# PIX/ASA 7.x: Port Redirection(Forwarding) mit NAT-, Global-, statischen und Zugriffslistenbefehlen

# Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Zugehörige Produkte Konventionen Netzwerkdiagramm Erstkonfiguration Ausgehenden Zugriff zulassen Zugriff für interne Hosts auf externe Netzwerke mit NAT zulassen Zulassen des Zugriffs von internen Hosts auf externe Netzwerke mithilfe von PAT Einschränken des Zugriffs von internen Hosts auf externe Netzwerke Zugriff für nicht vertrauenswürdige Hosts auf Hosts in Ihrem vertrauenswürdigen Netzwerk zulassen Verwenden von ACLs auf PIX 7.0 und höher Deaktivieren von NAT für bestimmte Hosts/Netzwerke Port Redirection (Forwarding) mit Statistiken Netzwerkdiagramm - Port Redirection (Forwarding) Partielle PIX-Konfiguration - Port-Umleitung Einschränkung der TCP/UDP-Sitzung mithilfe von Static Zeitbasierte Zugriffsliste Informationen zum Sammeln, wenn Sie ein technisches Support-Ticket öffnen Zugehörige Informationen

# **Einführung**

Um die Sicherheit bei der Implementierung der Cisco PIX Security Appliance Version 7.0 zu maximieren, müssen Sie wissen, wie Pakete zwischen höheren Sicherheitsschnittstellen und niedrigeren Sicherheitsschnittstellen weitergeleitet werden, wenn Sie die Befehle **nat-control**, **nat**, **global**, **static**, **access-list und access-group** verwenden. In diesem Dokument werden die Unterschiede zwischen diesen Befehlen und die Konfiguration der Port Redirection (Forwarding) und der externen Network Address Translation (NAT)-Funktionen in der PIX-Software Version 7.x unter Verwendung der Befehlszeilenschnittstelle oder des Adaptive Security Device Manager (ASDM) erläutert.

**Hinweis:** Einige Optionen in ASDM 5.2 und höher können sich von den Optionen in ASDM 5.1 unterscheiden. Weitere Informationen finden Sie in der <u>ASDM-Dokumentation</u>.

# <u>Voraussetzungen</u>

#### **Anforderungen**

Informationen zur Konfiguration des Geräts durch den ASDM finden Sie unter Zulassen von HTTPS-Zugriff für ASDM.

#### Verwendete Komponenten

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

- Cisco PIX Security Appliance Software der Serie 500, Version 7.0 und höher
- ASDM Version 5.x oder höher

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

#### Zugehörige Produkte

Sie können diese Konfiguration auch mit Cisco ASA Security Appliance Version 7.x oder höher verwenden.

#### **Konventionen**

Weitere Informationen zu Dokumentkonventionen finden Sie in den <u>Cisco Technical Tips</u> <u>Conventions</u> (Technische Tipps zu Konventionen von Cisco).

### **Netzwerkdiagramm**



Die in dieser Konfiguration verwendeten IP-Adressierungsschemata sind im Internet nicht rechtlich routbar. Es handelt sich um RFC 1918-Adressen, die in einer Laborumgebung verwendet wurden.

### **Erstkonfiguration**

Die Schnittstellennamen lauten:

- interface ethernet 0 Name außerhalb
- interface ethernet 1 Name innen

**Hinweis:** Um weitere Informationen zu den in diesem Dokument verwendeten Befehlen zu erhalten, verwenden Sie das <u>Command Lookup Tool</u> (<u>nur registrierte</u> Kunden).

# Ausgehenden Zugriff zulassen

Der ausgehende Zugriff beschreibt Verbindungen von einer Schnittstelle mit höherer Sicherheitsstufe zu einer Schnittstelle mit niedrigerer Sicherheitsstufe. Dazu gehören Verbindungen von innen nach außen, von innen nach Demilitarized Zones (DMZs) und von DMZs nach außen. Dies kann auch Verbindungen von einer DMZ zu einer anderen umfassen, sofern die Schnittstelle der Verbindungsquelle eine höhere Sicherheitsstufe als das Ziel hat. Überprüfen Sie die Konfiguration der "Sicherheitsstufe" an den PIX-Schnittstellen, um dies zu bestätigen.

Dieses Beispiel zeigt die Sicherheitsstufe und die Konfiguration des Schnittstellennamen:

pix(config-if)#security-level 0
pix(config-if)#nameif outside
pix(config-if)#exit

PIX 7.0 führt den Befehl **nat-control ein**. Sie können den Befehl **nat-control** im Konfigurationsmodus verwenden, um anzugeben, ob NAT für externe Kommunikation erforderlich ist. Bei aktivierter NAT-Kontrolle ist eine Konfiguration von NAT-Regeln erforderlich, um ausgehenden Datenverkehr zuzulassen, wie dies bei früheren Versionen der PIX-Software der Fall ist. Wenn die NAT-Steuerung deaktiviert ist (**keine NAT-Kontrolle**), können interne Hosts ohne Konfiguration einer NAT-Regel mit externen Netzwerken kommunizieren. Wenn Sie jedoch interne Hosts haben, die keine öffentlichen Adressen haben, müssen Sie NAT für diese Hosts konfigurieren.

Um die NAT-Steuerung mithilfe von ASDM zu konfigurieren, wählen Sie im ASDM Home-Fenster die Registerkarte Configuration (Konfiguration) aus, und wählen Sie **NAT** im Funktionsmenü aus.

**Ermöglichen Sie ohne Übersetzung Datenverkehr durch die Firewall:** Diese Option wurde in PIX Version 7.0(1) eingeführt. Wenn diese Option aktiviert ist, wird in der Konfiguration kein Befehl zur **Nichtkontrolle** ausgegeben. Dieser Befehl bedeutet, dass keine Übersetzung erforderlich ist, um die Firewall zu passieren. Diese Option wird in der Regel nur aktiviert, wenn interne Hosts öffentliche IP-Adressen haben oder die Netzwerktopologie keine Übersetzung interner Hosts in eine beliebige IP-Adresse erfordert.

Wenn interne Hosts über private IP-Adressen verfügen, muss diese Option deaktiviert werden, damit interne Hosts in eine öffentliche IP-Adresse übersetzt werden und auf das Internet zugreifen können.

File Rules Se	.1 for PIX - 10. earch Options	.1.1 Tools Wizard	ds Help				_ 🗆 ×
Home I	Configuration	Monitoring	Back Forward	Q Q Search Retresh :	Save Help		ISCO STSTERS
Interfaces Security Policy	Configuration	n > NAT > Transi I III IIII & e traffic through t lation Rules iles for Interface:	ation Rules	translation; ption Rules			
NAT	Rule		Original			Translated	Add
VPN	Туре	Interface	Source Network	Destination Network	Interface	Address	Edit
Routing Global Objects Properties	۲ ۲۰ Stati	CNAT HI	Dynamic NAT 🔥 🔒 Stal	iic Policy NAT 🖓 D Aggly	ynamic Policy N/ Reset	AT Manage Pools	Delete
				<admin> NA</admin>	(15)	😹 🔂 🔰 🔒 7/11/06 6	3:02:29 PM UTC

Es gibt zwei Richtlinien, die erforderlich sind, um den ausgehenden Zugriff mit NAT-Kontrolle zu ermöglichen. Die erste Methode ist eine Übersetzungsmethode. Dabei kann es sich um eine statische Übersetzung mit dem **statischen** Befehl oder um eine dynamische Übersetzung mit einer **nat/global**-Regel handeln. Dies ist nicht erforderlich, wenn die NAT-Kontrolle deaktiviert ist und Ihre internen Hosts öffentliche Adressen haben.

