# PIX/ASA 7.x : Redirection (transfert) de port avec les commandes nat, global, static et access-list

## Contenu

Introduction Conditions préalables **Conditions requises Components Used** Produits connexes Conventions Diagramme du réseau Configuration initiale Autoriser l'accès sortant Autoriser les hôtes internes à accéder aux réseaux externes à l'aide de NAT Autoriser les hôtes internes à accéder aux réseaux externes à l'aide de PAT Restreindre l'accès des hôtes internes aux réseaux externes Autoriser les hôtes non approuvés à accéder à des hôtes sur votre réseau approuvé Utiliser des ACL sur PIX versions 7.0 et ultérieures Désactiver NAT pour des hôtes/réseaux spécifiques Port Redirection(Forwarding) avec des commandes static Diagramme de réseau - Port Redirection(Forwarding) Configuration partielle de PIX - Redirection de port Limiter une session TCP/UDP à l'aide de la commande static Liste d'accès basée sur le temps Informations à rassembler si vous ouvrez un dossier d'assistance technique Informations connexes

## **Introduction**

Afin de maximiser la sécurité quand vous mettez en application le dispositif de sécurité Cisco PIX version 7.0, il est important de comprendre comment les paquets passent entre les interfaces à sécurité plus élevée et les interfaces à sécurité de niveau inférieur quand vous utilisez les commandes nat-control, nat, global, static, access-list et access-group. Ce document explique les différences entre ces commandes et comment configurer Port Redirection(Forwarding) et les fonctionnalités de traduction d'adresses réseau (NAT) externes dans le logiciel PIX version 7.x, avec l'utilisation de l'interface de ligne de commande ou d'Adaptive Security Device Manager (ASDM).

**Remarque :** certaines options d'ASDM 5.2 et versions ultérieures peuvent apparaître différentes des options d'ASDM 5.1. Référez-vous à <u>Document ASDM</u> pour plus d'informations.

## **Conditions préalables**

### **Conditions requises**

Référez-vous à <u>Permettre l'accès HTTPS pour ASDM afin de permettre au périphérique d'être</u> <u>configuré par ASDM.</u>

### **Components Used**

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Logiciel du dispositif de sécurité de la gamme Cisco PIX 500 version 7.0 et ultérieures
- ASDM version 5.x et ultérieures

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.

### **Produits connexes**

Vous pouvez également utiliser cette configuration avec le dispositif de sécurité Cisco ASA version 7.x et ultérieures.

### **Conventions**

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à <u>Conventions relatives aux conseils techniques Cisco.</u>

### Diagramme du réseau



10.0.0.0/8

Les schémas d'adressage d'IP utilisés dans cette configuration ne sont pas légalement routables sur Internet. Ce sont des adresses RFC 1918 qui ont été utilisés dans un environnement de laboratoire.

## **Configuration initiale**

Les noms d'interface sont :

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

**Remarque :** Afin de trouver des informations supplémentaires sur les commandes utilisées dans ce document, utilisez l'<u>Outil de recherche de commandes</u> (clients <u>enregistrés</u> uniquement).

## Autoriser l'accès sortant

L'accès sortant décrit les connexions d'une interface à niveau de sécurité plus élevé à une interface à niveau de sécurité moins élevé. Cela inclut les connexions de l'intérieur vers l'extérieur, de l'intérieur vers des zones démilitarisées (DMZ), et de DMZ vers l'extérieur. Cela peut également inclure des connexions d'une DMZ vers une autre, tant que l'interface de la source de connexion a un niveau de sécurité plus élevé que la destination. Passez en revue la configuration du « niveau de sécurité » sur les interfaces PIX afin de vérifier cela.

L'exemple suivant montre la configuration du niveau de sécurité et du nom d'interface :

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

PIX 7.0 introduit la commande **nat-control**. Vous pouvez employer la commande **nat-control en mode de configuration afin de spécifier si NAT est requis pour les communications extérieures**. Avec le contrôle NAT activé, la configuration des règles NAT est requise afin de permettre le trafic sortant, comme cela est le cas avec les précédentes versions du logiciel PIX. Si le contrôle NAT est désactivé (**no nat-control**), les hôtes internes peuvent communiquer avec les réseaux externes sans configuration d'une règle NAT. Cependant, si vous avez des hôtes internes qui n'ont pas d'adresses publiques, vous devez encore configurer NAT pour ces hôtes.

Afin de configurer le contrôle NAT à l'aide d'ASDM, sélectionnez l'onglet Configuration de la fenêtre Home d'ASDM, et choisissez **NAT dans le menu de fonctionnalités.** 

**Enable traffic through the firewall without translation :** Cette option a été introduite dans PIX version 7.0(1). Quand cette option est activée, aucune commande **nat-control n'est émise dans la configuration.** Cette commande signifie qu'aucune traduction n'est requise pour passer à travers le pare-feu. Cette option est habituellement activée seulement quand les hôtes internes ont des adresses IP publiques ou que la topologie du réseau n'exige pas que les hôtes internes soient traduits en adresse IP.

Si les hôtes internes ont des adresses IP privées, alors cette option doit être désactivée de sorte que les hôtes internes puissent être traduits en adresse IP publique et accéder à Internet.

Eile Bules S	5.1 for PIX - 1	0.1.1.1 ps Tools Witter	de Heln				_[_] ×
Home	Configuratio	n Monitoring	Back Forward	Q Q Search Retresh	Save Help		tisco Systems
Interfaces Security Policy	Configurat Configurat	ion > NAT > Trans F   P   1   1   8 ble traffic through the nstation Rules Rules for Interface	lation Rules Par Co. Co. Co. Co. Ine firewall without addres C Translation Exem All Interfaces	s translation: ption Rules Thow All			
NAT	Rule	3	Original			Translated	Add
VPN	Туре	e Interface	Source Network	Destination Network	Interface	Address	Edil
Routing Global Objects Properties	<b>↓</b> •]• St	atic NAT	Dynamic NAT 🖓 Sta	Itic Policy NAT	Dynamic Policy NA Reset	T Manage Pools	Delete
				<admin> N/</admin>	A (15)	📓 🔂 🔰 🔒 7/11/06 6	02:29 PM UTC

Il y a deux stratégies qui sont requises afin d'autoriser l'accès sortant avec le contrôle NAT. La première est une méthode de traduction. Ce peut être une traduction statique avec l'utilisation de la commande **static, ou une traduction dynamique avec l'utilisation d'une règle nat/global.** Elle n'est pas requise si le contrôle NAT est désactivé et que vos hôtes internes ont des adresses publiques.

