PIX/ASA 7.x:nat、global、static および accesslist コマンドを使用したポート リダイレクション (フォワーディング)

内容

概要 前提条件 要件 使用するコンポーネント 関連製品 表記法 ネット<u>ワーク図</u> 初期設定 アウトバウンド 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 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 inside ホストから outside ネットワークへのアクセスの制限 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 PIX バージョン 7.0 以降での ACL の使用 特定のホストおよびネットワークでの NAT の無効化 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) ネットワーク ダイアグラム:ポート リダイレクション(フォワーディング) PIX 部分設定 - ポートリダイレクション static を使用した TCP/UDP セッションの制限 時間ベースのアクセス リスト テクニカルサポートのサービス リクエストをオープンする際に収集する情報 関連情報

<u>概要</u>

Cisco PIX セキュリティ アプライアンス バージョン 7.0 を実装した場合にセキュリティを最大限 に実現するには、nat-control、nat、global、static、access-list、access-group の各コマンドを使 用する際に、セキュリティの高いインターフェイスと低いインターフェイスの間をパケットが流 れる仕組みを理解することが重要です。このドキュメントでは、これらのコマンドの違い、ポー ト リダイレクション(フォワーディング)の設定方法、コマンドライン インターフェイスまたは Adaptive Security Device Manager (ASDM)を使用した PIX ソフトウェア バージョン 7.x での Outside ネットワーク アドレス変換 (NAT)の機能について説明します。

注:ASDM 5.2以降の一部のオプションは、ASDM 5.1のオプションとは異なる場合があります。 詳細については、<u>ASDMのドキュメントを参照</u>してください。



<u>要件</u>

ASDM でデバイスを設定できるようにする方法については、『<u>ASDM 用の HTTPS アクセスの許</u> <u>可</u>』を参照してください。

<u>使用するコンポーネント</u>

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 PIX 500 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 7.0 以降
 ASDM バージョン 5.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 。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的 な影響について確実に理解しておく必要があります。

関連製品

この設定は、Cisco ASA セキュリティ アプライアンス バージョン 7.x 以降でも使用できます。

表記法

ドキュメント表記の詳細については、『<u>シスコ テクニカル ティップスの表記法</u>』を参照してくだ さい。

<u>ネットワーク図</u>



10.0.0.0/8

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。

初期設定

インターフェイス名は次のとおりです。

- interface ethernet 0 : Outside \mathcal{O} nameif
- interface ethernet 1 : Inside の nameif

注:このドキュメントで使用されているコマンドの詳細を調べるには、<u>Command Lookup</u> <u>Tool(</u>登録ユーザ<u>専用)を使用</u>してください。

<u>アウトバウンド アクセスの許可</u>

アウトバウンド アクセスは、セキュリティ レベルの高いインターフェイスからセキュリティ レベルの低いインターフェイスへの接続を意味します。これには、inside から outside への接続、 inside から非武装地帯(DMZ)への接続、および DMZ から outside への接続が含まれます。発信 元インターフェイスのセキュリティ レベルが宛先より高いという条件下では、ある DMZ から別 の DMZ への接続もこれに含まれる可能性があります。これを確認するには、PIX インターフェ イス上の「セキュリティ レベル」設定を確認します。

次の例は、セキュリティレベルとインターフェイス名の設定を示しています。

PIX 7.0 では nat-control コマンドが導入されています。コンフィギュレーション モードで natcontrol コマンドを使用すると、Outside 通信用に NAT が必要であるかどうかを指定できます。 NAT 制御をイネーブルにすると、PIX ソフトウェアの以前のバージョンと同じように、アウトバ ウンド トラフィックを許可するために NAT ルールの設定が必要です。NAT 制御がディセーブル になっている場合 (no nat-control)、Inside ホストは、NAT ルールの設定なしで、Outside ネッ トワークと通信できます。ただし、パブリック アドレスを持たない Inside ホストがある場合は、 これらのホスト用に NAT を設定する必要があります。

ASDM を使用して NAT 制御を設定するには、ASDM Home ウィンドウから Configuration タブを 選択し、機能メニューから NAT を選択します。

Enable traffic through the firewall without translation: このオプションは PIX バージョン 7.0(1) で 導入されました。 このオプションにチェックマークが付いていると、コンフィギュレーションで は nat-control コマンドは発行されません。このコマンドは、ファイアウォールを通過するために 変換が必要ではないことを意味します。通常、このオプションにチェックマークが付いているの は、内部ホストにパブリック IP アドレスがある場合、またはネットワーク トポロジで内部ホス トが IP アドレスに変換される必要がない場合だけです。

内部ホストにプライベート IP アドレスがある場合は、このオプションのチェックマークを外して 、内部ホストをパブリック IP アドレスに変換でき、内部ホストがインターネットにアクセスでき るようにする必要があります。

Cisco ASDM 5.1 File Rules Sea	for PIX - 10.1 rch Options	.1.1 Tools Wizard	ds Help				_ 🗆 X
Home Co	antiguration	Monitoring	Back Forward	Q Q Search Refresh	Save Help		Cisco Systems
Interfaces Security Policy	Sontiguration • (*) PEnable (* Transl Show Ru	n > NAT > Transi ■2 ① & e traffic through t ation Rules les for Interface:	ation Rules R R R R R R R A he firewall without address C Translation Exemp All Interfaces	translation; plion Rules The Show All			
NAT	Rule		Original			Translated	Add
VPN	Туре	Interface	Source Network	Destination Network	Interface	Address	Edit
Routing Globel Objects Properties		NAT 👯 [Dynamic NAT 🖓 Stal	ic Policy NAT Policy NAT	Dynamic Policy N Reset	AT Manage Pools	0e/ete

NAT 制御を使用してアウトバウンド アクセスを許可するために必要な 2 つのポリシーがありま す。最初のポリシーは変換方式です。変換方式は static コマンドを使用したスタティック変換、 または nat/global ルールを使用したダイナミック変換のどちらかになります。NAT 制御がディセ ーブルになっていて、Inside ホストがパブリック アドレスを持っている場合、この変換方式は必 要ありません。

