# 帶有兩個內部網路的ASA 8.3(x)動態PAT和網際網路配置示例

## 目錄

<u>簡介</u> <u>必要條件</u> <u>需求</u> <u>採用元件</u> <u>慣例</u> <u>組態</u> <u>網路圖表</u> <u>ASA CLI配置</u> <u>ASDM配置</u> <u>驗證 檢驗通用PAT規則</u> <u>驗證特定PAT規則</u> <u>疑難排解</u> <u>相關資訊</u>

# <u> 簡介</u>

本文檔提供運行軟體版本8.3(1)的思科自適應安全裝置(ASA)上的動態PAT配置示例。 通過將實際源 地址和源埠轉換為對映地址和唯一對映埠,動態PAT將多個實際地址轉換為單個對映IP地址。由於 每個連線的源埠不同,因此每個連線都需要單獨的轉換會話。

# <u>必要條件</u>

### <u>需求</u>

嘗試此組態之前,請確保符合以下要求:

- 確保內部網路在ASA內部有兩個網路: 192.168.0.0/24 直接連線到ASA的網路。
   192.168.1.0/24 位於ASA內部、但在其他裝置(例如路由器)之後的網路。
- •確保內部使用者按如下方式獲得PAT:192.168.1.0/24子網上的主機將獲得PAT到 ISP(10.1.5.5)提供的備用IP地址。ASA內部的任何其他主機都將將PAT獲取到ASA的外部介面 IP地址(10.1.5.1)。

#### <u>採用元件</u>

本文中的資訊係根據以下軟體和硬體版本:

- •思科調適型安全裝置(ASA)版本8.3(1)
- ASDM版本6.3(1)

註:請參閱<u>允許ASDM進行HTTPS訪</u>問,以便允許ASDM配置ASA。

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。

#### <u>慣例</u>

請參閱思科技術提示慣例以瞭解有關檔案慣例的資訊。

## <u> 組態</u>

#### 網路圖表

本檔案會使用以下網路設定:



**注意:**此配置中使用的IP編址方案在Internet上不能合法路由。它們是<u>RFC 1918</u> 位址,已在實驗室 環境中使用。

- ASA CLI配置
- ASDM配置

#### <u>ASA CLI配置</u>

本文檔使用如下所示的配置。

#### ASA動態PAT配置

```
ASA#configure terminal
Enter configuration commands, one per line. End with
CNTL/Z.
!--- Creates an object called OBJ_GENERIC_ALL. !--- Any
host IP not already matching another configured !---
object will get PAT to the outside interface IP !--- on
the ASA (or 10.1.5.1), for internet bound traffic.
ASA(config)#object network OBJ_GENERIC_ALL
ASA(config-obj)#subnet 0.0.0.0 0.0.0.0
ASA(config-obj)#exit
ASA(config)#nat (inside,outside) source dynamic
OBJ_GENERIC_ALL interface
```

