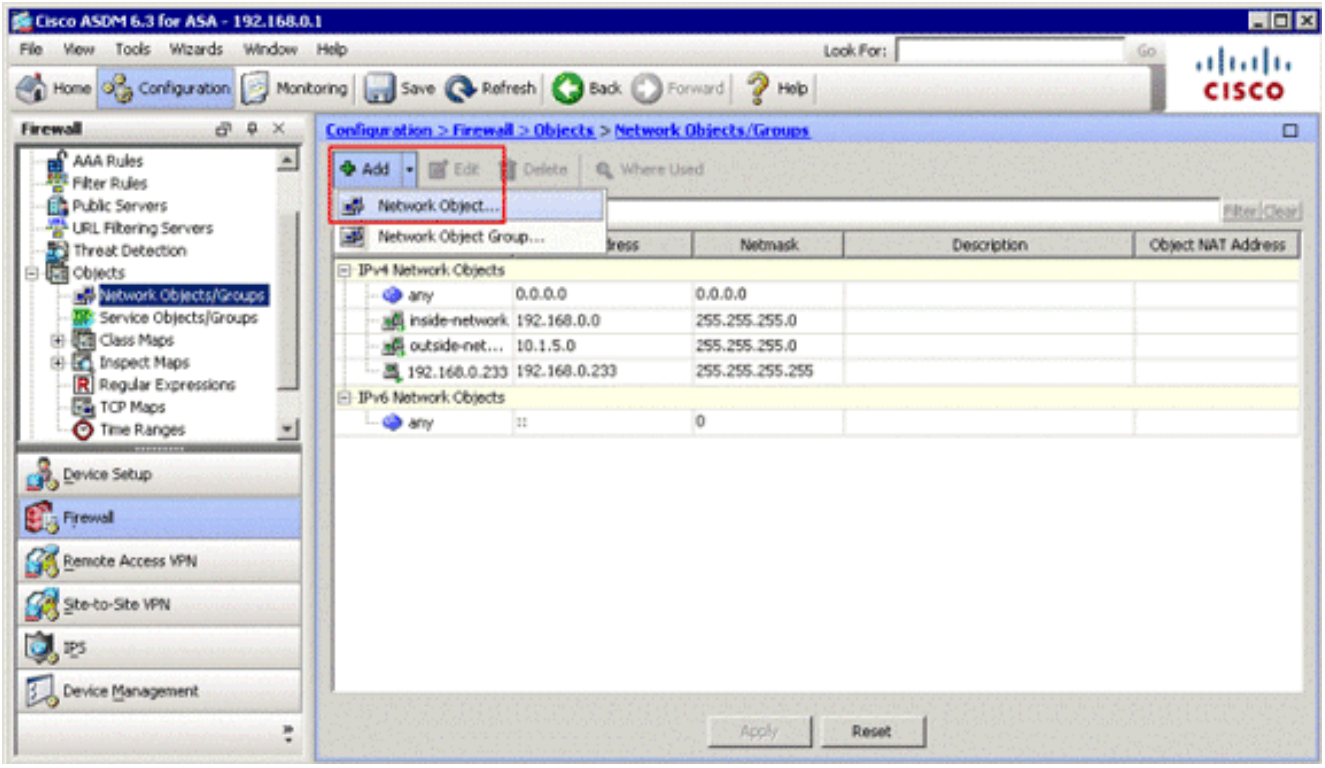
Agregue los objetos de red

Complete estos pasos para agregar los objetos de red:

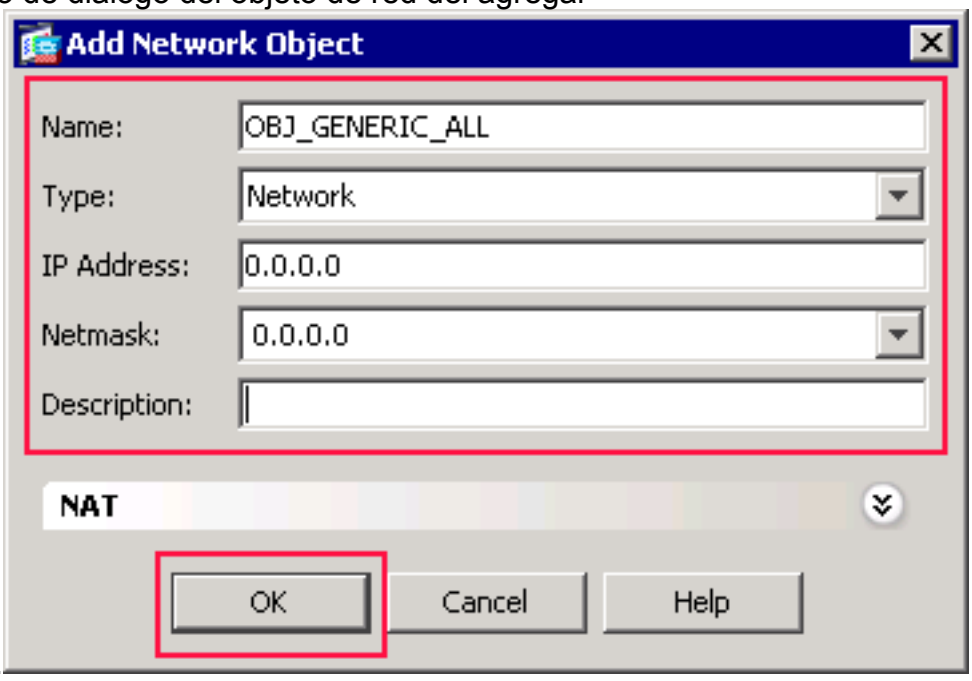
1. Inicie sesión al ASDM, y elija la **configuración > el Firewall > los objetos > los objetos de red/a los grupos**.



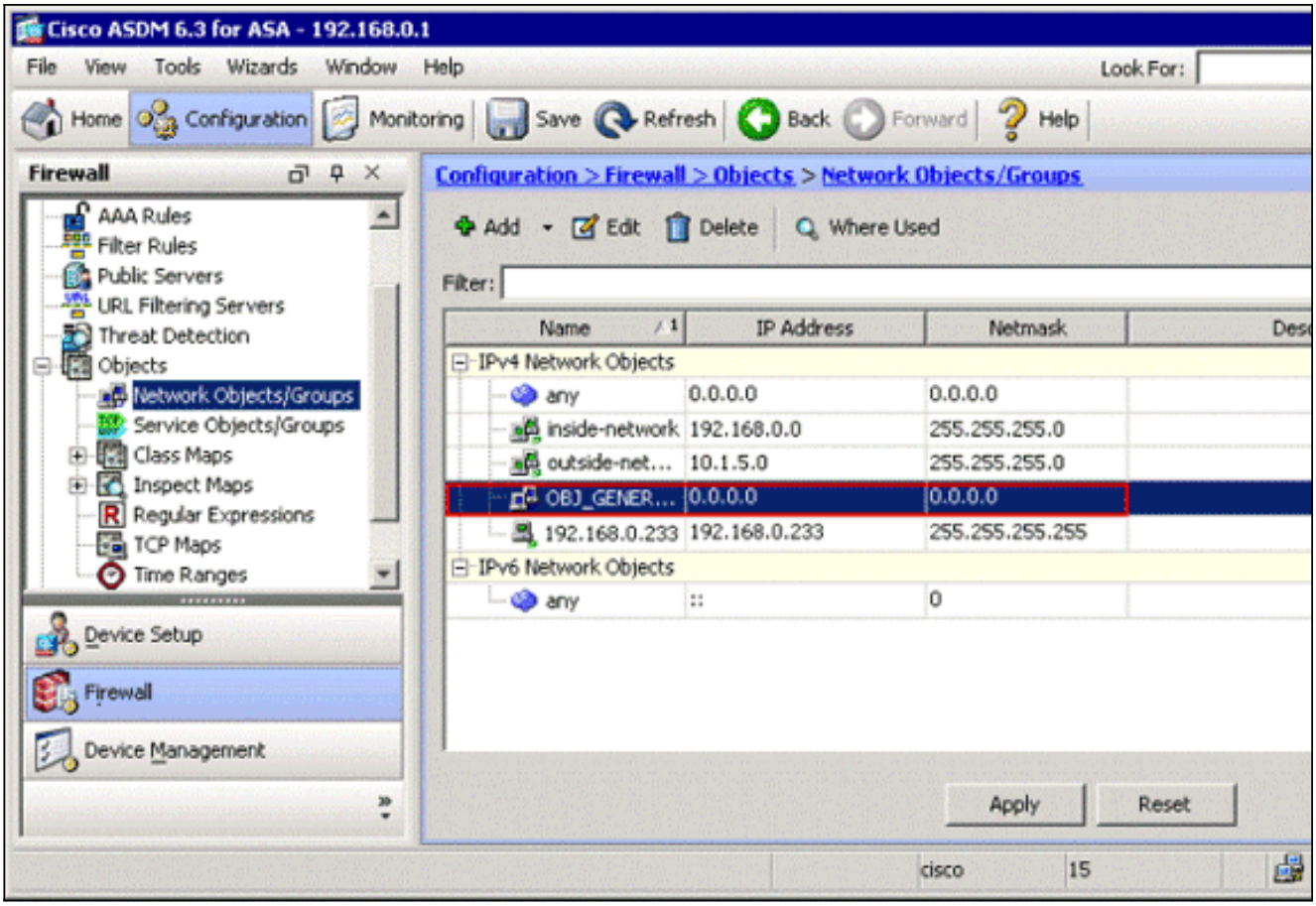
2. Elija **agregan > objeto de red** para agregar un objeto de red.



