Esempio di ASA 8.3(x) Dynamic PAT con due reti interne e configurazione Internet

Sommario

Introduzione

In questo documento viene fornita una configurazione di esempio per una porta dinamica su una appliance Cisco Adaptive Security (ASA) con software versione 8.3(1). PAT dinamico converte più indirizzi reali in un singolo indirizzo IP mappato convertendo l'indirizzo e la porta di origine reali nell'indirizzo mappato e nella porta mappata univoca. Ogni connessione richiede una sessione di conversione separata perché la porta di origine è diversa per ogni connessione.

Prerequisiti

Requisiti

Prima di provare questa configurazione, accertarsi di soddisfare i seguenti requisiti:

- Verificare che la rete interna abbia due reti posizionate all'interno dell'appliance ASA:192.168.0.0/24: rete connessa direttamente all'appliance ASA.192.168.1.0/24: dalla rete all'interno dell'ASA, ma dietro un altro dispositivo (ad esempio, un router).
- Assicurarsi che gli utenti interni ricevano PAT come segue:Gli host della subnet 192.168.1.0/24 otterranno PAT da un indirizzo IP di riserva fornito dall'ISP (10.1.5.5).Tutti gli altri host dietro l'appliance ASA ricevono il pacchetto PAT all'indirizzo IP dell'interfaccia esterna dell'appliance (10.1.5.1).

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Adaptive Security Appliance (ASA) con versione 8.3(1)
- ASDM versione 6.3(1)

Nota: per consentire all'ASDM di configurare l'appliance ASA, consultare il documento sull'autorizzazione dell'accesso HTTPS per ASDM.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

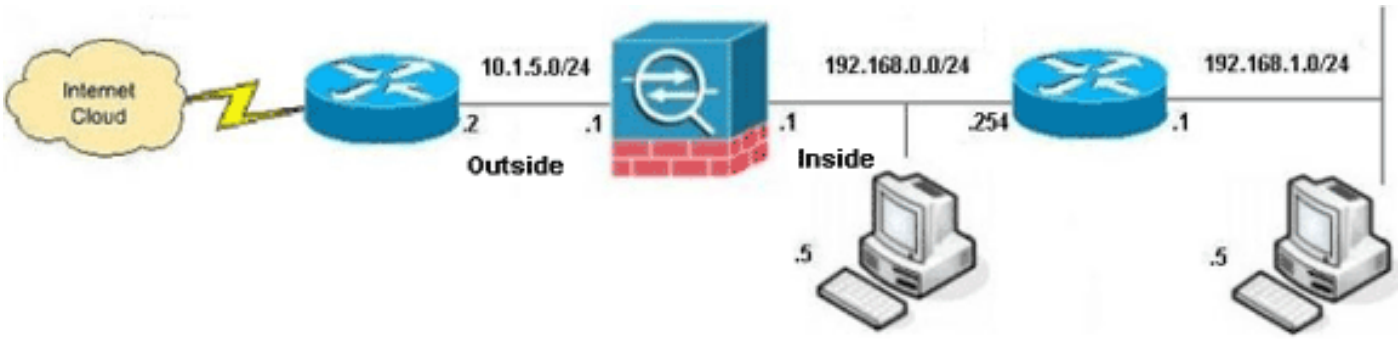
Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per informazioni sulle convenzioni dei documenti.

Configurazione

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Nota: gli schemi di indirizzamento IP utilizzati in questa configurazione non sono legalmente instradabili su Internet. Si tratta degli indirizzi RFC 1918 utilizzati in un ambiente lab.

- Configurazione ASA CLI
- Configurazione ASDM

Configurazione ASA CLI

Questo documento utilizza le configurazioni mostrate di seguito.

Configurazione percorso dinamico 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
```

ASA 8.3(1) con configurazione in esecuzione

