Cisco - PIX 7.0 and Adaptive Security Appliance Port Redirection with nat, global, static, conduit, and access-list Comm

# **Table of Contents**

PIX 7.0 and Adaptive Security Appliance Port Redirection with nat, global, static, conduit, and
<u>access–list Commands</u> 1
<u>Document ID: 63872</u> 1
Introduction1
Prerequisites
Requirements
<u>Components Used</u> 1
Conventions
<u>Network Diagram</u>
Initial Configuration
Allow Outbound Access
Allow Inside Hosts Access to Outside Networks with NAT
Allow Inside Hosts Access to Outside Networks with the use of PAT
Restrict Inside Hosts Access to Outside Networks
Allow Untrusted Hosts Access to Hosts on Your Trusted Network
Use ACLs on PIX Versions 7.0 and Later
Disable NAT for Specific Hosts/Networks
Port Redirection with Statics
<u>Network Diagram – Port Redirection</u>
Partial PIX Configuration – Port Redirection
Information to Collect if You Open a Technical Support Case
NetPro Discussion Forums – Featured Conversations
Related Information

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

#### Document ID: 63872

Introduction **Prerequisites** Requirements Components Used Conventions **Network Diagram Initial Configuration Allow Outbound Access** Allow Inside Hosts Access to Outside Networks with NAT Allow Inside Hosts Access to Outside Networks with the use of PAT Restrict Inside Hosts Access to Outside Networks Allow Untrusted Hosts Access to Hosts on Your Trusted Network Use ACLs on PIX Versions 7.0 and Later **Disable NAT for Specific Hosts/Networks Port Redirection with Statics** Network Diagram - Port Redirection Partial PIX Configuration - Port Redirection Information to Collect if You Open a Technical Support Case NetPro Discussion Forums – Featured Conversations **Related Information** 

## 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:

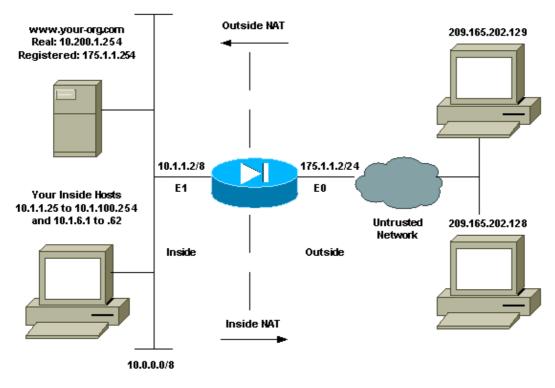
• Cisco PIX 500 Series Security Appliance Software version 7.0 and later

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

Cisco - PIX 7.0 and Adaptive Security Appliance Port Redirection with nat, global, static, conduit, and acces

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.

File Rules Sea	_			is Help					_ 🗆 X
G Home C		🍪 juration	Monitoring	Back Forwa	rd S	Q Q Refresh	Save Help		ISCO SYSTEMS
Features	_	_		AT > Translation Ru					
				科 🎰 🎼 🎼 🛍 🕯		handollon			
Interfaces			ation Rules						
Becurity Policy				C Translation	Exemp				
24		Show Ru	les for Interface:	All Interfaces		<ul> <li>Show All</li> </ul>			
NAT		Rule		Origin	nal			Translated	Add
		Туре	Interface	Source Netwo	irk	Destination Network	Interface	Address	Edit
* <u>2</u> 5									Delete
Routing									
Building Blocks									
2									
Device Administration									
Properties									
		•						<u> </u>	
		• Static	NAT 🚻 I	Dynamic NAT	👌 Stati	: Policy NAT 🛛 🖓	Dynamic Policy N	AT Manage Pools	
						Apply	Reset		
Wizards 🗠						14-14			
						test	NA (15)	🍰     🔂 20/03/06	14:38:38 UTC