Die andere Anforderung für den ausgehenden Zugriff (gilt für die Aktivierung oder Deaktivierung der NAT-Steuerung) besteht darin, dass eine Zugriffskontrollliste (ACL) vorhanden ist. Wenn eine ACL vorhanden ist, muss sie dem Quell-Host mithilfe des spezifischen Protokolls und Ports Zugriff auf den Zielhost gewähren. Standardmäßig gibt es keine Zugriffsbeschränkungen für ausgehende Verbindungen über den PIX. Wenn für die Ausgangsschnittstelle keine ACL konfiguriert ist, ist die ausgehende Verbindung standardmäßig zulässig, wenn eine Übersetzungsmethode konfiguriert wurde.

#### Zugriff für interne Hosts auf externe Netzwerke mit NAT zulassen

Diese Konfiguration gewährt allen Hosts im Subnetz 10.1.6.0/24 Zugriff auf die Außenseite. Verwenden Sie dazu die **nat-** und die **globalen** Befehle, wie in diesem Verfahren veranschaulicht wird.

1. Definieren Sie die interne Gruppe, die Sie für NAT einschließen möchten.

2. Geben Sie einen Adresspool auf der externen Schnittstelle an, in die die in der NAT-Anweisung definierten Hosts übersetzt werden.

```
global (outside) 1 172.16.1.5-172.16.1.10 netmask 255.255.255.0
```

 Verwenden Sie ASDM, um Ihren globalen Adresspool zu erstellen. Wählen Sie Configuration
 Features > NAT aus, und deaktivieren Sie Enable traffic through the firewall without address translation. Klicken Sie anschließend auf Hinzufügen, um die NAT-Regel zu konfigurieren

Cisco ASDM 5.1	for PIX - 10.1	.1.1 Tools Wigan	te Holn				_ [ ] X
Home C	onfiguration	Monitoring	Back Forward S	C C Search Refresh	Save Help		Cisco Systems
Interfaces	Configuration	> NAT > Transl	ation Rules Pa 📾 🕵 🛍 😂 I	translation			
Security Policy	© Transla	ation Rules	C Translation Exemp	tion Rules			
NAT	Show Rul	es for interface:	All Interfaces	Show All			
07	Rule		Original			Translated	Add
VPN	Туре	Interface	Source Network	Destination Network	Interface	Address	Edit
Routing Global Objects Properties	V Static	NAT III I	Dynamic NAT 🖓 Stati	c Policy NAT	ynamic Policy NAT	Manage Pools	Delete
			[	Apply	Reset		3:02:29 PM UTC

4. Klicken Sie auf **Pools verwalten**, um die NAT-Pooladressen zu definieren.

• Use NAT	0	Jse Policy NAT			
Source Ho	st/Network				
		Interface:	inside.	T	
		IP Address: Mask:	10.1.6.0	-	
			Browse		
					NAT Options
anslate Ado	dress on Inte	rface: outsi	de 💌		
Translate A	Address To				
Translate A	Address To - Static	IP Address.		<b>*</b>	
Translate A C י י	Address To - Static Redirect   C TCP C UDP	IP Address. port Original port	Trans	Iated port:	
Translate A C 11	Address To Static Redirect C TOP C UDP Dynamic	IP Address; port Original port Address Pool:	Trans	Iated port.	ige Pools
Translate A C 小	Address To - Static Redirect ( C TOP C UDP Dynamic Pool ID	IP Address; port Original port Address Pool:	Trans	Iated port.	ige Pools
Translate A C 1	Address To - Static Redirect   C TOP C UDP Dynamic Pool ID N/A	IP Address; port Original port Address Pool: No address po	Trans Trans Same address Address ol defined	Iated port.	ge Pools
Translate A C 1	Address To - Static Redirect   C TCP C UDP Dynamic Pool ID N/A.	IP Address; port Original port Address Pool: No address po	Same address	Iated port.	ge Pools

5. Wählen Sie **Außen > Hinzufügen**, und wählen Sie einen Bereich aus, um einen Adresspool anzugeben.

Interface	Pool ID	IP Address(es)	
utside			Add
			Edit
			Delete

6. Geben Sie Ihren Adressbereich ein, geben Sie eine Pool-ID ein, und klicken Sie auf **OK**.

<ul> <li>Range</li> <li>Port Address Translation (PAT)</li> <li>Port Address Translation (PAT) using the IP address of the interface</li> <li>IP Address: 172.16.1.5 – 172.16.1.10</li> <li>Network Mask (optional): 255.255.255.0</li> </ul>	erface: outside		Pool ID:	1	
<ul> <li>Port Address Translation (PAT)</li> <li>Port Address Translation (PAT) using the IP address of the interface</li> <li>IP Address: 172.16.1.5 – 172.16.1.10</li> <li>Network Mask (optional): 255.255.255.0</li> </ul>	Range				
<ul> <li>Port Address Translation (PAT) using the IP address of the interface</li> <li>IP Address: 172.16.1.5 – 172.16.1.10</li> <li>Network Mask (optional): 255.255.255.0</li> </ul>	Port Address Translation (	PAT)			
IP Address: 172.16.1.5 – 172.16.1.10 Network Mask (optional): 255.255.255.0	Port Address Translation (	PAT) using t	ne IP addres	s of the interfa	ace
IP Address: 172.16.1.5 - 172.16.1.10 Network Mask (optional): 255.255.255.0					
Network Mask (optional): 255.255.255.0	IP Addroce: 172464	E.	— _ r	170 10 1 10	
Network Mask (optional): 255,255,255,0	IF Address. [172.16.1.	.o		172.16.1.10	
	Notwork Mack (optional)	255.2	55:055:0		
	Network Mask (optional)	. 200.2	55.255.U		

- 7. Wählen Sie Konfiguration > Funktionen > NAT > Übersetzungsregeln, um die Übersetzungsregel zu erstellen.
- 8. Wählen Sie **Inside** als Quellschnittstelle aus, und geben Sie die Adressen ein, die Sie NAT hinzufügen möchten.
- 9. Wählen Sie zum Übersetzen der Adresse auf der Schnittstelle die Option **Außen aus**, wählen Sie **Dynamisch**, und wählen Sie den soeben konfigurierten Adresspool aus.
- 10. Klicken Sie auf

OK.

-		teres of the owner of the term				
<ul> <li>Use NAT</li> </ul>	C Use Policy NAT					
Source Host/Net	work					
	Interface:	inside	*			
	IP Address:	10.1.6.0				
	Mask:	255.255.255.0	-			
		Browse				
					NAT Options	
anelato Addroce	on Interface:	able all			-	
ansiale Address	on intenace. Jours	side				
Translate Addre	ss To					
Translate Addre:	ss To		<b>v</b>			
Translate Addre: C · I · Static C Re	ss To IP Address: edirect port		<b>*</b>			
Translate Addres	ss To IP Address: edirect port TCP UDP Original por	t: Tran	slated port.			
Translate Addres Color Static E Re Color Color Color Color Dyna	ss To IP Address: edirect port TOP Original por TOP Original por	t: Tran	slated port	anage Pool	IS	
Translate Addres	ss To IP Address: direct port TCP Original por UDP mic Address Pool:	t Trans 1	elated port	anage Pool	IS	
Translate Addres	ss To IP Address: direct port TOP Original por UDP onic Address Pool: pol ID	t: Trans 1 Address 2 16 1 10	slated port	lanage Pool	S	
Translate Addres	ss To IP Address: edirect port TOP Original por OUDP onic Address Pool: pol ID	t. Trans 1 Address 2 16 1 10	slated port.	anage Pool	IS	
Translate Addres	ss To IP Address: edirect port TCP Original por UDP Original por UDP	t. Trans 1. Trans 1. Address 2.16.1.10	slated port.	anage Pool	IS	
Translate Addres	ss To IP Address: edirect port TCP Original por UDP mic Address Pool: pol ID 1 172 16 1 5-17	t: Trans 1 1 Address 2 16 1 10	slated port	anage Pool	IS	

 Die Übersetzung wird unter Übersetzungsregeln unter Konfiguration > Funktionen > NAT > Übersetzungsregeln angezeigt.