```
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
```

Configurazione ASDM

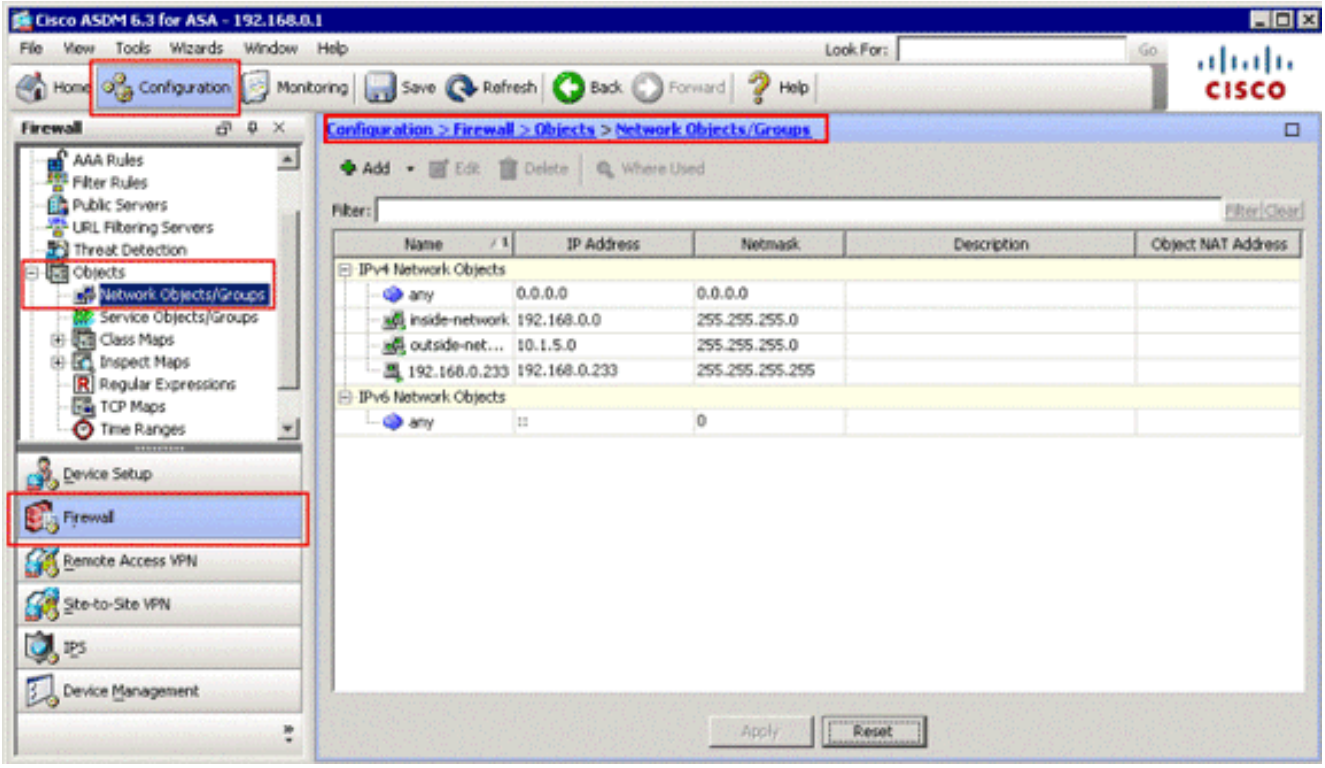
Per completare la configurazione tramite l'interfaccia ASDM, è necessario:

1. Aggiungere tre oggetti di rete. in questo esempio vengono aggiunti i seguenti oggetti di rete:OBJ_GENERIC_ALLOBJ_SPECIFIC_192-168-1-010.1.5.5
2. Creare due regole NAT/PAT; in questo esempio vengono create regole NAT per questi oggetti di rete:OBJ_GENERIC_ALLOBJ_SPECIFIC_192-168-1-0

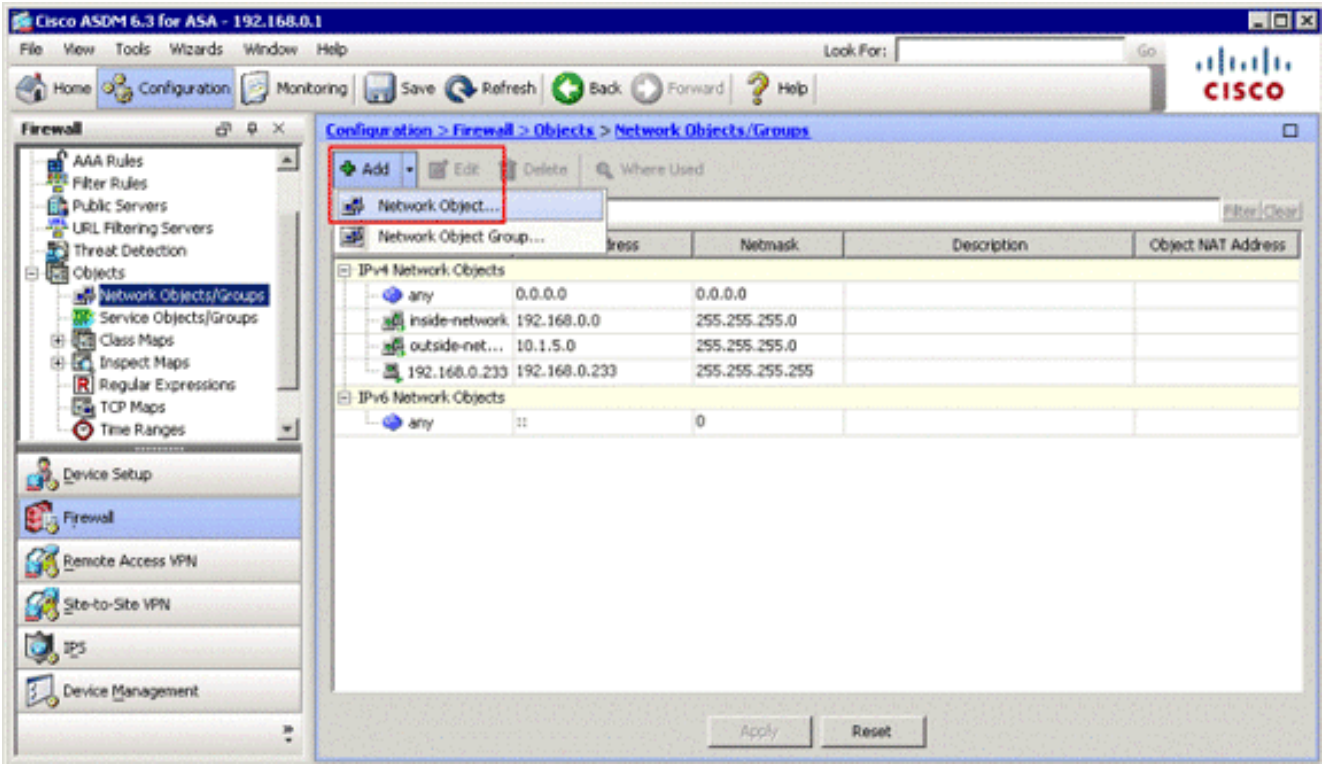
Aggiungi oggetti di rete

Per aggiungere oggetti di rete, completare i seguenti passaggi:

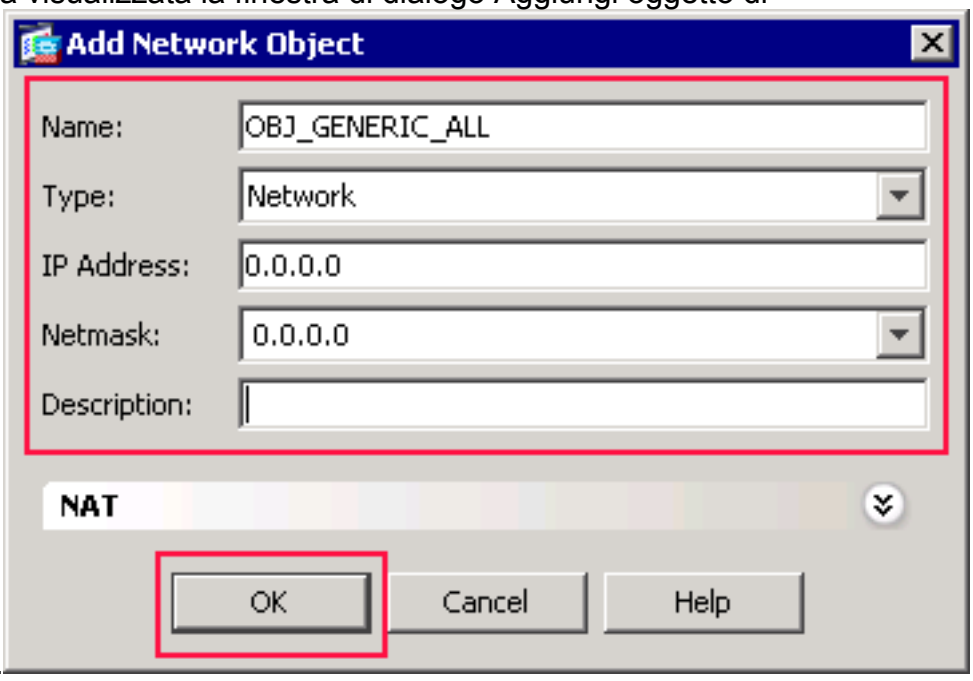
1. Accedere a ASDM e scegliere **Configurazione > Firewall > Oggetti > Oggetti/gruppi di rete**.



2. Per aggiungere un oggetto di rete, scegliere **Aggiungi > Oggetto** di rete.

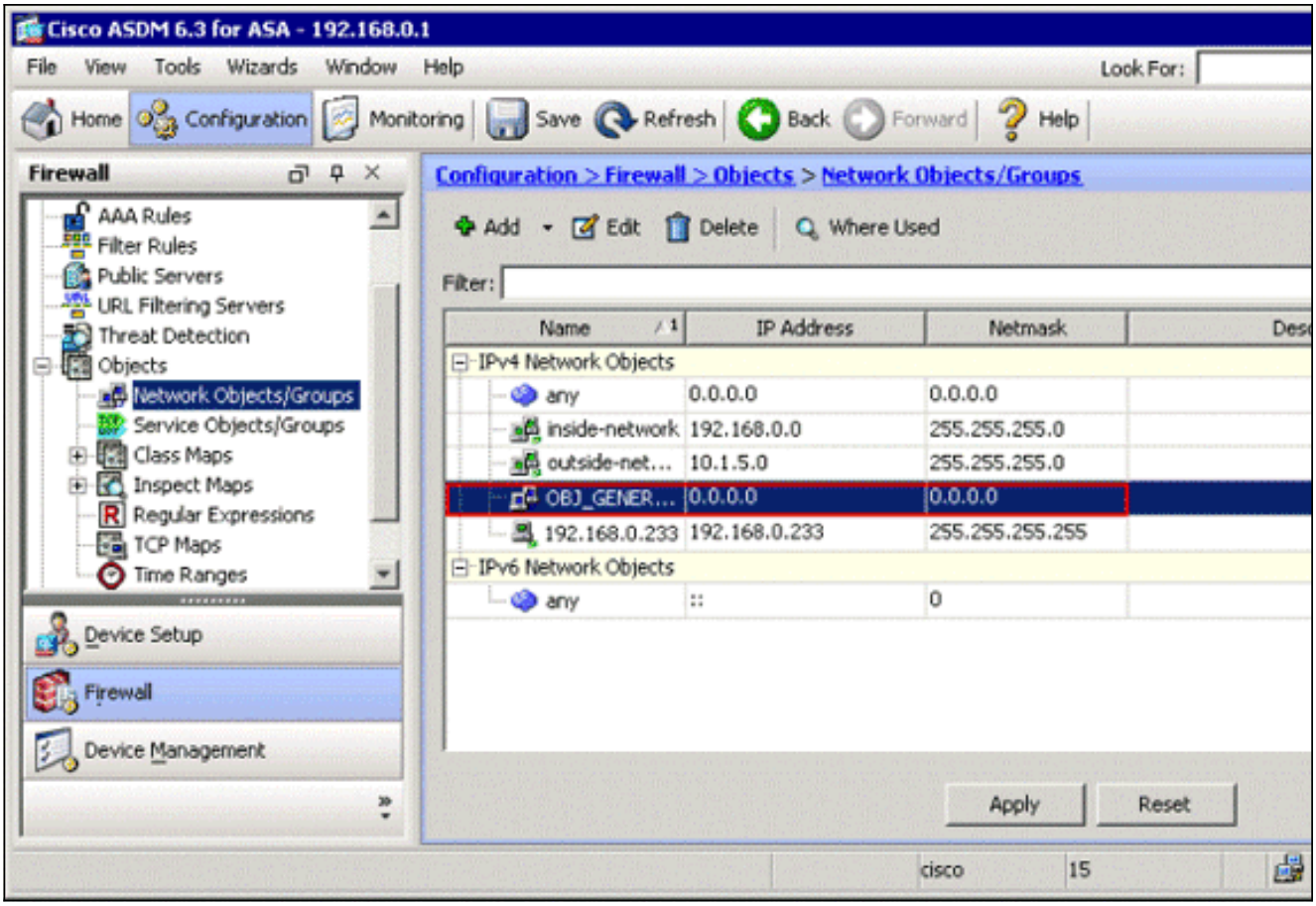


Verrà visualizzata la finestra di dialogo Aggiungi oggetto di

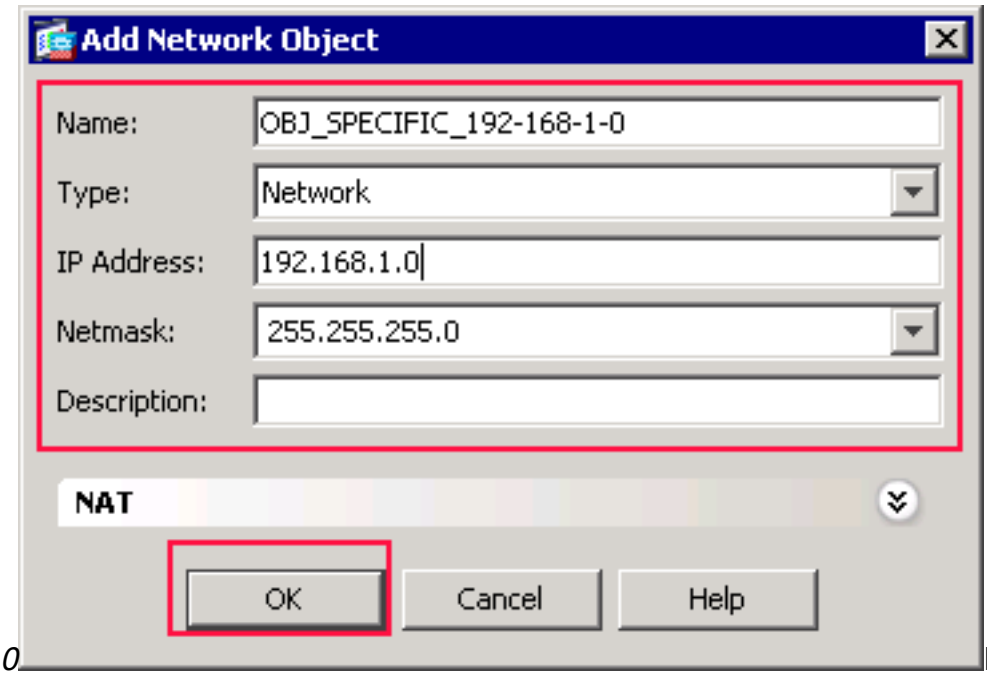


rete.

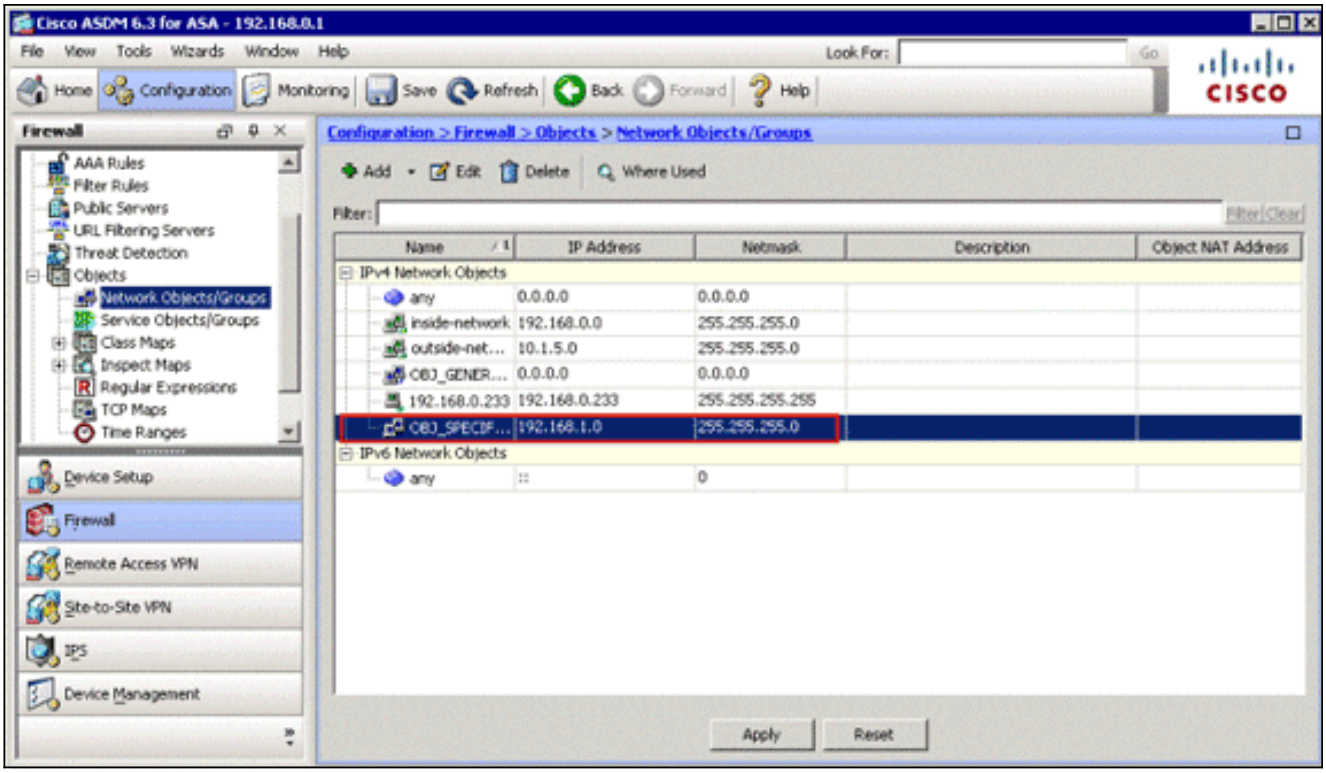
3. Immettere queste informazioni nella finestra di dialogo Aggiungi oggetto di rete:Nome dell'oggetto di rete. In questo esempio viene utilizzato *OBJ_GENERIC_ALL*.Tipo di oggetto di rete. In questo esempio viene utilizzato *Network*.Indirizzo IP dell'oggetto di rete. In questo esempio viene utilizzato *0.0.0.0*.Maschera di rete per l'oggetto di rete. In questo esempio viene utilizzato *0.0.0.0*.