L'autre condition pour l'accès sortant (qui s'applique si le contrôle NAT est activé ou désactivé), est si une liste de contrôle d'accès (ACL) est présente. Si une ACL est présente, alors elle doit permettre l'accès de l'hôte source à l'hôte de destination avec l'utilisation du protocole et du port spécifiques. Par défaut, il n'y a aucune restriction d'accès aux connexions sortantes via PIX. Cela signifie que s'il n'y a aucune ACL configurée pour l'interface source, alors par défaut, la connexion sortante est autorisée s'il y a une méthode de traduction configurée.

### Autoriser les hôtes internes à accéder aux réseaux externes à l'aide de NAT

Cette configuration permet à tous les hôtes sur le sous-réseau 10.1.6.0/24 d'accéder à l'extérieur. Afin d'accomplir cela, utilisez les commandes **nat** et global comme l'explique la procédure suivante.

1. Définissez le groupe interne que vous voulez inclure pour NAT.

nat (inside) 1 10.1.6.0 255.255.255.0

2. Spécifiez un pool d'adresses sur l'interface externe dans laquelle les hôtes définis dans l'instruction NAT sont traduits.

global (outside) 1 172.16.1.5-172.16.1.10 netmask 255.255.255.0

 Utilisez ASDM pour créer votre pool d'adresses globales. Choisissez Configuration > Features > NAT et désactivez Enable traffic through the firewall without address translation. Cliquez alors sur Add afin de configurer la règle NAT.

🗯 Cisco ASDM !	5.1 for	PIX - 10.1	.1.1						- 🗆 X
File Rules S	search	Options	Tools Wizard	ds Help					
San Home	Confi	guration	Monitoring	Back I	Forward 1	Contraction Contra	Save Help		and transferrers
Interfaces Security Policy	•	iniguration	NAT > Transl	ation Rules Pa (2), (2), ( he firewall wit C Trans [All Interface	K G	translation) tion Rules			
NAT		Rule			Original			Translated	Add
VPN		Туре	Interface	Source	Network	Destination Network	c Interface	Address	Edit
Routing Global Objects Properties		ৰ বৃ• Static	NAT 📲 [	Dynamic NAT	, <mark>∆</mark> Stat	ic Policy NAT	Dynamic Policy N	AT Manage Pools	Delete
	1.					<admin> I</admin>	NA (15)	😹 🔂 🔰 🔒 7/11/06 (	3:02:29 PM UTC

4. Cliquez sur Manage Pools afin de définir le pool d'adresses NAT.

-					
Source Ho	ost/Network-				
		Interface:	inside.	Ŧ	
		10.011	10160		
		IP Address:	10.1.070		
		Mask	255.255.255.0	Ψ.	
			· · · · · · · · · · · · · · · · · · ·		
			Browse		
					NAT Options
anslate Ad	dress on Inte	erface: outsi	ide 👻		
		and the second se	and the second se		
Tranciato	Addrees To				
Translate /	Address To				
Translate /	Address To Static	IP Address.		¥	
Translate / C ነ	Address To Static	IP Address; port		*	
Translate /	Address To Static Redirect C TCP C UDP	IP Address; port Original port	Trans	alated port:	
Translate C 1	Address To - Static Redirect ( C TCP C UDP Dynamic	IP Address; port Original port Address Pool;	Trans	alated port:	age Pools
Translate / C ····	Address To - Static Redirect ( C TCP C UDP Dynamic Pool ID	IP Address: port Original port Address Pool:	Trans	ated port:	age Pools
Translate /	Address To - Static Redirect   © TCP © UDP Dynamic Pool ID N/A.	IP Address: port Original port Address Pool: No address po	Trans Trans Same address Address ool defined	ated port:	ige Pools
Translate / C · ·	Address To - Static Redirect ( C TCP C UDP Dynamic Dynamic N/A.	IP Address: port Original port Address Pool: No address po	Same address	alated port:	age Pools
Translate /	Address To - Static Redirect ( TCP C UDP Dynamic Pool ID N/A	IP Address: port Original port Address Pool: No address po	Same address Address	lated port:	age Pools

5. Choisissez **Outside > Add**, et choisissent une plage pour spécifier un pool d'adresses.

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

6. Entrez votre plage d'adresses, entrez un ID de pool, et cliquez sur **OK**.

nterface:	outside	. 💌	F	ool ID:	1.		
Range							
C Port Ad	dress Translat	tion (PAT)					
C Port Ad	dress Translat	tion (PAT) ເ	using the II	<sup>o</sup> addres	s of the int	erface	
IP Ad	dress: 172.	.16.1.5	4	- 1	72.16.1.10	)	
IP Ad Netw	dress: 172. ork Mask (opti	.16.1.5 onal):	255.255.2	- [1	72.16.1.10	)	
IP Ad Netw	dress: 172. ork Mask (opti	16.1.5 onal):	255.255.2	- [1 255.0	72.16.1.10	)	

- 7. Choisissez Configuration > Features > NAT > Translation Rules pour créer la règle de traduction.
- 8. Choisissez Inside comme interface source, et entrez les adresses voulues pour NAT.
- 9. Pour Translate Address on Interface, sélectionnez **Outside**, choisissez **Dynamic**, et sélectionnez le pool d'adresses que vous venez de configurer.
- 10. Click

OK.

