SIPフェデレーションに関するCiscoAdaptive Security Appliance（ASA）の設定

（注） IM and Presence Release 9.0 以降では、Microsoft Lync とのドメイン間フェデレーションがサポートされています。 また IM and Presence Release 9.0 以降の場合、OCS とのドメイン間フェデレーションへの参照には、別途明示的な指定がない限り、Microsoft Lync が指定されます。

Cisco Adaptive Security Appliance（ASA）の [ユニファイド コミュニケーション（Unified Communication）] ウィザード

ご使用のドメイン間フェデレーション導入に**単一の** IM and Presence サーバを導入する場合は、Cisco Adaptive Security Appliance（ASA）で [ユニファイド コミュニケーション（Unified Communication）] ウィザードを使用して、Cisco Adaptive Security Appliance（ASA）と IM and Presence の間のプレゼンス フェデレーション プロキシを設定できます。

[ユニファイド コミュニケーション（Unified Communication）] ウィザードが表示されている設定例を、次の URL にある IM and Presence に関するドキュメンテーション wiki でご確認ください。

関連トピック

http://docwiki.cisco.com/wiki/Cisco_Unified_Presence%2C_Release_8.x

外部および内部インターフェイスの設定

Cisco Adaptive Security Appliance（ASA）で 2 つのインターフェイスを設定するには、次のようにします。

- 1 つのインターフェイスを**外部**インターフェイスとして使用します。 これは、インターネットおよび外部ドメイン サーバ（例、Microsoft アクセス エッジ/アクセス プロキシ）へのインターフェイスです。
- 2 番目のインターフェイスを**内部**インターフェイスとして使用します。 これは、ご使用の導入に応じて、IM and Presence へのインターフェイスか、ロード バランサのインターフェイスになります。
- インターフェイスを設定する際、イーサネットやギガビット イーサネットなどの**インターフェイス タイプ**と**インターフェイス スロット**を指定する必要があります。 Cisco Adaptive Security Appliance（ASA）のスロット 0 には、4 つのイーサネット ポートまたはギガビット ポートが備わっています。 任意に、スロット 1 に SSM-4GE モジュールを追加して、スロット 1 で 4 つのギガビット イーサネット ポートを実現することもできます。
- ルート トラフィックへのインターフェイスごとに、**インターフェイス名**と **IP アドレス**を設定する必要があります。 内部インターフェイスの IP アドレスと外部インターフェイスの IP アドレスは異なるサブネットに含まれる必要があります。つまり、異なるサブマスクがある必要があります。
- 各インターフェイスのセキュリティ レベルは、0（最低）～ 100（最高）の間である必要があります。 セキュリティ レベル値 100 は、最もセキュアなインターフェイス（内部インターフェイス）です。セキュリティ レベル値 0 は、最もセキュアでないインターフェイスです。内部インターフェイスや外部インターフェイスに対してセキュリティ レベルを明示的に設定しない場合、Cisco Adaptive Security Appliance（ASA）によりデフォルトで 100 に設定されます。
- CLI を使用して外部インターフェイスおよび内部インターフェイスを設定する方法の詳細については、『Cisco Security Appliance Command Line Configuration Guide』を参照してください。

（注） 内部インターフェイスおよび外部インターフェイスは、ASDM 起動（ASDM startup）ウィザードを使用して設定することもできます。 また、ASDM で [設定（Configuration）] > [デバイス設定（Device Setup）]>[インターフェイス（Interfaces）] を選択することによってインターフェイスを表示または編集することもできます。

スタティック IP ルートの設定

Cisco Adaptive Security Appliance（ASA）は、OSPF、RIP および EIGRP などのダイナミック ルーティング プロトコルとスタティック ルートを両方ともサポートしています。 本統合を実現するには、Cisco Adaptive Security Appliance（ASA）の内部インターフェイスにルーティングされる IP トラフィックと、外部インターフェイスにルーティングされるトラフィックに対するネクスト ホップアドレスを定義するスタティック ルートを設定する必要があります。 次の手順で、dest_ip マスクは接続先ネットワークの IP アドレス、gateway_ip 値はネクスト ホップのルータまたはゲートウェイのアドレスです。

