PIX/ASA 7.x :使用nat、global、static和accesslist命令的埠重定向(轉發)

目錄

簡介 必要條件 需求 採用元件 相關產品 慣例 網路圖表 初始配置 允許出站訪問 允許內部主機通過NAT訪問外部網路 允許內部主機使用PAT訪問外部網路 限制內部主機訪問外部網路 <u>允許不受信任的主機訪問受信任網路中的主機</u> 在PIX 7.0及更高版本上使用ACL 禁用特定主機/網路的NAT 連線埠重新導向(轉送)(含靜態) 網路圖表 — 連線埠重新導向(轉送) 部分PIX配置 — 埠重定向 使用靜態限制TCP/UDP會話 時間型存取清單 開啟技術支援案例時要收集的資訊 相關資訊

<u>簡介</u>

為了在實施Cisco PIX安全裝置7.0版時最大限度地提高安全性,在使用nat-control 、 nat 、 global 、 static 、 access-list和access-group命令時,瞭解資料包如何在較高安全介面和較低安全介面之 間傳遞非常重要。本檔案將說明這些命令之間的差異,以及如何使用指令行介面或調適型安全裝置 管理員(ASDM)在PIX軟體版本7.x中設定連線埠重新導向(轉送)和外部網路位址轉譯(NAT)功能。

注意:ASDM 5.2及更高版本中的某些選項可能會與ASDM 5.1中的選項不同。有關詳細資訊,請參 閱ASDM文檔。

<u>必要條件</u>

請參閱<u>允許ASDM進行HTTPS訪問</u>,以允許由ASDM配置裝置。

採用元件

本文中的資訊係根據以下軟體和硬體版本:

• Cisco PIX 500系列安全裝置軟體版本7.0及更高版本

• ASDM 5.x及更高版本

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路正在作用,請確保您已瞭解任何指令可能造成的影響。

相關產品

您還可以將此配置與Cisco ASA安全裝置7.x版及更高版本配合使用。

<u>慣例</u>

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

網路圖表



此配置中使用的IP編址方案在Internet上不能合法路由。這些地址是在實驗室環境中使用的RFC 1918地址。



介面名稱為:

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

注意:若要查詢有關本文檔中使用的命令的其他資訊,請使用<u>命令查詢工具(</u>僅限<u>註冊</u>客戶)。

<u> 允許出站訪問</u>

出站訪問描述從較高安全級別介面到較低安全級別介面的連線。這包括從內部到外部、從內部到非 軍事區(DMZ)以及從非軍事區到外部的連線。只要連線源介面的安全級別高於目標介面,這還可以 包括從一個DMZ到另一個DMZ的連線。檢查PIX介面上的「安全級別」配置以確認這一點。

此示例顯示安全級別和介面名稱配置:

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

PIX 7.0引入了**nat-control**命令。您可以在配置模式下使用**nat-control**命令,以指定外部通訊是否需要NAT。啟用NAT控制後,需要配置NAT規則才能允許出站流量,PIX軟體的早期版本也是如此。如果禁用NAT控制(**無nat-control**),則內部主機可以不配置NAT規則而與外部網路通訊。但是,如果內部主機沒有公有地址,則仍需要為這些主機配置NAT。

要使用ASDM配置NAT控制,請從ASDM主視窗中選擇Configuration頁籤,然後從功能選單中選擇 NAT。

啟用未經轉換的流量通過防火牆:此選項在PIX版本7.0(1)中引入。 選中此選項後,配置中不會發出 nat-control命令。此命令意味著穿越防火牆時無需任何轉換。僅當內部主機具有公有IP地址或網路 拓撲不需要將內部主機轉換為任何IP地址時,才會選中此選項。

如果內部主機具有私有IP地址,則必須取消選中此選項,以便內部主機可以轉換為公有IP地址並訪問Internet。

File Rules St	.1 for Plearch	IX - 10.1. Options	1.1 Tools Wizard	is Help				<u>_ ×</u>
di Home	ංදී Configu	artion	Monitoring	Back Forward	Search Retresh	Save Help		CISCO SYSTEMS
Interfaces Security Policy	Conti	gurstion	> NAT > Transil P	ation Rules Re Re Re Re I S he firewall without addres O Translation Even All Interfaces	s translation; ption Rules T			
NAT		Rule		Original			Translated	Add
VPN		Туре	Interface	Source Network	Destination Network	Interface	Address	Edit
Routing Global Objects Properties	-	• Static	NAT 👯 🛛	Xynamic NAT 🔥 Sta	Idic Policy NAT	ynamic Policy NA Reset	NT Manage Pools	Delete
					<admin> NA</admin>	(15)	🍜 🔂 🛛 🗄 7/11/061	3:02:29 PM UTC

要允許具有NAT控制的出站訪問,需要兩個策略。第一個是翻譯方法。這可以是使用**static**命令的靜 態轉換,也可以是使用**nat/global**規則的動態轉換。如果禁用NAT控制,並且內部主機具有公有地址 ,則不需要執行此操作。

出站訪問的另一個要求(適用於是啟用還是禁用NAT控制)是是否存在訪問控制清單(ACL)。如果存在ACL,則必須允許來源主機使用特定通訊協定和連線埠來存取目的地主機。預設情況下,對通過PIX的出站連線沒有訪問限制。這表示如果沒有為來源介面設定ACL,則在預設情況下,如果設定了轉譯方法,則會允許傳出連線。

