Contents

Introduction

This document explains how to configure Port Redirection (Forwarding) and the outside Network Address Translation (NAT) features in Adaptive Security Appliance (ASA) Software Version 9.x, with the use of the CLI or the Adaptive Security Device Manager (ASDM).

Refer to the Cisco ASA Series Firewall ASDM Configuration Guide for additional information.

Prerequisites

Requirements

Refer to Configuring Management Access in order to allow the device to be configured by the ASDM.

Components Used

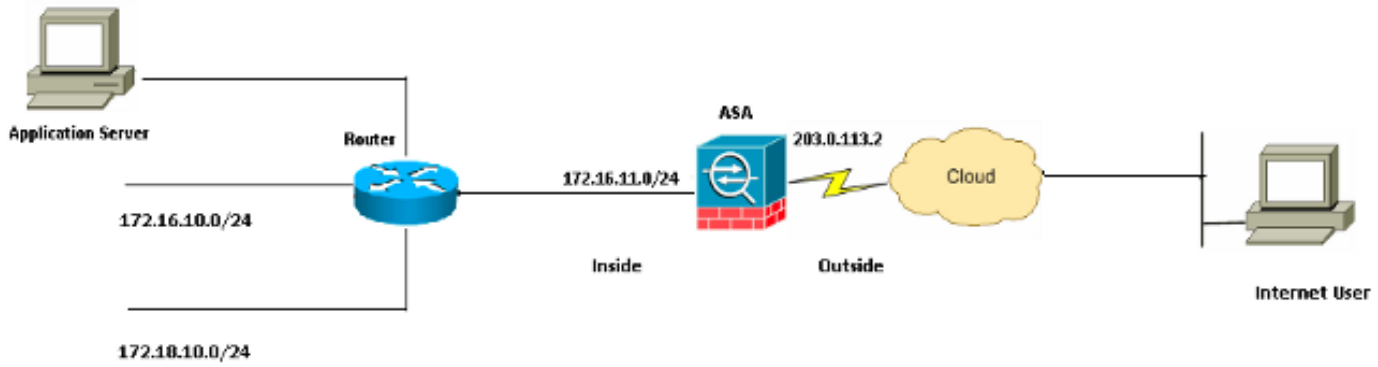
The information in this document is based on these software and hardware versions:

- Cisco ASA 5525 Series Security Appliance Software Version 9.x and later
- ASDM Version 7.x and later

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configure

Network Diagram



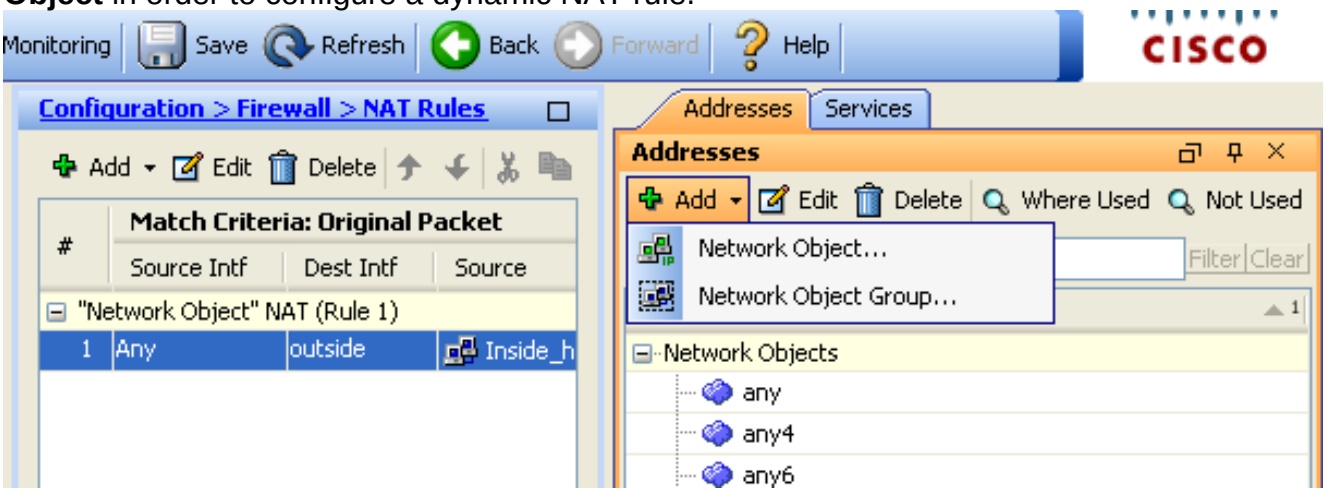
The IP addressing schemes used in this configuration are not legally routable on the Internet. They are RFC 1918 addresses which have been used in a lab environment.

Allow Inside Hosts Access to Outside Networks with PAT

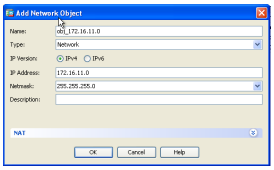
If you want inside hosts to share a single public address for translation, use Port Address Translation (PAT). One of the simplest PAT configurations involves the translation of all internal hosts to look like the outside interface IP address. This is the typical PAT configuration that is used when the number of routable IP addresses available from the ISP is limited to only a few, or perhaps just one.

Complete these steps in order to allow inside hosts access to outside networks with PAT:

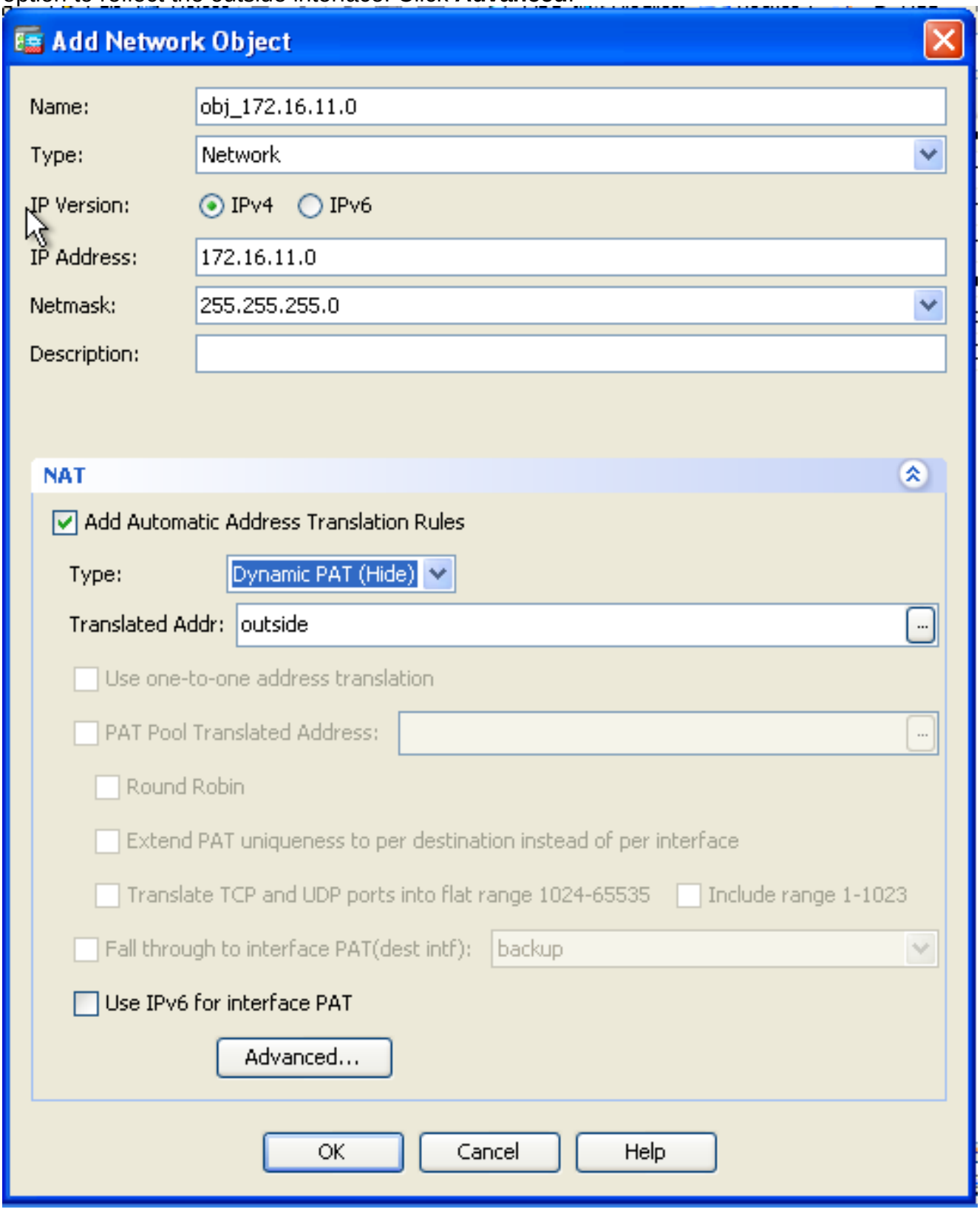
1. Choose **Configuration** > **Firewall** > **NAT Rules**. Click **Add** and then choose **Network Object** in order to configure a dynamic NAT rule.



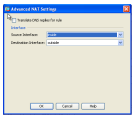
2. Configure the network/Host/Range for which **Dynamic PAT** is required. In this example, one of the inside subnets has been selected. This process can be repeated for other subnets you wish to translate in this manner.



3. Expand NAT. Check the **Add Automatic Address Translation Rules** check box. In the Type drop-down list, choose **Dynamic PAT (Hide)**. In the **Translated Addr** field, choose the option to reflect the outside interface. Click **Advanced**.



4. In the Source Interface and Destination Interface drop-down lists, choose the appropriate interfaces. Click **OK** and click **Apply** for the changes to take effect.