<ul> <li>USP NW1</li> </ul>	C	se Policy MAT						
O DE MAI		oe r unoy nevi						
Source Host/	Network							
		Interface:	inside.		Ψ.			
		IP Address:	10.1.6.0					
		Mack	D55 255 255	0	-			
		maon.	235.205.200					
			Browse					
							NAT Optio	ns
anslate Addre	ess on Inte	rface: outs	de 💌	]				
Tranciata Adv	trace Te							
Translate Ado	dress To –				_			
Translate Add	<b>fress To</b> — latic	IP Address:		-	<b>-</b>			
Translate Ado C ان Sl	<b>dress To</b> — tatic Redirect p	IP Address; port		•	-			
Translate Add C 1 SI	tress To – tatic Redirect p © TOP © UDP	IP Address: port Original port		Translate	e port			
Translate Add	tatic Redirect p TOP OUDP	IP Address: port Original port		Translate	d port			
Translate Add	tatic Redirect p O TOP O UDP ynamic	IP Address: port Original port Address Pool:	1	Translate	d port	age Pool	s	
Translate Add	tress To – tatic Redirect p © TOP © UDP ynamic Pool ID	IP Address: port Original port Address Pool:	[ [ 1 Ac	Translate Idress	d port	age Pool	s	
Translate Add	tress To – tatic Redirect ( C TCP C UDP ynamic Pool ID	IP Address: port Original port Address Pool: 172 16 1 5-17	[1 A0	Translate tdress	d port. Man	age Pool	S	
Translate Add	tress To – tatic Redirect p © TOP © UDP ynamic Pool ID	IP Address: oort Original port Address Pool: 172 16 1 5-17	[ [ [ 1 A0 2 16 1 10	Translate Idress	d port.	age Pool	S	
Translate Add	tress To – tatic Redirect p © TOP © UDP ynamic Pool ID	IP Address: oort Original port Address Pool: 172 16 1 5-17	1 1 2 16 1 10	Translate Idress	d port.	age Pool	S	
Translate Add	tress To – tatic Redirect ( TOP OUDP ynamic Pool ID	IP Address: port Original port Address Pool: 172 16 1 5-17	1 1 1 2 16 1 10	Translate Translate	d port	age Pool	S	

 La traduction apparaît dans les règles de traduction dans Configuration > Features > NAT > Translation Rules.

	nfiguration	Monitoring	Back Forward	Search Refresh	Save Help		adhaadh
	ontguration 争 全 事	NAT > Trans	nation Rules			_	_
Interfaces	Espable	traffic through	the firewall without address	e tranelation			
<u>6</u> ,	( Tranela	tion Rules	C Translation Even	ntion Rules			
Rear Policy	** Hanola	DON ROLES	< manalauon Exem				
NAT	Show Rul	as for Interface	All Interfaces	Show All			
03	Rule		Original			Translated	Add
VPN	Туре	Interface	Source Network	Destination Network	Interface	Address	Edit
420	1000	inside	<b>5<sup>2</sup> 10.1</b> ,6.0/8	🔹 any	outside	172.16.1.5-172.16.1.10	Delete
Routing							
8							
bal Objects							
roperties							
	100					<u>}</u>	1
	<u> </u>		the second se				

Maintenant les hôtes à l'intérieur peuvent accéder aux réseaux externes. Quand les hôtes de l'intérieur lancent une connexion vers l'extérieur, ils sont traduits en adresse du pool global. Les adresses sont assignées à partir du pool global sur une base du premier arrivé, premier traduit, et commencent avec l'adresse la plus faible du pool. Par exemple, si l'hôte 10.1.6.25 est le premier à lancer une connexion à l'extérieur, il reçoit l'adresse 172.16.1.5. L'hôte suivant reçoit 172.16.1.6, etc. Il ne s'agit pas d'une traduction statique, et la traduction expire après une période d'inactivité définie par la commande **timeout xlate hh:mm:ss**. S'il y a plus d'hôtes internes qu'il n'y a d'adresses dans pool, la dernière adresse du pool est utilisée pour la traduction d'adresses de port (PAT)

### Autoriser les hôtes internes à accéder aux réseaux externes à l'aide de PAT

Si vous voulez que les hôtes internes partagent une seule adresse publique pour la traduction, utilisez PAT. Si l'instruction global spécifie une adresse, cette adresse est une traduction de port. PIX autorise une traduction de port par interface et cette traduction prend en charge jusqu'à 65 535 objets xlate actifs sur l'adresse globale unique. Suivez les étapes suivantes afin de permettre aux hôtes internes d'accéder aux réseaux externes à l'aide de PAT.

1. Définissez le groupe interne que vous voulez inclure pour PAT (quand vous utilisez 0 0, vous sélectionnez tous les hôtes internes).

nat (inside) 1 10.1.6.0 255.255.255.0

2. Spécifiez l'adresse globale que vous voulez utiliser pour PAT. Ce peut être l'adresse de l'interface.

global (outside) 1 172.16.1.4 netmask 255.255.255.0

- 3. Dans ASDM, choisissez Configuration > Features > NAT et désactivez Enable traffic through the firewall without address translation.
- 4. Cliquez sur Add afin de configurer la règle NAT.
- 5. Choisissez Manage Pools afin de configurer votre adresse PAT.
- 6. Choisissez Outside > Add et cliquez sur Port Address Translation (PAT) afin de configurer une seule adresse pour PAT.
- 7. Entrez une adresse, un ID de pool, et cliquez sur

Interface:	outside	•	Pool ID:	1	
C Range					
Port Ad	dress Translatio	n (PAT)			
C Port Ad	dress Translatio	n (PAT) using	the IP addres	s of the interfac	e
IP Ad	dress: 172.16	i.1.4			
Netw	ork Mask (option	al): 255.	255.255.0		

- 8. Choisissez Configuration > Features > NAT > Translation Rules pour créer la règle de traduction.
- 9. Sélectionnez inside comme interface source, et entrez les adresses voulues pour NAT.
- Pour Translate Address on Interface, sélectionnez Outside, choisissez Dynamic, et sélectionnez le pool d'adresses que vous venez de configurer. Click OK.

