ASA 8.3(x) Dynamic PAT mit zwei internen Netzwerken und Konfigurationsbeispiel für das Internet

Inhalt

Einführung

Dieses Dokument enthält eine Beispielkonfiguration für eine dynamische PAT auf einer Cisco Adaptive Security Appliance (ASA), die die Softwareversion 8.3(1) ausführt. Dynamische PAT übersetzt mehrere reale Adressen in eine einzige zugeordnete IP-Adresse, indem die tatsächliche Quelladresse und der Quellport in die zugeordnete Adresse und den eindeutigen zugeordneten Port übersetzt werden. Für jede Verbindung ist eine eigene Übersetzungssitzung erforderlich, da sich der Quellport für jede Verbindung unterscheidet.

Voraussetzungen

Anforderungen

Stellen Sie sicher, dass Sie diese Anforderungen erfüllen, bevor Sie versuchen, diese Konfiguration durchzuführen:

- Stellen Sie sicher, dass das interne Netzwerk über zwei Netzwerke innerhalb der ASA verfügt:192.168.0.0/24 - Direkte Verbindung zum ASA-Netzwerk.192.168.1.0/24 - Netzwerk auf der ASA-Innenseite, aber hinter einem anderen Gerät (z. B. einem Router).
- Stellen Sie sicher, dass die internen Benutzer die folgende PAT erhalten:Hosts im Subnetz

192.168.1.0/24 erhalten PAT zu einer vom ISP angegebenen Ersatz-IP-Adresse (10.1.5.5).Jeder andere Host hinter der ASA erhält PAT zur externen Schnittstellen-IP-Adresse der ASA (10.1.5.1).

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Adaptive Security Appliance (ASA) mit Version 8.3(1)
- ASDM Version 6.3(1)

Hinweis: Informationen zur Konfiguration der ASA durch den ASDM finden Sie unter Zulassen von HTTPS-Zugriff für ASDM.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

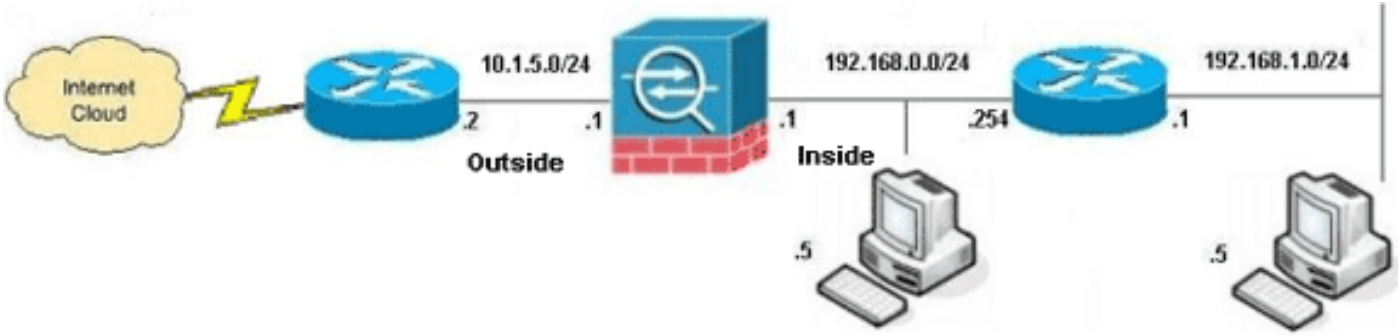
Konventionen

Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions.

Konfiguration

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Hinweis: Die in dieser Konfiguration verwendeten IP-Adressierungsschemata sind im Internet nicht rechtlich routbar. Sie sind RFC 1918 -Adressen, die in einer Laborumgebung verwendet werden.

- ASA CLI-Konfiguration
- ASDM-Konfiguration

ASA CLI-Konfiguration

In diesem Dokument werden die unten angegebenen Konfigurationen verwendet.

Dynamische ASA-PAT-Konfiguration

```
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) mit laufender Konfiguration