<u>允許內部主機通過NAT訪問外部網路</u>

此配置允許子網10.1.6.0/24中的所有主機訪問外部。為此,請使用nat和global命令,如以下過程所 示。

1. 定義要包含用於NAT的內部組。

nat (inside) 1 10.1.6.0 255.255.255.0

2. 在外部介面上指定一個地址池, NAT語句中定義的主機將轉換到該地址池。

global (outside) 1 172.16.1.5-172.16.1.10 netmask 255.255.255.0

3. 使用ASDM建立全域性地址池。選擇**Configuration > Features > NAT**,並取消選中**Enable** traffic through the firewall without address translation。然後按一下Add以配置NAT規則。

Cisco ASDM	5.1 for Pl	X - 10.1.	Toolo Witter	ic Holp						-10 ×
Home	Configu	ration	Monitoring	Back	Forward	Q Search	Refresh	Save He	P	CISCO SYSTEMS
Interfaces Security Policy	Confi Confi	Enable Transla	> NAT > Transl P 1 5 traffic through to dion Rules es for Interface:	ation Rules Ra (Ra) (Ra he firewall wi C Tran [All Interface	ithout address slation Exem	s translatio otion Rules	D] S Bhow All			
NAT		Rule			Originai				Translated	Add
VPN		Туре	Interface	Source	Network	Destina	ation Network	c Interface	Address	Edit
Routing Global Objects Properties										Defete
	1	• Static	NAT 📲 (Dynamic NAT	sta 🕒,	lic Policy N Appl	AT AB	Dynamic Policy Reset	NAT <u>Manage Pools.</u>	F.
						<a><a>	dmin> I	NA (15)	😹 🔂 🔰 🔒 7/11/06	6:02:29 PM UTC

4. 按一下Manage Pools以定義NAT池地址。

Source Ho	st/Network-		
		Interface:	inside.
		IP Address:	10.1.6.0
		Mask:	255.255.255.0
			Browse
			NAT Options
anslate Ad	dress on Inte	erface: outsi	ide 💌
Translate .	Address To		
0 11	Static	IP Address;	· ·
	Redirect	port	
	Redirect C TCP C UDP	port Original port	t. Translated port.
€ ¶]	Redirect C TCP C UDP Dynamic	original port Original port Address Pool:	t. Translated port. Same address Manage Pools
€ 1	Redirect C TCP C UDP Dynamic Pool ID	original port Original port Address Pool:	t. Translated port. Same address Manage Pools
• 1	Redirect TCP CUDP Dynamic Pool ID N/A.	Original port Address Pool: No address po	t. Translated port. Same address Manage Pools Address ool defined
• 1	Redirect TCP CUDP Dynamic Pool ID N/A.	Original port Address Pool: No address po	t. Translated port. Same address Manage Pools Address ool defined

5. 選擇Outside > Add,然後選擇範圍以指定地址池。

	Address Pools				and the second second		
Global Addres	s Pools						
Global Addres	s Pools are used	l to configu	ire Dynamic Netw	ork Addre	ess Translat	ion (NAT)	
addresses.							
Interface	Pool ID		IP Address	(es)			
inside						Add	1
outside							
						Edit	
						Delet	е
1							
		. 1	A	1		1	
	01	<	Cancel		Help		
入地址範圍,	아 輸入池ID,然行	《 】 多按一下(Cancel		Help		
入地址範圍, Add Global I	이 輸入池ID,然行 Pool Item	《 後按一下(Cancel OK。		Help		
、地址範圍, Add Global I	이 輸入池ID,然行 Pool Item	<	Cancel OK。		Help		
、地址範圍, Add Global I Interface:	아 輸入池ID,然行 Pool Item	く <u> 後</u> 按一下(Cancel OK。 Po	Dol ID:	Help		
地址範圍, Add Global I Interface:	이 輸入池ID,然行 Pool Item	く 後按一下(Cancel OK。 Po	Dol ID:	Help		
地址範圍, Add Global I Interface: © Range	이 輸入池ID,然行 Pool Item Outside	<u>《</u> 後按一下(Cancel OK。 Po	Dol ID:	Help		
入地址範圍, Add Global I Interface: ● Range	이 輸入池ID,然行 Pool Item Outside	 後按一下(Cancel OK。 P	Dol ID:	Help		
入地址範圍, Add Global I Interface: ○ Range ○ Port A	이 輸入池ID,然行 Pool Item Outside	く 後按一下(ation (PA	Cancel OK。 P(Dol ID:	Help		
入地址範圍, Add Global Interface: ○ Range ○ Port A ○ Port A	이 輸入池ID,然行 Pool Item Outside ddress Transla	く 後按一下(ation (PA ation (PA	Cancel OK。 P(T) T) using the IP	ool ID:	Help	erface	
▲址範圍, Add Global Interface: ● Range ● Port A ● Port A	이 輸入池ID,然行 Pool Item Outside ddress Transla	く 後按一下(ation (PA ation (PA	Cancel OK。 P(T) T) using the IP	ool ID:	Help	erface	
▲地址範圍, Add Global Interface: ● Range ● Port A ● Port A	이 輸入池ID,然行 Pool Item Outside ddress Transla ddress Transla	く 参按一下(ation (PA ation (PA	Cancel OK。 P(T) T) using the IP	ool ID:	Help	erface	
地址範圍, Add Global I Interface: ⓒ Range ⓒ Port A ⓒ Port A ⓒ Port A	이 輸入池ID,然行 Pool Item Outside ddress Transla ddress Transla	く を按一下(ation (PA ation (PA 2.16.1.5	Cancel OK。 T) T) using the IP	ool ID: addres	Help	erface	
×地址範圍, Add Global I Interface: ○ Range ○ Port A ○ Port A	이 輸入池ID,然行 Pool Item Outside ddress Transla ddress Transla	く を按一下(ation (PA ation (PA 2.16.1.5	Cancel OK。 T) T) using the IP	ool ID: addres	Help	erface	
Add Global I Add Global I Interface: ① Range ① Port A ① Port A ① Port A	이 輸入池ID,然行 Pool Item Outside ddress Transla ddress Transla ddress Transla	く 多按一下(多按一下(ation (PA ation (PA 2.16.1.5 tional):	Cancel OK。 P(T) T) using the IP	1	Help	erface	
Add Global I Add Global I Interface: ① Range ① Port A ① Port A ① Port A Net	OF 輸入池ID,然行 Pool Item Outside ddress Transla ddress Transla ddress Transla	く 多按一下(ation (PA ation (PA 2.16.1.5 tional):	Cancel OK。 P(T) T) using the IP	ool ID: addres - 1 55.0	Help 1. s of the int 72.16.1.10	erface	
Add Global Interface:	OF 輸入池ID,然行 Pool Item Outside ddress Transla ddress Transla ddress Transla	く 多按一下(き按一下(ation (PA ation (PA 2.16.1.5 tional):	Cancel OK。 P(T) T) using the IP 255.255.2	ool ID: addres - 1 55.0	Help 1. s of the int 72.16.1.10	erface	
Add Global I Interface: ④ Range ① Port A ① Port A ① Port A Net	or 輸入池ID,然行 ool Item outside ddress Transla ddress Transla ddress Transla ddress Transla	く 多按一下(多按一下(ation (PA ation (PA 2.16.1.5 tional):	Cancel OK。 P(T) T) using the IP 255.255.2	ool ID: addres - 1 55.0	Help	erface	