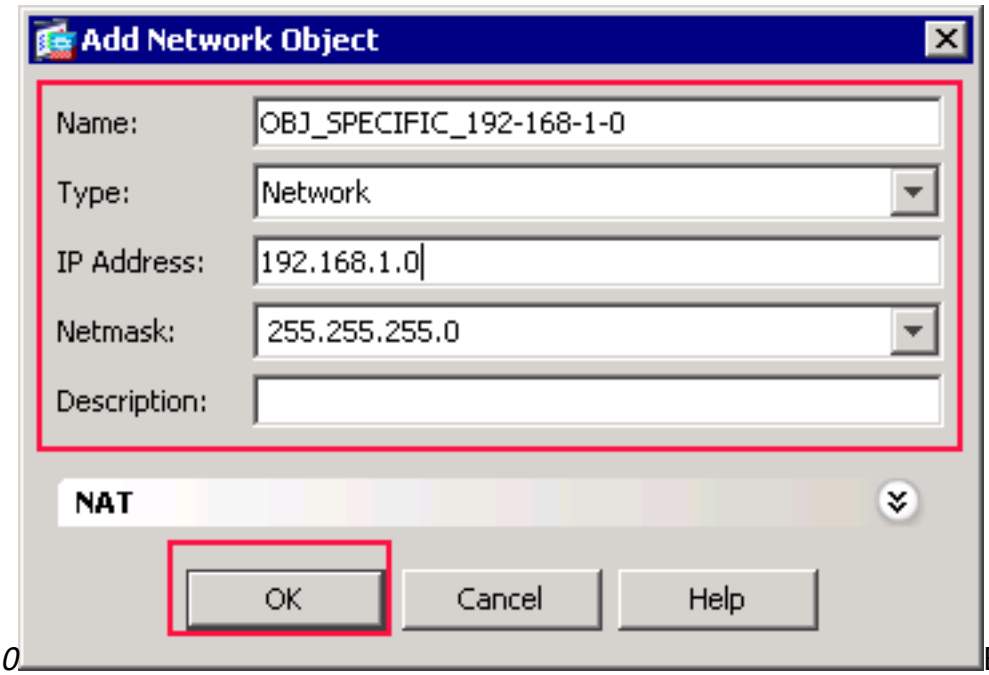
El cuadro de diálogo del objeto de red del agregar aparece.



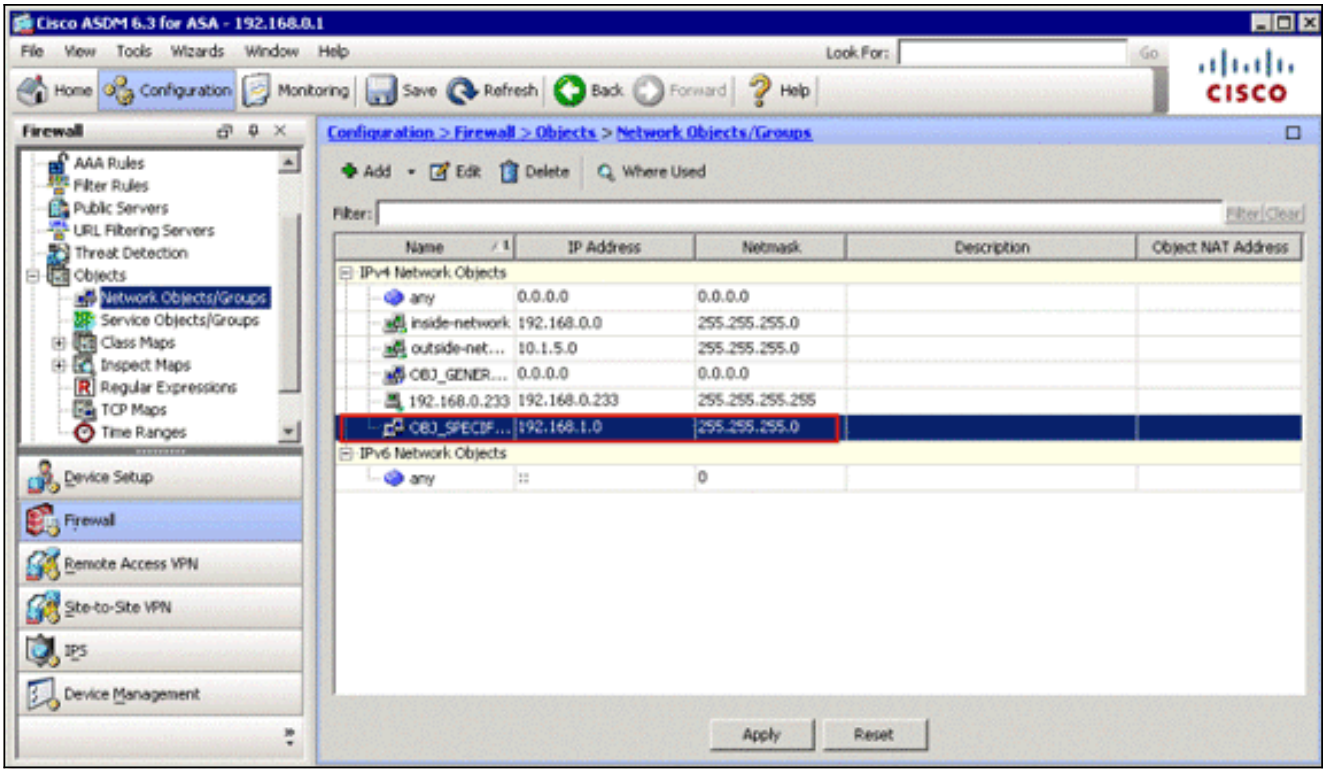
3. Ingrese esta información en el cuadro de diálogo del objeto de red del agregar:Nombre del objeto de red. (Este ejemplo utiliza *OBJ_GENERIC_ALL*.)Objeto del tipo de red. (Este ejemplo utiliza la *red*.)Dirección IP para el objeto de red. (Este ejemplo utiliza *0.0.0.0*.)Netmask para el objeto de red. (Este ejemplo utiliza *0.0.0.0*.)
4. Click OK.El objeto de red se crea y aparece en la lista de los objetos de red/de los grupos, tal y como se muestra en de esta imagen:

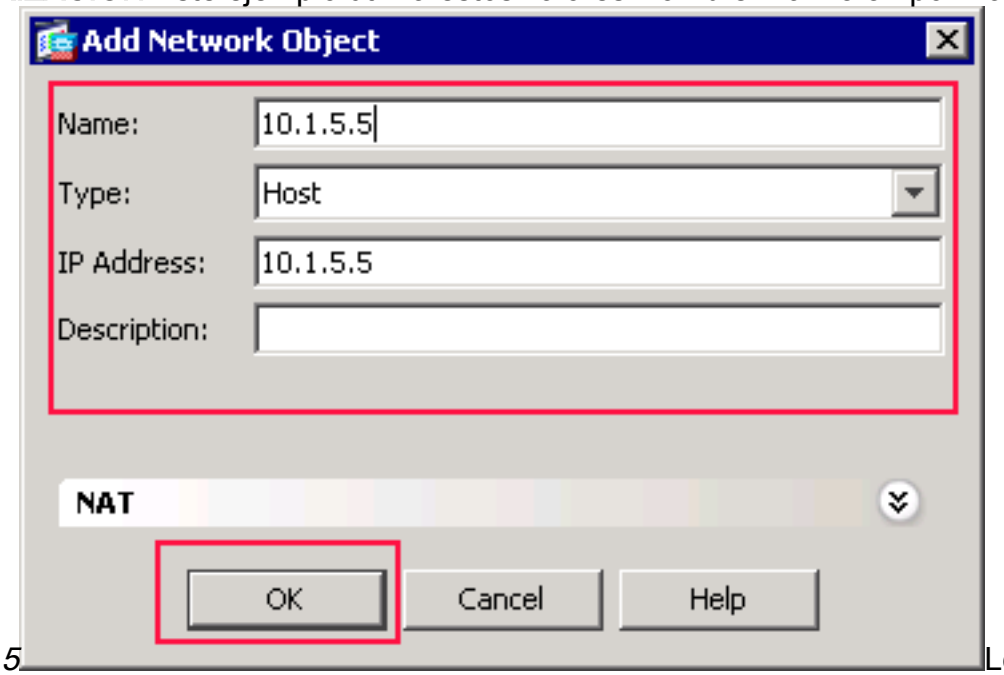


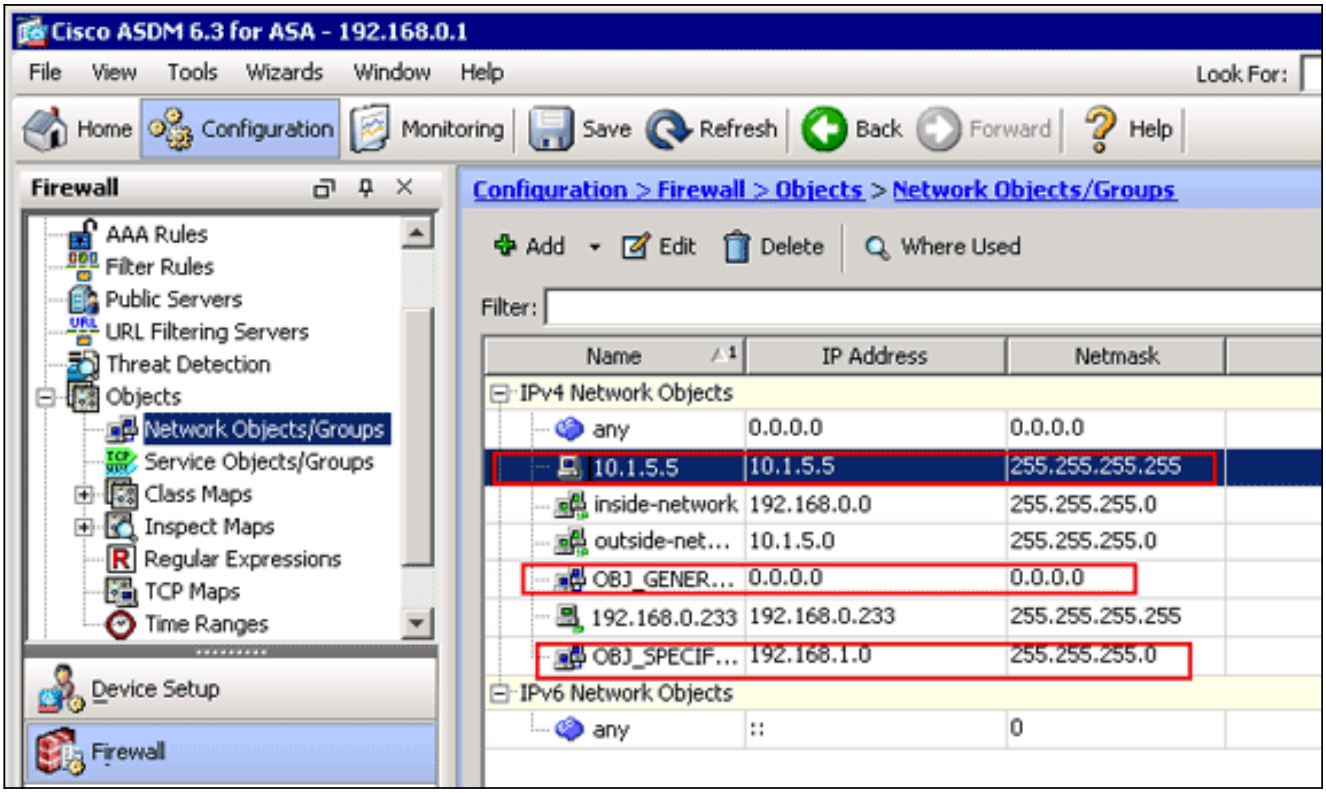
5. Relance los pasos anteriores para agregar un segundo objeto de red, y haga clic la **AUTORIZACIÓN**.Este ejemplo utiliza estos valores:Nombre: *OBJ_SPECIFIC_192-168-1-0*Tipo: *Red*Dirección IP: *192.168.1.0*Netmask:



*255.255.255.0*El segundo objeto se crea y aparece en la lista de los objetos de red/de los grupos, tal y como se muestra en de esta
imagen:



6. Relance los pasos anteriores para agregar un tercer objeto de red, y haga clic la **AUTORIZACIÓN**.Este ejemplo utiliza estos valores:Nombre: *10.1.5.5*Tipo: *Host*Dirección IP: *10.1.5.5* 
Los terceros objetos de red se crean y aparecen en la lista de los objetos de red/de los grupos.

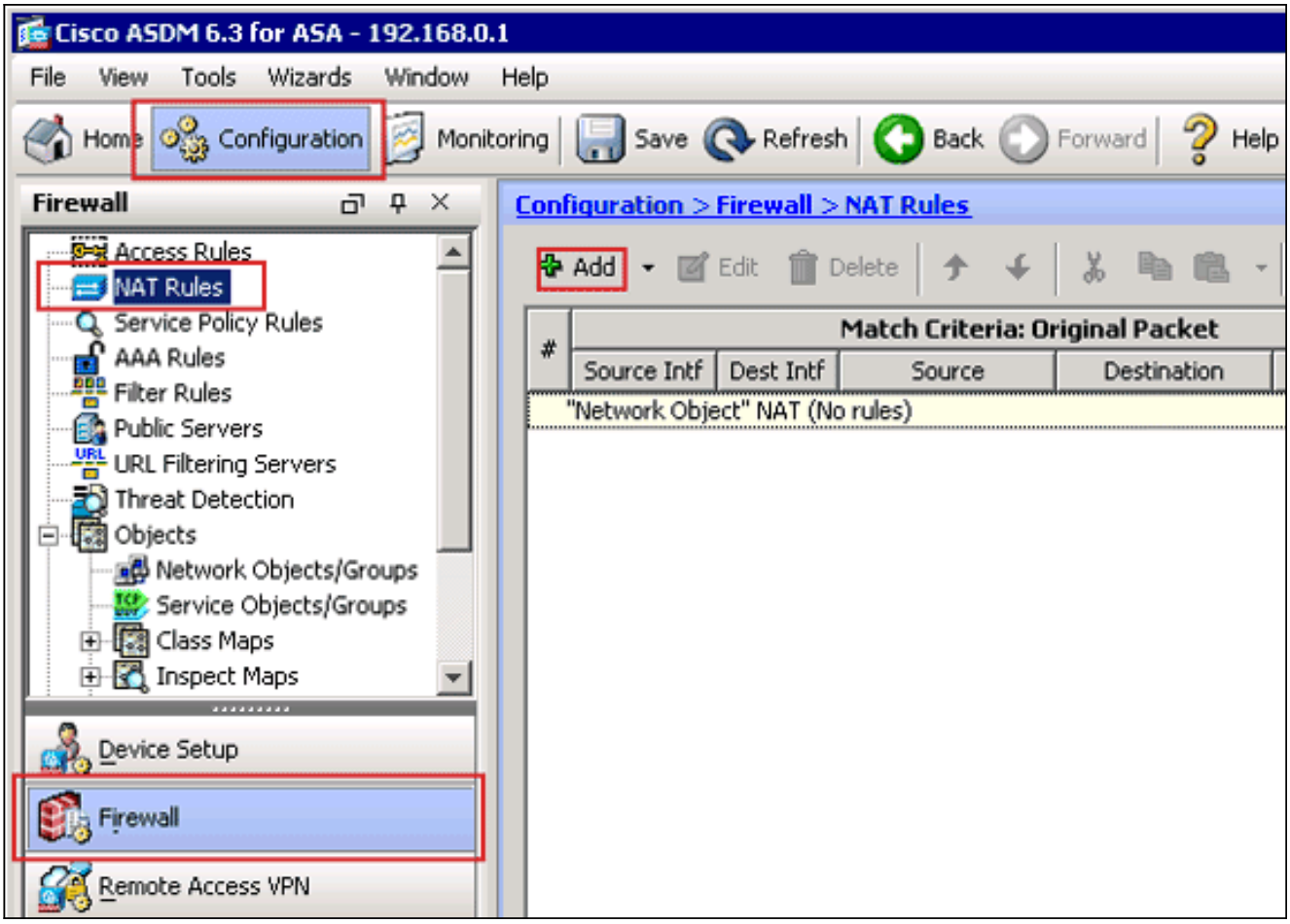


La lista de los objetos de red/de los grupos debe ahora incluir los tres objetos requeridos necesarios para que las reglas NAT se refieran.

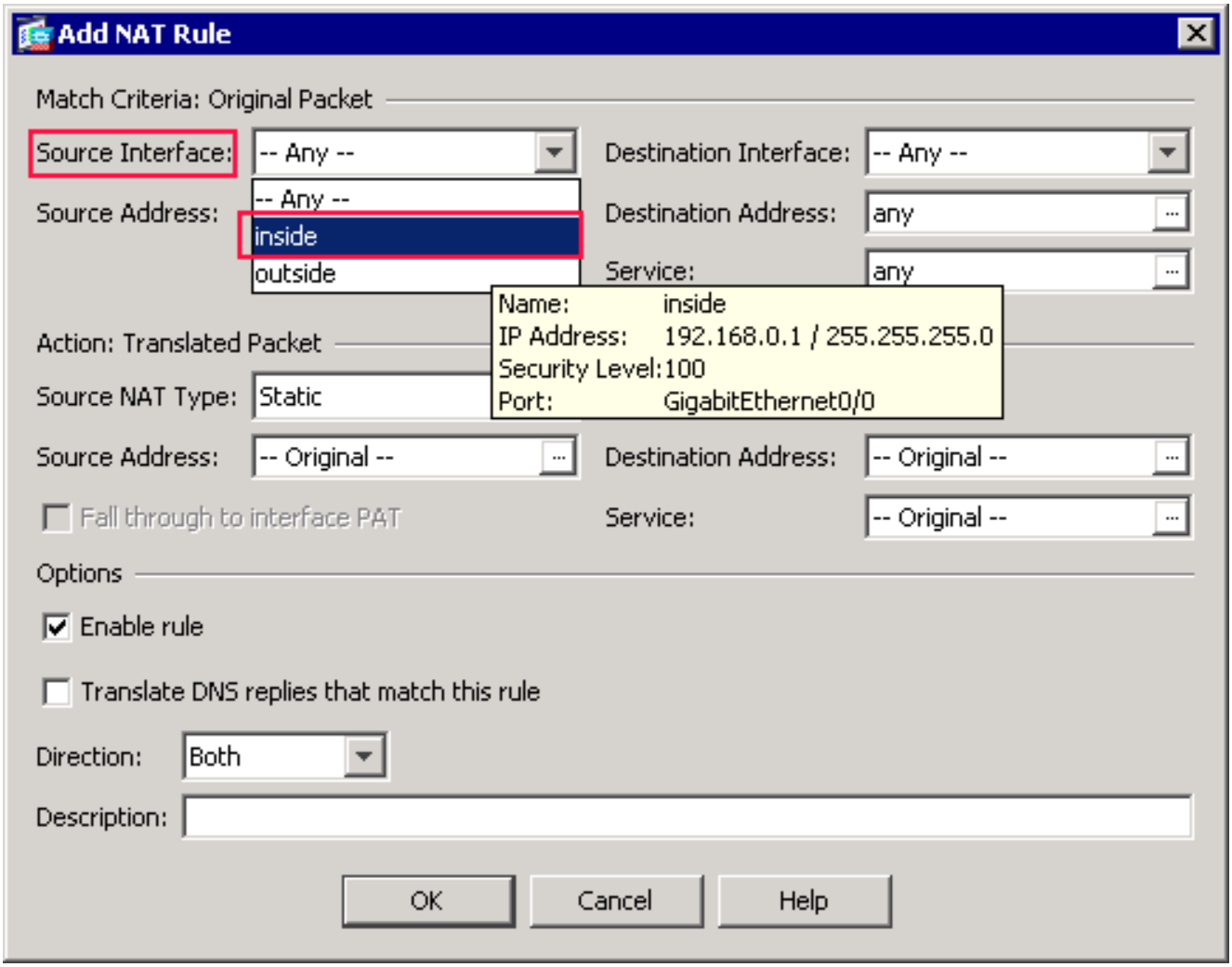
Cree las reglas NAT/PAT

Complete estos pasos para crear las reglas NAT/PAT:

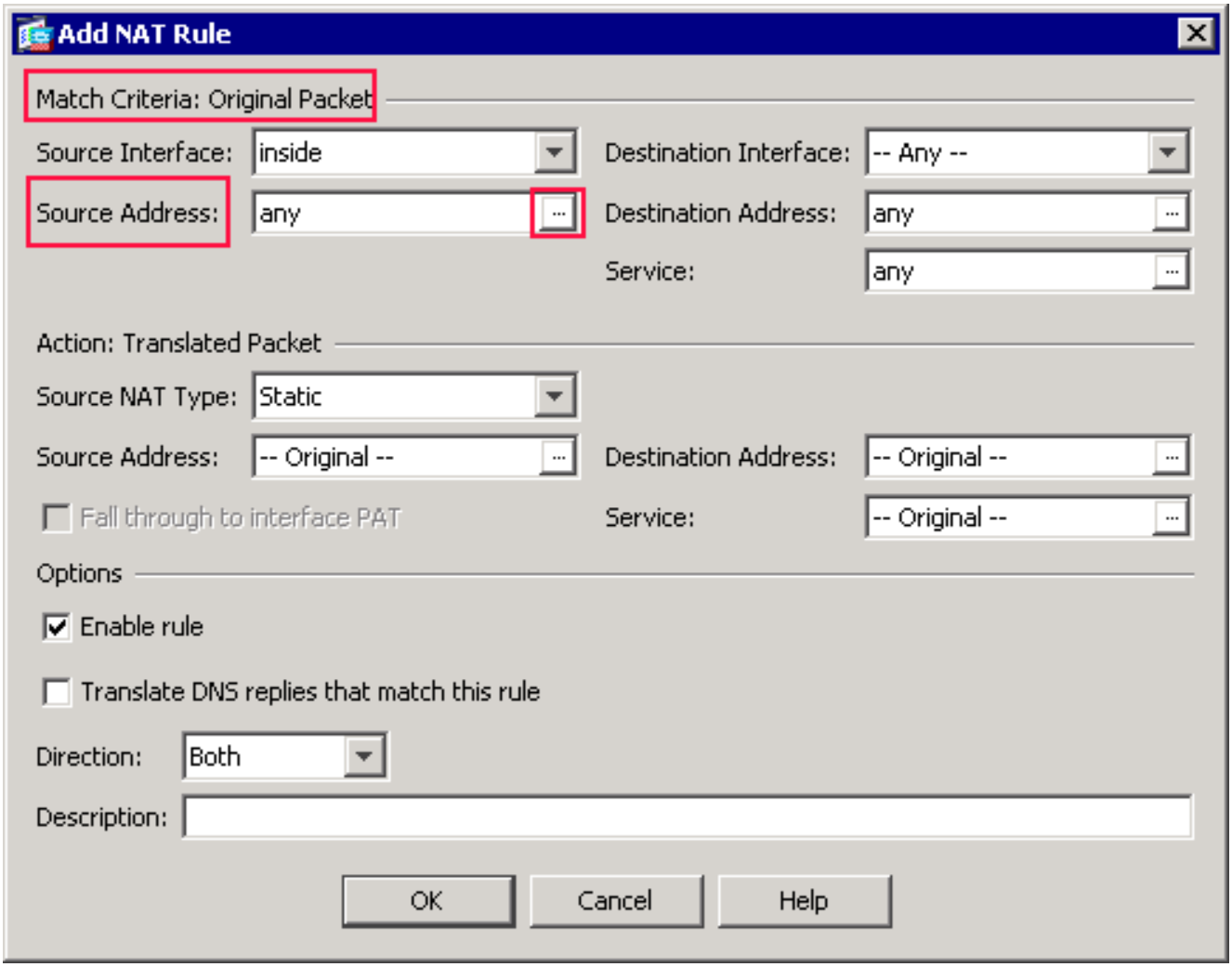
1. Cree la primera regla NAT/PAT:En el ASDM, elija la **configuración > el Firewall > las reglas NAT**, y el haga click en
   Add



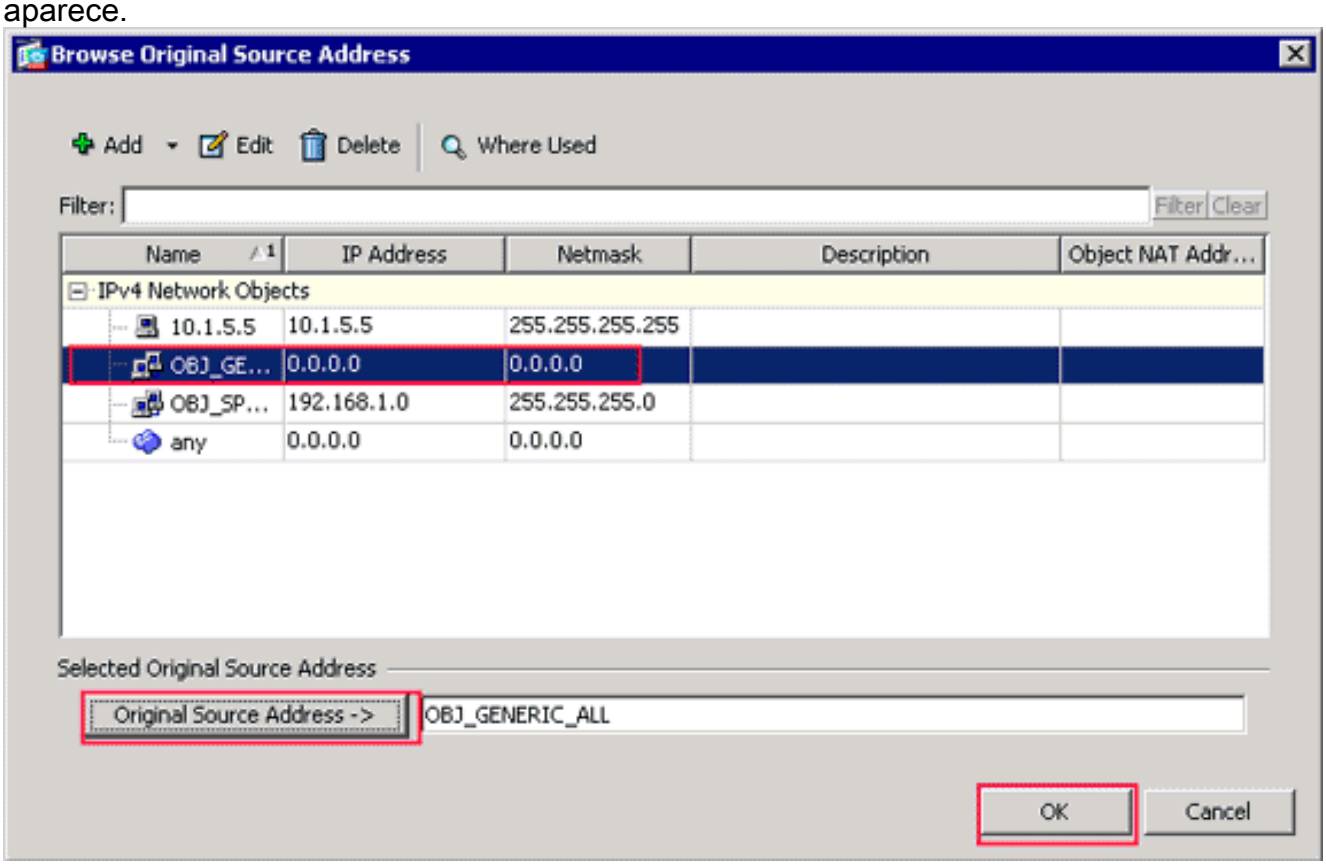
El cuadro de diálogo de la regla del agregar NAT aparece.



En los criterios de concordancia: El área del paquete original del cuadro de diálogo de la regla del agregar NAT, elige **dentro de la** lista desplegable de la interfaz de origen.