--- The above statements are the equivalent of the !--nat/global combination (as shown below) in v7.0(x), !-v7.1(x), v7.2(x), v8.0(x), v8.1(x) and v8.2(x) ASA code: nat (inside) 1 0.0.0.0 0.0.0.0 global (outside) 1 interface !--- Creates an object called OBJ\_SPECIFIC\_192-168-1-0. !--- Any host IP facing the the 'inside' interface of the ASA !--- with an address in the 192.168.1.0/24 subnet will get PAT !--- to the 10.1.5.5 address, for internet bound traffic. ASA(config)#object network OBJ\_SPECIFIC\_192-168-1-0 ASA(config-obj)#subnet 192.168.1.0 255.255.255.0 ASA(config-obj)#exit ASA(config)#nat (inside,outside) source dynamic OBJ\_SPECIFIC\_192-168-1-0 10.1.5.5 !--- The above statements are the equivalent of the nat/global !--- combination (as shown below) in v7.0(x),v7.1(x), v7.2(x), v8.0(x), !--- v8.1(x) and v8.2(x) ASA code: nat (inside) 2 192.168.1.0 255.255.255.0 global (outside) 2 10.1.5.5 ASA 8.3(1)運行配置 ASA#show run : Saved ASA Version 8.3(1) 1 hostname ASA enable password 8Ry2YjIyt7RRXU24 encrypted passwd 2KFQnbNIdI.2KYOU encrypted names ! *!--- Configure the outside interface.* ! interface GigabitEthernet0/0 nameif outside security-level 0 ip address 10.1.5.1 255.255.255.0 !--- Configure the inside interface. ! interface GigabitEthernet0/1 nameif inside security-level 100 ip address 192.168.0.1 255.255.255.0 ! interface GigabitEthernet0/2 shutdown no nameif no security-level no ip address ! interface GigabitEthernet0/3 shutdown no nameif no security-level no ip address ! interface Management0/0 shutdown no nameif no security-level no ip address management-only ! boot system disk0:/asa831-k8.bin ftp mode passive object network OBJ\_SPECIFIC\_192-168-1-0 subnet 192.168.1.0 255.255.255.0 object network OBJ\_GENERIC\_ALL subnet 0.0.0.0 0.0.0.0 pager lines 24 no failover icmp unreachable rate-limit 1 burst-size 1 asdm image disk0:/asdm-631.bin no asdm history enable arp timeout 14400 nat (inside,outside) source dynamic OBJ\_GENERIC\_ALL interface nat (inside,outside) source dynamic OBJ\_SPECIFIC\_192-

#### 168-1-0 10.1.5.5

```
route inside 192.168.1.0 255.255.255.0 192.168.0.254 1
route outside 0.0.0.0 0.0.0.0 10.1.5.2
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00
absolute
timeout tcp-proxy-reassembly 0:01:00
dynamic-access-policy-record DfltAccessPolicy
http server enable
http 192.168.0.0 255.255.254.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup
linkdown coldstart
crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes
4608000
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
class-map inspection_default
match default-inspection-traffic
1
1
policy-map type inspect dns preset_dns_map
parameters
 message-length maximum client auto
 message-length maximum 512
policy-map global_policy
class inspection_default
 inspect dns preset_dns_map
 inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
 inspect skinny
  inspect sunrpc
 inspect xdmcp
 inspect sip
 inspect netbios
 inspect tftp
 inspect ip-options
service-policy global_policy global
prompt hostname context
Cryptochecksum:6fffbd3dc9cb863fd71c71244a0ecc5f
: end
```



為了通過ASDM介面完成此配置,您必須:

- 1. 新增三個網路對象;此範例新增以下網路對象:OBJ\_GENERIC\_ALLOBJ\_SPECIFIC\_192-168-1-010.1.5.5
- 2. 建立兩個NAT/PAT規則;以下示例為這些網路對象建立NAT規則 : OBJ\_GENERIC\_ALLOBJ\_SPECIFIC\_192-168-1-0

#### 新增網路對象

完成以下步驟以新增網路對象:

1. 登入到ASDM,然後選擇Configuration > Firewall > Objects > Network Objects/Groups。

He View Tools Wizards Window Help	p g 🔛 Save 🔇 Refri	esh 🔾 Back 🔘	Forward ? Help		cisco
irewall 3 9 ×	onfiguration > Firewall	> Objects > Netwo	ek Objects/Groups		
Filter Rules	♥ Add ♥  Edit : Ⅲ Iter:	Delete   Q Where	: Used		Filter Gear
Threat Detection	Name /1	IP Address	Netmask	Description	Object NAT Address
- Cobjects	IPv4 Network Objects				
Network Objects/Groups	- 🧇 any	0.0.0.0	0.0.0.0		
Service Objects/Groups	- M inside-network	192.168.0.0	255.255.255.0		
Class Maps	- 💑 outside-net	10.1.5.0	255.255.255.0		
E Lo Inspect Maps	- 3 192.168.0.233	192.168.0.233	255.255.255.255		
EB TCP Mase	IPv6 Network Objects				
Time Ranges *	🧼 any	11	0		
			1		