Home Co	or tion	Monitoring	Back Forward	Search Refresh	Save Help		
	Configuration	> NAT > Trans	ilation Rules 동리 유 정 [ 슈 ]	_	_	_	
nterfaces	<b>A</b> 32 A	<b>•</b> •					
6.	□ (Enable	traffic through	the firewall without addres	s translation:			
curity Policy	<ul> <li>Transla</li> </ul>	ation Rules	C Translation Exem	ption Rules			
28	Show Rul	ies for Interface	All Interfaces	<ul> <li>Show All</li> </ul>			
NAT	Rule		Original			Translated	Add
VPN	Туре	Interface	Source Network	Destination Network	Interface	Address	Edit
430	4	inside	<b>C<sup>D</sup> 10.1,6.0/8</b>	🔹 any	outside	172.16.1.5-172.16.1.10	Delete
Routing							
8							
bal Objects							
roperties							
						•	J
	4						
		NAT 📲	Dynamic NAT 🛛 🞝 Sta	atic Policy NAT 🛛 🖓 D	ynamic Policy N	IAT Manage Pools	]

Die Hosts im Inneren können nun auf externe Netzwerke zugreifen. Wenn Hosts von innen eine Verbindung nach außen initiieren, werden sie in eine Adresse aus dem globalen Pool übersetzt. Die Adressen werden aus dem globalen Pool auf Basis des "first-come", "first-translated" zugewiesen und beginnen mit der "low address" im Pool. Wenn beispielsweise Host 10.1.6.25 als erster eine Verbindung mit der Außenseite initiiert, erhält er die Adresse 172.16.1.5. Der nächste Host erhält 172.16.1.6 usw. Dabei handelt es sich nicht um eine statische Übersetzung, und die Übersetzung wird nach einer Inaktivität gemäß dem Befehl **timeout xlate hh:mm:ss** abgebrochen. Wenn mehr interne Hosts vorhanden sind, als Adressen im Pool vorhanden sind, wird die letzte Adresse im Pool für die Port Address Translation (PAT) verwendet.

#### Zulassen des Zugriffs von internen Hosts auf externe Netzwerke mithilfe von PAT

Wenn interne Hosts eine einzige öffentliche Adresse für die Übersetzung freigeben möchten, verwenden Sie PAT. Wenn die **globale** Anweisung eine Adresse angibt, wird diese Adresse vom Port übersetzt. Das PIX ermöglicht die Übersetzung eines Ports pro Schnittstelle und unterstützt bis zu 65.535 aktive Xlate-Objekte in eine globale Adresse. Führen Sie diese Schritte aus, um internen Hosts den Zugriff auf externe Netzwerke mithilfe von PAT zu ermöglichen.

1. Definieren Sie die interne Gruppe, die Sie für PAT einschließen möchten (wenn Sie 0 0 verwenden, wählen Sie alle internen Hosts aus.)

nat (inside) 1 10.1.6.0 255.255.255.0

2. Geben Sie die globale Adresse an, die Sie für PAT verwenden möchten. Dies kann die

Schnittstellenadresse sein.

global (outside) 1 172.16.1.4 netmask 255.255.255.0

- 3. Wählen Sie im ASDM **Configuration > Features > NAT aus,** und deaktivieren Sie **Enable traffic through the firewall Without address translation**.
- 4. Klicken Sie auf Hinzufügen, um die NAT-Regel zu konfigurieren.
- 5. Wählen Sie **Pools verwalten**, um Ihre PAT-Adresse zu konfigurieren.
- 6. Wählen Sie **Outside > Add** und klicken Sie auf **Port Address Translation (PAT)**, um eine einzelne Adresse für PAT zu konfigurieren.
- 7. Geben Sie eine Adresse und eine Pool-ID ein, und klicken Sie auf

nterface:	outside	•	Pool ID:		
C Range					
Port Ad	dress Translation (P	'AT)			
C Port Ad	dress Translation (P	AT) using the	IP address (	of the interface	9
IP Ad	dress: 172.16.1.4	-	] - [_		
	ork Mask (optional):	255.255	.255.0		
Netw					
	ork Mask (optional):	255.255	.255.0		
Netw					

- 8. Wählen Sie **Konfiguration > Funktionen > NAT > Übersetzungsregeln**, um die Übersetzungsregel zu erstellen.
- 9. Wählen Sie als Quellschnittstelle aus, und geben Sie die Adressen ein, die Sie NAT hinzufügen möchten.
- Wählen Sie zum Übersetzen der Adresse auf der Schnittstelle außerhalb aus, wählen Sie Dynamic (Dynamisch), und wählen Sie den soeben konfigurierten Adresspool aus. Klicken Sie auf OK.

• Obertani	C L	Jse Policy NAT		
Source Ho	st/Network –			
		Interface: IP Address:	inside.	
		Masic	255.255.255.0	
			NAT Or	otions
anslate Ad	dress on Inte	erface: outs	ide	
Translate A	Address To -			
Translate A	Address To – Static C Redirect (	IP Address:		
Translate A ران C	Address To – Static Redirect ( C TCP C UDP	IP Address: port Original port	Translated port	
Translate A O 1 I	Address To – Static Redirect ( C TCP C UDP Dynamic	IP Address: port Original port Address Pool:	Translated port.	
Translate A O III	Address To – Static Redirect TCP C UDP Dynamic Pool ID	IP Address: port Original port Address Pool:	Translated port.	
Translate A	Address To – Static Redirect ( C TCP C UDP Dynamic Pool ID	IP Address: port Original port Address Pool: 172.16,1,4	Translated port.	

 Die Übersetzung wird unter Übersetzungsregeln unter Konfiguration > Funktionen > NAT > Übersetzungsregeln angezeigt.

nome (Co	onfiguration	Monitoring	Back Forward S	Search Refresh :	Save Help		<u>مدينا النم</u>
	Configuration。	NAT > Transl	ation Rules	_	_		
erfaces							
Ê,	E Enable tr	ame through t	he firewall without address	translation:			
urity Policy	<ul> <li>Translation</li> </ul>	in Rules	C Translation Exemp	tion Rules			
36	Show Rules	for Interface	All Interfaces	<ul> <li>Show All</li> </ul>			
AT CO	Rule		Original			Translated	Add
VPN	Туре	Interface	Source Network	Destination Network	Interface	Address	Edit
4.20	in:	side	<b>⊈</b> <sup>7</sup> 10.1,6,0/8	🗇 any	outside	172.18.1.4	Dele
Routing							
8							
al Objects							
5							
operties							
							1
	I. Static M	ат "Ш	Demomic NAT 🔿 Ctot	C Policy MAT	unamic Doliev N	AT NAMES TANK	1

Bei der Verwendung von PAT müssen einige Punkte beachtet werden.

