NATを使用したASAバージョン9ポートフォワー ディングの設定

内容

概要 前提条件 要件 <u>使用するコンポーネント</u> 設定 ネットワーク図 PAT を使用した inside ホストから outside ネットワークへのアクセスの許可 NAT を使用した inside ホストから outside ネットワークへのアクセスの許可 信頼できないホストから信頼できるネットワーク上のホストへのアクセスの許可 スタティック アイデンティティ NAT static を使用したポート リダイレクション(フォワーディング) 確認 Connection Syslog パケット トレーサ キャプチャ トラブルシュート 関連情報

概要

このドキュメントでは、CLIまたはAdaptive Security Device Manager(ASDM)を使用して、適応型 セキュリティアプライアンス(ASA)ソフトウェアバージョン9.xでポートリダイレクション(フォ ワーディング)と外部ネットワークアドレス変換(NAT)機能を設定する方法について説明します 。

詳細については、『<u>Cisco ASA シリーズ ファイアウォール ASDM 設定ガイド』を参照してくだ</u> <u>さい。</u>

前提条件

要件

デバイスを ASDM で設定できるようにするには、『<u>管理アクセスの設定』を参照してください。</u>

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco ASA 5525 シリーズ セキュリティ アプライアンス ソフトウェア バージョン 9.x 以降
- ASDM バージョン 7.x 以降

"このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています 。ネットワークが稼働中の場合は、コマンドの潜在的な影響について確実に理解しておく必要が あります」

設定

ネットワーク図



この設定で使用している IP アドレス スキームは、インターネット上で正式にルーティング可能 なものではありません。これらは、ラボ環境で使用された RFC 1918 のアドレスです。

PAT を使用した inside ホストから outside ネットワークへのアクセスの許可

変換用に inside ホストで 1 つのパブリック アドレスを共有する場合は、ポート アドレス変換 (PAT)を使用します。 PAT の最も単純な設定の 1 つに、すべての内部ホストを、外部インター フェイスの IP アドレスのように見えるよう変換することが含まれます。これは、ISP から使用で きるルーティング可能な IP アドレスの数が制限されているか少数、あるいはわずか 1 つの場合 に使われる、一般的な PAT の設定です。

PAT を使用して inside ホストから outside ネットワークへのアクセスを許可するには、次の手順 を実行します。

1. [Configuration] > [Firewall]> [NAT Rules] を選択します。ダイナミック NAT ルールを設定す るには、[Add] をクリックし、次に [Network Object] を選択します。

1onitoring 🔚 Save 🔇 Refresh 🔇 Back 🜔	Forward 2 Help CISCO
Configuration > Firewall > NAT Rules	Addresses Services
💠 Add 🗸 🌠 Edit 🏛 Delete 🛧 🗲 💃 🖿	Addresses 리 무 ×
	💠 Add 🗸 🗹 Edit 前 Delete 🔍 Where Used 🔍 Not Used
# Course Table Death Table Course	Network Object
Source Intr Dest Intr Source	Network Object Group
1 Apy outside P Toside b	Retwork Objects
	any
	anv4
	any6

Dynamic PAT が必要なネットワーク/ホスト/範囲を設定します。この例では、内部サブネットの1つが選択されました。このプロセスは、次のように変換する他のサブネットに対して繰り返すことができます。

📧 Add Networ	k Object	×
Name:	obj_172.16.11.0	
Туре:	Network	~
IP Version:	⊙ IPv4 ○ IPv6	
IP Address:	172.16.11.0	
Netmask:	255.255.255.0	~
Description:		
NOT		
		~
	OK Cancel Help	

 [NAT] を展開します。[Add Automatic Address Translation Rules] チェックボックスをオンに します。[Type] ドロップダウン リストから [Dynamic PAT (Hide)] を選択します。 [Translated Addr] フィールドで、外部インターフェイスを反映するオプションを選択します。 。[Advanced] をクリックします。

		A loss de		n L:	
	ATT	NPI	work		
- 100 C		1.100		~~	~~~

add Network	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	
NAT	
Add Automa	atic Address Translation Rules
Type:	Dynamic PAT (Hide) 🔽
Translated Ad	ldr: outside 💮
Use one-t	o-one address translation
PAT Pool	Translated Address:
Round F	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
E Fall throug	gh to interface PAT(dest intf): backup
Use IPv6	for interface PAT
	Advanced
	OK Cancel Help