• Use NAT	r ou	Jse Policy NAT						
Source Ho	st/Network							
		Interface:	inside		7			
		IP Address:	10.1.6.0					
		Mask	255.255.255	0	w.			
			Browse					
							NAT Optic	ns
anslate Ad	dress on Inte	erface: outsi	de 💌	f				
Translate /	Address To –							
Translate /	Address To – Static	IP Address:		-	<u>न</u>			
Translate / C اا ۲	Address To – Static C Redirect	IP Address:		• 	<b>-</b>			
Translate / C اب	Address To - Static Redirect ( C TCP C UDP	IP Address: port Original port		Translated	y j port.	_	]	
Translate / C 11	Address To - Static Redirect ( C TCP C UDP Dynamic	IP Address: port Original port Address Pool:	[ ]	Translated	T port. Mana	age Pools	] 	
Translate / C יוי	Address To - Static Redirect C TCP C UDP Dynamic Pool ID	IP Address: port Original port Address Pool:	[ ] [1 Ad	Translated dress	f port. Mana	age Pools	] 	
Translate / C 1	Address To - Static Redirect C UDP Dynamic Pool ID	IP Address: port Original port Address Pool: 172.16.1.4	[ ] [1 Ad	Translated dress	s port. Mana	age Pools		
Translate / C 1	Address To – Static Redirect ( C TCP C UDP Dynamic Pool ID	IP Address: port Original port Address Pool: 172.16.1.4	[1 Ad	Translated dress	J port Mana	age Pools	] 	
Translate / C 1	Address To – Static Redirect ( C TCP C UDP Dynamic Pool ID	IP Address: port Original port Address Pool: 172.16.1.4	[1 Ad	Translated	y port Mana	age Pools		

 La traduction apparaît dans les règles de traduction dans Configuration > Features > NAT > Translation Rules.

ionie (Ca	onfiguration	Monitoring	Back Forward	Search Refresh 1	Save Help		وتمريا التور
	Configuration =	NAT > Transl	ation Rules		_		
erfaces		<u> </u>					
<u>e</u> ,	E Enable b	raffic through t	he firewall without addres:	s translation:			
rity Policy	Translati	ion Rules	C Translation Exem	ption Rules			
Se l	Show Rule	s for Interface	All Interfaces	<ul> <li>Show All</li> </ul>			
NAT	Rule		Original			Translated	Add
SH VPN	Туре	Interface	Source Network	Destination Network	Interface	Address	Ed
4 <b>≩</b> e	ir ir	iside	<b>₫</b> <sup>7</sup> 10.1,6.0/8	🔹 any	outside	172.16.1.4	Dele
outing				··· ·			
8							
al Objects							
2							
perties							
	4				momia Dollaut	•	1
	I. Otate b	10			WESTERNIC RECIPTION	Managa Doolo	

Il y a certaines choses à considérer quand vous utilisez PAT.

- Les adresses IP que vous spécifiez pour PAT ne peuvent pas être dans un autre pool d'adresses globales.
- PAT ne fonctionne pas avec les applications H.323, la mise en cache de noms de serveurs et le protocole de tunnellisation point à point (PPTP). PAT fonctionne avec Domain Name Service (DNS), FTP et FTP passif, HTTP, la messagerie électronique, l'appel de procédure distante (RPC), rshell, Telnet, le filtrage URL et détermination de route de sortie.
- N'utilisez pas PAT quand vous devez exécuter des applications multimédias à travers le parefeu. Les applications multimédias peuvent être en conflit avec les mappages de port que PAT fournit.
- Dans le logiciel PIX version 4.2(2), la fonctionnalité PAT ne fonctionne pas avec les paquets de données IP qui arrivent en ordre inverse. Le logiciel PIX version 4.2(3) corrige ce problème.
- Les adresses IP dans le pool d'adresses globales spécifié avec la commande global exigent des entrées DNS inversées afin de s'assurer que toutes les adresses réseau externes sont accessibles à travers PIX. Pour créer les mappages DNS inversés, utilisez un enregistrement PTR (Pointer) DNS dans le fichier de mappage d'adresses en noms pour chaque adresse globale. Sans entrées PTR, les sites peuvent subir une connectivité Internet lente ou intermittente, et les requêtes FTP échouent systématiquement.Par exemple, si une adresse IP globale est 192.168.1.3 et le nom de domaine pour le dispositif de sécurité PIX est pix.caguana.com, l'enregistrement PTR est :

pix4.caguana.com & so on.

### Restreindre l'accès des hôtes internes aux réseaux externes

S'il y a une méthode de traduction valide définie pour l'hôte source, et aucune ACL définie pour l'interface PIX source, alors la connexion sortante est autorisée par défaut. Cependant, dans certains cas, il est nécessaire de restreindre l'accès en fonction de la source, de la destination, du protocole et/ou du port. Afin d'accomplir cela, configurez une ACL avec la commande **access-list et appliquez-la à l'interface PIX source de connexion avec la commande access-group.** Vous pouvez appliquer des ACL PIX 7.0 dans des directions entrantes et sortantes. Cette procédure est un exemple qui autorise l'accès HTTP sortant pour un sous-réseau, mais refuse à tous les autres hôtes l'accès HTTP vers l'extérieur, tout en permettant tout autre trafic IP pour chacun.

1. Définissez l'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
```

**Remarque :** les listes de contrôle d'accès PIX diffèrent des listes de contrôle d'accès sur les routeurs Cisco IOS® en ce sens que PIX n'utilise pas de masque générique comme Cisco IOS. Il utilise un masque de sous-réseau normal dans la définition de l'ACL. Comme avec les routeurs Cisco IOS, l'ACL PIX a un « refuser tout » implicite la fin de l'ACL. **Remarque :** les nouvelles entrées de liste d'accès seront ajoutées à la fin des ACE existantes. Si vous avez besoin d'un ACE spécifique traité en premier, vous pouvez utiliser le mot clé line dans la liste d'accès. Voici un exemple de résumé des commandes :

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

2. Appliquez l'ACL à l'interface interne.

