Table of Contents

PIX 7.0 and Adaptive Security Appliance Port Redirection with nat, global, static, conduit, and access−list Commands

Document ID: 63872

Introduction

In order to maximize security when you implement Cisco PIX Security Appliance version 7.0, it is important to understand how packets pass between higher security interfaces and lower security interfaces when you use the **nat−control**, **nat**, **global**, **static**, **access−list** and **access−group** commands. This document explains the differences between these commands and how to configure port redirection and the outside Network Address Translation (NAT) features in PIX software version 7.0, with the use of the command line interface or the Adaptive Security Device Manager (ASDM).

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

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

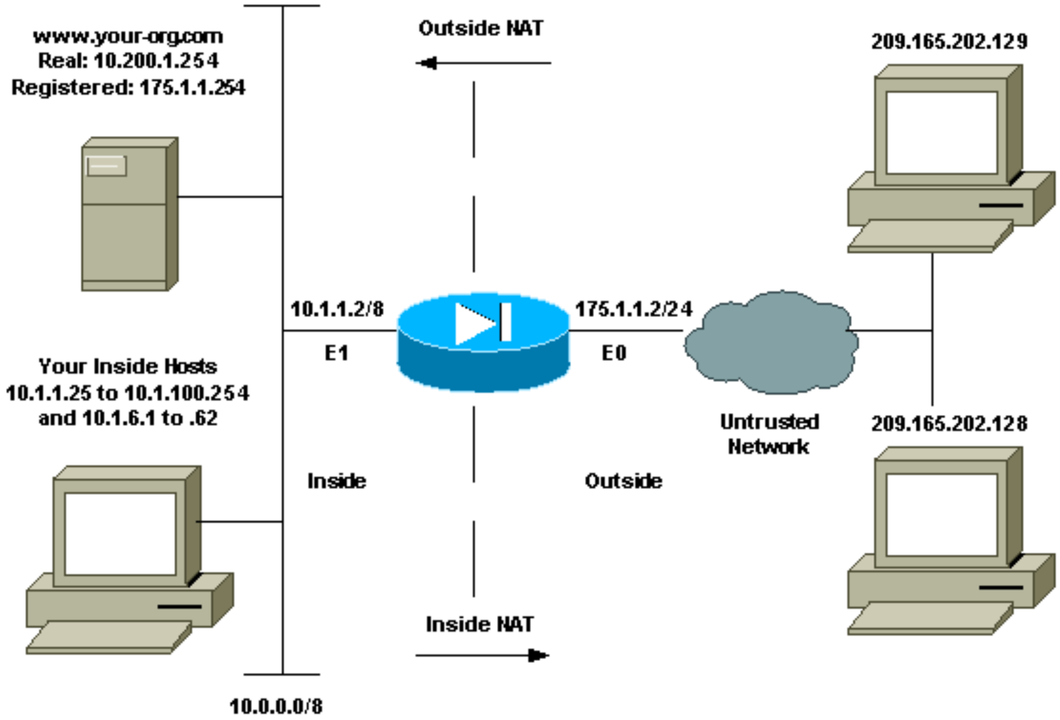
- Cisco PIX 500 Series Security Appliance Software version 7.0 and later

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.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Network Diagram



Initial Configuration

The interface names are:

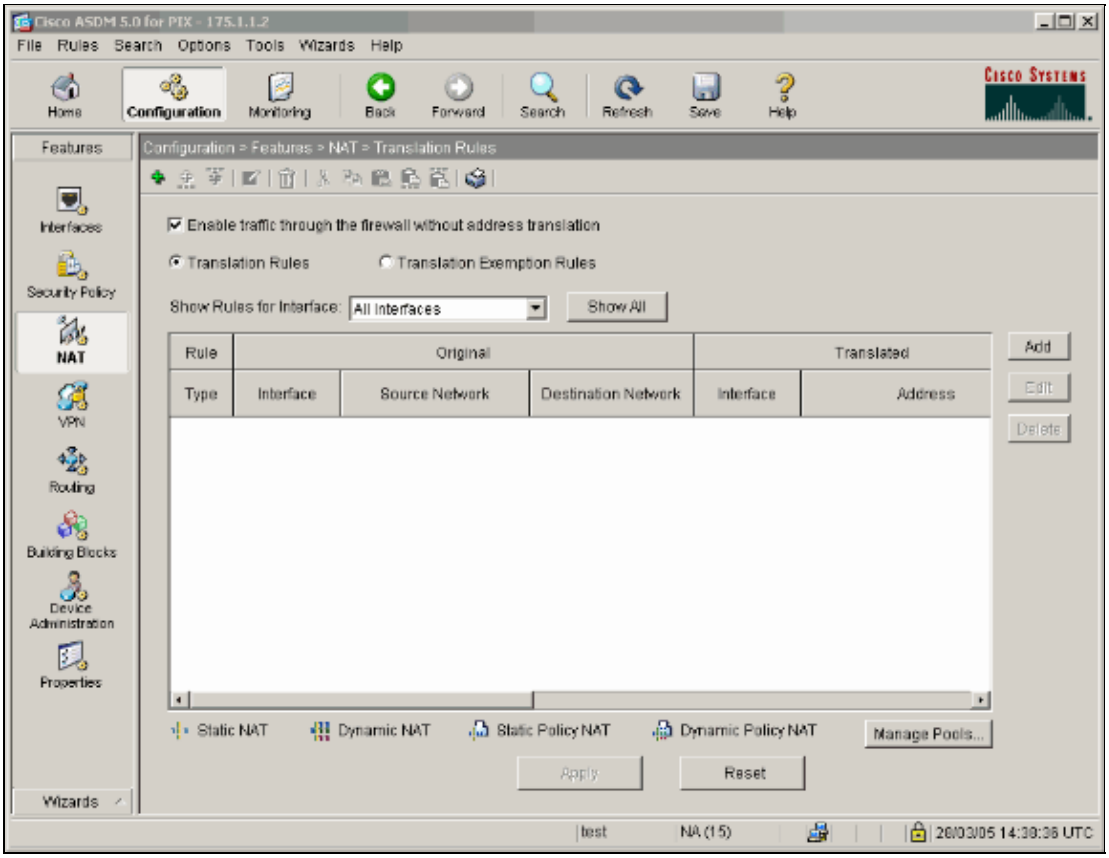
- **interface ethernet 0** nameif outside
- **interface ethernet 1** nameif inside

Allow Outbound Access

Outbound access describes connections from a higher security level interface to a lower security level interface. This includes connections from inside to outside, inside to Demilitarized Zones (DMZs), and DMZs to outside. This can also include connections from one DMZ to another, as long as the connection source interface has a higher security level than the destination. Review the "security−level" configuration on the PIX interfaces in order to confirm this.

In PIX 7.0, the **nat−control** command is introduced. You can use the **nat−control** command in order to specify if NAT is required for outside communications. With NAT control enabled, configuration of NAT rules is required in order to allow outbound traffic, as is the case with previous version of PIX software. If NAT control is disabled (**no nat−control**), inside hosts can communicate with outside networks without the configuration of a NAT rule. However, if you have inside hosts that do not have public addresses, you still need to configure NAT for those hosts.

In order to configure NAT control with the use of ASDM, select the Configuration tab from the ASDM Home screen and choose **NAT** from the features menu. Select the **Enable traffic through the firewall without translation** checkbox if you wish to allow traffic to pass through the firewall without requiring translation.



☑ Enable traffic through the firewall without address translation

● Translation Rules ○ Translation Exemption Rules

Show Rules for Interface: All Interfaces

There are two policies that are required in order to allow outbound access with NAT control. The first one is a translation method. This can be a static translation with the use of the **static** command, or a dynamic translation with the use of a **nat**/**global** rule. This is not required if NAT control is disabled and your inside hosts have public addresses.

The other requirement for outbound access (which applies whether NAT control is enabled or disabled), is if there is an access control list (ACL) present. If an ACL is present, then it must allow the source host access to the destination host with the use of the specific protocol and port. By default, there are no access restrictions on outbound connections through the PIX. This means that if there is no ACL configured for the source interface, then by default, the outbound connection is allowed if there is a translation method configured.

Allow Inside Hosts Access to Outside Networks with NAT

This configuration gives all of the hosts on the subnet 10.1.6.0/24 access to the outside. In order to accomplish this, use the **nat** and **global** commands as this procedure demonstrates.

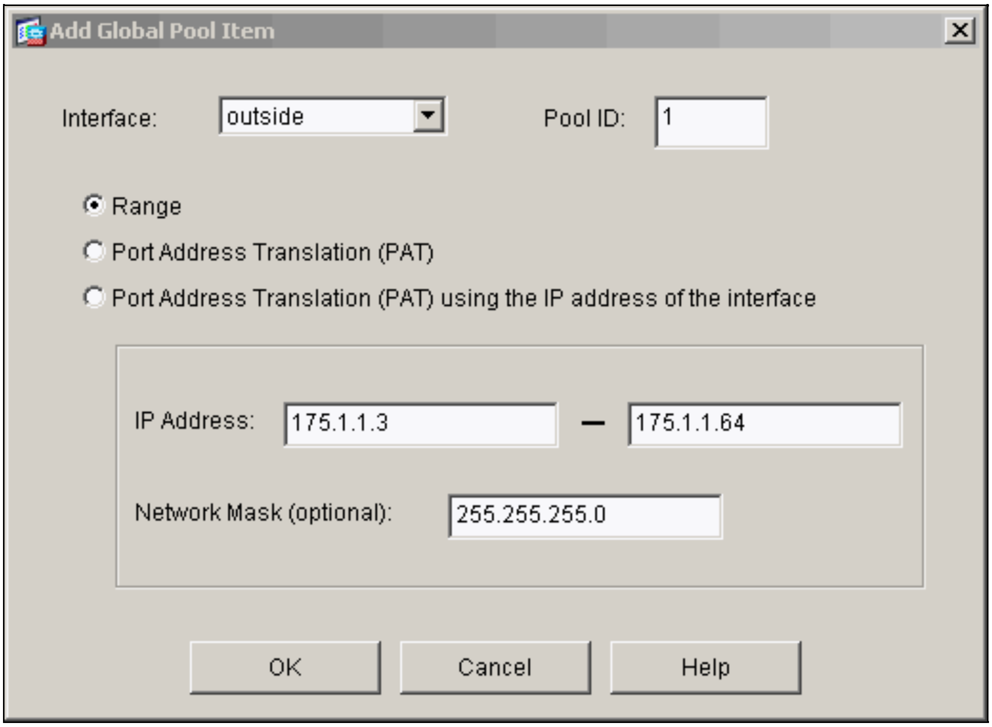
1. Define the inside group you want to include for NAT.

```
nat (inside) 1 10.1.6.0 255.255.255.0
```

2. Specify a pool of addresses on the outside interface to which the hosts defined in the NAT statement will be translated.

```
global (outside) 1 175.1.1.3−175.1.1.64 netmask 255.255.255.0
```

3. Use ASDM to create your global address pool. In order to do this, select **Configuration** > **Features** > **NAT** and choose **Manage Pools**.
4. Select **Outside** > **Add**, and choose a range to specify a pool of addresses.
5. Enter your address range, enter a Pool ID, and click **OK**.