4. [Source Interface] および [Destination Interface] のドロップダウン リストで、適切なインタ ーフェイスを選択します。[OK] をクリックし、次に [Apply] をクリックし、変更を有効にし ます。

🐻 Advanced NAT Set	tings	×
Ranslate DNS repli	es for rule	
Interface		_
Source Interface:	inside	*
Destination Interface:	outside	~
ОК	Cancel Help	

この PAT 設定に対応する CLI 出力を以下に示します。

object network obj_172.16.11.0 subnet 172.16.11.0 255.255.255.0 nat (inside,outside) dynamic interface

NAT を使用した inside ホストから outside ネットワークへのアクセスの許可

inside ホスト/ネットワークのグループに対して outside ネットワークへのアクセスを許可するに は、ダイナミック NAT ルールを設定します。PAT とは異なり、ダイナミック NAT はアドレス プールから変換されたアドレスを割り当てます。その結果、ホストは自身の変換された IP アドレ スにマッピングされ、2 つのホストが同じ変換された IP アドレスを共有することはできません。

このためには、アクセスを許可するホスト/ネットワークの実アドレスを選択し、変換 IP アドレスのプールにマップする必要があります。

NAT を使用して inside ホストから outside ネットワークへのアクセスを許可するには、次の手順 を実行します。

1. [Configuration] > [Firewall]> [NAT Rules] を選択します。ダイナミック NAT ルールを設定す るには、[Add] をクリックし、次に [Network Object] を選択します。

Monitoring 🔚 Save 💽 Refresh 💽 Back 💽	Forward ? Help CISCO
Configuration > Firewall > NAT Rules	Addresses Services
💠 Add 🗸 🌈 Edit 🗊 Delete 🛧 🗲 👗 🐚	Addresses 라우×
# Match Criteria: Original Packet * Source Intf Dest Intf Source	Add Add Carl Edit Carl Delete Carl Where Used Carl Network Object Filter Clear
"Network Object" NAT (Rule 1)	
1 Any outside 🚅 Inside_h	⊡-Network Objects

2. Dynamic PAT が必要なネットワーク/ホスト/範囲を設定します。この例では *inside-network* 全体が選択されています。

📴 Add Networl	k Object	×
Name:	obj_172.16.11.0	
Type:	Network	*
IP Version: 서	⊙ IPv4 ○ IPv6	
IP Address:	172.16.11.0	
Netmask:	255.255.255.0	*
Description:		
NAT		
	OK Cancel Help	

3. [NAT] を展開します。[Add Automatic Address Translation Rules] チェックボックスをオンに します。[Type] ドロップダウン リストから、[Dynamic] を選択します。[Translated Addr] フ ィールドで、適切なオプションを選択します。[Advanced] をクリックします。

📴 Edit Networ	k Object 🛛 🔀
ľ.,	
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	
Add Autom	atic Address Translation Rules
Typer	Dypamic
туре. т. 1. 1.	
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. [Add] をクリックして、ネットワーク オブジェクトを追加します。[Type] ドロップダウン リ ストから、[Range] を選択します。[Start Address] および [End Address] フィールドに、 PAT IP アドレスの開始と終了を入力します。[OK] をクリックします。

📧 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	S
	OK Cancel Help

5. [Translated Addr] フィールドで、アドレス オブジェクトを選択します。送信元と宛先インタ ーフェイスを選択するには、[Advanced] をクリックします。

📧 Edit Networ	k Object	×
Name:	obi 172 16 11 0	1
Tupor	Notwork	
Type:		
IP Version:	 ● IPv4 ● IPv6 	
IP Address:	172.16.11.0	1
Netmask:	255.255.255.0	
Description:]
NAT		
Add Autom	atic Address Translation Rules	
Туре:	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. [Source Interface] および [Destination Interface] のドロップダウン リストで、適切なインタ ーフェイスを選択します。[OK] をクリックし、次に [Apply] をクリックし、変更を有効にし ます。