This is the equivalent CLI output for this PAT configuration:

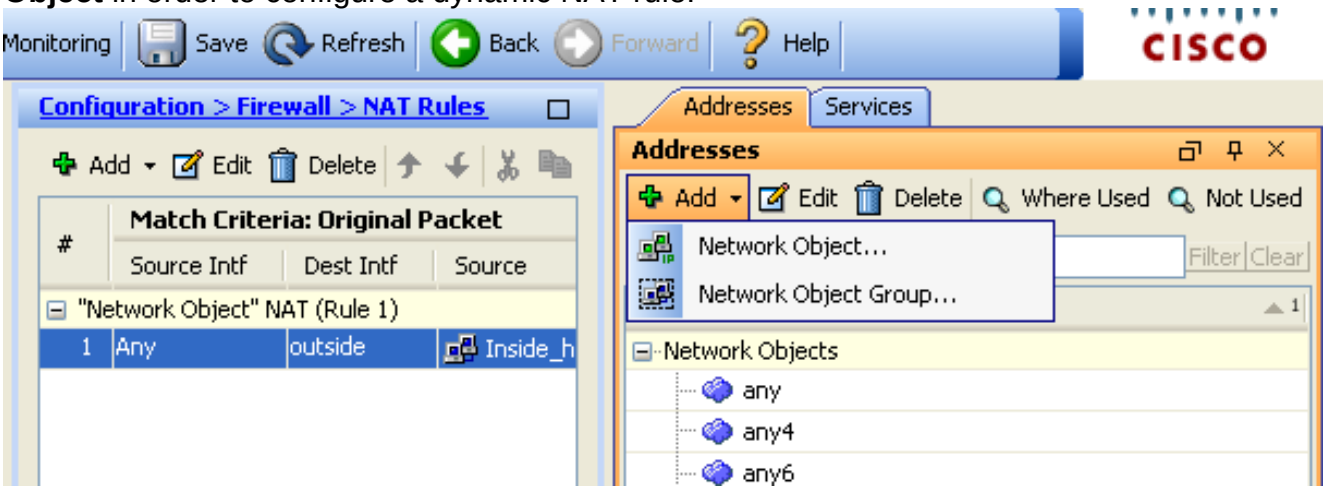
Allow Inside Hosts Access to Outside Networks with NAT

You could allow a group of inside hosts/networks to access the outside world with the configuration of the dynamic NAT rules. Unlike PAT, Dynamic NAT allocates translated addresses from a pool of addresses. As a result, a host is mapped to its own translated IP address and two hosts cannot share the same translated IP address.

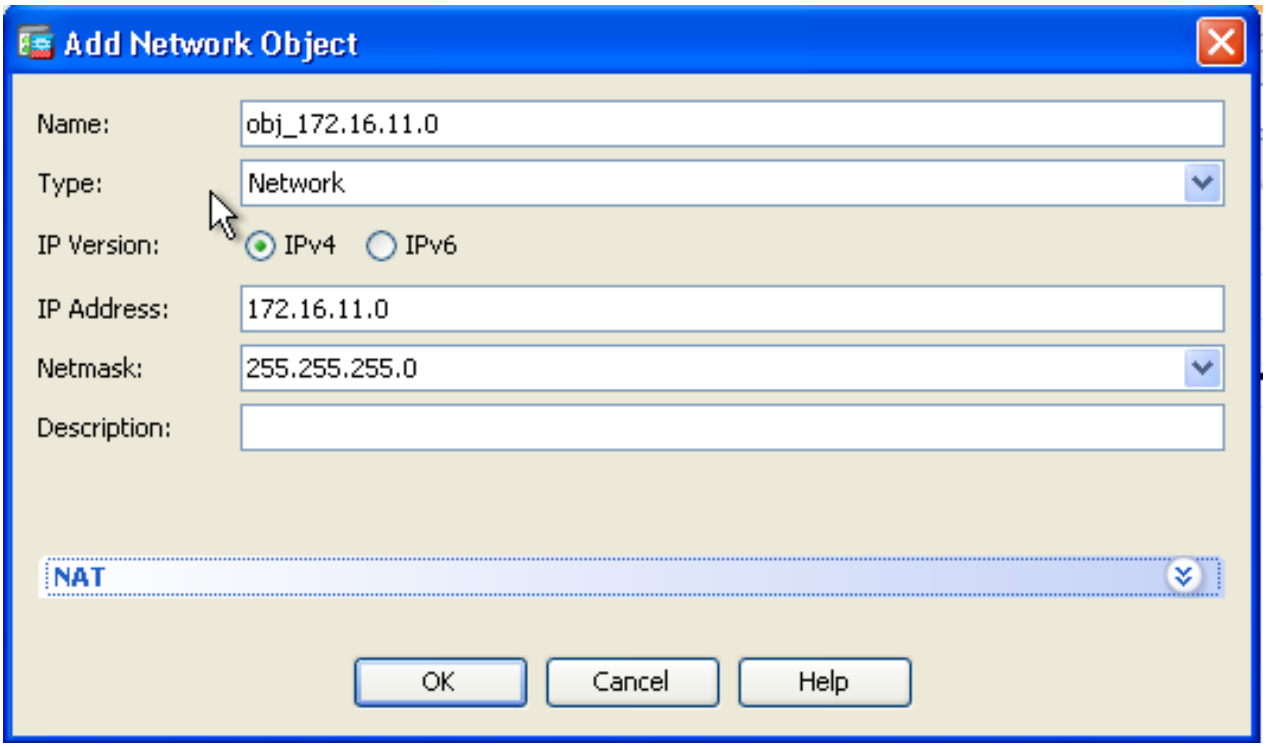
In order to accomplish this, you need to select the real address of the hosts/networks to be given access and they then have to be mapped to a pool of translated IP addresses.

Complete these steps in order to allow inside hosts access to outside networks with NAT:

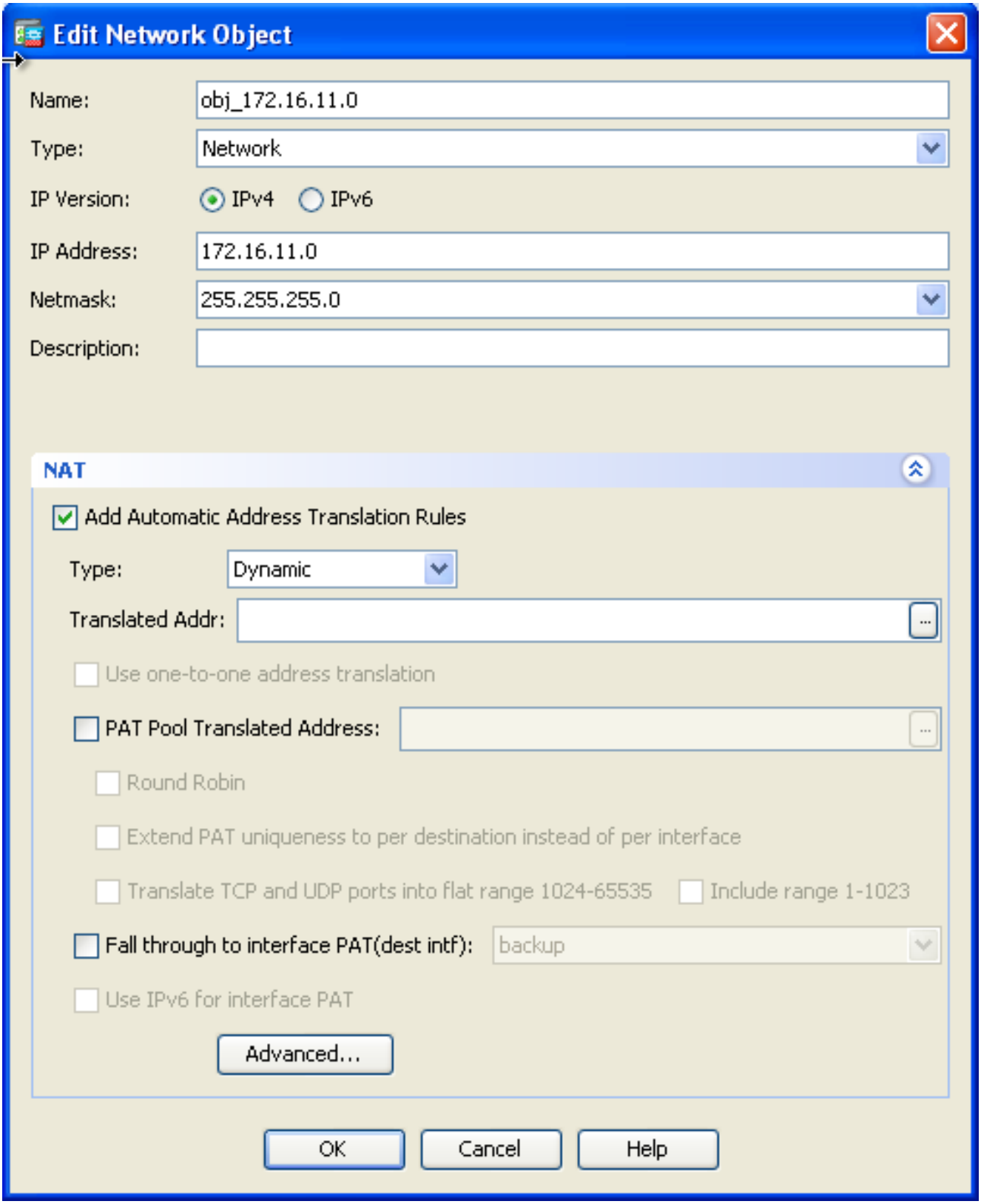
1. Choose **Configuration** > **Firewall** > **NAT Rules**. Click **Add** and then choose **Network Object** in order to configure a dynamic NAT rule.



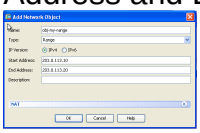
2. Configure the network/Host/Range for which Dynamic PAT is required. In this example, the entire *inside-network* has been selected.