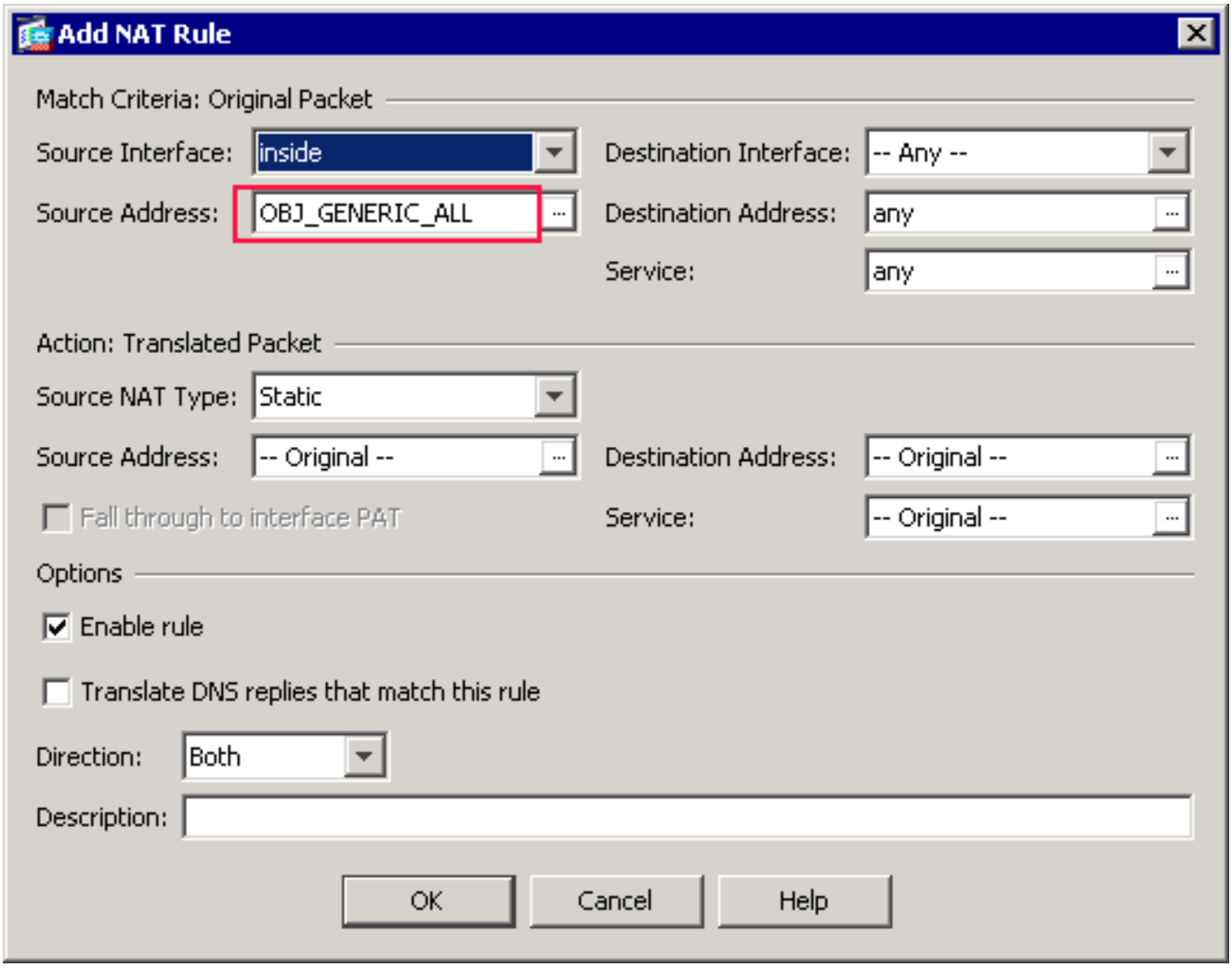


Haga clic la ojeada (...) abotone situado a la derecha del campo de texto de la dirección de origen.El cuadro de diálogo del direccionamiento de fuente original de la ojeada aparece.

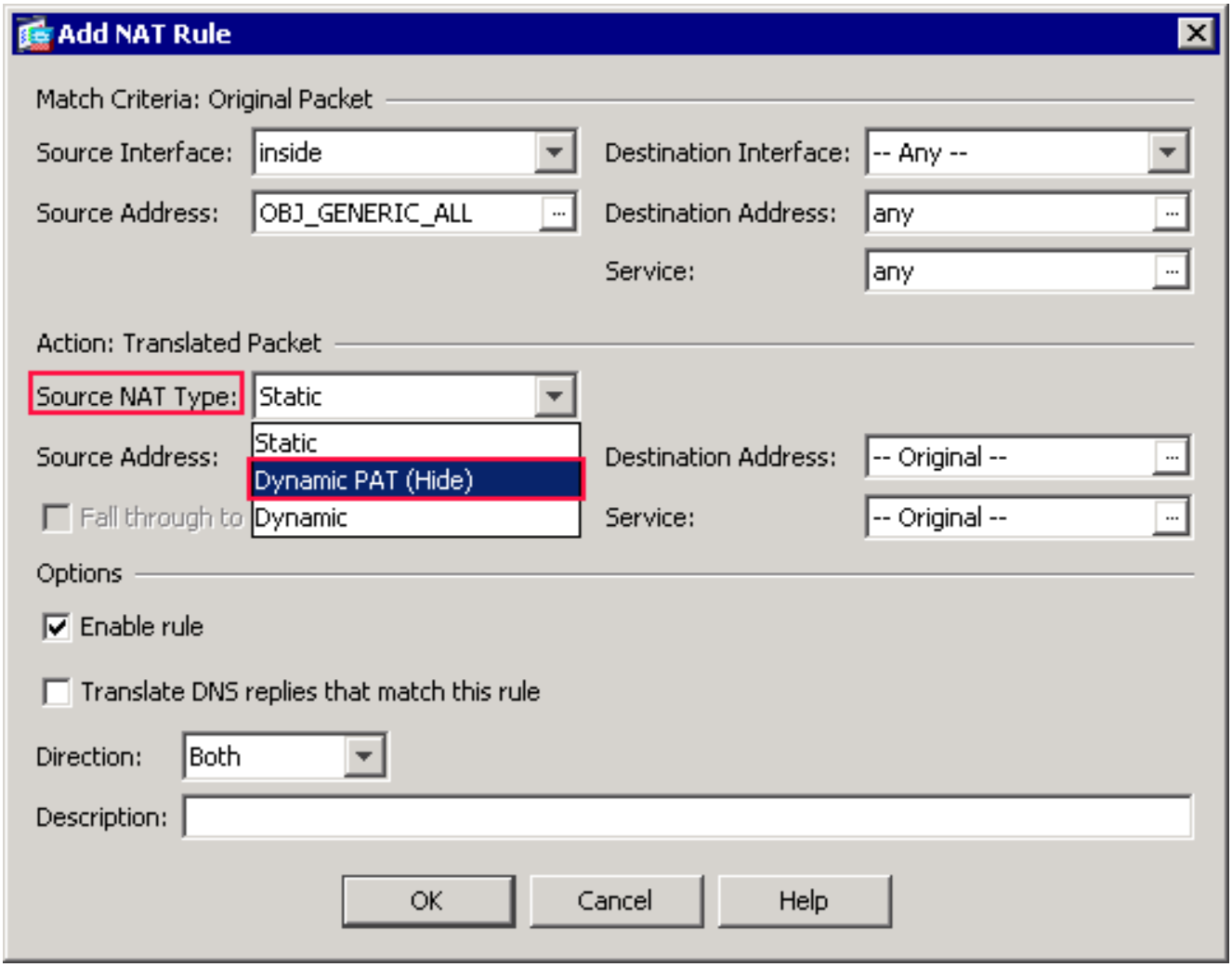


En el cuadro de diálogo del direccionamiento de fuente original de la ojeada, elija el primer

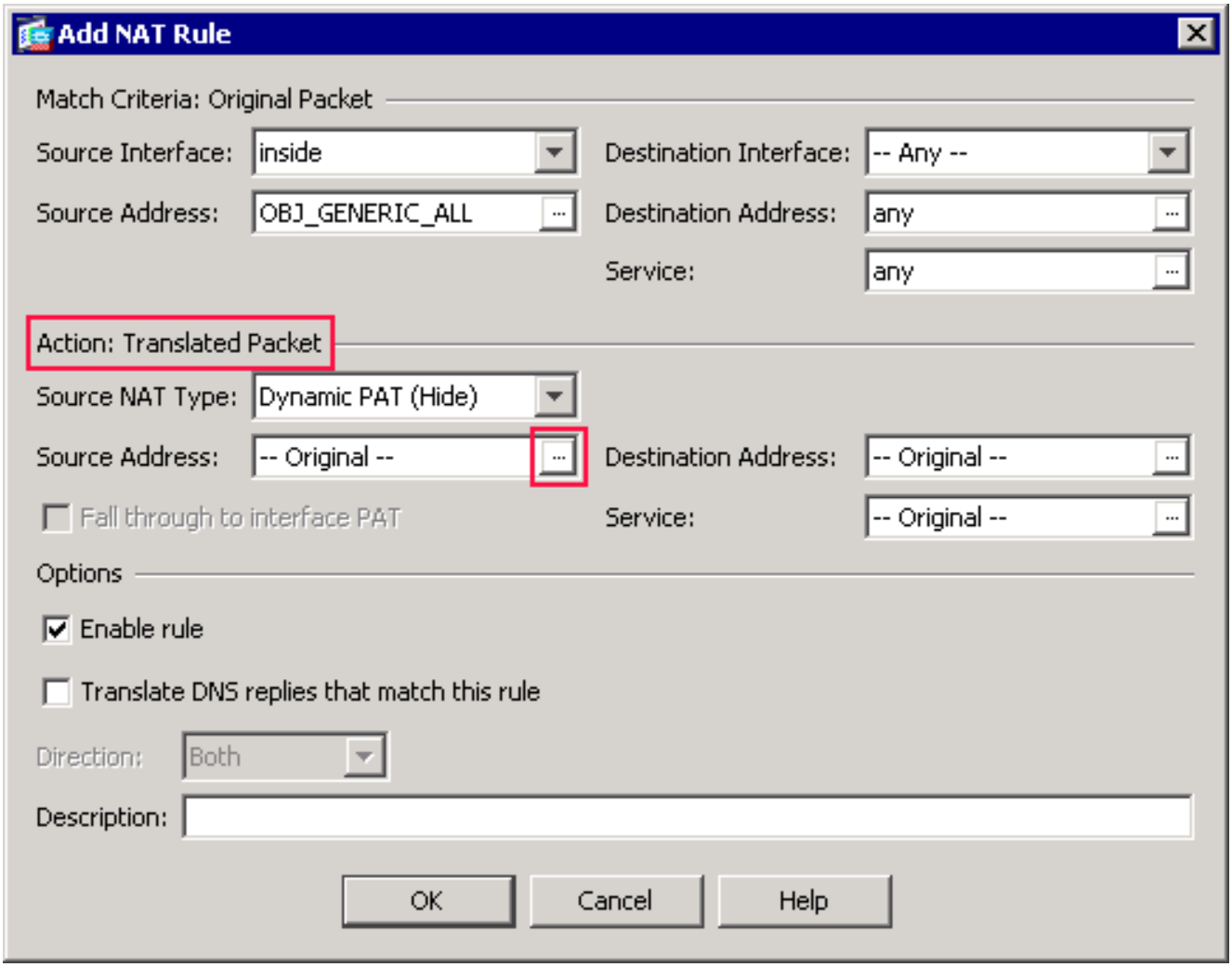
objeto de red que usted creó. (Por este ejemplo, elija **OBJ_GENERIC_ALL**.)Haga clic el **direccionamiento de fuente original**, y haga clic la **AUTORIZACIÓN**.El objeto de red *OBJ_GENERIC_ALL* ahora aparece en el campo de dirección de origen en los criterios de concordancia: Área del paquete original del cuadro de diálogo de la regla del agregar NAT.