- Die von Ihnen für PAT angegebenen IP-Adressen dürfen sich nicht in einem anderen globalen Adresspool befinden.
- PAT funktioniert nicht mit H.323-Anwendungen, Caching-Nameservern und Point-to-Point Tunneling Protocol (PPTP). PAT arbeitet mit Domain Name Service (DNS), FTP und passivem FTP, HTTP, E-Mail, RPC (Remote Procedure Call), Rshell, Telnet, URL-Filterung und Outbound Traceroute zusammen.
- Verwenden Sie PAT nicht, wenn Sie Multimedia-Anwendungen über die Firewall ausführen müssen. Multimedia-Anwendungen können mit Port-Zuordnungen kollidieren, die PAT bereitstellt.
- In der PIX-Softwareversion 4.2(2) funktioniert die PAT-Funktion nicht mit IP-Datenpaketen, die in umgekehrter Reihenfolge eintreffen. PIX Software Version 4.2(3) behebt dieses Problem.
- IP-Adressen im Pool globaler Adressen, die mit dem globalen Befehl angegeben werden, erfordern umgekehrte DNS-Einträge, um sicherzustellen, dass alle externen Netzwerkadressen über den PIX zugänglich sind. Um umgekehrte DNS-Zuordnungen zu erstellen, verwenden Sie einen DNS-Zeiger-Datensatz (PTR) in der Datei für die Zuordnung von Adressen zu Namen für jede globale Adresse. Ohne die PTR-Einträge können an Standorten langsame oder zeitweilige Internetverbindungen auftreten, und FTP-Anfragen fallen konsistent aus.Wenn eine globale IP-Adresse beispielsweise 192.168.1.3 lautet und der Domänenname für die PIX Security Appliance pix.caguana.com lautet, lautet der PTR-Datensatz:

3.1.1.175.in-addr.arpa. IN PTR
pix3.caguana.com
4.1.1.175.in-addr.arpa. IN PTR

#### Einschränken des Zugriffs von internen Hosts auf externe Netzwerke

Wenn für den Quellhost eine gültige Übersetzungsmethode definiert ist und für die Quell-PIX-Schnittstelle keine ACL definiert ist, ist die ausgehende Verbindung standardmäßig zulässig. In einigen Fällen ist es jedoch erforderlich, den ausgehenden Zugriff basierend auf Quelle, Ziel, Protokoll und/oder Port einzuschränken. Konfigurieren Sie dazu eine ACL mit dem Befehl **accesslist**, und wenden Sie sie mit dem Befehl **access-group** auf die PIX-Schnittstelle der Verbindungsquelle an. Sie können PIX 7.0-ACLs sowohl in ein- als auch in ausgehende Richtungen anwenden. Dieses Verfahren ist ein Beispiel, das den ausgehenden HTTP-Zugriff für ein Subnetz zulässt, aber allen anderen Hosts den HTTP-Zugriff auf die Außenseite verweigert, während der gesamte andere IP-Datenverkehr für alle zugelassen wird.

1. Definieren Sie die 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

**Hinweis:** PIX-ACLs unterscheiden sich von ACLs auf Cisco IOS®-Routern, da PIX keine Platzhaltermaske wie Cisco IOS verwendet. In der ACL-Definition wird eine reguläre Subnetzmaske verwendet. Wie auch bei Cisco IOS-Routern verfügt die PIX-ACL am Ende der ACL über eine implizite "Deny all" (Alle verweigern).**Hinweis:** Neue Zugriffslisteneinträge werden am Ende der bestehenden ACEs angefügt. Wenn Sie zuerst einen bestimmten ACE benötigen, können Sie das line-Schlüsselwort in der Zugriffsliste verwenden. Dies ist eine Beispielbefehlsübersicht:

access-list acl\_outbound line 1 extended permit tcp host 10.1.10.225 any

2. Wenden Sie die ACL auf die interne Schnittstelle an.

access-group acl\_outbound in interface inside

- 3. Verwenden Sie ASDM, um den ersten Zugriffslisteneintrag in Schritt 1 so zu konfigurieren, dass HTTP-Datenverkehr von 10.1.6.0/24 zugelassen wird. Wählen Sie **Konfiguration > Funktionen > Sicherheitsrichtlinie > Zugriffsregeln aus**.
- Klicken Sie auf Hinzufügen, geben Sie die Informationen wie in diesem Fenster angezeigt ein, und klicken Sie auf OK.

🖆 Add Access Rule	×
Action	Syslog
Select an action: permit	Default Syslog More Options
Apply to Traffic: incoming to src interface	Time Range Not Applied New
Source Host/Network	Destination Host/Network
IP Address C Name C Group	⑦ IP 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 inside 10.1.6.0/24	source interface outside any affic
Protocol and Service	
C TCP C UDP C ICMP C IP     Source Port     Service = ▼ any     Service Group ▼	Manage Service Groups  Destination Port  Service = vwww  Service Group
Please enter the description below (optional):	
	×
OK Can	icel Help

5. Wenn Sie die drei Zugriffslisteneinträge eingegeben haben, wählen Sie **Konfiguration > Funktion > Sicherheitsrichtlinie > Zugriffsregeln**, um diese Regeln anzuzeigen.



# Zugriff für nicht vertrauenswürdige Hosts auf Hosts in Ihrem vertrauenswürdigen Netzwerk zulassen

Die meisten Unternehmen müssen nicht vertrauenswürdigen Hosts den Zugriff auf Ressourcen in ihrem vertrauenswürdigen Netzwerk ermöglichen. Ein gängiges Beispiel ist ein interner Webserver. Standardmäßig verweigert der PIX Verbindungen von externen Hosts zu internen Hosts. Um diese Verbindung im NAT-Steuerungsmodus zuzulassen, verwenden Sie den **statischen** Befehl mit **Zugriffslisten-** und **Zugriffsgruppen-**Befehlen. Wenn die NAT-Kontrolle deaktiviert ist, sind nur die Befehle **für Zugriffslisten** und **Zugriffsgruppen** erforderlich, wenn keine Übersetzung durchgeführt wird.

Anwenden von ACLs auf Schnittstellen mit einem Befehl **access-group**. Dieser Befehl ordnet die ACL der Schnittstelle zu, um den Datenverkehr zu überprüfen, der in eine bestimmte Richtung fließt.

Im Gegensatz zu den **nat-** und **globalen** Befehlen, die interne Hosts erlauben, erstellt der **statische** Befehl eine bidirektionale Übersetzung, die es internen Hosts außerhalb und externen Hosts erlaubt, die richtigen ACLs/Gruppen hinzuzufügen.

Wenn ein externer Host in den in diesem Dokument gezeigten PAT-Konfigurationsbeispielen versucht, eine Verbindung zur globalen Adresse herzustellen, kann er von Tausenden von internen Hosts verwendet werden. Der **statische** Befehl erstellt eine Eins-zu-Eins-Zuordnung. Der Befehl **access-list** definiert, welcher Verbindungstyp für einen internen Host zulässig ist und wird immer benötigt, wenn ein Host mit niedrigerer Sicherheit eine Verbindung zu einem Host mit höherer Sicherheit herstellt. Der Befehl **access-list** basiert sowohl auf Port als auch auf Protokoll

und kann sehr permissiv oder sehr restriktiv sein, je nachdem, was der Systemadministrator erreichen möchte.

Das <u>Netzwerkdiagramm</u> in diesem Dokument veranschaulicht die Verwendung dieser Befehle, um das PIX so zu konfigurieren, dass alle nicht vertrauenswürdigen Hosts eine Verbindung zum internen Webserver herstellen können und nicht vertrauenswürdigen Host 192.168.1.1 den Zugriff auf einen FTP-Dienst auf demselben Computer ermöglichen.

#### Verwenden von ACLs auf PIX 7.0 und höher

Führen Sie diese Schritte für die PIX-Softwareversion 7.0 und höher durch, und verwenden Sie ACLs.

1. Wenn die NAT-Kontrolle aktiviert ist, definieren Sie eine statische Adressumwandlung für den internen Webserver in eine externe/globale Adresse.

```
static (inside, outside) 172.16.1.16 10.16.1.16
```

2. Legen Sie fest, welche Hosts eine Verbindung zu welchen Ports zu Ihrem Web/FTP-Server herstellen können.

```
access-list 101 permit tcp any host 172.16.1.16 eq www
access-list 101 permit tcp host 192.168.1.1 host 172.16.1.16 eq ftp
```

3. Wenden Sie die ACL auf die externe Schnittstelle an.

access-group 101 in interface outside

- 4. Wählen Sie **Configuration > Features > NAT** und klicken Sie auf **Add**, um diese statische Übersetzung mit ASDM zu erstellen.
- 5. Wählen Sie **als** Ausgangsschnittstelle aus, und geben Sie die interne Adresse ein, für die Sie eine statische Übersetzung erstellen möchten.
- Wählen Sie Statisch, und geben Sie die externe Adresse, in die übersetzt werden soll, in das IP-Adressfeld ein. Klicken Sie auf OK.