```
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
```

ASDM-Konfiguration

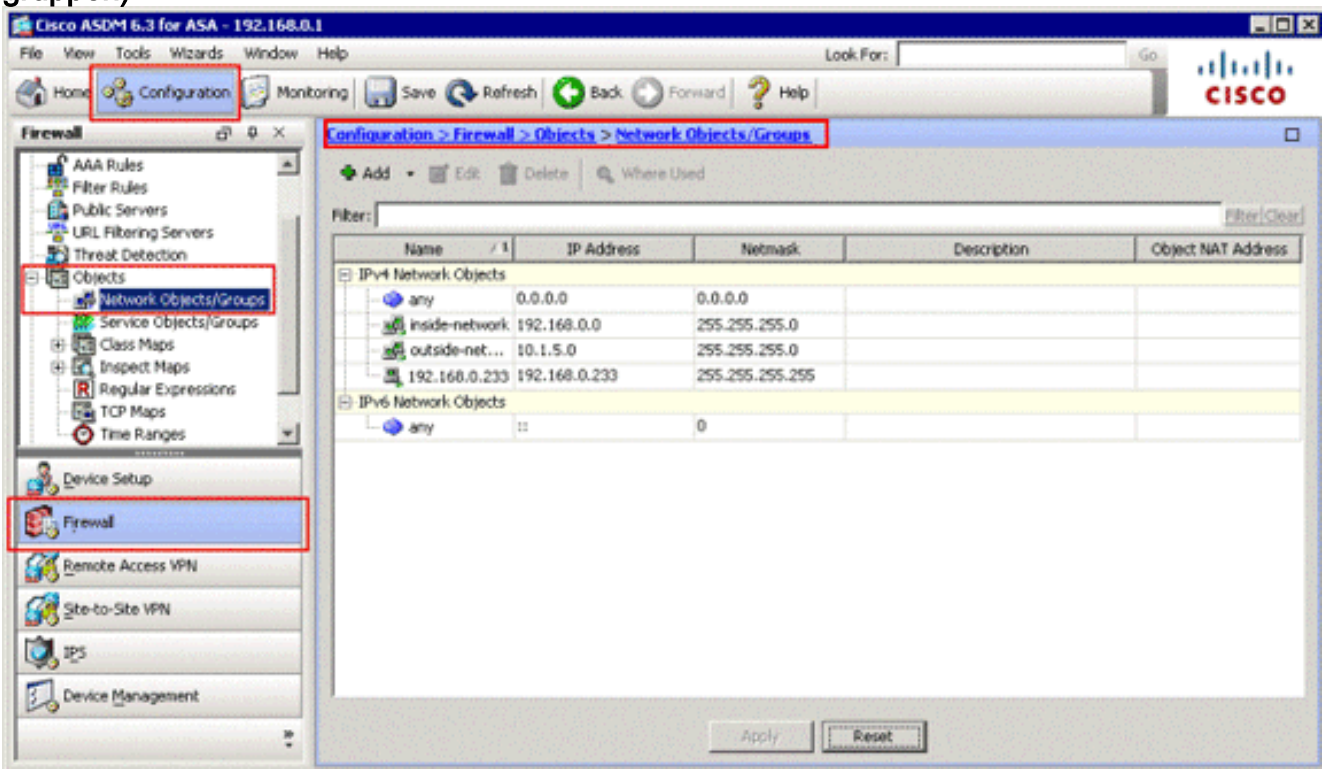
Um diese Konfiguration über die ASDM-Schnittstelle abzuschließen, müssen Sie:

1. Hinzufügen von drei Netzwerkobjekten In diesem Beispiel werden folgende Netzwerkobjekte hinzugefügt:OBJ_GENERIC_ALLOBJ_SPECIFIC_192-168-1-010.1.5.5
2. Erstellen Sie zwei NAT/PAT-Regeln. In diesem Beispiel werden NAT-Regeln für diese Netzwerkobjekte erstellt:OBJ_GENERIC_ALLOBJ_SPECIFIC_192-168-1-0

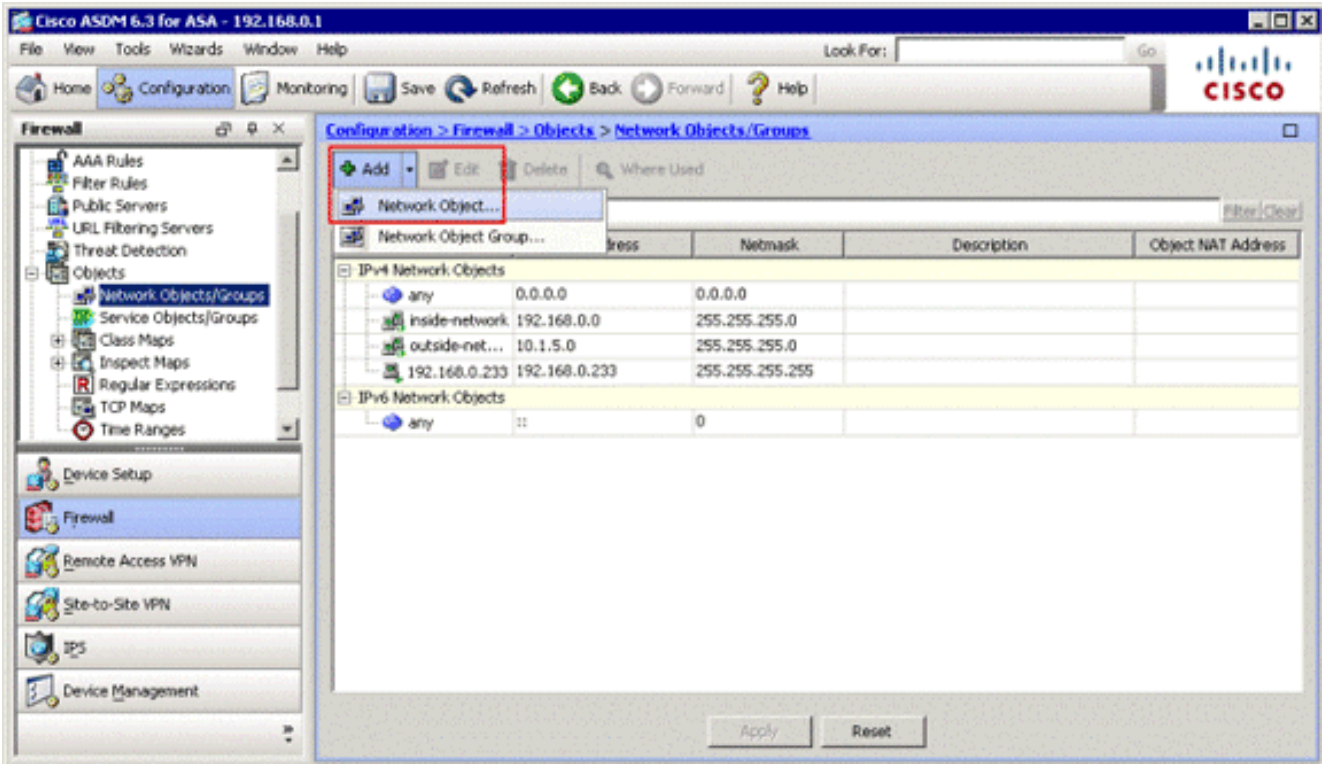
Netzwerkobjekte hinzufügen

Gehen Sie wie folgt vor, um Netzwerkobjekte hinzuzufügen:

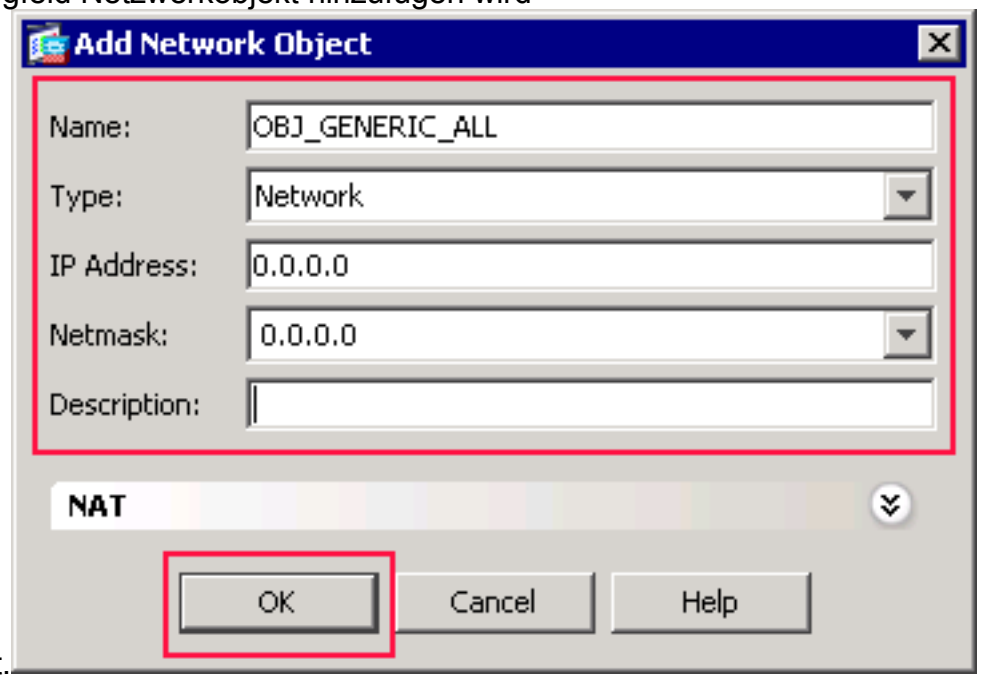
1. Melden Sie sich bei ASDM an, und wählen Sie **Configuration > Firewall > Objects > Network Objects/Groups (Konfiguration > Firewall > Objekte > Netzwerkobjekte/-gruppen)**.



2. Wählen Sie **Hinzufügen > Netzwerkobjekt**, um ein Netzwerkobjekt hinzuzufügen.

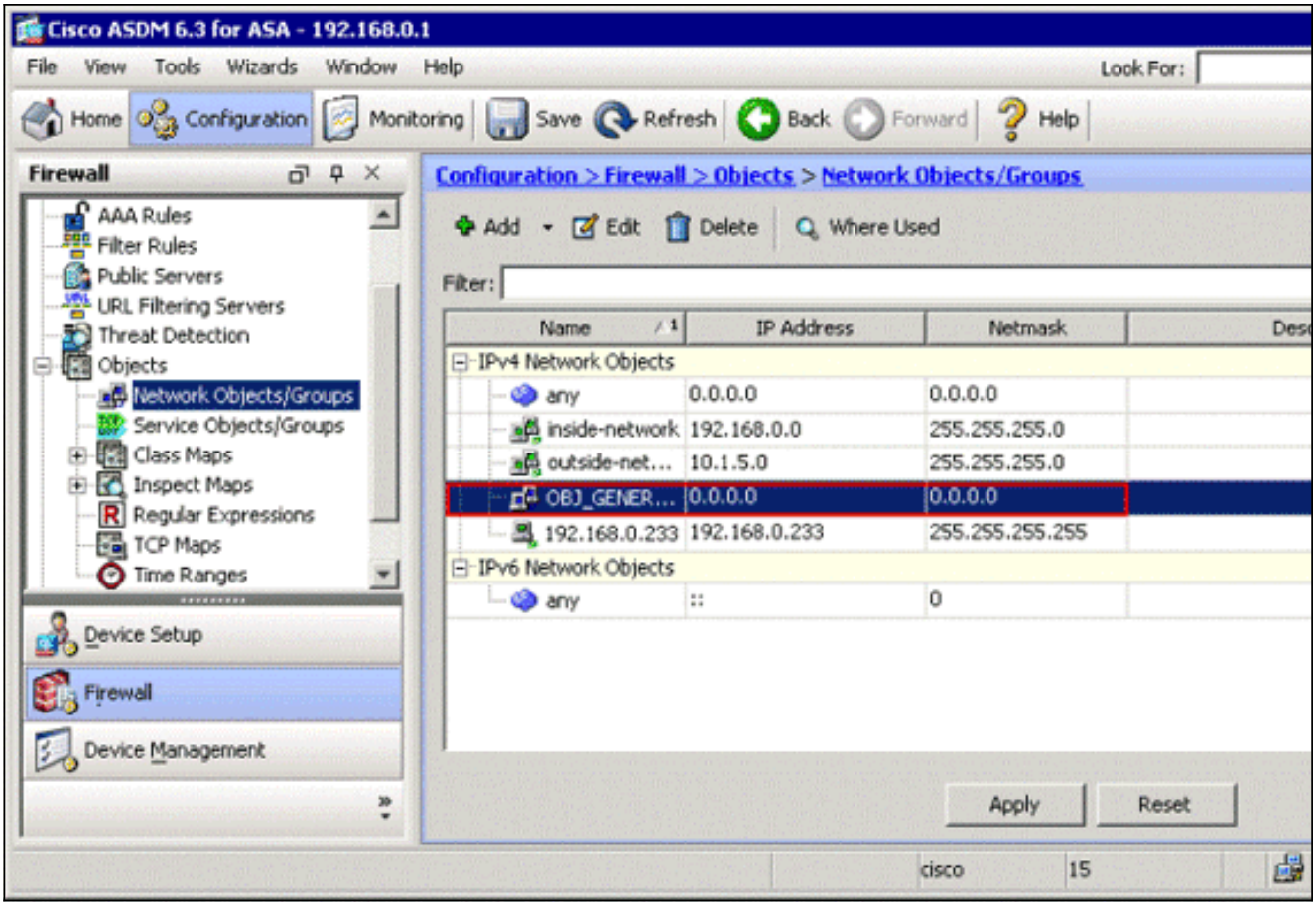


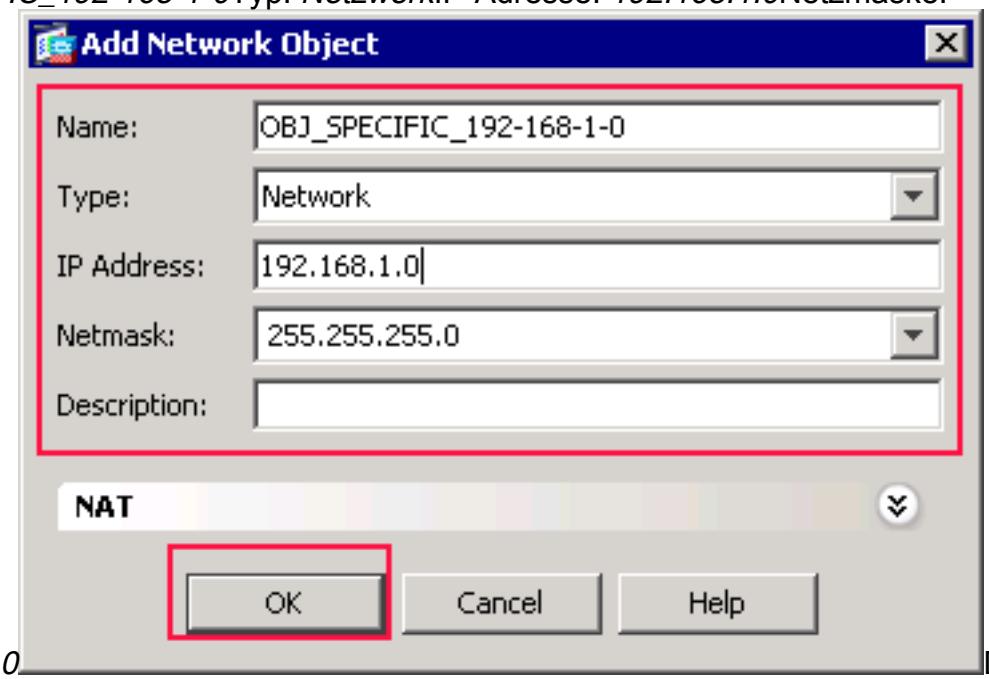
Das Dialogfeld Netzwerkobjekt hinzufügen wird



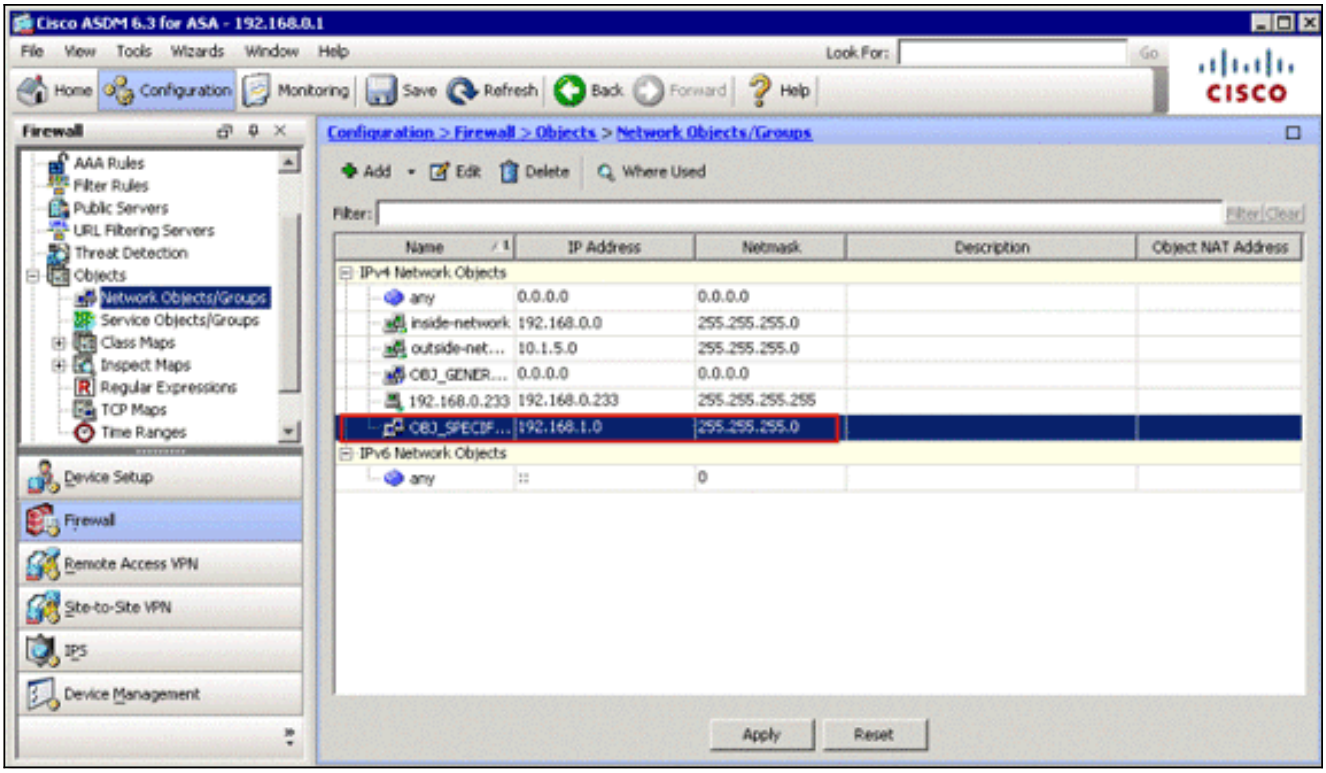
angezeigt.

3. Geben Sie diese Informationen im Dialogfeld Netzwerkobjekt hinzufügen ein:Name des Netzwerkobjekts. (In diesem Beispiel wird *OBJ_GENERIC_ALL* verwendet.)Typ des Netzwerkobjekts. (In diesem Beispiel wird *Netzwerk* verwendet.)IP-Adresse für das Netzwerkobjekt. (In diesem Beispiel wird *0.0.0.0* verwendet.)Netzmaske für das Netzwerkobjekt. (In diesem Beispiel wird *0.0.0.0* verwendet.)