Cisco Adaptive Security Appliance（ASA）でデフォルト ルートおよびスタティック ルートを設定する方法の詳細については、『Cisco Security Appliance Command Line Configuration Guide』を参照してください。

はじめる前に

外部および内部インターフェイスの設定，（2 ページ） の手順を実行します。

手順

ステップ 1 設定モードで、次のように入力します。

```
>Enable >password
>config t
```

ステップ 2 次のコマンドを入力して、内部インターフェイスにスタティック ルートを追加します。

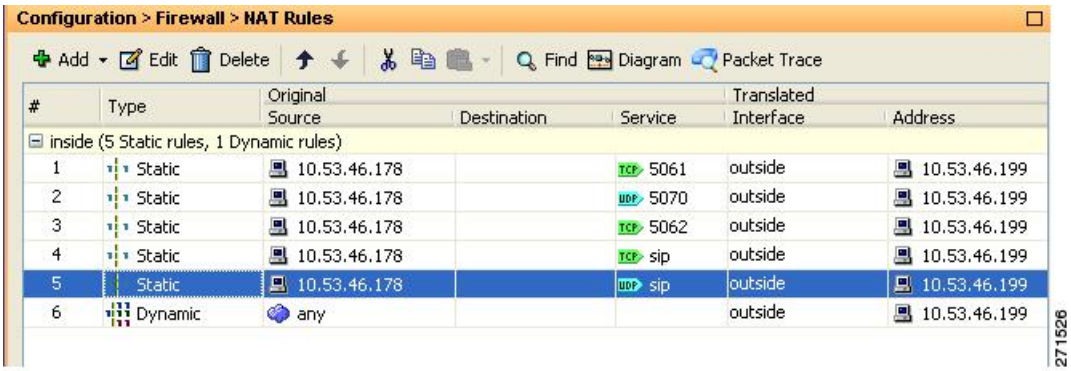
```
hostname(config)# route inside dest_ip mask gateway_ip
```

ステップ 3 次のコマンドを入力して、外部インターフェイスにスタティック ルートを追加します。

```
hostname(config)# route outside dest_ip mask gateway_ip
```

（注） また、ASDM で [設定（Configuration）] > [デバイス設定（Device Setup）] > [ルーティング（Routing）] > [スタティック ルート（Static Route）] を選択することによってスタティック ルートを表示および設定することもできます。

図 *1*：*ASDM* でのスタティック ルートの表示



次の作業

ポート アドレス変換（PAT）， （4 ページ）

ポート アドレス変換（PAT）

本統合に必要なポート アドレス変換

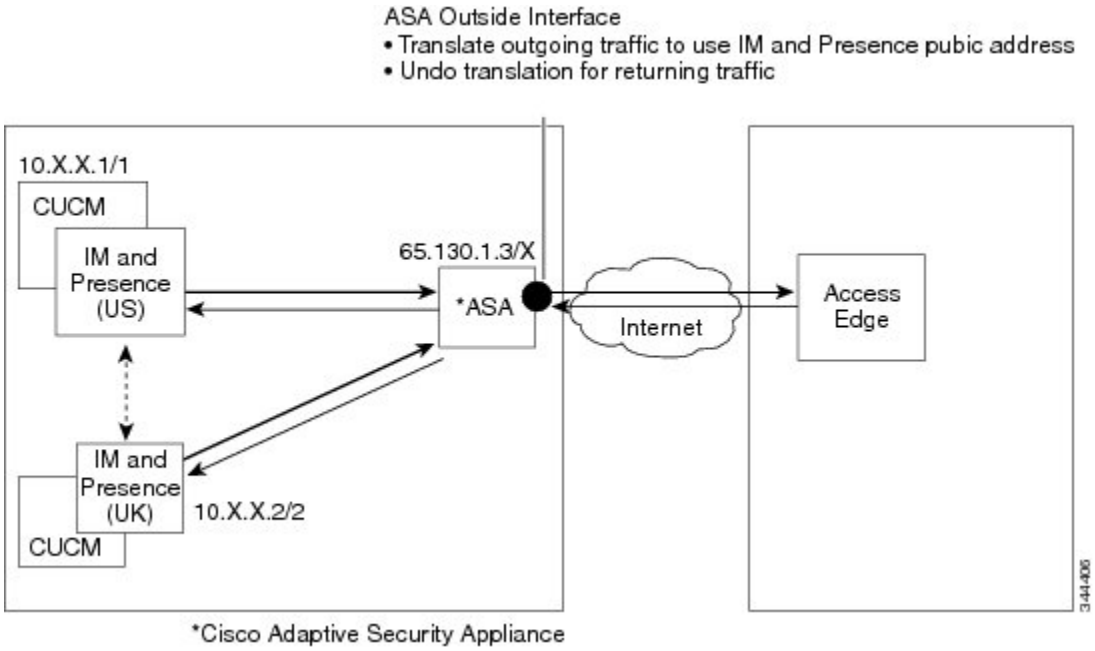
（注） 外部ドメインで別の IM and Presence 企業配置とのフェデレーションを行う場合は、ポート アドレス変換も使用します。