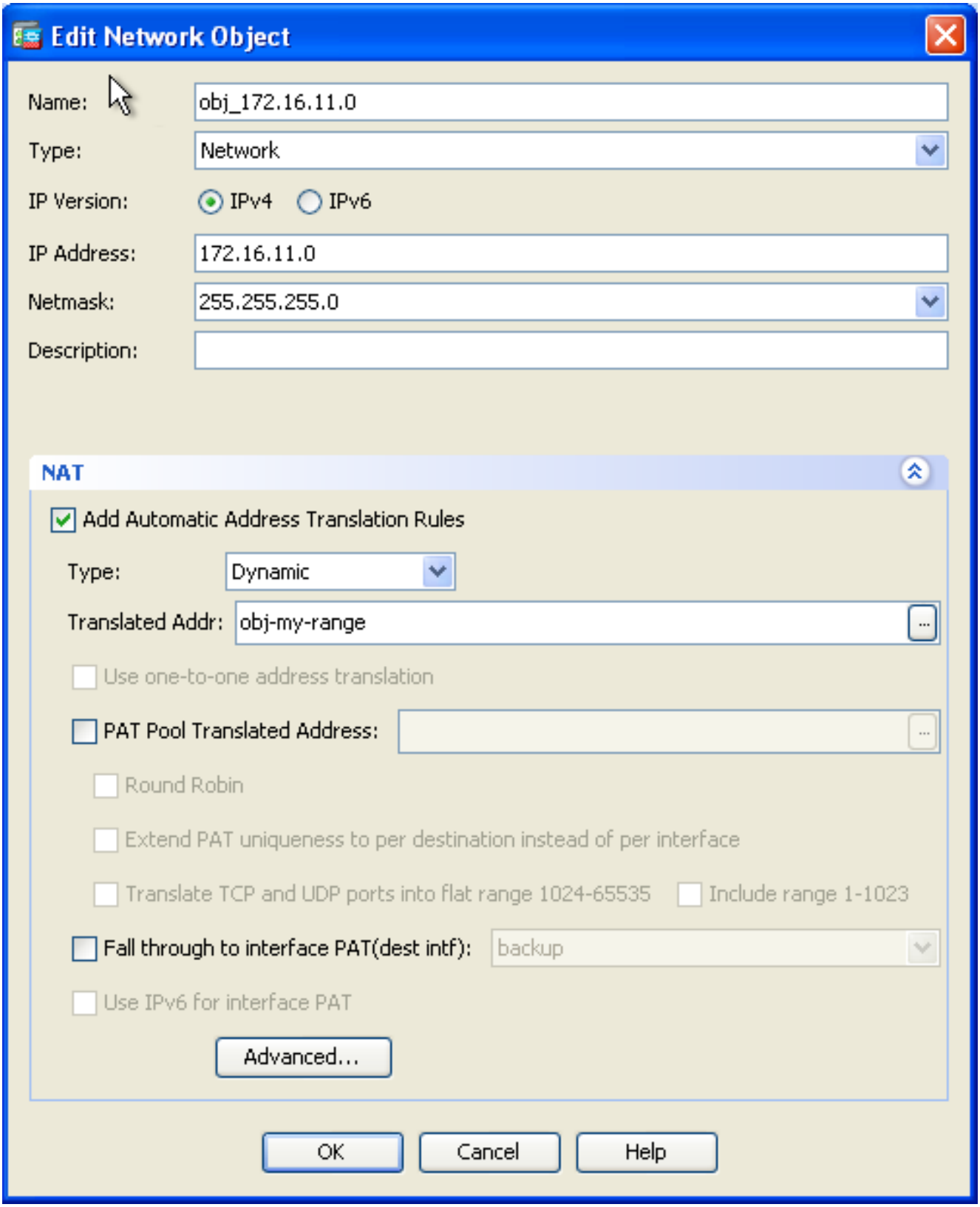
3. Expand NAT. Check the **Add Automatic Address Translation Rules** check box. In the Type drop-down list, choose **Dynamic**. In the Translated Addr field, choose the appropriate selection. Click **Advanced**.



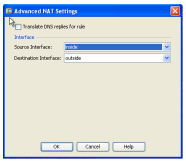
4. Click **Add** to add the network object. In the Type drop-down list, choose **Range**. In the Start Address and End Address fields, enter the starting and ending PAT IP addresses. Click **OK**.



5. In the Translated Addr field, choose the address object. Click **Advanced** in order to select the source and destination interfaces.



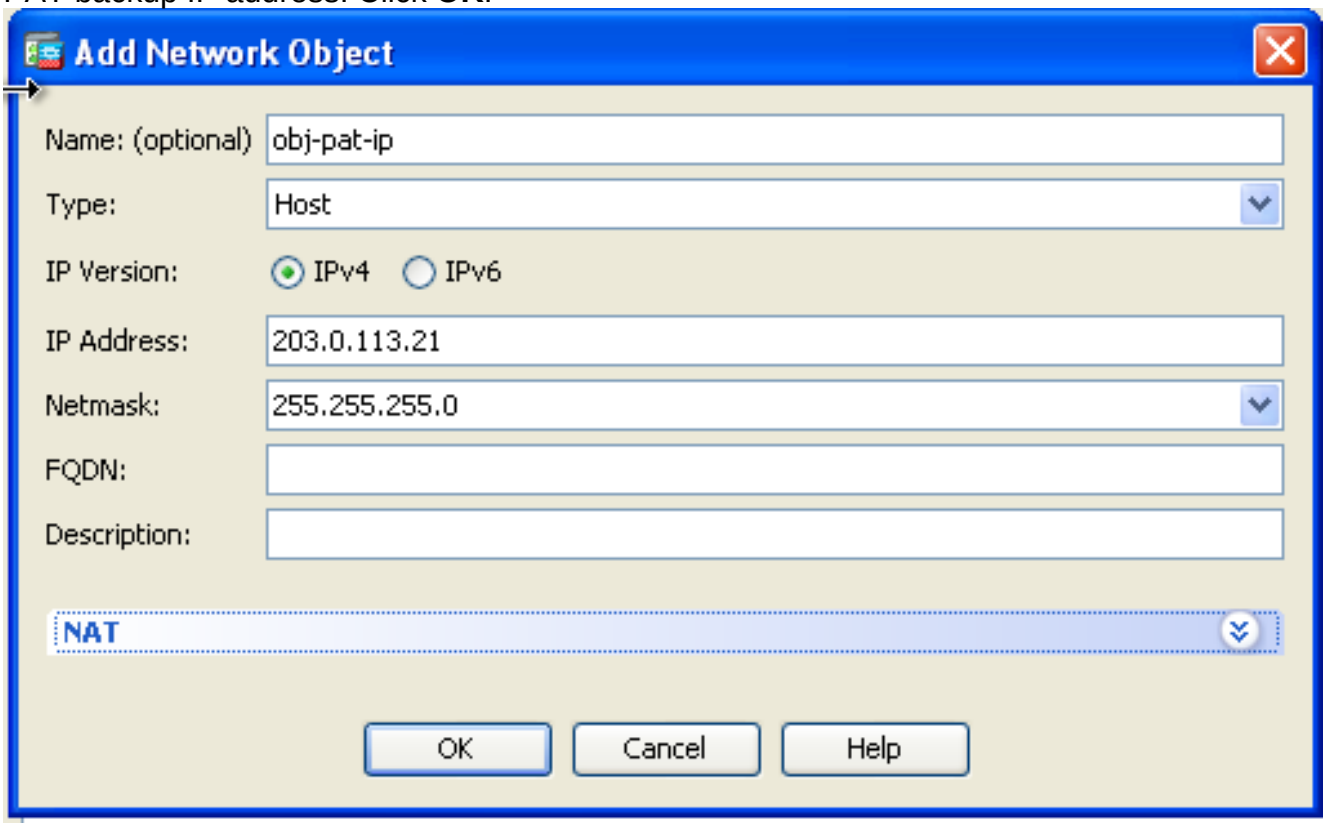
6. In the Source Interface and Destination Interface drop-down lists, choose the appropriate interfaces. Click **OK** and click **Apply** for the changes to take effect.



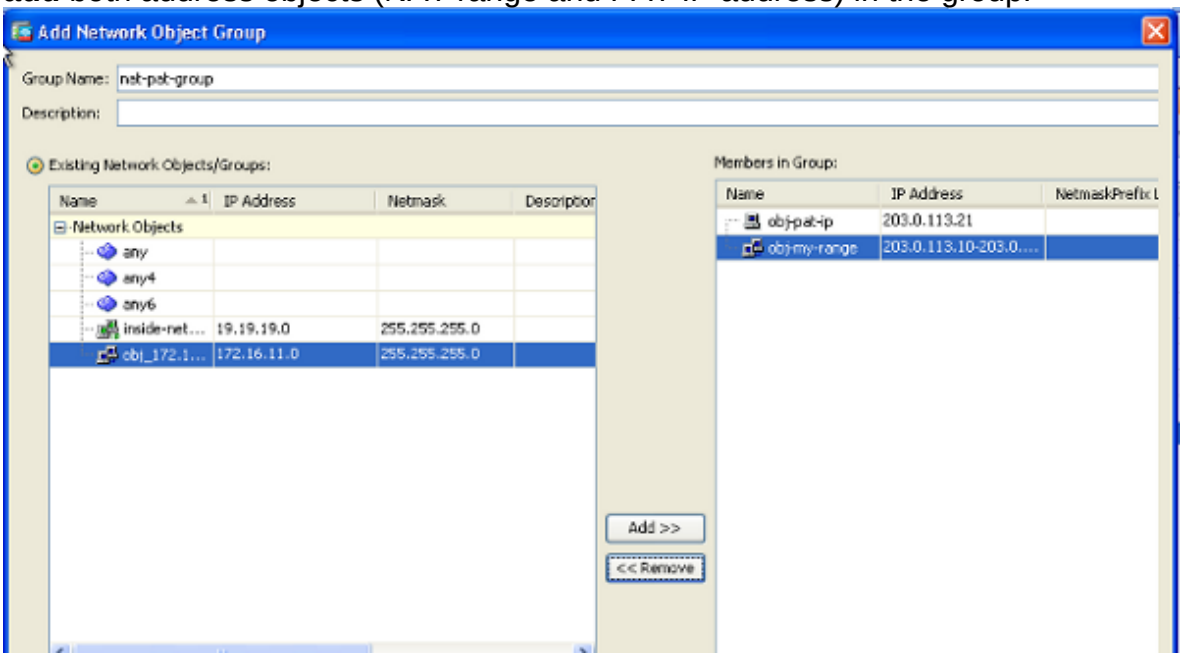
This is the equivalent CLI output for this ASDM configuration:

As per this configuration, the hosts in the 172.16.11.0 network will get translated to any IP address from the NAT pool, 203.0.113.10 - 203.0.113.20. If the mapped pool has fewer addresses than the real group, you could run out of addresses. As a result, you could try to implement dynamic NAT with dynamic PAT backup or you could try to expand the existing pool.