Add Global Pool Item

Interface: outside

Pool ID: 1

● Range

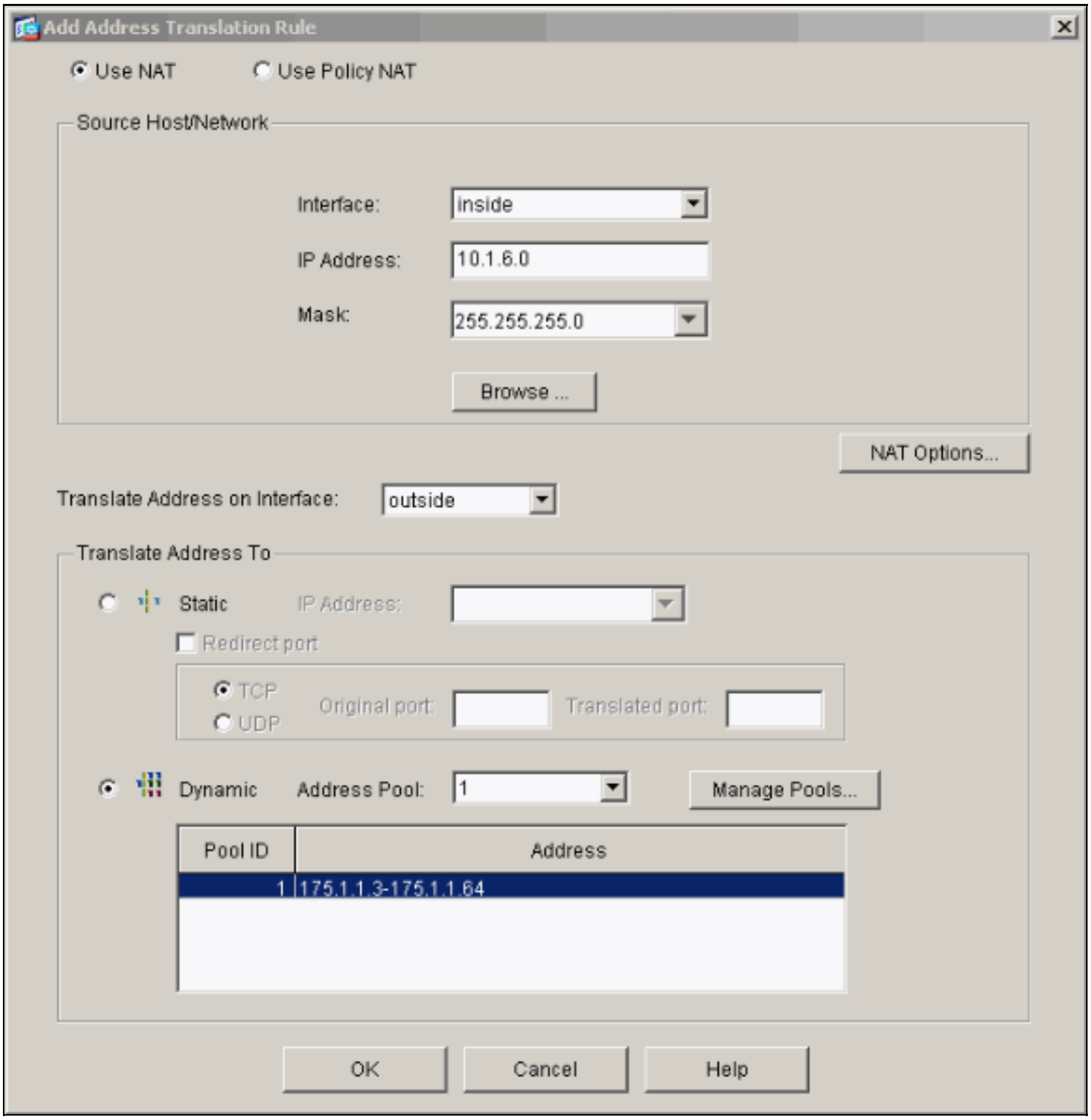
○ Port Address Translation (PAT)

○ Port Address Translation (PAT) using the IP address of the interface

IP Address: 175.1.1.3 – 175.1.1.64

Network Mask (optional): 255.255.255.0

6. Select **Configuration** > **Features** > **NAT** > **Translation Rules** in order to create the translation rule.
7. Select **Inside** as the Source Interface, and enter the addresses you want to NAT.
8. For Translate Address on Interface, select **Outside**, choose **Dynamic**, and select the Address Pool you just configured.
9. Click **OK**.



Add Address Translation Rule

● Use NAT ○ Use Policy NAT

Source Host/Network

Interface: inside

IP Address: 10.1.6.0

Mask: 255.255.255.0

Translate Address on Interface: outside

Translate Address To

○ Static IP Address:

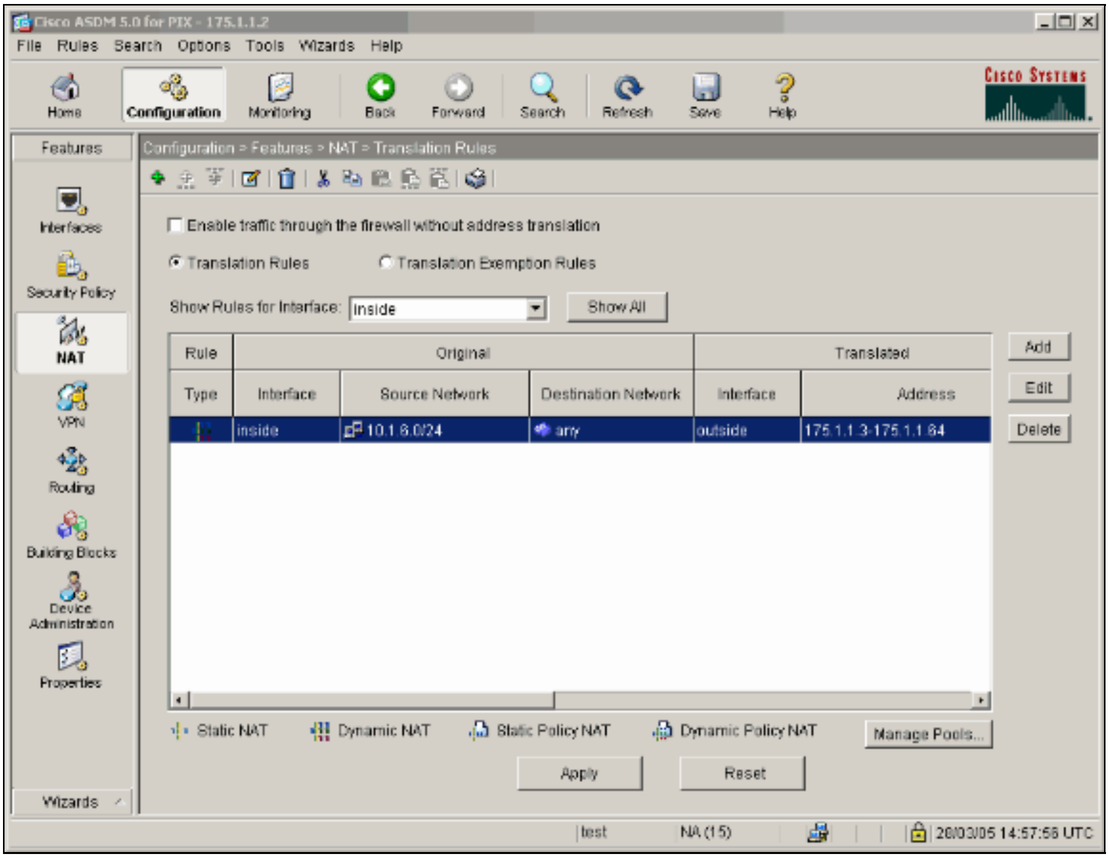
□ Redirect port

● TCP ○ UDP Original port: Translated port:

● Dynamic Address Pool: 1

Pool ID	Address
1	175.1.1.3-175.1.1.64

10. The translation appears in the Translation Rules at **Configuration** > **Features** > **NAT** > **Translation Rules**.



Configuration > Features > NAT > Translation Rules

□ Enable traffic through the firewall without address translation

● Translation Rules ○ Translation Exemption Rules

Show Rules for Interface: inside Show All

Rule	Original			Translated	
Type	Interface	Source Network	Destination Network	Interface	Address
	inside	10.1.6.0/24	any	outside	175.1.1.3-175.1.1.64

test NA (15) 28/03/05 14:57:56 UTC

Now the hosts on the inside can access outside networks. When hosts from the inside initiate a connection to the outside, they are translated to an address from the global pool. The addresses are assigned from the global pool on a first−come, first−translated basis, and start with the lowest address in the pool. For example, if host 10.1.6.25 is the first to initiate a connection to the outside, it receives address 175.1.1.3. The next host out receives 175.1.1.4, and so on. This is not a static translation, and the translation times out after a period of inactivity as defined by the **timeout xlate hh:mm:ss** command. If there are more inside hosts than there are addresses in the pool, the final address in the pool is used for Port Address Translation (PAT).

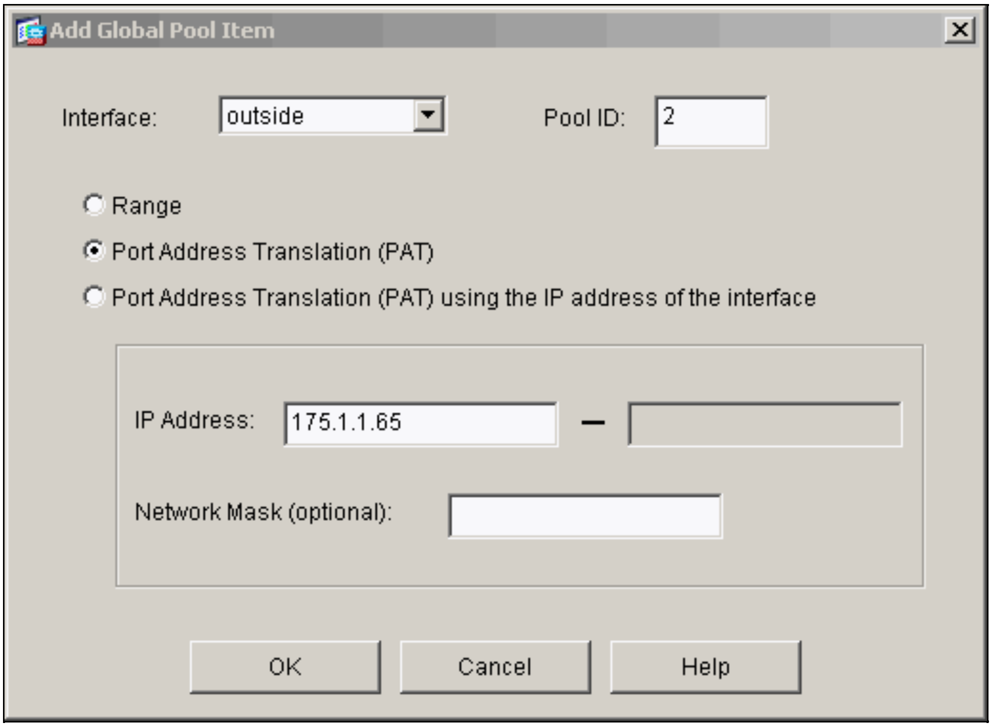
Allow Inside Hosts Access to Outside Networks with the use of PAT

If you want inside hosts to share a single public address for translation, use PAT. If the **global** statement specifies one address, that address is port translated. The PIX allows one port translation per interface and that translation supports up to 65,535 active xlate objects to the single global address. Complete these steps in order to allow inside hosts access to outside networks with the use of PAT.

1. Define the inside group you want to include for PAT (when you use 0 0, you select all inside hosts.)

   ```
   nat (inside) 1 10.1.6.0 255.255.255.0
   ```
2. Specify the global address you want to use for PAT. This can be the interface address.

   ```
   global (outside) 1 175.1.1.65 netmask 255.255.255.224
   ```
3. In ASDM, select **Configuration** > **Features** > **NAT** and choose **Manage Pools** in order to configure your PAT address.
4. Select **Outside** > **Add** and choose **Port Address Translation (PAT)** in order to configure a single address for PAT.
5. Enter an address, a Pool ID, and click **OK**.