本統合を実現するため、Cisco Adaptive Security Appliance（ASA）ではポート アドレス変換（PAT）およびスタティック PAT を使用してメッセージ アドレス変換を行っています。 Cisco Adaptive Security Appliance（ASA）では、本統合を実現するためにネットワーク アドレス変換（NAT）は使用していません。

本統合では、PAT を使用して、IM and Presence から送信されたメッセージを外部ドメインに（プライベート メッセージをパブリック メッセージに）変換します。 ポート アドレス変換（PAT）とは、パケット内の実際のアドレスおよびソース ポートが接続先ネットワーク上でルーティング可能なマップされたアドレスおよび固有のポートに置換されることを意味します。 この変換方法で使用される二段階のプロセスでは、実際の IP アドレスとポートをマップされた IP アドレスとポートに変換します。戻ってくるトラフィックでは、変換が “元に戻されます”。

Cisco Adaptive Security Appliance（ASA）が IM and Presence から送信されたメッセージを外部ドメインに（プライベート メッセージをパブリック メッセージに）変換する方法は、IM and Presence 上のプライベート IP アドレスとポートをパブリックの IP アドレスと 1 つ以上のパブリック ポートに変更することです。 このため、ローカルの IM and Presence ドメインでは 1 つのパブリック IP アドレスのみを使用します。 Cisco Adaptive Security Appliance（ASA）は、外部インターフェイスに NAT コマンドを割り当て、そのインターフェイスで受信された任意のメッセージの IP アドレスおよびポートを次の図に示すように変換します。

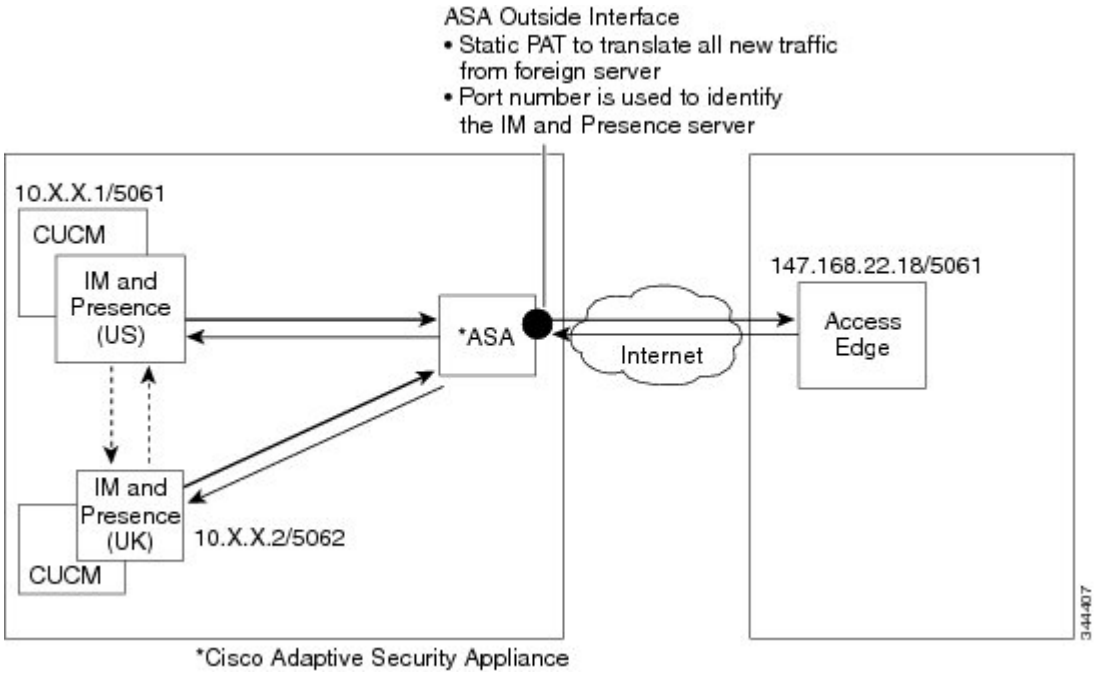
図 *2*：*IM and Presence* から外部ドメインに発信されたメッセージに対する *PAT* の例