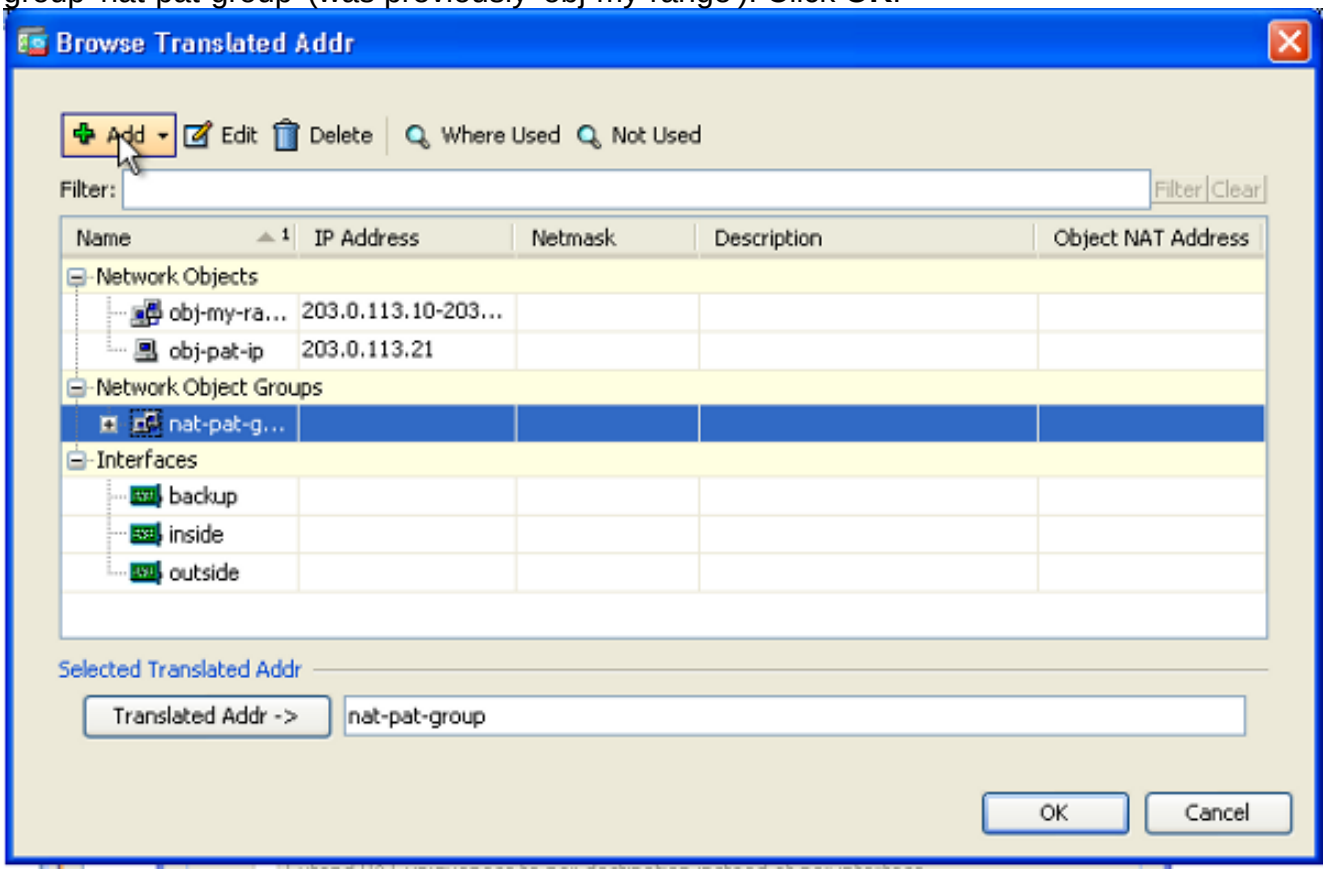
1. Repeat steps 1 to 3 in the previous configuration and click **Add** once again in order to add a network object. In the Type drop-down list, choose **Host**. In the IP Address field, enter the PAT backup IP address. Click **OK**.



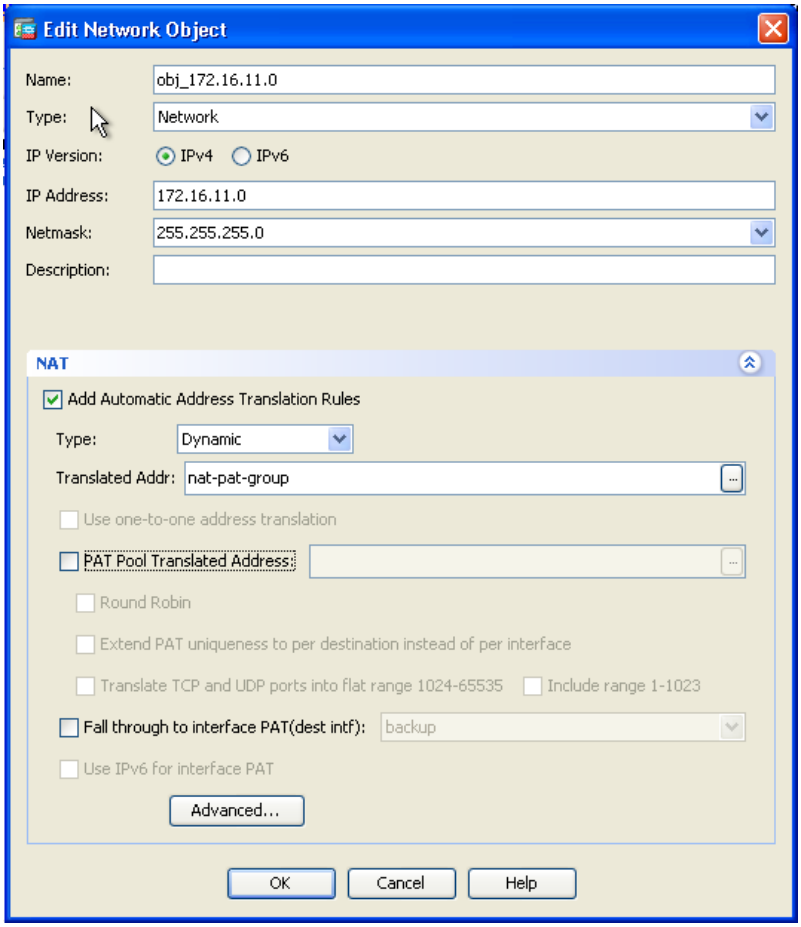
2. Click **Add** to add a network object group. In the Group Name field, enter a group name and **add** both address objects (NAT range and PAT IP address) in the group.



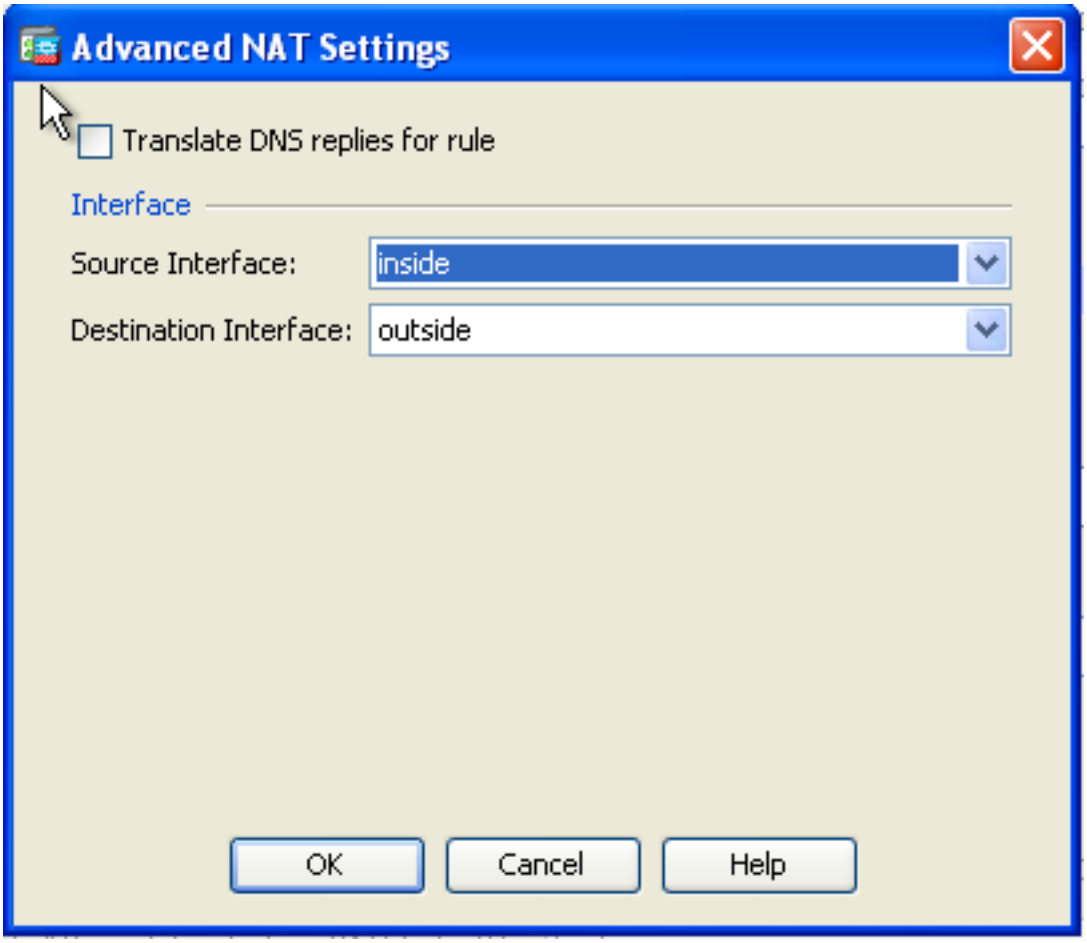
3. Choose the configured NAT rule and change the Translated Addr to be the newly configured group 'nat-pat-group' (was previously 'obj-my-range'). Click **OK**.



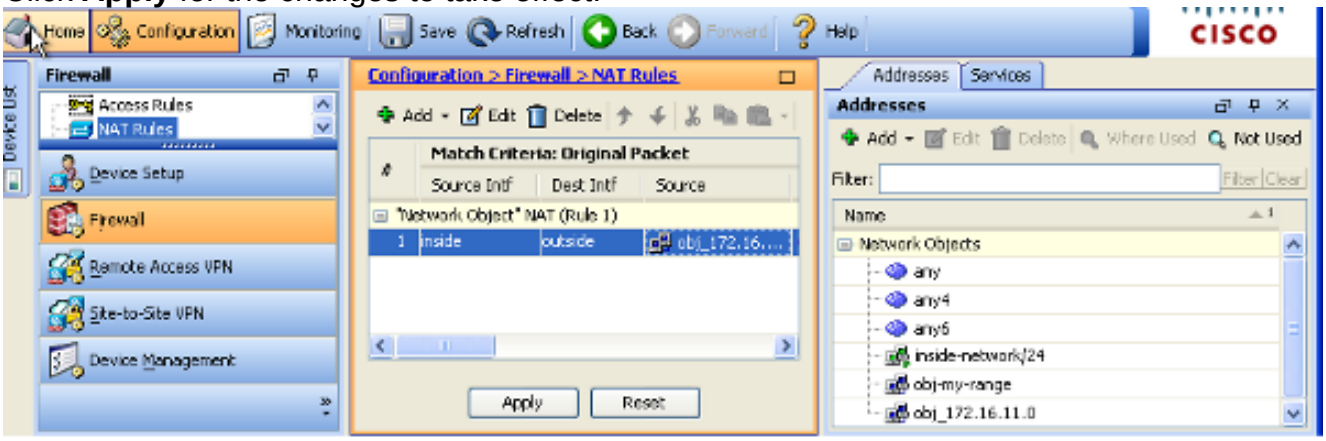
4. Click **OK** in order to add the NAT rule. Click **Advanced** in order to select the source and destination interfaces.