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

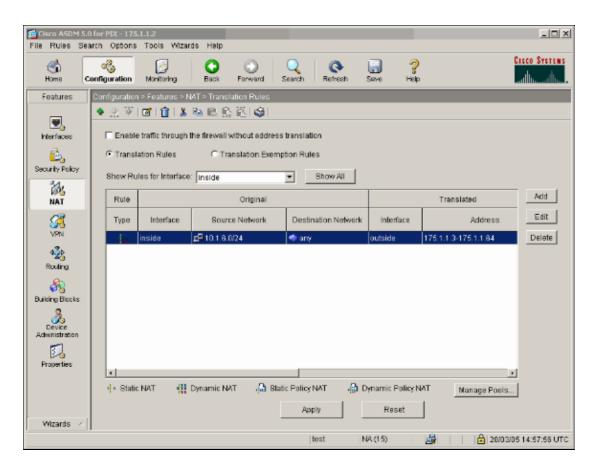
- 3. Use ASDM to create your global address pool. In order to do this, select **Configuration > Features >** NAT and choose Manage Pools.
- 4. Select **Outside > Add**, and choose a range to specify a pool of addresses.
- 5. Enter your address range, enter a Pool ID, and click **OK**.

🚰 Add Global Pool Item	×
Interface: outside  Pool ID: 1	
Range	
C Port Address Translation (PAT)	
O 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	
OK Cancel Help	

- 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 R	ule	2
Use NA	r ou	Ise Policy NAT	
-Source Ho	st/Network-		
		Interface;	inside
		IP Address:	10.1.6.0
		Mask:	255.255.255.0
			Browse
			NAT Options
Translate Ad	ldress on Inte	rface: outsi	ide 🔽
Translate	Address To		
C 11	Static		
	C UDP	Original port	t: Translated port:
• 👖	Dynamic	Address Pool:	1 Manage Pools
	Pool ID		Address
	1	175.1.1.3-175.1	.1.1.64
	1		
		OK	Cancel Help

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



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.

🕵 Add Global Pool Item	×
Interface: outside Pool ID: 2	
O Range	
Port Address Translation (PAT)	
O Port Address Translation (PAT) using the IP address of the interface	
IP Address: 175.1.1.65 —	
Network Mask (optional):	
OK Cancel Help	

- 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**.

	Translation Ru	ule		
🖲 Use NA	τ Ου	se Policy NAT		
-Source Ho	ost/Network			
		Interface:	inside 🔽	
		IP Address:	10.1.6.0	
		Mask:	255.255.255.0	
			Browse	
			NAT Options	
Translate Ar	ddress on Inter	rface: outsid		
	Address To	Journe		
Translate	Address TO -			
C de	01-11-	(D. f. d. france)		
C 11	Static Redirect p		V	
C II	Static Redirect p O TCP O UDP		Translated port:	
	Redirect p     TCP     OUDP	ort	Translated port: 2 Manage Pools	
	Redirect p     TCP     C UDP	ort Original port:		
	C Redirect p  TCP C UDP  Dynamic  Pool ID	ort Original port:	2 Manage Pools	
	C Redirect p  TCP C UDP  Dynamic  Pool ID	ort Original port: Address Pool:	2 Manage Pools	
	C Redirect p  TCP C UDP  Dynamic  Pool ID	ort Original port: Address Pool:	2 Manage Pools	
	C Redirect p  TCP C UDP  Dynamic  Pool ID	ort Original port: Address Pool:	2 Manage Pools	

