# 使用NAT配置ASA版本9埠轉發

# 目錄

簡介 必要條件 需求 採用元件 設定 網路圖表 允許內部主機通過PAT訪問外部網路 允許內部主機通過NAT訪問外部網路 允許不受信任的主機訪問受信任網路中的主機 靜態身份NAT 使用靜態的連線埠重新導向(轉送) 驗證 連線 系統日誌 **Packet Tracer** CAPTURE 疑難排解

<u>相關資訊</u>

# 簡介

本文說明如何使用CLI或調適型安全裝置管理員(ASDM),在調適型安全裝置(ASA)軟體版本9.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。

請參閱<u>Cisco ASA系列防火牆ASDM配置指南</u>瞭解更多資訊。

# 必要條件

## 需求

請參閱<u>配置管理訪問</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 ASA 5525系列安全裝置軟體版本9.x及更高版本

• ASDM 7.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。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。」

# 設定

#### 網路圖表



此配置中使用的IP地址方案在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。

#### 允許內部主機通過PAT訪問外部網路

如果您希望內部主機共用一個公共地址進行轉換,請使用埠地址轉換(PAT)。 最簡單的PAT配置之 一涉及將所有內部主機轉換為類似於外部介面IP地址。當ISP提供的可路由IP地址的數量限製為少數 幾個或只有一個時,通常使用這種PAT配置。

完成以下步驟,以允許內部主機使用PAT訪問外部網路:

1. 選擇Configuration > Firewall > NAT Rules。按一下Add,然後選擇Network Object以配置動態 NAT規則。

Monitoring 🔚 Save 🔇 Refresh 🔇 Back 🜔	Forward 🦻 Help CISCO
Configuration > Firewall > NAT Rules	Addresses Services
💠 Add 🗸 🌈 Edit 🎁 Delete 🛧 🖌 👗 🖿	Addresses 과 무 ×
Match Criteria: Original Packet	🕈 Add 🗸 🗹 Edit 📋 Delete 🔍 Where Used 🔍 Not Use
# Source Intf Dest Intf Source	Network Object
"Network Object" NAT (Rule 1)	Network Object Group
1 Any outside 🛃 Inside_h	- Network Objects
	- 🏟 any
	- 🧼 any4
	🚽 🛶 🦚 any6

2. 配置需要動態PAT的網路/主機/範圍。在此示例中,已選擇一個內部子網。對於要以此方式轉換的其他子網,可重複此過程。

🕫 Add Networ	k Object 🛛 🔀	
Name:	obj_172.16.11.0	
Туре:	Network	
IP Version:	⊙ IPv4 ○ IPv6	
IP Address:	172.16.11.0	
Netmask:	255.255.2	
Description:		
NAT	8	
	OK Cancel Help	

3. 展開NAT。選中Add Automatic Address Translation Rules覈取方塊。在「型別」下拉選單中 ,選擇**動態PAT(隱藏)**。 在Translated Addr欄位中,選擇反映外部介面的選項。按一下「 Advanced」。

NEWOR	s un er r
11010001	

📧 Add Networl	k Object 🛛	×
Name:	obi 172.16.11.0	1
Type:	Network	
.IP Version:		IJ
IP Address	172 16 11 0	
Notroacku	255 255 255 0	
Neunask:	255.255.255.0	
Description:		1
NAT	۲	
🔽 Add Automa	atic Address Translation Rules	
Type:	Dynamic PAT (Hide) 🐱	
Translated Ac	ddr: outside	
Use one-t	to-one address translation	
PAT Pool	Translated Address:	
Round	Robin	
Extend	PAT uniqueness to per destination instead of per interface	
🔄 Transla	te TCP and UDP ports into flat range 1024-65535 👘 Include range 1-1023	
🔄 Fall throu	igh to interface PAT(dest intf): backup	
Use IPv6	for interface PAT	
	Advanced	
	OK Cancel Help	

4. 在Source Interface和Destination Interface下拉選單中,選擇適當的介面。按一下**OK**,然後按 一下Apply以使更改生效。

🐻 Advanced NAT Set	ttings	×
Translate DNS repli	es for rule	
Interface		
Source Interface:	inside 💉	
Destination Interface:	outside 💌	
ОК	Cancel Help	