外部ドメインから IM and Presence に送信された新しいメッセージに対しては、Cisco Adaptive Security Appliance（ASA）はスタティック PAT を使用して、IM and Presence のパブリックの IP アドレスおよびポートに送信された任意のメッセージを指定された IM and Presence サーバにマップします。 スタティック PAT を使用することで、実際の IP アドレスをマップされた IP アドレスに変換し、実際のポート番号をマップされたポート番号に変換できます。 実際のポート番号を同じポート番号にも異なるポート番号にも変換することができます。 この場合、ポート番号は次の図に示すように、適切な IM and Presence サーバを識別して、メッセージ要求を処理します。

（注） IM and Presence サーバにユーザが存在しない場合、IM and Presence ルーティング サーバはクラスタ間ルーティングを使用してメッセージをリダイレクトします。 すべての応答が、IM and Presence ルーティング サーバから Cisco Adaptive Security Appliance（ASA）に送信されます。

図 *3*：外部ドメインから発信されたメッセージに対するスタティック *PAT*



プライベート要求のポート/アドレスのパブリック要求のポート/アドレスへの変換（PAT）

本統合を実現するため、プライベート メッセージ ドレスのパブリック メッセージ ドレスへの変換には次の設定が必要になります。

- 変換したい実際の IP アドレスおよびポート番号を識別する NAT ルールを定義します。 この場合、Cisco Adaptive Security Appliance（ASA）が内部インターフェイスで受信された任意のメッセージに NAT 操作を適用するという NAT ルールを設定します。
- 外部インターフェイスから発信されるメッセージに使用するマップされたアドレスを指定するグローバル NAT 操作を設定します。 本統合を実現するには、ただ 1 つのアドレスを指定します（PAT を使用するため）。 NAT操作では、（内部インターフェイスで受信されたメッセージの）IP アドレスを IM and Presence のパブリック アドレスにマップします。

プライベート要求のポート/アドレスのパブリック要求のポート/アドレスへの変換（PAT），（6 ページ） に、Cisco Adaptive Security Appliance（ASA） Release 8.2 と 8.3 のグローバル アドレス変

換コマンドの例を示します。 最初の行は、単一の IM and Presence 導入でも複数の IM and Presence 導入でも必須です。 2 番目の行は、単一の IM and Presence 導入のみを対象としています。 3 番目の行は、複数の IM and Presence 導入を対象としています。

表 *1*：グローバル アドレス変換コマンドの例

設定例	Cisco Adaptive Security Appliance（ASA） Release 8.2 グローバル コマンド	Cisco Adaptive Security Appliance（ASA） Release 8.3 グローバル コマンド
この NAT 設定例は、内部インターフェイスに 1 つ以上の IM and Presence サーバがあり、それ以外のファイアウォール トラフィックがない導入で使用できます。	`global (outside) 1 <public_cup_address>nat (inside) 1 0 0`	`object network obj_any host 0.0.0.0` `  nat (inside,outside) dynamic <public cup address>`