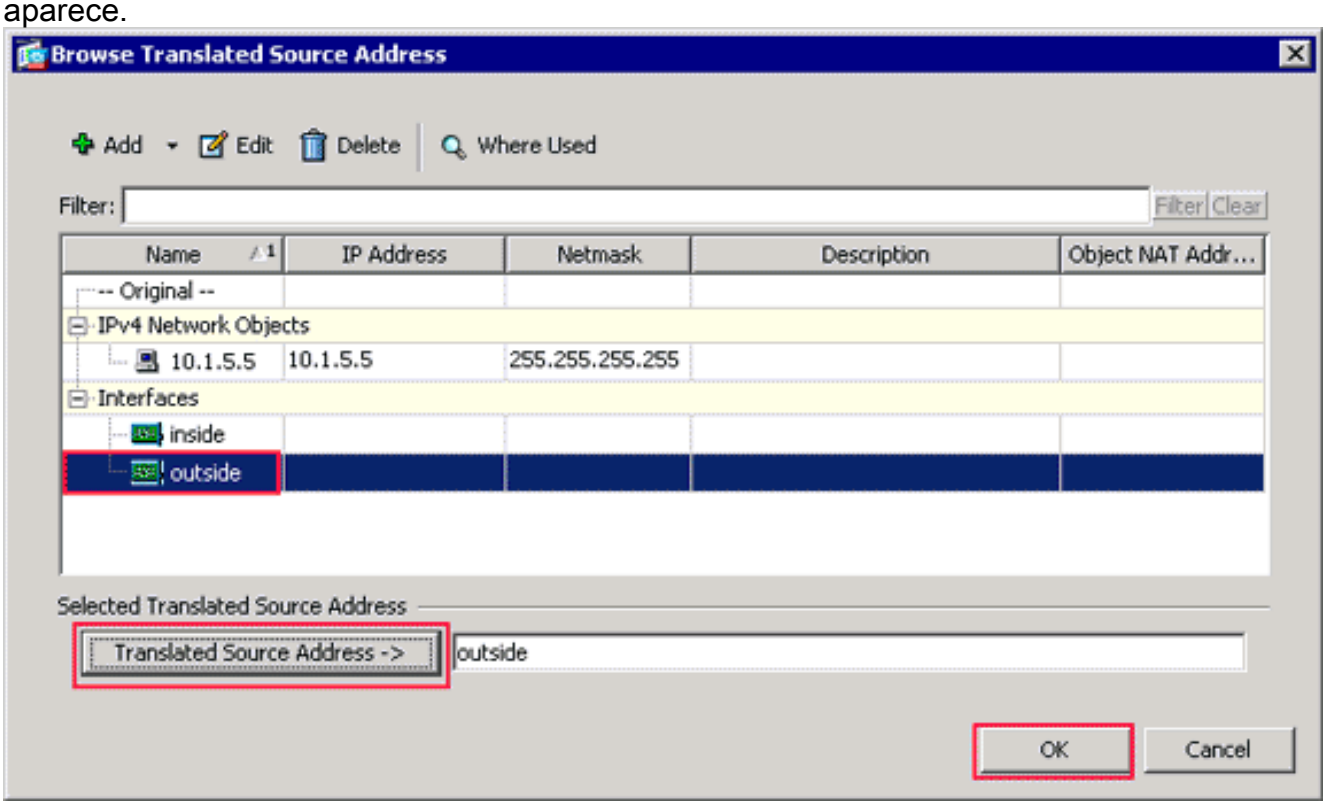
En la acción: El área traducida del paquete del cuadro de diálogo de la regla del agregar NAT, elige la **PALMADITA dinámica (piel) del** cuadro de diálogo del tipo de la fuente NAT.



Haga clic la ojeada (...) abotone situado a la derecha del campo de dirección de origen.

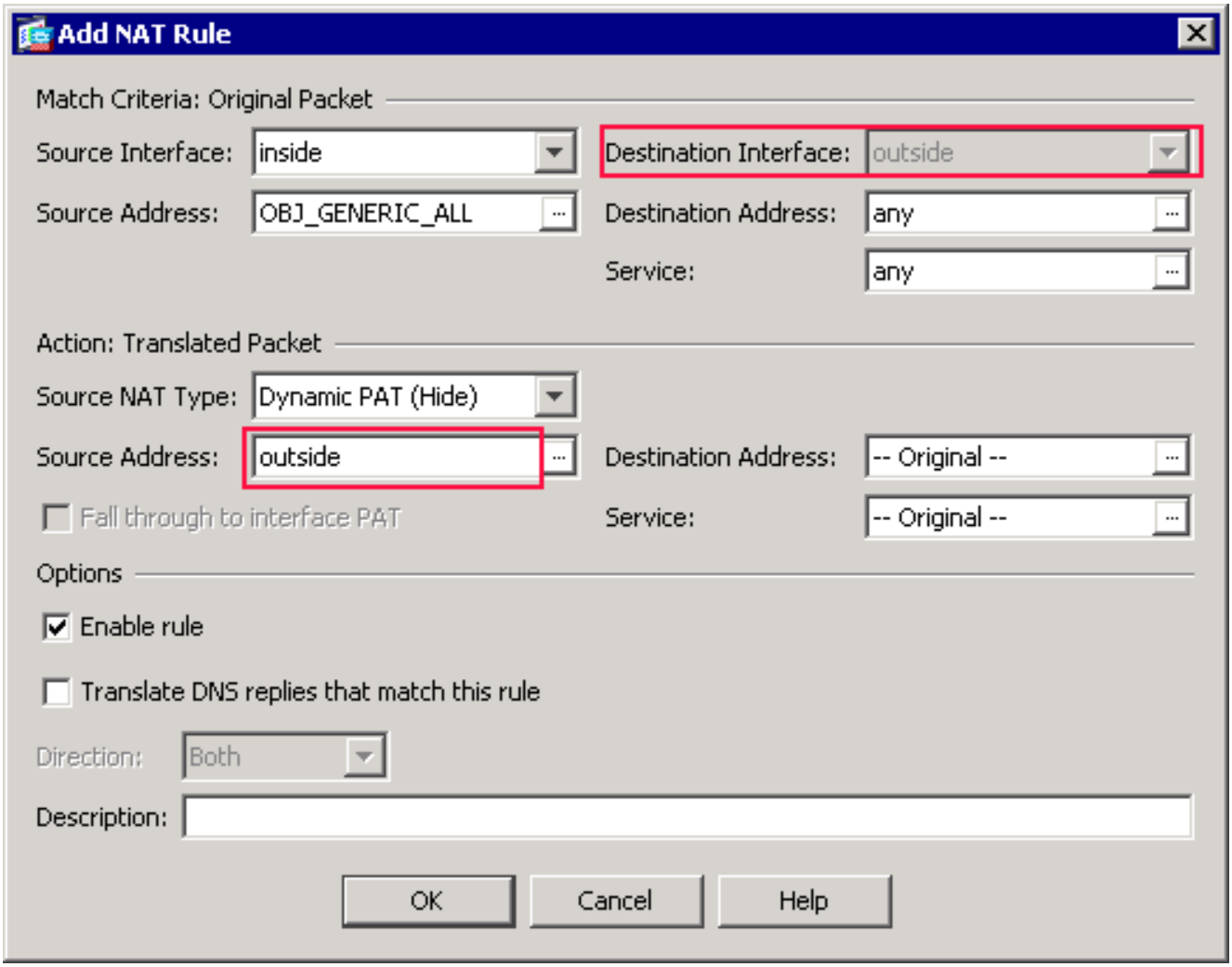


El cuadro de diálogo traducido ojeada de la dirección de origen aparece.

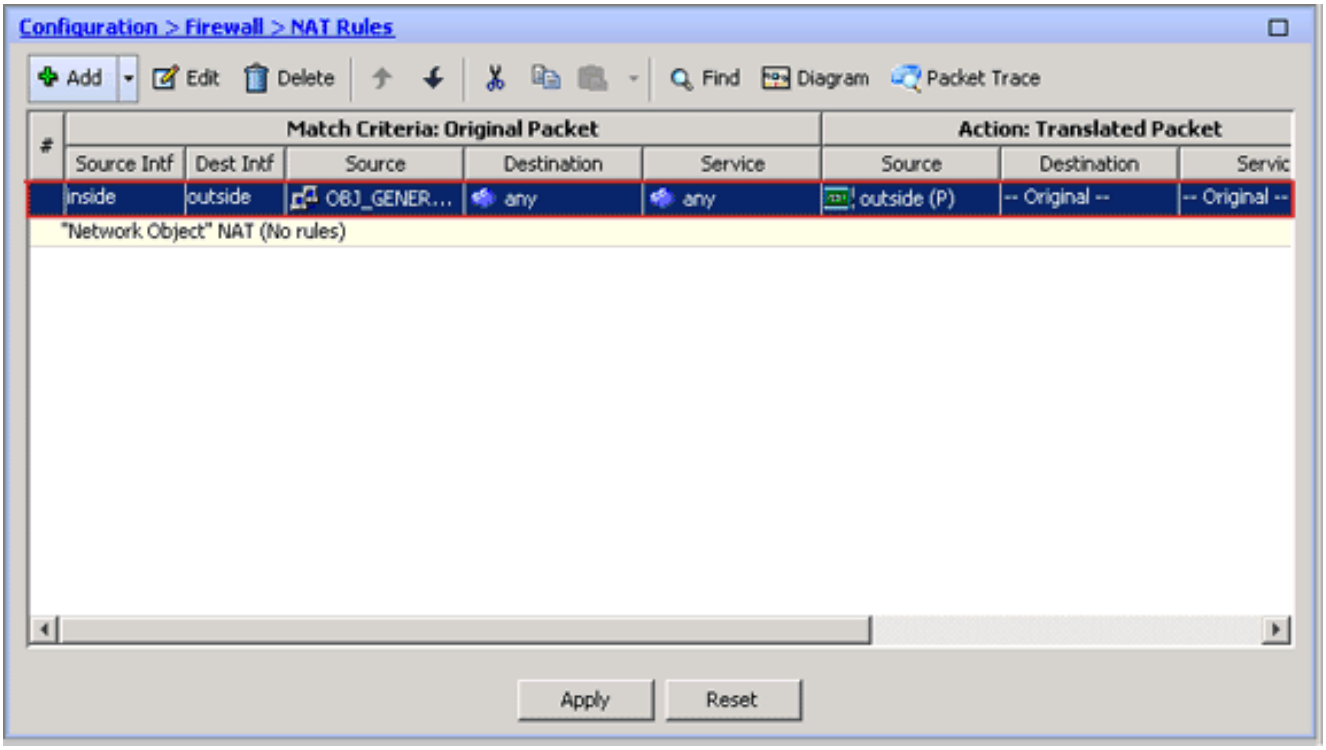


En la ojeada el cuadro de diálogo traducido de la dirección de origen, elige el objeto de la **interfaz exterior**. (Esta interfaz se ha creado ya porque es parte de la configuración de origen.)**Dirección de origen traducida** tecleo, y **AUTORIZACIÓN del** tecleo.La interfaz