4. Klicken Sie auf **OK**.Das Netzwerkobjekt wird erstellt und in der Liste Netzwerkobjekte/Gruppen angezeigt, wie in diesem Bild gezeigt:

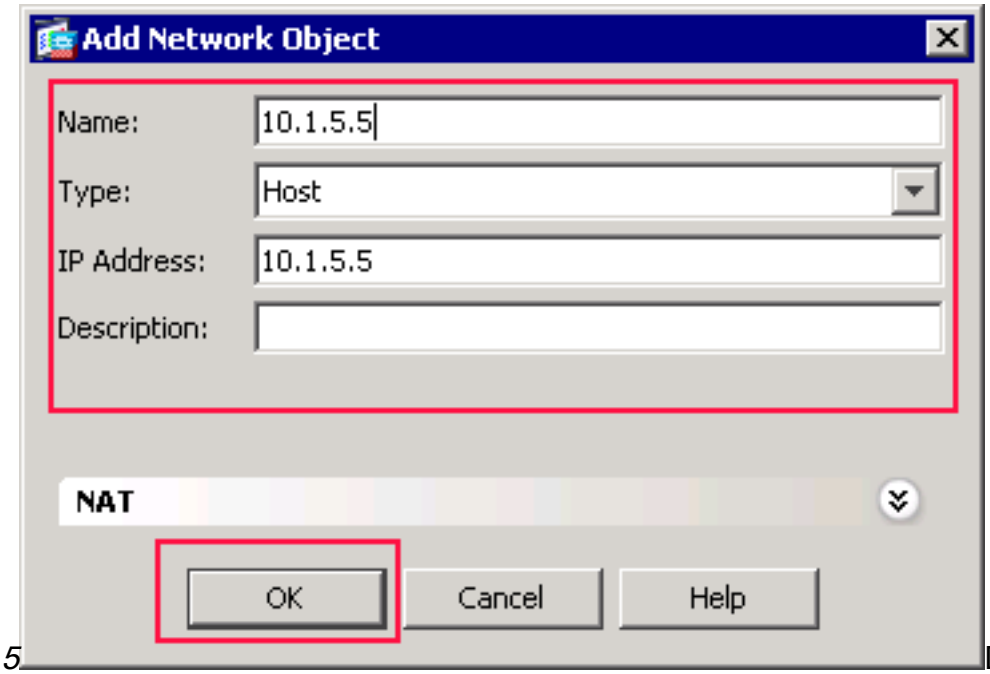


5. Wiederholen Sie die vorherigen Schritte, um ein zweites Netzwerkobjekt hinzuzufügen, und klicken Sie auf **OK**.In diesem Beispiel werden folgende Werte verwendet:Name: *OBJ_SPECIFIC_192-168-1-0*Typ: *Netzwerk*IP-Adresse: *192.168.1.0*Netzmaske: *255.255.255.0* 

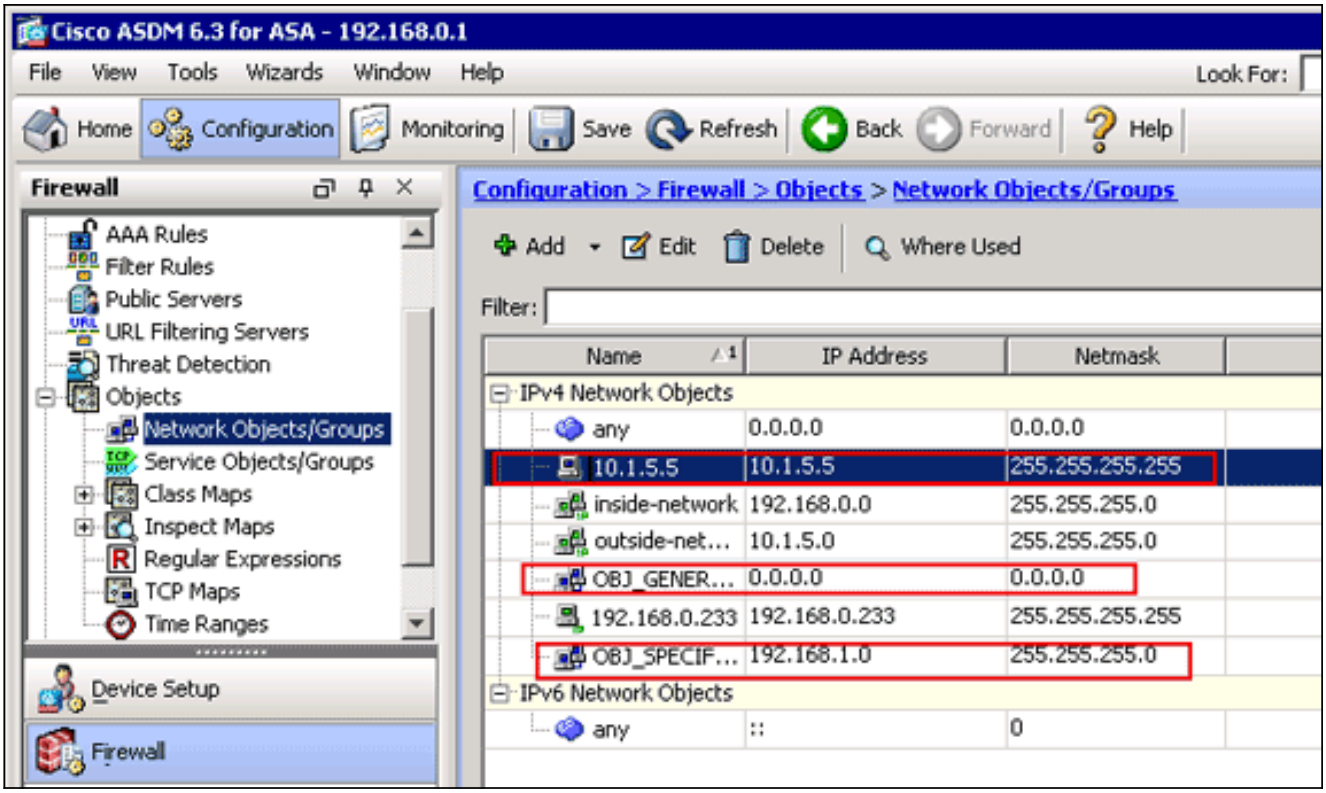
Das zweite Objekt wird erstellt und in der Liste Netzwerkobjekte/Gruppen angezeigt, wie in diesem Bild
gezeigt:



6. Wiederholen Sie die vorherigen Schritte, um ein drittes Netzwerkobjekt hinzuzufügen, und klicken Sie auf **OK**.In diesem Beispiel werden folgende Werte verwendet:Name: *10.1.5.5*Typ: *Host*IP-Adresse:



*10.1.5.5*Das dritte Netzwerkobjekt wird erstellt und in der Liste Netzwerkobjekte/-gruppen angezeigt.

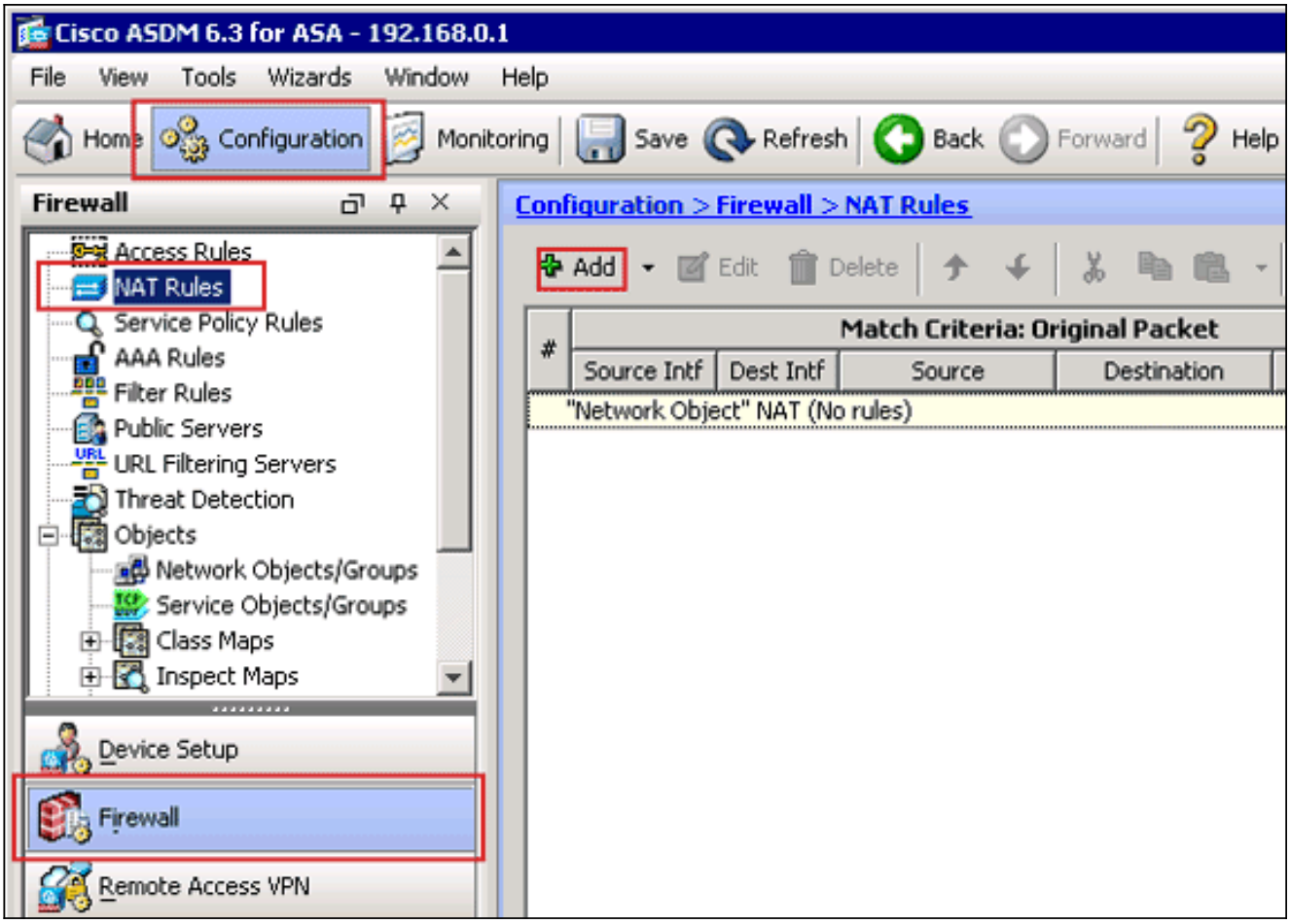


Die Liste Netzwerkobjekte/Gruppen sollte nun die drei erforderlichen Objekte enthalten, die für die Bezugnahme auf die NAT-Regeln erforderlich sind.