この NAT 設定例は、内部インターフェイスに 1 つの IM and Presence サーバとその他のファイアウォール トラフィックがある導入で使用できます。	`global (outside) 1 <public_cup_address>nat (inside) 1 <private_cup_address> 255.255.255.255`
	
	`global (outside) 2 interface`
	`nat (inside) 2 0 0`
		`host <private cup address>`
		`nat (inside,outside) dynamic <public cup address>`
		
		`object network my_inside`
		`  subnet 0.0.0.0 0.0.0.0`
		`  nat (inside,outside) dynamic interface`

この NAT 設定例は、内部インターフェイスに複数の IM and Presence サーバとその他のファイアウォール トラフィックがある導入で使用できます。	`global (outside) 1 <public cup ip>nat (inside) 1 <private_cup_net> <private_cup_netmask>`
	
	`global (outside) 2 interface`
	`nat (inside) 2 0 0`
		`object network obj_<private subnet>.0_255.255.255.0  subnet <private subnet> 255.255.255.0`
		`  nat (inside,outside) dynamic <public cup address>`
		
		`object network my_inside`
		`  subnet 0.0.0.0 0.0.0.0`
		`  nat (inside,outside) dynamic interface`

（注） プライベート要求のポート/アドレスのパブリック要求のポート/アドレスへの変換（PAT），（6 ページ）で最後の行に示した設定例では、Cisco Adaptive Security Appliance（ASA）の背後に複数の IM and Presence サーバがある場合に、これらの IM and Presence サーバがすべて同じサブネットに含まれることを想定しています。具体例を挙げると、すべての内部 IM and Presence サーバが 2.2.2.x/24 ネットワーク内にある場合、NAT コマンドは nat (inside) 1 2.2.2.0 255.255.255.0 となります。

関連トピック

本統合に必要なポート アドレス変換，（4 ページ）

新規要求に対するスタティック PAT

本統合を実現するため、プライベート メッセージ ドレスのパブリック メッセージ ドレスへの変換には次の設定が必要になります。

- TCP でポート 5060、5061、5062 および 5080 に対してスタティック PAT コマンドを設定します。
- UDP でポート 5080 に対して別のスタティック PAT コマンドを設定します。

本統合で使用するポートの説明は、次のとおりです。

- 5060：このポートは、Cisco Adaptive Security Appliance（ASA）で一般的な SIP 検査を行うために使用されます。
- 5061：このポートに SIP 要求が送信され、それによって TLS ハンドシェイクがトリガーされます。
- 5062、5080：これらのポートは、IM and Presence により SIP VIA/CONTACT ヘッダー内で使用されます。

（注） [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [システム（System）] > [アプリケーション リスナー（Application Listeners）] の順に選択することで、IM and Presence のピア認証リスナー ポートを確認できます。