2. 選擇Add > Network Object以新增網路對象。

📬 Cisco ASDM 6.3 for ASA - 192.168.0.1					_ O ×
File Wew Tools Wizards Window I	Help		Look For	c	
Home S Configuration Monito	oring 🔄 Save 🔇 Refresh 🤇	Back 🕐 F	orward 🦿 💙 Help		CISCO
Firewall & P ×	Configuration > Firewall > Object	cts > Network	k Objects/Groups		
AAA Rules	💠 Add 🔹 🗃 Edit 👔 Delete	Q. Where L	Jsed		
- Public Servers	Network Object				Etherichard
	Network Object Group	tress	Netmask	Description	Object NAT Address
Collects	Pv4 Network Objects				
Network Objects/Groups	- 🥎 any 0.0.0.0		0.0.0.0		
Service Objects/Groups	inside-network 192.168	.0.0	255.255.255.0		
Class Maps	outside-net 10.1.5.0	)	255.255.255.0		
Englisseet Maps		.0.233	255.255.255.255		
TCP Maps	<ul> <li>IPv6 Network Objects</li> </ul>				
Time Ranges *	- 🍫 any 💠		0		
A Device Setup					
E Firewal					
Remote Access VPN					
🙀 Ste-to-Site VPN					
🖏 🕫					
Device Management					
:			Apply Res	et	

系統將顯示Add Network Object對話方塊。

:

ľ	🚰 Add Network Object 🛛 🔀							
	Name:	OBJ_GENERIC_ALL						
	Туре:	Network						
	IP Address:	0.0.0.0						
	Netmask:	0.0.0.0						
	Description:							
	NAT	*						
		OK Cancel Help						

- 3. 在新增網路對象對話方塊中輸入以下資訊:網路對象的名稱。(此示例使用 OBJ\_GENERIC\_ALL。)網路對象的型別。(此示例使用Network。)網路對象的IP地址。(此示例 使用0.0.0.0。)網路對象的網路掩碼。(此示例使用0.0.0.0。)
- 4. 按一下「OK」(確定)。網路對象即建立並顯示在「網路對象/組」清單中,如下圖所示

Home 🍪 Configuration 🔯 Moni	Help toring   🔜 Save 🔇 Refr	esh 🔇 Back 🔘	Loo Forward   🍞 Help	k For:
Firewall	Configuration > Firewall ♣ Add • ☑ Edit ① Filter:	> Objects > Netwo	r <u>k Objects/Groups</u> Used	
	Name / 1	IP Address	Netmask	Des
Diects	- IPv4 Network Objects			
Network Objects/Groups	- 🎱 any	0.0.00	0.0.00	
Service Objects/Groups	- inside-network	192.168.0.0	255.255.255.0	
E-Class Maps	and outside-net	10.1.5.0	255.255.255.0	
Inspect Maps	OBJ_GENER	0.0.0	0.0.0.0	
Regular Expressions	- 3 192.168.0.233	192.168.0.233	255.255.255.255	
Time Ranges	- IPv6 Network Objects			
	- 🏈 any	::	0	
			Apply	Reset

5. 重複前面的步驟以新增第二個網路對象,然後按一下**確定**。此示例使用以下值:名稱 :*OBJ\_SPECIFIC\_192-168-1-0*Type:*網路*IP 位址:*192.168.1.0*網路掩碼

	🔂 Add Netwo	rk Object 🛛 🗙	
	Name:	OBJ_SPECIFIC_192-168-1-0	
	Туре:	Network	
	IP Address:	192.168.1.0	
	Netmask:	255.255.255.0	
	Description:		
	NAT	*	
		OK Cancel Help	
5.255.255.0			