- 7. 選擇Configuration > Features > NAT > Translation Rules以建立轉換規則。
- 8. 選擇Inside作為Source Interface,然後輸入您要進行NAT的地址。
- 9. 對於Translate Address on Interface,選擇**Outside**,選擇**Dynamic**,然後選擇您剛才配置的地 址池。
- 10. <u>按一下「OK」(確定)。</u>

		Interface:	inside.		¥		
		IP Address:	10.1.6.0				
		Mask:	255.255.255.0		~		
			Browse				
							NAT Options
anslate Ad	idress on Inte	erface: outs	de 💌				
Translate	Address To -						
Translate.	Address To - Static	IP Address:		<u>*</u>]		
Translate C יוי	Address To - Static	IP Address: port	[]		
Translate C 1	Address To - Static Redirect O TOP O UDP	IP Address: port Original port		Translated p] Port.		
Translate C 1/1	Address To - Static Redirect © TOP © UDP Dynamic	IP Address: port Original port Address Pool:	1	Franslated p) port Manage	Pools	
Translate C 1	Address To - Static Redirect C TOP C UDP Dynamic Pool ID	IP Address: port Original port Address Pool:	1 Addr	Franslated p ress) port Manage	Pools	
Translate C 1	Address To - Static Redirect O TOP O UDP Dynamic Pool ID	IP Address: port Original port Address Pool: 172 16 1 5-17	1 Addr	Franslated p ress) port. [Manage	Pools	_]

11. 轉換將顯示在Configuration > Features > NAT > Translation Rules的Translation Rules中。

	Configuration	 NAT > Trans 	lation Rules	See on Reliesh	save nep		
	🗣 <u>@</u> 🐺	🖉 🔒 🐰	°≥ (2. £. 18) (\$				
enaces	EEnable	traffic through	the firewall without addres	s translation:			
urity Policy	Transla	tion Rules	C Translation Exem	ption Rules			
28	Show Rul	es for Interface	All Interfaces	 Show All 			
NAT	Rule		Original			Translated	Add
VPN	Туре	Interface	Source Network	Destination Network	Interface	Address	Edit
430	the state of the	inside	⊈ 10.1,6.0/8	💠 any	outside	172.16.1.5-172.16.1.10	Dele
Routing							
8							
al Objects							
operties							
operties							
operties							
operties						•	

現在,內部主機可以訪問外部網路。當來自內部的主機啟動到外部的連線時,它們將轉換為來自全域性池的地址。地址從全域性池中按先到先轉換的方式分配,並以池中最小的地址開頭。例如,如果主機10.1.6.25是第一個啟動到外部的連線,那麼它接收地址172.16.1.5。下一個出站的主機接收172.16.1.6,以此類推。這不是靜態轉換,轉換在timeout xlate hh:mm:ss命令定義的不活動時間段後超時。如果內部主機的數量多於池中的地址,則池中的最終地址用於埠地址轉換(PAT)。

<u>允許內部主機使用PAT訪問外部網路</u>

如果希望內部主機共用一個公共地址進行轉換,請使用PAT。如果global**語句**指定一個地址,則該 地址為埠轉換。PIX允許每個介面有一個埠轉換,該轉換支援最多65,535個活動xlate對象到單個全 域性地址。完成這些步驟,以便允許內部主機使用PAT訪問外部網路。