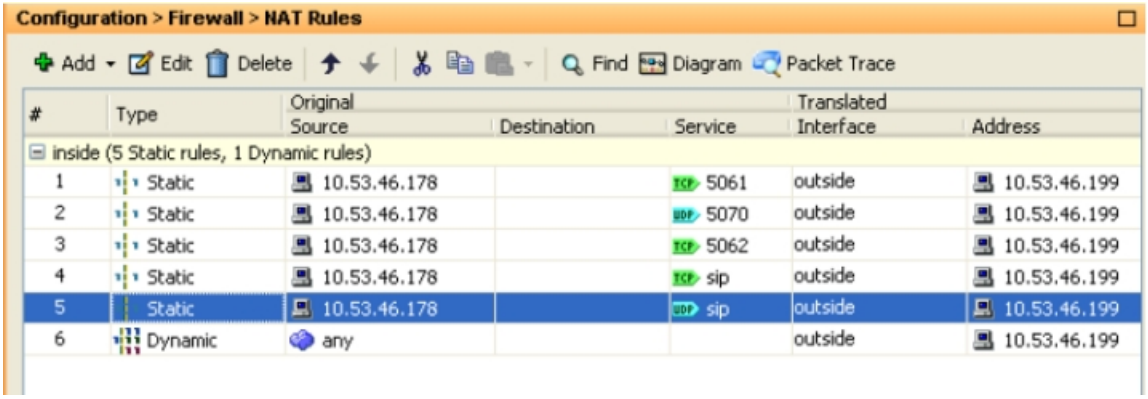
関連トピック

スタティック PAT コマンドの例，（9 ページ）
Cisco Adaptive Security Appliance（ASA）の設定例

ASDM での NAT ルール

ASDM で NAT ルールを表示するには、[設定（Configuration）] > [ファイアウォール（Firewall）] > [NAT ルール（NAT Rules）] を選択します。 次の図に示されている最初の 5 つの NAT ルールはスタティック PAT エントリで、最後のダイナミック エントリはすべての発信トラフィックをパブリック IM and Presence IP アドレスおよびポートにマップする発信 PAT 設定です。

図 *4*：*ASDM* での *PAT* ルールの表示



関連トピック

スタティック PAT コマンドの例, （9 ページ）
Cisco Adaptive Security Appliance（ASA）の設定例

スタティック PAT コマンドの例

（注） この項では、Cisco Adaptive Security Appliance（ASA） Release 8.3 および Release 8.2 のコマンドの例を示します。 これらのコマンドは、フェデレーション用に Cisco Adaptive Security Appliance（ASA）の新規設定を行う場合に実行する必要があります。

ルーティング IM and Presence ノードに対する PAT 設定

次の表に、ピア認証リスナー ポートが 5062 の場合のルーティング IM and Presence ノードに対する PAT コマンドを示します。

（注） Cisco Adaptive Security Appliance（ASA） 8.3 設定の場合、オブジェクトは一度定義するだけで複数のコマンド内で参照できます。同じオブジェクトを何度も定義する必要はありません。

表 *2*：ルーティング *IM and Presence* ノードに対する *PAT* コマンド

Cisco Adaptive Security Appliance（ASA）Release 8.2 のスタティック コマンド	Cisco Adaptive Security Appliance（ASA）Release 8.3 の NAT コマンド

`static (inside,outside) tcp <public cup ipaddress> 5061 <routing cup private address> 5062 netmask 255.255.255.255`
 	
ルーティング IM and Presence のピア認証リスニング ポートが 5061 の場合は、次のコマンドを使用します。
 	
`static (inside,outside) tcp <public cup ipaddress> 5061 <routing cup private address> 5061 netmask 255.255.255.255`
	`Object network obj_host_<public cup ip address>(e.g. object network obj_host_10.10.10.10) #host <public cup ip address>`
	
	`object network obj_host_<routing cup private address> host <routing cup private address>`
	
	`object service obj_tcp_source_eq_5061 service tcp source eq 5061`
	
	`object service obj_tcp_source_eq_5062 service tcp source eq 5062`
	
	`nat (inside,outside) source static obj_host_<routing cup private address> obj_host_<public cup ip address> service obj_tcp_source_eq_5062 obj_tcp_source_eq_5061`
	
	ルーティング IM and Presence のピア認証リスニング ポートが 5061 の場合は、次のコマンドを使用します。
	
	`nat (inside,outside) source static obj_host_<routing cup private address> obj_host_<public cup ip address> service obj_tcp_source_eq_5061 obj_tcp_source_eq_5061`

Cisco Adaptive Security Appliance（ASA）Release 8.2 のスタティック コマンド	Cisco Adaptive Security Appliance（ASA）Release 8.3 の NAT コマンド

`static (inside,outside) tcp <public cup ip address> 5080 <routing cup private address> 5080 netmask 255.255.255.255`	`object service obj_tcp_source_eq_5080 service tcp source eq 5080`
	
	`nat (inside,outside) source static obj_host_<routing cup private address> obj_host_<public cup ip address> service obj_tcp_source_eq_5080 obj_tcp_source_eq_5080`