(NAT 制御がイネーブルになっているかディセーブルになっているかに関係なく適用される)ア ウトバウンド アクセスのもう 1 つの要件は、Access Control List (ACL; アクセス コントロール リスト)が存在するかどうかです。ACL が存在する場合、ACL は特定のプロトコルとポートを使 用して、発信元ホストが宛先ホストにアクセスするのを許可する必要があります。デフォルトで は、PIX 経由のアウトバウンド接続に対するアクセス制限はありません。これは、発信元インタ ーフェイスに ACL が設定されていない場合、デフォルトでは、変換方式が設定されていればアウ トバウンド接続が可能になることを意味します。

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

この設定では、サブネット 10.1.6.0/24 上のすべてのホストに外部へのアクセスが付与されます。 これを行うには、手順で示すように、nat コマンドと global コマンドを使用します。

1. NAT に含める Inside グループを定義します。

nat (inside) 1 10.1.6.0 255.255.255.0

2. NAT文で定義されたホストが変換される外部インターフェイスのアドレスプールを指定しま す。

global (outside) 1 172.16.1.5-172.16.1.10 netmask 255.255.255.0

3. グローバル アドレス プールを作成するには、ASDM を使用します。Configuration > Features > NAT の順に選択し、Enable traffic through the firewall without address translation のチェックマークを外します。続いて Add をクリックして、NAT Rule を設定します。

🖆 Cisco ASDM	5.1 for PE	x - 10.1.	1.1		23.59 <u>0</u> -					- 🗆 X
File Rules 8	search C	ptions		is Help		0				Ciero Sverime
	Configure	ation	Unatara	O	O .	Q Description	Q			ult
riume	Conniga	auon	Montorry	Dock	Forward	Search	siesn	Save http		• من اللاليسينا اللاتي
		unation B 25	≥ INAT ≥ Transis IZ2 m X	Da Ca Ca	11 A		_			
Interfaces			ын III 1 0×	(H 463 24						
G.		Enable	traffic through t	he firewall w	ithout addres	s translation				
Security Policy	•	Transla	tion Rules	C Tran	slation Exem	nption Rules				
24	si	now Rule	es for Interface:	All Interfac	es	- Sho	w All			
NAT	Ē							1		Add
93		Rule			Unginai				Translated	
VPN		Туре	Interface	Source	Network	Destination	n Network	Interface	Address	Edit
* <u>*</u> *										Deiete
Routing										
- 88										
Global Objects										
Properties										
		1							•	l,
	1	Static	NAT 📲 I)ynamic NA1	r 🖓 Sta	atic Policy NAT	(B)	Dynamic Policy N	AT Manage Pools	
						Apply		Reset		
						<adm< td=""><td>in> IN</td><td>IA (15)</td><td>🛃 🔂 🕴 🔒 7/11/06 i</td><td>3:02:29 PM UTC</td></adm<>	in> IN	IA (15)	🛃 🔂 🕴 🔒 7/11/06 i	3:02:29 PM UTC

4. [Manage Pools] をクリックして、NAT プール アドレスを定義します。

	C I	Jse Policy NAT			
Source Ho	ost/Network-				
		Interface:	inside.	Y	
		IP Address:	10.1.6.0		
		Mask:	255.255.255.0	-	
			Browse		
					NAT Options.
anslate Ad	Idress on Inte	erface: outsi	ide 💌		
Translate.	Address To -				
Translate . C ' '	Address To - Static	IP Address:		-	
Translate. C יוי	Address To - Static	IP Address; port	[•	
Translate. C יי	Address To - Static Redirect © TCP © UDP	IP Address; port Original port	Translat	ed port:	
Translate C 1	Address To - Static Redirect C TOP C UDP Dynamic	IP Address; port Original port Address Pool:	Translat	ed port: Manag	e Pools
Translate C 1	Address To - Static Redirect C TCP C UDP Dynamic Pool ID	IP Address: port Original port Address Pool:	Translat	ed port: Manag	e Pools
Translate	Address To - Static Redirect © TCP © UDP Dynamic Pool ID N/A	IP Address; port Original port Address Pool: No address po	Translat	ed port: Manag	e Pools
Translate.	Address To - Static Redirect © TOP © UDP Dynamic Pool ID N/A.	IP Address: port Original port Address Pool: No address po	Translat	ed port: Manag	e Pools
Translate	Address To - Static Redirect © TOP © UDP Dynamic Pool ID N/A	IP Address: port Original port Address Pool: No address po	Translat same address 💽 Address	ed port: Manag	e Pools