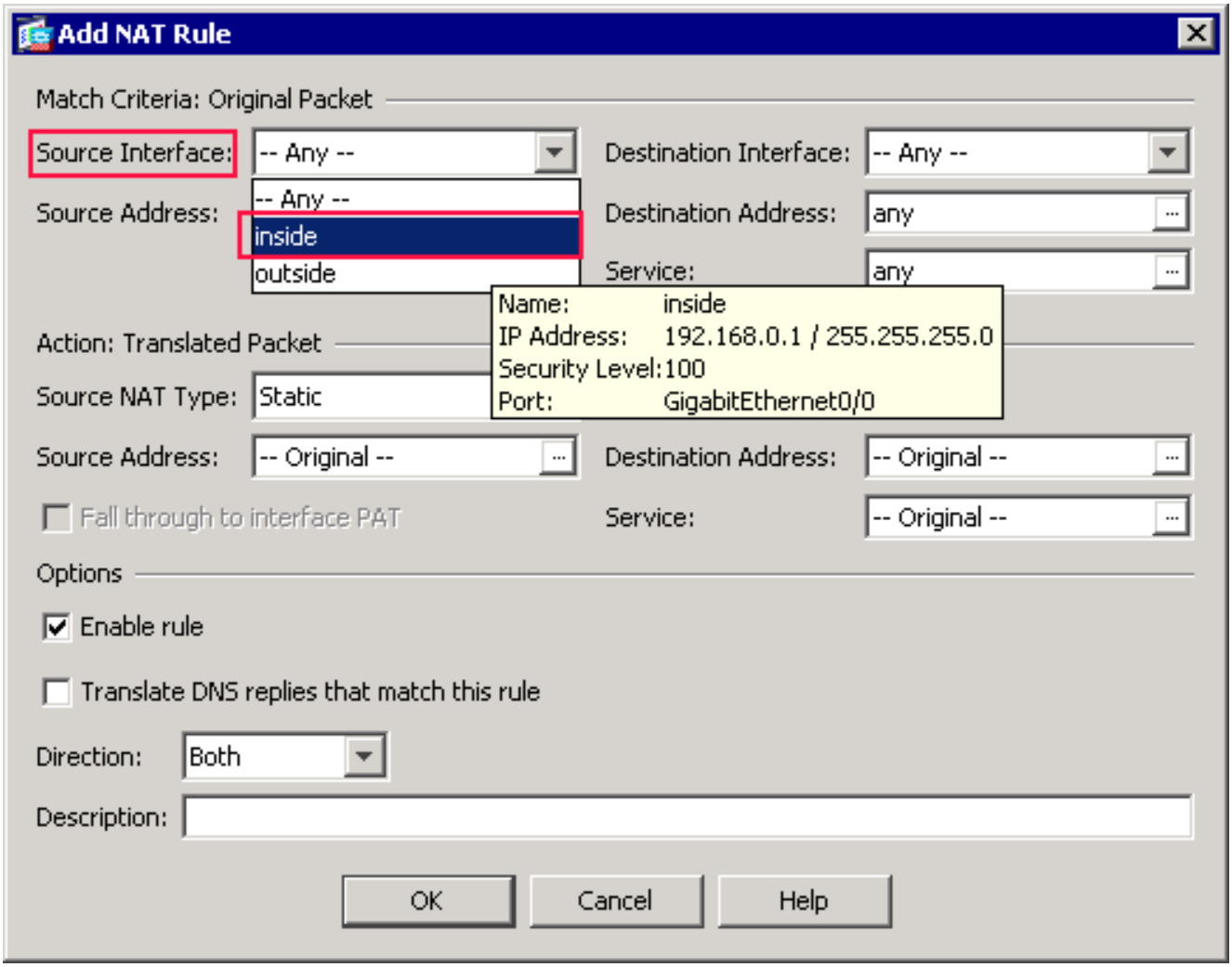
Erstellen von NAT/PAT-Regeln

Gehen Sie wie folgt vor, um NAT-/PAT-Regeln zu erstellen:

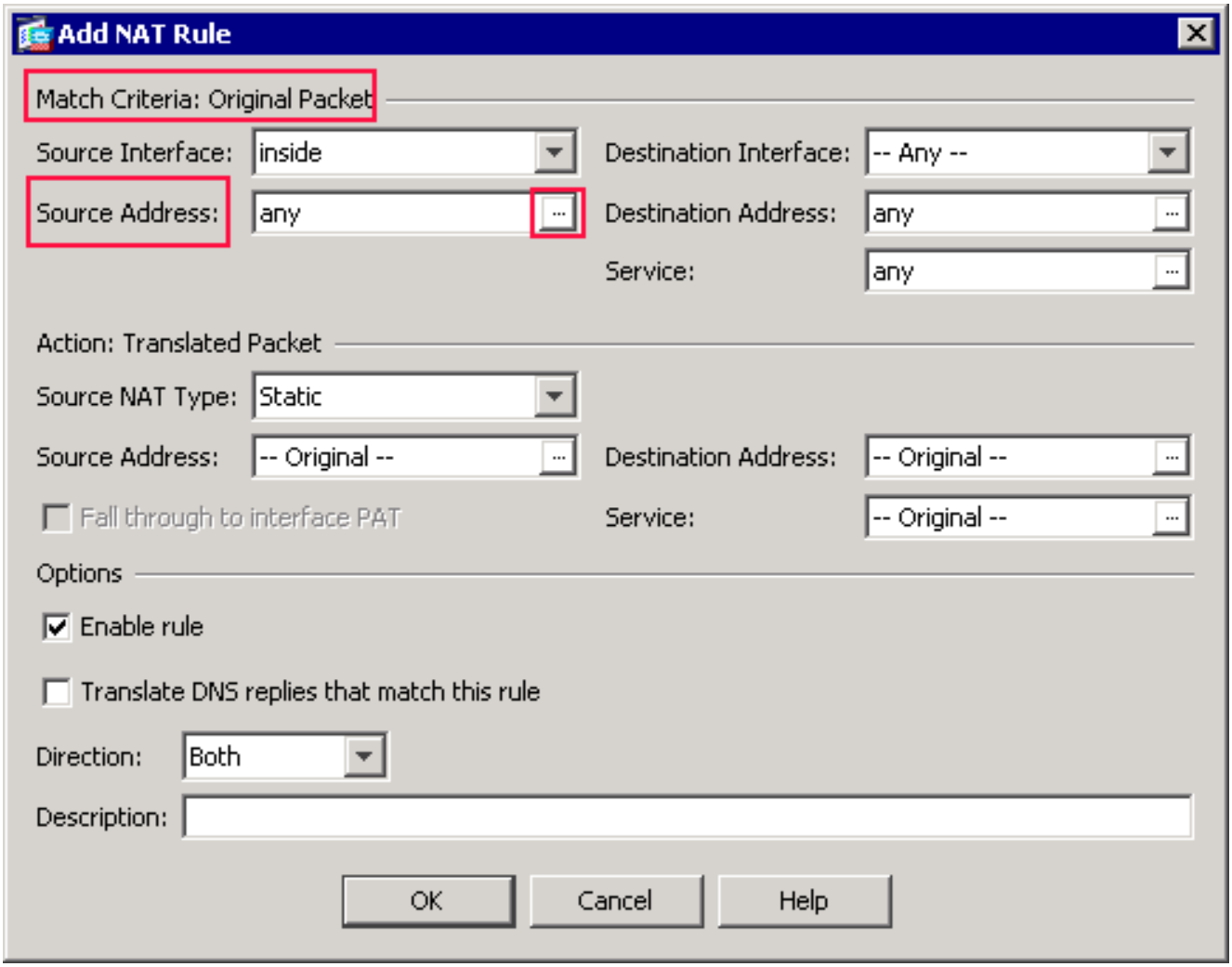
1. Erstellen Sie die erste NAT/PAT-Regel:Wählen Sie im ASDM **Configuration > Firewall > NAT Rules aus**, und klicken Sie auf **Add**.



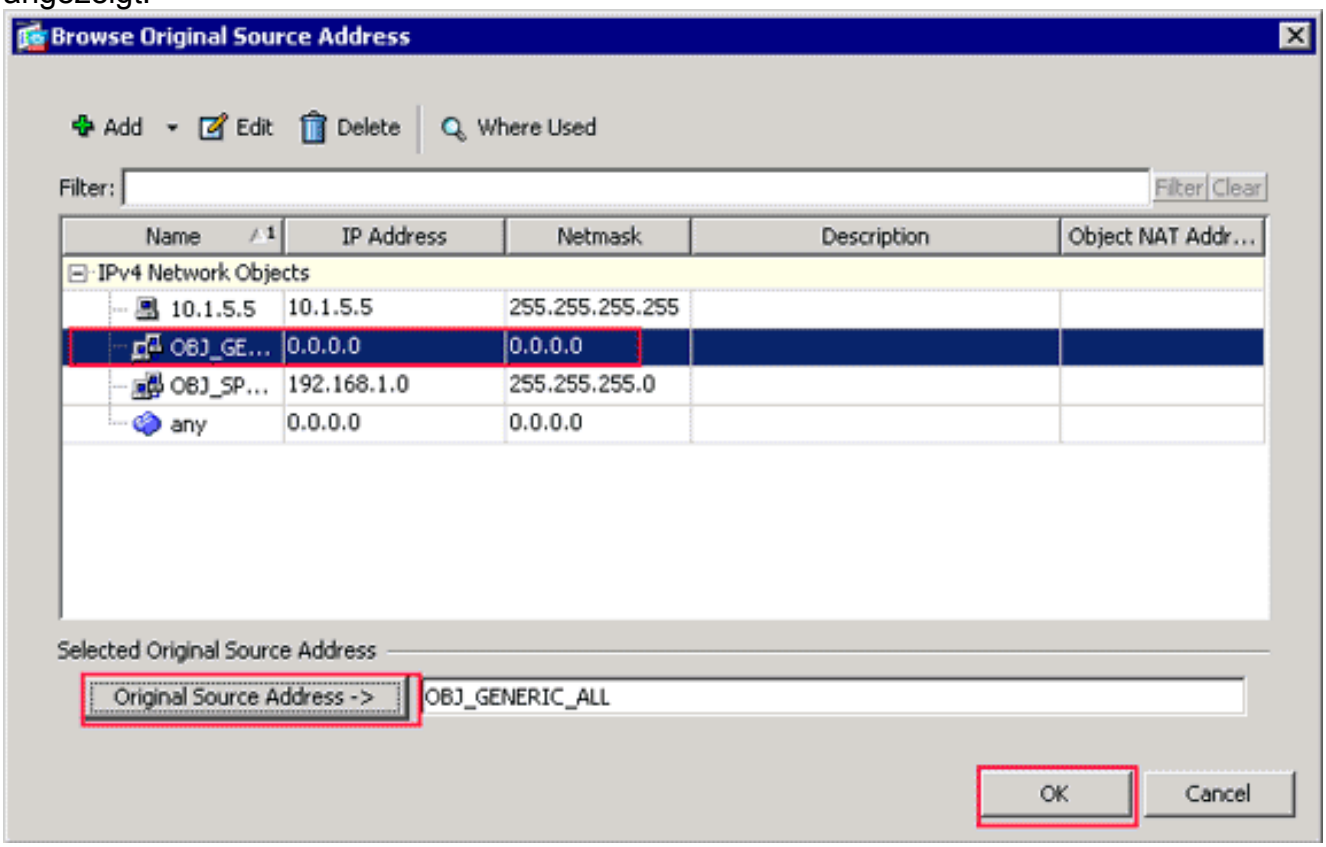
Das Dialogfeld "NAT-Regel hinzufügen" wird angezeigt.



In den Match Criteria: Der ursprüngliche Paketbereich im Dialogfeld NAT-Regel hinzufügen wählen Sie **innerhalb** der Dropdownliste Quellschnittstelle aus.

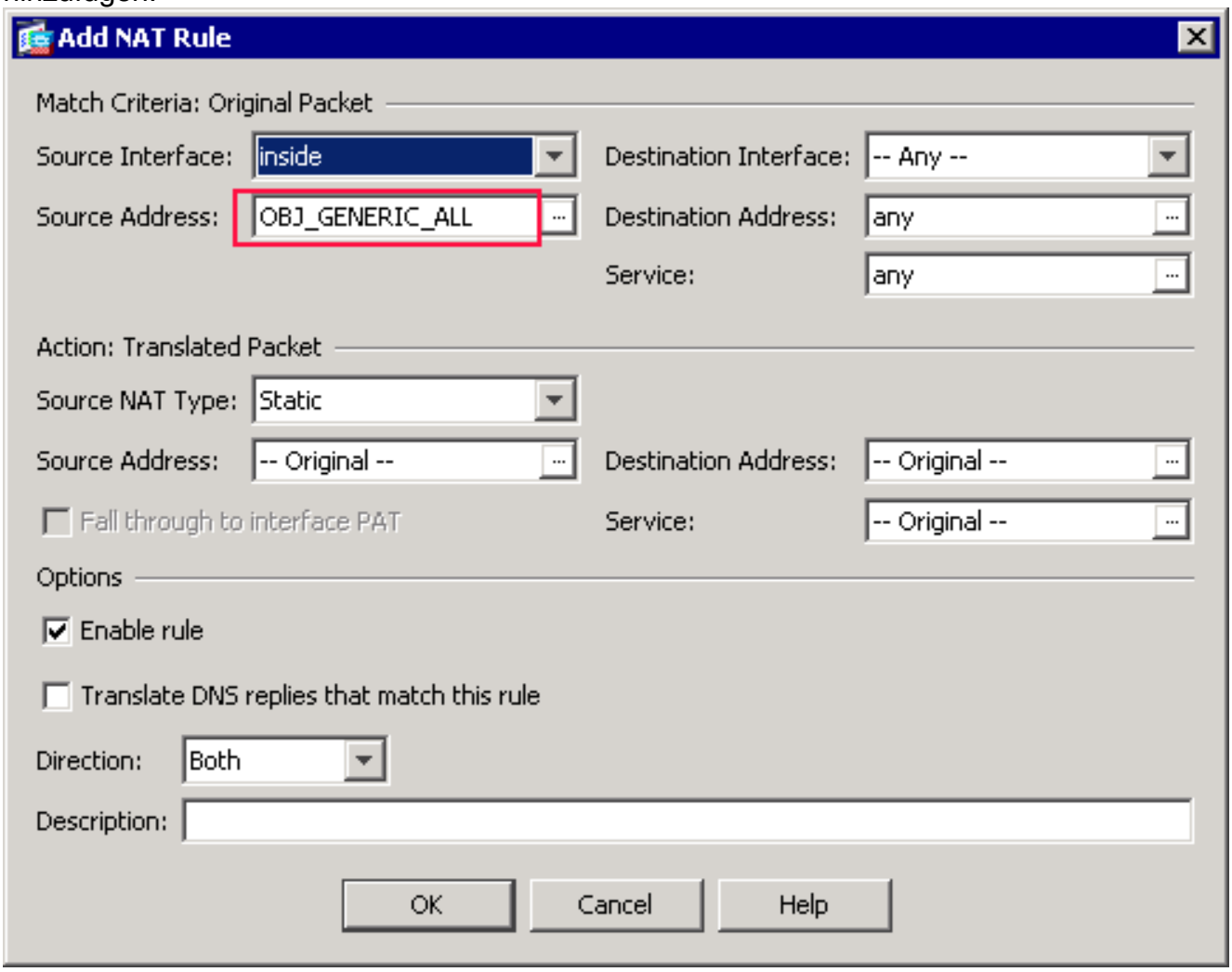


Klicken Sie auf die Schaltfläche Durchsuchen (...) rechts neben dem Textfeld Quelladresse.Das Dialogfeld Ursprüngliche Quelladresse durchsuchen wird angezeigt.

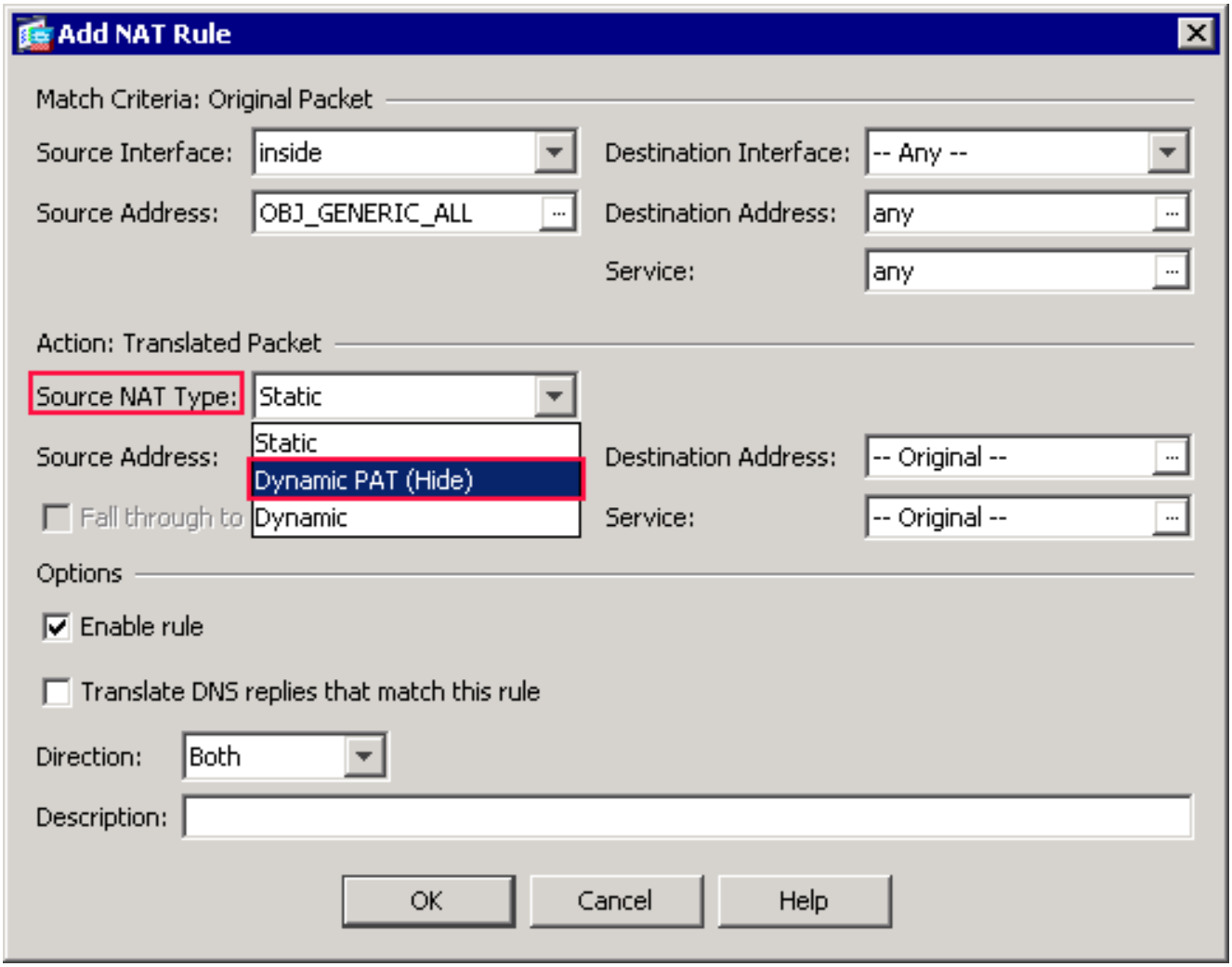


Wählen Sie im Dialogfeld Original-Quelladresse durchsuchen das erste Netzwerkobjekt aus,

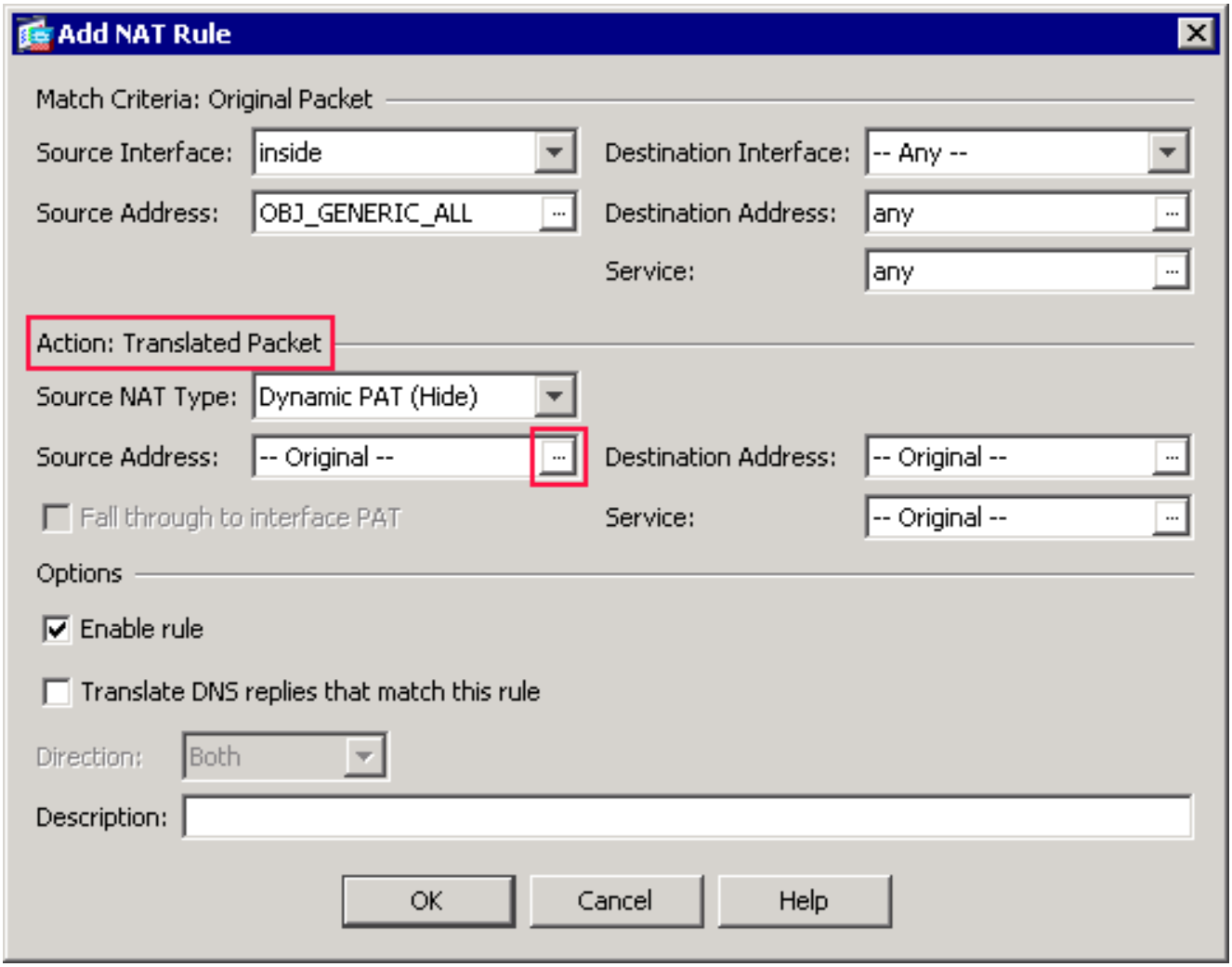
das Sie erstellt haben. (Wählen Sie in diesem Beispiel **OBJ_GENERIC_ALL**.)Klicken Sie auf **Originalquelladresse** und dann auf **OK**.Das *OBJ_GENERIC_ALL*-Netzwerkobjekt wird nun im Feld Quelladresse unter "Match Criteria:" (Kriterien für Übereinstimmung) angezeigt.
Originalpaketbereich des Dialogfelds NAT-Regel
hinzufügen.



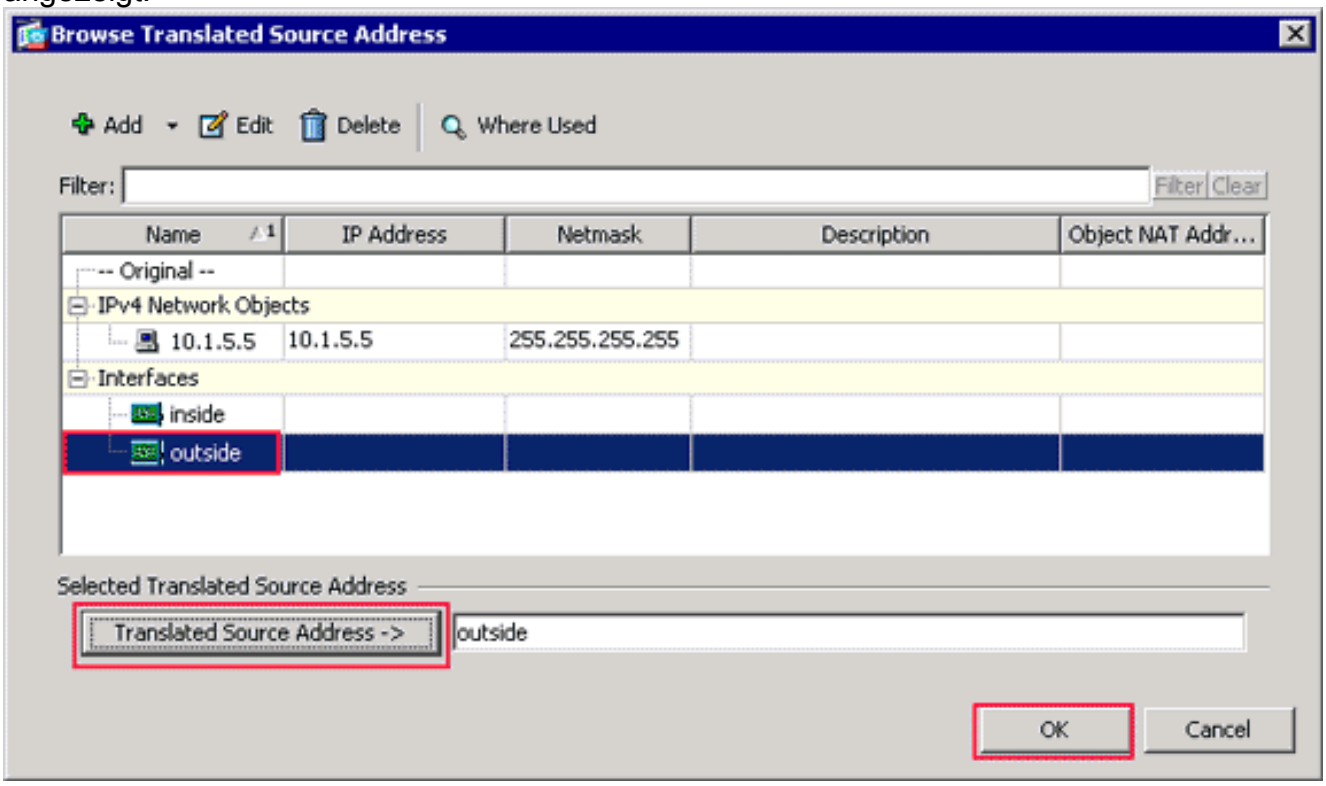
