ASA 7.x/PIX 6.x 以降 : ポートのオープンまたは ブロックの設定例

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

 設定

 ネットワーク図

 ポートをブロッキングする設定

 ポートをオープンする設定

 ASDM 経由の設定

 確認

 トラブルシュート

 関連情報

<u>概要</u>

このドキュメントでは、セキュリティ アプライアンスで各種トラフィック(http、ftp など)に対 してポートをオープンまたはクローズする方法に関する設定例について説明します。

注:「ポートを開く」および「ポートを許可する」という用語は、同じ意味を持ちます。同様に 、「ポートをブロッキングする」と「ポートを制限する」も同じ意味を示します。

前提条件

<u>要件</u>

このドキュメントでは、PIX/ASA が設定されていて適切に動作していることを前提としています 。

<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。

 バージョン 8.2(1) で稼働する Cisco 5500 シリーズ適応型セキュリティ アプライアンス (ASA) • Cisco Adaptive Security Device Manager (ASDM) バージョン 6.3(5)

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、ソフトウェア バージョン 6.x 以降の Cisco 500 シリーズ PIX ファイアウォール ア プライアンスにも適用できます。

<u>表記法</u>

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>設定</u>

各インターフェイスのセキュリティレベルは、0(最低)から100(最高)にする必要がありま す。たとえば、内部ホストネットワークなどの最もセキュアなネットワークをレベル100に割り 当てる必要があります。インターネットに接続する外部ネットワークはレベル0にできますが、 DMZなどの他のネットワークは中間に配置できます。複数のインターフェイスを同じセキュリティレベルに割り当てることができます。

デフォルトでは、セキュリティ アプライアンスの外部インターフェイス(セキュリティ レベル 0)ではすべてのポートがブロックされ、内部インターフェイス(セキュリティ レベル 100)で はすべてのポートがオープンになります。このように、すべての発信トラフィックは設定なしで セキュリティ アプライアンスを通過できますが、着信トラフィックはセキュリティ アプライアン スのアクセス リストとスタティック コマンドの設定によって許可できます。

注:一般に、すべてのポートはLower Security ZoneからHigher Security Zoneにブロックされ、す べてのポートはHigher Security ZoneからLower Security Zoneにオープンして、インバウンドとア ウトバウンドの両方のトラフィックに対してステートフルインスペクションが有効になります。

このセクションは、次に示すサブセクションで構成されます。

- <u>ネットワーク図</u>
- <u>ポートをブロッキングする設定</u>
- <u>ポートをオープンする設定</u>

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供して います。

注:このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool(登録ユーザ専用)を参照してください。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。

<u>ネットワーク図</u>

このドキュメントでは、次のネットワーク セットアップを使用します。



<u>ポートをブロッキングする設定</u>

セキュリティ アプライアンスは、拡張アクセス リストで明示的にブロックされていない限り、あ らゆる発信トラフィックの通過を許可します。

アクセス リストは、1 つ以上のアクセス コントロール エントリで構成されます。アクセス リストの種類によっては、送信元および宛先アドレス、プロトコル、ポート(TCP または UDP の場合)、ICMP のタイプ(ICMP の場合)または EtherType を指定できます。

注:ICMPなどのコネクションレス型プロトコルの場合、セキュリティアプライアンスは単方向セッションを確立するため、両方向(送信元インターフェイスと宛先インターフェイスへのアクセスリストの適用)にアクセスリストが必要か、ICMPインスペクションエンジンを有効にする必要があります。ICMP インスペクション エンジンは、ICMP セッションを双方向接続として扱います。

ポートをブロックするには、次の手順を実行します。通常は、内部(高いセキュリティ ゾーン)から DMZ(低いセキュリティ ゾーン)、または DMZ から外部に対して発信されるトラフィックに適用されます。