5. Outside > Add の順に選択して、範囲を選択し、アドレスのプールを指定します。

Global Address I	Pools					
			- Domentic Materia	ul é dalar e e Tur		_
addresses.	'ools are used	to configure	e Dynamic Netwo	ork Address Tra	nsiation (NA I)
Interface	Pool ID		IP Address(es)		
inside						Add
outside						
						Edit
					E)elete
						- Cricito
1						
	OF		Cancel	Help		
<u>[×]レス範囲を入</u>	力し、Pool	ID を入力	して OK をク!	ノックします	0	
ドレス範囲を入 Add Global Po	力し、Pool ol Item	ID を入力	して OK をク ⁱ	ノックします	0	
ドレス範囲を入 Add Global Po	カし、Pool ol Item	ID を入力	して OK をク!	リックします	0	
ドレス範囲を入 Add Global Po	カし、Pool ol Item	ID を入力	してOKをクリ	リックします	•	
ドレス範囲を入 Add Global Po Interface:	カし、Pool ol Item outside	ID を入力	して OK をクリ	リックします ol ID: 1	•	
ドレス範囲を入 Add Global Po Interface:	カし、Pool ol Item outside	ID を入力	して OK をクリ	リックします ol ID: 1	°	
ドレス範囲を入 Add Global Po Interface: ・ Range	カし、Pool ol Item outside	ID を入力	して OK をクロ	リックします ol ID: 1	•	
ドレス範囲を入 Add Global Po Interface: で Range	カし、Pool ol Item outside	ID を入力	して OK をクリ	リックします ol ID: 1	0	
ドレス範囲を入 Add Global Po Interface: ・ Range ・ Port Add	カし、Pool ol Item outside ress Transla	ID を入力 Ation (PAT	して OK をクリ Po	リックします ol ID: 1	0	
ドレス範囲を入 Add Global Po Interface: C Range C Port Add C Port Add	カし、Pool ol Item outside ress Transla	ID を入力 ation (PAT ation (PAT	して OK をクロ Po)) using the IP :	リックします ol ID: 1	e interface	
ドレス範囲を入 Add Global Po Interface: ・ Range ・ Port Add ・ Port Add	カし、Pool ol Item outside ress Transla ress Transla	ID を入力 ation (PAT ation (PAT	して OK をクリ Po)) using the IP :	リックします ol ID: 1 address of th	。 e interface	
ドレス範囲を入 Add Global Po Interface:	力し、Pool ol Item outside ress Transla ress Transla	ID を入力 ation (PAT ation (PAT	して OK をクロ Po)) using the IP :	リックします ol ID: 1	e interface	
ドレス範囲を入 Add Global Po Interface: C Range C Port Add C Port Add	カレ、Pool ol Item outside ress Transla ress Transla	ID を入力 ation (PAT ation (PAT	して OK をクリ Po)) using the IP :	リックします ol ID: 1 address of th	° e interface	
ドレス範囲を入 Add Global Po Interface: ・ Range ・ Port Add ・ Port Add	カし、Pool ol Item outside ress Transla ress Transla	ID を入力 ation (PAT ation (PAT 2.16.1.5	して OK をクリ Po)) using the IP :	リックします ol ID: 1: address of th - 172.16	e interface	
ドレス範囲を入 Add Global Po Interface: C Range C Port Add C Port Add	カし、Pool ol Item outside ress Transla ress Transla	ID を入力 ation (PAT ation (PAT 2.16.1.5	して OK をクリ Po)) using the IP :	リックします ol ID: 1 address of th - 172.16	e interface	
ドレス範囲を入 Add Global Po Interface: ・ Range ・ Port Add ・ Port Add	カし、Pool ol Item outside ress Transla ress Transla	ID を入力 ation (PAT ation (PAT 2.16.1.5	して OK をクリ Po)) using the IP :	Jックします ol ID: 1 address of th - 172.16	o e interface .1.10	
ドレス範囲を入 Add Global Po Interface:	カし、Pool ol Item outside ress Transla ress Transla ress Transla	ID を入力 ation (PAT ation (PAT 2.16.1.5 iional):	して OK をクリ Po)) using the IP : 255.255.25	リックします ol ID: 1 address of th - 172.16	e interface	
ドレス範囲を入 Add Global Po Interface: ・ Range ・ Port Add ・ Port Add ・ IP Add Netwo	カし、Pool ol Item outside ress Transla ress Transla ress Transla	ID を入力 ation (PAT ation (PAT 2.16.1.5 tional):	して OK をクリ Po) using the IP : 255.255.25	<u>Jックします</u> ol ID: 1: address of th - 172.16	o e interface .1.10	
ドレス範囲を入 Add Global Po Interface:	カし、Pool ol Item outside ress Transla ress Transla ress Transla	ID を入力 ation (PAT ation (PAT 2.16.1.5 iional):	して OK をクロ Po)) using the IP : 255.255.25	リックします ol ID: 1 address of th - 172.16	e interface	
×レス範囲を入 Add Global Po Interface:	カレ、Pool ol Item outside ress Transla ress Transla Iress: 172 ork Mask (opt	ID を入力 ation (PAT ation (PAT 2.16.1.5 iional):	して OK をクロ Po)) using the IP : 255.255.25	リックします ol ID: 1 address of th - 172.16 5.0	e interface	
×レス範囲を入 Add Global Po Interface: ・Range ・Port Add ・Port Add ・IP Add Netwo	カレ、Pool ol Item outside ress Transla ress Transla ress Transla	ID を入力 ation (PAT ation (PAT 2.16.1.5 tional):	して OK をクロ Po)) using the IP : 255.255.25	リックします ol ID: 1 address of th 172.16	e interface	

- 7. Configuration > Features > NAT > Translation Rules の順に選択して、変換ルールを作成し ます。
- 8. 発信元インターフェイスとして Inside を選択し、NAT を適用するアドレスを入力します。
- 9. Translate Address on Interface では、**Outside** を選択し、**Dynamic** を選択して、設定したア ドレス プールを選択します。
- 10. [OK] をクリックします。

	SUIVERVOIN					
		Interface:	inside'		-	
		IP Address:	10.1.6.0			
		Mask:	255.255.255	i.0 .	-	
			Browse			
						NAT Options
ranslate ، r ان	Address To - Static C Redirect	IP Address: port		<u>*</u>]	
	C UDP	Original port		Translated p	ort.	
• 11	Dynamic	Address Pool:	1	•	Manage Po	ols
• 11	Dynamic Pool ID	Address Pool:	1 Ad	.▼ idress	Manage Po	ols

11. **Configuration > Features > NAT > Translation Rules** の順に選択すると、Translation Rules に変換が表示されます。

	Configuration	> NAT > Trans	lation Rules				
erfaces	🗣 😤 🐺	🗹 🔒 🐰	B C £ € € S				
<u>e</u> ,	⊡ (Enable	traffic through	the firewall without addres	s translation			
rity Policy	Transla	tion Rules	C Translation Exem	nption Rules			
65	Show Rul	es for Interfaci	All Interfaces	✓ Show All			
02	Rule		Original			Translated	Add
VPN	Туре	Interface	Source Network	Destination Network	Interface	Address	Edit
430	10 AL	inside	⊈ 10.1,6.0/8	🔹 any	outside	172161.5-17216.1.10	Dele
louting							
80							
V 🔉 👘							
al Objects							
al Objects							
al Objects							
al Objects							
operties							

これで、内部のホストは外部ネットワークにアクセスできます。内部のホストは外部へ接 続を開始すると、グローバル プールのアドレスに変換されます。アドレスは、先着順、先 に変換される順に、グローバル プール内の一番低いアドレスから割り当てられます。たと えば、ホスト10.1.6.25が最初に外部への接続を開始する場合、アドレス172.16.1.5を受信 します。次のホストが172.16.1.6を受信します。これはスタティック変換ではなく、 timeout xlate hh:mm:ss コマンドで定義されている非アクティブ期間が過ぎると、タイムア ウトします。プール内のアドレスよりも多くの Inside ホストが存在する場合、プールの最 後のアドレスが Port Address Translation (PAT; ポート アドレス変換)に使用されます。