Interface: outside

Pool ID: 2

○ Range

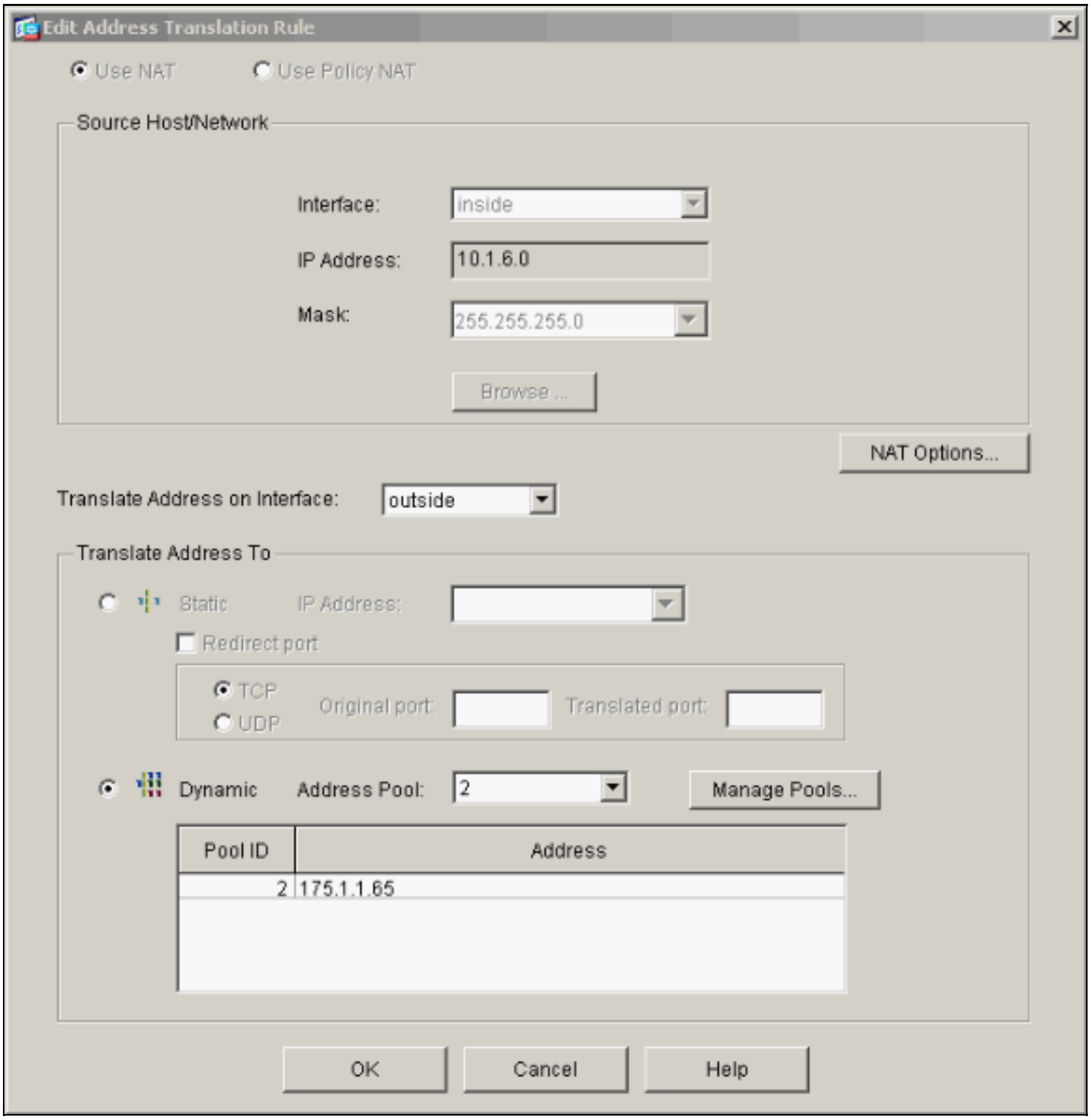
● Port Address Translation (PAT)

○ Port Address Translation (PAT) using the IP address of the interface

IP Address: 175.1.1.65 –

Network Mask (optional):

6. Select **Configuration > Features > NAT > Translation Rules** in order to create the translation rule.
7. Select **inside** as the source interface, and enter the addresses you want to NAT.
8. For Translate Address on Interface, select **outside**, choose **Dynamic**, and select the Address Pool you just configured. Click **OK**.



Edit Address Translation Rule

● Use NAT ○ Use Policy NAT

Source Host/Network

Interface: inside

IP Address: 10.1.6.0

Mask: 255.255.255.0

Translate Address on Interface: outside

Translate Address To

○ Static IP Address:

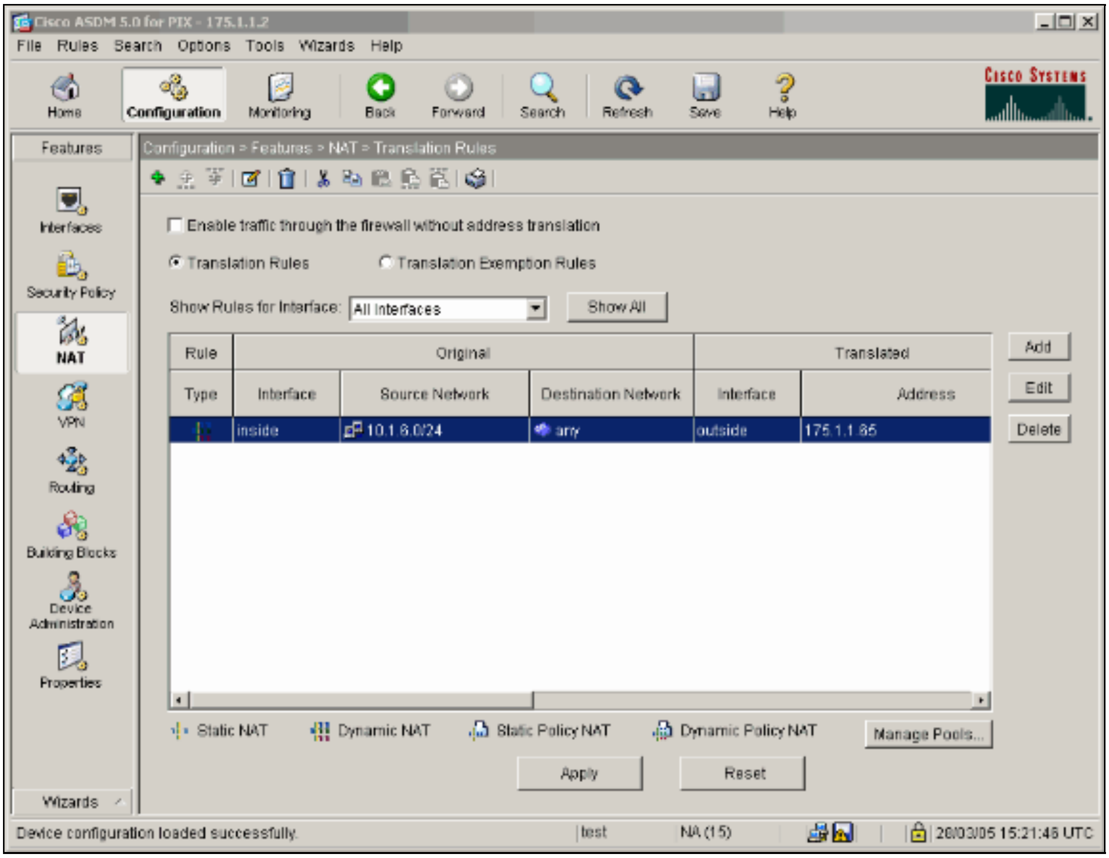
□ Redirect port

● TCP ○ UDP Original port: Translated port:

● Dynamic Address Pool: 2

Pool ID	Address
2	175.1.1.65

9. The translation appears in the Translation Rules at **Configuration > Features > NAT > Translation Rules**.



Configuration > Features > NAT > Translation Rules

☐ Enable traffic through the firewall without address translation

● Translation Rules ○ Translation Exemption Rules

Show Rules for Interface: All Interfaces

Rule	Original			Translated	
Type	Interface	Source Network	Destination Network	Interface	Address
	inside	10.1.6.0/24	any	outside	175.1.1.65

Device configuration loaded successfully. test NA (15) 20/03/05 15:21:46 UTC

There are a few things to consider when you use PAT.

- The IP addresses you specify for PAT cannot be in another global address pool.
- PAT does not work with H.323 applications, caching nameservers, and Point−to−Point Tunneling Protocol (PPTP). PAT works with Domain Name Service (DNS), FTP and passive FTP, HTTP, mail, remote−procedure call (RPC), rshell, Telnet, URL filtering, and outbound traceroute.
- Do not use PAT when you need to run multimedia applications through the firewall. Multimedia applications can conflict with port mappings that PAT provides.
- In PIX software release 4.2(2), the PAT feature does not work with IP data packets that arrive in reverse order. PIX software release 4.2(3) corrects this problem.
- IP addresses in the pool of global addresses specified with the **global** command require reverse DNS entries in order to ensure that all external network addresses are accessible through the PIX. In order to create reverse DNS mappings, use a DNS Pointer (PTR) record in the address−to−name mapping file for each global address. Without the PTR entries, sites can experience slow or intermittent Internet connectivity and FTP requests fail consistently.

  For example, if a global IP address is 175.1.1.3 and the domain name for the PIX Security Appliance is pix.caguana.com, the PTR record is:

  ```
  3.1.1.175.in−addr.arpa. IN PTR
  pix3.caguana.com
   4.1.1.175.in−addr.arpa. IN PTR
  pix4.caguana.com & so on.
  ```

Restrict Inside Hosts Access to Outside Networks

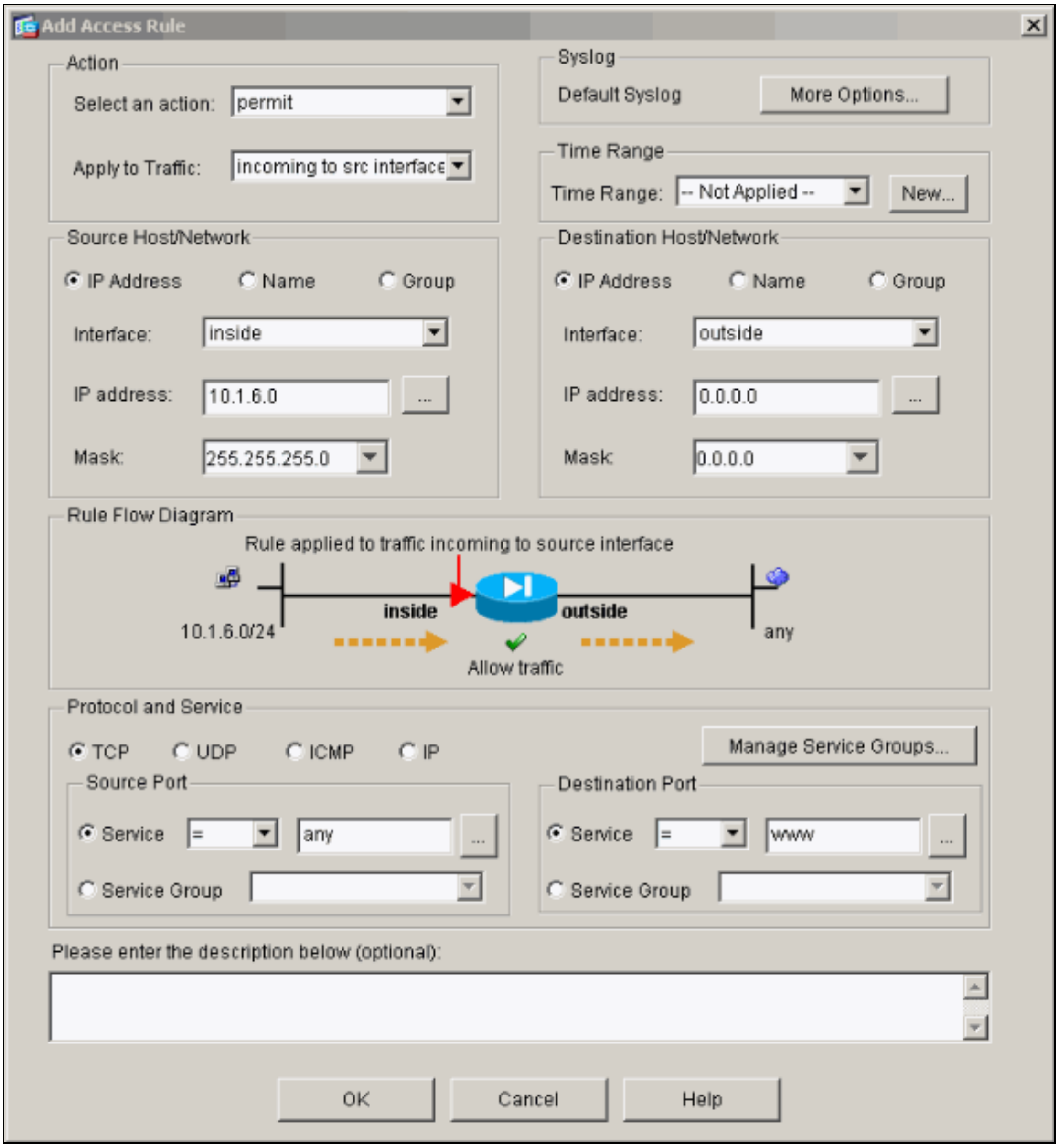
If there is a valid translation method defined for the source host, and no ACL defined for the source PIX interface, then the outbound connection is allowed by default. However, in some cases it is necessary to restrict outbound access based on source, destination, protocol, and/or port. In order to accomplish this, configure an ACL with the **access−list** command and apply it to the connection source PIX interface with the **access−group** command. You can apply PIX 7.0 ACLs in both inbound and outbound directions. This procedure is an example that allows outbound HTTP access for one subnet, but denies all other hosts HTTP access to the outside, while allowing all other IP traffic for everyone.