1. 定義要為PAT包括的內部組(使用00時,選擇所有內部主機)。

nat (inside) 1 10.1.6.0 255.255.255.0

2. 指定要用於PAT的全域性地址。可以是介面地址。

global (outside) 1 172.16.1.4 netmask 255.255.255.0

- 3. 在ASDM中,選擇Configuration > Features > NAT,並取消選中Enable traffic through the firewall without address translation。
- 4. 按一下Add以配置NAT規則。
- 5. 選擇Manage Pools以配置您的PAT地址。
- 6. 選擇Outside > Add, 然後按一下Port Address Translation(PAT), 為PAT配置單個地址。

7. <u>輸入地址、池ID,</u>	然後按一下OK。		
付 Add Global Po	ol Item		
Interface:	outside 💌	Pool ID:	1
C Range			
Port Add	fress Translation (PAT)		

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

Network	Mask (optional):	255.255.2	55.0	-	
NEWOIKI	wask (optional).	235.255.2	.00.0		

×

- 8. 選擇Configuration > Features > NAT > Translation Rules以建立轉換規則。
- 9. 選擇inside作為源介面,然後輸入要進行NAT的地址。
- 10. 對於Translate Address on Interface,選擇**outside**,選擇**Dynamic**,然後選擇您剛才配置的 地址池。按一下「**OK**」(確定)。

e oberieri	0.	Jse Policy NAT		
Source Ho	st/Network			
		Interface:	inside.	
		Mask	255.255.255.0	
anslate Ad	dress on Inte	erface: outs	ide 💌	AT Options
Translate A	Address To -			
Translate A	Address To - Static C Redirect	IP Address:		
Translate / ۲۰۱۰	Address To- Static Redirect OTCP OUDP	IP Address: port Original port	Translated port.	
Translate / O ili	Address To – Static Redirect C UDP Dynamic	IP Address: port Original port Address Pool:	Translated port.	
Translate /	Address To - Static Redirect C UDP Dynamic Pool ID	IP Address: port Original port Address Pool: 172.16,1.4	Translated port.	
Translate / C 1	Address To - Static Redirect C UDP Dynamic Pool ID	IP Address: port Original port Address Pool: 172.16.1.4	Translated port.	

11. 轉換將顯示在Configuration > Features > NAT > Translation Rules的Translation Rules中。

Home C	onfiguration	Monitoring	Back Forward	Search Refresh	Save Help		
terfaces	Configuration	> NAT > Trans	Iation Rules	s translationi option Rules Show All			
NAT	Rule		Original			Translated	Ade
VPN VPN	Туре	Interface	Source Network	Destination Network	Interface	Address	Edi
4.4		inside	成²101.6.0/8	🔹 any	outside	172.16.1.4	Dele
al Objects							
	A Ctatic	NAT 📲	Dynamic NAT 🛛 🖓 Sta	atic Policy NAT 🛛 🖓 D	ynamic Policy N	AT Manage Pools	1 1

使用PAT時需要考慮以下幾點。

- 為PAT指定的IP地址不能位於另一個全域性地址池中。
- PAT不能與H.323應用程式、快取名稱伺服器和點對點隧道協定(PPTP)一起使用。PAT與域名 服務(DNS)、FTP和被動FTP、HTTP、郵件、遠端過程呼叫(RPC)、rshell、Telnet、URL過濾 和出站traceroute配合使用。
- 當您需要透過防火牆執行多媒體應用時,請勿使用PAT。多媒體應用可能與PAT提供的埠對映 衝突。
- 在PIX軟體版本4.2(2)中,PAT功能不適用於反向到達的IP資料包。PIX軟體版本4.2(3)糾正了此問題。
- 使用global命令指定的全域性地址池中的IP地址需要反向DNS條目,以確保所有外部網路地址 都可以通過PIX訪問。要建立反向DNS對映,請在地址到名稱對映檔案中為每個全域性地址使 用DNS指標(PTR)記錄。如果沒有PTR條目,站點可能會遇到慢速或間歇性的Internet連線,並 且FTP請求始終失敗。例如,如果全域性IP地址為192.168.1.3,PIX安全裝置的域名為 pix.caquana.com,則PTR記錄為:

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

限制內部主機訪問外部網路

如果為源主機定義了有效的轉換方法,但沒有為源PIX介面定義ACL,則預設情況下允許出站連線。 但是,在某些情況下,有必要根據源、目標、協定和/或埠限製出站訪問。為此,請使用accesslist命令配置ACL,並使用access-group命令將其應用於連線源PIX介面。您可以在入站和出站方向 應用PIX 7.0 ACL。此過程是一個示例,它允許一個子網的出站HTTP訪問,但拒絕所有其他主機對 外部的HTTP訪問,同時允許所有其它主機的IP流量。

1. 定義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 **注意**: PIX ACL與Cisco IOS®路由器上的ACL不同,因為PIX不使用萬用字元掩碼,如Cisco IOS。在ACL定義中使用常規子網掩碼。與Cisco IOS路由器一樣,PIX ACL的末尾有一個隱含 的「deny all」。**注意**: 新的訪問清單條目將附加到現有ACE的末尾。如果您需要先處理特定 ACE,則可以在access-list中使用_{line}關鍵字。以下是命令摘要範例: access-list acl_outbound line 1 extended permit tcp host 10.1.10.225 any