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 PAT を使用します。 global ステートメントに 1 つのアドレスが指定されている場合、そのアドレスはポート変換され ます。PIX ではインターフェイスごとに 1 つのポート変換が可能であり、この変換では、単一の グローバル アドレスへのアクティブな xlate オブジェクトが最大で 65,535 個サポートされます。 PAT を使用して Inside ホストが Outside ネットワークにアクセスするのを許可するには、次の手 順を実行します。

1. PAT に含める Inside グループを定義します(0.0 を使用すると、すべての Inside ホストを 選択することになります)。

nat (inside) 1 10.1.6.0 255.255.255.0

2. PAT で使用するグローバル アドレスを指定します。このアドレスには、インターフェイス アドレスを使用できます。 global (outside) 1 172.16.1.4 netmask 255.255.255.0

- 3. ASDM で Configuration > Features > NAT の順に選択し、Enable traffic through the firewall without address translation のチェックマークを外します。
- 4. Add をクリックして、NAT ルールを設定します。
- 5. Manage Pools をクリックして、PAT アドレスを設定します。
- 6. Outside > Add の順に選択し、Port Address Translation (PAT) をクリックして、PAT 用の 1 つのアドレスを設定します。
- 7. <u>アドレスを入力し、Pool ID を入力して、OK をクリックします。</u>

🚰 Add Global Pool Item	×
Interface: outside 💌 Pool ID: 1	
C Range	
Port Address Translation (PAT)	
C Port Address Translation (PAT) using the IP address of the interface	
IP Address: 172.16.1.4 -	
Network Mask (optional): 255.255.255.0	
OK Cancel Help	

- 8. Configuration > Features > NAT > Translation Rules の順に選択して、変換ルールを作成し ます。
- 9. 発信元インターフェイスとして inside を選択し、NAT を適用するアドレスを入力します。
- 10. Translate Address on Interface では、**Outside** を選択し、**Dynamic** を選択して、設定した アドレス プールを選択します。[OK] をクリックします。

• USEINAT	CU	ise Policy NAT					
Source Hos	t/Network						
		Interface: IP Address:	inside. 10.1.6.0		F		
		Mask	255 255 255 (Browse	D *	-		
							NAT Options
ranslate Add	ress on Inte	rface: outsi	de 💌				
Translate Ad	ddress To –						
Translate Ac بان O آ	ddress To – Btatic T Redirect (IP Address:			-		
Translate Ad C اب S C C	ddress To – Btatic Redirect ; © TCP © UDP	IP Address port Original port		Translate	f port]
Translate Ad ○ 1 1 2 [[• 1]] (ddress To – Static Redirect (TCP C UDP Dynamic	IP Address: port Original port Address Pool:	[[]	Translate	s port. Mana	age Pools]
Translate Ad	ddress To – Static T Redirect (TCP C UDP Dynamic Pool ID	IP Address: port Original port Address Pool:	[]] Add	Translate dress	T port. Mana	age Pools]
Translate Ad	ddress To – Btatic Redirect (TCP C UDP Dynamic Pool ID	IP Address oort Original port Address Pool: 172.16.1.4	[] [1 Ada	Translate Translate	s port. Mana	age Pools	

11. Configuration > Features > NAT > Translation Rules の順に選択すると、Translation Rules に変換が表示されます。

rione (C	onfiguration	Monitoring	Back Forward	Search Refresh :	Save Help		antillina ant
	<u>م</u> بو ا	3 🔒 🕺	₽ 8 6 6 6 9				
terfaces	E (Enable i	raffic through	the firewall without address	s translation:			
urity Policy	Translation	ion Rules	C Translation Exem	ption Rules			
34	Show Rule	s for interface	All Interfaces	T Show All			
NAT		o for meshace	[An interfaces				- ante
53	Rule		Original	1		Translated	
VPN	Туре	Interface	Source Network	Destination Network	Interface	Address	Edit
420	in the second	nside	₫⁷ 10.1,6,0/8	< any	outside	172.16.1.4	Delet
Routing							
80							
bal Objects							
bal Objects							
bal Objects							
bai Objects							
bail Objects							
bal Objects	×						

PAT を使用するときは、次の事項を考慮する必要があります。

- ・別のグローバル アドレス プール内にある IP アドレスは PAT では指定できない。
- PAT は H.323 アプリケーション、キャッシング ネーム サーバ、および Point-to-Point Tunneling Protocol (PPTP; ポイントツーポイント トンネリング プロトコル)と連携して機 能させることはできません。PAT は、Domain Name Service (DNS)、FTP と受動 FTP、 HTTP、メール、Remote-Procedure Call (RPC; リモート プロシージャ コール)、rshell、 Telnet、URL フィルタリング、および発信 traceroute とは連携します。
- ファイアウォール経由でマルチメディア アプリケーションを実行する必要があるときは、
 PAT を使用しない。マルチメディア アプリケーションは、PAT によって提供されるポート
 マッピングと競合する可能性があります。
- PIX ソフトウェア リリース 4.2(2) では、逆順で着信する IP データ パケットに対しては PAT 機能が働かない。PIX ソフトウェア リリース 4.2(3) ではこの問題が修正されています。
- global コマンドで指定されたグローバル アドレスのプール内の IP アドレスは、すべての外部ネットワーク アドレスを PIX でアクセス可能にするために、逆 DNS エントリを必要とする。逆 DNS マッピングを作成するには、アドレスとホスト名のマッピング ファイルにある、各グローバル アドレスに対応する DNS Pointer (PTR)レコードを使用します。PTR エントリがない場合、サイトではインターネット接続が低速または断続的になる可能性があり、 FTP 要求では常にエラーが発生します。たとえば、グローバル IP アドレスが 192.168.1.3 でPIX セキュリティ アプライアンスのドメイン名が pix.caguana.com の場合、PTR レコードは次のようになります。

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.

inside ホストから outside ネットワークへのアクセスの制限

有効な変換方式が発信元ホストに対して定義されており、ACL が発信元 PIX インターフェイスに 対して定義されていない場合、デフォルトでアウトバウンド接続が許可されます。ただし状況に よっては、発信元、宛先、プロトコル、ポートのいずれかまたはすべてに基づいたアウトバウン ドアクセス制限が必要です。そのためには、access-list コマンドで ACL を設定し、accessgroup コマンドでその ACL を接続発信元の PIX インターフェイスに適用する必要があります。 PIX 7.0 ACL は、インバウンドとアウトバウンド両方の方向に適用できます。次に示す手順は、1 つのサブネットに関してはアウトバウンド HTTP アクセスを許可する一方で、他のすべてのホス トによる Outside への HTTP アクセスを拒否し、それ以外のすべての IP トラフィックをすべて の人に対して許可する例です。