對象即建立並顯示在「網路對象/組」清單中,如下圖所示

isco ASDM 6.3 for ASA - 192.168.0.1	de .	Look For		
		LOOKPORT		
Home S Configuration Monitor	ng 🔛 Save 🔇 Refresh 🚺 Back 🕻	Forward 7 Help		CISCO
ewall 🗗 Ə Ə 🗙	onfiguration > Firewall > Objects > Netw	ork Objects/Groups		
AAA Rules	Add - REAR TO Delete O Whe	re Lised		
Piter Rules	where a contract of the	TE OPEO		
Public Servers	Filter:			Elker C
Threat Detection	Name / 1 IP Address	Notmask.	Description	Object NAT Addres
Cobjects	E IPv4 Network Objects			
Network Objects/Groups	- 🍅 any 0.0.0.0	0.0.0.0		
Service Objects/Groups	- 30 inside-network 192.168.0.0	255.255.255.0		
Gig Class Maps     G. EA toroact Maps	- m outside-net 10.1.5.0	255.255.255.0		
Regular Expressions	- 60_GENER 0.0.0.0	0.0.0.0		
TCP Maps	- 📇 192.168.0.233 192.168.0.233	255.255.255.255		
💿 Time Ranges 🛛 💌	L-g3 083_SPECDF 192.168.1.0	255.255.255.0		
	IPv6 Network Objects	-		
5 Device Setup	- 🥹 any 💠	0		
Firewal				
Remote Access VPN				
Ste-to-Site VPN				
195				
Device Management				
-		And Dent	1	

6. 重複前面的步驟以新增第三個網路對象,然後按一下確定。此示例使用以下值:名稱 :*10.1.5.5*Type:*主機*IP 位址

	付 Add Netwo	rk Obje	ect		×
	Name:	10.1.5	5.5		
	Туре:	Host			•
	IP Address:	10.1.5	5.5		
	Description:				
	NAT				*
.10 1 5 5		ОК	Cancel	Help	(注) (注) (注) (注) (注) (注) (注) (注) (注) (注)
即建立並顯	<b>頁示在「網路對</b>	家/組」	清單中。		——————————————————————————————————————
🔂 Cisco ASI	DM 6.3 for ASA - 1	92.168.0.	.1		
File View	Tools Wizards	Window	Help toring 🔲 Save 🙉 Refr	esh 🙆 Back 🕥 f	Look For:
Firewall		ΦX		> Objects > Network	ō k Objects/Groups
AAA	Rules Rules	-	∲ Add • 🕑 Edit 🗍	Delete Q. Where I	Used
URL	c Servers Filtering Servers		Filter:	-	
- 🔂 Thre	at Detection		Name A1	IP Address	Netmask
E-liss Obje	cts Jetwork Objects/Grou	uns.	E IPV4 Network Objects	0.0.0.0	0.0.0.0
	Service Objects/Grou	ps		10.1.5.5	255.255.255.255
🗉 🖸 🖉	lass Maps		- A inside-network	192.168.0.0	255.255.255.0
I 🔁 🖸 I	nspect Maps		- 🙀 outside-net	10.1.5.0	255.255.255.0
	CP Maps		OBJ_GENER	0.0.0.0	0.0.0.0
0	ime Ranges	-	- 📇 192.168.0.233	192.168.0.233	255.255.255.255
0	*******		OBJ_SPECIF	192.168.1.0	255.255.255.0
Device Device	Setup		IPv6 Network Objects		
Firewa		*1*1*1*1*1*	🍪 any	••	U

Network Objects/Groups清單現在應包括NAT規則需要參考的三個必要對象。

## 建立NAT/PAT規則

完成以下步驟以建立NAT/PAT規則:

1. 建立第一個NAT/PAT規則:在ASDM中,選擇**Configuration > Firewall > NAT Rules**,然後按 一下**Add**。

📬 Ci	isco ASDM 6.3 l	for ASA - 19	2.168.0	.1						
File	View Tools	Wizards W	indow	He	lp					
	Home 🖓 Cor	figuration	🗿 Moni	tori	ng	Sav	Q	Refrest	h 🖸 🕄 Back 🔘	Forward 🖓 Help
Fire	wall	5 P	×	9	ion	figuration	> Fir	ewall >	NAT Rules	
	Access Rules	]	1		\$	Add 👻	🗹 Ed	it 💼 D	Delete 🕈 🗲	3 B 🛍 -
		/ Kules			#				Match Criteria: 0	riginal Packet
	Filter Rules					Source In	ltf D	est Intf	Source	Destination
	🐴 Public Server:	s				"Network (	bject	NAT (No	o rules)	
	Turk Filtering	Servers								
	🔯 Threat Detec	tion								
Ē.	🔯 Objects									
	Network	Objects/Group	s							
	Service C	bjects/Groups								
	E Ray Lass Map	ps Aano	_							
	E B Inspect i		<u> </u>							
2	Device Setup									
9	Firewall									
8	Remote Acces	s VPN								