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

Image: Source Name   Image:	File Rules Sea			ds Help				_0 ×
Image: Properties     Image: Properties <th></th> <th></th> <th>2</th> <th>Back Forward S</th> <th>Q Q Search Refresh</th> <th></th> <th></th> <th>Cisco Systems</th>			2	Back Forward S	Q Q Search Refresh			Cisco Systems
Interfaces   Interfaces   Security Folicy   Image Properties   Image Properties     Image Properties	Features	Configuration	i > Features > N	AT > Translation Rules				
Herraces   Image Properties     Image Properties   <			1 🗹   👔   👗	8a 🛍 🕼 🛍 🗳 I				
Security Policy   Image Policy		🗖 Enable	e traffic through t	he firewall without address	translation			
Show Rules for Interface:     Aut     Interface:     Add     Interface:     Show All     Rule     Original     Translated     Add     Interface:     Show All     Rule     Original     Translated     Add:     Type     Interface:     Show All     Rule     Original     Translated     Add:     Type     Interface:     Show All     Rule     Original     Translated     Add:     Type     Interface:     Show All     Rule     Original     Type     Interface:     Show All     Rule     Original     Type     Interface:     Show All     Rule     Type     Interface:     Show All     Rule     Type     Interface:     Show All     Rule     I		Transl	ation Rules	C Translation Exemp	tion Rules			
NAT       Rule       Original       Translated       Rod         VPN       Type       Interface       Source Network       Destination Network       Interface       Address       Edit         VPN       inside       Isl       Interface       Source Network       Destination Network       Interface       Address       Edit         Working       inside       Isl       Interface       Source Network       Destination Network       Interface       Address       Delete         Maining Blocks       Inside       Isl       Isl       Isl       Isl       Isl       Delete       Isl       Isl       Delete       Isl       Isl		Show Ru	les for Interface	All Interfaces	<ul> <li>Show All</li> </ul>			
Image Protected     Image Protected       Roding     Image Protected       Building Blocks     Image Protected       Image Protected     Image Protected	NAT	Rule		Original			Translated	Add
Image Protected     Image Protected       Roding     Image Protected       Building Blocks     Image Protected       Image Protected     Image Protected	2	Туре	Interface	Source Network	Destination Network	Interface	Address	Edit
Routing       Image: Properties         Properties       Image: Properties         Image: Properties       Image: Properties		44	inside	g <sup>pi</sup> 10.1.6.0/24	🧇 any	outside 1	75.1.1.85	Delete
Buiking Blocks         Buiking Blocks         Buiking Blocks         Adwinistration         Properties         Image Properties         Image Pools								
Building Blocks       Device Administration       Properties       Image Pools       Image Pools       Image Pools       Image Pools       Image Pools	Routing							
Device         Administration         Properties         *         *         *         *         *         *         Static NAT         *         Apply         Reset								
Administration Properties * Static NAT Apply Reset Apply Reset	Q.							
Properties								
Properties								
Image Pools     Apply     Reset	<u>~</u>							
Apply Reset			NOT			manufa Dalla Ala		
		ii. State	NAT 1	oynamic NAT 🧃 Stat	e Honey NAT 1 450 D	ynamic Policy NA	Manage Pools	·
Withins / II	180-rede			_	Apply	Reset		
There configuration loaded successfully. Lest NA (15) 📑 🛃 📋 🔂 2003/05 15:21:46 UTC	Wizards <	on londed are			linet 1	0.45		0545-04-46400

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

Cisco - PIX 7.0 and Adaptive Security Appliance Port Redirection with nat, global, static, conduit, and access

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	Syslog
Select an action: permit	Default Syslog More Options
Apply to Traffic: incoming to src interface ▼	Time Range Time Range: Not Applied 💌 New
Source Host/Network	Destination Host/Network
IP Address ⊂ Name ⊂ Group	CIP Address C Name C Group
Interface: inside	Interface: outside
IP address: 10.1.6.0	IP address: 0.0.0.0
Mask: 255.255.255.0 💌	Mask: 0.0.0.0
Rule Flow Diagram Rule applied to traffic incoming to	source interface
#	<u>e</u>
10.1.6.0/24 inside	any any
Protocol and Service	
© TCP C UDP C ICMP C IP Source Port	Manage Service Groups
Source Fort	Destnation Pon
Service = _ any	• Service = vwww
C Service Group	C Service Group
Please enter the description below (optional):	
	ant Hole
OK Can	cel Help