1. ACL を定義します。

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: PIX ACLはCisco IOS®ルータのACLとは異なり、PIXはCisco IOSのようなワイルドカー ドマスクを使用しません。その代わりに、正規のサブネット マスクを ACL 定義で使用しま す。Cisco IOS ルータと同様に、PIX の ACL には暗黙的な「deny all」が ACL の最後に存在 します。注:新しいアクセスリストエントリは、既存のACEの末尾に追加されます。最初に 特定のACEを処理する必要がある場合は、アクセスリスlineキーワードを使用できます。次 に、コマンドの要約の例を示します。

access-list acl_outbound line 1 extended permit tcp host 10.1.10.225 any 2. ACL を内部インターフェイスに適用します。

- 3. ASDMを使用して、ステップ1の最初のアクセスリストエントリを設定し、10.1.6.0/24からのHTTPトラフィックを許可します。[Configuration] > [Features] > [Security Policy] > [Access Rules]を選択します。
- 4. Add をクリックし、このウィンドウに表示される情報を入力し、OK をクリックします。

access-group acl_outbound in interface inside

🖆 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
10.1.6.0/24 Allow tr	any any
Protocol and Service	
C TCP C UDP C ICMP C IP Source Port Service = ▼ any Service Group ▼	Manage Service Groups Destination Port Service = v www Service Group
Please enter the description below (optional):	
	×
OK Car	Help

5.3 つの access-list エントリを入力したら、**Configuration > Feature > Security Policy >** Access Rules の順に選択し、これらのルールを表示します。



<u>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</u> <u>アクセスの許可</u>

ほとんどの組織では、その組織の信頼できるネットワーク内にあるリソースに対して信頼できな いホストのアクセスを許可する必要があります。その一般的な例は、社内 Web サーバです。デ フォルトでは、PIX は外部ホストから内部ホストへの接続を拒否します。NAT 制御モードでこの 接続を許可するには、static コマンドを access-list コマンドおよび access-group コマンドと組み 合せて使用します。NAT 制御がディセーブルになっている場合、変換を行わないのであれば、 access-list コマンドと access-group コマンドのみが必要です。

access-group コマンドで ACL をインターフェイスに適用します。このコマンドにより ACL がインターフェイスに関連付けられ、特定の方向に流れるトラフィックが検査されます。

Inside ホストの外部へのアクセスを許可する nat および global コマンドとは対照的に、static コ マンドでは、適切な ACL/グループが追加されている場合、両方向の変換が作成され、Inside ホス トによる外部へのアクセスと Outside ホストによる内部へのアクセスが許可されます。

このドキュメントで示した PAT の設定例では、Outside ホストからのグローバル アドレスへの接続が試みられると、そのアドレスが多数の Inside ホストに使用されてしまう可能性があります。 static コマンドでは 1 対 1 のマッピングが作成されます。access-list コマンドでは Inside ホスト に許可される接続のタイプが定義され、これはセキュリティ レベルの低いホストが高いホストに 接続する場合には常に必要です。access-list コマンドはポートとプロトコルの両方に基づき、ま たシステム管理者の裁量に基づいてアクセスを緩やかに許容したり、逆に厳しく制限したりでき ます。 このドキュメント内の「<u>ネットワーク ダイアグラム</u>」では、これらのコマンドを使用して、すべ ての信頼できないホストが Inside Web サーバに接続でき、信頼できないホスト 192.168.1.1 が同 じマシン上の FTP サービスにアクセスできるように PIX を設定する例を示しています。

<u>PIX バージョン 7.0 以降での ACL の使用</u>

PIX ソフトウェア バージョン 7.0 以降で、ACL を使用して次の手順を実行します。

1. NAT 制御がイネーブルになっている場合、Inside Web サーバに対して、Outside アドレス またはグローバル アドレスへのスタティック アドレス変換を定義します。

static (inside, outside) 172.16.1.16 10.16.1.16

2. どのホストがどのポートを使用して Web/FTP サーバに接続できるかを定義します。

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. アクセスリストを、アクセスグループを使って外部インターフェイスに適用します。

access-group 101 in interface outside

- 4. ASDM を使用してこのスタティック変換を作成するには、Configuration > Features > NAT の順に選択して、Add をクリックします。
- 5. 発信元インターフェイスとして inside を選択し、スタティック変換を作成する対象である内 部アドレスを入力します。
- 6. **Static** を選択し、変換先 Outside アドレスを IP address フィールドに入力します。[OK] を クリックします。

• Use NAT	OU	se Policy NAT					
Source Host/Ne	etwork						
		Interface: IP Address: Mask:	inside 10.16.1.16 255.255.255.25	5	-		
anslate Addres	s on Inter	face: outsi	de 💌			NAT	Options
Translate Addre	ess To — lic	IP Address:	172.16.1.16	¥.			
Franslate Addre • • • • Stat	ess To — lic Cedirect p IC TCP IC UDP	IP Address: ort Original port	172.16.1.16 T	T	rt:		
Franslate Addre Translate Addre Stat F F Dyn	ess To — ic (edirect p IC TCP IC UDP amic	IP Address: ort Original port Address Por	172.16.1.16 T	ranslated po	rt: Manage F	°ools	
Translate Addre Translate Addre Stat Dyn	ess To — ic Cedirect p C UDP amic Pool ID	IP Address: ort Original port Address Por	172.16.1.16 T Same address Addre	ranslated po	rt: Manage f	200IS	
Translate Addre	ess To — ic (edirect p (C UDP amic 2001 ID	IP Address: ort Original port Address Poc	172.16.1.16 T Same address Addre	ranslated po	rt: Manage F	Pools	