In der Aktion: Im Dialogfeld NAT-Regel hinzufügen wählen Sie im Bereich Übersetztes Paket im Dialogfeld **Dynamische PAT (Ausblenden)** im Dialogfeld Source NAT Type (NAT-Ausgangstyp)
aus.



Klicken Sie auf die Schaltfläche Durchsuchen (...) rechts neben dem Feld Quelladresse.

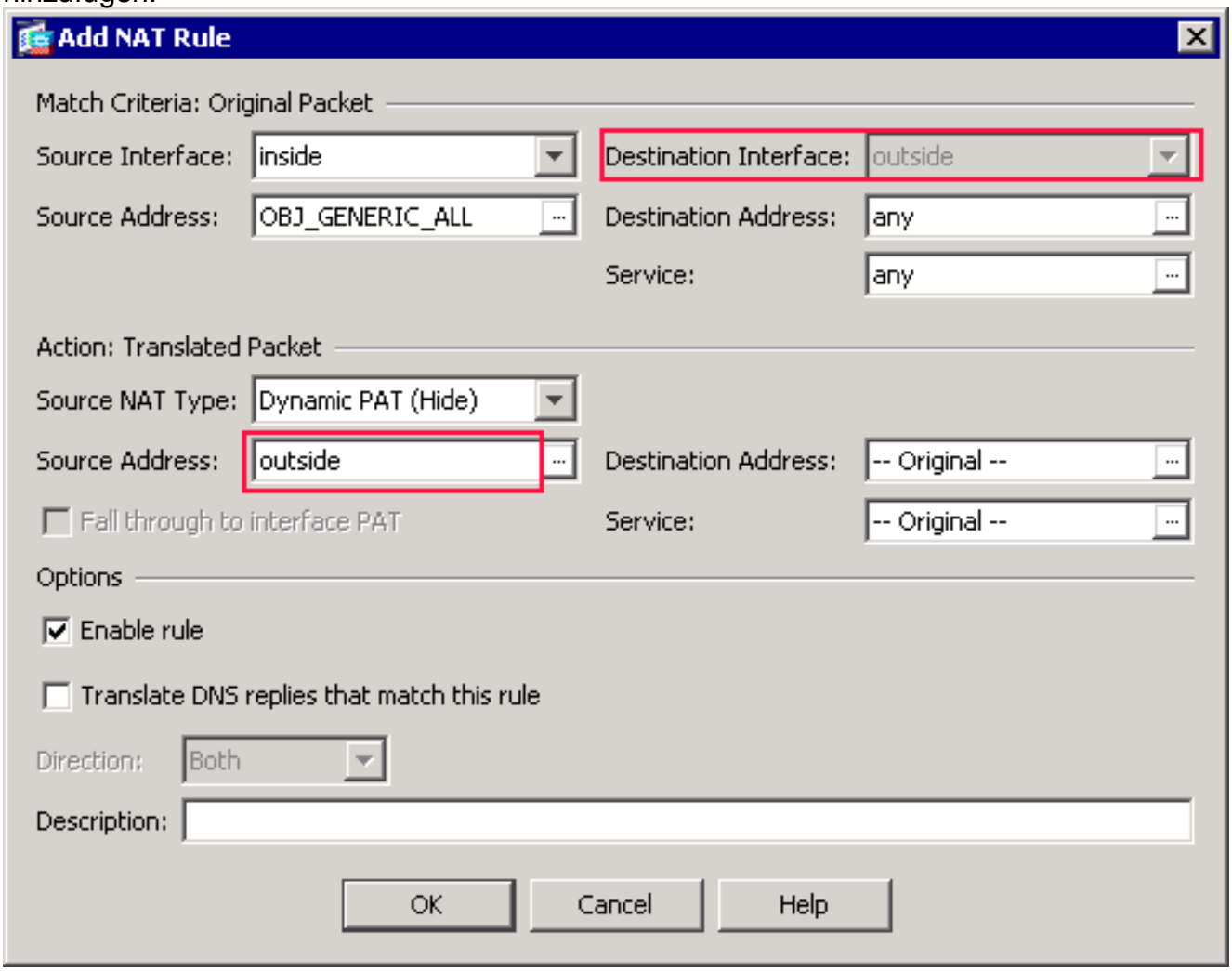


Das Dialogfeld "Übersetzte Quelladresse durchsuchen" wird angezeigt.

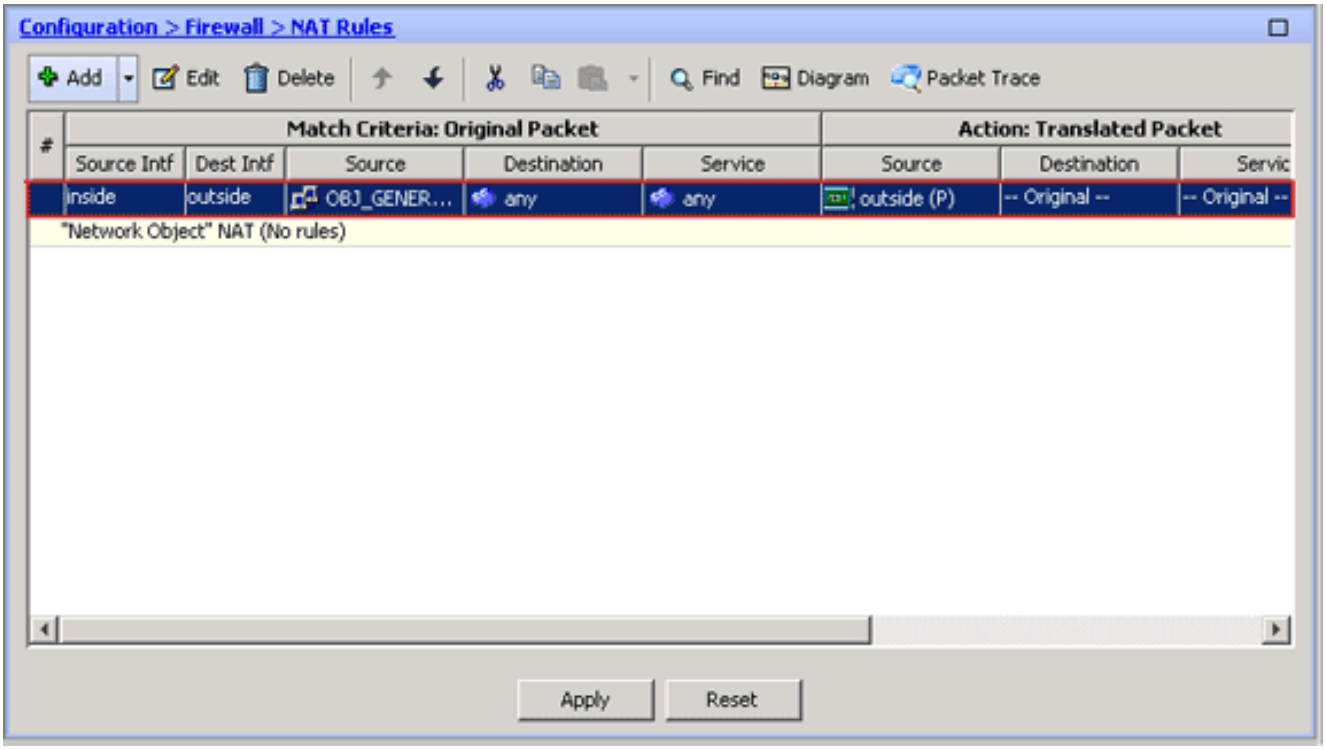


Wählen Sie im Dialogfeld Übersetzen Quelladresse durchsuchen das **externe** Schnittstellenobjekt aus. (Diese Schnittstelle wurde bereits erstellt, da sie Teil der ursprünglichen Konfiguration ist.)Klicken Sie auf **Übersetzte Quelladresse** und dann auf

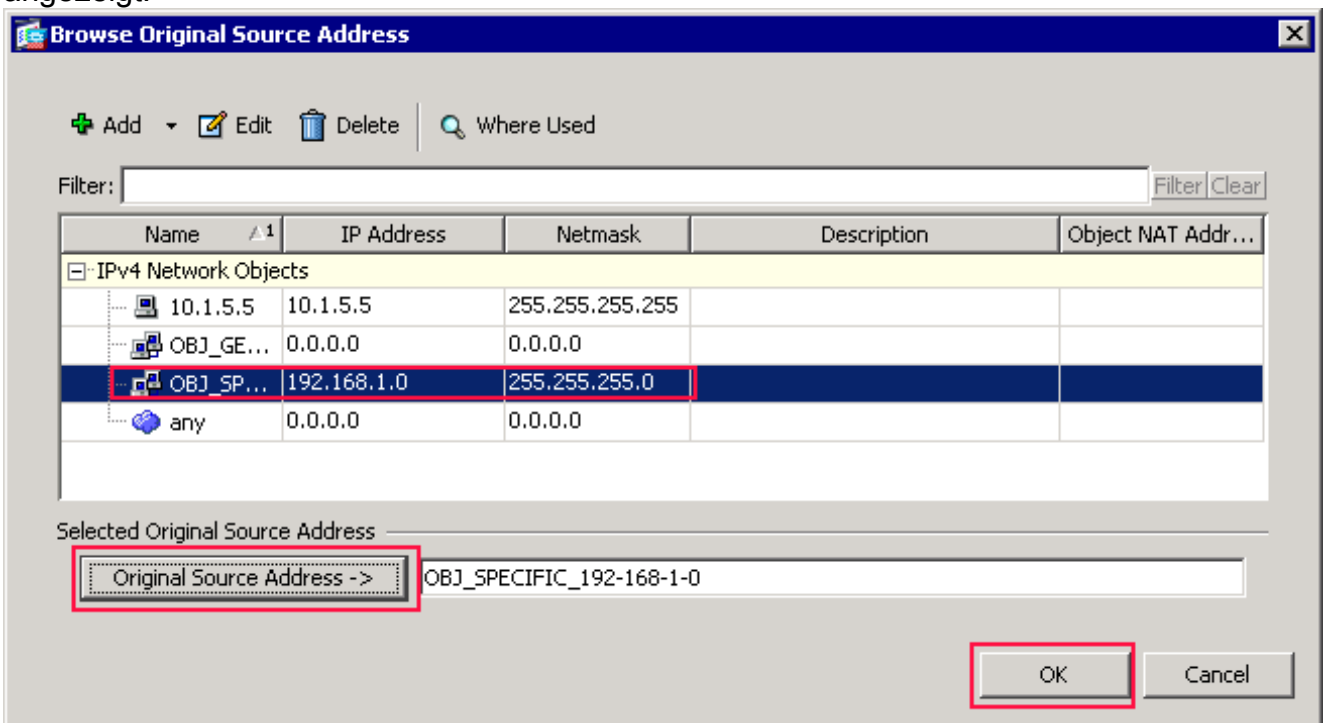
OK.Die externe Schnittstelle wird nun im Feld Quelladresse in Aktion: Übersetzter Paketbereich im Dialogfeld NAT-Regel hinzufügen.



Hinweis: Das Feld *Zielschnittstelle* wird auch an die externe Schnittstelle geändert.Überprüfen Sie, ob die erste ausgefüllte PAT-Regel wie folgt angezeigt wird:In den Match Criteria: Überprüfen Sie die folgenden Werte:Quellschnittstelle = innenQuelladresse = OBJ_GENERIC_ALLZieladresse = beliebigeService = anyIn der Aktion: Übersetzter Paketbereich: Überprüfen Sie die folgenden Werte:Source NAT Type = Dynamic PAT (Ausblenden)Quelladresse = externZieladresse = OriginalService = OriginalKlicken Sie auf **OK**.Die erste NAT-Regel wird im ASDM angezeigt, wie in diesem Bild gezeigt:

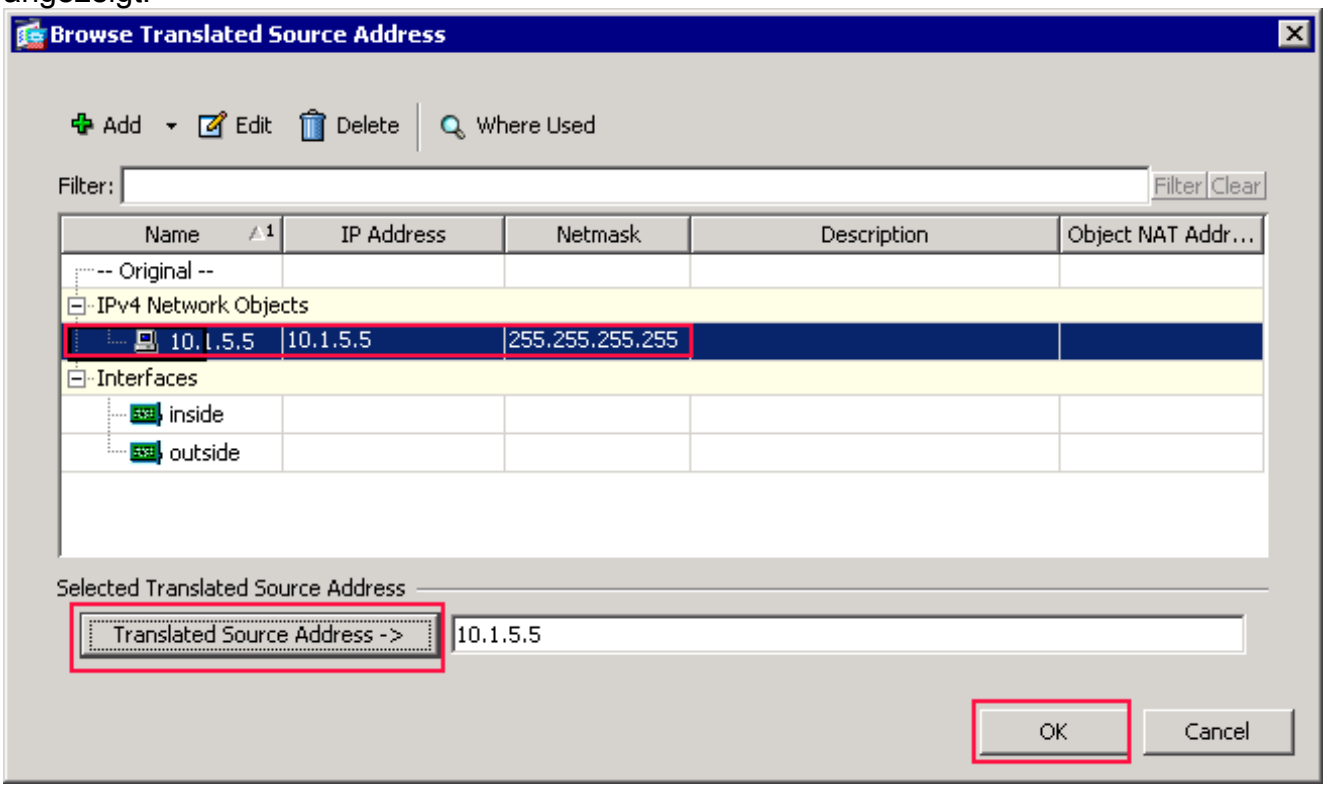


2. Erstellen Sie die zweite NAT/PAT-Regel:Wählen Sie im ASDM **Configuration > Firewall > NAT Rules aus**, und klicken Sie auf **Add**.In den Match Criteria: Der ursprüngliche Paketbereich im Dialogfeld NAT-Regel hinzufügen wählen Sie **innerhalb** der Dropdownliste Quellschnittstelle aus.Klicken Sie auf die Schaltfläche Durchsuchen (**...**) rechts neben dem Feld Quelladresse.Das Dialogfeld Ursprüngliche Quelladresse durchsuchen wird angezeigt.

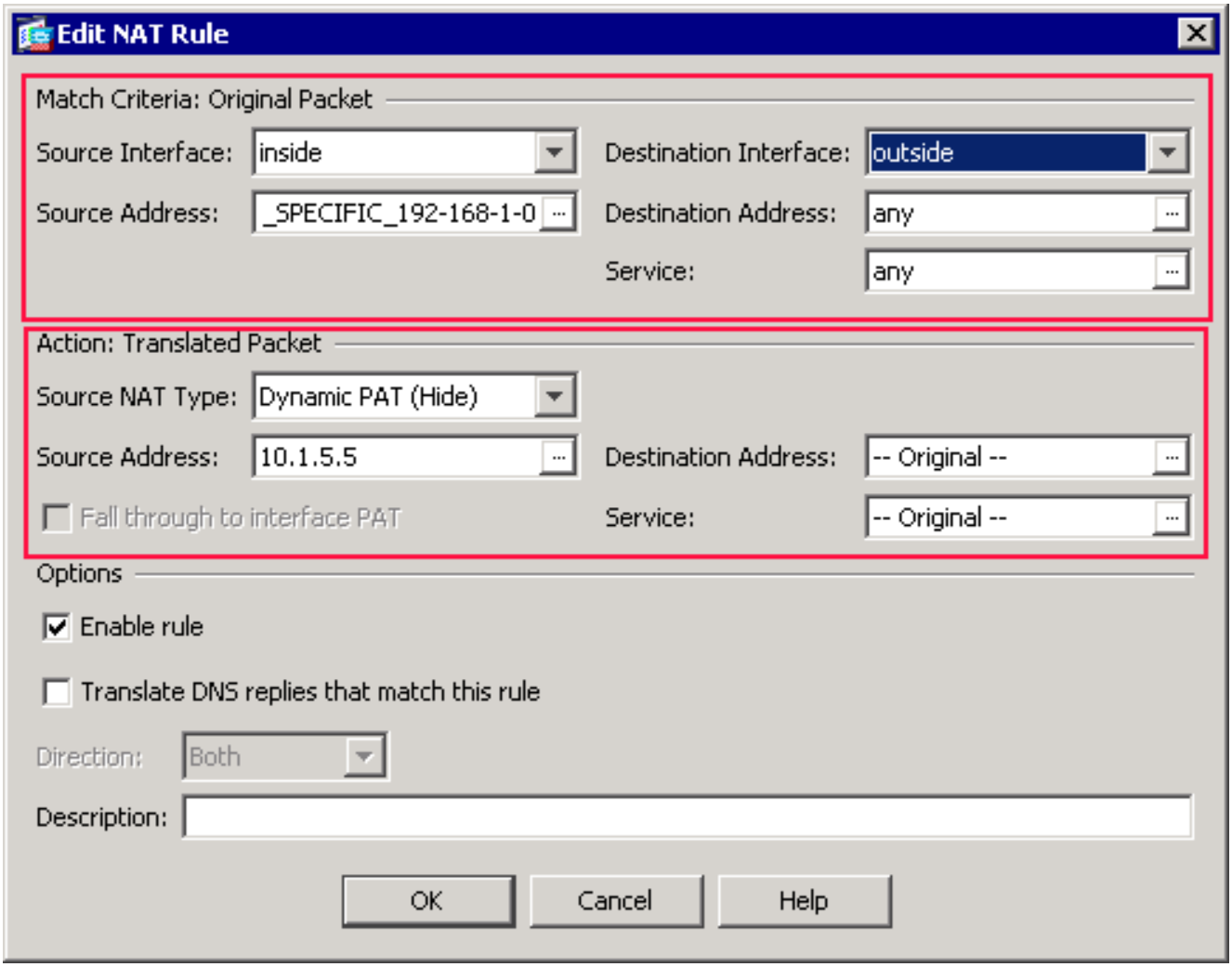


Wählen Sie im Dialogfeld Quelladresse durchsuchen das zweite Objekt, das Sie erstellt haben. (Wählen Sie in diesem Beispiel **OBJ_SPECIFIC_192-168-1-0 aus**.)Klicken Sie auf **Originalquelladresse** und dann auf **OK**.Das Netzwerkobjekt *OBJ_SPECIFIC_192-168-1-0* wird im Feld "Source Address" (Quelladresse) im Feld "Match Criteria:" (Suchkriterien) angezeigt. Originalpaketbereich des Dialogfelds NAT-Regel hinzufügen.In der Aktion: Im Dialogfeld NAT-Regel hinzufügen wählen Sie im Bereich Übersetztes Paket im Dialogfeld **Dynamische PAT (Ausblenden)** im Dialogfeld Source NAT Type (NAT-Ausgangstyp)

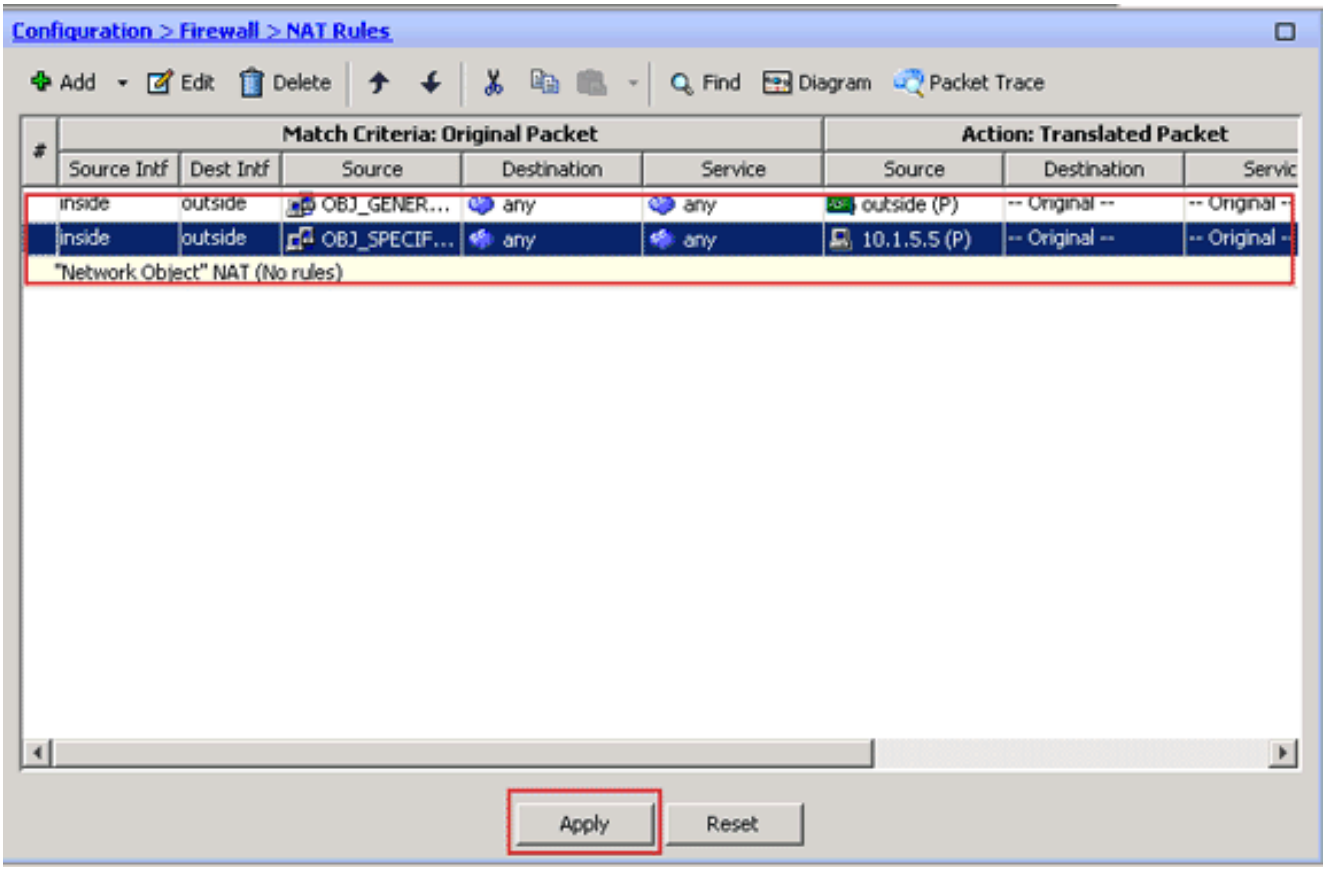