🔂 Add NAT Rule			×
Match Criteria: Original Packet			
Source Interface: Any	-	Destination Interface:	Apy
Source Address ADV		Destination Address	
inside		Destination Address:	
outside		Service:	any 🔄
Action: Translated Packet	Name: IP Addr Security	inside ess: 192.168.0.1 / 255 / Level:100	5.255.255.0
Source NAT Type: Static	Port:	GigabitEthernet0/	0
Source Address: Original		Destination Address:	Original 🛄
Fall through to interface PAT		Service:	Original 🛛 🖳
Options			
🔽 Enable rule			
Translate DNS replies that match this	s rule		
Direction: Both			
Description:			
		ancel Halo	1

系統將顯示Add NAT Rule對話方塊。

在匹配條件中:在Add NAT Rule對話方塊的Original Packet區域,從Source Interface下拉選單中選擇**inside**。

Match Criteria: Original Packet	
	_
Source Interface: inside 💌 Destination Interface: Any	-
Source Address: any Destination Address: any	-
Service:	-
	-
Action: Translated Packet	_
Source NAT Type: Static	_
Source Address: Original Destination Address: Original	· ]
Fall through to interface PAT Service: Original	-
Options	_
Enable rule	
Translate DNS replies that match this rule	
Direction: Both	
	_
Description:	
OK Cancel Help	
按一下位於「 <b>源地址</b> 」文本欄位右側的瀏覽()按鈕。將出現「瀏覽原始源地址」對話方均	0
Browse Original Source Address	X
🗣 Add 👻 📝 Edit 👔 Delete 🔍 Where Used	
Filter:	1
Name         ▲1         IP Address         Netmask         Description         Object NAT Addr	ſ
IPv4 Network Objects	
- nd OBJ SP 192.168.1.0 255.255.255.0	
any 0.0.0.0 0.0.0.0	
J Selected Original Source Address	
Original Source Address -> OBJ_GENERIC_ALL	
OK Cancel	

在「瀏覽原始源地址」對話方塊中,選擇您建立的第一個網路對象。(在本例中,選擇

## $OBJ_GENERIC_ALL$ 。)按一下Original Source Address,然後按一下OK。

*OBJ\_GENERIC\_ALL*網路對象現在出現在「匹配條件」的「源地址」欄位中:Add NAT Rule對話方塊的Original Packet區域。

付 Add NAT Rule			×				
Match Criteria: Ori	iginal Packet						
Source Interface:	inside 💌	Destination Interface:	Any				
Source Address:	OBJ_GENERIC_ALL	Destination Address:	any 🖳				
		Service:	any 🖳				
Action: Translated	Packet						
Source NAT Type:	Static						
Source Address:	Original	Destination Address:	Original				
Eall through to	interface PAT	Service:	Original				
Options		20111001					
Enable rule							
Translate DNS	replies that match this rule						
Direction: Both	<u> </u>						
Description:							
	ОК	ancel Help					

在Action:在Add NAT Rule對話方塊的Translated Packet區域中,從Source NAT Type對話方 塊中選擇**Dynamic PAT(Hide)**。

薩 Add NAT Rule		×				
Match Criteria: Original Packet						
Source Interface: inside	Destination Interface:	Any				
Source Address: OBJ_GENERIC_ALL	Destination Address:	any				
	Service:	any				
Action: Translated Packet						
Source NAT Type: Static						
Source Address: Static	Destination Address:	Original				
Dynamic PAT (Hide)	Service:	Original ···				
Options						
🔽 Enable rule						
Translate DNS replies that match this rule						
Direction: Both						
Description:						
OK OK	Cancel Help					
	 鈕。					