7. Configuration > Features > NAT > Translation Rules の順に選択すると、Translation Rules に変換が表示されます。

ile Rules Se	arch Options	Tools Wiza	ds Help				Charle Suprem
Home C	Sonfiguration	Monitoring	Back Forward	Q Q Search Refresh	Save Help		
Niterfaces	Configuration	≥ NAT > Trans I IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	lation Rules Ba Ba Ba Ba Ba Sa Sa Sa the firewall without address C Translation Exem	s translation			
NAT	Rule	les for interface	Criginal	Show All		Translated	Add
VPN	Туре	Interface	Source Network	Destination Network	Interface	Address	Edit
Routing Global Objects Properties							
	i¶ static	NAT 📲	Dynamic NAT 🔒 Ste	itic Policy NAT	Dynamic Policy N	IAT Manage Pools	•

 Inside ホストから Outside ネットワークへのアクセスの制限」の手順を使用して、 access-list のエントリを入力します。注:これらのコマンドを実装する場合は注意してくだ さい。access-list 101 permit ip any any コマンドを実装すると、アクティブな変換がある限 り、信頼できないネットワーク上の任意のホストが、信頼できるネットワークの任意のホス トに IP を使用してアクセスできます。

<u>特定のホストおよびネットワークでの NAT の無効化</u>

NAT 制御を使用し、Inside ネットワーク上にパブリック アドレスが存在し、特定の Inside ホストが変換なしで Outside にアクセスできるようにする必要がある場合は、nat 0 または static コマンドを使用して、これらのホストに対して NAT をディセーブルにすることができます。

nat コマンドの例を次に示します。

nat (inside) 0 10.1.6.0 255.255.255.0 ASDM を使用して特定のホスト/ネットワークに対して NAT をディセーブルにするには、次の手 順を実行します。

- 1. Configuration > Features > NAT の順に選択し、Add をクリックしします。
- 2. 発信元インターフェイスとして inside を選択し、スタティック変換を作成する対象である内 部アドレス/ネットワークを入力します。
- 3. Dynamic を選択し、Address Pool には同じアドレスを選択します。[OK] をクリックします

Edit Address 1	ranslation R	ule						
🖲 Use NAT	r ou	se Policy NAT						
Source Ho	st/Network							
		Interface:	incide		ন			
		intenace.			_			
		IP Address:	10.1.6.0					
		Mask:	255.255.255.0		~			
			Browse					
							NAT Options	1
Translate Ad	dress on Inter	rface: outsid	ie 💌			_		
- Translate	Address To	,	_					
C ala	01-5-	(D. talabase et						
0.4	Bedirect n	IP Address:	1					
	© TOP © UDP	Original port:	Т	ranslated po	rt 📃			
• 📲	Dynamic	Address Pool:	same addres	s 💌	Manage F	ools		
	Pool ID		Addre	ess				
	N/A	No address po	ol defined					
	-							

4. **Configuration > Features > NAT > Translation Rules** の順に選択すると、Translation Rules に新しいルールが表示されます。

Home C	anniguration	Monitoring	Back	Eorward	Search	Refresh	Seve	? Help		
eatures	Configuration	= Features = I	VAT = Transi	ation Rules						
terfaces by arity Policy	● ☆ ♥ F Enable © Transk Show Ru	e traffic through ation Rules las for Interface	the firewalls C Tra	R R Straight	ss translation mption Rules	how All				
NAT	Rule	Rule Original							Translated	Add
Set.	Туре	Type Interface Source Network		Destinat	ion Network	Interfa	ace	Address	Edit	
VPN		inside	dF 10.1 8.0	1/24	🥠 any		outside	sam	e as original addres	e Delet
ofre Blacks Device winistration	×									L
	斗 Static	NAT (]]	Dynamic N/	а 🕼 ти	latic Policy N/	ज _∰ 	Dynamic Po	alicy NAT	Manage Pools	
					ADDIV	6	Rese	35		

5. (発信元と宛先に基づいて)変換しないトラフィックをより細かく制御できる ACL を使用 する場合は、次のコマンドを使用します。

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

- 6. ASDM を使用し、Configuration > Features > NAT > Translation Rules の順に選択します。
- 7. Translation Exemption Rules を選択し、Add をクリックしします。次の例に、10.1.6.0/24 ネットワークから任意の場所へのトラフィックを変換から除外する方法を示します。

Edit Address Translation Rule	x
Action Select an action: exempt	
Host/Network Exempted From NAT	When Connecting To
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 Ca	ncel Help

8. Configuration > Features > NAT > Translation Exemption Rules の順に選択して、新しいル ールを表示します。



9. Web サーバに対する static コマンドは、次の例に示すように変わります。

static (inside, outside) 10.16.1.16 10.16.1.16

- 10. ASDM から、Configuration > Features > NAT > Translation Rules の順に選択します。
- 11. Translation Rules を選択し、Add をクリックしします。発信元アドレス情報を入力し、 Static を選択します。IP Address フィールドに同じアドレスを入力します。

0001411	C Use Polic	y NAT		
Source Host/Ne	atwork			
	Interface	e: inside		
	IP Addre	ess: 10.16.1.16		
	Mask	255.255.255.255	-	
		Browse		
			NAT Opt	ons
anslate Addres	s on Interface:	outside		
Translate Addro	ess To			
Translate Addre	ess To ic IP Addre	ass: 10.16.1.16	V	
Translate Addre I i stat	ess To ic IP Addre edirect port	ass: 10,16.1.16	¥	
Translate Addro 1 Stat	ess To ic IP Addre redirect port TCP Origin	ess: 10.16.1.16	ated port	
Translate Addro Translate Addro Transl	ess To ic IP Addre edirect port TCP Origin CUDP Addre	ess: 10.16.1.16 hel port Transl ss Pool: Same address 💽	lated port	
Translate Addre Translate Addre Stat Translate Addre Translate Addre Tr	ess To ic IP Addre redirect port © TCP © UDP Origin amic Addre	ess: 10.16.1.16 nel port: Transi es Pool: Same address I Address	ated port	
Translate Addre	ess To ic IP Addre redirect port TCP Origin CUDP Origin amic Addre	ess: 10.16.1.16 nel port Transi es Pool: Same address I Address	ated port	
Translate Addre	ess To ic IP Addre redirect port TCP Origin CUDP Origin amic Addre	ess: 10.16.1.16 nel port Transi es Pool: Same address I Address	lated port.	
Translate Addre	ess To ic IP Addre redirect port TCP Origin CUDP Origin amic Addre	ess: 10.16.1.16 nel port Transi es Pool: Same address I Address	Inted port	