5. In the Source Interface and Destination Interface drop-down lists, choose the appropriate interfaces. Click **OK**.



6. Click **Apply** for the changes to take effect.



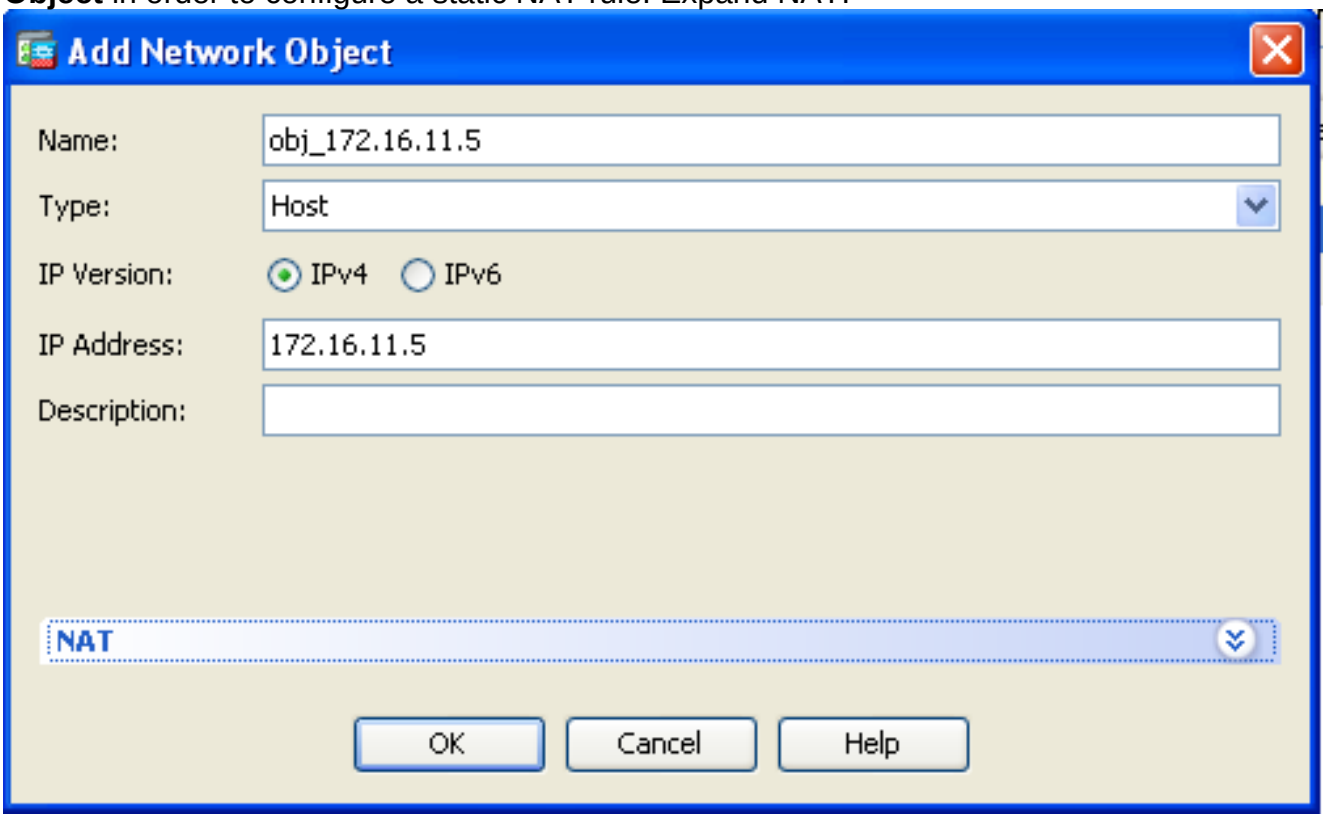
This is the equivalent CLI output for this ASDM configuration:

Allow Untrusted Hosts Access to Hosts on Your Trusted Network

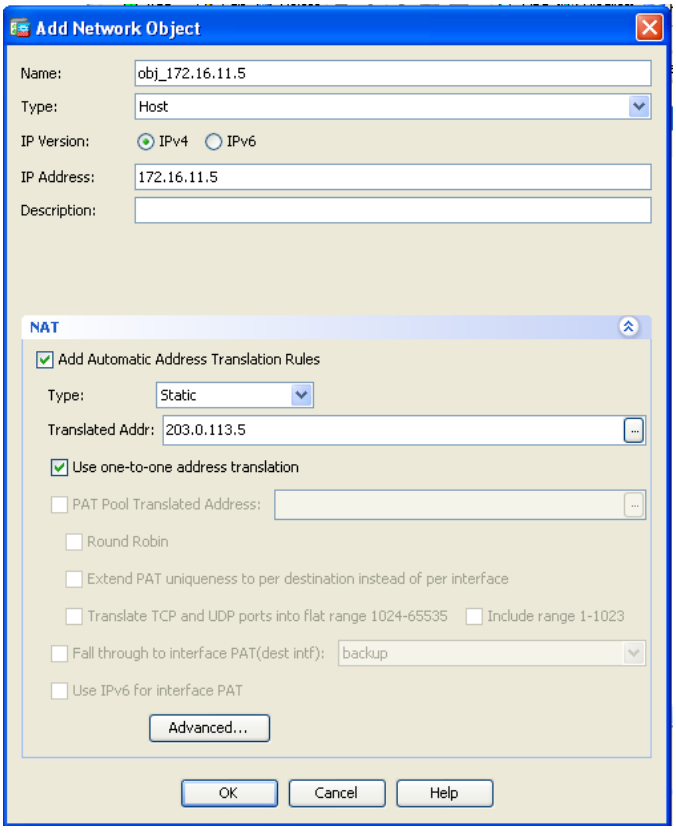
This can be achieved through the application of a static NAT translation and an access rule to permit those hosts. You are required to configure this whenever an outside user would like to access any server that sits in your internal network. The server in the internal network will have a private IP address which is not routable on the Internet. As a result, you need to translate that private IP address to a public IP address through a static NAT rule. Suppose you have an internal

server (172.16.11.5). In order to make this work, you need to translate this private server IP address to a public IP address. This example describes how to implement the bidirectional static NAT to translate 172.16.11.5 to 203.0.113.5.

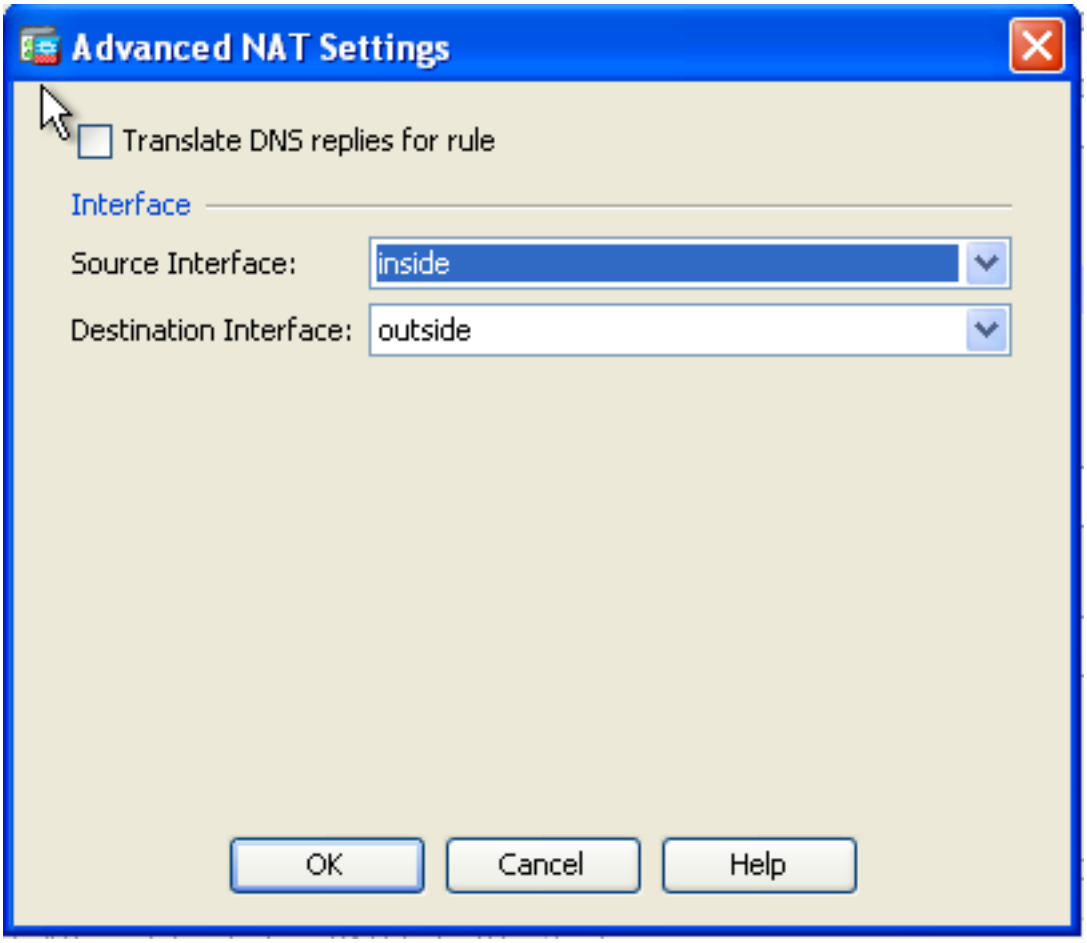
1. Choose **Configuration** > **Firewall** > **NAT Rules**. Click **Add** and then choose **Network Object** in order to configure a static NAT rule. Expand NAT.



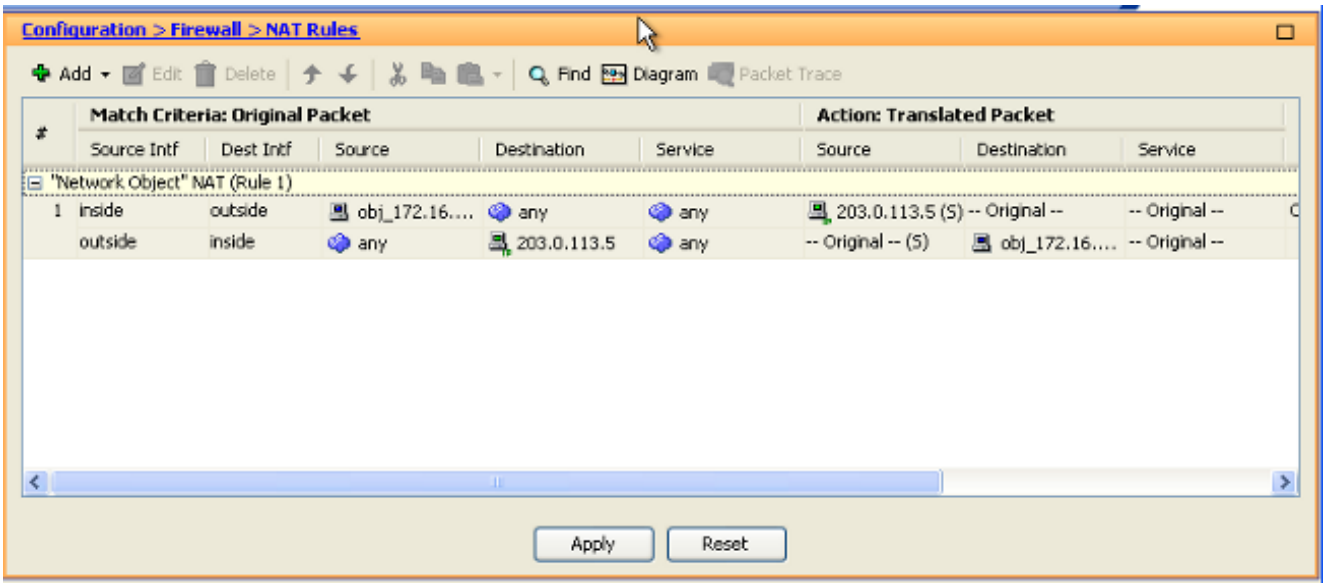
2. Check the **Add Automatic Address Translation Rules** check box. In the Type drop-down list, choose **Static.** In the Translated Addr field, enter the IP address. Click **Advanced** in order to select the source and destination interfaces.