4. Fare clic su **OK**.L'oggetto di rete viene creato e visualizzato nell'elenco Oggetti/gruppi di rete, come mostrato nell'immagine
seguente:



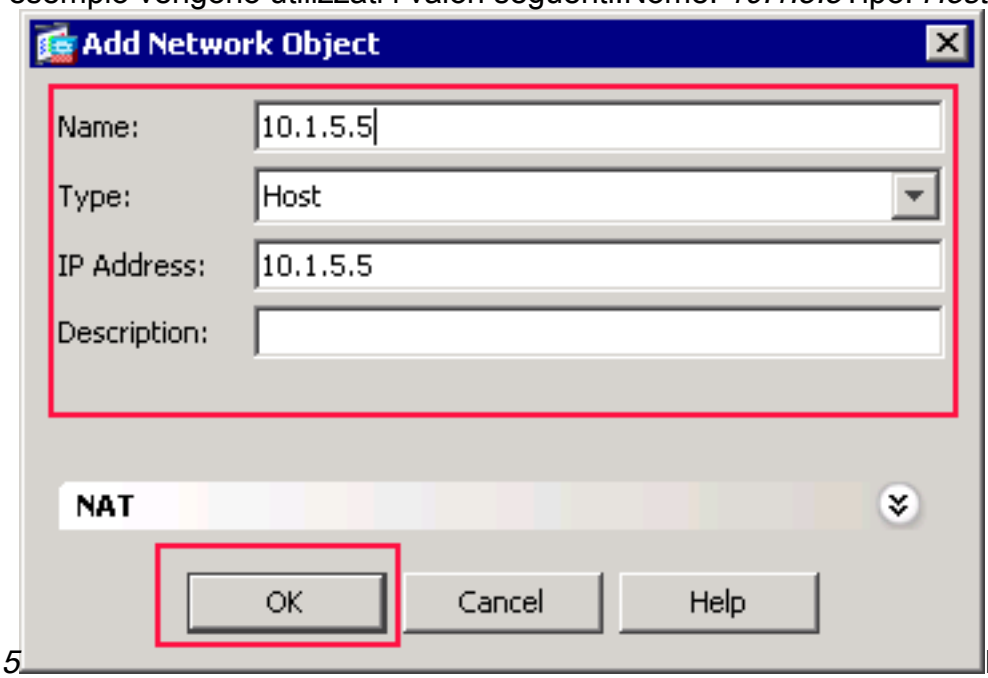
5. Ripetere i passaggi precedenti per aggiungere un secondo oggetto di rete e fare clic su **OK**.In questo esempio vengono utilizzati i valori seguenti:Nome: *OBJ_SPECIFIC_192-168-1-0*Tipo: *Rete*Indirizzo IP: *192.168.1.0*Maschera di rete:



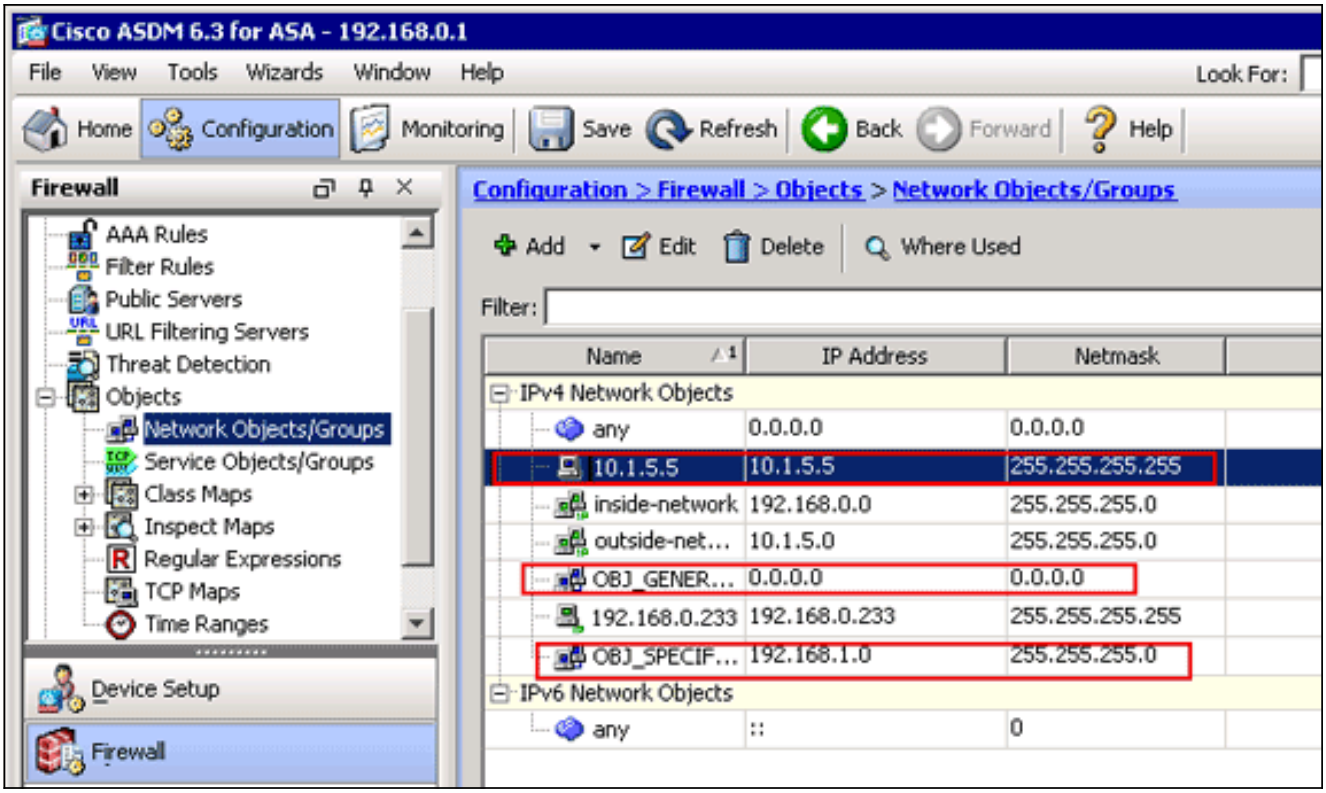
*255.255.255.0*Il secondo oggetto viene creato e visualizzato nell'elenco Oggetti/gruppi di rete, come mostrato nell'immagine
seguente:



6. Ripetere i passaggi precedenti per aggiungere un terzo oggetto di rete e fare clic su **OK**.In questo esempio vengono utilizzati i valori seguenti:Nome: *10.1.5.5*Tipo: *Host*Indirizzo IP:



*10.1.5.5*Il terzo oggetto di rete viene creato e visualizzato nella lista Oggetti/gruppi di rete.

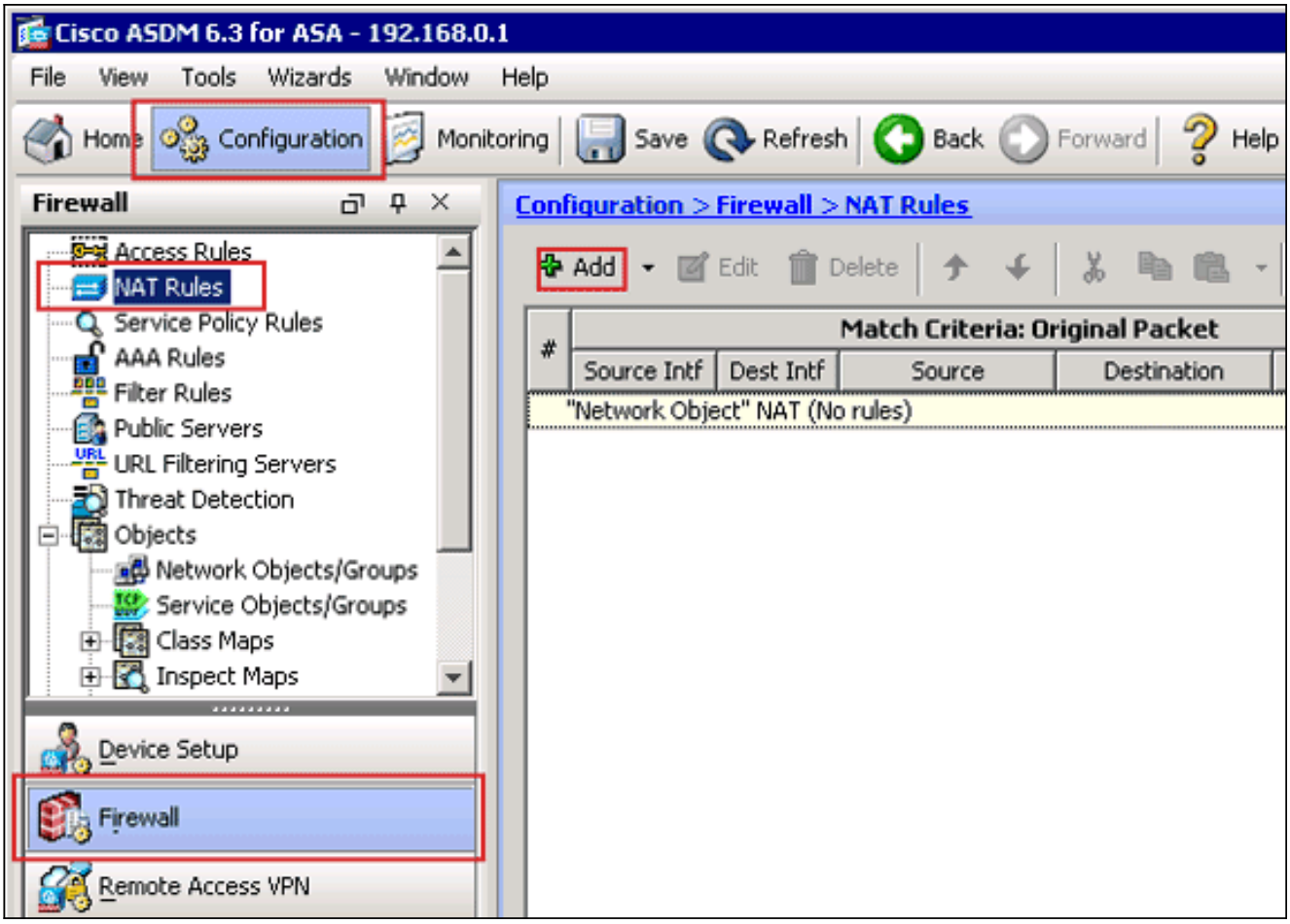


L'elenco Oggetti/gruppi di rete deve ora includere i tre oggetti necessari per il riferimento alle regole NAT.

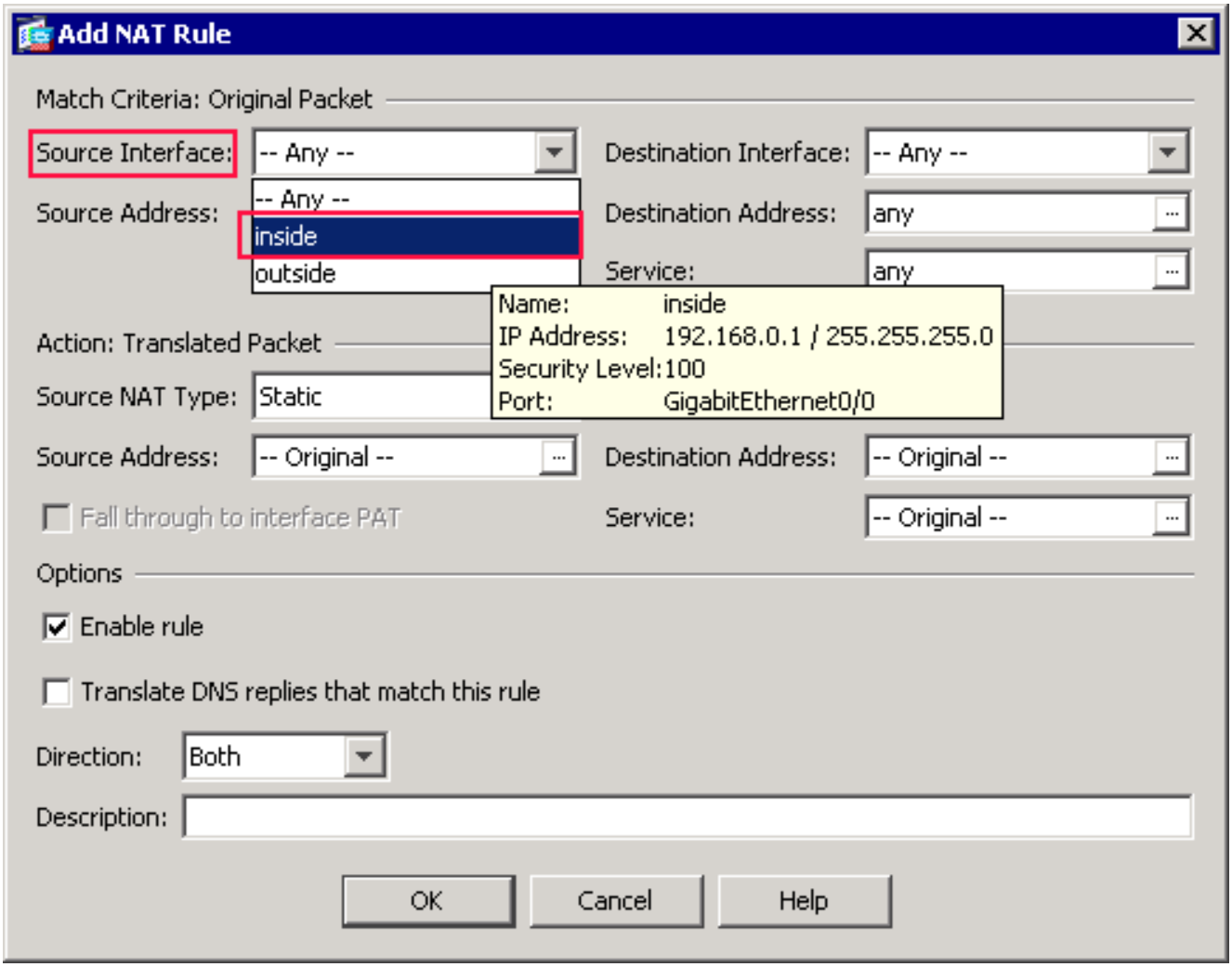
Crea regole NAT/PAT

Completare questi passaggi per creare le regole NAT/PAT:

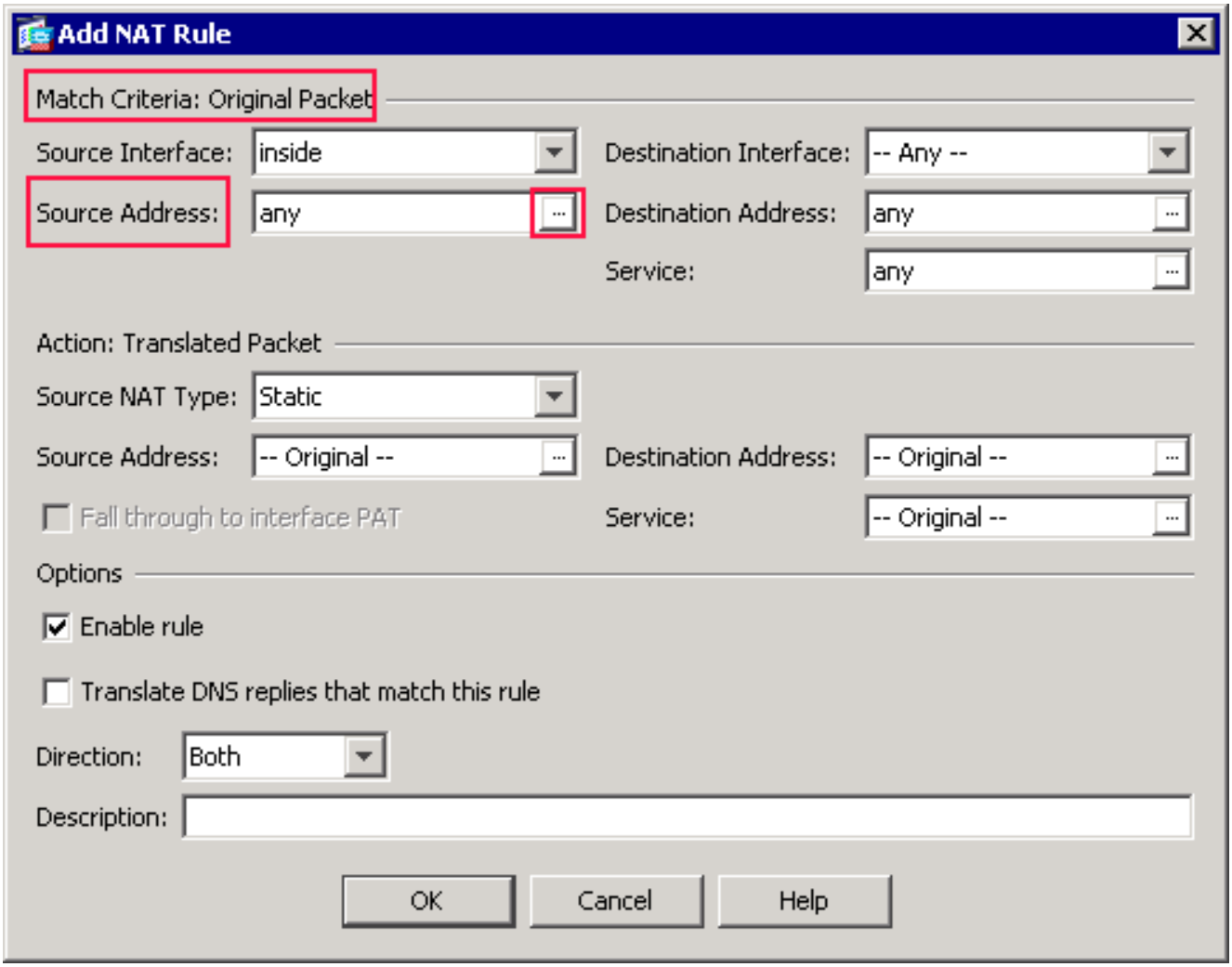