```
access-group acl_outbound in interface inside
```

- Employez ASDM afin de configurer la première entrée de la liste d'accès à l'étape 1 pour permettre le trafic HTTP en provenance de 10.1.6.0/24. Choisissez Configuration > Features > Security Policy > Access Rules.
- 4. Cliquez sur **Add**, entrez les informations lorsque cette fenêtre s'affiche, puis cliquez sur **OK**.

🖆 Add Access Rule	×
Action	Syslog
Select an action: permit	Default Syslog More Options
Apply to Traffic: incoming to src interface ▼	Time Range New
Source Host/Network	Destination Host/Network
	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 applied to traffic incoming to Inside 10.1.6.0/24	outside any
Protocol and Service	
C TCP C UDP C ICMP C IP     Source Port     Service = ▼ any     C Service Group ▼	Manage Service Groups  Destination Port  Service =  Www  Service Group
Please enter the description below (optional):	
	×
OK Can	cel Help

5. Une fois que vous avez entré les trois entrées de la liste d'accès, choisissez Configuration > Feature > Security Policy > Access Rules afin d'afficher ces règles.



## Autoriser les hôtes non approuvés à accéder à des hôtes sur votre réseau approuvé

La plupart des organisations doivent permettre aux hôtes non approuvés d'accéder aux ressources de leur réseau approuvé. Un exemple courant est un serveur Web interne. Par défaut, PIX refuse les connexions d'hôtes externes vers des hôtes internes. Afin de permettre cette connexion en mode de contrôle NAT, utilisez la commande static, avec les commandes access-list et access-group. Si le contrôle NAT est désactivé, seules les commandes access-list et access-group sont requises, si aucune traduction n'est exécutée.

Appliquez des ACL aux interfaces avec une commande **access-group.** Cette commande associe l'ACL à l'interface pour examiner le trafic qui passe dans une direction particulière.

Contrairement aux commandes **nat** et global qui autorisent les hôtes internes vers l'extérieur, la commande **static crée une traduction bidirectionnelle qui autorisent les hôtes internes vers l'extérieur et les hôtes externes vers l'intérieur si vous ajoutez les ACL/groupes appropriés.** 

Dans les exemples de configuration PAT montrés dans ce document, si un hôte externe essaie de se connecter à l'adresse globale, il peut être utilisé par des centaines d'hôtes internes. La commande static crée un mappage un-à-un. La commande access-list définit quel type de connexion est permis à un hôte interne et est toujours requise quand un hôte à niveau de sécurité inférieur se connecte à un hôte à niveau de sécurité plus élevée. La commande access-list est basé à la fois sur le port et sur le protocole, et peut être très laxiste ou très restrictive, en fonction de ce que l'administrateur système veut réaliser.

Le diagramme de réseau dans ce document montre l'utilisation de ces commandes afin de configurer PIX pour permettre à tout hôte non approuvé pour se connecter au serveur Web interne, et permet à l'hôte non approuvé 192.168.1.1 d'accéder à un service FTP sur la même machine.

### Utiliser des ACL sur PIX versions 7.0 et ultérieures

Complétez les étapes suivantes pour le logiciel PIX versions 7.0 et ultérieures avec l'utilisation d'ACL.

1. Si le contrôle NAT est activé, définissez une traduction d'adresse statique pour le serveur Web interne en adresse externe/globale.

static (inside, outside) 172.16.1.16 10.16.1.16

2. Définissez quels hôtes peuvent se connecter sur quels ports à votre serveur Web/FTP.

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. Appliquez l'ACL à l'interface externe.

access-group 101 in interface outside

- 4. Choisissez Configuration > Features > NAT et cliquez sur Add pour créer cette traduction statique à l'aide d'ASDM.
- 5. Sélectionnez inside comme interface source, et entrez l'adresse interne pour laquelle vous voulez créer une traduction statique.
- Choisissez Static et entrez l'adresse externe que vous voulez traduire dans le champ d'adresse IP. Click OK.

Source Host/N	Vetwork-					
			-	_		
		Interface:	inside	-		
		IP Address:	10.16.1.16			
		Mask:	255 255 255 255	-		
			Browse			
						NAT Options
onoloto Addro	co on Into	rfaco: laitei	-			
ansiale annre	SS HELIND	nace initer	de 💌			
	00 0111110	Todisi				
Translate Add	Iress To –	Todisi				
Translate Add	Iress To — atic	IP Address:	172.16.1.16	-		
Translate Add • • • Sta	Iress To — atic Redirect p	IP Address:	172.16.1.16	<u> </u>		
Translate Add	Iress To – atic Redirect p	IP Address:	172.16.1.16	<u> </u>		
Translate Add	Iress To – atic Redirectp O UDP	IP Address: port Original port	172.16.1.16 Transl	ated port:		
Translate Add	Iress To – atic Redirect p © TCP © UDP mamic	IP Address: port Original port	172.16.1.16 Transl	ated port:	inage Pools.	
Translate Add	Iress To – atic Redirect p © TCP © UDP mamic	IP Address: port Original port Address Poo	172.16.1.16 Transl	ated port:	inage Pools.	
Translate Add	Iress To – atic Redirect p O UDP mamic Pool ID	IP Address: port Original port Address Poo	172.16.1.16 Transl	ated port.	inage Pools.	
Translate Add	Iress To – atic Redirect p C UDP mamic Pool ID	IP Address: port Original port Address Poo	172.16.1.16 Transi	ated port:	inage Pools.	
Translate Add	Iress To – atic Redirect p O UDP mamic Pool ID	IP Address: bort Original port Address Poo	172.16.1.16 Transl	ated port:	inage Pools.	
Translate Add	Iress To atic Redirect p C UDP mamic Pool ID	IP Address: port Original port Address Poo	172.16.1.16 Transl	ated port:	inage Pools.	

 La traduction apparaît dans les règles de traduction quand vous choisissez Configuration > Features > NAT > Translation Rules.

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. Utilisez la procédure <u>Restreindre l'accès des hôtes internes aux réseaux externes afin</u> <u>d'entrer les entrées</u> access-list.Remarque : Soyez prudent lorsque vous mettez en œuvre ces commandes. Si vous mettez en œuvre la commande access-list 101 permit ip any any, tout hôte sur le réseau non approuvé peut accéder à tout hôte sur le réseau approuvé à l'aide de l'IP tant qu'il y a une traduction active.

## Désactiver NAT pour des hôtes/réseaux spécifiques

Si vous utilisez le contrôle NAT, que vous avez des adresses public sur le réseau interne et que vous voulez que ces hôtes internes spécifiques sortent à l'extérieur sans translation, vous pouvez désactiver NAT pour ces hôtes, avec les commandes **nat 0 ou static**.

Voici un exemple de la commande nat :

nat (inside) 0 10.1.6.0 255.255.255.0

Suivez les étapes suivantes afin de désactiver NAT pour des hôtes/réseaux spécifiques à l'aide d'ASDM.

- 1. Choisissez Configuration > Features > NAT et cliquez sur Add.
- 2. Choisissez inside comme interface source, et entrez l'adresse/le réseau interne pour lequel vous voulez créer une traduction statique.
- 3. Choisissez **Dynamic et sélectionnez la même adresse pour le pool d'adresses.** Click OK.

🔂 Edit Address 1	Franslation Ru	ıle					X
🖲 Use NAT	r ou	se Policy NAT					
- Source Ho	st/Network-						
		Interface:	inside	Ψ.			
		IP Address:	10.1.6.0				
		Maek:					
		maon.	255.255.255.0	<u> </u>			
			Browse				
						NAT Options	
Translate Ad	dress on Inter	rface: outsid	le 💌		_		1
—Translate /	Address To —	,					
C ala	Static	IP åddress:		<b>x</b>			
	Redirect p	ort	1				
	C TOP				_		
	O UDP	Original port:	Trans	slated port			
e 📲	Dynamic	Address Pool:	same address	Manage	Pools	1	
	Pool ID		Address		_		
	NIA	No address poo	)i defined				
	1						
		OF	Cancal	Help	1		
	_	UK		Help			

 La nouvelle règle apparaît dans les règles de traduction quand vous choisissez Configuration > Features > NAT > Translation Rules.