薩 Add NAT Rule		×					
Match Criteria: Original Packet							
Source Interface: inside	Destination Interface:	Any					
Source Address: OB1 GENERIC AU		any .					
	Comisso						
	Service:						
Action: Translated Packet							
Source NAT Type: Dynamic PAT (Hide)	<b>-</b>						
Source Address: Original		Original					
Fall through to interface PAT	Service:	Original ···					
Options							
Enable rule							
Translate DNS replies that match this rule							
Direction: Both							
Description:							
OK	Cancel Help						
 將出現Browse Translated Source Addres							
Browse Translated Source Address		×					
💠 Add 👻 🗹 Edit 📋 Delete 🛛 🔍 Where Use	d						
Filter:		Filter Clear					
Name A1 IP Address Net	tmask Description	Object NAT Addr					
■ 10.1.5.5 10.1.5.5 255.255	.255.255						
Interfaces							
🔤 inside							
utside							
, Selected Translated Source Address							
Translated Source Address -> Outside							
		OK Cancel					

在Browse Translated Source Address對話方塊中,選擇**outside**介面對象。(已建立此介面 ,因為它是原始配置的一部分。)按一下**Translated Source Address**,然後按一下**OK**。外部 介面現在顯示在Action:Translated Packet區域。

薩 Add NAT Rule		×						
Match Criteria: Original Packet								
Source Interface: inside	Destination Interface:	outside 🔽						
Source Address: OBJ_GENERIC_ALL	Destination Address:	any 🖳						
	Service:	any 🖳						
Action: Translated Packet								
Source NAT Type: Dynamic PAT (Hide)								
Source Address: outside	Destination Address:	Original 🛛 🖳						
Fall through to interface PAT	Service:	Original						
Options								
🔽 Enable rule								
Translate DNS replies that match this rule								
Direction: Both 💌								
Description:								
		1						
<b>汪慐:</b> Destination Interface <b>欄位也曾更收為外部介面。</b> 驗證第一個完成的PAT規則是否如卜所 示:在匹配條件中:Original Packet area,驗證以下值:源介面=內部源地址= OBJ_GENERIC_ALL目的地位址=任意服務=任意在Action:Translated Packet area,驗證以下 值:源NAT型別=動態PAT(隱藏)源地址=外部目的地位址=原始服務=原始按一下「 <b>OK</b> 」 (確定)。第一個NAT規則出現在ASDM中,如下圖所示								
Configuration > Firewall > NAT Rules								
💠 Add 🗸 🗭 Edit 📋 Delete 🗇 🗲 👗 🖻 🛍	🗸 🔍 Çind 💀 Diagram 🥰	Packet Trace						
# Match Criteria: Original Packet Source Intf Dest Intf Source Destination	Service Sour	Action: Translated Packet ce Destination Servic						
Inside outside gA O8J_GENER I any "Network Object" NAT (No rules)	🔹 any 🔤 outside	(P) Original Original						
		<u> </u>						

2. 建立第二個NAT/PAT規則:在ASDM中,選擇Configuration > Firewall > NAT Rules,然後按 一下Add。在匹配條件中:在Add NAT Rule對話方塊的Original Packet區域,從Source Interface下拉選單中選擇inside。按一下位於「源地址」欄位右側的瀏覽(...)按鈕。將出現「瀏 覽原始源地址」對話方塊。

Name At	IP Address	Netmask	Description	Object NAT Addr
PIPV4 Network Obj		255 255 255 255		
	0.0.0.0	0.0.0.0		
OBJ_SP	192.168.1.0	255.255.255.0		
🌕 🌍 any	0.0.0.0	0.0.0.0		
	·	· · ·		
ected Original Sour	e Address			

在「瀏覽原始源地址」對話方塊中,選擇建立的第二個對象。(在本例中,選擇 OBJ\_SPECIFIC\_192-168-1-0。)按一下Original Source Address,然後按一下OK。 *OBJ\_SPECIFIC\_192-168-1-0*網路對象將出現在「匹配條件」的「源地址」欄位中:Add NAT Rule對話方塊的Original Packet區域。在Action:在Add NAT Rule對話方塊的Translated Packet區域中,從Source NAT Type對話方塊中選擇Dynamic PAT(Hide)。按一下Source Address欄位右側的……按鈕。將出現Browse Translated Source Address對話方塊。

, Name ∧1	IP Address	Netmask	Description	Object NAT Addr.
···· Original	I Hadross	Hoemask	Description	object Ant Hoard
- IPv4 Network Obje	ects			
. 9 10.1.5.5	10.1.5.5	255.255.255.255		
Interfaces	:			
🔤 inside				
🔤 outside				
elected Translated So	urce Address			
lected Translated So	urce Address			