這是此PAT配置的等效的CLI輸出:

object network obj\_172.16.11.0 subnet 172.16.11.0 255.255.255.0 nat (inside,outside) dynamic interface

## 允許內部主機通過NAT訪問外部網路

您可以通過配置動態NAT規則,允許一組內部主機/網路訪問外部世界。與PAT不同,動態NAT從地 址池分配轉換的地址。因此,一台主機對映到其自己的轉換IP地址,兩台主機不能共用同一個轉換 IP地址。

為此,您需要選擇要授予訪問許可權的主機/網路的實際地址,然後必須將其對映到已轉換的IP地址 池。

完成以下步驟,以允許內部主機通過NAT訪問外部網路:

1. 選擇Configuration > Firewall > NAT Rules。按一下Add,然後選擇Network Object以配置動態 NAT規則。

Monitoring 🔚 Save 🔇 Refresh 🔇 Back 🚫	Forward 🦻 Help	CISCO
Configuration > Firewall > NAT Rules	Addresses Services	
💠 Add 🗸 📝 Edit 🏛 Delete 🛧 🗲 👗 🖿	Addresses	а т ×
#         Match Criteria: Original Packet           #         Source Intf         Dest Intf         Source	<ul> <li>♣ Add ▼</li></ul>	re Used <b>Q</b> Not Used
1 Any outside Birside_h	·Network Objects ··· ·· ··· ··· ··· ··· ··· ··· ···· ····	

## 2. 配置需要動態PAT的網路/主機/範圍。在本示例中,已選擇整個內部網路。

🕫 Add Networ	k Object	$\times$
Name:	obj_172.16.11.0	
Туре:	Network	~
IP Version:	⊙ IPv4 ○ IPv6	
IP Address:	172.16.11.0	
Netmask:	255.255.255.0	~
Description:		
NAT	8	Σ
	OK Cancel Help	

3. 展開NAT。選中Add Automatic Address Translation Rules覈取方塊。在「型別」下拉式清單 中選擇「動態」。在Translated Addr欄位中,選擇適當的選項。按一下「Advanced」。

📴 Edit Networ	k Object 🛛 🔀
*	
Name:	obj_172.16.11.0
Туре:	Network
IP Version:	⊙ IPv4 ○ IPv6
IP Address:	172.16.11.0
Netmask:	255.255.255.0
Description:	
NAT	۲
🔽 Add Autom	atic Address Translation Rules
Туре:	Dynamic 💌
Translated A	ddr:
Use one-	to-one address translation
PAT Pool	Translated Address:
Round	Robin
Extend	PAT uniqueness to per destination instead of per interface
🔄 Transla	ate TCP and UDP ports into flat range 1024-65535 👘 Include range 1-1023
🔄 Fall throu	ugh to interface PAT(dest intf): backup
Use IPv6	for interface PAT
	Advanced
	OK Cancel Help

4. 按一下Add以新增網路對象。在「型別」下拉選單中,選擇「範圍」。在Start Address和End Address欄位中,輸入起始和結束PAT IP地址。按一下「OK」(確定)。

📧 Add Networ	k Object 🛛 🔀
Name:	obj-my-range
Туре:	Range
IP Version:	⊙ IPv4 🔿 IPv6
Start Address:	203.0.113.10
End Address:	203.0.113.20
Description:	
NAT	<ul> <li>(\$)</li> </ul>
	OK Cancel Help

5. 在Translated Addr欄位中,選擇地址對象。按一下Advanced以選擇來源介面和目的地介面。

🥫 Edit Networ	k Object	×
Name:	obi 172 16 11 0	7
Tupor	Notwork	
Type:		
IP Version:	<ul> <li>● IPv4</li> <li>● IPv6</li> </ul>	_
IP Address:	172.16.11.0	
Netmask:	255.255.255.0	1
Description:		
NAT	*	4
Add Autom	atic Address Translation Rules	
Type:	Dynamic 🔽	
Translated A	ddr: obj-my-range	]
Use one-	to-one address translation	
PAT Pool	Translated Address:	
Round	Robin	
Extend	PAT uniqueness to per destination instead of per interface	
🔄 Transla	ate TCP and UDP ports into flat range 1024-65535 📃 Include range 1-1023	
🔄 Fall throu	ugh to interface PAT(dest intf): backup	
Use IPv6	for interface PAT	
	Advanced	
	OK Cancel Help	