12. Configuration > Features > NAT > Translation Rules の順に選択すると、Translation Rules に変換が表示されます。

	Configuration > NAT > Tr	anslation Rules	•			
	٠ 🖻 🕸 🛬 🕈	3 阳 R 🖗 🛍 🗳 l				
6 A	🗆 Enable traffic throu	igh the firewall without addres	s translation			
urity Policy	Translation Rules	C Translation Exen	nption Rules			
28	Show Rules for Interf	ace: All Interfaces	Show All			
NAT	Rule	Original			Translated	Add
VPN	Type Interface	e Source Network	Destination Network	Interface	Address	Edit
30	, inside	g [□] 10.16.1.16	🛷 any	outside	10.16.1.16	Dele
Routing			de c			
80						
oal Objects						
xel Objects						
oal Objects						
pai Objects						
operfiles						

13. ACL を使用する場合は、次のコマンドを使用します。

access-list 102 permit tcp any host 10.16.1.16 eq www access-group 102 in interface outside ASDM での ACL の設定についての詳細は、このドキュメントの「<u>Inside ホストから</u> <u>Outside ネットワークへのアクセスの制限</u>」セクションを参照してください。ネットワー ク/マスクを指定しながら nat 0 を使用する場合と、Inside からのみの接続開始を許可する ネットワーク/マスクを使う ACL を使用する場合の違いに注意してください。nat 0 ととも に ACL を使用すると、インバウンドまたはアウトバウンド トラフィックによる接続の開 始が可能になります。PIX インターフェイスを別のサブネットに配置して、到達可能性に 問題が発生しないようにする必要があります。

<u>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)</u>

PIX 6.0 では、ポート リダイレクション(フォワーディング)機能が追加されたことにより、 Outside ユーザが特定の IP アドレス/ポートに接続し、PIX がトラフィックを適切な Inside サー バ/ポートにリダイレクトすることが可能になりました。また、static コマンドが変更されていま す。共有アドレスを一意のアドレスまたは共有アウトバウンド PAT アドレスにしたり、外部イン ターフェイスと共有させることができます。この機能は、PIX 7.0 で利用できます。

注:スペースの制限により、コマンドは2行で表示されます。

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:スタティックNATが外部IP(global_IP)アドレスを変換に使用する場合、変換が発生する可能 性があります。そのため、スタティック変換では IP アドレスではなくキーワード interface を使 用します。

このネットワークの例でのポート リダイレクション(フォワーディング)は次のようになります 。

- 外部ユーザは Telnet 要求を一意の IP アドレス 172.18.124.99 に送り、PIX はこれを 10.1.1.6 にリダイレクトする。
- 外部ユーザは FTP 要求を一意の IP アドレス 172.18.124.99 に送り、PIX はこれを 10.1.1.3 にリダイレクトする。
- 外部ユーザは Telnet 要求を PAT アドレス 172.18.124.208 に送り、PIX はこれを 10.1.1.4 に リダイレクトする。
- 外部ユーザは Telnet 要求を PIX Outside IP アドレス 172.18.124.216 に送り、PIX はこれを 10.1.1.5 にリダイレクトする。
- 外部ユーザは HTTP 要求を PIX 外部 IP アドレス 172.18.124.216 に送り、PIX はこれを 10.1.1.5 にリダイレクトする。
- 外部ユーザは HTTP ポート 8080 要求を PAT アドレス 172.18.124.208 に送り、PIX はこれ を 10.1.1.7 のポート 80 にリダイレクトする。

この例では、ACL 100を使用して、内部から外部への一部のユーザのアクセスをブロックします 。この手順はオプションです。ACL を設定しなければ、すべてのトラフィックは発信が許可され ます。



ネットワーク ダイアグラム:ポート リダイレクション(フォワーディング)

<u>PIX 部分設定 - ポートリダイレクション</u>

次に抜粋した設定では、スタティック ポート リダイレクション(フォワーディング)の使用方法 を示しています。 「<u>ポート リダイレクション(フォワーディング)のネットワーク ダイアグラ</u> PIX 7.x 設定の抜粋:ポート リダイレクション(フォワ ーディング)

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 accesslist 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: PIX/ASAにsysopt noproxyarp outsideコマンドが設定されている場合、ファイアウォールは PIX/ASAでproxyarpおよびスタティックNAT変換を実行できません。これを解決するには、 PIX/ASA設定でsysopt noproxyarp outsideコマンドを削除し、gratuitous ARPを使用してARPエン トリを更新します。これにより、スタティックNATエントリが正常に動作できるようになります。

この手順は、ポート リダイレクション(フォワーディング)を設定する方法の例で、外部ユーザ は Telnet 要求を一意の IP アドレス 172.18.124.99 に送信でき、PIX はこれを 10.1.1.6 にリダイ レクトします。

- 1. ASDM を使用し、Configuration > Features > NAT > Translation Rules の順に選択します。
- 2. Translation Rules を選択し、Add をクリックしします。
- 3. Source Host/Network には、Inside IP アドレスの情報を入力します。
- 4. Translate Address To では、**Static** を選択し、Outside IP アドレスを入力して、**Redirect port** にチェックマークを付けます。
- 5. 変換前および変換後のポート情報を入力します(この例ではポート 23 が維持されます)。 [OK] をクリックします。

🔂 Add Address Translation	Rule						x
Use NAT C	Use Policy NAT						
- Source Host/Network							-
	Interface:	inside		•			
	IP Address:	10.1.1.6		_			
	Mask:	- 	6 266	-			
	index.	200.200.20	0.200	<u> </u>			
		Browse					
					Γ	NAT Options	1
Translate Address on in	terface: outsid	de 🔻	1		_		_
G ulu Otatio	ID åddroppi	170 10 10		a			
Redirec	t port	p72.18.124	.99				
© TOP	,				_		
CUD	Original port: P	23	Translated	port: 23			
C 🖞 Dynamic	Address Pool:	same add	ress 🔻	Manage	Pools		
Pool ID		Ad	dress				
					_		
	OK	Can	cel	Help			
	OK	Can	cel	Help			

Configuration > Features > NAT > Translation Rulesの順に選択すると、Translation Rules に変換 が表示されます。