Home C	configuration	Monitoring	Back Forward	Search Refresh	Save Helt	)	million
eatures	Configuration	≥ Features > N	NAT > Translation Rules				
terfaces	● 😤 爭   □ Enable ○ Transla	raffic through stion Rules	the firewall without addres	ss translation nption Rules			
24	Show Rul	les for Interface	8: All interfaces	Show All		Translated	Add
G	Туре	Interface	Source Network	Destination Network	Interface	Address	Edit
A ADMI			And a second	and the second se			A la serie de serie
423		insidė	<u></u> ⊈ <sup>I</sup> 1018.0/24	🧆 ary	outside	same as original address	Delet
Routing oring Blacks Device ministration Device ministration		inside	g≓1018.024	M arre	outside	same as original addres:	Deleti
Routing Routing Blacks Device sinistration		insida	g≓ 10 1 8.0/24		outside	same as original addres	Deleti

5. Si vous utilisez des ACL, ce qui permet un contrôle plus précis du trafic que vous ne devez pas traduire (basé sur la source/destination), utilisez les commandes suivantes.

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

- 6. Utilisez ASDM et choisissez Configuration > Features > NAT > Translation Rules.
- 7. Choisissez **Translation Exemption Rules et cliquez sur Add**.Cet exemple montre comment exempter le trafic du réseau 10.1.6.0/24 vers n'importe où d'être traduit.

🗲 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
Please enter the description below (optional):	
	×
OK Can	Icel Help

 Choisissez Configuration > Features > NAT > Translation Exemption Rules afin d'afficher les nouvelles règles.



9. La commande static pour le serveur Web change comme le montre l'exemple suivant.

static (inside, outside) 10.16.1.16 10.16.1.16

- 10. Dans ASDM, choisissez Configuration > Features > NAT > Translation Rules.
- Sélectionnez Translation Rules et cliquez sur Add. Entrez les informations de l'adresse source, et sélectionnez Static. Entrez la même adresse dans le champ IP Address.

		se Policy NAT			
Source Host	Network				
		Interface:	inside		
		IP Address:	10.16.1.16		
		Mask:	255.255.255.255	-	
			Browse		
					NAT Options.
anslate Addr	ess on Inter	face: outsi	de 💌		
			and the second s		
Translate Ad	ldress To —	2			
Translate Ad	ldress To — Static	IP Address:	10.16.1.16	Ŧ	
Translate Ad • • • s	ldress To — Static T Redirect p	IP Address:	10,16.1.16	<b>*</b>	
Translate Ad • • • • 8	Idress To Static Redirect p © TCP © UDP	IP Address: ort Original port	10,16.1.16 Transla	ted port	-
Translate Ad	Idress To Static Redirect p © TCP © UDP Dynamic	IP Address: ort Original port Address Pool:	10.16.1.16 Transla	ted port.	ols
Translate Ad	Idress To Static Redirect p C UDP Oynamic Pool ID	IP Address: ort Original port Address Pool	10.16.1.16 Transia same address 💽 Address	ted port Manage Po	ols
Translate Ad	Idress To Static Redirect p C UDP Oynamic Pool ID	IP Address: ort Original port Address Pool	10.16.1.16 Transla same address 💽 Address	ted port.	ols
Translate Ad	Idress To Static Redirect p C UDP Oynamic Pool ID	IP Address: ort Original port Address Pool:	10.16.1.16 Transla same address	ted port Manage Po	pols
Translate Ad	Idress To Static TRedirect p C UDP Oynamic Pool ID	IP Address: ort Original port Address Pool:	10.16.1.16 Transla same address 💽 Address	ted port	pols

 La traduction apparaît dans les règles de traduction quand vous choisissez Configuration > Features > NAT > Translation Rules.

	Configuration	≥ NAT > Trans	lation Rules				
erfaces	* 2 P	3 1 1	₩ EL 10 EL 🗳				
<b>G</b>	☐ Enable	raffic through	the firewall without addres	s translation			
rity Policy	Transla	tion Rules	C Translation Exem	nption Rules			
25	Show Rule	s for Interface	all Interfaces	▼ Show All			
NAT	Rule		Original			Translated	Add
VPN	Туре	Interface	Source Network	Destination Network	Interface	Address	Edi
1.0	1	nside	<b>£</b> <sup>2</sup> 10.16.1.16	🧇 any	outside	10.16.1.16	Dele
touting							
8							
el Objects							
Total and Total							
20							
operties							
operties							
operties							

13. Si vous utilisez des ACL, utilisez ces commandes.

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

Consultez la section <u>Restreindre l'accès des hôtes internes aux réseaux externes de ce</u> <u>document pour des informations supplémentaires sur la configuration des ACL dans</u> <u>ASDM.</u>Notez la différence quand vous utilisez **nat 0** quand vous spécifiez un réseau/masque par rapport à quand vous utilisez une ACL qui utilise un réseau/masque qui permet le déclenchement de connexions à partir de l'intérieur seulement. L'utilisation d'ACL avec **nat 0 permet déclenchement de connexions par le trafic entrant ou sortant.** Les interfaces PIX doivent être dans différents sous-réseaux afin d'éviter des problèmes d'accessibilité.

## Port Redirection(Forwarding) avec des commandes static

Dans PIX 6.0, la fonctionnalité Port Redirection(Forwarding) a été ajoutée afin de permettre à des utilisateurs externes de se connecter à une adresse IP/un port particulier et que PIX redirige le trafic vers le serveur interne/port approprié. La commande **static a été modifiée.** L'adresse partagée peut être une adresse unique, une adresse PAT sortante partagée, ou partagé avec l'interface externe. Cette fonctionnalité est disponible dans PIX 7.0.

Remarque : en raison des limites d'espace, les commandes sont affichées sur deux lignes.

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]]]

**Remarque :** si la NAT statique utilise l'adresse IP externe (global\_IP) pour la traduction, cela peut entraîner une traduction. Par conséquent, utilisez le mot clé **interface au lieu de l'adresse IP dans la traduction statique.** 

Ces transferts Port Redirections(Forwarding) sont en cet exemple de réseau :

- Les utilisateurs externes dirigent les demandes Telnet vers l'adresse IP unique 172.18.124.99, que PIX redirige vers 10.1.1.6.
- Les utilisateurs externes dirigent les demandes FTP vers l'adresse IP unique 172.18.124.99, que PIX redirige vers 10.1.1.3.
- Les utilisateurs externes dirigent les demandes Telnet vers l'adresse PAT 172.18.124.208, que PIX redirige vers 10.1.1.4.
- Les utilisateurs externes dirigent la demande Telnet vers l'adresse IP externe PIX 172.18.124.216, que PIX redirige vers 10.1.1.5.
- Les utilisateurs externes dirigent la demande HTTP vers l'adresse IP externe PIX 172.18.124.216, que PIX redirige vers 10.1.1.5.
- Les utilisateurs externes dirigent les demandes de port 8080 HTTP vers l'adresse PAT 172.18.124.208, que PIX redirige vers le port 80 10.1.1.7.

Cet exemple bloque également l'accès de certains utilisateurs de l'intérieur vers l'extérieur avec l'ACL 100. This step is optional. Tout le trafic sortant est permis sans l'ACL en place.



### Diagramme de réseau - Port Redirection(Forwarding)

### Configuration partielle de PIX - Redirection de port

Cette configuration partielle illustre l'utilisation de port de Static Port Redirection(Forwarding). Consultez le <u>diagramme de réseau de Port Redirection(Forwarding)</u>.

#### Configuration partielle de PIX 7.x - 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 access-
list 100 deny tcp any any eq www access-list 100 permit
tcp 10.0.0.0 255.0.0.0 any access-list 100 permit udp
10.0.0.0 255.0.0.0 host 172.18.124.100 eq domain access-
list 101 permit tcp any host 172.18.124.99 eq telnet
access-list 101 permit tcp any host 172.18.124.99 eq ftp
access-list 101 permit tcp any host 172.18.124.208 eq
telnet access-list 101 permit tcp any host
172.18.124.216 eq telnet access-list 101 permit tcp any
host 172.18.124.216 eq www access-list 101 permit tcp
any host 172.18.124.208 eq 8080 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
```