aus.Klicken Sie auf die Schaltfläche **..** rechts neben dem Feld Quelladresse.Das Dialogfeld "Übersetzte Quelladresse durchsuchen" wird
angezeigt.



Wählen Sie im Dialogfeld Quelladresse durchsuchen das Objekt **10.1.5.5**. (Diese Schnittstelle wurde bereits erstellt, da sie Teil der ursprünglichen Konfiguration ist.)Klicken Sie auf **Übersetzte Quelladresse** und dann auf **OK**.Das Netzwerkobjekt **10.1.5.5** wird im Feld Quelladresse in Aktion: Übersetzter Paketbereich des Dialogfelds NAT-Regel hinzufügen.In den Match Criteria: Wählen Sie in der Dropdown-Liste "Zielschnittstelle" die Option "Original Packet Area" **außerhalb** aus.**Hinweis:** Wenn Sie diese Option nicht *außerhalb* auswählen, wird die Zielschnittstelle auf *Any (Beliebig)*
verweisen.



Überprüfen Sie, ob die zweite abgeschlossene NAT/PAT-Regel wie folgt angezeigt wird:In den Match Criteria: Überprüfen Sie die folgenden Werte:Quellschnittstelle = innenQuelladresse = OBJ_SPECIFIC_192-168-1-0Zieladresse = außerhalbService = anyIn der Aktion: Übersetzter Paketbereich: Überprüfen Sie die folgenden Werte:Source NAT Type = Dynamic PAT (Ausblenden)Quelladresse = 10.1.5.5Zieladresse = OriginalService = OriginalKlicken Sie auf **OK**.Die abgeschlossene NAT-Konfiguration wird im ASDM angezeigt, wie in diesem Bild
gezeigt:



3. Klicken Sie auf die Schaltfläche **Apply**, um die Änderungen auf die aktuelle Konfiguration anzuwenden.

Damit ist die Konfiguration der dynamischen PAT auf einer Cisco Adaptive Security Appliance (ASA) abgeschlossen.

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

Überprüfen der allgemeinen PAT-Regel

- show local-host - Zeigt die Netzwerkstatus der lokalen Hosts an.

```
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 - Zeigt den Verbindungsstatus für den festgelegten Verbindungstyp an.

```
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 - Zeigt Informationen zu den Übersetzungssteckplätzen an.

```
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
```

Überprüfen einer bestimmten PAT-Regel

- show local-host - Zeigt die Netzwerkstatus der lokalen Hosts an.

```
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 - Zeigt den Verbindungsstatus für den festgelegten Verbindungstyp an.

```
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 - Zeigt Informationen zu den Übersetzungssteckplätzen an.

```
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
```

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- Cisco Adaptive Security Device Manager
- Cisco Adaptive Security Appliances der Serie ASA 5500
- Anforderungen für Kommentare (RFCs)
- Technischer Support und Dokumentation - Cisco Systems