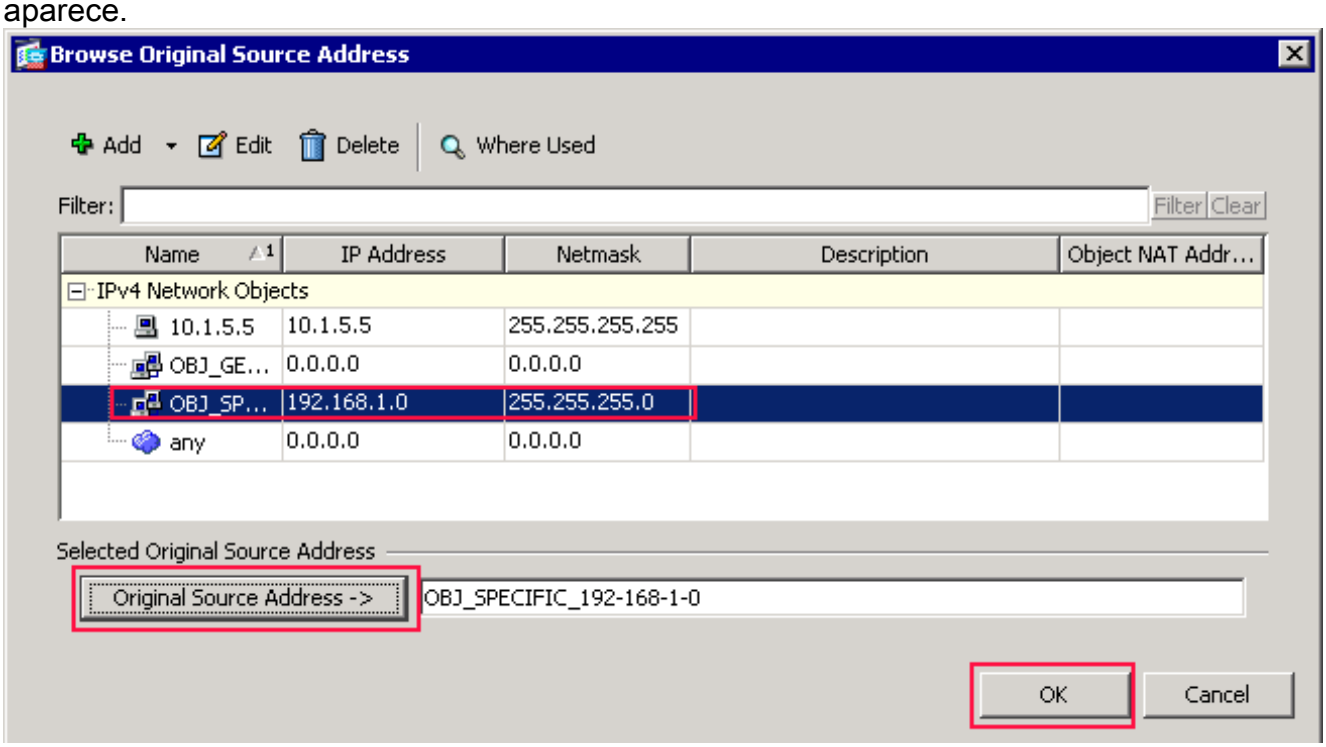
exterior ahora aparece en el campo de dirección de origen en la acción: Área traducida del paquete en el cuadro de diálogo de la regla del agregar
NAT.



Note: El campo de la *interfaz de destino* también cambia a la interfaz exterior.Verifique que aparezca la primera regla completada de la PALMADITA como sigue:En los criterios de concordancia: El área del paquete original, verifica estos valores:Interfaz de origen = dentroDirección de origen = OBJ_GENERIC_ALLDirección destino = ningunosServicio = ningunosEn la acción: El área traducida del paquete, verifica estos valores:Tipo de la fuente NAT = PALMADITA dinámica (piel)Dirección de origen = afueraDirección destino = originalServicio = originalClick OK.La primera regla NAT aparece en el ASDM, tal y como se muestra en de esta
imagen:

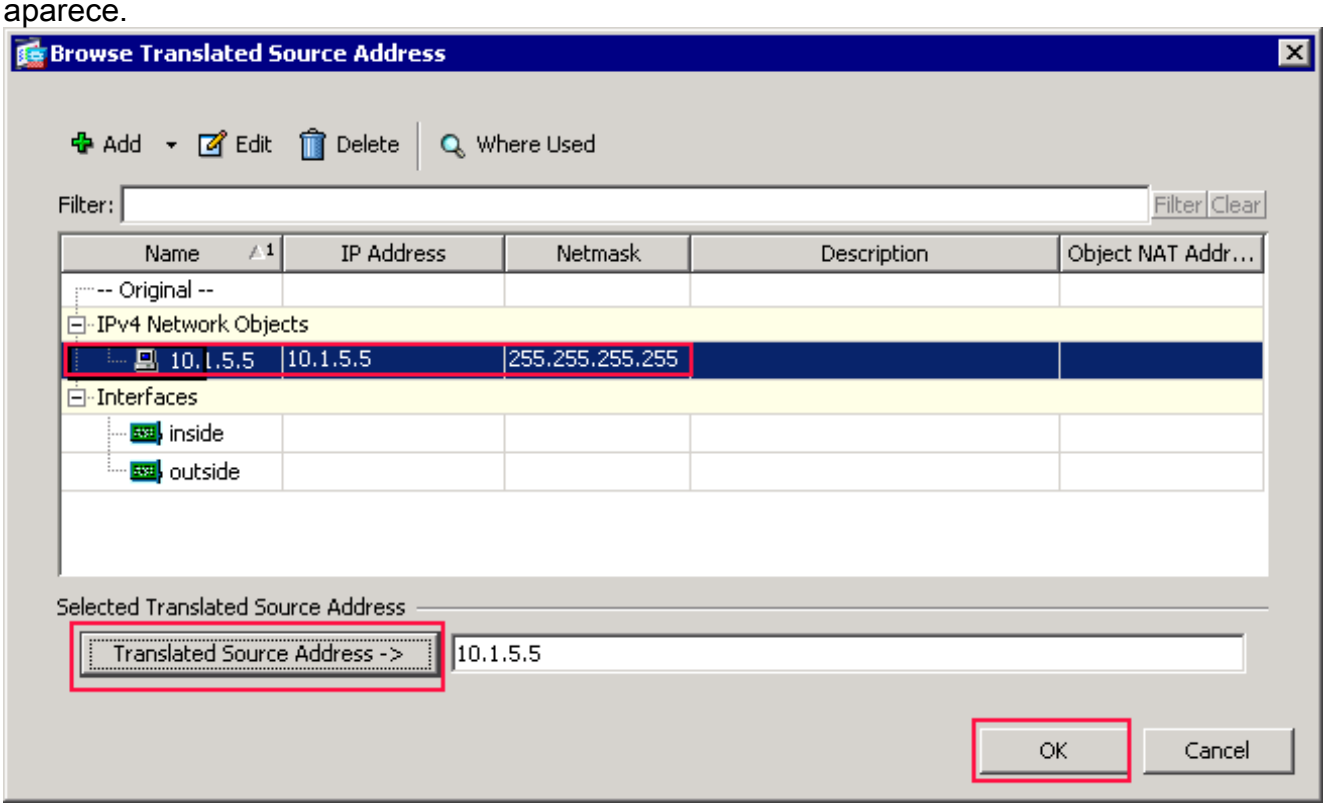


2. Cree la segunda regla NAT/PAT:En el ASDM, elija la **configuración > el Firewall > las reglas NAT**, y el haga click en AddEn los criterios de concordancia: El área del paquete original del cuadro de diálogo de la regla del agregar NAT, elige **dentro de la** lista desplegable de la interfaz de origen.Haga clic la ojeada (**...**) abotone situado a la derecha del campo de dirección de origen.El cuadro de diálogo del direccionamiento de fuente original de la ojeada aparece.