6. 在Source Interface和Destination Interface下拉選單中,選擇適當的介面。按一下**OK**,然後按 一下**Apply**以使更改生效。

🐻 Advanced NAT Set	ttings	×
Translate DNS repli	es for rule	
Interface		-
Source Interface:	inside 🛛 👻	•
Destination Interface:	outside 💌	•
ОК	Cancel Help	

這是此ASDM配置的等效的CLI輸出:

object network obj-my-range range 203.0.113.10 203.0.113.20

object network obj\_172.16.11.0 subnet 172.16.11.0 255.255.255.0 nat(inside,outside) dynamic obj-my-range

根據此配置,172.16.11.0網路中的主機將轉換為NAT池(203.0.113.10 - 203.0.113.20)中的任何IP地 址。如果對映池的地址少於實際組的地址,則地址可能會用盡。因此,您可以嘗試使用動態PAT備 份實施動態NAT,也可以嘗試擴展當前池。

1. 在先前的配置中重複步驟1到3,然後再次按一下**Add**以新增網路對象。在「型別」下拉選單中 ,選擇**主機**。在IP Address欄位中,輸入PAT備份IP地址。按一下「**OK**」(確定)。

📧 Add Networ	k Object	×
• Name: (optional)	obj-pat-ip	
Туре:	Host	*
IP Version:	⊙ IPv4 ○ IPv6	
IP Address:	203.0.113.21	
Netmask:	255.255.255.0	*
FQDN:		
Description:		
NAT	8	
	OK Cancel Help	

2. 按一下Add以新增網路對象組。在Group Name欄位中,輸入組名稱,並在組中同時新增兩個 地址對象(NAT範圍和PAT IP地址)。

🔁 A	dd Netw	ork Object	Group						
Gro	up Name:	nat-pat-group	,						
Des	cription:								
•	Existing Ne	stwork Objects	s/Groups:				Members in Group:	1D Addees	Kisto ad Deaffert
	Name	±1	IP Address	Netmask	Description		Ivane	IP Address	Netmaskerenct
	<ul> <li>Network</li> </ul>	rk Objects					obj-pat-ip	203.0.113.21	
	- 4	any					🚽 🚅 obj-my-range	203.0.113.10-203.0	
	- 4	any4							
	- 4	any6							
		inside-net	19.19.19.0	255.255.255.0					
	ي ا	obj_172.1	172.16.11.0	255.255.255.0					
						Add >>			
						<< Remove			
					100				

3. 選擇配置的NAT規則,並將Translated Addr更改為新配置的組「nat-pat-group」(以前為「 obj-my-range」)。 按一下「**OK**」(確定)。

Name       Network Objects	▲ 1 IP Address	Netmask	Description	Filter Clear
Network Objects	- · IF Address	Neuridsk	Describuon	C MAAGE BLO L O DEFAGE
- B obj-pat-ip				Object NAT Address
- 🖪 obj-pat-ip	203.0.113.10-203			
	203.0.113.21			
-Network Object (	Groups			
🔳 🚮 nat-pat-g	h			
😑 Interfaces				
🔤 backup				
🔤 inside				
🔤 outside				
Selected Translated	Addr			
Translated Add	r -> nat-pat-group			

4. 按一下OK以新增NAT規則。按一下Advanced以選擇來源介面和目的地介面。

📧 Edit Networ	k Object 🛛 🔀
News	
Name:	ODj_1/2.16.11.0
Type: 💦	Network
IP Version:	⊙ IPv4 ○ IPv6
IP Address:	172.16.11.0
Netmask:	255.255.255.0
Description:	
NAT	۸
🔽 Add Automa	atic Address Translation Rules
Type:	Dynamic 🖌
Translated A	ddr: nat-pat-group
Use one-	to-one address translation
PAT Pool	Translated Address:
Round	Robin
Extend	PAT uniqueness to per destination instead of per interface
🔄 Transla	ate TCP and UDP ports into flat range 1024-65535 📃 Include range 1-1023
🔄 Fall throu	gh to interface PAT(dest intf): backup
Use IPv6	for interface PAT
	Advanced
	OK Cancel Help