1. Define the ACL.

   ```
   access−list acl_outbound permit tcp 10.1.6.0 255.255.255.0 any eq www
   access−list acl_outbound deny tcp any any eq www
   access−list acl_outbound permit ip any any
   ```

   Note: PIX ACLs differ from ACLs on Cisco IOS® routers in that the PIX does not use a wildcard mask like Cisco IOS. It uses a regular subnet mask in the ACL definition. As with Cisco IOS routers, the PIX ACL has an implicit "deny all" at the end of the ACL.
2. Apply the ACL to the inside interface.

   ```
   access−group acl_outbound in interface inside
   ```
3. Use ASDM in order to configure the first access−list entry in step 1 to allow HTTP traffic from 10.1.6.0/24. Select **Configuration > Features > Security Policy > Access Rules**.
4. Click **Add**, enter the information as this window shows, and click **OK**.



Add Access Rule

Action

Select an action: permit

Apply to Traffic: incoming to src interface

Syslog

Default Syslog

Time Range

Time Range: -- Not Applied --

Source Host/Network

● IP Address ○ Name ○ Group

Interface: inside

IP address: 10.1.6.0

Mask: 255.255.255.0

Destination Host/Network

● IP Address ○ Name ○ Group

Interface: outside

IP address: 0.0.0.0

Mask: 0.0.0.0

Rule Flow Diagram

Protocol and Service

● TCP ○ UDP ○ ICMP ○ IP

Source Port

● Service = any

○ Service Group

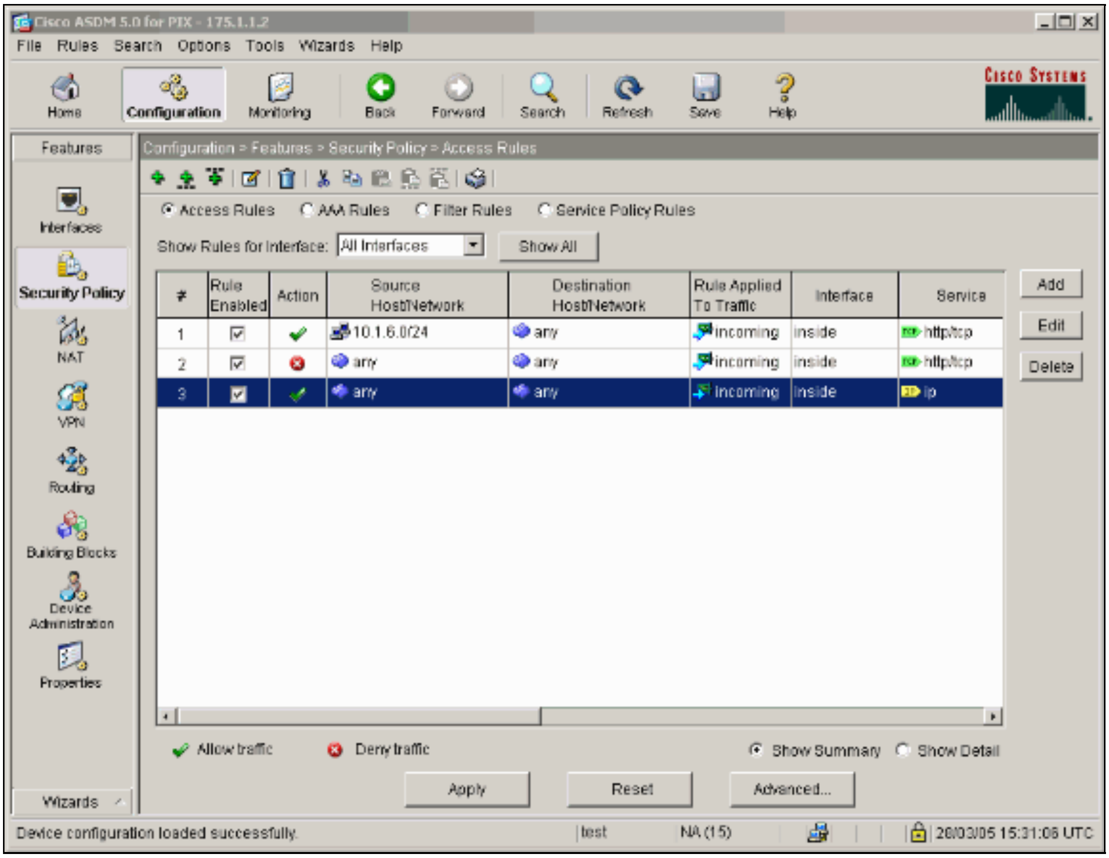
Destination Port

● Service = www

○ Service Group

Please enter the description below (optional):

5. Once you enter the three access−list entries, select **Configuration** > **Feature** > **Security Policy** > **Access Rules** in order to display these rules.



Configuration > Features > Security Policy > Access Rules

● Access Rules ○ AAA Rules ○ Filter Rules ○ Service Policy Rules

Show Rules for Interface: All Interfaces Show All

#	Rule Enabled	Action	Source Host/Network	Destination Host/Network	Rule Applied To Traffic	Interface	Service
1	☑	✓	10.1.6.0/24	any	incoming	inside	http/tcp
2	☑	☒	any	any	incoming	inside	http/tcp
3	☑	✓	any	any	incoming	inside	ip

✓ Allow traffic ☒ Deny traffic ● Show Summary ○ Show Detail

Device configuration loaded successfully. test NA (15) 28/03/05 15:31:06 UTC

Allow Untrusted Hosts Access to Hosts on Your Trusted Network

Most organizations need to allow untrusted hosts access to resources in their trusted network. A common example is an internal web server. By default, the PIX denies connections from outside hosts to inside hosts. In order to allow this connection in NAT control mode, use the **static** command, with **access−list** and **access−group** commands. If NAT control is disabled, only the **access−list** and **access−group** commands are required, if no translation is performed.

Apply ACLs to interfaces with an **access−group** command. This command associates the ACL with the interface to examine traffic that flows in a particular direction.

In contrast to the **nat** and **global** commands which allow inside hosts out, the **static** command creates a two−way translation that allows inside hosts out and outside hosts in if you add the proper ACLs/groups.

In the PAT configuration examples shown in this document, if an outside host tries to connect to the global address, it can be used by thousands of inside hosts. The **static** command creates a one−to−one mapping. The **access−list** command defines what type of connection is allowed to an inside host and is always required when a lower security host connects to a higher security host. The **access−list** command is based on both port and protocol and can be very permissive or very restrictive, based on what the system administrator wants to achieve.

The network diagram in this document illustrates the use of these commands in order to configure the PIX to allow any untrusted hosts to connect to the inside web server, and allow untrusted host 199.199.199.24 access to an FTP service on the same machine.

Use ACLs on PIX Versions 7.0 and Later

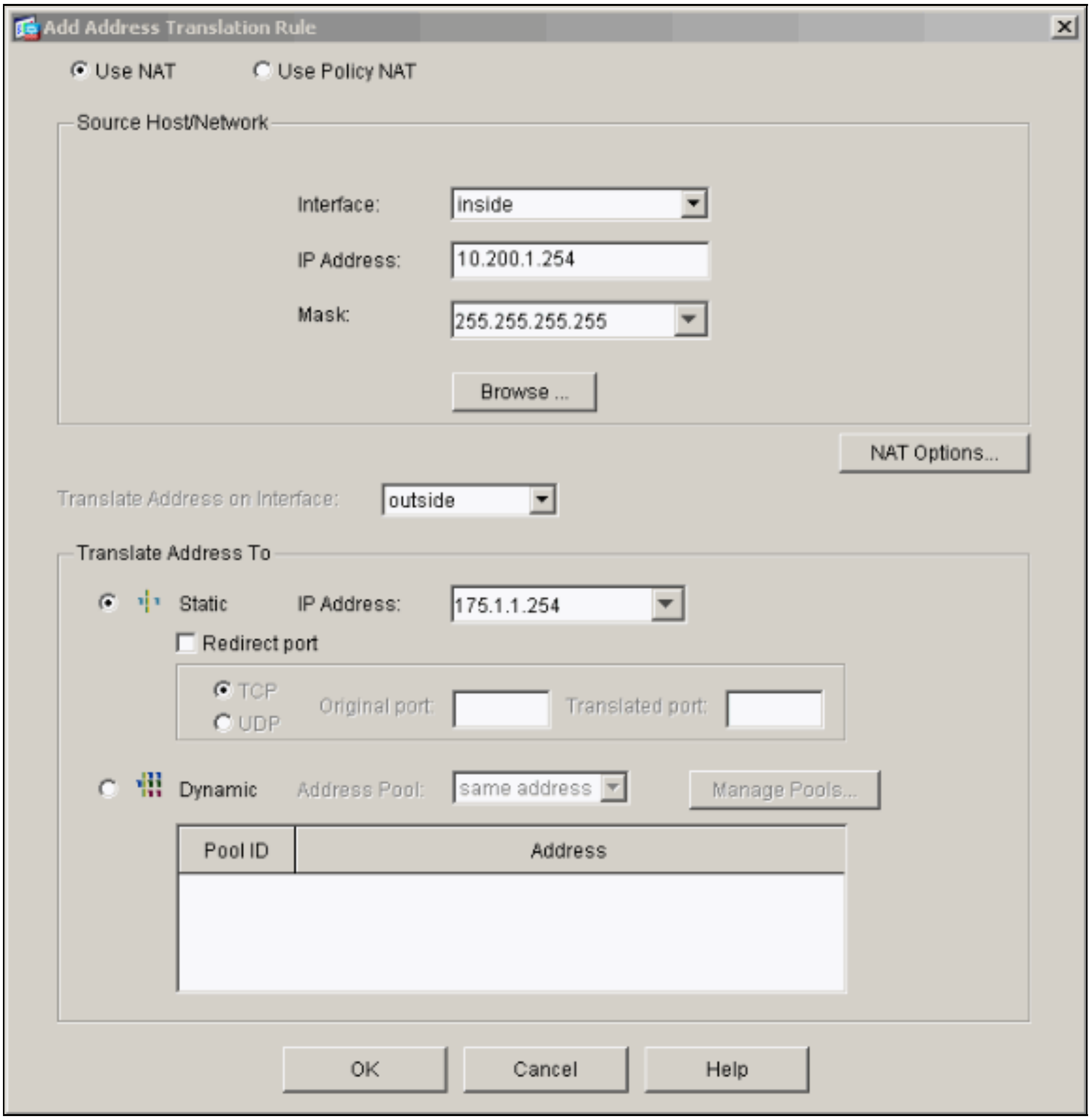
Complete these steps for PIX software versions 7.0 and later with the use of ACLs.