次のように、指定されたポートのトラフィックをブロックする方法でアクセス コントロール リストを作成します。

access-list

2. 次に、access-group コマンドを使用してアクティブにするアクセス リストをバインドします。

access-group

/m.i	
451	•
L N J	

 HTTP ポート トラフィックのブロック: DMZ ネットワークに配置された IP 172.16.1.1 を持 つ http (Web サーバ)へのアクセスから内部ネットワーク 10.1.1.0 をブロックするには、 次のように ACL を作成します。 ciscoasa(config)#access-list 100 extended deny tcp 10.1.1.0 255.255.255.0 host 172.16.1.1 eq 80 ciscoasa(config)#access-list 100 extended permit ip any any ciscoasa(config)#access-group 100 in interface inside
 注:ポートのブロックを解除するには、noの後にaccess listコマンドを続けて使用します。

2. FTP ポート トラフィックのブロック: DMZ ネットワークに配置された IP 172.16.1.2 を持 っFTP(ファイル サーバ)へのアクセスから内部ネットワーク 10.1.1.0 をブロックするに は、次のように ACL を作成します。 ciscoasa(config)#access-list 100 extended deny tcp 10.1.1.0 255.255.255.0 host 172.16.1.2 eq 21 ciscoasa(config)#access-list 100 extended permit ip any any ciscoasa(config)#access-group 100 in interface inside

注:ポートの割り当てに関す<u>る詳細</u>については、IANAのポートを参照してください。

このセクションでは、ASDM 経由で設定を行う詳細な手順を紹介しています。

1. [Configuration] > [Firewall] > [Access Rules] に移動します。アクセス リストを作成するため に、[Add Access Rule] をクリックします。

Add Access Rule			
the second se			Destination
Insert	-	.10.100	🌍 any
🖃 🖏 inside (2 outgoi	ng rules)		any any
1	. 172.1	6.10.50	🏟 any
2	🏈 any		🏟 any

2. このアクセス ルールが関連付けられるインターフェイスとともに、アクセス ルールの送信

元と宛先およびアクションを定義します。詳細を選択し、ブロックする特定のポートを選択

Add Acc	ess Rule		
Interface: (inside 🔽 🌖		
Action: 🔘	ermit 💿 Deny		
Source: (10.1.1.0		[]
Destination	172,16.1.1		
Service:	ip		
Description:			
Enable L	ogging		
Logging I	evel: Default	~	
More Opt	005		
, for c opc	UID		
		ОК	Cancel

3. 使用できるポートのリ<u>ストから [http] を選択し、[OK] をクリックして [Add Access Rule]</u>ウ

libert						FV
Narte	Protocol	Source Ports	Destination Ports	ICMP Type	Description	
- 18 discard	top	default (1-65535)	9			
- me damain	top	default (1-65535)	53			
- me echo	top	default (1-65535)	7			
18 ovec	top	default (1-65535)	512			
339 finger	top	default (1-65535)	79			
- ate-ftp	top	default (1-65535)	21			
12 ftp-data	top	default (1-65535)	20			
- 18- gopher	top	default (1-65535)	70			
10 h323	top	default (1-65535)	1720			
38 hostname	top	default (1-65535)	101			
ap nto	top.	default (1-65535)	80	8. c	10	
Mtps	top	default (1-65535)	443			
12- ident	top	default (1-65535)	113			
- 18 in ap4	top	default (1-65535)	143			
mire	top	default (1-65535)	194			
328 Revberos	top.	default (1-65535)	750			
na- kiogn	top	default (1-65535)	543			
11 Jubel	top	default (1-65535)	544			
- att-Idap	top	default (1-65835)	389			
-ma-lidaps	top	default (1-65535)	636			
alastari Kendre	×	—XeX				

ィンドウに戻ります。

4. [OK] をクリックして、アクセス ルールの設定を完了します。

🖆 Add Aco	cess Rule
Interface:	inside. 💌
Action: 🔘	Permit 💿 Deny
Source:	10.1.1.0
Destination	172.16.1.1
Service:	(tcp/http
Description:	
Enable L	Level: Default
More Opt	tions
	OK Cancel Help
同じアクセス	リストにアクセス ルールを追加するには、[Insert After] をクリック
Configuratio	on > Firewall > Access Rules