5. 在Source Interface和Destination Interface下拉選單中,選擇適當的介面。按一下「OK」(確 定)。

🖼 Advanced NAT Settings 🛛 🛛 🔀						
Translate DNS replies for rule						
Interface						
Source Interface:	inside 🛛 🗸 🗸					
Destination Interface:	outside 💌					
ОК	Cancel Help					

6. 按一下Apply以使更改生效。

	Home 🦓 Configuration 📴 M	Monitorir	•	🛛 Save 🔇 Re	afresh 🔇 E	Sack 🚫 Forward 💡	Ныр	CISCO	
	Firewall 🗗	÷	Con	figuration > Fi	rewall > NAT	Rules 🗆	Addresses Services		
e Us	Access Rules	_		Add - 🏹 Edit	👔 Delete 👍	- 4日本 昭一	Addresses	с н х С	
Devic	MAT Rules		Match Criteria: Original Packet			Packet	💠 Add - 📷 Edit 🏢 Delste 🔍 Where Used 🔍 Not Us		
	Device Setup		~	Source Intf	Dest Intf	Source	Fiker:	Filter Clear	
	Frowall			"Network Object" NAT (Rule 1)			Name 🔺 1		
				l inside	outside	📲 obj_172.16	Network Objects	~	
	Remote Access VPN						- 🎱 any		
	2 Site-to-Site VPN						- 🎱 any4		
	90	_	1			N	- 🎱 anyó	E	
	Device Management					<u>e</u>	- 📸 inside-network/24		
		30				(equit	- 📸 obj-my-range		
		-		-		10001	і- 🚮 obj_172.16.11.0	~	

#### 這是此ASDM配置的等效的CLI輸出:

object network obj-my-range range 203.0.113.10 203.0.113.20

object network obj-pat-ip
host 203.0.113.21

object-group network nat-pat-group network-object object obj-my-range network-object object obj-pat-ip

object network obj\_172.16.11.0 subnet 172.16.11.0 255.255.255.0

## 允許不受信任的主機訪問受信任網路中的主機

這可以通過應用靜態NAT轉換和允許這些主機的訪問規則來實現。每當外部使用者想要訪問位於內 部網路中的任何伺服器時,都需要進行此項配置。內部網路中的伺服器可以擁有不可在Internet上路 由的專用IP地址。因此,您需要通過靜態NAT規則將該私有IP地址轉換為公有IP地址。假設您有一 個內部伺服器(172.16.11.5)。為了讓此功能正常工作,您需要將此專用伺服器IP地址轉換為公共 IP地址。本示例說明如何實施雙向靜態NAT以將172.16.11.5轉換為203.0.113.5。

1. 選擇Configuration > Firewall > NAT Rules。按一下Add,然後選擇Network Object以配置靜態 NAT規則。展開NAT。

📧 Add Networ	k Object 🛛 💽	
News	-F: 170.16.11.5	
Name:	00]_172.16.11.5	
Туре:	Host	
IP Version:	● IPv4 ○ IPv6	
IP Address:	172.16.11.5	
Description:		
NAT	♥	
	OK Cancel Help	

 2. 選中Add Automatic Address Translation Rules覈取方塊。在「型別」下拉選單中,選擇「靜 態」。在Translated Addr欄位中,輸入IP地址。按一下Advanced以選擇來源介面和目的地介 面。

🔚 Add Networ	k Object 🛛 🛛 🔀						
Name:	obj_172.16.11.5						
Туре:	Host						
IP Version:	⊙ IPv4 ○ IPv6						
IP Address:	172.16.11.5						
Description:							
NAT	🔊						
Add Automa	atic Address Translation Rules						
Туре:	Static						
Translated Ac	idr: 203.0.113.5						
🔽 Use one-t	to-one address translation						
PAT Pool	Translated Address:						
Round	Robin						
Extend	PAT uniqueness to per destination instead of per interface						
Transla	te TCP and UDP ports into flat range 1024-65535 📄 Include range 1-1023						
🔄 Fall throu	gh to interface PAT(dest intf): backup						
Use IPv6	for interface PAT						
	Advanced						
	OK Cancel Help						

3. 在Source Interface和Destination Interface下拉選單中,選擇適當的介面。按一下「OK」(確 定)。

🖼 Advanced NAT Settings 🛛 🛛 🔀						
Translate DNS replies for rule						
Interface						
Source Interface:	inside 🛛 🗠					
Destination Interface:	outside 💌					
ОК	Cancel Help					