`static (inside,outside) tcp <public cup ipaddress> 5060 <routing cup private address> 5060 netmask 255.255.255.255`	`object service obj_tcp_source_eq_5060service tcp source eq 5060`
	
	（注） 5060 はサービス オブジェクト内では "sip" と表示されます。
	
	`nat (inside,outside) source static obj_host_<routing cup private address> obj_host_<public cup ip address> service obj_tcp_source_eq_5060 obj_tcp_source_eq_5060`

`static (inside,outside) tcp <public cup ipaddress> 5062 <routing cup private address> 5062 netmask 255.255.255.255`	`nat (inside,outside) source static obj_host_<routing cup private address> obj_host_<public cup ip address> service obj_tcp_source_eq_5062 obj_tcp_source_eq_5062`

関連トピック

新規要求に対するスタティック PAT, （8 ページ）
クラスタ間およびクラスタ内 IM and Presence ノードの PAT 設定, （11 ページ）

クラスタ間およびクラスタ内 IM and Presence ノードの PAT 設定

マルチノードまたはクラスタ間の IM and Presence 導入で IM and Presence クラスタ内の非ルーティング ノードが直接 Cisco Adaptive Security Appliance（ASA）と通信する場合、これらのノードごとにスタティック PAT コマンドのセットを設定する必要があります。 次にリストするコマンドは、単一のノードに対して設定する必要があるスタティック PAT コマンドのセットの例です。

任意のポートを使用できますが、未使用のポートである必要があります。 対応する番号を選択することを推奨します。たとえば、5080 の場合は、未使用の任意のポート X5080 を使用します。ここで、X は IM and Presence クラスタ間またはクラスタ内サーバに固有にマップされている番号に相当します。 例を挙げると、45080 は特定のノードに固有にマップされており、55080 は別のノードに固有にマップされています。

次の表に、非ルーティング IM and Presence ノードに対する NAT コマンドを示します。非ルーティング IM and Presence ノードごとにコマンドを繰り返します。

（注） Cisco Adaptive Security Appliance（ASA） 8.3 設定の場合、オブジェクトは一度定義するだけで複数のコマンド内で参照できます。同じオブジェクトを何度も定義する必要はありません。

表 *3*：非ルーティング *IM and Presence* ノードに対する *NAT* コマンド

Cisco Adaptive Security Appliance（ASA）Release 8.2 のスタティック コマンド	Cisco Adaptive Security Appliance（ASA）Release 8.3 の NAT コマンド

`static (inside,outside) tcp <public CUPaddress> 45062 <intercluster cup8 private address> 5062 netmask 255.255.255.255`
 	
クラスタ間 IM and Presence のピア認証リスニング ポートが 5061 の場合は、次のコマンドを使用します。
 	
`static (inside,outside) tcp <public CUP address> 45061 <intercluster cup8 private address> 5061 netmask 255.255.255.255`
	`object network obj_host_<intercluster cup8 privateaddress> host <intercluster cup8 private address>`
	
	`object service obj_tcp_source_eq_45062 service tcp source eq 45062`
	
	`nat (inside,outside) source static obj_host_<intercluster cup8 private address> obj_host_<public cup ip address> service obj_tcp_source_eq_5062 obj_tcp_source_eq_45062`
	
	クラスタ間 IM and Presence のピア認証リスニング ポートが 5061 の場合は、次のコマンドを使用します。
	
	`object service obj_tcp_source_eq_45061 service tcp source eq 45061`
	
	`nat (inside,outside) source static obj_host_<intercluster cup8 private address> obj_host_<public cup ip address> service obj_tcp_source_eq_5061 obj_tcp_source_eq_45061`

Cisco Adaptive Security Appliance（ASA）Release 8.2 のスタティック コマンド	Cisco Adaptive Security Appliance（ASA）Release 8.3 の NAT コマンド

`static (inside,outside) tcp <public cup ipaddress> 45080 <intercluster cup8 private address> 5080 netmask 255.255.255.255`	`object service obj_tcp_source_eq_45080service tcp source eq 45080`
	
