SIP フェデレーションのための Cisco 適応型セキュリティ アプライアンスの構成

ここでは、SIP フェデレーション用の Cisco 適応型セキュリティ アプライアンスの設定について説明します。

Cisco 適応型セキュリティ アプライアンス ユニファイド コミュニケーション ウィザード

ドメイン間フェデレーション展開に単一の IM and Presence Service を展開する場合は、Cisco 適応型セキュリティアプライアンス の Unified Communication ウィザードを使用して、Cisco 適応型セキュリティアプライアンス と IM and Presence Service間のプレゼンス フェデレーション プロキシを構成できます。

Unified Communication ウィザードを示す構成例は、 適応型セキュリティ アプライアンス のドキュメント Wiki で提供されています。次の URL を参照してください。

関連情報

Cisco Unified Presence リリース 8.x

外部および内部インターフェイスの構成

Cisco 適応型セキュリティ アプライアンス では、次のように 2 つのインターフェイスを構成する必要があります。

- 1 つのインターフェイスを外部インターフェイスまたは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（Microsoft Access Edge/Access Proxy など）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または内部インターフェイスとして使用します。これは、展開に応じて、 IM and Presence Service またはロード バランサへのインターフェイスです。
- インターフェイスを構成する場合は、インターフェイス タイプ（イーサネットやギガビット イーサネットなど）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 適応型セキュリティ アプライアンス には、スロット 0 に 4 つの組み込みイーサネットまたはギガビット イーサネット ポートがあります。オプションで、スロット 1 に SSM-4GE モジュールを追加して、スロット 1 に 4 つのギガビット イーサネット ポートを追加できます。
- トラフィックをルーティングするインターフェイスごとに、インターフェイス名と IP アドレスを構成する必要があります。内部インターフェイ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存在する必要があります。つまり、異なるサブマスクが必要です。
- 各インターフェイスには、0 ～ 100（最低から最高）までのセキュリティ レベル範囲が必要です。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、最も安全性の低いインターフェイスです。内部インターフェイスまたは外部インターフェイスのセキュリティ レベルを明示的に設定しない場合、Cisco 適応型セキュリティ アプライアンス はセキュリティ レベルをデフォルトで 100 に設定します。
- CLI を使用した外部および内部インターフェイスの設定の詳細については、『*Cisco* セキュリティ アプライアンス コマンド ライン構成ガイド』を参照してください。

（注） ASDM スタートアップ ウィザードを使用して、内部インターフェイスと外部インターフェイスを構成できます。**[構成（Configuration）]** > **[デバイス設定（Device Setup）]** > **[インターフェイス（Interfaces）]** を選択して、ASDM で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 ルートの構成

Cisco 適応型セキュリティ アプライアンス は、スタティック ルートと、OSPF、RIP、EIGRP などのダイナミック ルーティング プロトコルの両方をサポートします。この統合では、Cisco 適応型セキュリティ アプライアンス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のネクスト ホップ アドレスを定義するスタティック ルートを構成する必要があります。次の手順では、dest_ip mask は接続先ネットワークの IP アドレスであり、gateway_ip 値はネクストホップ ルータまたはゲートウェイのアドレスです。

Cisco 適応型セキュリティ アプライアンスでのデフォルトルートおよびスタティック ルートの設定の詳細については、『*Cisco* セキュリティ アプライアンス コマンド ライン構成ガイド』を参照してください。