4. 您可以在此處看到配置的靜態NAT條目。按一下Apply以將此命令傳送到ASA。

	Match Crite	ria: Original	Packet			Action: Translated Packet			
F	Source Intf	Dest Intf	Source	Destination	Service	Source	Destination	Service	
"N	etwork Object"	NAT (Rule 1)							
1	inside	outside	🖳 obj_172.16	🌍 any	🥥 any	📇 203.0.113.5 (S)	Original	Original	
	outside	inside	🏟 any	3 203.0.113.5	🏟 any	Original (S)	🖪 obj_172.16	Original	

以下是此NAT配置的等效的CLI輸出:

object network obj\_172.16.11.5
host 172.16.11.5
nat (inside,outside) static 203.0.113.5

## 靜態身份NAT

NAT豁免是一個有用的功能,內部使用者可以在不完成NAT的情況下嘗試訪問遠端VPN主機/伺服器 或ASA的任何其他介面後託管的一些主機/伺服器。為此,內部伺服器(具有私有IP地址)可以轉換 為自己的身份,從而允許其訪問執行NAT的目標。 在本示例中,內部主機172.16.11.15需要訪問遠端VPN伺服器172.20.21.15。

完成以下步驟,在完成NAT後,允許內部主機訪問遠端VPN網路:

1. 選擇Configuration > Firewall > NAT Rules。按一下Add以配置NAT豁免規則。



2. 在Source Interface和Destination Interface下拉選單中,選擇適當的介面。在「源地址」欄位 中,選擇適當的條目。

🔄 Add NAT Rule						×
Match Criteria: Original Packet						
Source Interface:	inside		🔽 Des	tination Interface:	outside	~
Source Address:	any		Des	tination Address:	any	···
			Ser	vice:	any	
Action: Translated Packet						
Source NAT Type:	Static	🖬 Browse (	Original	Source Addres	s	
Source Address:	Origina					
Use one-to-one address transla	ation	🔂 Add	🗕 📝 Edit	📋 Delete 🛛 🔍	Where Used 🔍 N	ot Used
PAT Pool Translated Address:		Filter:				
Round Robin		Name		1 IP Address		Netmask
Extend PAT uniqueness to pe	er destinal	L- Ketwo	rk Objects Lany			
Translate TCP and UDP ports	; into flat r			'		
Fall through to interface PAT						
Use IPv6 for source interface F	'AT					
Options						
🔽 Enable rule						
Translate DNS replies that mate	th this rule					

#### 3. 按一下Add以新增網路對象。配置主機IP地址。

📧 Add Netwo	rk Object 🛛 🔀
Name:	obj_172.16.11.15
Туре:	Host
IP Version:	⊙ IPv4 ○ IPv6
IP Address:	172.16.11.15
Description:	
NAT	
NAT	
	OK Cancel Help

4. 同樣,瀏覽目**的地地址**。按一下Add以新增網路對象。配置主機IP地址。

📧 Add Netwo	rk Object	
Name: Type: IP Version: IP Address:	<pre>pbj_172.20.21.15 Host</pre>	~
Description:		
NAT		۲
	OK Cancel Help	

5. 選擇已配置的源地址和目標地址對象。選中Disable Proxy ARP on egress interface和Lookup route table to locate egress interface覈取方塊。按一下「OK」(確定)。

📧 Add NAT Rule				×	
Match Criteria: Original Packet					
Source Interface:	inside 💌	Destination Interface:	outside	~	
Source Address:	obj_172.16.11.15	Destination Address:	obj_172.20.21.15		
		Service:	any		
Action: Translated Packet					
Source NAT Type:	Static 💌				
Source Address:	Original 📰	Destination Address:	Original		
🔲 Use one-to-one address transla	ation				
PAT Pool Translated Address:		Service:	Original		
Round Robin					
Extend PAT uniqueness to pe	er destination instead of per int	erface			
Translate TCP and UDP ports	into flat range 1024-65535	Include range 1-1023	3		
Fall through to interface PAT					
Use IPv6 for source interface P	AT	Use IPv6 for destin	ation interface PAT		
Options					
🗹 Enable rule					
Translate DNS replies that mate	h this rule				
✓ Disable Proxy ARP on egress interface					
Lookup route table to locate egress interface					
Direction: Both					
Description:					
OK Cancel Help					

