

# 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](#)

[ポートをブロックする設定](#)

[ポートをオープンする設定](#)

[ASDM 経由の設定](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

## 概要

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、「ポートをブロックする」と「ポートを制限する」も同じ意味を示します。

## 前提条件

### 要件

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。

### 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。

- 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。

## 表記法

ドキュメント表記の詳細については、『[シスコテクニカルティップスの表記法](#)』を参照してください。

## 設定

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。

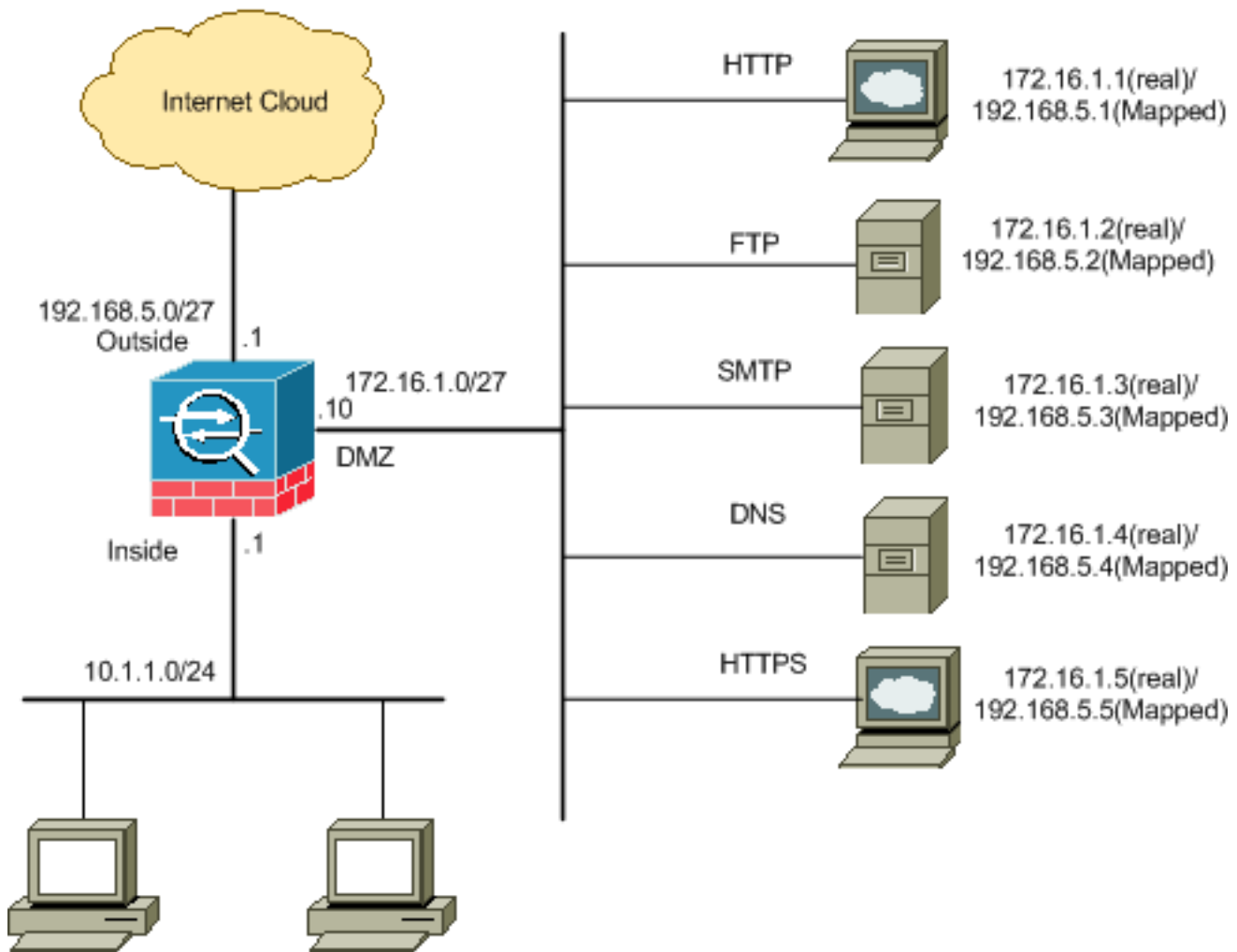
- [ネットワーク図](#)
- [ポートをブロックする設定](#)
- [ポートをオープンする設定](#)

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。

## ネットワーク図

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。



## ポートをブロックする設定

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спекション エンジン を有効にする必要があります。ICMP インспек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。