在Browse Translated Source Address對話方塊中,選擇10.1.5.5對象。(已建立此介面,因 為它是原始配置的一部分)。按一下**Translated Source Address**,然後按一下**OK**。10.1.5.5網 路對象出現在Action:「新增NAT規則」對話方塊的「轉換的資料包」區域。在匹配條件中 : Original Packet area,從Destination Interface下拉選單中選擇**outside**。**註:如**果不為此選 項選擇*outside*,則目標介面將引用*Any*。

🞼 Edit NAT Rule		×					
Match Criteria: Original Packet							
Source Interface: inside	Destination Interface:	outside					
Source Address: _SPECIFIC_192-168-1-0	Destination Address:	any					
	Service:	any					
Action: Translated Packet							
Source Address: 10.1.5.5	Destination Address:	Original					
Fall through to interface PAT	Service:	Original 🖳					
Options							
🔽 Enable rule	🔽 Enable rule						
Translate DNS replies that match this rule							
Direction: Both							
Description:							
OK Cancel Help							

驗證第二個完成的NAT/PAT規則是否如下所示:在匹配條件中:Original Packet area,驗證 以下值:源介面=內部源地址= OBJ\_SPECIFIC\_192-168-1-0目的地址=外部服務=任意在 Action:Translated Packet area,驗證以下值:源NAT型別=動態PAT(隱藏)源地址= 10.1.5.5目的地位址=原始服務=原始按一下「OK」(確定)。完整的NAT配置將出現在 ASDM中,如下圖所示

:

Co	nfiguration > Firewall	> NAT Rules						
4	💠 Add 👻 📝 Edit 📋 Delete 🔶 🗲 👗 🗈 🛍 - 🔍 Find 🖭 Diagram 💐 Packet Trace							
	* Match Criteria: Original Packet			Action: Translated Packet				
Ľ	Source Intf Dest Intf	f Source	Destination	Service	Source	Destination	Servic	
	inside outside	B OBJ_GENER	🧐 any	🧐 any	outside (P)	Original	Orignal	
	inside outside	GA OBJ_SPECIF	🧇 any	🧇 any	🔜 10.1.5.5 (P)	Original	Original -	
	"Network Object" NAT (I	No rules)						
4							Þ	
	Apply Reset							

3. 按一下「**Apply**」按鈕,將變更應用到運行配置。 這將完成思科自適應安全裝置(ASA)上的動態PAT配置。

# <u>驗證</u>

使用本節內容,確認您的組態是否正常運作。

<u>輸出直譯器工具</u>(僅供<u>已註冊</u>客戶使用)(OIT)支援某些**show**命令。使用OIT檢視**show**命令輸出的分析 。

## <u>檢驗通用PAT規則</u>

• show local-host — 顯示本地主機的網路狀態。 ASA#**show local-host** Interface outside: 1 active, 2 maximum active, 0 denied local host: <125.252.196.170>, TCP flow count/limit = 2/unlimited TCP embryonic count to host = 0TCP intercept watermark = unlimited UDP flow count/limit = 0/unlimited !--- The TCP connection outside address corresponds !--- to the actual destination of 125.255.196.170:80 Conn: TCP outside 125.252.196.170:80 inside 192.168.0.5:1051, idle 0:00:03, bytes 13758, flags UIO TCP outside 125.252.196.170:80 inside 192.168.0.5:1050, idle 0:00:04, bytes 11896, flags UIO Interface inside: 1 active, 1 maximum active, 0 denied local host: <192.168.0.5>, TCP flow count/limit = 2/unlimited TCP embryonic count to host = 0TCP intercept watermark = unlimited UDP flow count/limit = 0/unlimited

```
!--- The TCP PAT outside address corresponds to the !--- outside IP address of the ASA -
 10.1.5.1. Xlate: TCP PAT from inside:192.168.0.5/1051 to outside:10.1.5.1/32988 flags
           ri idle 0:00:17 timeout 0:00:30
     TCP PAT from inside:192.168.0.5/1050 to outside:10.1.5.1/17058 flags
           ri idle 0:00:17 timeout 0:00:30
   Conn:
     TCP outside 125.252.196.170:80 inside 192.168.0.5:1051, idle 0:00:03,
           bytes 13758, flags UIO
     TCP outside 125.252.196.170:80 inside 192.168.0.5:1050, idle 0:00:04,
          bytes 11896, flags UIO
• show conn — 顯示指定連線型別的連線狀態。
 ASA#show conn
 2 in use, 3 most used
 TCP outside 125.252.196.170:80 inside 192.168.0.5:1051, idle 0:00:06,
           bytes 13758, flags UIO
 TCP outside 125.252.196.170:80 inside 192.168.0.5:1050, idle 0:00:01,
          bytes 13526, flags UIO
• show xlate — 顯示有關轉換插槽的資訊。
 ASA#show xlate
 4 in use, 7 most used
 Flags: D - DNS, I - dynamic, r - portmap, s - static, I - identity,
           T - twice
 TCP PAT from inside:192.168.0.5/1051 to outside:10.1.5.1/32988 flags
           ri idle 0:00:23 timeout 0:00:30
 TCP PAT from inside:192.168.0.5/1050 to outside:10.1.5.1/17058 flags
           ri idle 0:00:23 timeout 0:00:30
```