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

Gisco ASDM 5.0 i File Rules Sear		_	_	ards Help						_ 🗆 ×
Home Co	ofigurati		illoring	Back Fo	inward Se	arch Refres	h Save	<b>?</b> Help		CO SYSTEMS
				Security Policy > /						
				B 🗈 🕼 🛱		_				
Interfaces				AA Rules C Fi		C Service Polic	y Rules			
۵.	Show P	Rules for	interíace:	All Interfaces	• Si	IOW/All				
Security Policy	*	Rule Ensbled	Action	Source HostiNetwo	ork	Destination Host/Network	Rule Appl To Traffic	ied Interface	Service	Add
24	1	V	×	💑 10.1.6.0/24	٩	any	🔊 incom	-	😎 http/top	Edit
NAT	2	V	0	🧼 any	-	any	📌 incom	-	₩ http/tcp	Delete
<u> 3</u>	3		- 🎸 -	🧇 any	*	any	🛹 incomi	ing inside	🍱 ip	
Routing Routing Building Blocks Device Administration Fraperties										
	•								•	
	🖌 🖌 I	llow traffi	c	Oeny traffic			(	Show Summary	C Show Detail	
Wizards 🕢					Apply	Res	et 🖌	kdvanced		

# 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 T	ranslation R	ule					2
Use NAT	00	Ise Policy NAT					
Source Ho	st/Network						
		Interface: IP Address: Mask:	Inside 10.200.1.254 255.255.255.25	is <b>v</b>			
Translate Adv	dress on Inte	rface: outsi	Browse	]		NAT Option	ns
Translate A	Address To						
	Static	IP Address: port	175.1.1.254	•			
	C UDP	Original port:	Tra	inslated port:			
o 41	Dynamic	Address Pool:	same address	<b>Y</b>	Manage P	ools	
	Pool ID		Addres	s			
		ОK	Cancel		Help		

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

Gisco ASDM 5. File Rules Se		5.1.1.2 s Tools Wiza	rds Help					_ 🗆 ×
💰 Home	ang and a configuration	Monitoring	O Back Fo	nward Search	<b>Q</b> Refresh	Save Help		CISCO SYSTEMS
Features	Configuratio	in > Features > I	VAT > Translation	n Rules				
	* * *	1 🗹   📋   👗	B 🗈 🔂 🛱	S   🍪				
Interfaces	🗆 Enab	le traffic through	the firewall witho	out address trans	ation			
<u>6</u> ,	C Trans	slation Rules	C Transla	ation Exemption R	ules			
Security Policy	Show R	ules for Interfac	a All Interfaces	•	Show All			
NAT	Rule		0	iriginal			Translated	Add
	Туре	Interface	Source Ne	etwork De	tination Networ	k Interface	Address	Edit
	1.0	inside	🚨 10.200.1.25	4 🥠 a	ny	outside	175.1.1.254	Delete
* <b>2</b> 5								
Routing								
Suilding Blocks								
Salar & Dictors								
Device Administration								
Properties								
								-
	• Stat	IC NAT	Dynamic NAT	🖓 Static Poli	CYNAT 🎲	Dynamic Policy N	IAT Manage Pools.	-
					4oply	Reset		
Wizards 🗠								
					best	NA (15)	😹 🔂 🔰 🔂 26/03/	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.

_	for PIX - 175.1.1.2 rch Options Tools W	zards Help				_ [ ] ×
Home Co	nfiguration Monitoring	Back Forward	Q Q Search Refresh	Save Help		Cisco Systems
Features	Configuration > Features	> Security Policy > Access F	Rules			
	🗢 👷 🍹 🗹 👔 🛙	🌡 🔁 🕮 💁 🔣 🤤 I				
Interfaces	C Access Rules C Show Rules for Interfac	AVA Rules C Filter Rule e: outside	s C Service Policy Ru Show All	iles		
Security Policy	≠ Rule Enabled Action		Destination Host/Network	Rule Applied	Interface Ser	Add
24	1 🗹 🧹	🧇 any	🛋 10.200.1.254	🖓 incoming of	utsicle 🐵 http/tc	p Edit
NAT	2 🗹 🖌	A 199.199.199.24	a 10.200.1.254	🚚 incoming o	itside 🚥 fip/top	Delete
VPN Rouling Building Blocks Device Administration Fraperties	•					3
	🖌 Allow traffic	3 Deny traffic		Show	Summary C Show (	Detail
Wizards 🔺		Apply	Reset	Advance	ed	
Configuration char	iges saved successfully.		<admin></admin>	NA (15)	🛃 🔂 📔 🔒 26/0	305 16:11:21 UT