1. 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
```

- 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:

- 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。

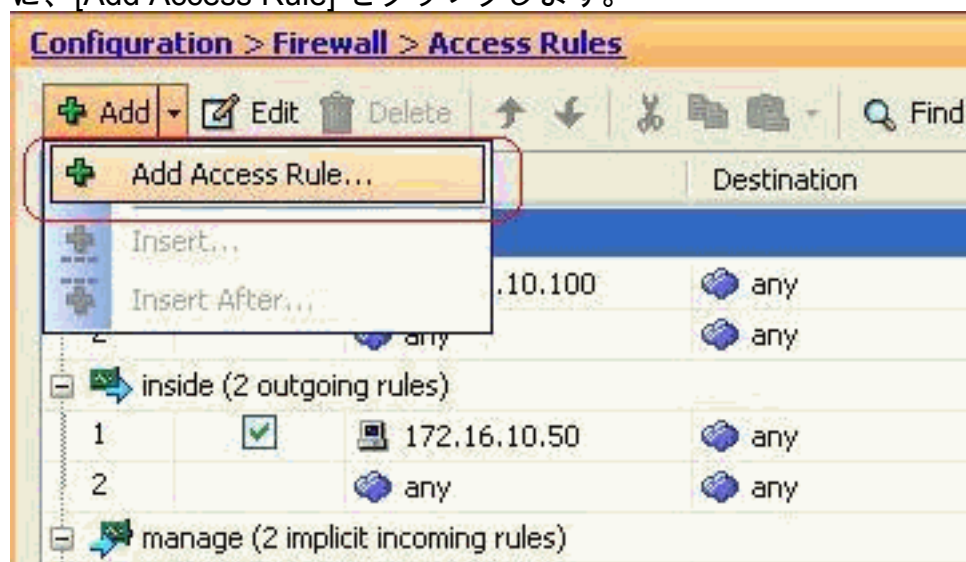
- FTP ポート トラフィックのブロック : DMZ ネットワークに配置された IP 172.16.1.2 を持つ FTP ( ファイル サーバ ) へのアクセスから内部ネットワーク 10.1.1.0 をブロックするには、次のように ACL を作成します。

```
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る[詳細](#)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。

- [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。



- 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 Access Rule**

Interface:

Action:  Permit  Deny

Source:

Destination:

Service:

Description:

Enable Logging

Logging Level:

**More Options**

OK Cancel Help

します。

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

**Browse Service**

Filter:

Name	Protocol	Source Ports	Destination Ports	ICMP Type	Description
discard	tcp	default (1-65535)	9		
daman	tcp	default (1-65535)	53		
echo	tcp	default (1-65535)	7		
exec	tcp	default (1-65535)	512		
finger	tcp	default (1-65535)	79		
ftp	tcp	default (1-65535)	21		
ftp-data	tcp	default (1-65535)	20		
gopher	tcp	default (1-65535)	70		
h323	tcp	default (1-65535)	1720		
hostname	tcp	default (1-65535)	101		
<b>http</b>	<b>tcp</b>	<b>default (1-65535)</b>	<b>80</b>		
https	tcp	default (1-65535)	443		
ident	tcp	default (1-65535)	113		
inapt	tcp	default (1-65535)	143		
irc	tcp	default (1-65535)	194		
kerberos	tcp	default (1-65535)	750		
klogin	tcp	default (1-65535)	543		
labeled	tcp	default (1-65535)	544		
ldap	tcp	default (1-65535)	389		
ldaps	tcp	default (1-65535)	636		