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

この ASDM 設定に対応する CLI 出力を以下に示します。

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

この設定により、172.16.11.0ネットワーク内のホストは、NATプール203.0.113.10 ~ 203.0.113.20の任意のIPアドレスに変換されます。マッピングされたプールのアドレスが実際の グループよりも少ない場合、アドレスが不足する可能性があります。その結果、ダイナミック PATバックアップを使用してダイナミックNATを実装したり、現在のプールを拡張したりすることができます。

1. ネットワーク オブジェクトを追加するには、前の設定の手順 1~3 を繰り返し、[Add] をも う一度クリックします。[Type] ドロップダウン リストから、[Host] を選択します。[IP Address] フィールドに、PAT バックアップの IP アドレスを入力します。[OK] をクリックし ます。

🔄 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	× 1
	OK Cancel Help

2. [Add] をクリックして、ネットワーク オブジェクト グループを追加します。[Group Name] フィールドにグループ名を入力し、グループの両方のアドレス オブジェクト(NAT 範囲お よび PAT IP アドレス)を追加します。

cription:							
Existing Network Objects	s/Groups:				Members in Group:		
Name 🔺 1	IP Address	Netmask	Description		Name	IP Address	NetmaskPr
⊟-Network Objects					💬 🖳 obj-pat-ip	203.0.113.21	
- 🏈 any					👆 🚅 ob)-my-range	203.0.113.10-203.0	
- 🧼 any4							
- 🏈 any6							
- 📸 inside-net	19.19.19.0	255.255.255.0					
- 🛃 obj_172.1	172.16.11.0	255.255.255.0					
				Addasa			
				- Has 222			

3. 設定した NAT ルールを選択し、[Translated Addr] を新しく設定されたグループ「nat-patgroup」(以前は「obj-my-range」だった)に変更します。 [OK] をクリックします。

📴 Browse Translate	d Addr			X
Filter:	📋 Delete 🛛 🔍 Where	Used Q Not I	Jsed	Filter Clear
Name 4	IP Address	Netmask	Description	Object NAT Address
-Network Objects				
- 🥵 obj-my-ra	203.0.113.10-203			
🔜 obj-pat-ip	203.0.113.21			
-Network Object G	roups			
🔳 🚮 nat-pat-g.				
Interfaces				
- 🔤 backup				
- 🔤 inside				
www.outside				
al a fair a fair de la fair				
Selected Translated A	aar			
Translated Addr	-> nat-pat-group			
				OK Cancel

4. NAT ルールを追加するには、[OK] をクリックします。送信元と宛先インターフェイスを選 択するには、[Advanced] をクリックします。

📧 Edit Networ	k Object 🛛 🔀
Namer	obi 172 16 11 0
Name:	00_172.16.11.0
Type: 💦	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: 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. [Source Interface] および [Destination Interface] のドロップダウン リストで、適切なインタ ーフェイスを選択します。[OK] をクリックします。

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

6. [Apply] をクリックして変更を有効にします。

S)	Home 🦓 Configuration 🔯 Monitor	ng) Save 🔇 Ref	resh 🔇 🔾 B	ack 🔘 Forward 🛛 🢡	ныр	CISCO
	Firewall 🗗 🖓		ionf	iguration > Fire	wall > NAT I	Rules 🗆	Addresses Services	
e Da	Access Rules	Г	۰.	Add - 📝 Edit 1	Delete 🛧	4 X 時間。	Addresses	다 슈 ×
Devic	NAT Rules			Match Crite	ria: Original I	Packet	💠 Add - 📷 Edit 🏢 Delete 🔍 W	here Used Q, Not Used
	Device Setup		ş	Source Intf	Dest Intf	Source	Fiker:	Filter Clear
	Frewall		۴ 🗉	Vetwork Object" N	IAT (Rule 1)		Name	<u></u> 1
		U	1	inside	outside	🛃 obj_172.16	Network Objects	~
	Remote Access VPN	L					- 🎱 any	
	2 Site-to-Site VPN	L					- 🌗 any4	
	<u>0</u> -0 -		1			N	- 🎱 any6	Ξ
	Device Management	1	-			<u>e</u>	- M inside-network/24	
				000		e cont	- 🚮 obj-my-range	
	:	L		-10		0301	່- 🚮 obj_172.16.11.0	~