**Remarque :** si PIX/ASA est configuré avec la commande **sysopt noproxyarp outside**, alors il ne permet pas au pare-feu d'effectuer les traductions proxyarp et NAT statiques dans PIX/ASA. Afin de résoudre cela, supprimez la commande **sysopt noproxyarp outside dans la configuration PIX/ASA, puis mettez à jour les entrées ARP à l'aide de l'ARP gratuit.** Cela permet à des entrées NAT statiques de fonctionner correctement.

Cette procédure est un exemple de la façon de configurer le Port Redirection(Forwarding) qui permet à des utilisateurs externes de diriger des demandes Telnet à l'adresse IP unique 172.18.124.99, que PIX redirige vers 10.1.1.6.

- 1. Utilisez ASDM et choisissez Configuration > Features > NAT > Translation Rules.
- 2. Sélectionnez Translation Rules et cliquez sur Add.
- 3. Pour Source Host/Network, entrez les informations pour l'adresse IP interne.
- 4. Pour Translate Address To, sélectionnez **Static**, entrez l'adresse IP externe et activez **Redirect port**.
- 5. Entrez les informations de pré-traduction et de post-traduction (cet exemple maintient le port 23). Click OK.

Add Address Transla	tion Rule			
Use NAT	C Use Policy NAT			
Source Host/Netw	vork			
			_	
	Interface:	inside	]	
	IP Address:	10.1.1.6		
	Mask:	255.255.255.255	]	
		- Deserver - 1		
		Browse		
				NAT Options
Translate Address o	on interface: outsid	ie 💌		
Translate Addres	s To			
• • Static	IP Address:	172.18.124.99		
Rec	direct port			
	TCP Original port	23 Translated por	23	
C 👭 Dynan	nic Address Pool:	same address 💌	Manage Pools	3
Poo	DIID	Address		
			1	
	OK	Cancel	Help	

La traduction apparaît dans les règles de traduction quand vous choisissez **Configuration > Features > NAT > Translation Rules**.