1. Creare la prima regola NAT/PAT:In ASDM, scegliere **Configurazione > Firewall > Regole NAT**, quindi fare clic su **Aggiungi**.



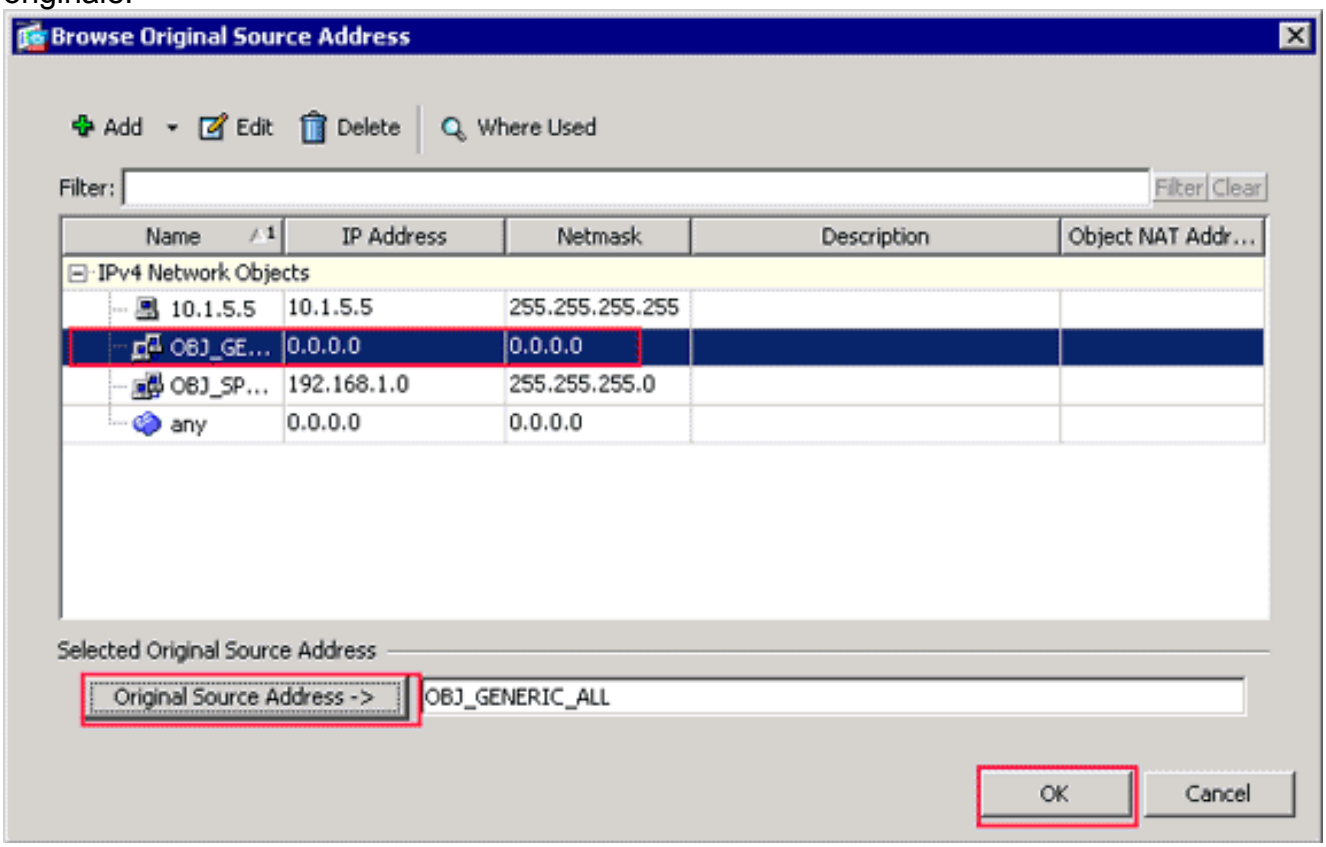
Verrà visualizzata la finestra di dialogo Aggiungi regola NAT.



Nella finestra di dialogo Criteri di corrispondenza: Nell'area Pacchetto originale della finestra di dialogo Aggiungi regola NAT, scegliere **all'interno** dall'elenco a discesa Interfaccia origine.

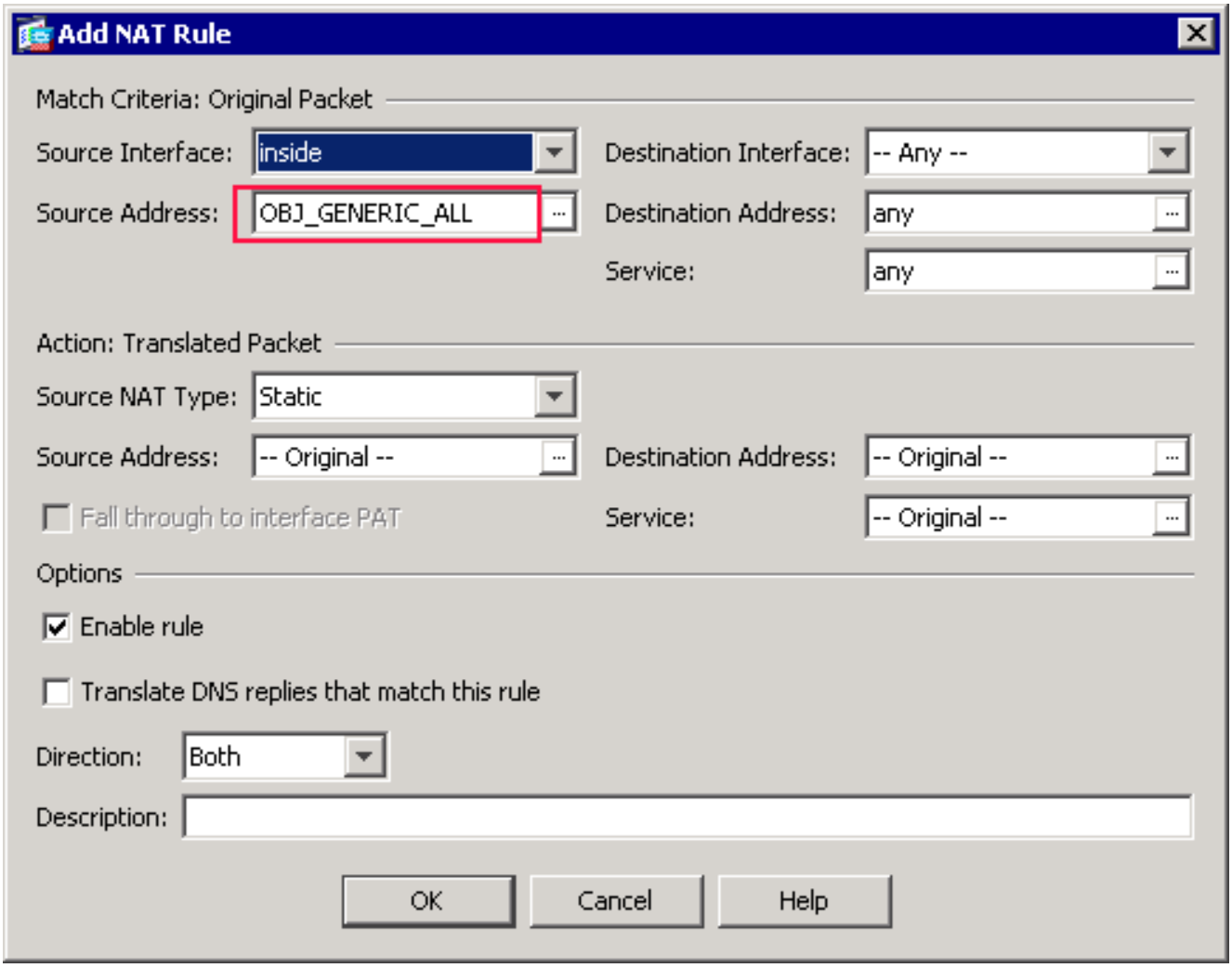


Fare clic sul pulsante Sfoglia (**...**) situato a destra del campo di testo Indirizzo di origine.Verrà visualizzata la finestra di dialogo Sfoglia indirizzo di origine originale.

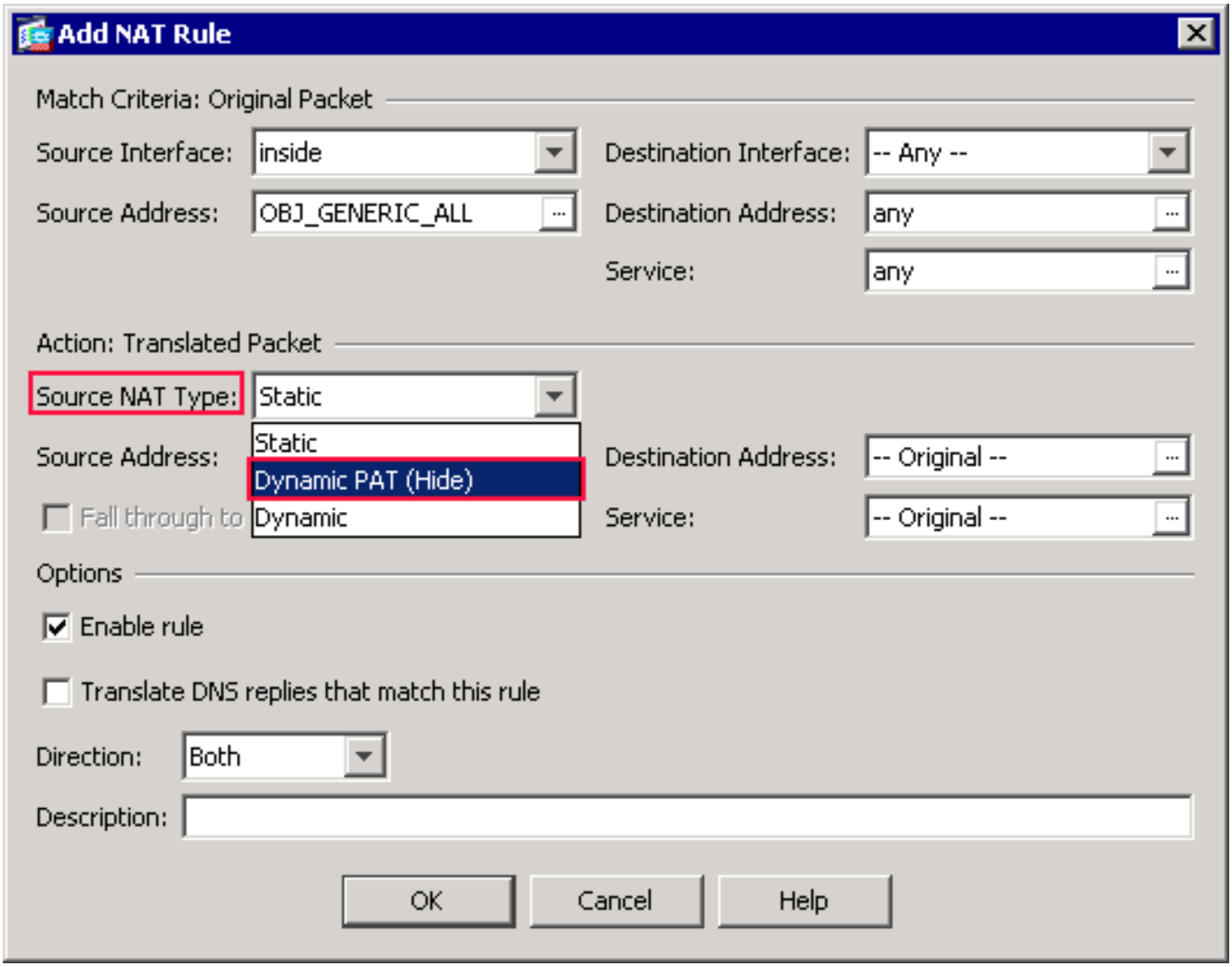


Nella finestra di dialogo Sfoglia indirizzo di origine originale scegliere il primo oggetto di rete

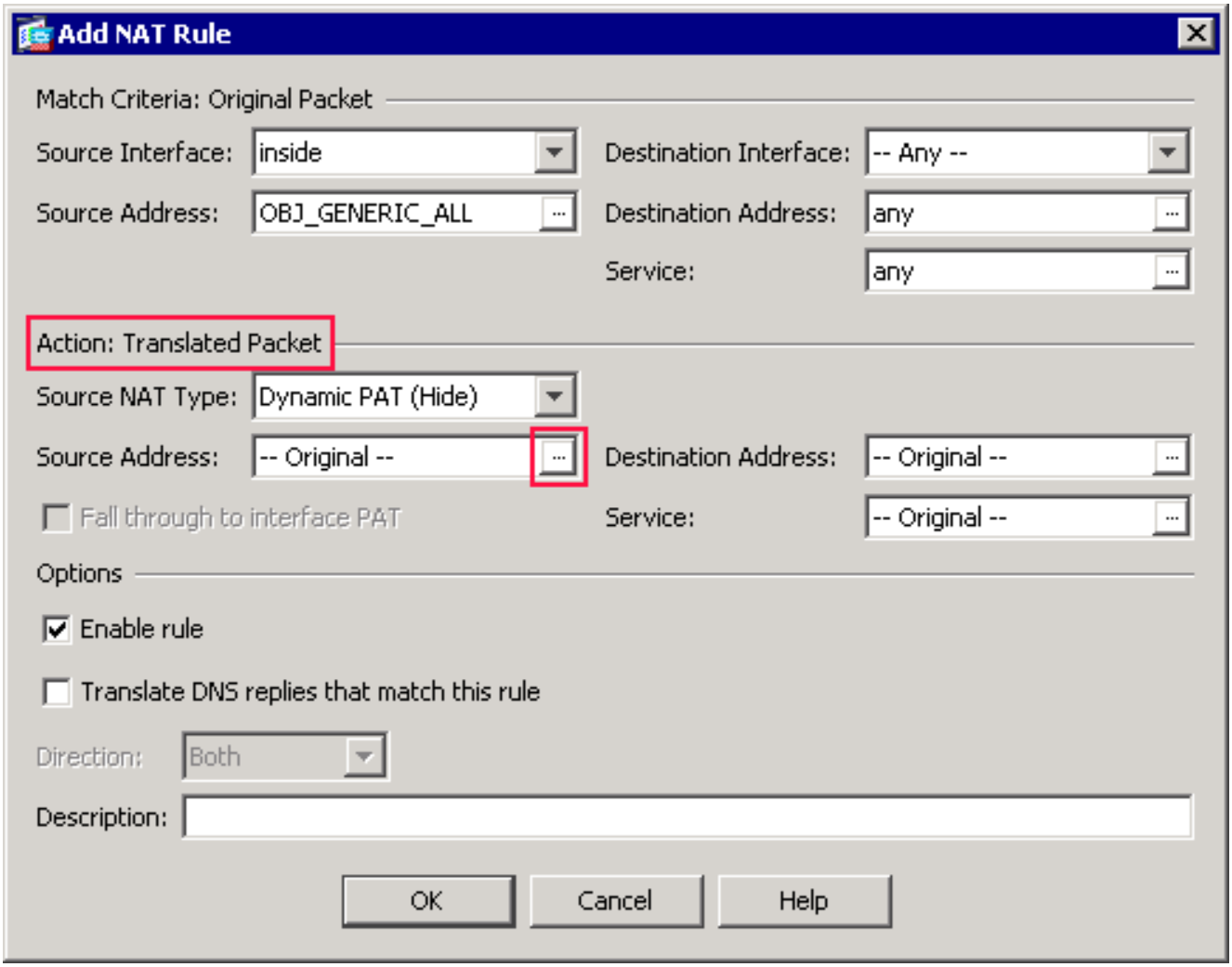
creato. Per questo esempio, selezionate **OBJ_GENERIC_ALL**.Fare clic su **Indirizzo origine originale**, quindi su **OK**.L'oggetto di rete *OBJ_GENERIC_ALL* viene ora visualizzato nel campo Source Address (Indirizzo di origine) in Match Criteria: Area Pacchetto originale della finestra di dialogo Aggiungi regola
NAT.



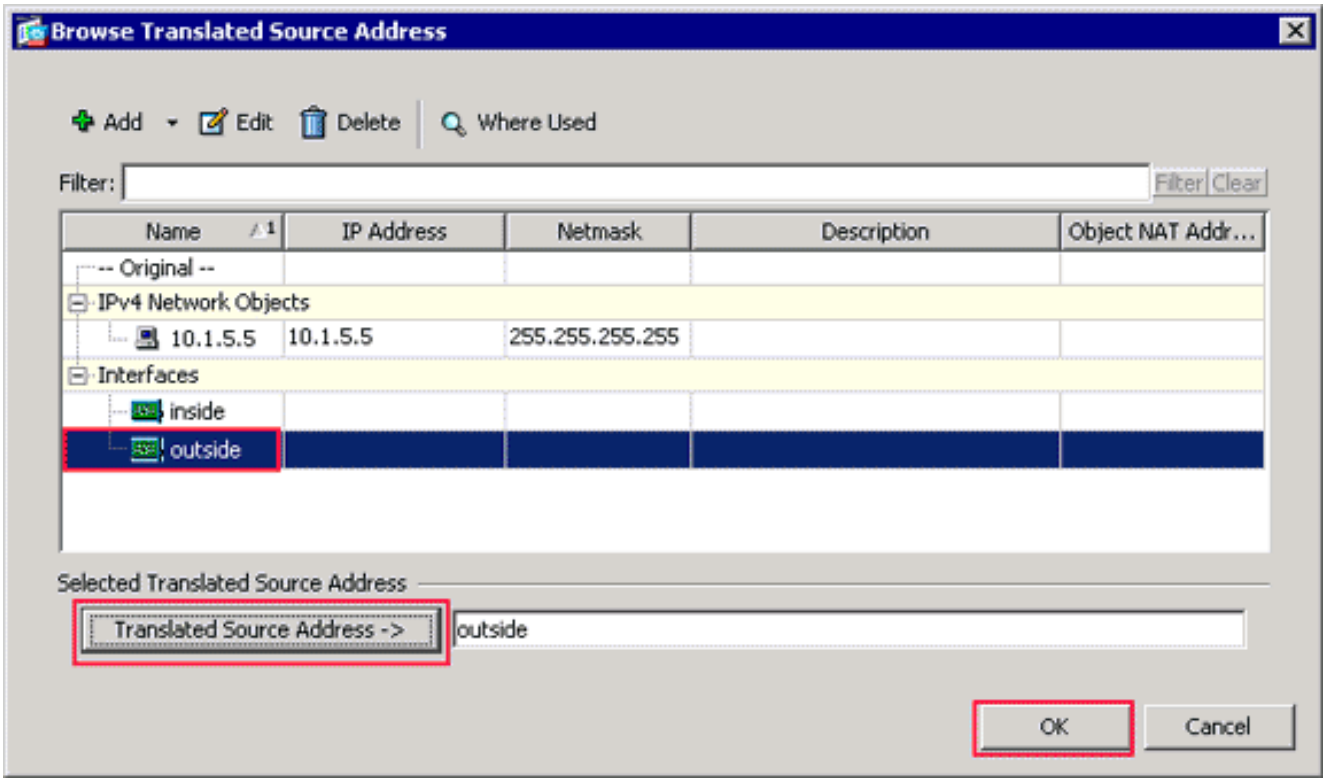
Nell'Azione: Nell'area Pacchetto tradotto della finestra di dialogo Aggiungi regola NAT, scegliere **Dynamic PAT (Nascondi)** dalla finestra di dialogo Source NAT
Type.