6. 按一下Apply以使更改生效。

🗞 Configuration 📴 Monitoring 🔚 Save 🔇 Refresh 🔇 Back 🚫 Forward 🢡 Help							
a e 🔀	Confi	guration > Fire	wall > NAT R	tules.		Addresses	ŋ
ess Rules	💠 A	dd 🔻 🗃 Edit 🕯	🖹 Delete 🛉	4日本 南島・	Q, Find	🗣 Add 👻 🎬 Edit 🏢 Delete 🔍 Where Used 🔍	
rice Policy Rules		Match Criter	ria: Original P	acket		Fiter:	Fi
(Rules	*	Source Intf	Dest Intf	Source	Destina	Name	
r Rules	1	inside	outside	🖪 obj_172.16	🔳 obj_	<ul> <li>Network Objects</li> </ul>	
e Setup	"N	"Network Object" NAT (No rules)				- 🧇 any	
						- 🏟 any4	
al						- 🏈 any6	
te Access VPN						- 🚎 inside-network/24	
						- 📇 obj_172.16.11.15	
to-Site VPN						🔳 obj_172.20.21.15	
e <u>M</u> anagement	<	11			>		
ě			Apply	Reset			

這是NAT豁免或身份NAT配置的等效的CLI輸出:

object network obj\_172.16.11.15 host 172.16.11.15 object network obj\_172.20.21.15 host 172.20.21.15

nat (inside,outside) source static obj\_172.16.11.15 obj\_172.16.11.15
destination static obj\_172.20.21.15 obj\_172.20.21.15 no-proxy-arp route-lookup

## 使用靜態的連線埠重新導向(轉送)

埠轉發或埠重定向是一項有用的功能,外部使用者可嘗試訪問特定埠上的內部伺服器。為此,內部伺服器(具有私有IP地址)可以轉換為公有IP地址,從而允許特定埠訪問。

在本例中,外部使用者想要訪問埠25上的SMTP伺服器203.0.113.15。這可通過兩個步驟完成:

1. 將埠25上的內部郵件伺服器172.16.11.15轉換為埠25上的公共IP地址203.0.113.15。

2. 允許訪問埠25上的公共郵件伺服器203.0.113.15。

當外部使用者嘗試訪問埠25上的伺服器203.0.113.15時,此流量將重定向到埠25上的內部郵件伺服 器172.16.11.15。

1. 選擇Configuration > Firewall > NAT Rules。按一下Add,然後選擇Network Object以配置靜態 NAT規則。

Monitoring	Ionitoring 🔚 Save 🔇 Refresh 🔇 Back 🚫 Forward 🦓 Help CISCO						
Confi	quration > Fi	rewall > NAT	Rules 🗆	Addresses Services			
4 <b>4</b> A	dd 👻 📝 Edit	🗊 Delete 🖪	- ∡ X ⊫	Addresses	ъъ×		
	Match Crit	eria: Original	Packet	🖶 Add 🔻 🕜 Edit 📋 Delete 🔍 Wher	re Used 🔍 Not Used		
#	Source Intf	Dest Intf	Source	Network Object	Filter Clear		
🖃 "N	etwork Object"	NAT (Rule 1)		Network Object Group	<u>▲</u> 1		
1	Any	outside	🛃 Inside_h	■ Network Objects			
				- 🏟 any			
				- 🌍 any4			
				- 🌍 any6			

🖬 Edit Network Object 🛛 🔀				
Name:	obj_172.16.11.15			
Туре:	Host			
IP Version:	⊙ IPv4 🔿 IPv6			
IP Address:	172.16.11.15			
Description:				
NAT	(S)			
	OK Cancel Help			

3. 展開NAT。選中Add Automatic Address Translation Rules覈取方塊。在「型別」下拉式清單 中選擇「靜態」。在Translated Addr欄位中,輸入IP地址。按一下Advanced以選擇服務和來 源及目的地介面。