5. ます。

÷	Add Access Rule		Destination
÷	Insert	1	
4	Insert After		💻 172.16.1.1
			🏈 any
ė 🎝	🕈 manage (2 implicit inco	oming rules)	
1	🏈 a	ny	Any less secu
2	🥝 a	nγ	any 🖉

6.「any」から「any」へのトラフィックを許可し、「暗黙拒否」を回避します。 次に、[OK] をクリックして、このアクセス ルールの追加を完了します。

🚰 Insert A	fter Access Rule
Interface:	inside 😽
Action: 💿	Permit 🔿 Deny
Source:	any
Destination	any 💮
Service:	ip 🗔
Description:	
💽 Enable L	ogging
Logging	Level: Default
More Opt	ions
	OK Cancel Help

7. 設定したアクセス リストは、[Access Rules] タブに表示されます。[Apply] をクリックして 、セキュリティ アプライアンスに設定を送信します。

¥	Enabled	Source	Destination	Service	Action	Hits
🥵 in	side (3 incom	ing rules)				
1		■ 10.1.1.0	172.16.1.1	100/ http	😮 Deny	0
2		< any	🔄 any	😰 ip	🧹 Permit	0
3		🌍 any	🌍 any	<u>⊥</u> /ip	🕴 Deny	
🥵 m	anage (2 imp	licit incoming rules)				
1		🏟 any	Any less secure ne	IP ip	🖌 Permit	
2		🌑 any	🏟 any	1e> ip	😮 Deny	
🥬 ot	itside (1 impl	licit incoming rule)				
1		any	 any 	IP ip	3 Deny	
왜						

ASDM から送信された設定の結果は、ASA のコマンドライン インターフェイス(CLI)の 次のコマンド セットになります。 access-list inside_access_in extended deny tcp host 10.1.1.0 host 172.16.1.1 eq www access-list inside_access_in extended permit ip any any access-group inside_access_in in interface inside

この手順では、10.1.1.0ネットワークがWebサーバ172.16.1.1にアクセスするのをブロック するために、例1がASDMを介して実行されています。例2も、10.1.1.0ネットワーク全体が FTPサーバ172.16.1.2にアクセスすることをブロックする方法と同じです。唯一の違いは、 ポートを選択する点です。注:このアクセスルール設定(例2)は、新しい設定であると想 定されています。

8. FTP トラフィックをブロックするアクセス ルールを定義し、[Details] **タブをクリックして 宛先ポートを選択します。**

🚰 Add Acc	ess Rule
Interface:	inside 💌
Action: 🔘 I	Permit 💿 Deny
Source:	10.1.1.0
Destination	172.16.1.1
Service:	ip (iii)
Description:	
🔽 Enable L	ogging
Logging I	Level: Default 💙
More Opt	ions
	OK Cancel Help

9. [ftp] ポートを選択し、[OK] をクリックして [Add Access Rule] ウィンドウに戻ります。

ter:					
Jame	Protocol	Source Ports	Destination Ports	ICMP Type	Description
100 cibrix-ica	tcp	default (1-65535)	1494		
tiqbe	tcp	default (1-65535)	2748		
- 100 daytime	tcp	default (1-65535)	13		
ter discard	top	default (1-65535)	9		
👷 domain	tcp	default (1-65535)	53		
w echo	top	default (1-65535)	7		
to exec	tcp	default (1-65535)	512		
10 finger	tcp	default (1-65535)	79		
- ඟ ftp	top	default (1-65535)	21		-
ttp-data	top	default (1-65535)	20		
gopher	tcp	default (1-65535)	70		
10 h323	tcp	default (1-65535)	1720		
👷 hostname	tcp	default (1-65535)	101		
tte http	top	default (1-65535)	80		
- 😥 https	top	default (1-65535)	443		
ident	tcp	default (1-65535)	113		
10 imap4	tcp	default (1-65535)	143		
TO inc	tcp	default (1-65535)	194		
- 100 kerberos	tcp	default (1-65535)	750		
and Marsia	ten.	dofout (1 ceeses	E40		
lected Service					