この ASDM 設定に対応する CLI 出力を以下に示します。

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

信頼できないホストから信頼できるネットワーク上のホストへのアクセスの許可

スタティック NAT 変換とアクセス ルールを適用して、これらのホストに対しアクセスを許可し ます。外部ユーザが内部ネットワーク上の任意のサーバにアクセスできるようにするには、この ように設定する必要があります。内部ネットワークのサーバには、インターネット上でルーティ ングできないプライベートIPアドレスを設定できます。このため、スタティック NAT ルールを使 用してプライベート IP アドレスをパブリック IP アドレスに変換する必要があります。1 つの内 部サーバ(172.16.11.5)があるとします。 このようにアクセスを許可するには、このプライベー ト サーバ IP アドレスをパブリック IP アドレスに変換する必要があります。この例では、 172.16.11.5 を 203.0.113.5 に変換するために双方向スタティック NAT を実装する方法を説明し ます。

1. [Configuration] > [Firewall]> [NAT Rules] を選択します。スタティック NAT ルールを設定す るには、[Add] をクリックし、次に [Network Object] を選択します。[NAT] を展開します。

🛅 Add Networ	k Object 🛛 🚺	<
Name:	obj_172.16.11.5	
Туре:	Host	
IP Version:	⊙ IPv4 O IPv6	
IP Address:	172.16.11.5	
Description:		
NAT		
	Ŷ	
	OK Cancel Help	

2. [Add Automatic Address Translation Rules] チェックボックスをオンにします。[Type] ドロ ップダウン リストから、[Static] を選択します。[Translated Addr] フィールドに、IP アドレ スを入力します。送信元と宛先インターフェイスを選択するには、[Advanced] をクリック します。

🖀 Add Networ	k Object 🛛 🛛 🔀
Name:	obj_172.16.11.5
Туре:	Host
IP Version:	⊙ IPv4 ○ IPv6
IP Address:	172.16.11.5
Description:	
NAT	۲
🔽 Add Automa	atic Address Translation Rules
Туре:	Static 💙
Translated Ac	idr: 203.0.113.5
🔽 Use one-t	co-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. [Source Interface] および [Destination Interface] のドロップダウン リストで、適切なインタ ーフェイスを選択します。[OK] をクリックします。

🔄 Advanced NAT Set	tings	×
Translate DNS repli	es for rule	
Interface		-
Source Interface:	inside	 Image: A set of the set of the
Destination Interface:	outside	·
ОК	Cancel Help	

4. 設定したスタティック NAT エントリは次のように表示されます。[Apply] をクリックしてこ れを ASA に送信します。

	Match Crite	eria: Original	Packet			Action: Transla	ted Packet	
	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 (5)	🖪 obj_172.16	Original

この NAT 設定に対応する CLI 出力を以下に示します。

object network obj_172.16.11.5
host 172.16.11.5
nat (inside,outside) static 203.0.113.5

スタティック アイデンティティ NAT

NAT 免除は、内部のユーザが NAT の完了なしに、リモート VPN ホスト/サーバ、または ASA の 他のインターフェイスの背後にあるホスト/サーバにアクセスしようとする場合に便利な機能です

。これを実現するために、プライベートIPアドレスを持つ内部サーバは、それ自体にID変換でき 、次にNATを実行する宛先へのアクセスを許可されます。

この例では、内部ホスト 172.16.11.15 は、リモート VPN サーバの 172.20.21.15 にアクセスする 必要があります。

NAT を完了して inside ホストから リモート VPN ネットワークへのアクセスを許可するには、次の手順を実行します。

1. [Configuration] > [Firewall]> [NAT Rules] を選択します。[Add] をクリックして、NAT 免除ル ールを設定します。

Firewall D' 4	Co	mfic	uration > Fir	ewall > NAT	Rules			
Access Rules	4	A 4	dd 👻 📝 Edit	🗎 Delete 🗲	4 X Pa B	🛓 - 🔍 Find 📴 Dia	gram 🛒 Packet T	
- Q Service Policy Rules			Match Crite	ria: Original	Packet			F
AAA Rules	*	*	Source Intf	Dest Intf	Source	Destination	Service	
Public Servers		"Ne	etwork Object" I	NAT (No rules)				
URL Filtering Servers								
² Identity Options								
The second se								
Objects								
Objects Unified Communications								