OSENAI	ΟU	se Policy NAT				
Source Host/N	letwork -					
		Interface: IP Address: Mask:	inside 10.16.1.16 255.255.255.255	• •		
anslate Addres	s on Inter	rface: outsi	Browse			NAT Options
Translate Addr Sta ان ان Sta	ress To — tic Redirect r	IP Address:	172.16.1.16	¥		
Translate Addr	ess To — tic Redirect p © TCP © UDP	IP Address: Fort Original port	172.16.1.16 Tra	nslated port:		
Translate Addr	ess To — tic Redirect p © TCP © UDP namic	IP Address: Fort Original port Address Poo	172.16.1.16 Tra	nslated port:	Manage Poo	IS
Translate Addr	ess To — tic Redirect p © TCP © UDP namic Pool ID	IP Address: Fort Original port Address Poo	172.16.1.16 Tra Same address Addres	nslated port:	Manage Poo	IS
Translate Addr	tic Redirect p © TCP © UDP namic Pool ID	IP Address: Fort Original port Address Poo	172.16.1.16 Tra same address Addres	nslated port:	Manage Poo	IS

 Die Übersetzung wird in den Übersetzungsregeln angezeigt, wenn Sie Configuration > Features > NAT > Translation Rules auswählen.

File Rules Sear	For PIX - 10.1 rch Options	.1.1 Tools Wizar	ds Help				
Home Co	ogy Infiguration	Monitoring	Back Forward	Q Q Search Refresh	Save Help		Cisco Systems
Hierfaces	Configuration • 2 4 (Enable • Transle Show Ru	<ul> <li>NAT &gt; Trans</li> <li>1 1 1 1 4</li> <li>braffic through ation Rules</li> <li>les for interface</li> </ul>	ation Rules Pa R. R. R. E () the firewall without address C Translation Exemp : All Interfaces	Translation: ofion Rules			
NAT	Rule		Original			Translated	Add
VPN	Туре	Interface	Source Network	Destination Network	Interface	Address	Edit
Routing Global Objects Properties							

8. Verwenden Sie die Prozedur <u>Restrict Inside Hosts Access to Outside Networks (Zugriff auf externe Netzwerke einschränken)</u>, um die **Zugriffslisteneinträge** einzugeben. Hinweis: Seien Sie vorsichtig, wenn Sie diese Befehle implementieren. Wenn Sie die **Zugriffsliste 101 permit ip any** command implementieren, kann jeder Host im nicht vertrauenswürdigen Netzwerk mit IP auf jeden Host im vertrauenswürdigen Netzwerk zugreifen, sofern eine aktive Übersetzung vorliegt.

# Deaktivieren von NAT für bestimmte Hosts/Netzwerke

Wenn Sie die NAT-Kontrolle verwenden und im internen Netzwerk über einige öffentliche Adressen verfügen und diese spezifischen internen Hosts ohne Übersetzung nach außen gehen sollen, können Sie NAT für diese Hosts mit **nat 0**- oder **statischen** Befehlen deaktivieren.

Dies ist ein Beispiel für den Befehl nat:

#### nat (inside) 0 10.1.6.0 255.255.255.0

Führen Sie diese Schritte aus, um NAT für bestimmte Hosts/Netzwerke unter Verwendung von ASDM zu deaktivieren.

- 1. Wählen Sie Konfiguration > Funktionen > NAT aus, und klicken Sie auf Hinzufügen.
- 2. Wählen Sie als Ausgangsschnittstelle aus, und geben Sie die interne Adresse bzw. das interne Netzwerk ein, für die Sie eine statische Übersetzung erstellen möchten.
- 3. Wählen Sie Dynamic (Dynamisch) aus, und wählen Sie die gleiche Adresse für den

# Adresspool aus. Klicken Sie auf **OK**.

Use NA	T OU	se Policy NAT				
-Source H	ost/Network—					
		Interface:	inside		~	
		IP Address:	10.1.6.0		_	
		Mask:	255 255 255	0	<b>T</b>	
			200.200.200			
			Browse			
						NAT Options.
ranslate Ad	dress on Inte	rface: outsid	ie 🔻			
ranslate Ao - Translate	idress on Inter Address To —	rface: outsid	ie 💌			
ranslate Ar Translate ۲ ۲	ldress on Inte Address To — Static	rface: outsid	ie 👤		]	
ranslate Ad Translate ۲۰۱۰	ddress on Inter Address To — Static Redirect p	rface: outsid	e V	<u>*</u>	]	
ranslate Ad Translate (۲۰۱۰	ddress on Inter Address To — Static Redirect p © TCP © UDP	rface: outsid IP Address: ort Original port:		Translated p	] ort	
ranslate Ad Translate ۲۰۱۰	ddress on Inter Address To — Static Redirect p © TCP © UDP Dynamic	rface: outsid IP Address: ort Original port: Address Pool:	ie 💌	Translated p	ort Manage P	Pools
ranslate Ad Translate ۲۰۱۰	ddress on Inter Address To — Static Redirect p © TCP © UDP Dynamic Pool ID	rface: outsid	ie 💌	Translated p ss 💽 ress	] fort:   Manage P	200ls
ranslate Ad Translate O 1	ddress on Inter Address To — Static Redirect p © TCP © UDP Dynamic Dynamic	rface: outsid IP Address: ort Original port: Address Pool: No address pool	de	Translated p ss 💽 ress	ort: Manage P	Pools
ranslate Ad Translate	ddress on Inter Address To — Static Redirect p © TCP © UDP Dynamic Pool ID N/A	rface: outsid IP Address: ort Original port: Address Pool: No address pool	de 💌	Translated p ss 💽 ress	ort Manage P	Pools
Translate A	ddress on Inter Address To	rface: outsid	de	Translated p ss 💽 ress	ort: Manage P	Pools

 Die neue Regel wird in den Übersetzungsregeln angezeigt, wenn Sie Configuration > Features > NAT > Translation Rules auswählen.