1. If NAT control is enabled, define a static address translation for the inside web server to an outside/global address.

   ```
   static (inside, outside) 175.1.1.254 10.200.1.254
   ```
2. Define which hosts can connect on which ports to your web/FTP server.

   ```
   access-list 101 permit tcp any host 175.1.1.254 eq www
   access-list 101 permit tcp host 199.199.199.24 host 175.1.1.254 eq ftp
   ```
3. Apply the ACL to the outside interface.

   ```
   access-group 101 in interface outside
   ```
4. Select **Configuration** > **Features** > **NAT** and click **Add** in order to create this static translation with the use of ASDM.
5. Select **inside** as the source interface, and enter the internal address you want to create a static translation for.
6. Choose **Static** and enter the outside address you want to translate to in the IP address field. Click **OK**.



Add Address Translation Rule

● Use NAT ○ Use Policy NAT

Source Host/Network

Interface: inside

IP Address: 10.200.1.254

Mask: 255.255.255.255

Translate Address on Interface: outside

Translate Address To

● Static IP Address: 175.1.1.254

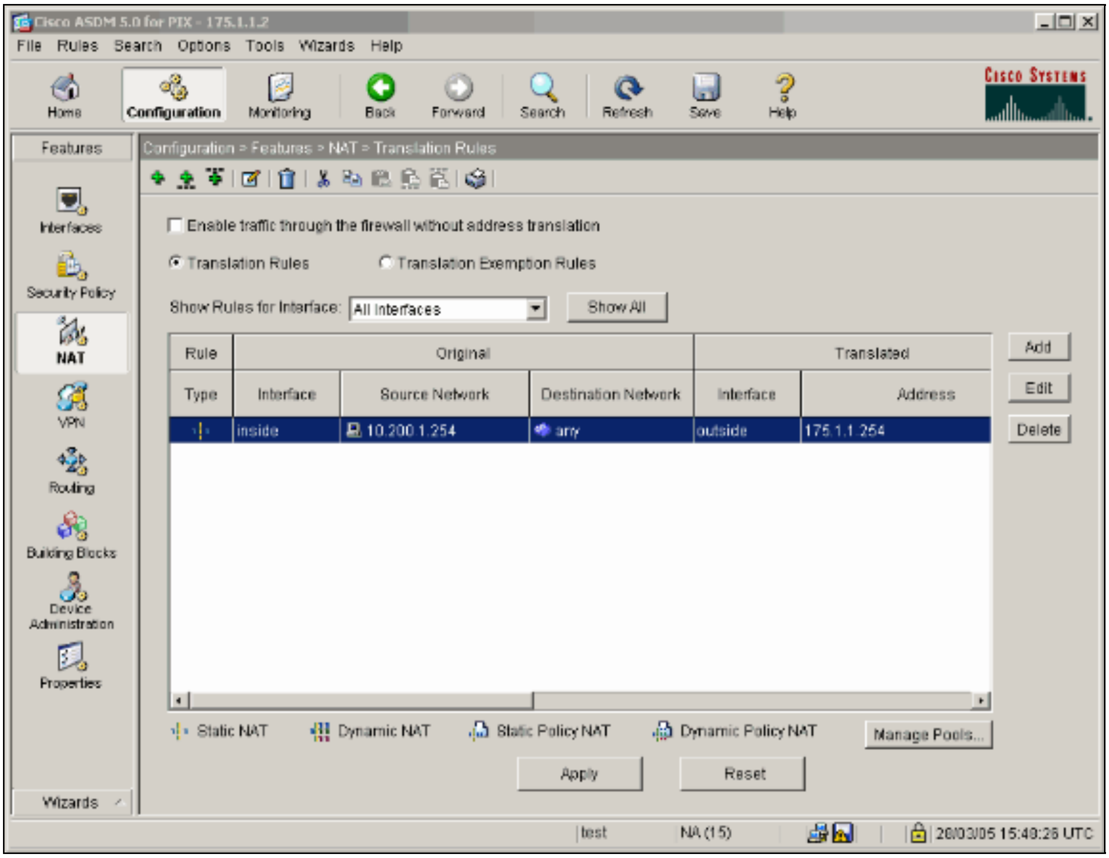
□ Redirect port

● TCP ○ UDP Original port: Translated port:

○ Dynamic Address Pool: same address

Pool ID	Address

7. The translation appears in the Translation Rules when you select **Configuration** > **Features** > **NAT** > **Translation Rules**.



Configuration > Features > NAT > Translation Rules

☐ Enable traffic through the firewall without address translation

● Translation Rules ○ Translation Exemption Rules

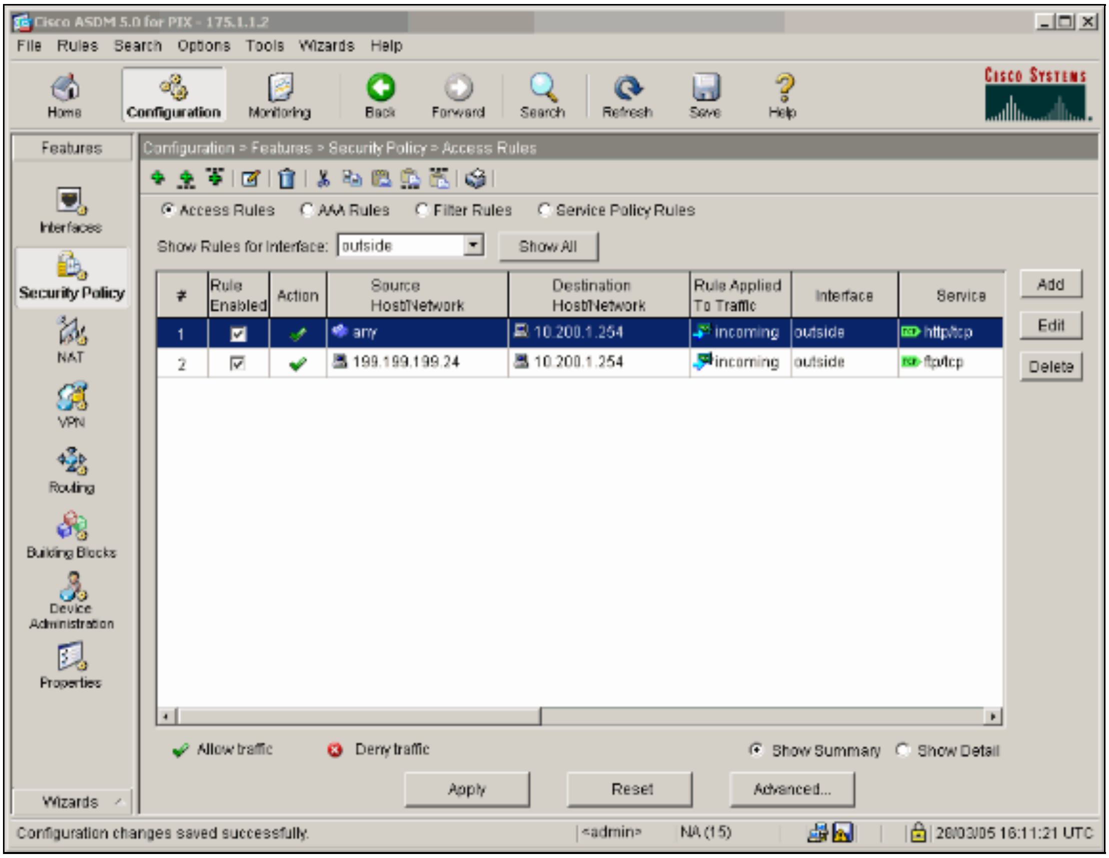
Show Rules for Interface: All Interfaces [Show All]

Rule	Original			Translated	
Type	Interface	Source Network	Destination Network	Interface	Address
↔	inside	10.200.1.254	any	outside	175.1.1.254

test NA (15) 28/03/05 15:48:28 UTC

8. Use the Restrict Inside Hosts Access to Outside Networks procedure in order to enter the **access−list** entries.

   Note: Be careful when you implement these commands. If you implement the **access−list 101 permit ip any any** command, any host on the untrusted network can access any host on the trusted network with the use of IP as long as there is an active translation.



Configuration > Features > Security Policy > Access Rules

● Access Rules ○ AAA Rules ○ Filter Rules ○ Service Policy Rules

Show Rules for Interface: outside

#	Rule Enabled	Action	Source Host/Network	Destination Host/Network	Rule Applied To Traffic	Interface	Service
1	☑	✓	any	10.200.1.254	incoming	outside	http/tcp
2	☑	✓	199.199.199.24	10.200.1.254	incoming	outside	ftp/tcp

✓ Allow traffic ⊗ Deny traffic ● Show Summary ○ Show Detail

Configuration changes saved successfully. <admin> NA (15) 28/03/05 16:11:21 UTC

Disable NAT for Specific Hosts/Networks

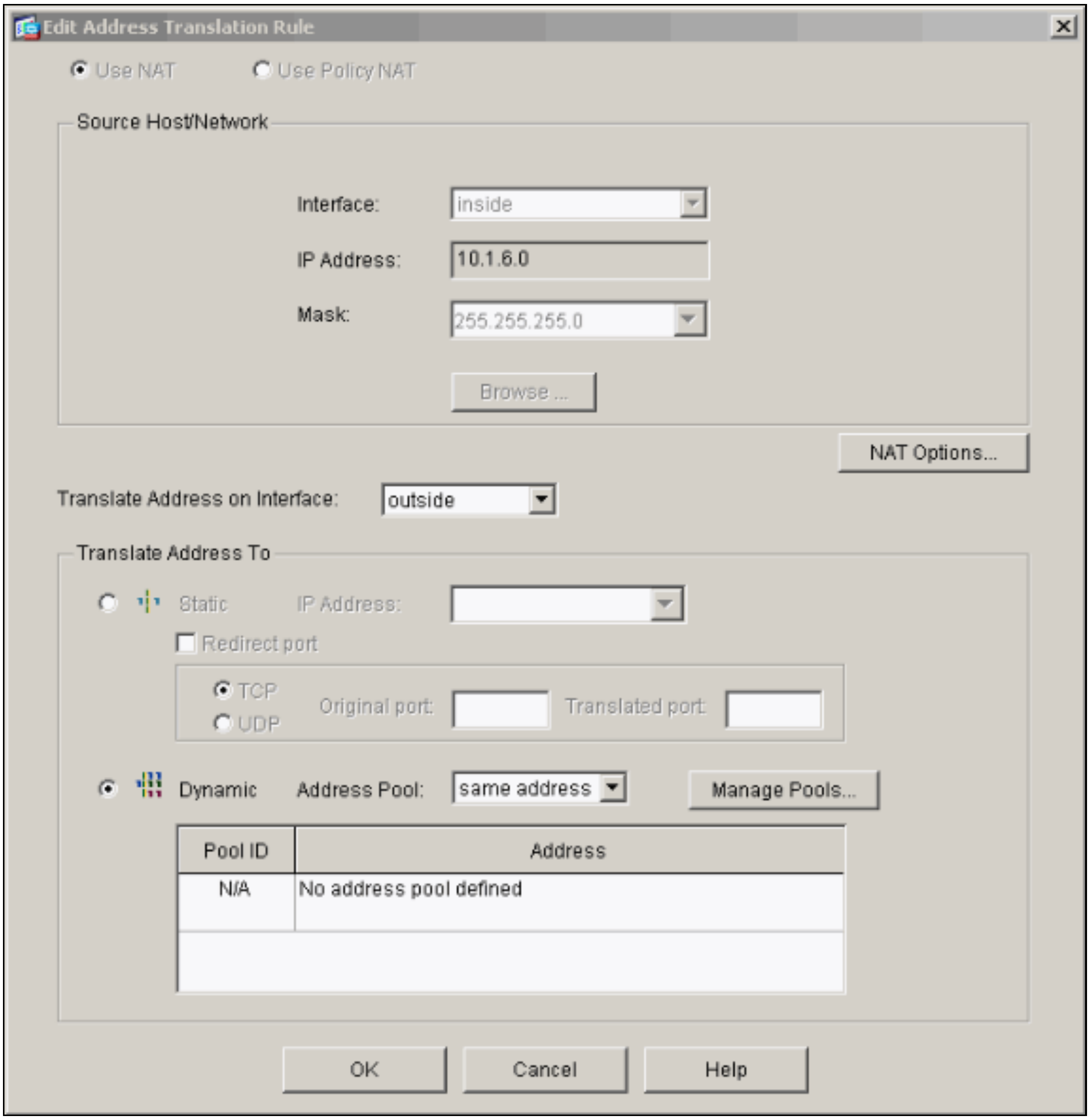
If you use NAT control and have some public addresses on the inside network, and you want those specific inside hosts to go out to the outside without translation, you can disable NAT for those hosts, with **nat 0** or **static** commands.