Fare clic sul pulsante Sfoglia (**...**) a destra del campo Indirizzo di origine.

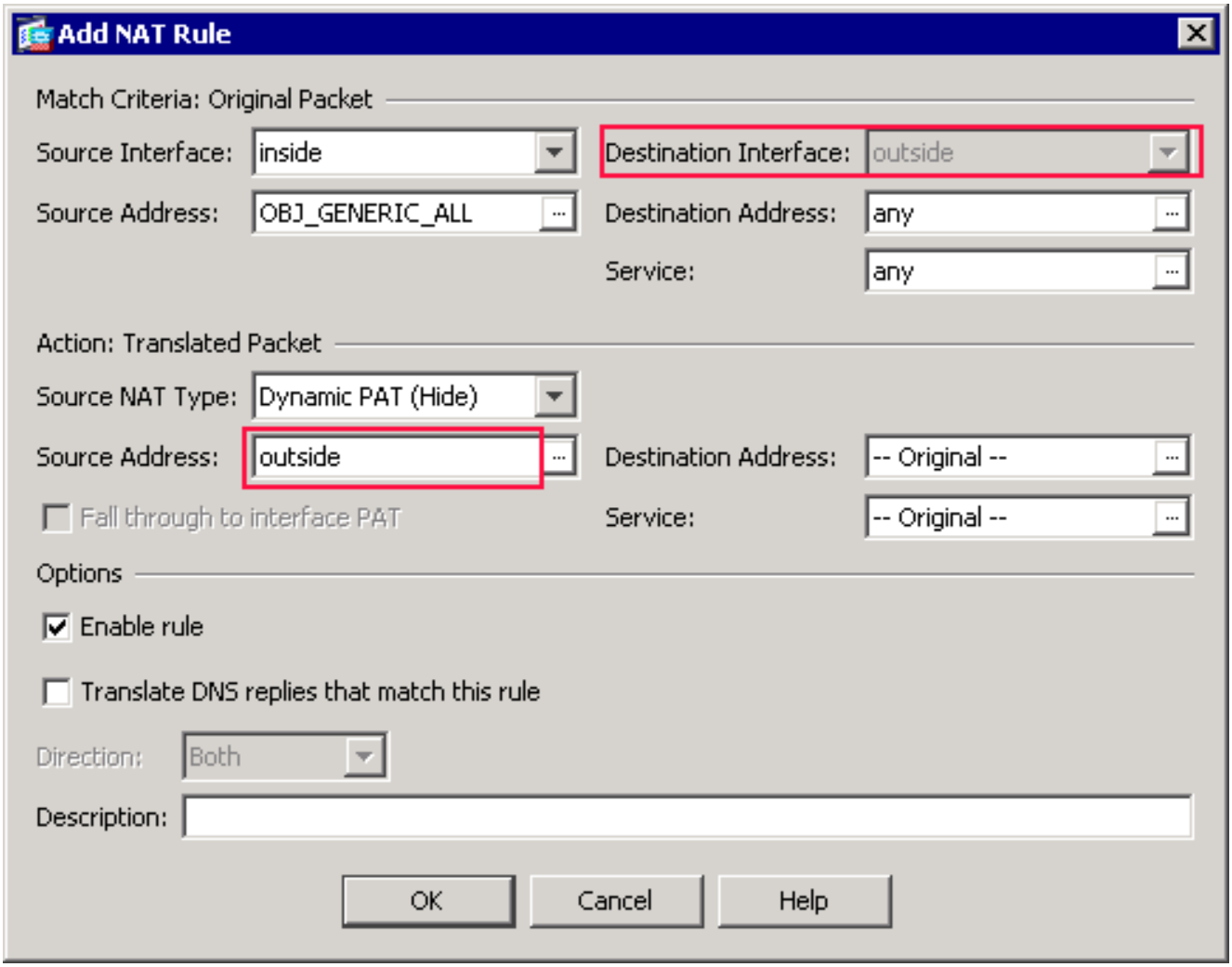


Verrà visualizzata la finestra di dialogo Sfoglia indirizzo di origine tradotto.

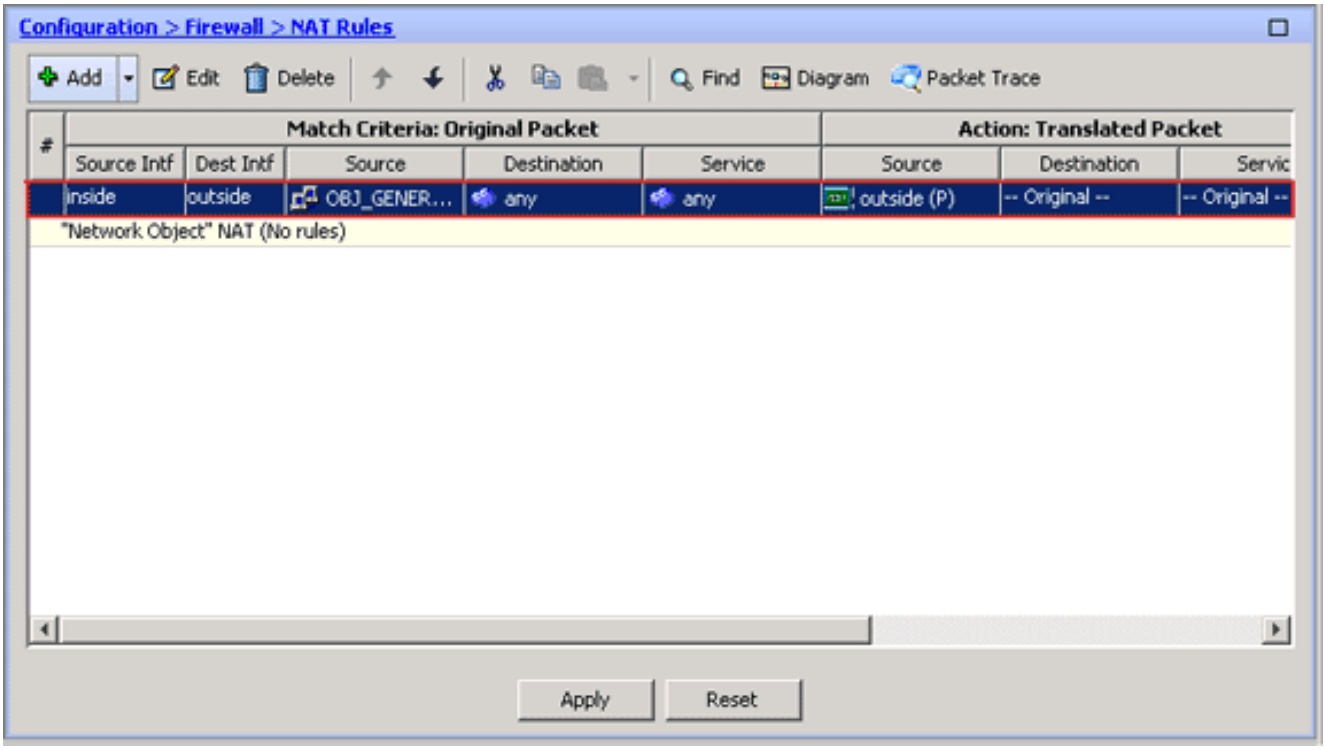


Nella finestra di dialogo Sfoglia indirizzo origine convertito scegliere l'oggetto interfaccia **esterna**. Questa interfaccia è già stata creata perché fa parte della configurazione originale.Fare clic su **Indirizzo origine tradotto** e quindi su **OK**.L'interfaccia esterna viene ora

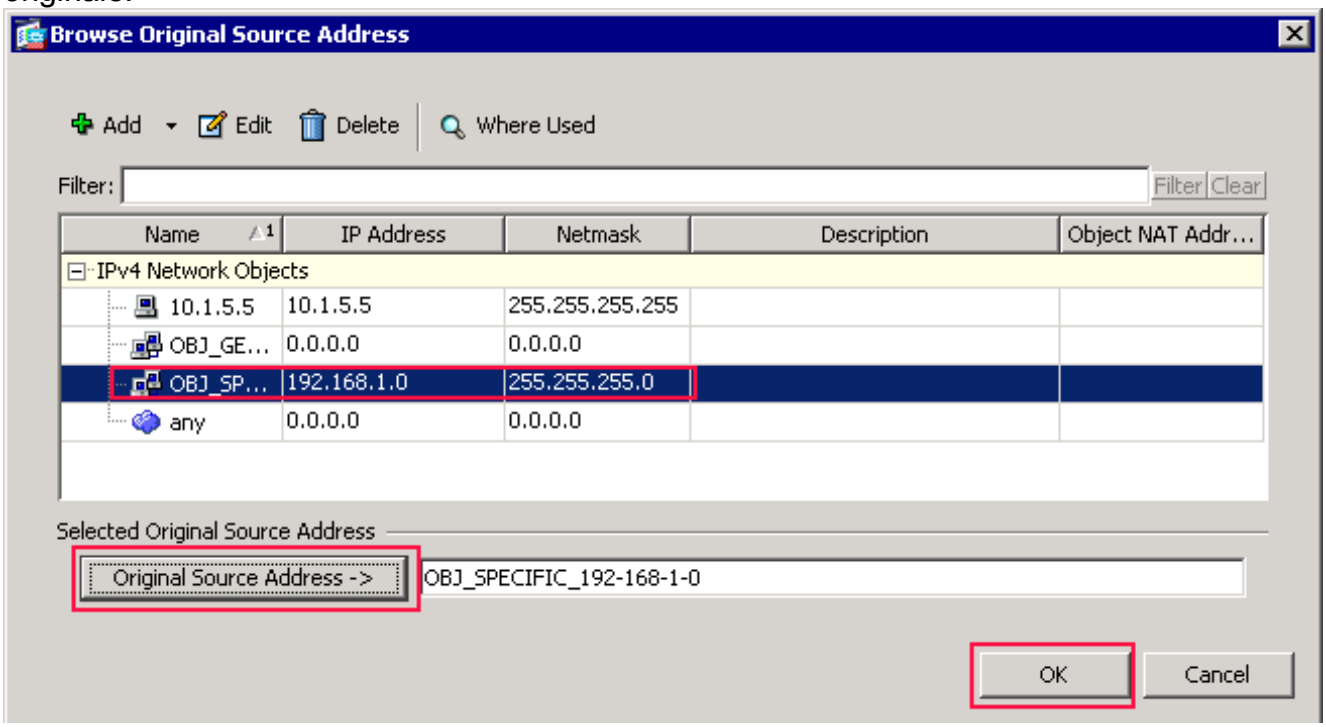
visualizzata nel campo Source Address in Action: Area Pacchetto tradotto nella finestra di dialogo Aggiungi regola
NAT.



Nota: il campo *Interfaccia di destinazione* viene modificato anche nell'interfaccia esterna.Verificate che la prima regola PAT completata venga visualizzata nel modo seguente:Nella finestra di dialogo Criteri di corrispondenza: Area Pacchetto originale, verificare i seguenti valori:Source Interface = internoIndirizzo di origine = OBJ_GENERIC_ALLDestination Address = qualsiasiService = qualsiasiNell'Azione: Area Pacchetti tradotti, verificare i seguenti valori:Tipo NAT di origine = PAT dinamico (Nascondi)Source Address = esternoIndirizzo di destinazione = OriginaleService = originaleFare clic su **OK**.La prima regola NAT viene visualizzata in ASDM, come mostrato nell'immagine:

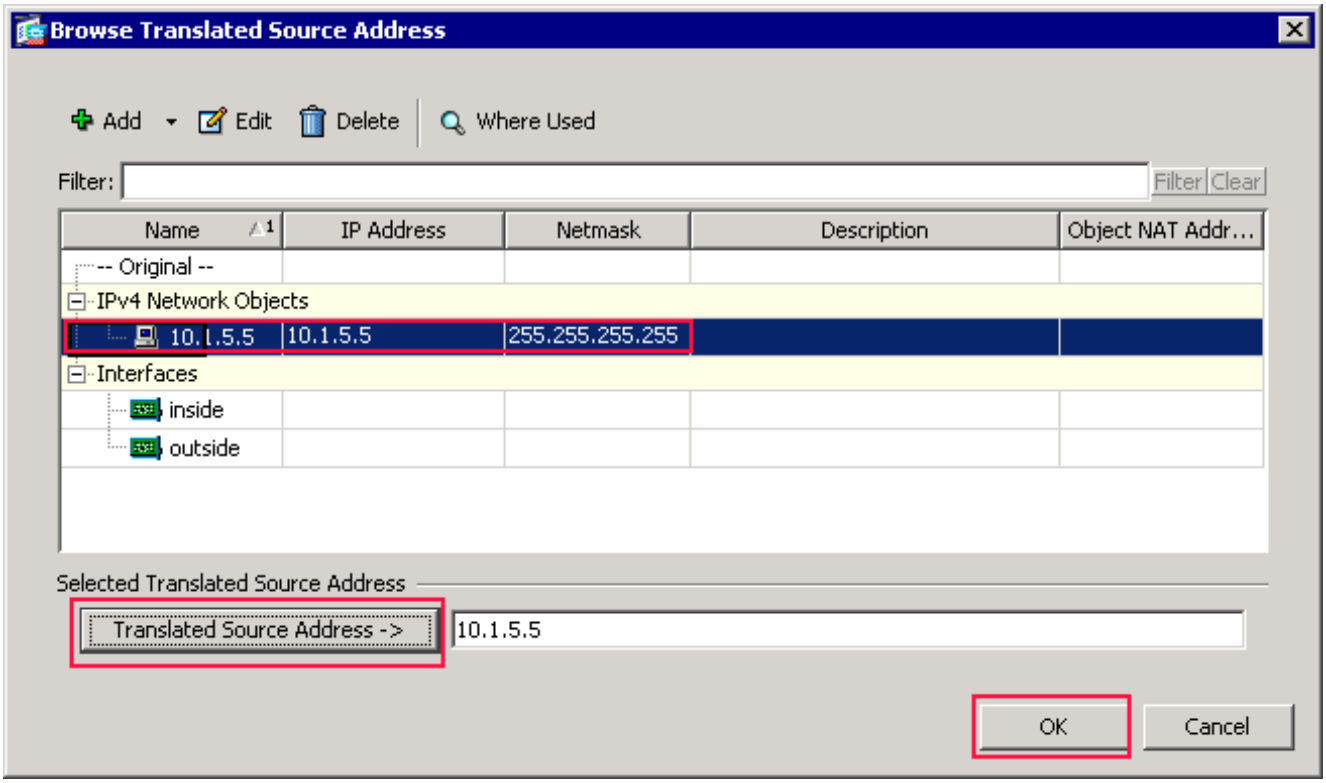


2. Creare la seconda regola NAT/PAT:In ASDM, scegliere **Configurazione > Firewall > Regole NAT**, quindi fare clic su **Aggiungi**.Nella finestra di dialogo Criteri di corrispondenza: Nell'area Pacchetto originale della finestra di dialogo Aggiungi regola NAT, scegliere **all'interno** dall'elenco a discesa Interfaccia origine.Fare clic sul pulsante Sfoglia (**...**) a destra del campo Indirizzo di origine.Verrà visualizzata la finestra di dialogo Sfoglia indirizzo di origine originale.

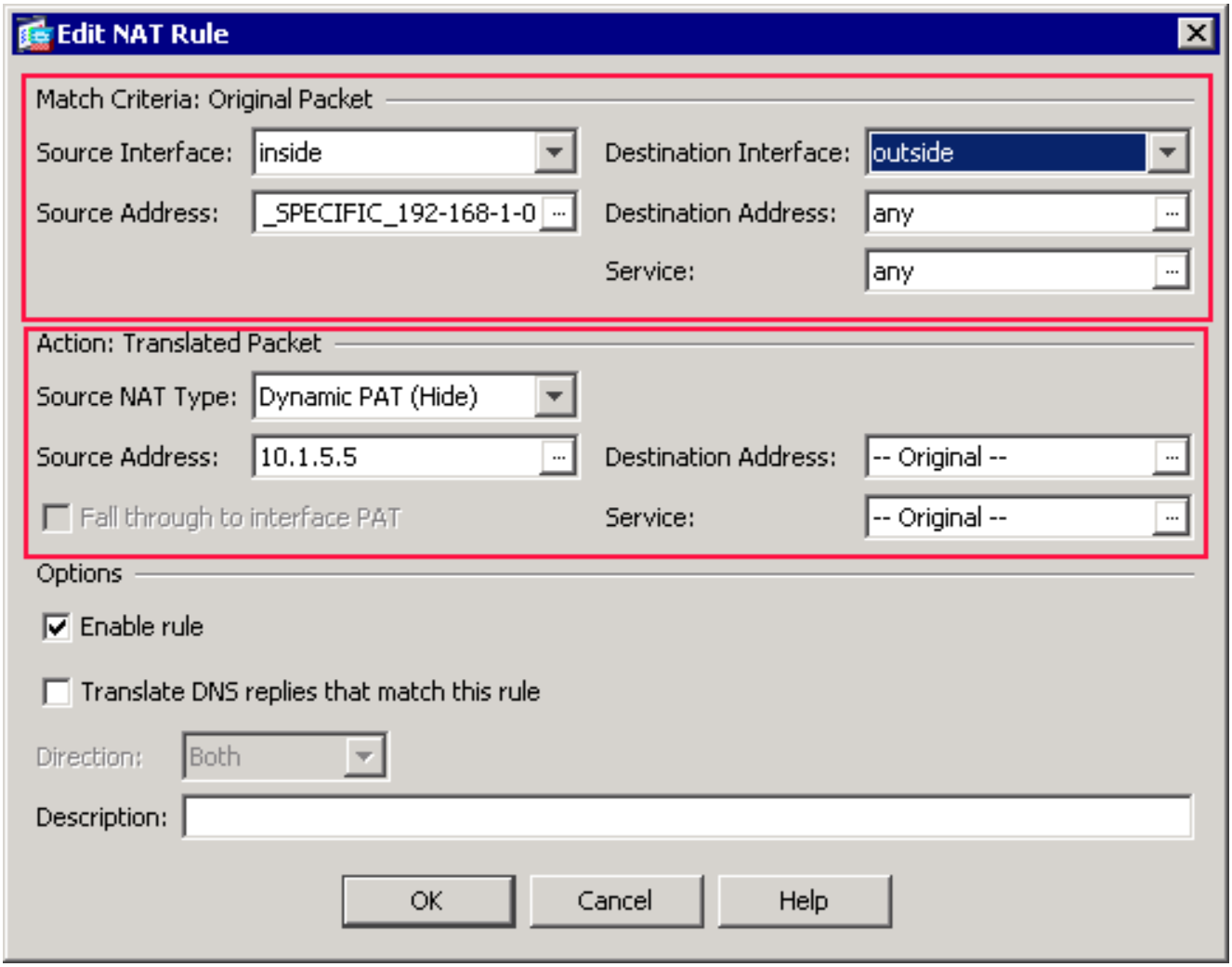


Nella finestra di dialogo Sfoglia indirizzo di origine originale scegliere il secondo oggetto creato. Per questo esempio, scegliere **OBJ_SPECIFIC_192-168-1-0**.Fare clic su **Indirizzo origine originale**, quindi su **OK**.L'oggetto di rete *OBJ_SPECIFIC_192-168-1-0* viene visualizzato nel campo Source Address in Match Criteria: Area Pacchetto originale della finestra di dialogo Aggiungi regola NAT.Nell'Azione: Nell'area Pacchetto tradotto della finestra di dialogo Aggiungi regola NAT, scegliere **Dynamic PAT (Nascondi)** dalla finestra di dialogo Source NAT Type.Fare clic sul pulsante **...** a destra del campo Source Address

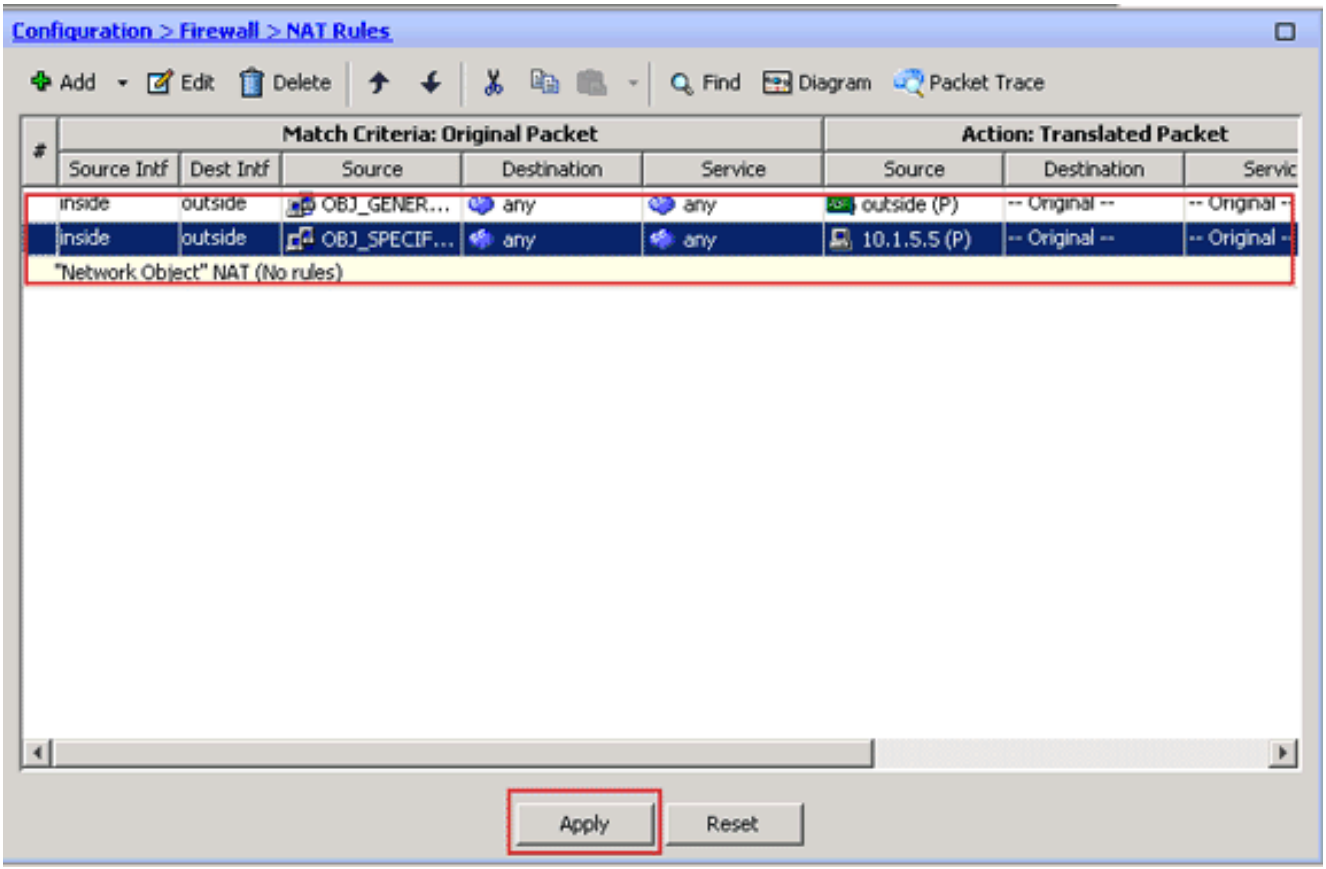
(Indirizzo di origine).Verrà visualizzata la finestra di dialogo Sfoglia indirizzo di origine tradotto.