2. 將ACL套用到內部介面。

access-group acl_outbound in interface inside

- 3. 使用ASDM配置步驟1中的第一個訪問清單條目,以允許來自10.1.6.0/24的HTTP流量。選擇 Configuration > Features > Security Policy > Access Rules。
- 4. 按一下Add,輸入此視窗顯示的資訊,然後按一下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
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	source interface outside any
Protocol and Service	
	Manage Service Groups Destination Port Service = vwww Service Group
Please enter the description below (optional):	
OK Can	Help

5. 輸入三個存取清單專案後,選擇Configuration > Feature > Security Policy > Access Rules以 顯示這些規則。



<u> 允許不受信任的主機訪問受信任網路中的主機</u>

大多陣列織需要允許不受信任的主機訪問其受信任網路中的資源。一個常見的例子是內部Web伺服器。預設情況下,PIX拒絕從外部主機到內部主機的連線。要在NAT控制模式下允許此連線,請使用static命令和access-list和access-group命令。如果禁用NAT控制,則在不執行轉換的情況下,僅需要access-list和access-group命令。

使用access-group命令將ACL應用到介面。此命令可將ACL與介面相關聯,以檢查流向特定方向的 流量。

與允許內部主機外部的nat和global命令相比,如果您新增適當的ACL/組,static命令將建立允許內 部主機外部和外部主機的雙向轉換。

在本文檔中顯示的PAT配置示例中,如果外部主機嘗試連線到全域性地址,則數千個內部主機可以 使用它。static命令用於建立一對一對映。access-list命令定義允許到內部主機的連線型別,並且當 較低安全級別的主機連線到較高安全級別的主機時始終需要該命令。access-list命令基於埠和協定 ,根據系統管理員希望實現的目標,可以非常寬鬆或非常嚴格。

本文檔中的網路圖說明了使用這些命令來配置PIX,以允許任何不受信任的主機連線到內部Web伺服器,並允許不受信任的主機192.168.1.1訪問同一台電腦上的FTP服務。

在PIX 7.0及更高版本上使用ACL

使用ACL完成PIX軟體7.0版及更高版本的以下步驟。

1. 如果啟用NAT控制,則定義內部Web伺服器到外部/全域性地址的靜態地址轉換。

static (inside, outside) 172.16.1.16 10.16.1.16

2. 定義哪些主機可以在哪些埠上連線到Web/FTP伺服器。

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. 將ACL套用到外部介面。

- access-group 101 in interface outside
- 4. 選擇Configuration > Features > NAT,然後按一下Add以使用ASDM建立此靜態轉換。
- 5. 選擇inside作為源介面,然後輸入要為其建立靜態轉換的內部地址。
- 6. 選擇Static, 然後在IP地址欄位中輸入要轉換到的外部地址。按一下「OK」(確定)。

×

		Interface:	inside	
		IP Address:	10.16.1.16	
		Mask:	255.255.255.255	
			Browse	
				NAT Options
anslate Ad Translate /	dress on Inte Address To —	rface: outsid	ie 💌	
anslate Ad Translate / (• 1 1	dress on Inte Address To — Static F Redirect p	rface: outsid IP Address:	ie 💌 172.16.1.16	
anslate Ad Translate / (• 1 1	dress on Inte Address To – Static E Redirect p © TCP © UDP	rface: outsid IP Address: port Original port.	te 172.16.1.16 Translated port:	
anslate Ad Translate / • 1 1	dress on Inte Address To — Static E Redirect p © TCP © UDP Dynamic	rface: outsid IP Address: port Original port. Address Pool	te	Dols
anslate Ad Translate / (• 1 1	dress on Inte Address To – Static E Redirect p © TCP © UDP Dynamic Pool ID	rface: outsid	te	00ls
anslate Ad Translate / • •	dress on Inte Address To — Static E Redirect p C UDP Dynamic Pool ID	rface: outsid	de	pols

7. 當您選擇**Configuration > Features > NAT > Translation Rules**時,轉換將顯示在Translation Rules中。

_	Configuration	> NAT > Trans	slation Rules				
merfaces	🗣 🖄 🐺	🗹 📋 🕺	₩ 6. 6 ũ \$				
<u>6</u> .	□ (Enable	traffic through	the firewall without add	ress translation			
ourity Policy	Transl	ation Rules	C Translation Ex	emption Rules			
×.	Show Ru	les for Interfac	e: All Interfaces	▼ Show All			
NAT	Rule		Original			Translated	Add
VPN	Туре	Interface	Source Network	Destination Network	Interface	Address	Edit
***	1	inside	£ ² 10.16.1.16	🐢 any	outside	172.16.1.16	Delete
Routing							
8							
king Sel Objects							
AN pail Objects							
osei Objects							
ool Objects							
kei Objects							

8. 使用<u>Restrict Inside Hosts Access to Outside Networks</u>過程輸入access-list條目。注意:實作 這些命令時請小心。如果實施access-list 101 permit ip any any命令,則只要存在活動轉換 ,不受信任網路上的任何主機都可以使用IP訪問受信任網路上的任何主機。

<u>禁用特定主機/網路的NAT</u>

如果使用NAT控制並在內部網路上有一些公有地址,並且希望這些特定的內部主機不進行轉換而向 外輸出,則可以使用**nat 0**或**static**命令禁用這些主機的NAT。