	`nat (inside,outside) source static obj_host_<intercluster cup8 private address> obj_host_<public cup ip address> service obj_tcp_source_eq_5080 obj_tcp_source_eq_45080`

`static (inside,outside) tcp <public cup ipaddress> 45060 <intercluster cup8 private address> 5060 netmask 255.255.255.255`	`object service obj_tcp_source_eq_45060service tcp source eq 45060`
	
	`nat (inside,outside) source static obj_host_<intercluster cup8 private address> obj_host_<public cup ip address> service obj_tcp_source_eq_5060 obj_tcp_source_eq_45060`

関連トピック

新規要求に対するスタティック PAT, （8 ページ）
ルーティング IM and Presence ノードに対する PAT 設定, （9 ページ）

既存の導入に対する Cisco Adaptive Security Appliance（ASA）アップグレードオプション

Cisco Adaptive Security Appliance（ASA） の Release 8.2 を Release 8.3 にアップグレードすると、Cisco Adaptive Security Appliance（ASA）では既存のコマンドがシームレスに移行されます。

（注） IM and Presence Release 9.0 に移行した場合は、Cisco Adaptive Security Appliance（ASA）に管理されている IM and Presence 9.0 ノードごとに、Cisco Adaptive Security Appliance（ASA）のポート 5080 をオープンする必要があります。 これは、Cisco Adaptive Security Appliance（ASA）もアップグレードしたかどうかには無関係です。

既存のフェデレーション導入で IM and Presence と Cisco Adaptive Security Appliance（ASA）の両方をアップグレードする場合は、次のいずれかのアップグレード手順を使用してください。

アップグレード手順オプション 1：

1. IM and Presence を Release 9.0 にアップグレードします。
2. Cisco Adaptive Security Appliance（ASA）のポート 5080 に NAT ルールを設定します。
3. IM and Presence のアップグレード後にフェデレーションが導入で機能していることを確認します。
4. Cisco Adaptive Security Appliance（ASA）を Release 8.3 にアップグレードします。
5. Cisco Adaptive Security Appliance（ASA） のアップグレード後にフェデレーションが導入で機能していることを確認します。

アップグレード手順オプション 2：

1. IM and Presence ノードを Release 9.0、Cisco Adaptive Security Appliance（ASA）を Release 8.3 にそれぞれアップグレードします。
2. 両方のアップグレード後、Cisco Adaptive Security Appliance（ASA）のポート 5080 に NAT ルールを設定します。
3. フェデレーションが導入で機能していることを確認します。

Cisco Adaptive Security Appliance（ASA）に管理されているすべての IM and Presence Release 9.0 ノードに対してポート 5080 をオープンするには、必要なコマンドがあります。

Cisco Adaptive Security Appliance（ASA）Release 8.2 のスタティック コマンド	**Cisco Adaptive Security Appliance（ASA）Release 8.3 の NAT コマンド**

`static (inside,outside) tcp <public cup ip address> 5080 <routing cup private address> 5080 netmask 255.255.255.255`
 	
`static (inside,outside) tcp <public cup ip address> 45080 <intercluster cup8 private address> 5080 netmask 255.255.255.255`
 	
（注） クラスタ間 IM and Presence 9.0 サーバごとにこれらのコマンドを設定し、サーバごとに異なる任意のポートを使用します。
	`object service obj_tcp_source_eq_5080`
	`# service tcp source eq 5080`
	
	`nat (inside,outside) source static obj_host_<routing cupprivate address> obj_host_<public cup ip address> serviceobj_tcp_source_eq_5080 obj_tcp_source_eq_5080`
	
	`object service obj_tcp_source_eq_45080`
	`# service tcp source eq 45080`
	
	`nat (inside,outside) source static obj_host_<intercluster cup8 private address> obj_host_<public cup ip address>service obj_tcp_source_eq_5080 obj_tcp_source_eq_45080`
	
	（注） クラスタ間 IM and Presence 9.0 サーバごとにこれらのコマンドを設定し、サーバごとに異なる任意のポートを使用します。