-10. [OK] をクリックして、アクセス ルールの設定を完了します。

🖆 Add Acc	ess Rule
Interface:	inside 💌
Action: 🔘	Permit 💿 Deny
Source:	10.1.1.0
Destination	172.16.1.1
Service:	tcp/ftp
Description:	
💽 Enable L	ogging
Logging I	Level: Default 💉
More Opt	ions
	OK Cancel Help

11. その他のトラフィックを許可する別のアクセス ルールを追加します。そうしないと、暗黙 拒否ルールによってインターフェイス上のすべてのトラフィックがブロックされます。

Interface	inside	~			
Action:	🗩 Permit (🔵 Deny			
Source:	any				
Dectinatio					
Descinacio					
Service:	ip				
Descriptio	n:				
3					
💌 Enable	e Logging				
	a ta su ta 🗖	22.302			
Logain	id Level: 100	eraulo			
Loggir	ig Level: Di	erault 💌			
Loggir More O	ptions		OK Cancel	ה	
Loggir More 0 成したア	ptions クセスリス	erault くトの設定は、[A	OK Cancel Access Rules] タブの下][「に次のように表:	示されます。
Loggir More O 成したア Configurat	ig Level: し ptions クセスリス ion > Firewa	erault くトの設定は、[A all > Access Rule	OK Cancel Access Rules] タブの下	〕[「に次のように表	示されます。
Loggir More O 成したア Configurati	ig Level: し ptions クセスリス ion > Firewa ぼ Edit 値	erault くトの設定は、[A all > Access Rule Delete ナ チ	OK Cancel Access Rules] タブの下 5 ※ 唱 電 へ Q Find)[「に次のように表: En Diagram)。」E	示されます。 cport ・ 69 Cle
Loggir More O 成したア Configurati	ig Level: し ptions クセスリス ion > Firewa ご Edit 1 Enabled	erault くトの設定は、[A all > Access Rule Delete ナ チ Source	OK Cancel Access Rules] タブの下 S & B M - Q Find Destination) 「に次のように表: 「En Diagram 」」 Service	示されます。 cport ・ 67 Cle Action
Loggir More O 成したア Configurati	ig Level: し ptions クセスリス ion > Firewa ion > Firewa Enabled de (3 incoming	erault くトの設定は、[A all > Access Rule Delete 今 ← Source grules)	OK Cancel Access Rules] タブの下 S & Pa R - Q Find Destination	こ に次のように表: En Diagram 。この Service	示されます。 cport - 69 Cle Action
Loggir More O 成したア Onfigurat 争 Add ・ #	ig Level: し ptions クセスリス ion > Firewa Enabled de (3 incoming	erault くトの設定は、[A all > Access Rule Delete 今 く Source grules) 10.1.1.0	OK Cancel Access Rules] タブの下 & & Pa R - Q Find Destination	こに次のように表 に次のように表 Diagram ここの Service	示されます。 cport - 69 Cle Action
Loggir More O 成したア onfigurat 争 Add +	ig Level: Di ptions クセスリス ion > Firewa ion > Firewa Enabled de (3 incoming	erault 、トの設定は、[A all > Access Rule Delete ク チ Source grules) 10.1.1.0	OK Cancel Access Rules] タブの下 S B Destination I 172.16.1.1	C に次のように表: C に次のように表: Diagram 。 E Service	示されます。 cport - 69 Cle Action ③ Deny 《 Perm
Loggir More O 成したア Onfigurat 中 Add ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・	ig Level: Di ptions クセスリス ion > Firewa ion > Firewa Enabled de (3 incoming	erault A トの設定は、[A all > Access Rule Delete ク チ Source grules) 10.1.1.0 の any シ any Lincoming rules)	OK Cancel Access Rules] タブの下	Cに次のように表: Cに次のように表: Diagram 。この Service 1000 ftp 1000 ftp 1000 ftp 1000 jp	示されます。 cport ・ 6分 Cle Action ② Deny ② Deny ③ Deny
Loggir More O 成したア Configurati ゆ Add ・ # 1 2 3 3 3 3 3 1	ig Level: し ptions クセスリス ion > Firewa Enabled de (3 incoming で age (2 implici	erault くトの設定は、[A all > Access Rules Delete クチー Source grules) 10.1.1.0 any any tincoming rules) any	OK Cancel Access Rules] タブの下	に次のように表: 「に次のように表: Diagram 。」E Service	示されます。 (port + 6) Cle Action ③ Deny ③ Deny ④ Perm
Loggir More O 成したア Onfigurat 中 Add ・ # 日 学 insic 1 2 3 日 学 mar 1 2	ig Level: し ptions クセスリス ion > Firewa ion > Firewa Enabled de (3 incoming で inage (2 implici	erault A トの設定は、[A all > Access Rule Delete 今 ← Source grules) I 10.1.1.0 any any t incoming rules) any any any	OK Cancel Access Rules] タブの下 と しestination ② any ③ Any less secure i ③ any	に次のように表: をに次のように表: Diagram 。 E Service 100 ftp 100 ftp 100 ip 100 jp 100 jp	示されます。 (port + (か) Cle Action ③ Deny ③ Deny ④ Perm ③ Deny
Loggir More O 成したア Onfigurat 中 Add マ ダ insit 1 2 3 第 mar 1 2	ig Level: し ptions クセスリス ion > Firewa Enabled de (3 incoming レー inage (2 implicit () () () () () () () () () ()	erault 、トの設定は、[A all > Access Rule: Delete 今 《 Source grules) 10.1.1.0 any any tincoming rules) any any incoming rule)	OK Cancel Access Rules] タブの下 た しestination 別 172.16.1.1 (**********************************	C に次のように表 C に次のように表 Diagram 。 E Service 100 ftp 100 ftp 100 ftp 100 ftp 100 ftp 100 ftp 100 ftp 100 ftp 100 ftp 100 ftp	示されます。 cport ・ 6 Cle Action ② Deny ② Deny ② Deny ③ Deny