This is an example of the **nat** command:

```
nat (inside) 0 10.1.6.0 255.255.255.0
```

Complete these steps in order to disable NAT for specific hosts/networks with the use of ASDM.

1. Select **Configuration** > **Features** > **NAT** and click **Add**.
2. Select **inside** as the source interface, and enter the internal address/network you want to create a static translation for.
3. Choose **Dynamic** and select the same address for Address Pool. Click **OK**.



Edit Address Translation Rule

● Use NAT ○ Use Policy NAT

Source Host/Network

Interface: inside

IP Address: 10.1.6.0

Mask: 255.255.255.0

Translate Address on Interface: outside

Translate Address To

○ Static IP Address:

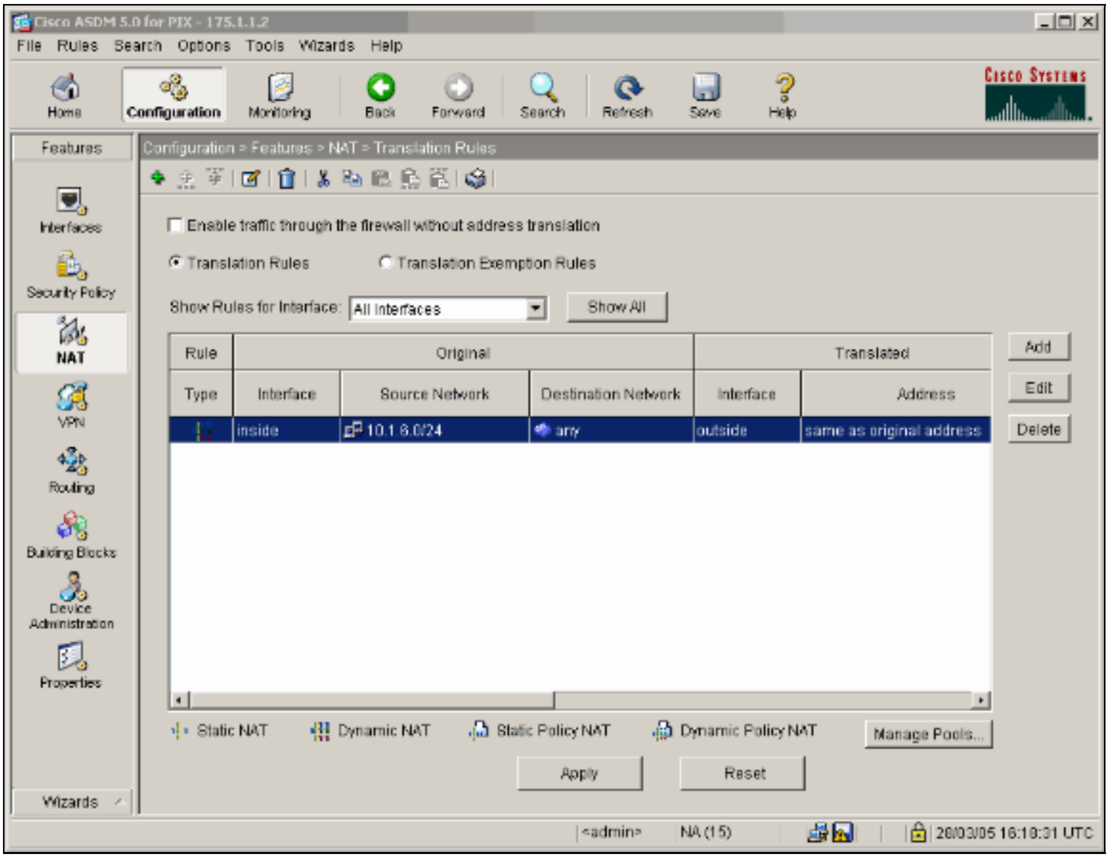
□ Redirect port

● TCP ○ UDP Original port: Translated port:

● Dynamic Address Pool: same address

Pool ID	Address
N/A	No address pool defined

4. The new rule appears in the Translation Rules when you select **Configuration** > **Features** > **NAT** > **Translation Rules**.



□ Enable traffic through the firewall without address translation

● Translation Rules ○ Translation Exemption Rules

Show Rules for Interface: All Interfaces

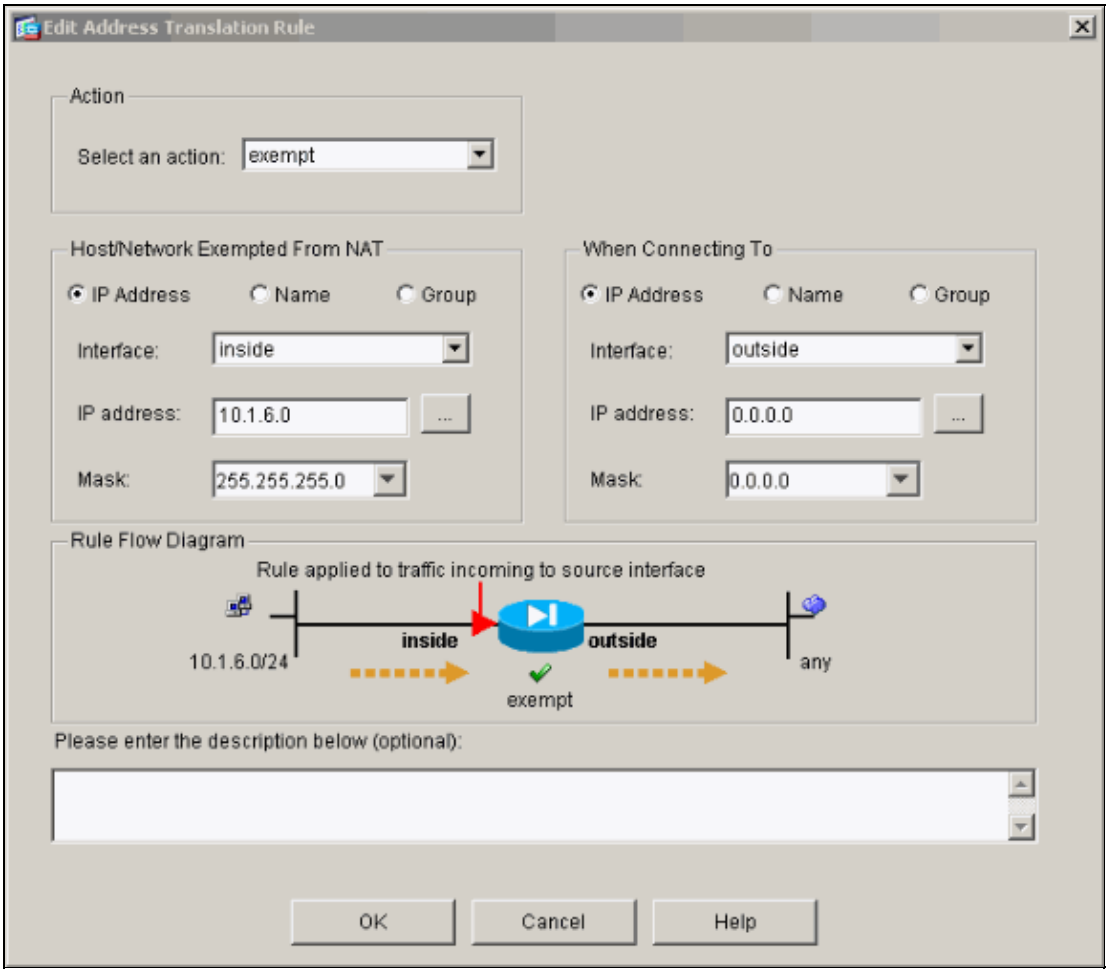
Rule	Original			Translated	
Type	Interface	Source Network	Destination Network	Interface	Address
	inside	10.1.6.0/24	any	outside	same as original address

5. If you use ACLs, which allow more precise control of traffic which you should not translate (based on source/destination), use these commands.

```
access-list 103 permit ip 10.1.6.0 255.255.255.0 any
nat (inside) 0 access-list 103
```

6. Use ASDM and select **Configuration** > **Features** > **NAT** > **Translation Rules**.
7. Select **Translation Exemption Rules** and click **Add**.

   This example shows how to exempt traffic from the 10.1.6.0/24 network to anywhere from being translated.



Edit Address Translation Rule

Action

Select an action: exempt

Host/Network Exempted From NAT

● IP Address ○ Name ○ Group

Interface: inside

IP address: 10.1.6.0

Mask: 255.255.255.0

When Connecting To

● IP Address ○ Name ○ Group

Interface: outside

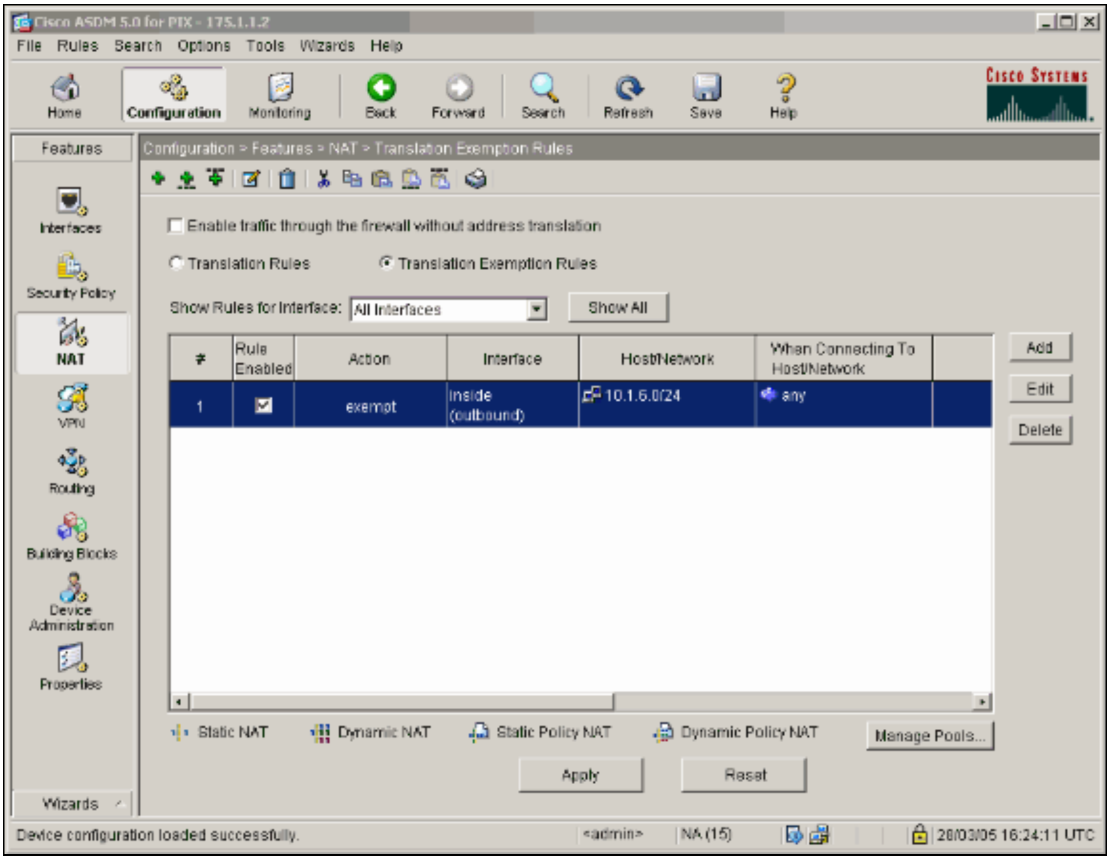
IP address: 0.0.0.0

Mask: 0.0.0.0

Rule Flow Diagram

Please enter the description below (optional):

8. Select **Configuration** > **Features** > **NAT** > **Translation Exemption Rules** in order to display the new rules.