readures       Examplement = readures = real rest = reaction Rules         interfaces       Image: Figure interface         interfaces       Image: Figure interface         interfaces       Image: Figure interface         interfaces       Image: Figure interface         interface       Source Network         inside       Image: Figure interface         Image: Figure interface       Image: Figure i	Image: Start Stranslation Rules         affic through the firewall without address translation         on Rules       Translation Exemption Rules         affic through the firewall without address translation         on Rules       Translation Exemption Rules         affic through the firewall without address translation         on Rules       Translation Exemption Rules         affic through the firewall       Show All         Original       Translated         Address       Edit         interface       Source Network       Destination Network       Interface         side       If 101 8 0/24       arry       outside       same as original address         outside       same use original address       Delete	exacting       Image: Construction of the section of the	Iation Rules Show All Translated stination Network Interface Address	Add Edit
Image: Section of the sec	affic through the firewall without address translation on Rules Translation Exemption Rules for Interface: All interfaces Show All Original Translated Add Interface Source Network Destination Network Interface Address Edit Side CF 10.1 8.0/24 any outside same as original address Delete	Enable traffic through the firewall without address tran Translation Rules Translation Exemption Show Rules for Interface: All Interfaces Rule Original Type Interface Source Network Type Inside Source Network To 1 8.0/24	lation Rules Show All Translated stination Network Interface Address	Add
Image: Section Sect	affic through the firewall without address translation on Rules Translation Exemption Rules ifor Interface: All Interfaces Show All Original Translated Address Edit interface Source Network Destination Network Interface Address Edit side EF 10 1 8.0/24 any outside same as original address Delete	Image: Section and the section of	Iation Rules Show All Translated stination Network Interface Address	Add
Image: Second secon	an Rules Translation Exemption Rules sfor Interface: All Interfaces Show All Original Translated Add Interface Source Network Destination Network Interface Address Edit side 2010 1 8 0/24 any outside same as original address Delete Address Version Rules Address Add	Image: Second secon	Rules           Show All         Translated           stination Network         Interface         Address	Add
Show Rules for Interface: All Interfaces     NAT     Rule     Original     Rule     Original     Type     Interface     Source Network     Destination Network     Interface     Address     Show All     Rule     Original     Type     Interface     Source Network     Destination Network     Interface     Address     Inside     Ins	At Att Description MAT Contract Att Contract Con	Autry Policy Show Rules for Interface: All Interfaces Rule Original Type Interface Source Network Du inside cF 10 1 8 0/24	Show All Translated stination Network Interface Address	Add
NAT     Rule     Original     Translated       VPN     Rule     Original     Translated       VPN     Inside     © 10 1 8 0/24     outside       Sing Blocks     Sing Blocks     Sing Blocks     Sing Blocks	Original     Translated     Add       Interface     Source Network     Destination Network     Inlerface     Address     Edit       Side     cF 10.1.8.0/24     Image: arry     Outside     same as uriginal address     Delete	NAT     Rule     Original       What     Rule     Original       Type     Interface     Source Network       What     Inside     Image: Control of the one of the on	Stick Address	Add Edit
NAT     Rule     Original     Translated       VPN     Type     Interface     Source Network     Destination Network     Interface     Address       VPN     Inside     Imside     Imside     Imside     Address       Routing     Imside     Imside     Imside     Imside     Imside       Imside     Imside     Imside     Imside     Imside     Imside       I	Original     Translated     Add       Interface     Source Network     Destination Network     Interface     Address     Edit       side     cF 10.1.8.0/24     any     Outside     same as original address     Delete	NAT     Rule     Original       VPN     Type     Interface     Source Network     Dr       VPN     Inside     EP 10 1 8.0/24     Image: Compare Network     Dr       VPN     Image: Compare Network     Image: Compare Network     Image: Compare Network     Image: Compare Network       VPN     Image: Compare Network     Image: Compare Network     Image: Compare Network     Image: Compare Network       VPN     Image: Compare Network       VPN     Image: Compare Network       VPN     Image: Compare Network     Image: Compare Network     Image: Compare Network     Image: Compare Network       VPN     Image: Compare Network     Image: Compare Network     Image: Compare Network     Image: Compare Network       VPN     Image: Compare Network     Image: Compare Network     Image: Compare Network     Image: Compare Network       VPN     Image: Compare Network     Image: Compare Network     Image: Compare Network     Image: Compare Network       VPN     Image: Compare Network     Image: Compare Network     Image: Compare Network     Image: Compare Network       VPN     Image: Compare Network <td< td=""><td>stination Network Interface Address</td><td>Edit</td></td<>	stination Network Interface Address	Edit
VPN       Type       Interface       Source Network       Destination Network       Interface       Address         VPN       inside       cP1018.0/24       any       outside       same as original address         Routing       inside       cP1018.0/24       any       outside       same as original address         Sing Blocks       inside       cP1018.0/24       any       outside       same as original address         Device       contract       contract       contract       contract       contract       contract	Interface Source Network Destination Network Interface Address Edit Side CF 10.1.8.0/24 • any outside same as original address Delete Address Interface Same as original address Interface Address Interface Same Address Interface Address Interfac	VPv     Type     Interface     Source Network     Du       VPv     inside     cP10.1.6.0/24        Sing Blacks     Source Network     Inside	stination Network Interface Address	Edit
VPN     inside     cP 10.1.8.0/24     any     outside     same as original address       A22	side pF 10 1 6 0/24 Interview outside same as original address Delete	VPN inside pP 10 1 6 0/24	enterida e arma are ariginad addraina	6
Routing arg Blacks Device ministration	AT dll Duramic MAT O Chair Coline MAT A Chair Coline MAT	Routing Sing Blocks Device ministration	Internet internet internet and the second se	Delet
AG Routing Sing Blocks Device Instration	AT dll Dunamic MAT D Chair Coline MAT A Chair Coline MAT	Ag Routing Sing Blocks Crevice Instration		
ing Blocks Bevice Instration	AT dll Paramic MAT A Chefe Police MAT A Deriveric Police MAT	ing Blocks Device unistration		
ang Blocks Device winistration	AT dll Puramic MAT A Object Dalice MAT A Designed Dalice MAT	PB Sing Blocks Device ministration		
So Device ministration	AT dll Paramic MAT A Object Dalice MAT A Deriveric Online MAT	Bevice ministration		
Cevice Instration	AT dll Duramic MAT D Older Online MAT D Duramic Online MAT	Device enistration		
inistration	AT All Demantic MAT Delice MAT Demantic Delice MAT	inistration		
	AT All Demantic MAT D Object MAT D Demantic Delive MAT			
团	AT dll Danamic MAT D Olete Online MAT D Danamic Online MAT Avenue Provid	<b>1</b>		
operties	AT All Demantic MAT A Object Online MAT A Demantic Online MAT	operties		
	AT All Demarkie MAT Children MAT Children Dation Matter Matter Matter State			1
Low we we we have a set of the se	11 11 official and a construction of the forest of the forest of the Manage Pools	🕴 Static NAT 🛛 📲 Dynamic NAT 🖓 Static Po		

5. Wenn Sie ACLs verwenden, die eine präzisere Kontrolle des Datenverkehrs ermöglichen, den Sie nicht übersetzen sollten (basierend auf Quelle/Ziel), verwenden Sie diese Befehle.

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

- 6. Wählen Sie unter ASDM Configuration > Features > NAT > Translation Rules aus.
- 7. Wählen Sie Übersetzungsfreistellungsregeln aus und klicken Sie auf Hinzufügen. In diesem Beispiel wird veranschaulicht, wie der Datenverkehr aus dem Netzwerk 10.1.6.0/24 an einen beliebigen Ort von der Übersetzung ausgenommen wird.

🗲 Edit Address Translation Rule	x
Action Select an action: exempt	
Host/Network Exempted From NAT	When Connecting To
	© IP 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 inside 10.1.6.0/24	source interface outside any pt
Please enter the description below (optional):	
	-
OK Can	icel Help

8. Wählen Sie **Konfiguration > Funktionen > NAT > Übersetzungsfreistellungsregeln**, um die neuen Regeln anzuzeigen.



9. Der statische Befehl für den Webserver ändert sich, wie im folgenden Beispiel gezeigt.

static (inside, outside) 10.16.1.16 10.16.1.16

- 10. Wählen Sie im ASDM Configuration > Features > NAT > Translation Rules aus.
- 11. Wählen Sie Übersetzungsregeln aus, und klicken Sie auf Hinzufügen. Geben Sie die Quelladressinformationen ein, und wählen Sie Statisch aus. Geben Sie dieselbe Adresse in das Feld IP-Adresse ein.