#### <u>驗證特定PAT規則</u>

```
• show local-host — 顯示本地主機的網路狀態。
 ASA#show local-host
 Interface outside: 1 active, 2 maximum active, 0 denied
 local host: <125.252.196.170>,
     TCP flow count/limit = 2/unlimited
     TCP embryonic count to host = 0
     TCP intercept watermark = unlimited
     UDP flow count/limit = 0/unlimited
  !--- The TCP connection outside address corresponds to !--- the actual destination of
 125.255.196.170:80. Conn: TCP outside 125.252.196.170:80 inside 192.168.1.5:1067,
           idle 0:00:07, bytes 13758, flags UIO
     TCP outside 125.252.196.170:80 inside 192.168.1.5:1066,
           idle 0:00:03, bytes 11896, flags UIO
 Interface inside: 1 active, 1 maximum active, 0 denied
 local host: <192.168.0.5>,
     TCP flow count/limit = 2/unlimited
     TCP embryonic count to host = 0
     TCP intercept watermark = unlimited
     UDP flow count/limit = 0/unlimited
  !--- The TCP PAT outside address corresponds to an !--- outside IP address of 10.1.5.5.
 Xlate: TCP PAT from inside:192.168.1.5/1067 to outside:10.1.5.5/35961 flags
           ri idle 0:00:17 timeout 0:00:30
     TCP PAT from inside:192.168.1.5/1066 to outside:10.1.5.5/23673 flags
           ri idle 0:00:17 timeout 0:00:30
   Conn:
     TCP outside 125.252.196.170:80 inside 192.168.1.5:1067, idle 0:00:07,
```

TCP outside 125.252.196.170:80 inside 192.168.1.5:1066, idle 0:00:03,

bytes 13758, flags UIO

bytes 11896, flags UIO

#### • show conn — 顯示指定連線型別的連線狀態。

ASA#**show conn** 2 in use, 3 most used TCP outside 125.252.196.170:80 inside 192.168.1.5:1067, idle 0:00:07, bytes 13653, flags UIO TCP outside 125.252.196.170:80 inside 192.168.1.5:1066, idle 0:00:03, bytes 13349, flags UIO

#### • show xlate — 顯示有關轉換插槽的資訊。

ASA#**show xlate** 

3 in use, 9 most used

Flags: D - DNS, I - dynamic, r - portmap, s - static, I - identity, T - twice

TCP PAT from inside:192.168.1.5/1067 to outside:10.1.5.5/35961 flags ri idle 0:00:23 timeout 0:00:30

TCP PAT from inside:192.168.1.5/1066 to outside:10.1.5.5/29673 flags ri idle 0:00:23 timeout 0:00:30

# 疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

# 相關資訊

- 思科調適型資安裝置管理員
- <u>Cisco ASA 5500系列調適型安全裝置</u>
- <u>要求建議 (RFC)</u>
- 技術支援與文件 Cisco Systems