3. In the Source Interface and Destination Interface drop-down lists, choose the appropriate interfaces. Click **OK**.



4. You can see the configured static NAT entry here. Click **Apply** in order to send this to the ASA.



This is the equivalent CLI output for this NAT configuration:

Static Identity NAT

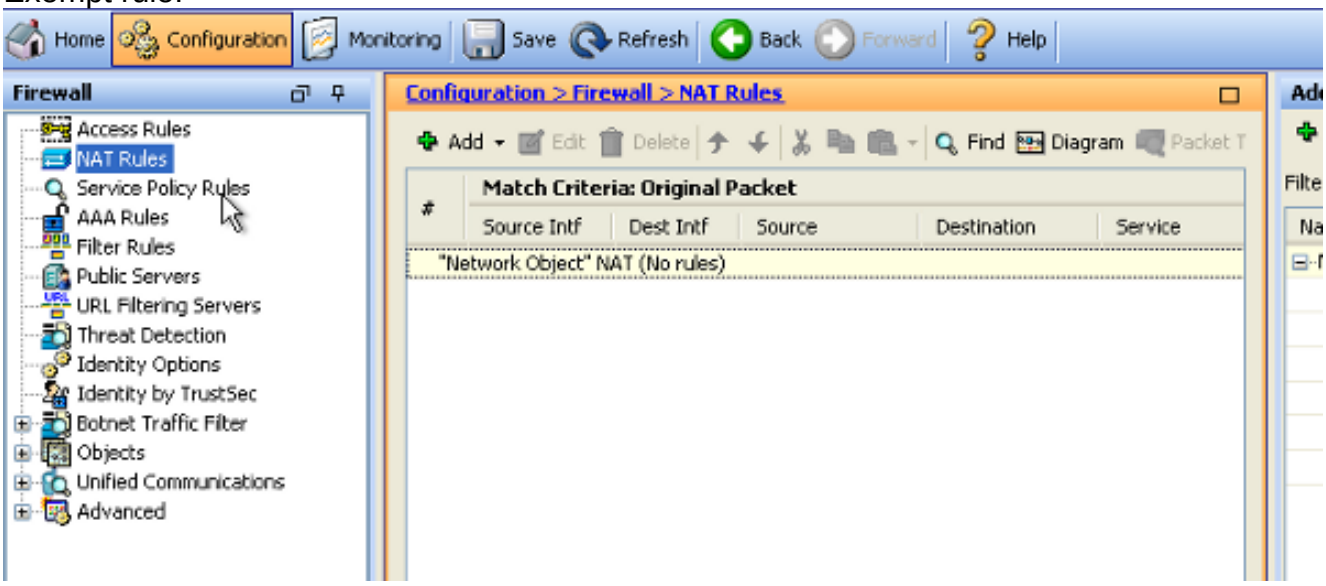
NAT Exempt is a useful feature where the inside users try to access a remote VPN host/server or some host/server hosted behind any other interface of the ASA without completion of a NAT. In

order to achieve this, the internal server, which has a private IP address, will be identity translated to itself and which in turn is allowed to access the destination which performs a NAT.

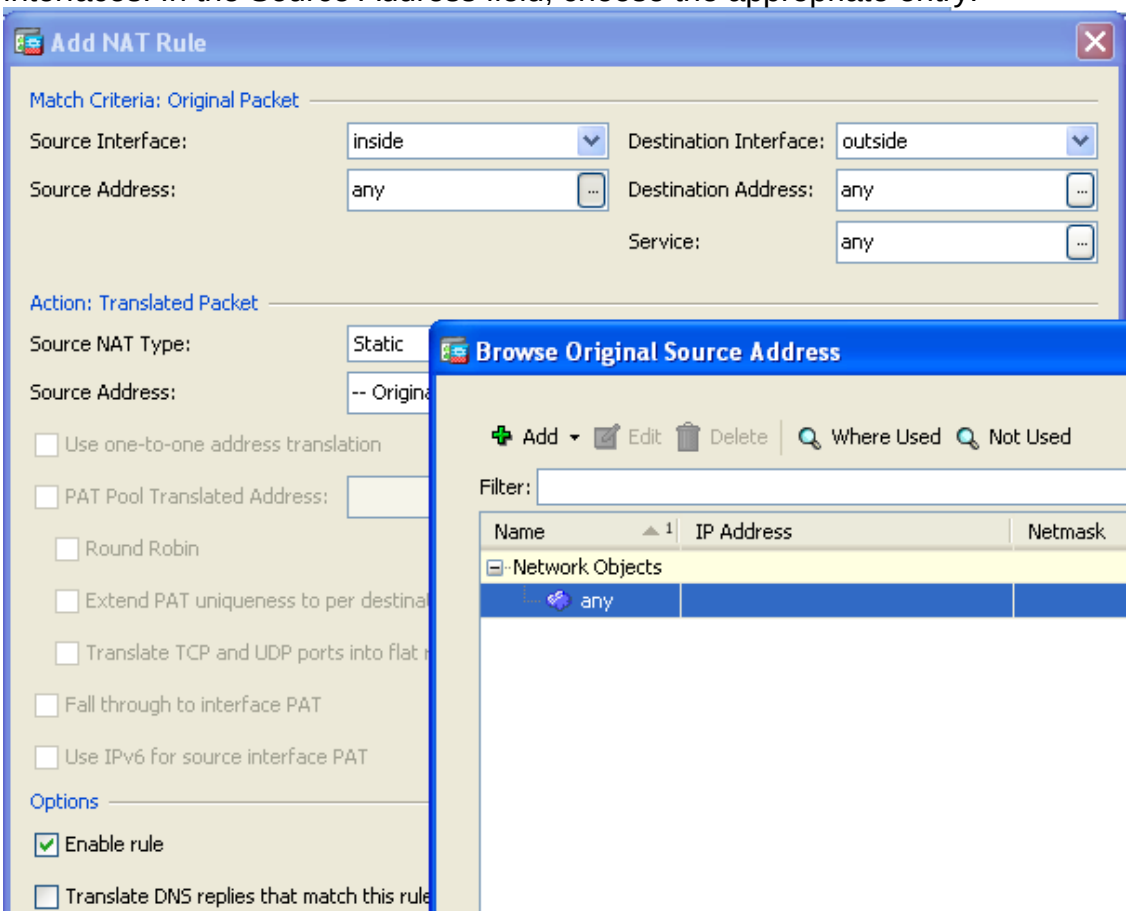
In this example, the inside host 172.16.11.15 needs to access the remote VPN server 172.20.21.15.

Complete these steps in order to allow inside hosts access to remote VPN network with completion of a NAT:

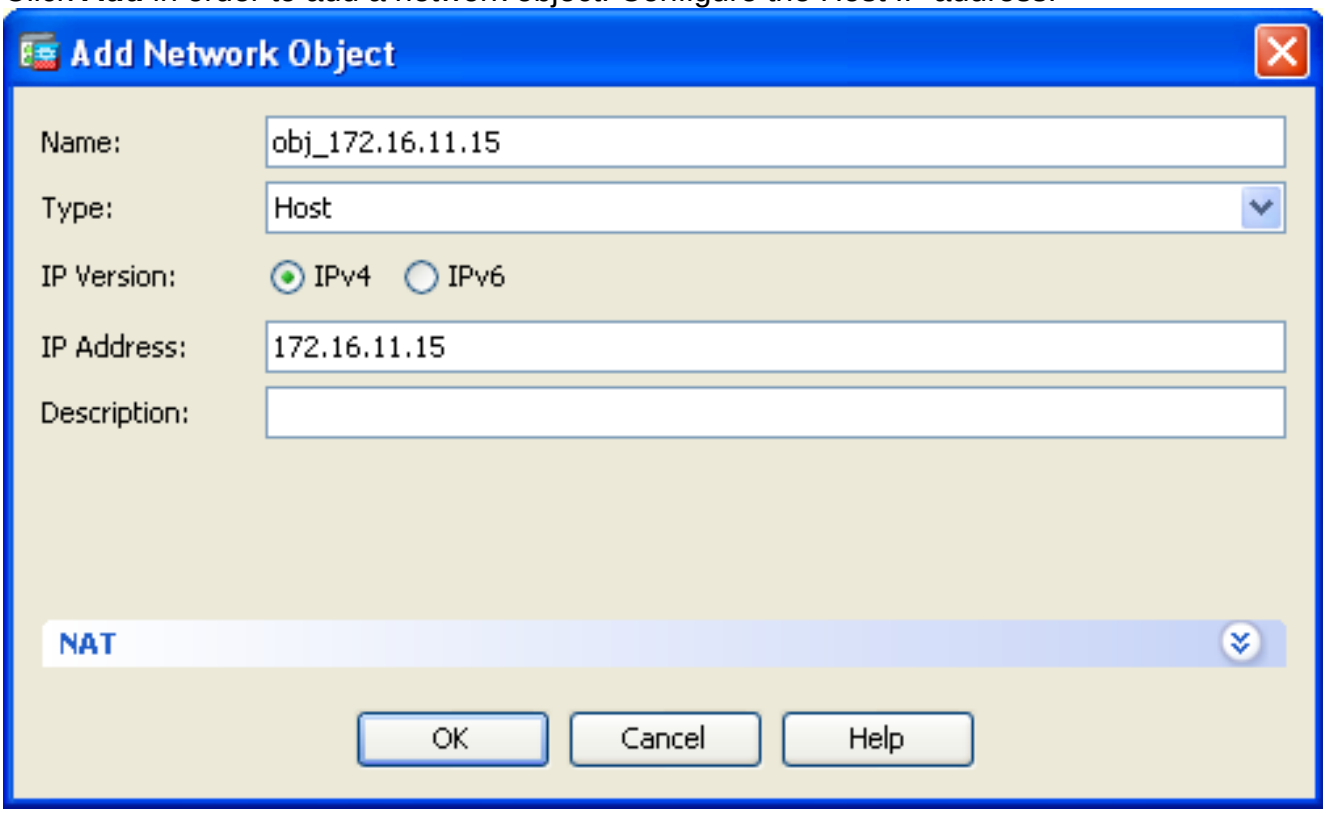
1. Choose **Configuration** > **Firewall** > **NAT Rules**. Click **Add** in order to configure a NAT Exempt rule.