2. [Source Interface] および [Destination Interface] のドロップダウン リストで、適切なインタ ーフェイスを選択します。[Source Address] フィールドで、適切なエントリを選択します。

📑 Add NAT Rule					×
Match Criteria: Original Packet —					
Source Interface:	inside	~	Destination Interface:	outside	~
Source Address:	any	····	Destination Address:	any	
			Service:	any	
Action: Translated Packet					
Source NAT Type:	Static 👔	Browse Orig	inal Source Addres	S	
Source Address:	Origina				
Use one-to-one address transla	ation	🔂 Add 🕶 🧾	Edit 📋 Delete 🔍	Where Used 🔍 No	ot Used
PAT Pool Translated Address:		Filter:			
Round Robin		Name	▲ 1 IP Address		Netmask
Extend PAT uniqueness to pe	er destinal	L- 🏀 any	njects		
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. [Add] をクリックして、ネットワーク オブジェクトを追加します。ホスト IP アドレスを設 定します。

📴 Add Networ	k Object 🔤 🚺	×
Name:	obj 172.16.11.15	1
Type:	Host	
IP Version		IJ
		1
IP Address:	1/2.16.11.15	J
Description:		1
NAT	*	
	OK Cancel Help	

4. 同様に、[Destination Address] を検索します。[Add] をクリックして、ネットワーク オブジェクトを追加します。ホスト IP アドレスを設定します。

🔤 Add Netwo	rk Object 🛛 🚺	K
Name: Type: IP Version:	obj_172.20.21.15 Host IPv4 IPv6	
Description:	172.20.21.15]
NAT	8	
	OK Cancel Help	

5. 設定された [Source Address] および [Destination Address] オブジェクトを選択します。 [Disable Proxy ARP on egress interface] および [Lookup route table to locate egress interface] のチェックボックスをオンにします。[OK] をクリックします。

🖀 Add NAT Rule			\mathbf{X}			
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	}			
Fall through to interface PAT						
Use IPv6 for source interface P	AT	Use IPv6 for destin	ation interface PAT			
Options	Options					
🔽 Enable rule						
Translate DNS replies that mate	th this rule					
✓ Disable Proxy ARP on egress interface						
Cookup route table to locate egress interface						
Direction: Both						
Description:						
OK Cancel Help						

6. [Apply] をクリックして変更を有効にします。

🍪 Configuration 📴 Monit	oring	🔒 Save 🔇	Refresh	Back 🕐 Forma	rd 💡 H	elp CIS
a e 🔀	Confi	guration > Fire	wall > NAT P	tules		Addresses D
ass Rules	💠 A	dd 🔻 💽 Edit	🖹 Delete 🕇	+ 3 ≈ ≈ -	Q, Find	🗣 Add 👻 🛒 Edit 📋 Delete 🔍 🔍 Where Used 🔍
rice Policy Rules		Match Crite	ria: Original P	Packet		Fiter:
(Rules	*	Source Intf	Dest Intf	Source	Destina	Name
r Rules	1	inside	outside	🖪 obj_172.16	🖪 obj	 Network Objects
e Setup	"N	etwork Object" N	IAT (No rules)			🧼 any
						- 🏟 any4
en .						🥥 any6
te Access VPN						- 🙀 inside-network/24
						- 🖳 obj_172.16.11.15
o-Site VPN						🔜 obj_172.20.21.15
e <u>M</u> anagement	<	Ш			>	
*			Apply	Reset		

この NAT 免除またはアイデンティティ NAT 設定に対応する CLI 出力を以下に示します。

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

static を使用したポート リダイレクション(フォワーディング)

ポート フォワーディング(ポート リダイレクション)は、外部ユーザが特定ポートから内部サー バにアクセスする場合に便利な機能です。これを実現するには、プライベートIPアドレスを持つ 内部サーバをパブリックIPアドレスに変換し、次に特定のポートに対するアクセスを許可します 。

この例では、外部ユーザがSMTPサーバ203.0.113.15にポート25でアクセスしようとしています。これは、次の2つの手順で実現します。

1. 内部メールサーバ(ポート25の172.16.11.15)をパブリックIPアドレス(ポート25の 203.0.113.15)に変換します。

2. パブリック メール サーバ 203.0.113.15 へのポート 25 でのアクセスを許可します。 外部ユーザがサーバ203.0.113.15(ポート25)にアクセスしようとすると、このトラフィックは 内部メールサーバ172.16.11 15(ポート25)にリダイレクトされます。