☐ Enable traffic through the firewall without address translation

○ Translation Rules ● Translation Exemption Rules

Show Rules for Interface: All Interfaces

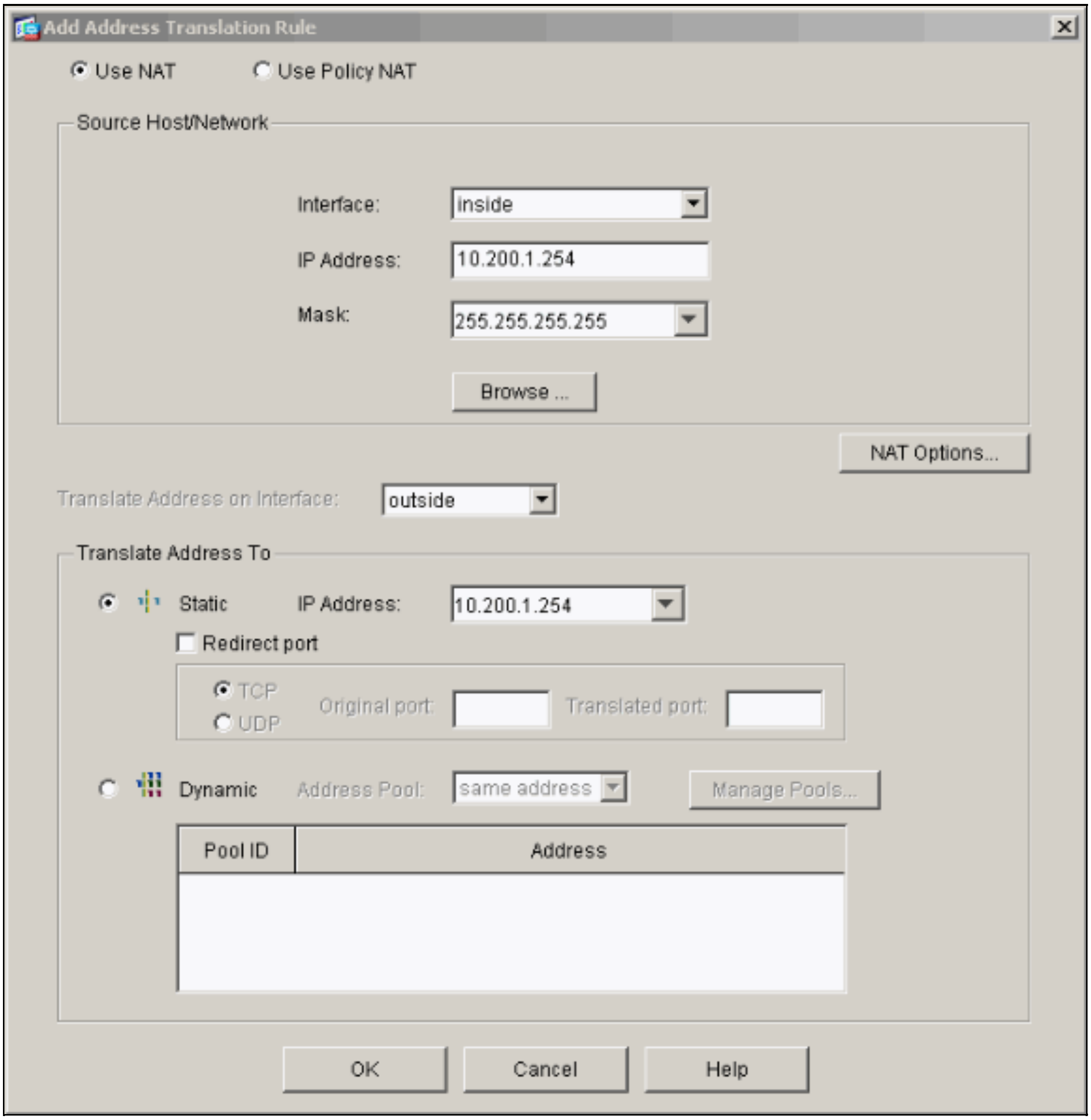
#	Rule Enabled	Action	Interface	Host/Network	When Connecting To Host/Network
1	☑	exempt	inside (outbound)	10.1.6.0/24	any

Device configuration loaded successfully. <admin> NA (15) 28/03/05 16:24:11 UTC

9. The **static** command for the web server changes as this example shows.

```
static (inside, outside) 10.200.1.254 10.200.1.254
```

10. From ASDM, select **Configuration** > **Features** > **NAT** > **Translation Rules**.
11. Select **Translation Rules** and click **Add**. Enter the source address information, and select **Static**. Enter the same address in the IP Address field.



Add Address Translation Rule

● Use NAT ○ Use Policy NAT

Source Host/Network

Interface: inside

IP Address: 10.200.1.254

Mask: 255.255.255.255

Translate Address on Interface: outside

Translate Address To

● Static IP Address: 10.200.1.254

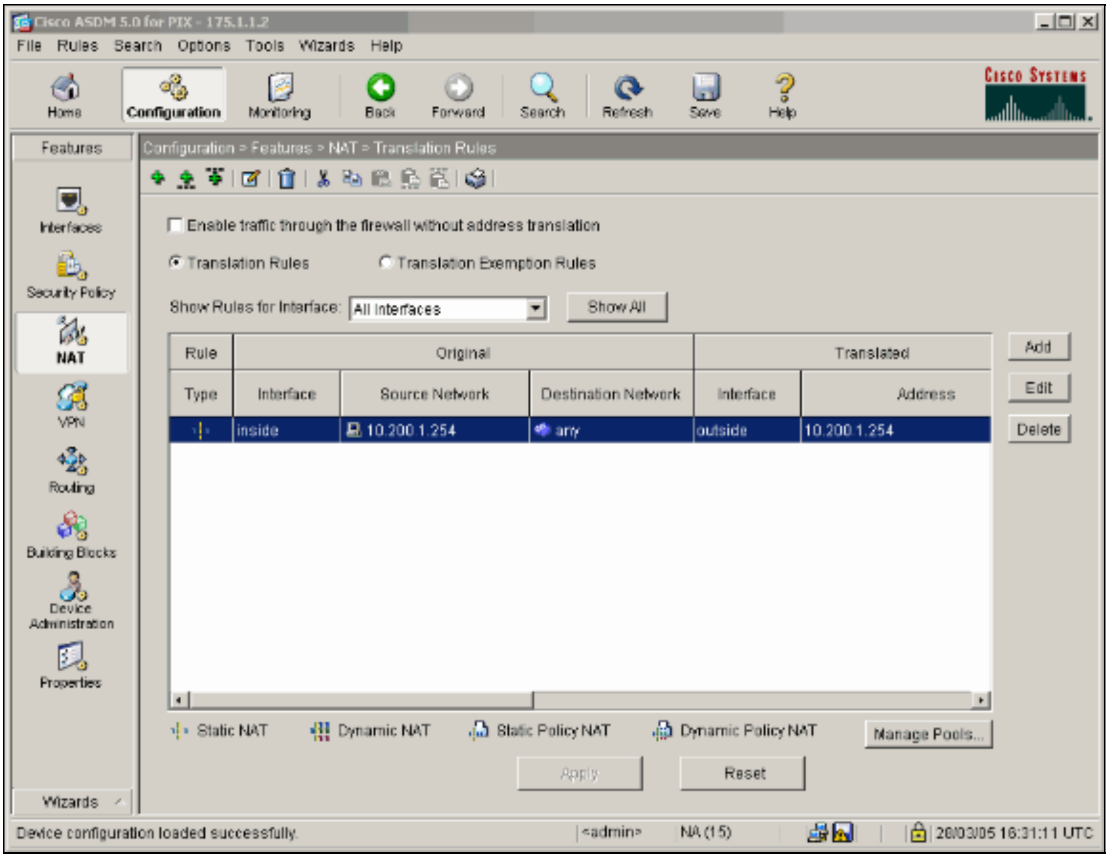
□ Redirect port

● TCP ○ UDP Original port: Translated port:

○ Dynamic Address Pool: same address

Pool ID	Address

12. The translation appears in the Translation Rules when you select **Configuration** > **Features** > **NAT** > **Translation Rules**.



Configuration > Features > NAT > Translation Rules

☐ Enable traffic through the firewall without address translation

● Translation Rules ○ Translation Exemption Rules

Show Rules for Interface: All Interfaces Show All

Rule	Original			Translated	
Type	Interface	Source Network	Destination Network	Interface	Address
	inside	10.200.1.254	any	outside	10.200.1.254

Device configuration loaded successfully. <admin> NA (15) 28/03/05 16:31:11 UTC

13. If you use ACLs, use these commands.

```
access−list 102 permit tcp any host 10.200.1.254 eq www
access−group 102 in interface outside
```

See the Restrict Inside Hosts Access to Outside Networks section of this document for additional information on the configuration of ACLs in ASDM.

Note the difference between when you use **nat 0** when you specify network/mask as opposed to when you use an ACL that uses a network/mask that permits the initiation of connections from inside only. The use of ACLs with **nat 0** permits the initiation of connections by inbound or outbound traffic. The PIX interfaces need to be in different subnets in order to avoid reachability issues.

Port Redirection with Statics

In PIX 6.0, the port redirection feature was added in order to allow outside users to connect to a particular IP address/port and have the PIX redirect the traffic to the appropriate inside server/port. The **static** command was modified. The shared address can be a unique address, a shared outbound PAT address, or shared with the external interface. This feature is available in PIX 7.0.

Note: Due to space limitations, commands are shown on two lines.

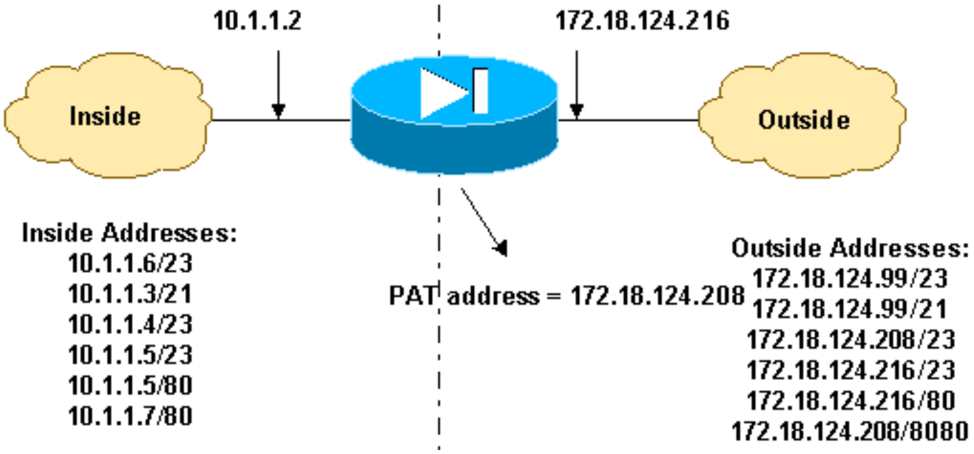
```
static [(internal_if_name, external_if_name)]
{global_ip|interface}local_ip [netmask mask] [max_conns
[emb_limit [norandomseq]]]


static [(internal_if_name, external_if_name)] {tcp|udp}
{global_ip|interface} global_port local_ip local_port
[netmask mask] [max_conns [emb_limit [norandomseq]]]
```

These port redirections are in this network example:

- External users direct Telnet requests to unique IP address 172.18.124.99, which the PIX redirects to 10.1.1.6.
- External users direct FTP requests to unique IP address 172.18.124.99, which the PIX redirects to 10.1.1.3.
- External users direct Telnet requests to PAT address 172.18.124.208, which the PIX redirects to 10.1.1.4.
- External users direct Telnet request to PIX outside IP address 172.18.124.216, which the PIX redirects to 10.1.1.5.
- External users direct HTTP request to PIX outside IP address 172.18.124.216, which the PIX redirects to 10.1.1.5.
- External users direct HTTP port 8080 requests to PAT address 172.18.124.208, which the PIX redirects to 10.1.1.7 port 80.