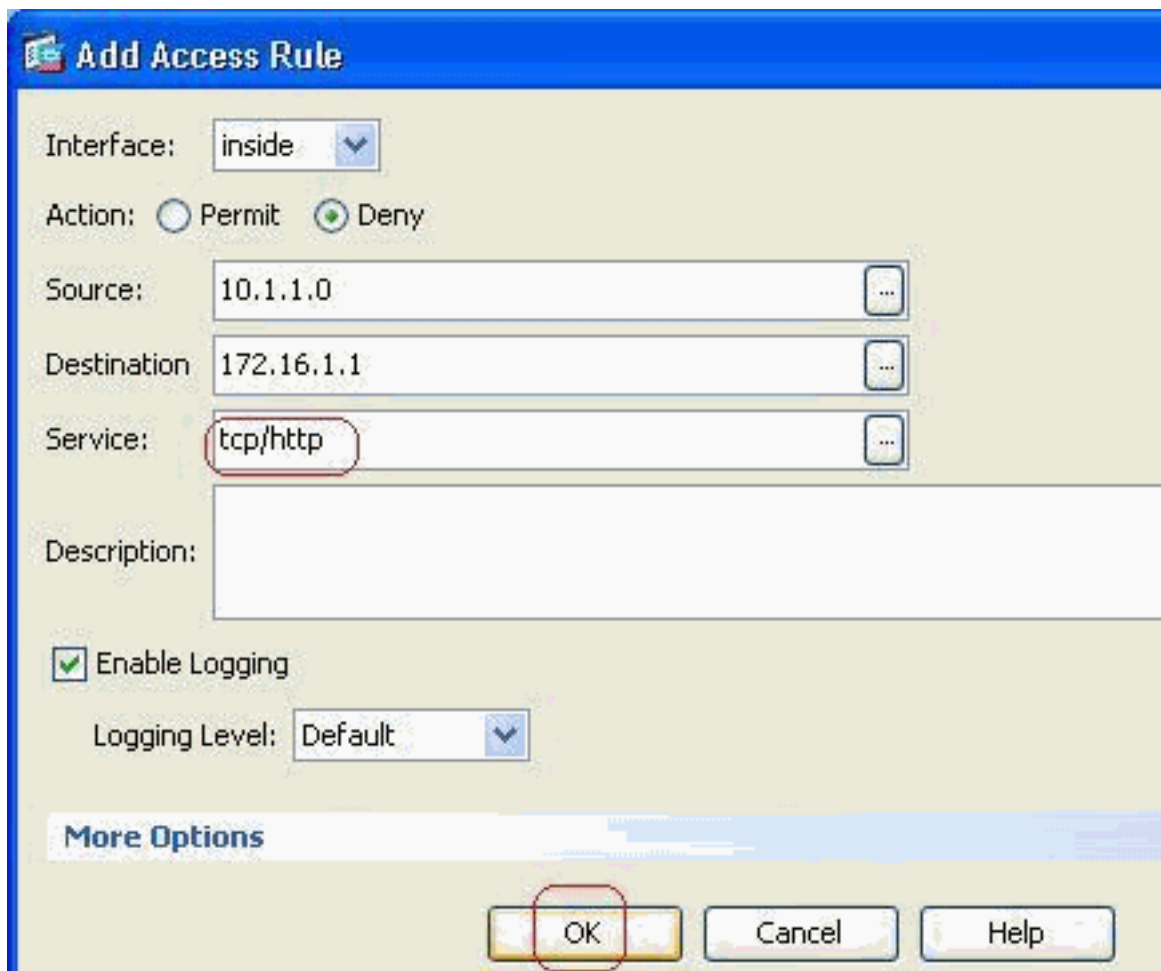
Selected Service:

Service ->

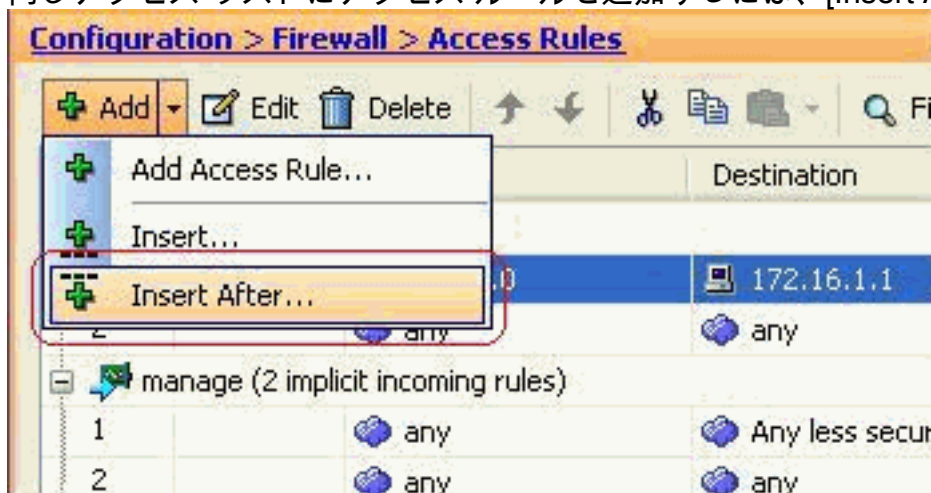
OK Cancel

インドウに戻ります。

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。



5. 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] をクリックします。



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 After Access Rule

Interface:

Action:  Permit  Deny

Source:

Destination:

Service:

Description:

Enable Logging

Logging Level:

**More Options**

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。

Configuration > Firewall > Access Rules

#	Enabled	Source	Destination	Service	Action	Hits
inside (3 incoming rules)						
1	<input checked="" type="checkbox"/>	10.1.1.0	172.16.1.1	http	Deny	0
2	<input checked="" type="checkbox"/>	any	any	ip	Permit	0
3	<input type="checkbox"/>	any	any	ip	Deny	0
manage (2 implicit incoming rules)						
1	<input type="checkbox"/>	any	Any less secure ne...	ip	Permit	
2	<input type="checkbox"/>	any	any	ip	Deny	
outside (1 implicit incoming rule)						
1	<input type="checkbox"/>	any	any	ip	Deny	

Access Rule Type  IPv4 and IPv6  IPv4 Only  IPv6 Only

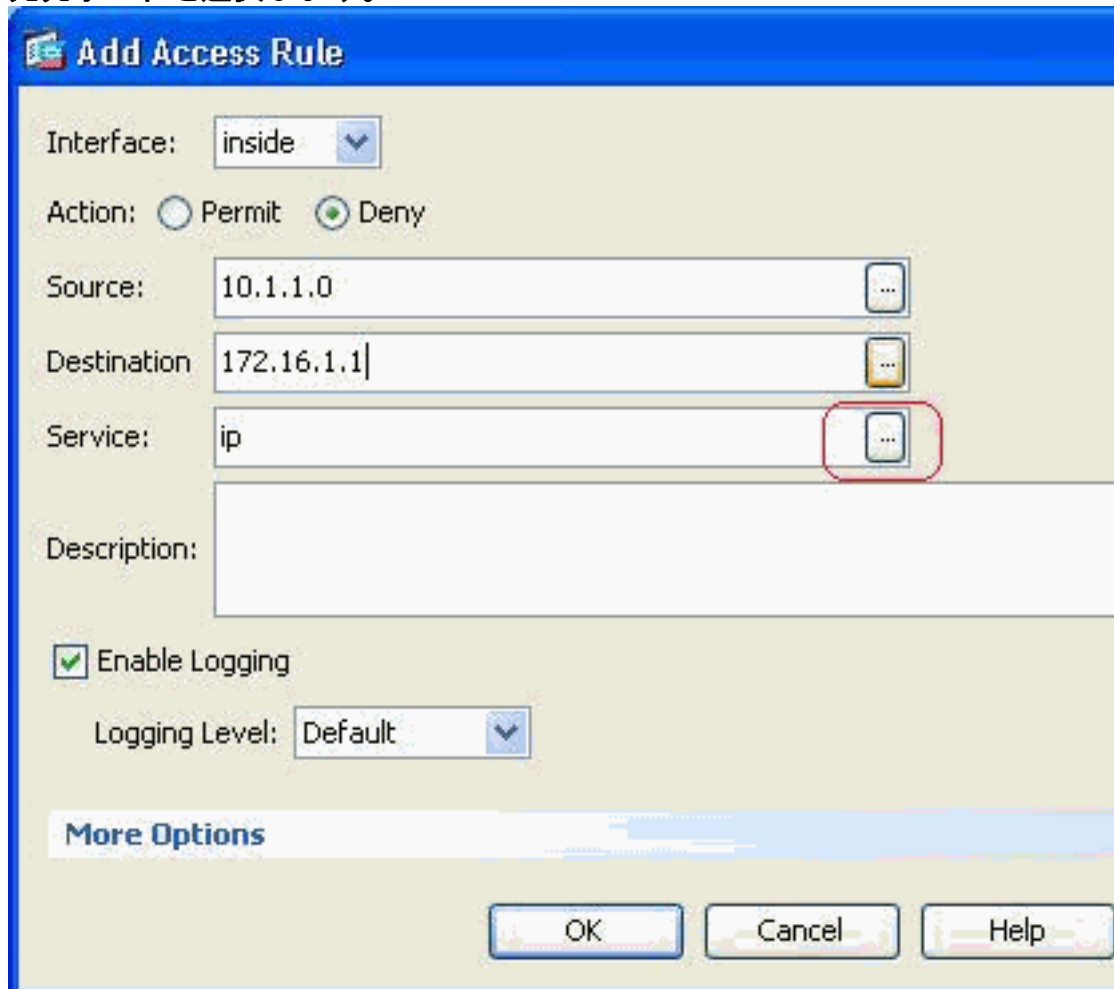
Apply Reset Advanced...