以下是**nat**命令的示例:

nat (inside) 0 10.1.6.0 255.255.255.0 完成這些步驟,以便使用ASDM禁用特定主機/網路的NAT。

- 1. 選擇Configuration > Features > NAT,然後按一下Add。
- 2. 選擇inside作為源介面,然後輸入要為其建立靜態轉換的內部地址/網路。
- 3. 選擇Dynamic,然後為地址池選擇相同的地址。按一下「OK」(確定)。

🔂 Edit Address Translation	Rule		x
Use NAT	Use Policy NAT		
Source Host/Network			
	Interface:	inside	
	IP Address:	10.1.6.0	
	Mask:	255 255 255 0	
		255.255.255.0	
		Browse	
L			NAT Options
Translate Address on Ir	terface: outsi	de	
- Translate Address To			
C 1 Static	IP Address:		
Redirec	t port		
© TCR	o Original port:	Translated port:	
	Address Deat		
• 🔐 Dynamic	Address Pool:	I same address 📩 Manage Pools	s
Pool ID		Address	
N/A	No address po	ol defined	
L			
	OK	Cancel Help	

4. 當您選擇**Configuration > Features > NAT > Translation Rules**時,新規則將出現在Translation Rules中。

10010		Monitoring	Back Forward	Search Refresh	Serve ment	0	millin
eatures	Configuration	> Features > N	VAT = Translation Rules				
	 ◆ 注 等 	01118	8 12 12 12 13 14				
terfaces	T Enable	traffic through	the firewall without addres	ss translation			
3.	Transk	ation Rules	C Translation Exer	nption Rules			
anity Policy							
34.	Show Ru	les for Interface	All Interfaces	Show All			1
NAT	Rule		Original			Translated	Add
63	Type	Interface	Source Network	Destination Network	Interface	Address	Edit
VPN	11.1						- Auguster
	100	inside	FE 10 1 6 0/24	🗳 arno	loutside	same as priginal address	Delete
434		inside	£ ¹⁷ 1016.0/24	🦇 any	outside	same as original addres	Deleti
423 Routing		inside	⊈ ^{III} 10 1 8.0/24	🦛 ary	outside	same as original addres	E Deleti
A Routing		inside	gF 10.1.8.0/24	4 any	outside	same as original addres	s Deleti
AZS Routing		inside	<u></u> ⊈ ² 1018.024	🥠 any	outside	same as original oddres	s Deleti
Routing Ang Dacks		inside	<u></u> ⊈ ² 1018.024		outside	same as original addres	s Deleti
And the second s		inside	<u></u> ⊈ ² 1018.024	* any	outside	same as original addres	a Deleti
Age Routing ang Blacks Device enstration		inside	g≓1018.024	* any	outside	same as original addres	B Deleti
Routing Routing Sing Blocks Device nunstration		inside	<u></u>	M any	outside	same as original addres	Deleti
Routing Sing Blacks Device anistration		inside	<u></u>	M any:	outside	same as original addres	B Deleti
Routing ing Blacks Device ministration		inside	<u></u>	any:	outside	same as original addres	E Deleti
Routing ding Blacks Device ministration	د با	Inside NAT III	Dynamic NAT → SI	any	outside	Same as original addres	

5. 如果使用ACL(它允許更精確地控制您不應轉換的流量(基於源/目標),請使用以下命令。

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

- 6. 使用ASDM並選擇Configuration > Features > NAT > Translation Rules。
- 7. 選擇**Translation Exemption Rules**,然後按一下**Add**。以下範例顯示如何避免將從 10.1.6.0/24網路到任何地點的流量進行轉換。

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	o source interface outside any
Please enter the description below (optional):	
OK Car	ncel Help

8. 選擇Configuration > Features > NAT > Translation Exemption Rules以顯示新規則。



9. Web伺服器的static命令將更改,如以下示例所示。

static (inside, outside) 10.16.1.16 10.16.1.16

- 10. 在ASDM中選擇Configuration > Features > NAT > Translation Rules。
- 11. 選擇**Translation Rules**,然後按一下**Add**。輸入源地址資訊,然後選擇**Static**。在IP地址欄位 中輸入相同的地址。

Ose MAI	O Us	se Policy NAT				
Source Host/N	letwork					
		Interface:	inside	•		
	l	IP Address: Mask:	255.255.255.255			
			Browse			
					NA	T Options
anslate Addre: Translate Addr	ss on Inter	face: Joutsi	de			
Translate Aud	less IU					
ransiate Add	i tic	IP Address:	10.16.1.16	Y		
• • • Sta	itic direct pr Redirect pr C UDP	IP Address: ort Original port	10.16.1.16	ated port		
• • • • Sta	ntic Redirect po TCP OUDP	IP Address: ort Original port Address Pool:	10.16.1.16 Transl	ated port	ge Pools	
• • • Sta	ness To nedirect pr TCP OUDP namic Pool ID	IP Address: ort Original port Address Pool	10.16.1.16 Transi Same address	ated port. Mana	ge Pools	
	ntic Redirect po TCP CUDP namic Pool ID	IP Address: ort Original port Address Pool:	10.16.1.16 Transl same address	ated port	ge Pools	

12. 當您選擇**Configuration > Features > NAT > Translation Rules**時,轉換將顯示在Translation Rules中。