This example also blocks the access of some users from inside to outside with ACL 100. This step is optional. All traffic is permitted outbound without the ACL in place.

Network Diagram − Port Redirection



Partial PIX Configuration − Port Redirection

This partial configuration illustrates the use of static port redirection. See the Port Redirection network diagram.

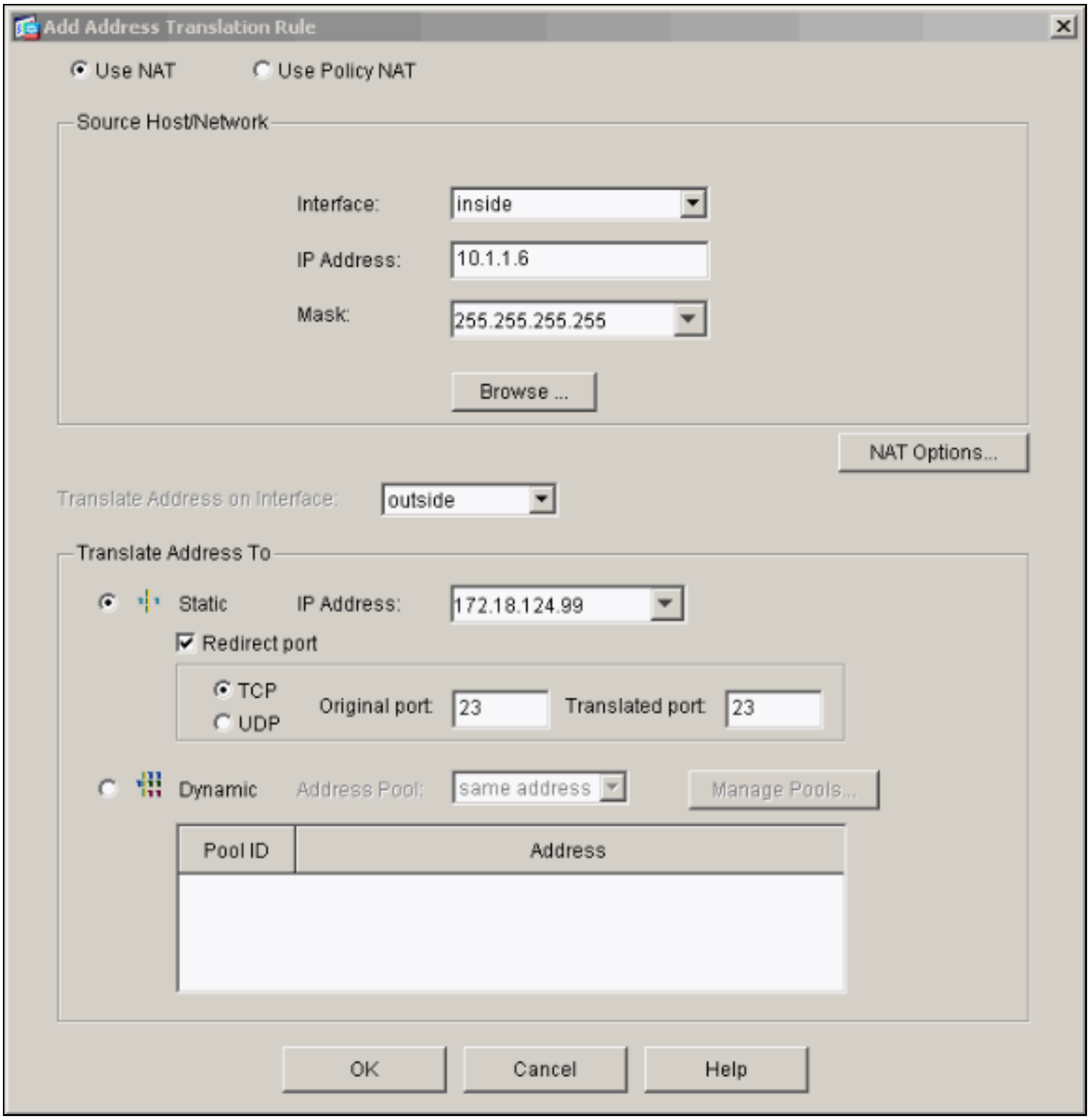
Partial PIX Configuration − Port Redirection

```
fixup protocol ftp 21

!−−− Use of an outbound ACL is optional.

access−list 100 permit tcp 10.1.1.0 255.255.255.128 any eq www
access−list 100 deny tcp any any eq www
access−list 100 permit tcp 10.0.0.0 255.0.0.0 any
access−list 100 permit udp 10.0.0.0 255.0.0.0 host 172.18.124.100 eq domain

access−list 101 permit tcp any host 172.18.124.99 eq telnet
access−list 101 permit tcp any host 172.18.124.99 eq ftp
access−list 101 permit tcp any host 172.18.124.208 eq telnet
```

```
access−list 101 permit tcp any host 172.18.124.216 eq telnet
access−list 101 permit tcp any host 172.18.124.216 eq www
access−list 101 permit tcp any host 172.18.124.208 eq 8080

ip address outside 172.18.124.216 255.255.255.0
ip address inside 10.1.1.2 255.255.255.0

global (outside) 1 172.18.124.208
nat (inside) 1 0.0.0.0 0.0.0.0 0 0

static (inside,outside) tcp 172.18.124.99 telnet 10.1.1.6
   telnet netmask 255.255.255.255 0 0
static (inside,outside) tcp 172.18.124.99 ftp 10.1.1.3
   ftp netmask 255.255.255.255 0 0
static (inside,outside) tcp 172.18.124.208 telnet 10.1.1.4
   telnet netmask 255.255.255.255 0 0
static (inside,outside) tcp interface telnet 10.1.1.5
   telnet netmask 255.255.255.255 0 0
static (inside,outside) tcp interface www 10.1.1.5
   www netmask 255.255.255.255 0 0
static (inside,outside) tcp 172.18.124.208 8080 10.1.1.7
   www netmask 255.255.255.255 0 0

!−−− Use of an outbound ACL is optional.

access−group 100 in interface inside
access−group 101 in interface outside
```

This procedure is an example of how to configure the port redirection which allows external users direct Telnet requests to unique IP address 172.18.124.99, which the PIX redirects to 10.1.1.6.

1. Use ASDM and select **Configuration** > **Features** > **NAT** > **Translation Rules**.
2. Select **Translation Rules** and click **Add**.
3. For Source Host/Network, enter the information for the inside IP address.
4. For Translate Address To, select **Static**, enter the outside IP address and check **Redirect port**.
5. Enter the pre−translation and post−translation port information (this example maintains port 23). Click **OK**.



Add Address Translation Rule

● Use NAT ○ Use Policy NAT

Source Host/Network

Interface: inside

IP Address: 10.1.1.6

Mask: 255.255.255.255

Translate Address on Interface: outside

Translate Address To

● Static IP Address: 172.18.124.99

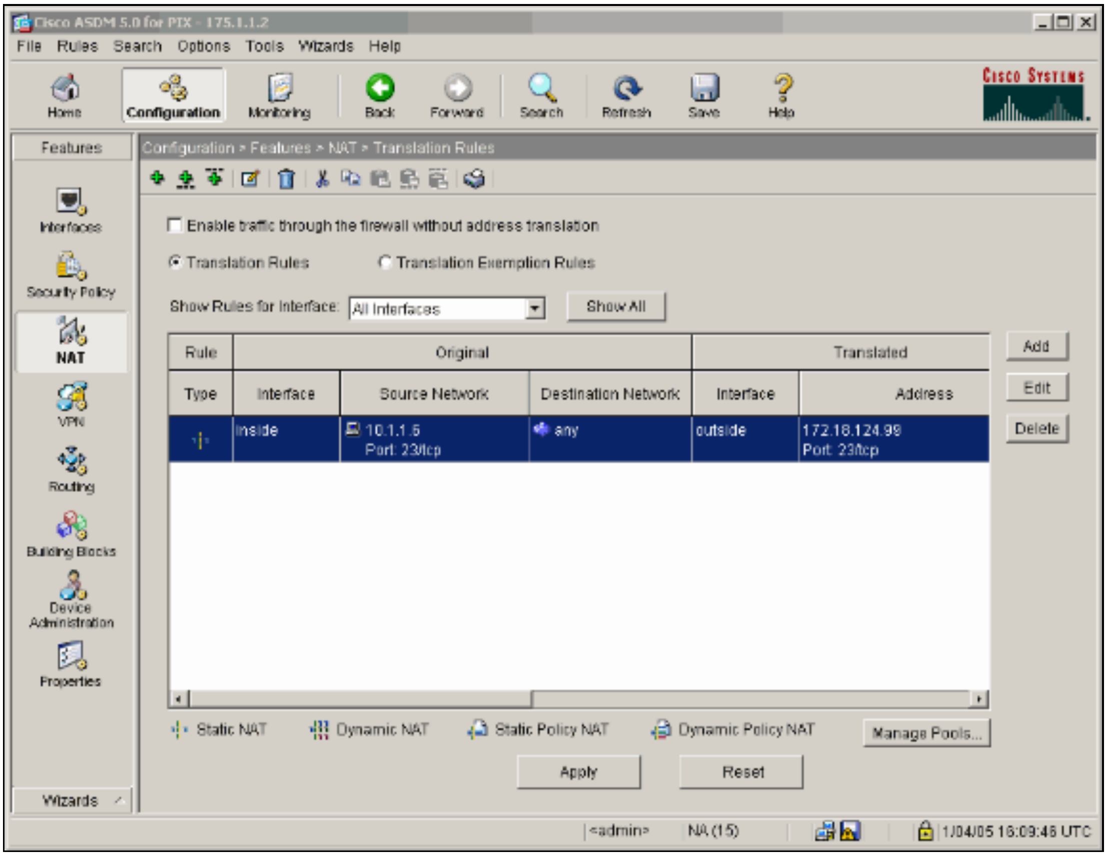
☑ Redirect port

● TCP ○ UDP Original port: 23 Translated port: 23

○ Dynamic Address Pool: same address

Pool ID	Address

The translation appears in the Translation Rules when you select **Configuration > Features > NAT > Translation Rules**.



☐ Enable traffic through the firewall without address translation

● Translation Rules ○ Translation Exemption Rules

Show Rules for Interface: All Interfaces

Rule	Original			Translated	
Type	Interface	Source Network	Destination Network	Interface	Address
	inside	10.1.1.5 Port: 23/tcp	any	outside	172.18.124.98 Port: 23/tcp

<admin> NA (15) 1/04/05 16:09:46 UTC

Information to Collect if You Open a Technical Support Case

If you still need assistance and want to open a case with Cisco Technical Support, be sure to include this information for troubleshooting your PIX Security Appliance.

- Problem description and relevant topology details.
- The steps you used to troubleshoot before you opened the case.
- Output from the **show tech−support** command.
- Output from the **show log** command after the **logging buffered debugging** command ran, or console captures that demonstrate the problem (if available).

Attach the collected data to your case in non−zipped, plain text format (.txt). You can attach information to your case in the TAC Service Request Tool (registered customers only) . If you cannot access the TAC Service Request Tool (registered customers only) , you can send the information in an E−mail attachment to attach@cisco.com with your case number in the subject line of your message.

NetPro Discussion Forums − Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums − Featured Conversations for Security
Security: Intrusion Detection [Systems]
Security: AAA
Security: General
Security: Firewalling

Related Information

- **PIX Support Page**
- **Documentation for PIX Firewall**
- **PIX Command References**
- **Requests for Comments (RFCs)**
- **Technical Support − Cisco Systems**

Updated: May 19, 2005 Document ID: 63872