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。

- 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。

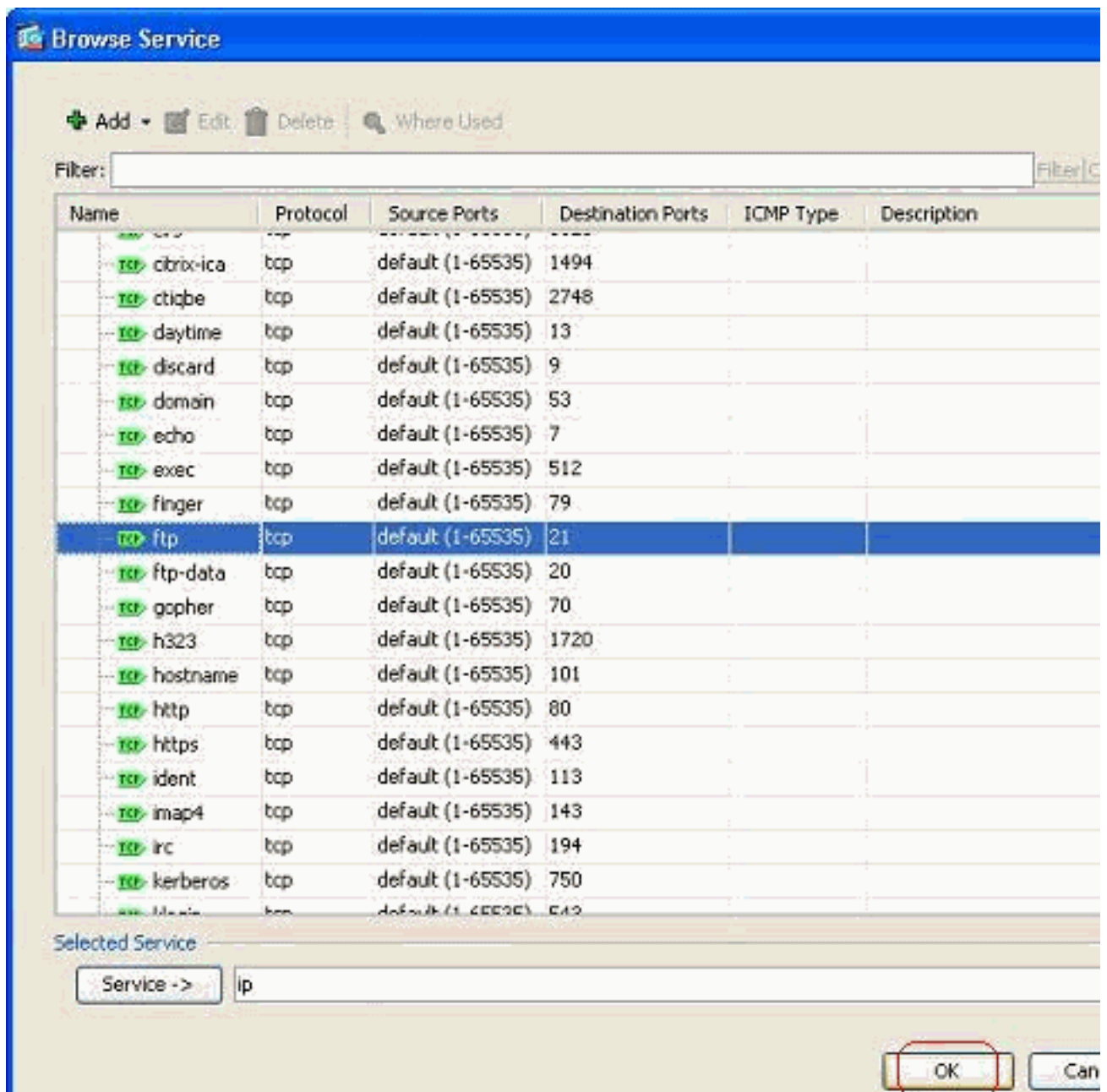


The screenshot shows the 'Add Access Rule' dialog box with the following configuration:

- Interface: inside
- Action:  Permit  Deny
- Source: 10.1.1.0
- Destination: 172.16.1.1
- Service: ip
- Description: (empty)
- Enable Logging
- Logging Level: Default
- More Options (highlighted)
- Buttons: OK, Cancel, Help

- [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。





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 Access Rule**

Interface:

Action:  Permit  Deny

Source:  ...

Destination:  ...

Service:  ...