1. [Configuration] > [Firewall]> [NAT Rules] を選択します。スタティック NAT ルールを設定す るには、[Add] をクリックし、次に [Network Object] を選択します。

Monit	oring:	🔚 Save (Refresh	🕒 Back 🜔) Forwa	rd 💡	elp		CIS	co
C	onfig	uration > Fire	ewall > NAT F	Rules 🗆		Addresses	Services			
	🔂 Ac	ld 👻 🌠 Edit '	î Delete 🛧	∡ X h	Add	resses			a	φ×
Γ	#	Match Crite	ria: Original F	Packet	↔ 	Add 👻 🗹 E Network C	Edit <u> Delet</u> i)bject	e 🔍 Whe	re Used 🔍	Not Used
G	B "Ne	twork Object" f	VAT (Rule 1)	Source		Network C	bject Group			<u>1</u>
	1	Any	outside	📑 Inside_h	⊡∼N	letwork Obje	ects			
						- 🏈 any - 🏈 any4				

2. ポート フォワーディングが必要なホストを設定します。

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

3. [NAT] を展開します。[Add Automatic Address Translation Rules] チェックボックスをオンに します。[Type] ドロップダウン リストから、[Static] を選択します。[Translated Addr] フィ ールドに、IP アドレスを入力します。サービスおよび送信元と宛先のインターフェイスを選 択するには、[Advanced] をクリックします。

📧 Edit Networl	k Ob	ject 🛛 🔀
Name	obi -	172 16 11 15
Turne:	Up at	
Type:	Host	
IP Kyrsion:	⊙ IF	V4 ○ IPv6
IP Address:	172.	16.11.15
Description:		
NAT		
🗹 Add Automa	atic Ad	Idress Translation Rules
Туре:	s	tatic 🖌
Translated Ac	idr:	203.0.115.15
📃 Use one-t	:0-016	address translation
PAT Pool	Trans	lated Address:
Round	Robin	
Extend	PAT	uniqueness to per destination instead of per interface
Transla	ite TC	P and UDP ports into flat range 1024-65535 🔄 Include range 1-1023
🔄 Fall throu	gh to	interface PAT(dest intf): backup
Use IPv6	for in	terface PAT
		Advanced
		OK Cancel Help

4. [Source Interface] および [Destination Interface] のドロップダウン リストで、適切なインタ ーフェイスを選択します。サービスを設定します。[OK] をクリックします。

🖷 Advanced NAT Settings 🛛 🛛 🔀					
Translate DNS repli	es 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. [Apply] をクリックして変更を有効にします。



この NAT 設定に対応する CLI 出力を以下に示します。

object network obj_172.16.11.15
host 172.16.11.15
nat (inside,outside) static 203.0.113.15 service tcp smtp smtp

確認

ここでは、設定が正常に機能しているかどうかを確認します。

<u>Cisco CLI アナライザ(登録ユーザ専用)は、特定の show コマンドをサポートします。</u>show コ

マンド出力の分析を表示するには、Cisco CLI アナライザを使用します。

ロックされないでファイアウォールの通過を許可されます。

Web ブラウザで HTTP を介して Web サイトにアクセスします。この例では、198.51.100.100で ホストされているサイトを使用しています。接続に成功した場合、この出力はASA CLIに表示さ れます。

Connection

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 はステートフル ファイアウォールであり、Web サーバからのリターン トラフィックはファ イアウォール接続テーブルの接続の 1 つと一致するため、ファイアウォールの通過を許可されま す。事前に存在する接続の 1 つと一致するトラフィックは、インターフェイス ACL によってブ

上の出力では、内部インターフェイス上のクライアントが外部インターフェイスからの 198.51.100.100 ホストへの接続を確立しました。この接続では TCP プロトコルが使用されてお り、6 秒間アイドル状態です。接続のフラグは、この接続の現在の状態を示します。接続のフラ グの詳細については、『ASA の TCP 接続フラグ』を参照してください。