	C Use Policy N/	AT
Source Host/N	etwork	
	Interface:	inside
	IP Address Mask:	255.255.255.255
		Browse
Translate Addr	ess To tic IP Address Redirect port	: 10.16.1.16
Translate Addr	ess To tic IP Address Redirect port © TCP © UDP Original I	port Translated port
Translate Addr	ess To tic IP Address Redirect port C TCP C UDP Original I C UDP	er 10.16.1.16 Pool: Same address Manage Pools
Translate Addr	ess To tic IP Address Redirect port TCP Original I C UDP Original I namic Address P Pool ID	s: 10.16.1.16 port Translated port Pool: same address Manage Pools Address
Translate Addr	ess To tic IP Address Redirect port C TCP C UDP Damic Address P Pool ID	: 10.16.1.16 port Translated port Pool: same address Manage Pools Address

12. Die Übersetzung wird in den Übersetzungsregeln angezeigt, wenn Sie **Configuration > Features > NAT > Translation Rules** auswählen.

	onguration	> NAT > Trans	station Pules	Search Ketresh	save net	p	
3	♣ ½ 平	<b>1</b>	<b>₽ 8 6 6 6 4</b>				_
inces	Enable	traffic through	the firewall without addres	ss translation			
B v Policy	Transl	ation Rules	C Translation Exer	nption Rules			
1,	Show Ru	les for Interfac	R: All Interfaces	Show All			
AT	Bula		Original			Tenneladad	
3	Kule	100-2	original			Translated	
PN	туре	Interface	Source Network	Destination Network	Interface	Address	
8	4.4	Inside	E=10.16.1.16	🦈 any	outside	10.16.1.16	De
ting							
R							
Objects							
2							
erties							
						<u>)</u>	<u> </u>
	4						

13. Wenn Sie ACLs verwenden, verwenden Sie diese Befehle.

access-list 102 permit tcp any host 10.16.1.16 eq www access-group 102 in interface outside

Weitere Informationen zur Konfiguration von ACLs in ASDM finden Sie im Abschnitt <u>Einschränken von Gastgebern für den Zugriff auf externe Netzwerke</u> in diesem Dokument.Beachten Sie den Unterschied zwischen der Verwendung von **nat 0** bei Angabe von Netzwerk/Maske im Gegensatz zu der Verwendung einer ACL, die ein Netzwerk/eine Maske verwendet, die nur die Initiierung von Verbindungen von innen ermöglicht. Die Verwendung von ACLs mit **nat 0** ermöglicht die Initiierung von Verbindungen durch eingehenden oder ausgehenden Datenverkehr. Die PIX-Schnittstellen müssen sich in unterschiedlichen Subnetzen befinden, um Probleme mit der Erreichbarkeit zu vermeiden.

# Port Redirection (Forwarding) mit Statistiken

In PIX 6.0 wurde die Funktion "Port Redirection (Forwarding)" (Weiterleitung) hinzugefügt, um externen Benutzern die Verbindung mit einer bestimmten IP-Adresse bzw. einem bestimmten Port zu ermöglichen und den PIX-Datenverkehr an den entsprechenden internen Server bzw. Port umzuleiten. Der **statische** Befehl wurde geändert. Bei der freigegebenen Adresse kann es sich um eine eindeutige Adresse, eine gemeinsam genutzte PAT-Adresse für ausgehende Anrufe oder um eine mit der externen Schnittstelle gemeinsam genutzte Adresse handeln. Diese Funktion ist in PIX 7.0 verfügbar.

Hinweis: Aufgrund von Platzbeschränkungen werden Befehle in zwei Zeilen angezeigt.

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]]]

**Hinweis:** Wenn die statische NAT die externe IP-Adresse (global\_IP) für die Übersetzung verwendet, kann dies zu einer Übersetzung führen. Verwenden Sie daher in der statischen Übersetzung das Schlüsselwort **interface** anstelle der IP-Adresse.

Diese Portumleitungen (Weiterleitungen) sind in diesem Netzwerkbeispiel enthalten:

- Externe Benutzer leiten Telnet-Anfragen an die eindeutige IP-Adresse 172.18.124.99 weiter, die PIX an 10.1.1.6 umleitet.
- Externe Benutzer leiten FTP-Anfragen an die eindeutige IP-Adresse 172.18.124.99 weiter, die PIX an 10.1.1.3 umleitet.
- Externe Benutzer leiten Telnet-Anfragen an die PAT-Adresse 172.18.124.208 weiter, die PIX an 10.1.1.4 umleitet.
- Externe Benutzer leiten Telnet-Anfragen an PIX außerhalb der IP-Adresse 172.18.124.216 weiter, die PIX an 10.1.1.5 umleitet.
- Externe Benutzer leiten HTTP-Anfragen an PIX außerhalb der IP-Adresse 172.18.124.216 weiter, die PIX an 10.1.1.5 umleitet.
- Externe Benutzer leiten HTTP-Port 8080-Anforderungen an die PAT-Adresse 172.18.124.208 weiter, die PIX an 10.1.1.7-Port 80 umleitet.

In diesem Beispiel wird auch der Zugriff einiger Benutzer von innen nach außen mit ACL 100 blockiert. Dieser Schritt ist optional. Der gesamte ausgehende Datenverkehr ist ohne die vorhandene ACL zulässig.

#### Netzwerkdiagramm - Port Redirection (Forwarding)



Partielle PIX-Konfiguration - Port-Umleitung

Diese Teilkonfiguration veranschaulicht die Verwendung von Static Port Redirection (Weiterleitung). Siehe <u>Netzwerkdiagramm</u> für die <u>Port-Umleitung(Weiterleitung)</u>.

#### Partielle PIX 7.x-Konfiguration - Port Redirection(Forwarding)

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 accesslist 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 accesslist 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 interface Ethernet0 nameif outside security-level 0 ip address 172.18.124.216 255.255.255.0 ! interface Ethernet1 nameif inside security-level 100 ip address 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

**Hinweis:** Wenn PIX/ASA mit dem Befehl **sysopt noproxyarp outside** konfiguriert ist, erlaubt es der Firewall nicht, die Proxys und statische NAT-Übersetzungen in PIX/ASA auszuführen. Um dieses Problem zu beheben, entfernen Sie den Befehl **sysopt noproxyarp outside** in der PIX/ASA-Konfiguration und aktualisieren Sie dann die ARP-Einträge mithilfe von freiem ARP. Dadurch können statische NAT-Einträge einwandfrei funktionieren.

Dieses Verfahren ist ein Beispiel für die Konfiguration der Port Redirection (Forwarding), die externen Benutzern ermöglicht, Telnet-Anfragen an eine eindeutige IP-Adresse 172.18.124.99 weiterzuleiten, die von PIX zu 10.1.1.6 umgeleitet wird.

- 1. Wählen Sie unter ASDM Configuration > Features > NAT > Translation Rules aus.
- 2. Wählen Sie Übersetzungsregeln aus, und klicken Sie auf Hinzufügen.
- 3. Geben Sie als Quellhost/Netzwerk die Informationen für die interne IP-Adresse ein.
- 4. Wählen Sie als Übersetzen der Adresse in die Option **Statisch** aus, geben Sie die externe IP-Adresse ein, und aktivieren Sie **Redirect port**.
- 5. Geben Sie die Informationen für den Port vor und nach der Übersetzung ein (in diesem Beispiel wird Port 23 verwaltet). Klicken Sie auf **OK**.