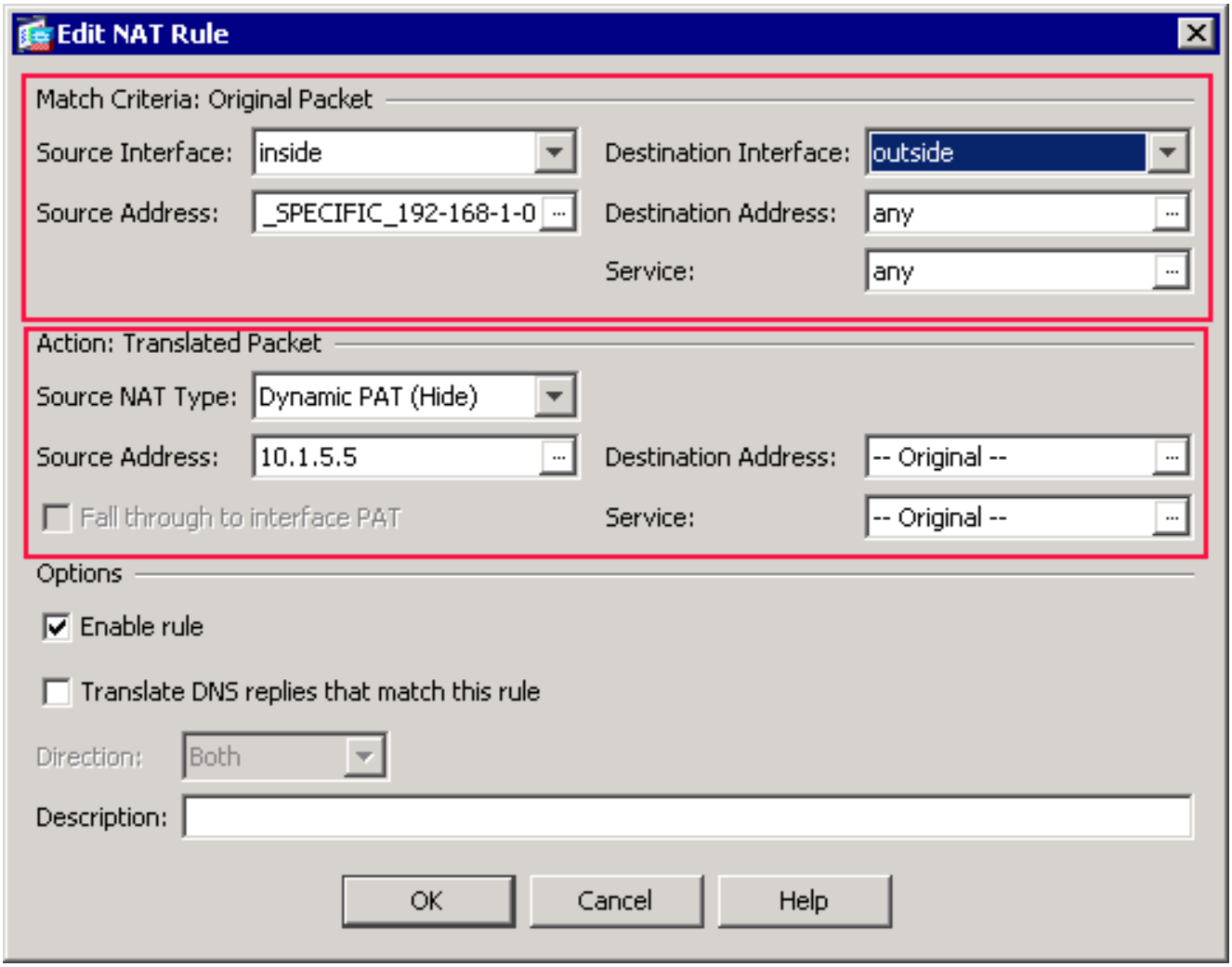


En el cuadro de diálogo del direccionamiento de fuente original de la ojeada, elija el segundo objeto que usted creó. (Por este ejemplo, elija **OBJ_SPECIFIC_192-168-1-0**.)Haga clic el **direccionamiento de fuente original**, y haga clic la **AUTORIZACIÓN**.El objeto de red *OBJ_SPECIFIC_192-168-1-0* aparece en el campo de dirección de origen en los criterios de concordancia: Área del paquete original del cuadro de diálogo de la regla del agregar NAT.En la acción: El área traducida del paquete del cuadro de diálogo de la regla del agregar NAT, elige la **PALMADITA dinámica (piel) del** cuadro de diálogo del tipo de la fuente

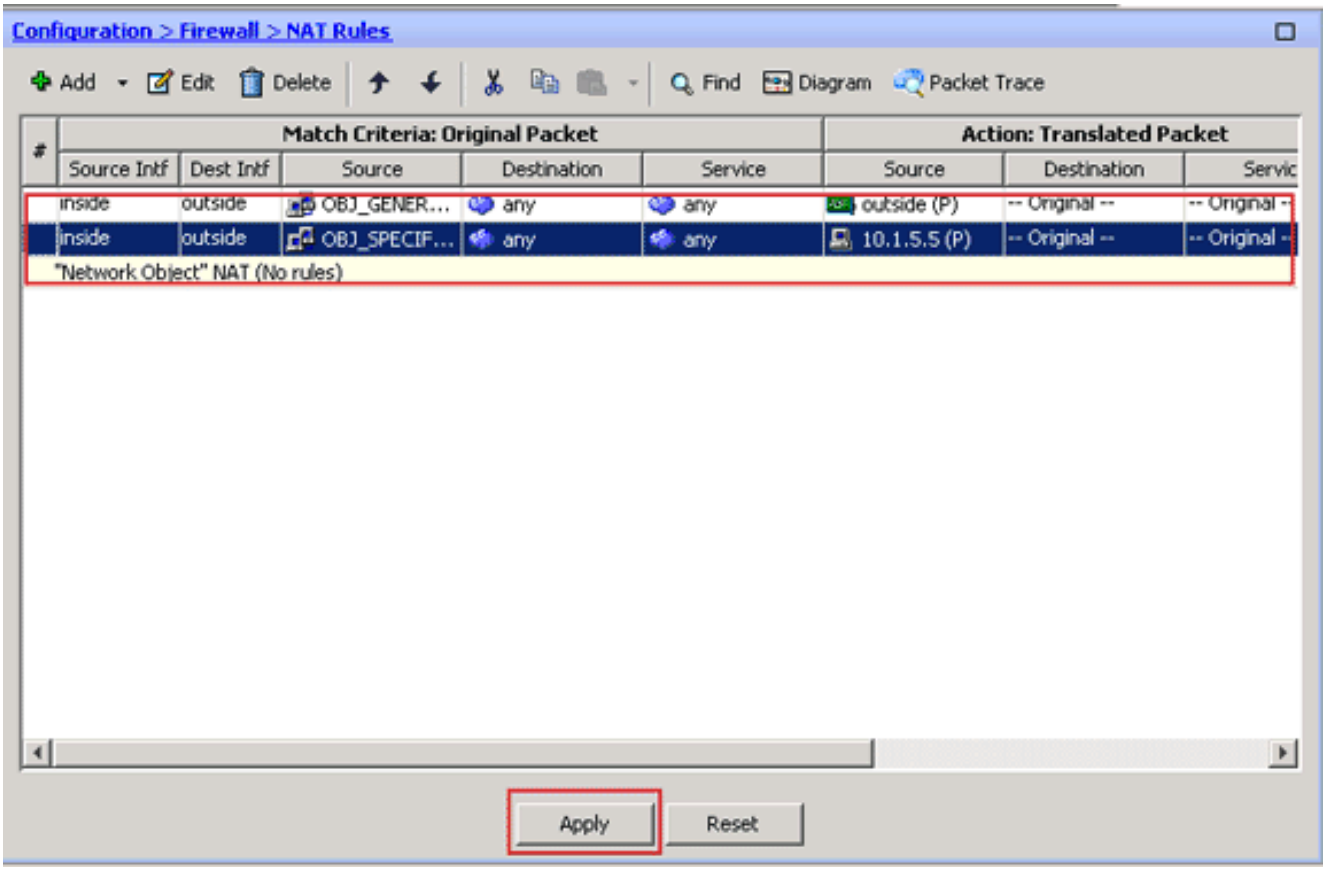
NAT.Haga clic**… el** botón situado a la derecha del campo de dirección de origen.El cuadro de diálogo traducido ojeada de la dirección de origen
aparece.



En la ojeada el cuadro de diálogo traducido de la dirección de origen, elige el objeto de **10.1.5.5**. (Esta interfaz se ha creado ya porque es parte de la configuración de origen).Haga clic a la **dirección de origen traducida**, y después haga clic la **AUTORIZACIÓN**.El objeto de red de **10.1.5.5** aparece en el campo de dirección de origen en la acción: Área traducida del paquete del cuadro de diálogo de la regla del agregar NAT.En los criterios de concordancia: El área del paquete original, elige **afuera de la** lista desplegable de la interfaz de destino.**Note**: Si usted no elige *afuera* para esta opción, la interfaz de destino se referirá a *ningunos*.



Verifique que aparezca la segunda regla completada NAT/PAT como sigue:En los criterios de concordancia: El área del paquete original, verifica estos valores:Interfaz de origen = dentroDirección de origen = OBJ_SPECIFIC_192-168-1-0Dirección destino = afueraServicio = ningunosEn la acción: El área traducida del paquete, verifica estos valores:Tipo de la fuente NAT = PALMADITA dinámica (piel)Dirección de origen = 10.1.5.5Dirección destino = originalServicio = originalClick OK.La configuración del NAT completada aparece en el ASDM, tal y como se muestra en de esta
imagen:



3. Haga clic el **botón Apply Button** para aplicar los cambios a la configuración corriente.

Esto completa la configuración de la PALMADITA dinámica en un dispositivo de seguridad adaptante de Cisco (ASA).

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

Verificar la regla genérica de la PALMADITA

- host local de la demostración — Muestra a los estados de la red de host locales.

```
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 — Muestra al estado de la conexión para el Tipo de conexión señalado.

```
ASA#show conn
2 in use, 3 most used
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
```

- xlate de la demostración — Muestra la información sobre los slots de traducción.

```
ASA#show xlate
4 in use, 7 most used
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
```

Verificar la regla específica de la PALMADITA

- host local de la demostración — Muestra a los estados de la red de host locales.

```
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 — Muestra al estado de la conexión para el Tipo de conexión señalado.

```
ASA#show conn
2 in use, 3 most used
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
```

- xlate de la demostración — Muestra la información sobre los slots de traducción.

```
ASA#show xlate
3 in use, 9 most used
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
```

Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- Cisco Adaptive Security Device Manager
- Cisco ASA 5500 Series Adaptive Security Appliances
- Solicitudes de Comentarios (RFC)
- Soporte Técnico y Documentación - Cisco Systems