Syslog

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 ファイアウォールは正常動作中に syslog を生成します。Syslog の詳細レベルはログ設定に 基づきます。この出力はレベル 6、つまり「情報」レベルでの 2 種類の syslog を示します。

この例では、2 つの Syslog が生成されています。1 番目は、ファイアウォールが変換を作成した こと、具体的にはダイナミック TCP 変換(PAT)を行ったことを示すログ メッセージです。 こ れは、トラフィックが内部インターフェイスから外部インターフェイスに渡るときの、送信元 IP アドレスとポート、および変換後の IP アドレスとポートを示します。

2番目の Syslog はファイアウォールがクライアントとサーバ間のこの特定のトラフィック用に接 続テーブルで接続を作成したことを示しています。この接続試行をブロックするようにファイア ウォールが設定された場合や、その他の要因(リソース制約または設定ミスの可能性)によって この接続の作成が妨げられる場合は、ファイアウォールは接続が確立されたことを示すログを生 成しません。通常は、代わりに、接続が拒否される理由や、接続の作成を妨げた要因に関する兆 候を記録します。

パケット トレーサ

--Omitted--

Result: input-interface: inside input-status: up output-line-status: up output-status: up output-status: up output-line-status: up Action: allow

ASA のパケット トレーサ機能を使用すると、シミュレートされたパケットを指定して、ファイア ウォールでトラフィックを処理するときに通るさまざまなステップ、チェック、機能をすべて確 認できます。このツールを使用すると、ファイアウォールの通過を許可できると考えられるトラ フィックの例を特定し、その5タプルを使用してトラフィックをシミュレートできます。前記の例 では、以下の条件を満たす接続試行をシミュレートするために、パケット トレーサを使用します 。

- シミュレートされたパケットが内部に到達する。
- ・使用されているプロトコルが TCP である。
- •シミュレートされたクライアントの IP アドレスが 172.16.11.5 である。
- クライアントは送信元がポート 1234 であるトラフィックを送信している。
- トラフィックは、IP アドレス 198.51.100.100 のサーバ宛てに送信されます。
- トラフィックの宛先はポート 80 です。

コマンドにインターフェイス outside に関する言及がないことに注意してください。これはパケ ット トレーサの設計による動作です。このツールは、このタイプの接続試行をファイアウォール でどのように処理するのかを示し、ルーティングの方法や、どのインターフェイスから送信する のかが含まれます。パケット トレーサの詳細については、『パケット トレーサを使用したパケッ トのトレース』を参照してください。

キャプチャ

キャプチャの適用

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 ファイアウォールでは、インターフェイスに着信または発信するトラフィックをキャプチャ できます。このキャプチャ機能は、トラフィックがファイアウォールに着信したかやファイアウ ォールから送信したかを確実に保証できるため便利です。前の例は、内部インターフェイスの capin と外部インターフェイスの capout という 2 個のキャプチャの設定を示しています。 capture コマンドは、match キーワードを使用します。キャプチャするトラフィックを具体的に 指定できます。

キャプチャcapin で、TCPホスト172.16.11.5ホスト198.51.100.100と一致する内部インターフェ イス (入力または出力)上のトラフィックを照合することを指定しました。つまり、ホスト 172.16.11.5からホスト198.51.100.100に送信されるすべてのTCPトラフィックをキャプチャしま す。match キーワードを使用することで、ファイアウォールでトラフィックを双方向でキャプチ ャできます。外部インターフェイスに定義された capture コマンドは、ファイアウォールがその クライアントの IP アドレスに PAT を実行するため、内部クライアントの IP アドレスを参照しま せん。したがって、そのクライアントの IP アドレスとは照合できません。代わりに、この例では 、可能性のあるすべての IP アドレスがその基準と一致することを示すために any を使用します。

キャプチャを設定したら、次に接続の確立を再試行してから、show capture <capture_name> コ マンドによるキャプチャの表示に進みます。この例では、キャプチャにある TCP の 3 ウェイ ハ ンドシェイクによって明らかなようにクライアントがサーバに接続できたことを確認できます。

トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- ・<u>ASA Syslog の設定例</u>
- <u>CLI および ASDM を使用した ASA パケット キャプチャの設定例</u>
- ・テクニカル サポートとドキュメント Cisco Systems

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。