Nella finestra di dialogo Sfoglia indirizzo di origine tradotto scegliere l'oggetto **10.1.5.5**. (L'interfaccia è già stata creata perché fa parte della configurazione originale).Fare clic su **Indirizzo origine tradotto** e quindi su **OK**.L'oggetto di rete **10.1.5.5** viene visualizzato nel campo Source Address in Action: Area Pacchetto tradotto della finestra di dialogo Aggiungi regola NAT.Nella finestra di dialogo Criteri di corrispondenza: Nell'area Pacchetto originale, selezionare **esternamente** dall'elenco a discesa Interfaccia di destinazione.**Nota:** se non si sceglie *esterno* per questa opzione, l'interfaccia di destinazione farà riferimento a *Qualsiasi*.



Verificate che la seconda regola NAT/PAT completata venga visualizzata come segue:Nella finestra di dialogo Criteri di corrispondenza: Area Pacchetto originale, verificare i seguenti valori:Source Interface = internoIndirizzo di origine = OBJ_SPECIFIC_192-168-1-0Indirizzo di destinazione = esternoService = qualsiasiNell'Azione: Area Pacchetti tradotti, verificare i seguenti valori:Tipo NAT di origine = PAT dinamico (Nascondi)Source Address = 10.1.5.5Indirizzo di destinazione = OriginaleService = originaleFare clic su **OK**.La configurazione NAT completata viene visualizzata in ASDM, come mostrato nella seguente immagine:



3. Per applicare le modifiche alla configurazione corrente, fare clic sul pulsante **Apply** (Applica).

La configurazione della porta dinamica su un'appliance Cisco Adaptive Security (ASA) è completata.

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

Verifica della regola PAT generica

- show local-host: visualizza gli stati di rete degli host locali.

```
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: visualizza lo stato della connessione per il tipo di connessione designato.

```
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
```

- show xlate - Visualizza le informazioni sugli slot di traslazione.

```
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
```

Verifica di una regola PAT specifica

- show local-host: visualizza gli stati di rete degli host locali.

```
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: visualizza lo stato della connessione per il tipo di connessione designato.

```
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
```

- show xlate - Visualizza le informazioni sugli slot di traslazione.

```
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
```

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni correlate

- Cisco Adaptive Security Device Manager
- Cisco ASA serie 5500 Adaptive Security Appliance
- RFC (Requests for Comments)
- Documentazione e supporto tecnico – Cisco Systems