🔁 Add Address 1	Franslation R	ule						×
Use NAT	r ou	Jse Policy NAT						
Source Ho	st/Network-							-
		Interface:	inside		•			
		IP Address:	10.1.1.6					
		Mask:	255.255.25	5.255	-			
					_			
			Browse					
							NAT Options	1
Translate Ad	dress on inte	erface: outsid	ie 💌	1		_		_
- Translate	Address To							_
@	Static	IP Address:	172.18.124	.99	-			
	Redirect p	port			_			
	C TCP C UDP	Original port:	23	Translated	port: 23			
e 📲	Dynamic	Address Pool:	same add	ress 🔻	Manage F	ools	]	
	Pool ID		Ad	dress				
	1							
	Г					1		
		OK	Can	cel	Help			

Die Übersetzung wird in den Übersetzungsregeln angezeigt, wenn Sie **Configuration > Features > NAT > Translation Rules** auswählen.

ione Co	onfiguration	Monitoring	Back Forward	Q Q Search Retiresh	Save Hel	p	Cisco Sys
atures	Configuration	n - Feiltures - N	IAT - Translation Rules				
	* * *	1 1 %	10.0.9 E				
rfaces	Enable	e traffic through	the firewall without addre	ss translation			
a.	G Transl	ation Bules	C Translation Ever	malion Rules			
ty Policy							
34.	Show Ru	iles for Interface	All Interfaces	Show All			
IAT	Rule		Original			Translated	Add
3	Туре	Interface	Source Network	Destination Network	Interface	Address	Edit
VPN		Inside	A 101.1 5	🔹 any	outside	172.18.124.98	Delet
N.		e	Port: 23/tcp		i ka se	Port 23ftcp	
outing							
2							
ne Blacks							
3							
evice							
nistration							
20							
pernes	1						
	🕂 Statio	NAT I	Dynamic NAT 🛛 🔏 S	tatic Policy NAT 🛛 🔒 C	ynamic Policy	NAT Manage Pool	5
				and the second sec	Plane ad 1		

# Einschränkung der TCP/UDP-Sitzung mithilfe von Static

Wenn Sie die TCP- oder UDP-Sitzungen auf den internen Server in PIX/ASA beschränken möchten, verwenden Sie den **statischen** Befehl.

Gibt die maximale Anzahl gleichzeitiger TCP- und UDP-Verbindungen für das gesamte Subnetz an. Der Standardwert ist 0, d. h. unbegrenzte Verbindungen (Inaktive Verbindungen werden geschlossen, nachdem die Leerlaufzeitüberschreitung durch den Befehl **timeout conn** angegeben wurde.) Diese Option gilt nicht für externe NAT. Die Sicherheits-Appliance verfolgt nur Verbindungen von einer höheren Sicherheitsschnittstelle zu einer niedrigeren Sicherheitsschnittstelle.

Die Beschränkung der Anzahl an embryonalen Verbindungen schützt Sie vor einem DoS-Angriff. Die Sicherheits-Appliance verwendet das embryonale Limit, um TCP Intercept auszulösen, das interne Systeme vor einem DoS-Angriff schützt, der durch Überflutung einer Schnittstelle mit TCP-SYN-Paketen erfolgt. Eine embryonale Verbindung ist eine Verbindungsanforderung, die den erforderlichen Handshake zwischen Quelle und Ziel noch nicht beendet hat. Diese Option gilt nicht für externe NAT. Die TCP-Abhörfunktion gilt nur für Hosts oder Server mit einer höheren Sicherheitsstufe. Wenn Sie den Embryonalgrenzwert für eine externe NAT festlegen, wird der Embryonalgrenzwert ignoriert.

Beispiel:

ASA(config)#static (inside,outside) tcp 10.1.1.1 www 10.2.2.2 www tcp 500 100 !--- The maximum number of simultaneous tcp connections the local IP !--- hosts are to allow is 500, default is 0 which means unlimited !--- connections. Idle connections are closed after the time specified !--- by the **timeout conn** command !--- The maximum number of embryonic connections per host is 100.

#### %PIX-3-201002: Zu viele Verbindungen auf {static|xlate} global\_address! Verbindungen

Dies ist eine verbindungsbezogene Nachricht. Diese Meldung wird protokolliert, wenn die maximale Anzahl von Verbindungen mit der angegebenen statischen Adresse überschritten wurde. Die econns-Variable ist die maximale Anzahl an embryonalen Verbindungen und nconns ist die maximale Anzahl von Verbindungen, die für die statische oder Xlate zulässig ist.

Es wird empfohlen, den Befehl **show static** zu verwenden, um die Beschränkung für Verbindungen mit einer statischen Adresse zu überprüfen. Das Limit ist konfigurierbar.

# %ASA-3-2011: Die Verbindungsgrenze für eingehende Pakete überschreitet 1000/1000 von 10.1.26.51/2393 bis 10.0.86.155/135 für die externe Schnittstelle.

Diese Fehlermeldung beruht auf der Cisco Bug ID <u>CSCsg52106</u> (nur <u>registrierte</u> Kunden) . Weitere Informationen finden Sie in diesem Bug.

### Zeitbasierte Zugriffsliste

Die Erstellung eines Zeitbereichs schränkt den Zugriff auf das Gerät nicht ein. Der Befehl **für die Zeitspanne** definiert nur den Zeitbereich. Nachdem ein Zeitraum definiert wurde, können Sie ihn an Verkehrsregeln oder eine Aktion anhängen.

Verwenden Sie zum Implementieren einer zeitbasierten Zugriffskontrollliste den Befehl **Time Range (Zeitbereich)**, um bestimmte Zeiten für Tag und Woche festzulegen. Verwenden Sie dann den Befehl **mit dem Befehl access-list extended time-range**, um den Zeitbereich an eine ACL zu binden.

Der Zeitraum hängt von der Systemuhr der Sicherheits-Appliance ab. Diese Funktion funktioniert jedoch am besten bei der NTP-Synchronisierung.

Nachdem Sie einen Zeitbereich erstellt und den Konfigurationsmodus für den Zeitbereich eingegeben haben, können Sie Zeitbereichsparameter mit den **absoluten** und **periodischen** Befehlen definieren. Um die Standardeinstellungen für absolute und periodische Schlüsselwörter für **Zeitbereichsbefehle** wiederherzustellen, verwenden Sie den **standardmäßigen** Befehl im Zeitbereichskonfigurationsmodus.

Verwenden Sie zum Implementieren einer zeitbasierten Zugriffskontrollliste den Befehl **Time Range (Zeitbereich)**, um bestimmte Zeiten für Tag und Woche festzulegen. Verwenden Sie dann den Befehl **mit dem Befehl access-list extended**, um den Zeitbereich an eine ACL zu binden. Im nächsten Beispiel wird eine ACL mit dem Namen "Sales" (Vertrieb) an einen Zeitbereich mit der Bezeichnung "New York Minute" gebunden:

In diesem Beispiel wird ein Zeitbereich mit dem Namen "New York Minute" erstellt und in den Zeitbereichskonfigurationsmodus gewechselt:

# Informationen zum Sammeln, wenn Sie ein technisches Support-Ticket öffnen

Wenn Sie weiterhin Hilfe benötigen und ein Ticket beim technischen Support von Cisco eröffnen möchten, geben Sie zur Fehlerbehebung für Ihre PIX Security Appliance diese Informationen an.

- Problembeschreibung und relevante Topologiedetails.
- Die Schritte zur Fehlerbehebung, die Sie vor dem Öffnen des Gehäuses durchgeführt haben.
- Ausgabe über den Befehl show tech-support.
- Ausgabe über den Befehl show log nach dem Ausführen des Befehls logging buffered debugging oder Konsolenerfassung, die das Problem (falls verfügbar) demonstrieren.

Hängen Sie die erfassten Daten im unverzippten Textformat (.txt) an Ihren Fall an. Sie können Informationen zu Ihrem Ticket im <u>TAC Service Request</u> <u>Tool</u> hinzufügen (nur <u>registrierte</u> Kunden). Wenn Sie nicht auf das <u>TAC Service Request Tool</u> zugreifen können (nur <u>registrierte</u> Kunden), können Sie die Informationen in einem E-Mail-Anhang an <u>attach@cisco.com</u> mit Ihrer Fallnummer in der Betreffzeile Ihrer Nachricht senden.

# Zugehörige Informationen

- Support-Seite für PIX Security Appliance
- PIX-Befehlsreferenzen
- Fehlerbehebung und Warnmeldungen mit dem Cisco Adaptive Security Device Manager
   (ASDM)
- Anforderungen für Kommentare (RFCs)
- <u>Technischer Support und Dokumentation Cisco Systems</u>