📧 Edit Network Object 🛛 🛛 🔀				
Namer	obi 172 16 11 15	7		
Turne.	00_1/2.10.11.15			
iype:	Host			
IP Grsion:	⊙ IPv4 ○ IPv6			
IP Address:	172.16.11.15			
Description:				
NAT	\$			
🔽 Add Automa	atic Address Translation Rules			
Type:	Static 💌			
Translated Ac	ddr: 203.0.115.15			
Use one-l	to-one address translation			
PAT Pool	Translated Address:			
Round	Robin			
Extend	PAT uniqueness to per destination instead of per interface			
Translate TCP and UDP ports into flat range 1024-65535 Include range 1-1023				
Fall through to interface PAT(dest intf): backup				
Use IPv6 for interface PAT				
Advanced				
OK Cancel Help				

4. 在Source Interface和Destination Interface下拉選單中,選擇適當的介面。配置服務。按一下「OK」(確定)。

🖼 Advanced NAT Settings 🛛 🛛 🔀							
Translate DNS repli	Translate DNS replies for rule						
Disable Proxy ARP	on egress interface						
Lookup route table	to locate egress interface						
Interface							
Source Interface:	inside 💌						
Destination Interface:	outside 💌						
Service							
Protocol:	🚥> tcp 🛛 👻						
Real Port:	smtp						
Mapped Port:	smtp						
OK Cancel Help							

#### 5. 按一下Apply以使更改生效。

07 P	Configuration > Firewall > NAT Rules					Addresses c
^	💠 Add 🗸 🧭 Edit 📋 Delete 🎓 🌾 🐰 ங 💼 - 🔍 Find			<b>€</b>  ≵ <b>№</b> ₿.	💠 Add 🔻 🗹 Edit 📋 Delete 🔍 Where Used 🕻	
		Match Criteria: Original Packet				Filter:
~	#	Source Intf	Dest Intf	Source	Destina	Name
	🗆 "N	etwork Object" I	VAT (Rule 1)			-Network Objects
	1	inside	outside	📕 obj_172.16	🉁 any	🧼 any
		outside	inside	🏟 any	르, 203.	🧼 any4
						🧼 any6
						- 🚰 inside-network/24
						🔜 obj_172.16.11.15
						· 🖳 203.0.115.15
	<	ш )			>	
÷			Apply	Reset		

以下是此NAT配置的等效的CLI輸出:

object network obj\_172.16.11.15
host 172.16.11.15
nat (inside,outside) static 203.0.113.15 service tcp smtp smtp

驗證

使用本節內容,確認您的組態是否正常運作。

<u>Cisco CLI Analyzer(僅供已註冊客戶使用)支援某些 show</u> 指令。使用 Cisco CLI Analyzer 檢視

#### show 指令輸出的分析。

使用Web瀏覽器通過HTTP訪問網站。此示例使用託管在198.51.100.100的站點。如果連線成功 ,則可在ASA CLI上看到此輸出。

#### 連線

ASA(config)# **show connection address 172.16.11.5** 6 in use, 98 most used TCP outside 198.51.100.100:80 inside 172.16.11.5:58799, idle 0:00:06, bytes 937, flags UIO

ASA是有狀態防火牆,並且允許來自Web伺服器的返回流量通過防火牆,因為它與防火牆連線表中 的連**接**。與預先存在的連線匹配的流量允許通過防火牆,不會被介面ACL阻止。

在前面的輸出中,內部介面上的客戶端已經從外部介面建立了到198.51.100.100主機的連線。此連 線是使用TCP協定建立並且已空閒六秒。連線標誌指示此連線的當前狀態。有關連線標誌的詳細資 訊,請參閱ASA TCP連線標誌。

#### 系統日誌

ASA(config)# show log | in 172.16.11.5

Apr 27 2014 11:31:23: %ASA-6-305011: Built dynamic TCP translation from inside: 172.16.11.5/58799 to outside:203.0.113.2/58799

Apr 27 2014 11:31:23: %ASA-6-302013: Built outbound TCP connection 2921 for outside: 198.51.100.100/80 (198.51.100.100/80) to inside:172.16.11.5/58799 (203.0.113.2/58799)

ASA防火牆在正常運行期間生成系統日誌。系統日誌的範圍取決於日誌記錄配置。輸出顯示在級別 6或「資訊」級別上可見的兩個系統日誌。

在此示例中,生成了兩個系統日誌。第一個是指示防火牆已建立轉換(尤其是動態TCP轉換 [PAT])的日誌消息。 它表示流量從內部到外部介面傳輸時的源IP地址和埠以及轉換後的IP地址和 埠。