Description:

Enable Logging

Logging Level:

**More Options**

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。

**Insert After Access Rule**

Interface:

Action:  Permit  Deny

Source:

Destination:

Service:

Description:

Enable Logging

Logging Level:

**More Options**

12. 完成したアクセス リストの設定は、[Access Rules] タブの下に次のように表示されます。

**Configuration > Firewall > Access Rules**

#	Enabled	Source	Destination	Service	Action
inside (3 incoming rules)					
1	<input checked="" type="checkbox"/>	10.1.1.0	172.16.1.1	TCP ftp	Deny
2	<input checked="" type="checkbox"/>	any	any	IP ip	Permit
3	<input type="checkbox"/>	any	any	IP ip	Deny
manage (2 implicit incoming rules)					
1	<input type="checkbox"/>	any	Any less secure ne...	IP ip	Permit
2	<input type="checkbox"/>	any	any	IP ip	Deny
outside (1 implicit incoming rule)					
1	<input type="checkbox"/>	any	any	IP ip	Deny

Access Rule Type  IPv4 and IPv6  IPv4 Only  IPv6 Only

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

```
o
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
```

## ポートをオープンする設定

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。

1. 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、『[PIX/ASA のコマンド リファレンス](#)』の「[スタティック NAT](#)」セクションを参照してください。

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:

1. 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 255.255.255.255
```

```
ciscoasa(config)#access-list 100 extended permit tcp
any host 192.168.5.3 eq 25
ciscoasa(config)#access-group 100 in interface outside
```

2. 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 255.255.255.255
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。

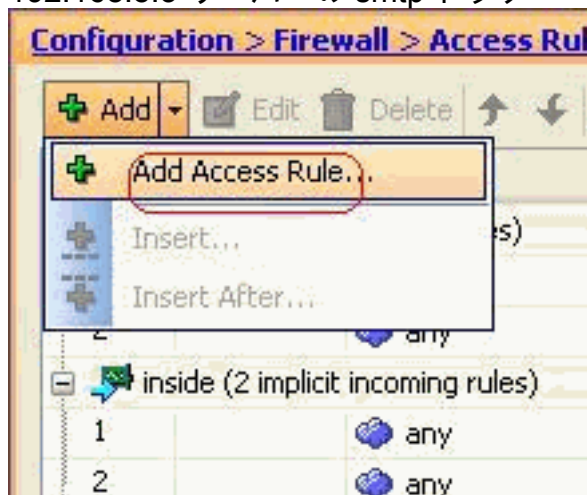
```
ciscoasa(config)#static (DMZ,Outside) 192.168.5.4 172.16.1.4
netmask 255.255.255.255
ciscoasa(config)#access-list 100 extended permit udp
any host 192.168.5.4 eq 53
ciscoasa(config)#access-group 100 in interface outside
```

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。

## ASDM 経路の設定

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。



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 Access Rule**

Interface:

Action:  Permit  Deny

Source:

Destination:

Service:

Description:

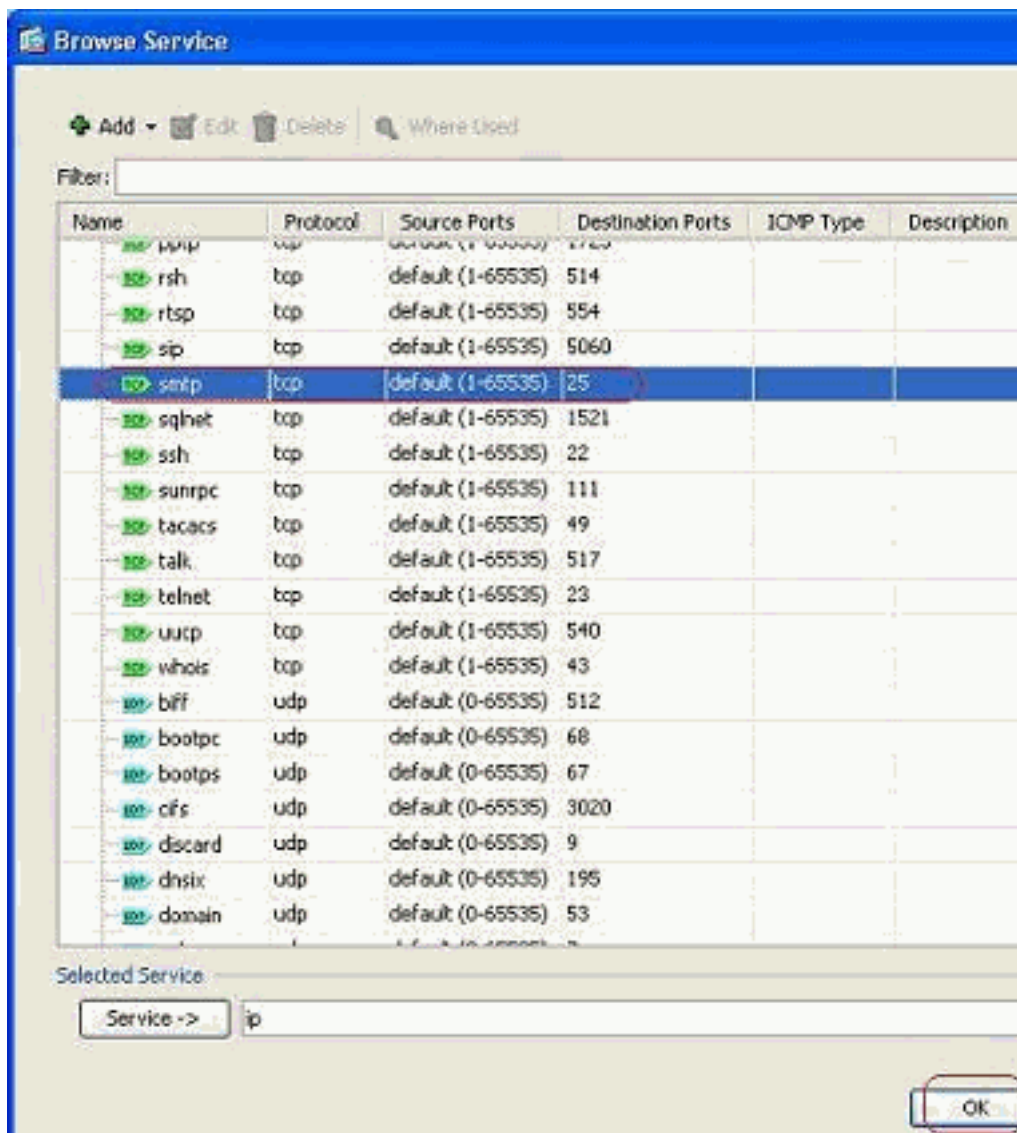
Enable Logging

Logging Level:

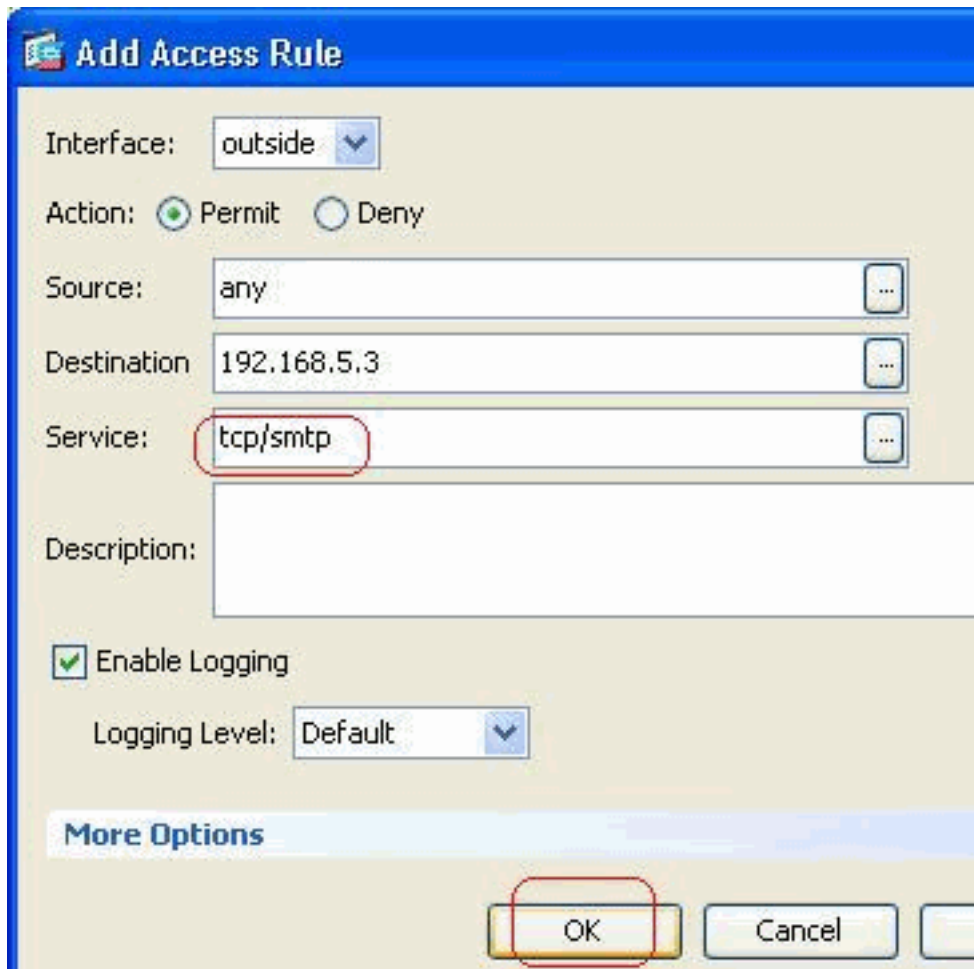
**More Options**

OK Cancel Help

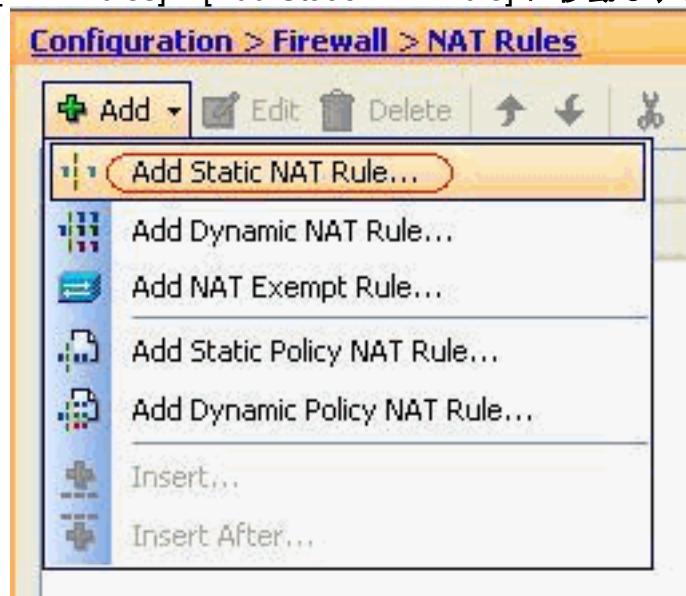
3. ポートに [SMTP] を選択し、[OK] をクリックします。



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。



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



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 Rule**

Original

Interface: DMZ

Source: 172.16.1.3

Translated

Interface: outside

Use IP Address: 192.168.5.3

Use Interface IP Address

Port Address Translation (PAT)

Enable Port Address Translation (PAT)

Protocol:  TCP  UDP

Original Port:

Translated Port:

Connection Settings

OK Cancel Help

このイメージは、「例」セクションに記載されている3つのスタティックルールすべてを图示しています。