Access Rule Type O IPv4 and IPV6 O IPv4 Only IPv6 Only

 Apply
 Reset
 Advanced...

13. [Apply] をクリックして設定を ASA に送信します。同等の CLI 設定は次のようになります

access-list inside_access_in extended deny tcp host 10.1.1.0 host 172.16.1.1 eq ftp access-list inside_access_in extended permit ip any any access-group inside_access_in in interface inside

<u>ポートをオープンする設定</u>

0

セキュリティ アプライアンスは、拡張アクセス リストで明示的に許可されていないかぎり、どの ような着信トラフィックの通過も許可しません。

外部ホストから内部ホストにアクセスできるようにする場合は、外部インターフェイス上で着信 アクセス リストを適用できます。内部ホストの変換後アドレスは外部ネットワーク上で使用でき るアドレスであるため、変換後アドレスをアクセス リストで指定する必要があります低いセキュ リティ ゾーンから高いセキュリティ ゾーンに対してポートをオープンするには、次の手順を実行 します。たとえば、外部(低いセキュリティ ゾーン)から内部インターフェイス(高いセキュリ ティ ゾーン)、または DMZ から内部インターフェイスへのトラフィックを許可します。

 スタティック NAT では、実際のアドレスからマッピング アドレスへの固定変換が作成され ます。マッピングされたこのアドレスはインターネット上でホストされるアドレスで、サー バの実際のアドレスを知らなくても DMZ 上のアプリケーション サーバに対するアクセスに 使用できるアドレスです。

static (real_ifc,mapped_ifc) mapped_ip {real_ip [netmask mask] |
 access-list access_list_name | interface}

詳細については、『<u>PIX/ASA のコマンド リファレンス』の「スタティック NAT」セクショ</u> <u>ンを参照してください。</u>

2.1 つの ACL を作成して特定のポートのトラフィックを許可します。

access-list

3. 次に、access-group コマンドを使用してアクティブにするアクセス リストをバインドします。

access-group

例:

 SMTP ポート トラフィックのオープン:ポート tcp 25 をオープンし、外部(インターネット)からのホストが DMZ ネットワークに配置されたメール サーバにアクセスできるようにします。Static コマンドは、外部アドレスの 192.168.5.3 を実際の DMZ アドレス 172.16.1.3 にマッピングします。
 ciscoasa(config)#static (DMZ,Outside) 192.168.5.3 172.16.1.3
 netmask 255.255.255 ciscoasa(config)#access-list 100 extended permit tcp any host 192.168.5.3 eq 25 ciscoasa(config)#access-group 100 in interface outside

HTTPS ポート トラフィックのオープン:ポート tcp 443 をオープンし、外部(インターネット)からのホストが DMZ ネットワークに配置された Web サーバ(セキュア)にアクセスできるようにします。

ciscoasa(config)#static (DMZ,Outside) 192.168.5.5 172.16.1.5
netmask 255.255.255
ciscoasa(config)#access-list 100 extended permit tcp
any host 192.168.5.5 eq 443
ciscoasa(config)#access-group 100 in interface outside

3. DNS トラフィックの許可:ポート udp 53 をオープンし、外部(インターネット)からのホ ストが DMZ ネットワークに配置された DNS サーバ(セキュア)にアクセスできるように します。 ciscoasa(config)#static (DMZ,Outside) 192.168.5.4 172.16.1.4 netmask 255.255.255.255 ciscoasa(config)#access-list 100 extended permit udp any host 192.168.5.4 eq 53 ciscoasa(config)#access-group 100 in interface outside

注:ポートの割り当てに関する詳細については、IANAのポートを参照してください。

<u>ASDM 経由の設定</u>

このセクションでは、前述したタスクを ASDM で実行するための詳細な手順を紹介しています。

1. 192.168.5.3 サーバへの smtp トラフィックを許可するアクセス ルールを作成します。 Configuration > Firewall > Access Rul



2. アクセス ルールの送信元と宛先、このルールがバインドされるインターフェイスを定義します。また、[Action] に [Permit] を定義します。

🚰 Add Aco	cess Rule
Interface: (outside 🕥
Action: 🧿	Permit O Deny
Source: (any
Destination	192.168.5.3
Service:	ip 🚺
Description:	
💽 Enable L	ogging
Logging	Level: Default
More Opt	tions
	OK Cancel Help

3. ポートに [SMTP] を選択し、[OK] をクリックします。

	L					
Nam	e	Protocol	Source Ports	Destination Ports	ICMP Type	Descriptio
- 10	We top	hen	default (1-65535)	514		
	and step	tro	default (1-65535)	554		
	in in	top	default (1-65535)	5060		
- 1	CO streto	ltro	(default (1-65535))	25	K	1
1	- solvet	tro	default (1-65535)	1521		
	son sch	tcp	default (1-65535)	22		
	NO- SUNTOC	top	default (1-65535)	111		
1	tacacs	top	default (1-65535)	49		
- 1	- 100 talk	top	default (1-65535)	517		
	telnet	top	default (1-65535)	23		
1	NO- UUCD	top	default (1-65535)	540		
	se whois	top	default (1-65535)	43		
	ww.biff	udp	default (0-65535)	512		
-	pot bootpc	udp	default (0-65535)	68		
1	pootps	udp	default (0-65535)	67		
- 3	ter crs	udp	default (0-65535)	3020		
	www.discard	udp	default (0-65535)	9		
	ter distr	udp	default (0-65535)	195		
1	👷 domain	udp	default (0-65535)	53		
		0.65	I.F. A. In Jennet	1997		

4. [OK] をクリックして、アクセス ルールの設定を完了します。

🔹 Add Aco	ess Rule
Interface:	outside 💌
Action: 💿	Permit 🔘 Deny
Source:	any
Destination	192.168.5.3
Service; (tcp/smtp
Description:	
💽 Enable L	ogging
Logging	Level: Default
More Opt	ions
	OK Cancel

5. 172.16.1.3 を 192.168.5.3 に変換するために、スタティック NAT を設定します。 [Configuration] > [Firewall] > [NAT Rules] > [Add Static NAT Rule] **に移動し、スタティック**