第二個系統日誌表示防火牆在其連線表中為客戶端和伺服器之間的此特定流量建立了連線。如果防 火牆配置為阻止此連線嘗試,或者某個其他因素阻止了此連線的建立(資源限制或可能的配置錯誤 ),則防火牆不會生成指示已建立連線的日誌。相反,它將記錄拒絕連線的原因,或有關禁止建立 連線的因素的指示。

#### **Packet Tracer**

ASA(config)# packet-tracer input inside tcp 172.16.11.5 1234 198.51.100.100 80

--Omitted--

Result: input-interface: inside input-status: up input-line-status: up output-interface: outside output-status: up ASA上的Packet Tracer功能允許您指定*模擬*資料包,並檢視防火牆處理流量時執行的所有各種步驟 、檢查和功能。使用此工具,識別您認為可以允許通過防火牆的流量范*例,並使用*該5元組來模擬流 量會非常有用。在上一個示例中,使用Packet Tracer模擬符合以下條件的連線嘗試:

- 模擬資料包到達內部。
- 使用的協定是TCP。
- •模擬客戶端IP地址為172.16.11.5。
- 使用者端會傳送源自連線埠1234的流量。
- •流量將發往IP地址為198.51.100.100的伺服器。
- •流量將傳至連線埠80。

請注意,命令中沒有提到外部介面。這是通過Packet Tracer設計的。該工具將告訴您防火牆如何處 理該型別的連線嘗試,包括它將如何路由它以及從哪個介面發出。有關Packet Tracer的詳細資訊 ,請參閱使用Packet Tracer跟蹤資料包。

#### CAPTURE

#### 應用捕獲

ASA# capture capin interface inside match tcp host 172.16.11.5 host 198.51.100.100 ASA# capture capout interface outside match tcp any host 198.51.100.100

#### ASA#show capture capin

3 packets captured

1: 11:31:23.432655 172.16.11.5.58799 > 198.51.100.100.80: S 780523448: 780523448(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK> 2: 11:31:23.712518 198.51.100.100.80 > 172.16.11.5.58799: S 2123396067: 2123396067(0) ack 780523449 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8> 3: 11:31:23.712884 172.16.11.5.58799 > 198.51.100.100.80: . ack 2123396068 win 32768

#### ASA#**show** capture capout

3 packets captured

1: 11:31:23.432869 203.0.113.2.58799 > 198.51.100.100.80: S 1633080465: 1633080465(0) win 8192 <mss 1380,nop,wscale 2,nop,nop,sackOK> 2: 11:31:23.712472 198.51.100.100.80 > 203.0.113.2.58799: S 95714629: 95714629(0) ack 1633080466 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8> 3: 11:31:23.712914 203.0.113.2.58799 > 198.51.100.100.80: . ack 95714630 win 32768/pre>

ASA防火牆可以捕獲進入或離開其介面的流量。此捕獲功能非常棒,因為它可以明確證明流量是到 達防火牆還是離開防火牆。上例顯示了分別在內外部介面上配置兩個名為capin和capout的捕獲。 capture命令使用match關鍵字,允許您具體說明要捕獲的流量。

對於捕獲,您指示想要匹配在與TCP主機172.16.11.5主機198.51.100.100匹配的內部介面(入口或 出口)上看到的流量。換句話說,您要捕獲從主機172.16.11.5傳送到主機198.51.100.100的任何 TCP流量,或者反之亦然。使用match關鍵字允許防火牆雙向捕獲該流量。為外部介面定義的 capture命令不引用內部客戶端IP地址,因為防火牆在該客戶端IP地址上執行PAT。因此,您無法與 該客戶端IP地址匹配。相反,此示例使用any來表示所有可能的IP地址都將與該條件匹配。 設定擷取後,您會嘗試再次建立連線,並繼續使用**show capture** *<capture\_name>* 指令檢視擷取。 在此範例中,您可以看到使用者端能夠連線到伺服器,從擷取中看到的TCP 3次交握可以清楚看到 。

# 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

- ASA系統日誌配置示例
- 使用CLI和ASDM的ASA資料包捕獲配置示例
- 技術支援與文件 Cisco Systems

#### 關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。