## **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 1	ranslation R	ule	>
🖲 Use NA	r ou	Ise Policy NAT	
- Source Ho	st/Network		
		Interface: inside	
		IP Address: 10.1.6.0	
		Mask: 255.255.255.0	
		Browse	
		NAT Options	
Translate Ad	dress on Inte	rface: outside	
Translate.	Address To		
0.1	Static	IP Address:	
	🗖 Redirect p	rort	
	C TOP	Original port: Translated port	
• 📲	Dynamic	Address Pool: same address 💌 Manage Pools	
	Pool ID	Address	
	N/A	No address pool defined	
		OK Cancel Help	

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

File Rules Sea	for PIX - 175 irch Options	Tools Wizar	ds Help					202
Home C	onfiguration	i Monitoring	Back Forward	Search	Refresh	🔜 ? Seve Нер		CISCO SYSTEMS
Features			IAT > Translation Rule:					
-		3	86 🗈 🛱 🗟 🗳					
Interfaces	🗖 Enabl	e traffic through (	the firewall without add	iress transia	tion			
<u>6</u> ,	C Transl	lation Rules	C Translation E	xemption Ru	iles			
Security Policy	Show Ru	iles for Interface	All Interfaces	•	Show All			
NAT	Rule		Original				Translated	Add
<u> </u>	Type	Interface	Source Network	Des	ination Network	Interface	Address	Edit
VPN		inside	g <mark>≓</mark> 10.1.6.0/24	🧇 an	γ	outside	same as original address	Delete
* <u>2</u> %								
Routing								
<i>8</i> 3								
Building Blocks								
Jevice								
Administration								
Properties				Static Polic				<u>-</u>
~ ~		A1477 111		Static Polic	KINAL JEL	Dynamic Policy N	AT Manage Pools	
20	vie Statio	NAT 🚻	Dynamic NAT 🖓 🖓		,			
~ 5		: NAT 📲	Dynamic NAT dad		aply	Reset		

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	When Connecting To
Interface: Inside	Interface: outside
IP address: 10.1.6.0	IP address: 0.0.0.0
Mask: 255.255.255.0 💌	Mask: 0.0.0.0
Rule Flow Diagram Rule applied to traffic incoming to Inside	outside any
Please enter the description below (optional):	
	×
OK Car	ncel Help

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

	) for PIX - 175.1.1.2 arch Options Tools	Mizarda Help				<u>_0 ×</u>
Home Co	onfiguration Monitoria	g Back F	Forward Search	Refresh Save	<mark>о</mark> Најр	CISCO SYSTEMS
Features	Configuration > Feature					
	********	🏅 🖻 🖪 🔝 i	5 9			
Interfaces	Enable traffic thr	ough the firewall with	hout address transla	tion		
<u>6</u> ,	C Translation Rule	s 📀 Trans	lation Exemption Ru	les		
Security Policy	Show Rules for Inte	rface: All Interfaces	s 💌	Show All		
NAT	≠ Ruis Enabled	Action	Interface	Host/Network	When Connecting To Host/Network	Add
SK VPN	1 🖬	exempt	inside (outbound)	<b>g</b> ≌ 10.1.6.0/24	💠 any	Edit
Routing						Delete
Ruiking Blocks						
Device Administration						
Froperties	•					
	1 Static NAT	🚻 Dynamic NAT	🛺 Static Policy	y NAT 🛛 🔒 Dynamic	Policy NAT Manage Po	ools
			A	apty Re	eset	
Wizards 🗠						
Device configuration	on loaded successfully.			<admin> NA (15)</admin>	😡 🍰 🔰 🔒 2	8/03/05 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 Translatio	on Rule	J
• Use NAT	C Use Policy NAT	
Source Host/Networ	rk	
	Interface: inside IP Address: 10.200.1.254 Mask: 255.255.255	
Translate Address on	Interface: outside	
⊙ י <mark>י</mark> Static		
C U	CP Original port	
C 🖞 Dynamic	Address Pool: same address 💌 Manage Pools	
Pool I	D Address	

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



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.