Home Co	anfiguration Monitoring	Back Forward	Search Refresh	Save Help		adhasa
,	• 옷 후 🗹 💼	iii 🛍 🛍 🏦 🛍 🤤 🗌				
certaces	🗆 (Enable traffic throu	igh the firewall without addre	ss translation			
urity Policy	Translation Rules	C Translation Exer	mption Rules			
23	Show Rules for Interf	ace: All Interfaces	Show All			
NAT	Rule	Original			Translated	Add
VPN VPN	Type Interface	Bource Network	Destination Network	Intenace	Address	Edit
4.74	inside	⊑ [□] 10.16.1.16	🥠 any	outside	10.16.1.16	Delet
Routing			and a			
80						
bai Objacts						
operties						
	•				eT.	
	Static NAT	🔛 Dynamic NAT 🛛 🖓 Si	tatic Policy NAT 🛛 🙀 D	ynamic Policy N	Manage Pools	S.

13. 如果使用ACL,請使用以下命令。

access-list 102 permit tcp any host 10.16.1.16 eq www access-group 102 in interface outside 有關在ASDM中配置ACL的其他資訊,請參閱本文檔的<u>限制內部主機訪問外部網路</u>部分。請 注意指定網路/掩碼時使用 nat 0與使用只允許從內部發起連線的網路/掩碼的ACL之間的區別 。將ACL與nat 0配合使用允許通過入站或出站流量發起連線。為了避免可達性問題,PIX介 面需要位於不同的子網中。

<u>連線埠重新導向(轉送)(含靜態)</u>

在PIX 6.0中,新增了埠重定向(轉發)功能,以允許外部使用者連線到特定IP地址/埠,並讓PIX將 流量重定向到適當的內部伺服器/埠。static命令已修改。共用地址可以是唯一地址、共用出站PAT地 址或與外部介面共用。此功能在PIX 7.0中提供。

注意:由於空間限制,命令顯示在兩行上。

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]]]

注意:如果靜態NAT使用外部IP(global_IP)地址進行轉換,則可能導致轉換。因此,在靜態轉譯中 使用關鍵字interface,而不是使用IP位址。 以下網路範例中的連線埠重新導向(轉送):

- •外部使用者將Telnet請求定向到唯一IP地址172.18.124.99,PIX將該IP地址重定向到10.1.1.6。
- 外部使用者將FTP請求定向到唯一IP地址172.18.124.99,PIX將該IP地址重定向到10.1.1.3。
- 外部使用者將Telnet請求定向到PAT地址172.18.124.208,PIX將地址重定向到10.1.1.4。
- 外部使用者將Telnet請求定向到IP地址為172.18.124.216之外的PIX,PIX會將其重定向到 10.1.1.5。
- 外部使用者將HTTP請求定向到IP地址為172.18.124.216之外的PIX,PIX會將其重定向到 10.1.1.5。
- 外部使用者將HTTP埠8080請求定向到PAT地址172.18.124.208,PIX將地址重定向到10.1.1.7埠80。

此示例還使用ACL 100阻止某些使用者從內部到外部的訪問。此步驟是可選的。在未設定ACL的情況下允許所有流量出站。

<u>網路圖表 — 連線埠重新導向(轉送)</u>



<u>部分PIX配置—埠重定向</u>

此部分組態說明使用靜態連線埠重新導向(轉送)。請參閱連線埠重新導向(轉送)網路圖表。

部分PIX 7.x配置 — 埠重定向(轉發) 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 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

注意:如果使用**sysopt noproxyarp outside**命令配置PIX/ASA,則它不允許防火牆在PIX/ASA中執行 proxyarp和靜態NAT轉換。為了解決此問題,請在PIX/ASA配置中刪除**sysopt noproxyarp outside**命 令,然後使用免費ARP更新ARP條目。這樣靜態NAT條目可以正常工作。

以下過程是一個如何配置埠重定向(轉發)的示例,允許外部使用者將Telnet請求定向到唯一IP地 址172.18.124.99,PIX將該IP地址重定向到10.1.1.6。

- 1. 使用ASDM並選擇Configuration > Features > NAT > Translation Rules。
- 2. 選擇Translation Rules, 然後按一下Add。
- 3. 對於源主機/網路,輸入內部IP地址的資訊。
- 4. 對於Translate Address To,選擇Static,輸入外部IP地址,然後選中Redirect port。
- 5. 輸入翻譯前和翻譯後埠資訊(此示例維護埠23)。 按一下「OK」(確定)。

🔂 Add Address Tr	anslation R	ule						×
Use NAT	00	se Policy NAT						
Source Hos	t/Network							-
		Interface:	inside	1	•			
		IP Address:	10.1.1.6					
		Mask:	255.255.255.2	55	-			
					_			
			Browse					
						N	AT Options	
Translate Add	ress on inter	rface: outsid	ie 💌					-
-Translate Ac	dress To —							-
· · · ·	Static	IP Address:	172.18.124.99	Ŧ				
F	Redirect p	ort	·					
	○ TCP ○ UDP	Original port	23 Tr	anslated po	rt 23			
o 👭 (Dynamic	Address Pool:	same addres	s 🔻	Manage P	ools		
	Pool ID		Addre	ISS				
	Г	014			Liele	1		
	_	UK	Cancel		Help			