р не с	Sonfiguration	Montoring	Back Forward	Q Q Search Retiresh	Save Hel	) 0	CISCO SY
bures	Configuration	- Feidures - N	AT = Translation Rules				
	* * *	0 1 %	0. L. S. E. S.				
-a faces	Enable	s traffic through t	he firewall without addre	ss translation			
3.	@ Transl	ation Rules	C Translation Ever	motion Rules			
ty Policy							
1.	Show Ru	ies for interface:	All Interfaces	Show All			
AT	Rulé		Original			Translated	Ad
2	Туре	Interface	Source Network	Destination Network	Interface	Address	Ed
APAN	4.	inside	🛋 10.1.1.6	🛸 any	outside	172.18.124.99	Dele
Ž5		- ÷1	Port: 23/tcp	- ( · · · · · · · · · · · · · · · · · ·		Port 23ftcp	
uting							
<b>R</b> 3							
g Blocks							
30 evice							
istration							
2							
An Des							1
	· Static	NAT 📲 C	)ynamic NAT 🛛 🖓 S	tatic Policy NAT 🛛 🔒 O	ynamic Policy	NAT Manage Pool	is
				Apply	Reset		
						<b>_</b> .,	

## Limiter une session TCP/UDP à l'aide de la commande static

Si vous voulez limiter les sessions TCP ou UDP au serveur interne placé dans PIX/ASA, alors utilisez la commande **static.** 

Spécifiez le nombre maximal de connexions TCP et UDP simultanées pour tout le sous-réseau. La valeur par défaut est 0, ce qui signifie les connexions illimitées. (Les connexions inactives sont fermées après le délai d'inactivité spécifié par la commande **timeout conn.**) Cette option ne s'applique pas à la NAT externe. Le dispositif de sécurité suit seulement les connexions d'une interface à niveau de sécurité plus élevé vers une interface à niveau de sécurité inférieur.

La limitation du nombre de connexions embryonnaires vous protège d'une attaque DoS. Le dispositif de sécurité emploie la limite embryonnaire pour déclencher l'interception TCP, ce qui protège les systèmes internes d'une attaque DoS commise par l'inondation d'une interface avec des paquets SYN TCP. Une connexion embryonnaire est une demande de connexion qui n'a pas terminé l'établissement de liaison entre la source et la destination. Cette option ne s'applique pas à la NAT externe. La fonctionnalité d'interception TCP s'applique seulement aux hôtes ou serveurs sur un niveau de sécurité supérieur. Si vous définissez la limite embryonnaire pour la NAT externe, la limite embryonnaire est ignorée.

Exemple :

**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 : Trop de connexions sur {static|xlate} global\_address ! econns nconns

C'est un message lié à la connexion. Ce message est enregistré quand le nombre maximal de connexions à l'adresse statique spécifiée a été dépassé. La variable econns est le nombre maximal de connexions embryonnaires et nconns est le nombre maximal de connexions autorisé pour static ou xlate.

L'action recommandée est d'utiliser la commande **show static afin de contrôler la limite imposée sur les connexions à une adresse statique.** La limite est configurable.

## %ASA-3-201011 : La limite de connexion a dépassé 1000/1000 pour le paquet entrant de 10.1.26.51/2393 à 10.0.86.155/135 sur l'interface Outside

Ce message d'erreur est dû au bogue Cisco ID <u>CSCsg52106</u> (clients <u>enregistrés</u> uniquement). Référez-vous à ce bogue pour plus d'informations.

## Liste d'accès basée sur le temps

La création d'un intervalle de temps ne restreint pas l'accès au périphérique. La commande **timerange définit seulement l'intervalle de temps.** Une fois l'intervalle de temps défini, vous pouvez l'attacher aux règles de trafic ou à une action.

Afin de mettre en œuvre une ACL basée sur le temps, employez la commande **time-range pour définir des moments spécifiques du jour et de la semaine.** Utilisez ensuite la commande **with the access-list extended time-range pour lier l'intervalle de temps à une ACL**.

L'intervalle de temps repose sur l'horloge système du dispositif de sécurité. Cependant, la fonctionnalité fonctionne de façon optimale avec la synchronisation NTP.

Après avoir créé un intervalle de temps et être passé en mode de configuration de l'intervalle de temps, vous pouvez définir les paramètres de l'intervalle de temps avec les commandes **absolute et periodic.** Pour restaurer les paramètres par défaut pour les mots clés absolute et periodic de la commande **time-range, utilisez la default en mode de configuration de l'intervalle de temps.** 

Afin de mettre en œuvre une ACL basée sur le temps, employez la commande **time-range pour définir des moments spécifiques du jour et de la semaine.** Utilisez ensuite la commande **with the access-list extended pour lier l'intervalle de temps à une ACL.** L'exemple suivant lie une ACL nommée « Sales » à un intervalle de temps nommé « New York Minute » :

Cet exemple crée un intervalle de temps nommé « New York Minute » et passe en mode de configuration de l'intervalle de temps :

## Informations à rassembler si vous ouvrez un dossier d'assistance technique

Si vous avez encore besoin d'aide et que vous voulez ouvrir un dossier avec l'assistance technique Cisco, assurez-vous d'inclure les informations suivantes pour le dépannage de votre dispositif de sécurité PIX.

- Description du problème et des détails de topologie pertinents
- Les étapes que vous avez suivies pour le dépannage avant d'ouvrir le dossier.
- La sortie de la commande show tech-support.
- La sortie de la commande show log après avoir exécuté la commande logging buffered debugging, ou des captures de la console qui expliquent le problème (si disponibles).

Attachez les données rassemblées à votre dossier dans un format de texte brut (.txt) non compressé. Vous pouvez attacher les informations à votre dossier dans l'<u>Outil de demande de service TAC</u> (clients enregistrés seulement). Si vous ne pouvez pas accéder à l'<u>Outil de demande de service TAC</u> (client enregistrés seulement), vous pouvez envoyer les informations dans une pièce jointe de courrier électronique à attach@cisco.com avec votre numéro de dossier dans la ligne d'objet de votre message.

## Informations connexes

- Page d'assistance pour les dispositifs de sécurité PIX
- <u>Références des commandes du pare-feu PIX</u>
- Dépannage et alertes de Cisco Adaptive Security Device Manager (ASDM)
- Demandes de commentaires (RFC)
- Support et documentation techniques Cisco Systems