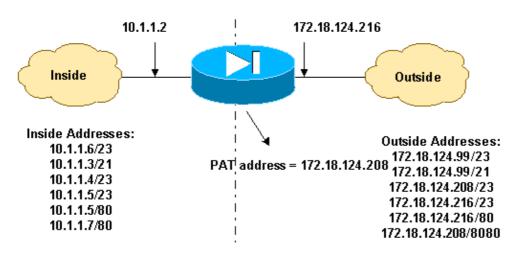
```
static [(internal_if_name, external_if_name)]
{global_ip/interface}local_ip [netmask mask] [max_conns
[emb_limit [norandomseq]]]
static [(internal_if_name, external_if_name)] {tcp/udp}
{global_ip/interface} global_port local_ip local_port
[netmask mask] [max_conns [emb_limit [norandomseq]]]
```

Cisco - PIX 7.0 and Adaptive Security Appliance Port Redirection with nat, global, static, conduit, and access

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 Redirectionfixup 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 wwwaccess-list 100 deny tcp any any eq wwwaccess-list 100 permit tcp 10.0.0.0 255.0.0.0 anyaccess-list 100 permit udp 10.0.0.0 255.0.0.0 host 172.18.124.100 eq domainaccess-list 101 permit tcp any host 172.18.124.99 eq telnetaccess-list 101 permit tcp any host 172.18.124.99 eq ftpaccess-list 101 permit tcp any host 172.18.124.208 eq telnet
```

Cisco - PIX 7.0 and Adaptive Security Appliance Port Redirection with nat, global, static, conduit, and access

```
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 R	ule					x
🖲 Use NA	т сі	Jse Policy NAT					
-Source He	ost/Network-						
		Interface:	inside		•		
		IP Address:	10.1.1.6				
		Mask:	255.255.255	.255	•		
			Browse				
-						NAT Options	
Translate Ac	ídress on inte	erface: outsid	ie 💌				
Translate	Address To –						
· •	Static Redirect	IP Address: port	172.18.124.9	99 <u>-</u>	]		
		Original port:	23	Translated p	ort. 23		
c 📲	Dynamic	Address Pool:	same addre	ss 🔻	Manage Poo	ls	
	Pool ID		Add	ress			
		OK	Cance		Help		

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

Eisco ASDM 5.0 File Rules Sea	_			ls Help				_ 🗆 X
Home C		le guration	Monitoring	Back Forward S	Q Q Search Refresh	📄 🢡 Save Help		Cisco Systems
Features	_			AT > Translation Rules				
Interfaces				🖎 🛍 🔝 📆 🚳 I	translation			
<u>6</u> ,		🖲 Transl	ation Rules	C Translation Exemp	tion Rules			
Security Policy		Show Ru	les for interface:	All Interfaces	Show All			_
NAT		Rule		Original			Translated	Add
ST VIPN		Туре	Interface	Source Network	Destination Network	Interface	Address	Edit
		- it	inside	B 10.1.1.5 Port: 23/lcp	💠 any	outside	172.18.124.99 Port 23/tcp	Delete
Routing								
Ruiking Blocks								
Sevice Administration								
Froperties		1						
		• Static	NAT 48 (	)ynamic NAT 🛛 , 🔒 Stati	Lic Policy NAT 🛛 🔒 D	ynamic Policy N		1
		,	m		Apply	Reset		
Wizards 🗠					<admin></admin>	NA (15)	🚔 🛃 🛛 🔒 1,104,10	15 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

All contents are Copyright © 1992–2005 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: May 19, 2005

Document ID: 63872