當您選擇**Configuration > Features > NAT > Translation Rules**時,轉換將顯示在Translation Rules中。

me Co	age offiguration	Monitoring	Back Forward	Q Q Search Refresh	Save Hel) n	Cisco Syst
atures	Configuration	n - Features - N	IAT - Translation Rules				
_	* * *	1 1 %	10.11.5.E. (\$				
-laces	Enabl	e traffic through	the firewall without addres	s translation			
0	@ Trans	Istion Rules	C Translation Even	volino Rulas			
ty Policy		auto rigina	· manadoo Exert				
31.	Show Ru	ules for interface	All Interfaces	Show All			
NAT	Rule		Original			Translated	Add
	Type	interface	Source Network	Destination Network	Interface	Address	Edit
VIPNU	100	inside	A 101.16	🔹 any	outside	172.18.124.98	Delete
NJp	100	e	Port: 23/tcp	<u></u>	k ·	Port 23ftcp	
35							
oung							
<u>8</u> 2							
ng Blocks							
3							
evice							
evice nistration							
evice nistration							
evice nistration	4						ы
evice nistration perties	د اب Stati	e NAT 411	Dynamic NAT 🛛 🖓 St	atic Policy NAT 🔒 0	lynamic Policy I	NAT Manage Pools	<u>ы</u>
evice nistration perties	ار با « Stati	e NAT - 4]]	Dynamic NAT 🔞 St	atic Policy NAT 🔞 0	lynamic Policy (NAT Managa Pools	
evice nistration Disperties	€ -{ + Stati	e NAT 📲	Dynamic NAT 🖓 St	atic Policy NAT 🔒 0 Apply	lynamic Policy Reset	NAT Manage Pools	

使用靜態限制TCP/UDP會話

如果要將TCP或UDP會話限製為放置在PIX/ASA中的內部伺服器,請使用static命令。

指定整個子網的最大同步TCP和UDP連線數。預設值為0,表示無限制連線(空閒連線在timeout conn命令指定的空閒超時後關閉。) 此選項不適用於外部NAT。安全裝置僅跟蹤從較高安全介面到 較低安全介面的連線。

限制初期連線的數量可以保護您免受DoS攻擊。安全裝置使用初始限制觸發TCP Intercept,TCP Intercept可保護內部系統免受通過用TCP SYN資料包泛洪介面實施的DoS攻擊。早期連線是尚未完 成源和目標之間必要握手的連線請求。此選項不適用於外部NAT。TCP攔截功能僅適用於安全級別 更高的主機或伺服器。如果為外部NAT設定初始限制,將忽略初始限制。

例如:

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. 這是一條與連線相關的消息。當超出與指定靜態地址的最大連線數時,將記錄此消息。econns變數 是初始連線的最大數目,nconns是靜態或xlate允許的最大連線數目。

建議的操作是使用show static命令檢查對連線到靜態地址施加的限制。此限制是可配置的。

%ASA-3-201011:從10.1.26.51/2393到外部介面10.0.86.155/135的入站資料包的連線限制超過 1000/1000

此錯誤訊息是由Cisco錯誤ID <u>CSCsg52106</u>(僅限<u>註冊</u>客戶)所產生。 如需詳細資訊,請參閱此錯誤 。

<u>時間型存取清單</u>

建立時間範圍不會限制對裝置的訪問。time-range命令僅定義時間範圍。定義時間範圍後,可以將 其附加到流量規則或操作。

若要實作時間型ACL,請使用time-range命令定義特定日期和時間。然後使用with the access-list extended time-range命令將時間範圍繫結到ACL。

時間範圍取決於安全裝置的系統時鐘。但是,此功能與NTP同步配合使用效果最佳。

建立時間範圍並進入時間範圍配置模式後,可以使用absolute和periodic命令定義時間範圍引數。要 恢復time-range命令的absolute和periodic關鍵字的預設設定,請在時間範圍配置模式下使用 default命令。

若要實作時間型ACL,請使用**time-range**命令定義特定日期和時間。然後使用**with the access-list extended命令**將時間範圍繫結到ACL。下一個示例將名為「Sales」的ACL繫結到名為「New York Minute」的時間範圍:

此示例建立一個名為「New York Minute」的時間範圍並進入時間範圍配置模式:

hostname(config)#time-range New_York_Minute
hostname(config-time-range)#periodic weekdays 07:00 to 19:00
hostname(config)#access-list Sales line 1 extended deny ip any any time-range New_York_Minute
hostname(config)#access-group Sales in interface inside

開啟技術支援案例時要收集的資訊

如果您仍然需要幫助並希望通過Cisco技術支援開啟案例 ,請確保包括此資訊以排除PIX安全裝置的故障。

- •問題描述和相關拓撲詳細資訊。
- 開啟案例之前用於進行故障排除的步驟。
- show tech-support命令的輸出。
- 運行logging buffered debugging命令後show log命令的輸出,或顯示問題的控制檯捕獲(如果可用)。
 將收集的資料以非壓縮純文字檔案格式(.txt)附加到您的案例。您可以在TAC服務請求工具(僅限註冊客戶)中將資訊 附加到您的案例。如果您無法存取TAC Service Request Tool(僅供註冊客戶使用),可以將電子郵件附件中的資訊

相關資訊

- <u>PIX安全裝置支援頁</u>
- <u>PIX命令參考</u>
- 思科自適應安全裝置管理器(ASDM)故障排除和警報
- <u>要求建議 (RFC)</u>
- 技術支援與文件 Cisco Systems