🚮 Iome Co	onfiguration	Monitoring	Back Forward	Search Retresh	Save Hel	p	Cisco Sys
atures	Configuration	n = Feiltures = N	IAT - Translation Rules				
	* * *	1 1 %	Q. ■ ● ■ ● ■				
rfaces	Enable	e traffic through	the firewall without addres	ss translation			
a.	@ Transl	ation Bules	C Translation Even	notion Rules			
ty Policy							
34.	Show Ru	iles for Interface	All Interfaces	Show All			
IAT	Rulé		Original			Add	
	Туре	Interface	Source Network	Destination Network	Interface	Address	Edit
VIPIN	1	Inside	A 10.1.1.5	🧆 any	outside	172.18.124.98	Delet
N.		- -	Port: 23/tcp			Port 23ftcp	
outing							
8							
ng Blocks							
3							
evice							
20 perties							
	1						1
	·[* Statio	t NAT	Dynamic NAT 🛛 🖓 St	atic Policy NAT 🛛 🔒 C	ynamic Policy	NAT Manage Pool	5
				Analy	Reset		
				C10000 1	110001		

<u>static を使用した TCP/UDP セッションの制限</u>

TCP または UDP セッションを PIX/ASA 内に配置されている内部サーバに制限する必要がある場合は、static コマンドを使用します。

サブネット全体の同時 TCP および UDP 接続の最大数を指定します。デフォルトは 0 で、接続が 無制限であることを意味します(アイドル状態の接続は、timeout conn コマンドにより指定され たアイドル タイムアウトが経過した後に閉じられます)。 このオプションは、Outside NAT に適 用されません。セキュリティ アプライアンスは、セキュリティ レベルの高いインターフェイスか らセキュリティ レベルの低いインターフェイスへの接続のみを追跡します。

初期接続数を制限すると、DoS 攻撃からの保護になります。セキュリティ アプライアンスは、初 期制限を使用して TCP インターセプトをトリガします。これにより、TCP SYN パケットでイン ターフェイスをフラッディングすることにより行われる DoS 攻撃から Inside システムが保護さ れます。初期接続は、発信元と宛先の間で必要なハンドシェイクを完了していない接続要求です 。このオプションは、Outside NAT に適用されません。TCP インターセプト機能は、セキュリテ ィレベルの高いホストまたはサーバにのみ適用されます。Outside NAT に初期制限を設定した場 合、初期制限は無視されます。

以下に、いくつかの例を示します。

time specified !--- by the **timeout conn** command !--- The maximum number of embryonic connections per host is **100**.

%PIX-3-201002:{static|xlate} global_addressの接続が多すぎます! ens nconns

これは接続に関連したメッセージです。このメッセージがログに記録されるのは、指定のスタティック アドレスへの最大接続数を超えた場合です。econns 変数は初期接続の最大数で、nconns は static または xlate に許可されている接続の最大数です。

スタティック アドレスへの接続に課せられている制限を確認するには、show static コマンドを使 用することを推奨いたします。この制限は設定可能です。

%ASA-3-201011:インターフェイスOutsideの10.1.26.51/2393から10.0.86.155/135への着信パケットの接続制限が1000/1000を超えました

このエラーメッセージは、Cisco Bug ID <u>CSCsg52106(登録ユーザ</u>専用)に起因します。 詳細は、 このバグを参照してください。

<u>時間ベースのアクセス リスト</u>

時間範囲を作成してもデバイスへのアクセスは制限されません。time-range コマンドで定義され るのは時間範囲だけです。時間範囲を定義してから、これをトラフィック ルールやアクションに 適用できます。

時間ベース ACL を実装するには、time-range コマンドを使用して、日および曜日の特定の時間を 定義します。続いて with the access-list extended time-range コマンドを使用して、その時間範囲 を ACL にバインドします。

時間範囲はセキュリティ アプライアンスのシステム クロックに基づきます。ただし、この機能は NTP 同期とともに使用すると最も効果的です。

時間範囲を作成し、時間範囲の設定モードを入ると、absolute および periodic コマンドを使用し て時間範囲のパラメータを定義できます。time-range コマンドの absolute キーワードと periodic キーワードをデフォルト設定に復元するには、時間範囲設定モードで default コマンドを使用しま す。

時間ベース ACL を実装するには、time-range コマンドを使用して、日および曜日の特定の時間を 定義します。続いて with the access-list extended コマンドを使用して、時間範囲を ACL にバイ ンドします。次の例では、「Sales」という名前の ACL を「New York Minute」という名前の時 間範囲にバインドしています。

この例では、「New York Minute」という名前の時間範囲を作成し、時間範囲設定モードに入り ます。

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

<u>テクニカルサポートのサービス リクエストをオープンする際に</u>

<u>収集する情報</u>

依然としてサポートが必要で、Cisco テクニカルサポー トでサービス リクエストをオープンする場合は、ご使用 の PIX セキュリティ アプライアンスのトラブルシューテ ィングにために、必ず下記の情報を添付するようにして ください。

- •問題の説明と関連するトポロジの詳細
- サービス リクエストをオープンする前のトラブルシ ューティングに使用した手順
- show tech-support コマンドの出力
- logging buffered debugging コマンド実行後の show log コマンドの出力、あるいは、問題を示す画面キャ プチャ(採取されている場合)

収集したデータは、圧縮しないプレーン テキスト形式 (.txt)でサービス リクエストに添付してください。 情 報をサービス リクエストに添付するには、<u>TAC Service</u> <u>Request Tool</u>(登録ユーザ専用)を使用します。 <u>TAC</u> <u>Service Request Tool</u>(登録ユーザ専用)にアクセスで きない場合は、情報をEメールの添付ファイルとし、メ ッセージの件名にサービス リクエスト番号を付けて <u>attach@cisco.com</u> 宛てに送信してください。一部ツール については、ゲスト登録のお客様にはアクセスできない 場合がありますことを、ご了承ください。

関連情報

- <u>PIX セキュリティ アプライアンスに関するサポート ページ</u>
- <u>PIX コマンド リファレンス</u>
- <u>Cisco Adaptive Security Device Manager (ASDM) Troubleshoot and Alerts</u>
- <u>Requests for Comments (RFCs)</u>
- <u>テクニカル サポートとドキュメント Cisco Systems</u>