4	dd 🗸 📷 Edit 📋 Delete 🛉 🗲 🐇
1	Add Static NAT Rule
H	Add Dynamic NAT Rule
e	Add NAT Exempt Rule
<u>م</u>	Add Static Policy NAT Rule
0	Add Dynamic Policy NAT Rule
*	Insert,
Ŧ	Insert After

NAT エントリを追加します。

関連付けられ

ているインターフェイスとともに変換前のソース アドレスと変換後の IP アドレスを選択し、[OK] をクリックしてスタティック NAT のルールの設定を完了します。

🛋 Add Static NAT F	Rule	l
Original		
Source: (172.16.1.3	
Translated		
Interface:	outside	
💿 Use IP Address:	192.168.5.3	
🚫 Use Interface IP	Address	
Port Address Translatio	n (PAT)	
Enable Port Ad	dress Translation (PAT)	
Protocol:		
Original Port:		
Translated Port		
Connection Setting	s 😜	χ
	Cancel Help	このイメージは
、「 <u>例」セクションに</u> 記	2載されている 3 つのスタティック ルールすべてを	図示しています

🗣 A(id • 🕑 Edit 📋	Delete 🕈 🐇 🕻	🔄 🎆 - 🗌 🔍 Find	📴 Diagram 🧯	🏹 Packet Trace	
#	Turne	Original			Translated	
	Type	Source	Destination	Service	Interface	Address
DM2	1					
1	• Static	3 172.16.1.3			outside	3 192.168.5.
2	• Static	172.16.1.5			outside	192.168.5.
3	Static	172.16.1.4			outside	192.168.5

このイメージは、「<u>例」セクションに記載されている 3 つのアクセス ルールすべてを図示</u> しています。

#	Enabled	Source	Destination	Service	Action
) 🧖 (OMZ (2 implicit	incoming rules)	Paste		
1		🏟 any	Any less secure ne	IP/ ip	🖌 Permil
2		🧼 any	any	IP> ip	🕴 Deny
ا 🧠 ا	nside (2 implic	it incoming rules)			
1		🌍 any	Any less secure ne	IP ip	🖌 Permi
2		🧼 any	any	IP/ ip	🕴 Deny
- 👎 r	manage (2 imp	licit incoming rules)			
1		🏟 any	Any less secure ne	IP ip	🖌 Permi
2		🏟 any	🏟 any	JE> ip	😢 Deny
5	outside (4 inco	ming rules)			
1	¥	🏟 any	192.168.5.3	100 smtp	🖌 Permi
2	\checkmark	🏟 any	192.168.5.5	100 https	🖌 Permi
3	V	🥌 any	192.168.5.4	🚥 domain	💉 Permit
4		 any 	any	IP ip	🕄 Deny

<u>確認</u>

次に示すように、特定の show コマンドで確認できます。

- ・show xlate:現在の変換情報の表示
- show access-list:アクセスポリシーのヒット カウンタの表示
- show logging:バッファ内のログの表示

<u>アウトプット インタープリタ ツール(登録ユーザ専用)(OIT)は、特定の show コマンドをサ</u> <u>ポートします。</u>OIT を使用して、show コマンドの出力の分析を表示します。

<u>トラブルシュート</u>

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>PIX/ASA 7.x: インターフェイス間通信の有効化および無効化</u>
- nat、global、static および access-list コマンドを使用した PIX 7.0 および適応型セキュリテ <u>ィアプライアンスのポート リダイレクション(フォワーディン</u>グ)
- <u>PIX での nat、global、static、conduit、および access-list の各コマンドとポート リダイレク</u> ション(フォワーディング)の使用方法
- <u>PIX/ASA 7.x:FTP/TFTP サービスをイネーブルにする設定例</u>
- ・<u>PIX/ASA 7.x:VoIP(SIP、MGCP、H323、SCCP)サービス有効化の設定例</u>
- <u>PIX/ASA 7.x : DMZ でのメール サーバ アクセスの設定例</u>
- ・<u>テクニカル サポートとドキュメント Cisco Systems</u>