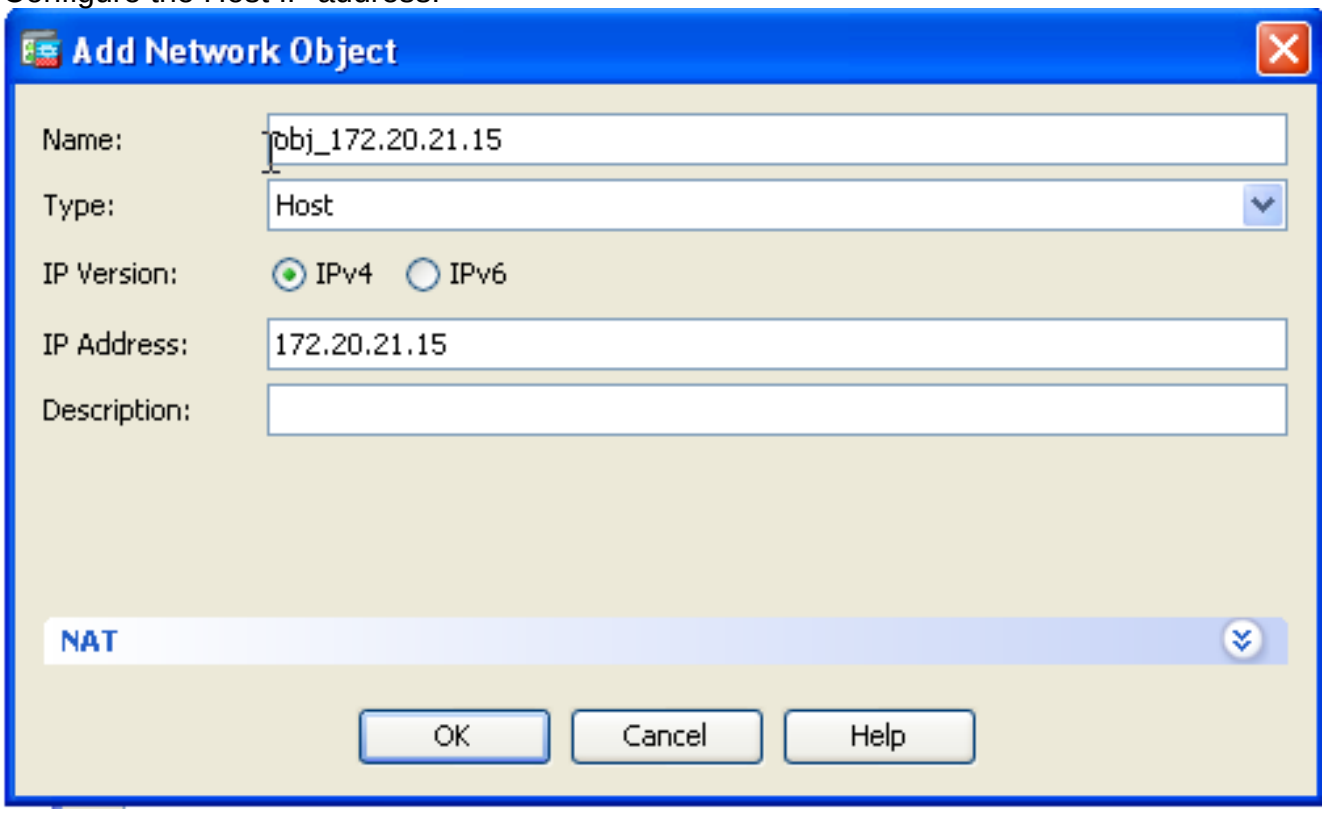
2. In the Source Interface and Destination Interface drop-down lists, choose the appropriate interfaces. In the Source Address field, choose the appropriate entry.



3. Click **Add** in order to add a network object. Configure the Host IP address.

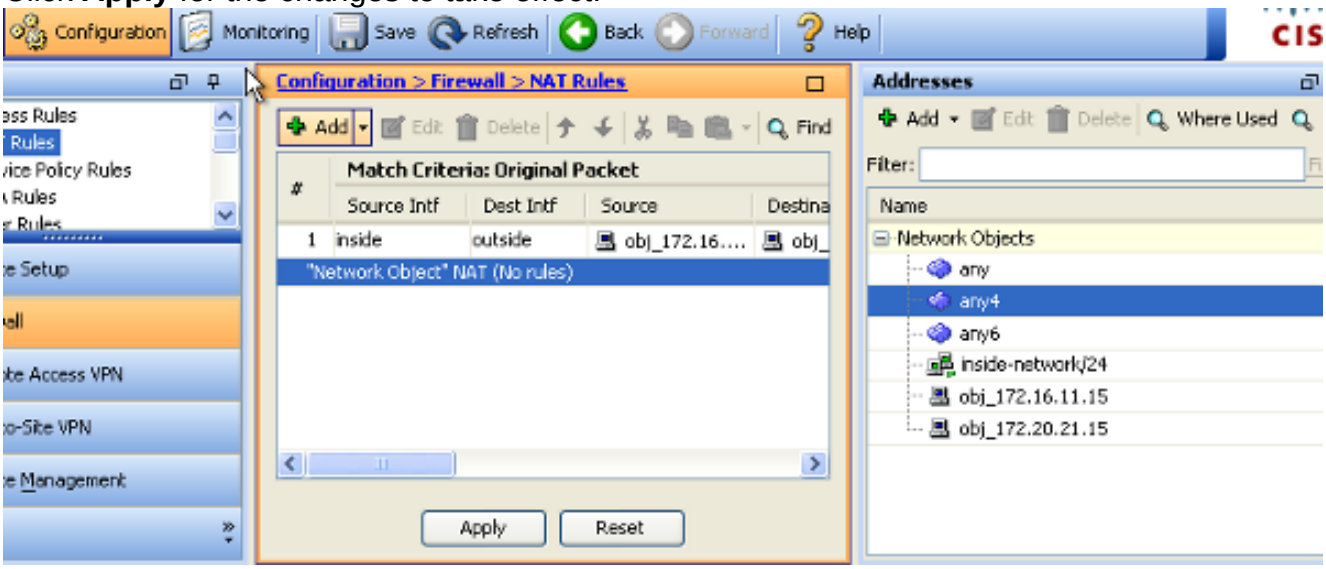


4. Similarly, browse the **Destination Address**. Click **Add** in order to add a network object. Configure the Host IP address.



5. Choose the configured Source Address and Destination Address objects. Check the **Disable Proxy ARP on egress interface** and **Lookup route table to locate egress interface** check boxes. Click **OK**.

6. Click **Apply** for the changes to take effect.



This is the equivalent CLI output for the NAT Exempt or Identity NAT configuration:

Port Redirection (Forwarding) with Static

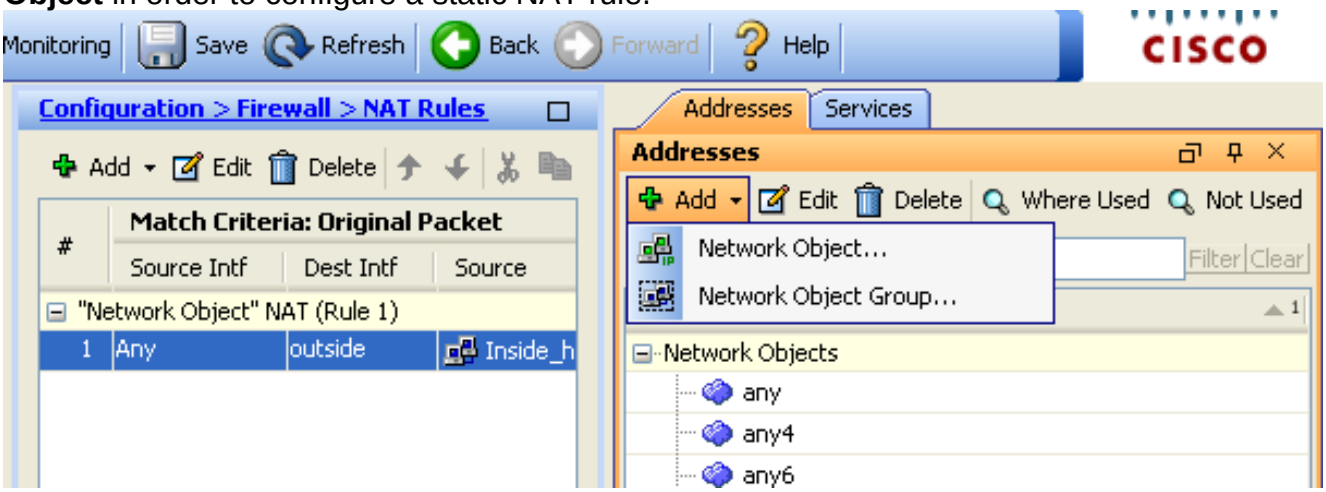
Port forwarding or port redirection is a useful feature where the outside users try to access an internal server on a specific port. In order to achieve this, the internal server, which has a private IP address, will be translated to a public IP address which in turn is allowed access for the specific port.

In this example, the outside user wants to access the SMTP server, 203.0.115.15 at port 25. This is accomplished in two steps:

1. Translate the internal mail server, 172.16.11.15 on port 25, to the public IP address, 203.0.115.15 at port 25.
2. Allow access to the public mail server, 203.0.115.15 at port 25.