**Configuration > Firewall > NAT Rules**

#	Type	Original			Translated	
		Source	Destination	Service	Interface	Address
DMZ						
1	Static	172.16.1.3			outside	192.168.5.3
2	Static	172.16.1.5			outside	192.168.5.5
3	Static	172.16.1.4			outside	192.168.5.4

このイメージは、「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图示しています。

Configuration > Firewall > Access Rules

Add Edit Delete Copy Paste Find Diagram Export Clear Hits

#	Enabled	Source	Destination	Service	Action
DMZ (2 implicit incoming rules)					
1		any	Any less secure ne...	IP ip	Permit
2		any	any	IP ip	Deny
inside (2 implicit incoming rules)					
1		any	Any less secure ne...	IP ip	Permit
2		any	any	IP ip	Deny
manage (2 implicit incoming rules)					
1		any	Any less secure ne...	IP ip	Permit
2		any	any	IP ip	Deny
outside (4 incoming rules)					
1	<input checked="" type="checkbox"/>	any	192.168.5.3	TCP smtp	Permit
2	<input checked="" type="checkbox"/>	any	192.168.5.5	TCP https	Permit
3	<input checked="" type="checkbox"/>	any	192.168.5.4	TCP domain	Permit
4		any	any	IP ip	Deny

## 確認

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

[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 コマンドをサポートします。OIT を使用して、show コマンドの出力の分析を表示します。

## トラブルシューティング

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

- [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](#)
- [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 \(フォワーディング\)](#)
- [PIX での nat、global、static、conduit、および access-list の各コマンドとポート リダイレクション \(フォワーディング\) の使用方法](#)
- [PIX/ASA 7.x : FTP/TFTP サービスをイネーブルにする設定例](#)
- [PIX/ASA 7.x : VoIP \( SIP、MGCP、H323、SCCP \) サービス有効化の設定例](#)
- [PIX/ASA 7.x : DMZ でのメール サーバ アクセスの設定例](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)