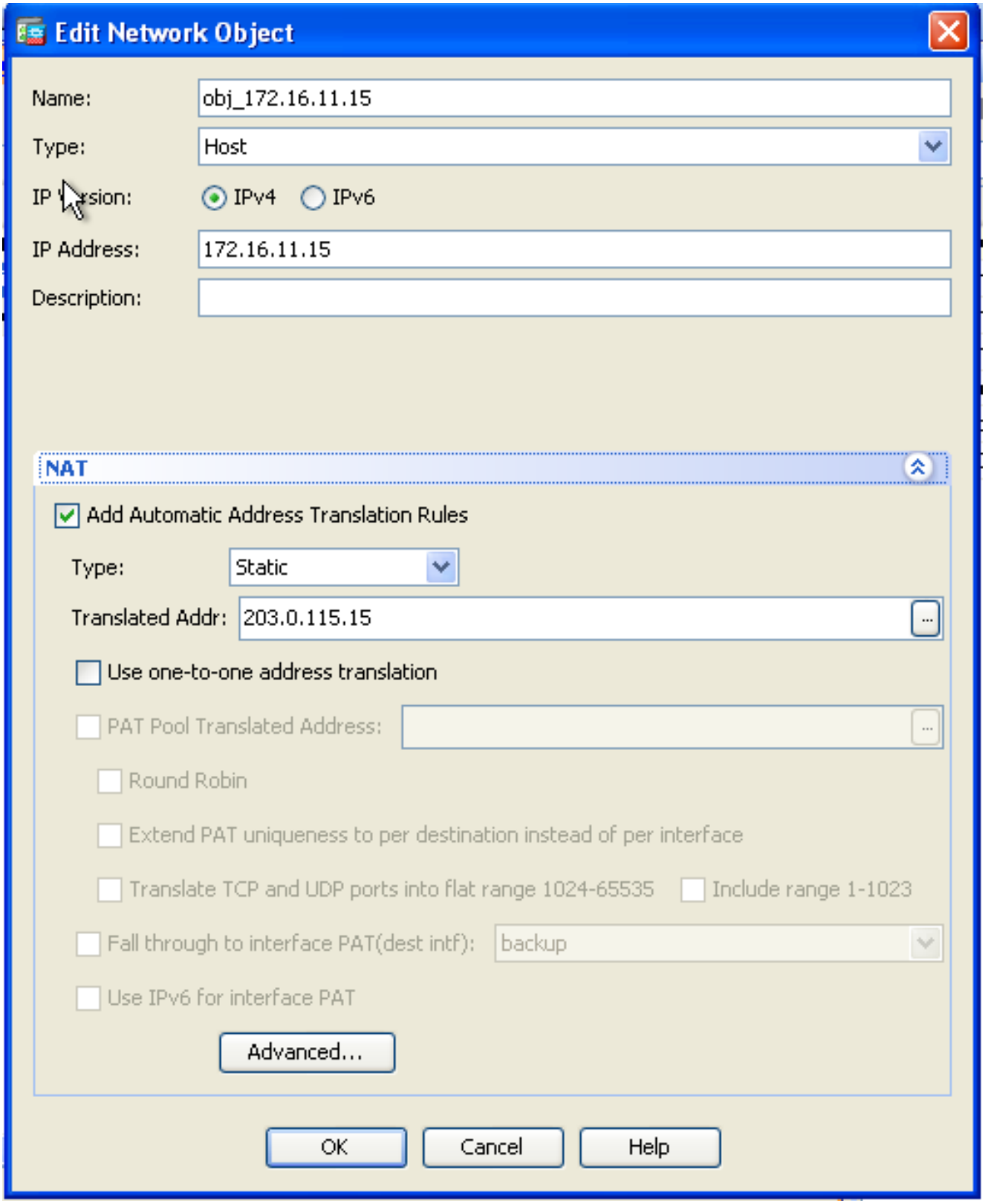
When the outside user tries to access the server, 203.0.115.15 at port 25, this traffic is redirected to the internal mail server, 172.16.11 15 at port 25.

1. Choose **Configuration > Firewall > NAT Rules**. Click **Add** and then choose **Network Object** in order to configure a static NAT rule.



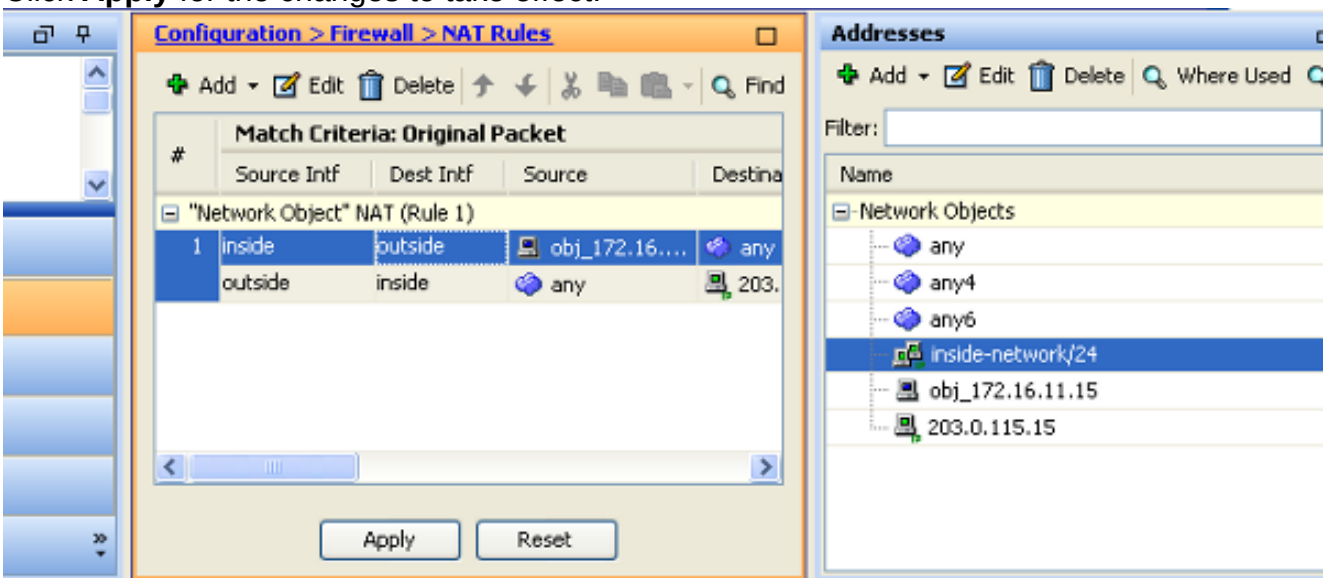
2. Configure the Host for which port forwarding is required.

3. Expand NAT. Check the **Add Automatic Address Translation Rules** check box. In the Type drop-down list, choose **Static**. In the Translated Addr field, enter the IP address. Click **Advanced** in order to select the service and source and destination interfaces.



4. In the Source Interface and Destination Interface drop-down lists, choose the appropriate interfaces. Configure the service. Click **OK**.

5. Click **Apply** for the changes to take effect.



This is the equivalent CLI output for this NAT configuration:

Verify

Use this section in order to confirm that your configuration works properly.

The Cisco CLI Analyzer (registered customers only) supports certain **show** commands. Use the Cisco CLI Analyzer in order to view an analysis of **show** command output.

Access a web site via HTTP with a web browser. This example uses a site that is hosted at 198.51.100.100. If the connection is successful, this output can be seen on the ASA CLI.

Connection

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

The ASA is a stateful firewall, and return traffic from the web server is allowed back through the firewall because it matches a ***connection*** in the firewall connection table. Traffic that matches a connection that preexists is allowed through the firewall without being blocked by an interface ACL.

In the previous output, the client on the inside interface has established a connection to the 198.51.100.100 host off of the outside interface. This connection is made with the TCP protocol and has been idle for six seconds. The connection flags indicate the current state of this connection. More information about connection flags can be found in ASA TCP Connection Flags.

Syslog

```
ASA(config)# show log | in 172.16.11.5

Apr 27 2014 11:31:23: %ASA-6-305011: Built dynamic TCP translation from inside:
172.16.11.5/58799 to outside:203.0.113.2/58799
```

```
Apr 27 2014 11:31:23: %ASA-6-302013: Built outbound TCP connection 2921 for outside:
198.51.100.100/80 (198.51.100.100/80) to inside:172.16.11.5/58799 (203.0.113.2/58799)
```

The ASA Firewall generates syslogs during normal operation. The syslogs range in verbosity based on the logging configuration. The output shows two syslogs that are seen at level six, or the 'informational' level.

In this example, there are two syslogs generated. The first is a log message that indicates that the firewall has built a translation, specifically a dynamic TCP translation (PAT). It indicates the source IP address and port and the translated IP address and port as the traffic traverses from the inside to the outside interfaces.

The second syslog indicates that the firewall has built a connection in its connection table for this specific traffic between the client and server. If the firewall was configured in order to block this connection attempt, or some other factor inhibited the creation of this connection (resource constraints or a possible misconfiguration), the firewall would not generate a log that indicates that the connection was built. Instead it would log a reason for the connection to be denied or an indication about what factor inhibited the connection from being created.

Packet Tracer

```
ASA(config)# packet-tracer input inside tcp 172.16.11.5 1234 198.51.100.100 80


--Omitted--

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

The packet tracer functionality on the ASA allows you to specify a *simulated* packet and see all of the various steps, checks, and functions that the firewall goes through when it processes traffic. With this tool, it is helpful to identify an example of traffic you believe *should* be allowed to pass through the firewall, and use that 5-tupple in order to simulate traffic. In the previous example, the packet tracer is used in order to simulate a connection attempt that meets these criteria:

- The simulated packet arrives on the inside.
- The protocol used is TCP.
- The simulated client IP address is 172.16.11.5.
- The client sends traffic sourced from port 1234.
- The traffic is destined to a server at IP address 198.51.100.100.
- The traffic is destined to port 80.

Notice that there was no mention of the interface outside in the command. This is by packet tracer design. The tool tells you how the firewall processes that type of connection attempt, which includes how it would route it, and out of which interface. More information about packet tracer can be found in Tracing Packets with Packet Tracer.

Capture

Apply Capture

```
ASA# capture capin interface inside match tcp host 172.16.11.5 host 198.51.100.100
ASA# capture capout interface outside match tcp any host 198.51.100.100ASA#show capture capin

3 packets captured

1: 11:31:23.432655 172.16.11.5.58799 > 198.51.100.100.80: S 780523448:
780523448(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
2: 11:31:23.712518 198.51.100.100.80 > 172.16.11.5.58799: S 2123396067:
2123396067(0) ack 780523449 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
3: 11:31:23.712884 172.16.11.5.58799 > 198.51.100.100.80: . ack 2123396068
win 32768ASA#show capture capout

3 packets captured

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

The ASA firewall can capture traffic that enters or leaves its interfaces. This capture functionality is fantastic because it can definitively prove if traffic arrives at, or leaves from, a firewall. The previous example showed the configuration of two captures named capin and capout on the inside and outside interfaces respectively. The capture commands used the match keyword, which allows you to be specific about what traffic you want to capture.

For the capture capin**,** you indicated that you wanted to match traffic seen on the inside interface (ingress or egress) that matches TCP host 172.16.11.5 host 198.51.100.100. In other words, you want to capture any TCP traffic that is sent from host 172.16.11.5 to host 198.51.100.100 or vice versa. The use of the match keyword allows the firewall to capture that traffic bidirectionally. The capture command defined for the outside interface does not reference the internal client IP address because the firewall conducts PAT on that client IP address. As a result, you cannot match with that client IP address. Instead, this example uses any in order to indicate that all possible IP addresses would match that condition.

After you configure the captures, you would then attempt to establish a connection again, and proceed to view the captures with the **show capture <*capture_name*>** command. In this example, you can see that the client was able to connect to the server as evident by the TCP 3-Way handshake seen in the captures.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Related Information

- **ASA Syslog Configuration Example**
- **ASA Packet Captures with CLI and ASDM Configuration Example**
- **Technical Support & Documentation - Cisco Systems**