始める前に

外部および内部インターフェイスの構成 （2 ページ） の手順を実行します

ステップ 1 次の設定モードを入力します。

```
> Enable
> <password>
> configure terminal
```

ステップ 2 内部インターフェイスのスタティック ルートを追加するには、次のコマンドを入力します。

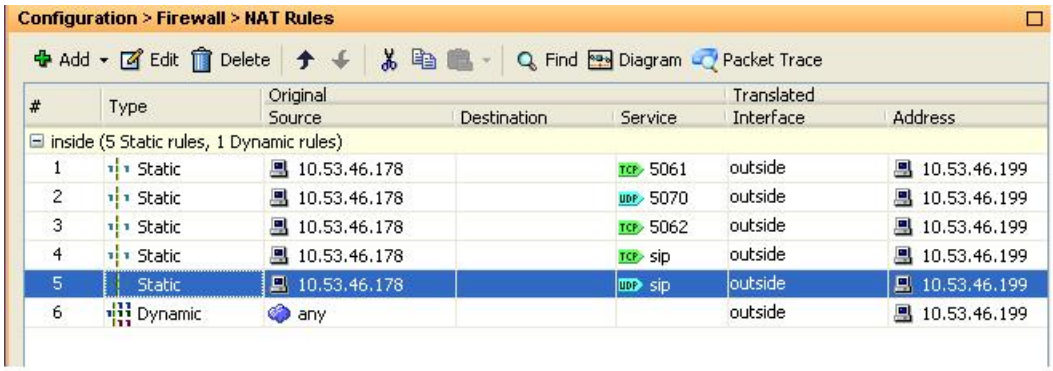
```
hostname(config)# route inside dest_ip mask gateway_ip
```

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のスタティック ルートを追加します。

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

（注） また、**[構成（Configuration）] > [デバイス セットアップ（Device Setup）] > [ルーティング（Routing）] > [スタティック ルート（Static routes）]** を選択して、ASDM からスタティック ルートを表示および構成することもできます。

図 *1 : ASDM* を介したスタティック ルートの表示



次のタスク

ポート アドレス変換（PAT） （4 ページ）

ポート アドレス変換（PAT）

ここでは、ポート アドレス変換の概念について説明します。

この統合向けのポート アドレス変換

（注） 外部ドメイン内の別の IM および Presence サービス エンタープライズ展開とフェデレーションする場合も、ポート アドレス変換を使用します。

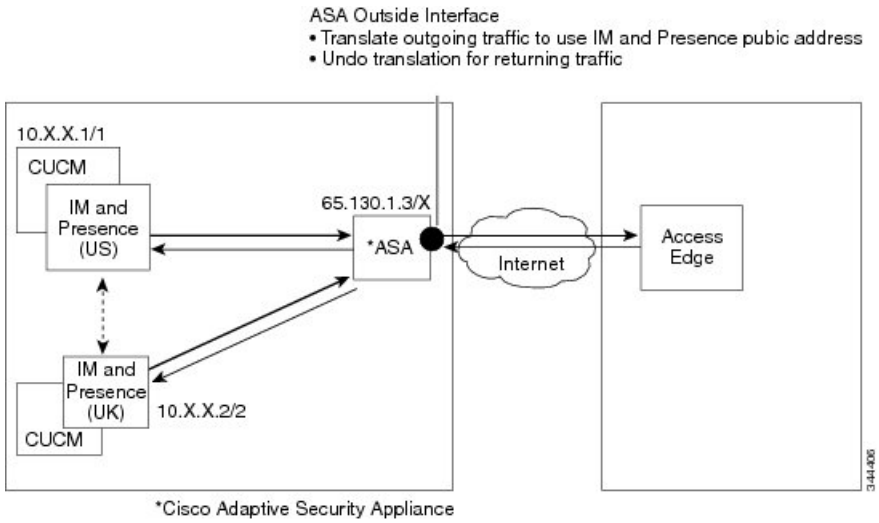
この統合のために、Cisco 適応型セキュリティ アプライアンス はポート アドレス変換（PAT）とスタティック PAT を使用してメッセージ アドレスを変換します。Cisco 適応型セキュリティ アプライアンス は、この統合にネットワークアドレス変換（NAT）を使用しません。

この統合では、PAT を使用して、 IM および Presence サービス から外部ドメインに送信されたメッセージを変換します（プライベート メッセージからパブリック メッセージへ）。ポート アドレス変換（PAT）は、パケット内の実際のアドレスを、宛先ネットワーク上でルーティング可能な、マッピングされた固有のポートと置き換えることを意味します。この変換方式では、実際の IP アドレスとポートをマッピング IP アドレスとポートに変換する 2 段階のプロセスを使用します。その後、変換はリターン トラフィックに対して「取り消されます」。

Cisco 適応型セキュリティ アプライアンスは、IM および Presence サービスのプライベート IP アドレスとポートを、パブリック 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、IM および Presence サービスから外部ドメイン（プライベート メッセージからパブリック メッセージ）に送信されたメッセージを変換します。したがって、ローカル IM および Presence

サービス ドメインは 1 つのパブリック IP アドレスのみを使用します。Cisco IM および Presence サービスは、次の図に示すように、NAT コマンドを外部インターフェイスに割り当て、そのインターフェイスで受信したメッセージの IP アドレスとポートを変換します。

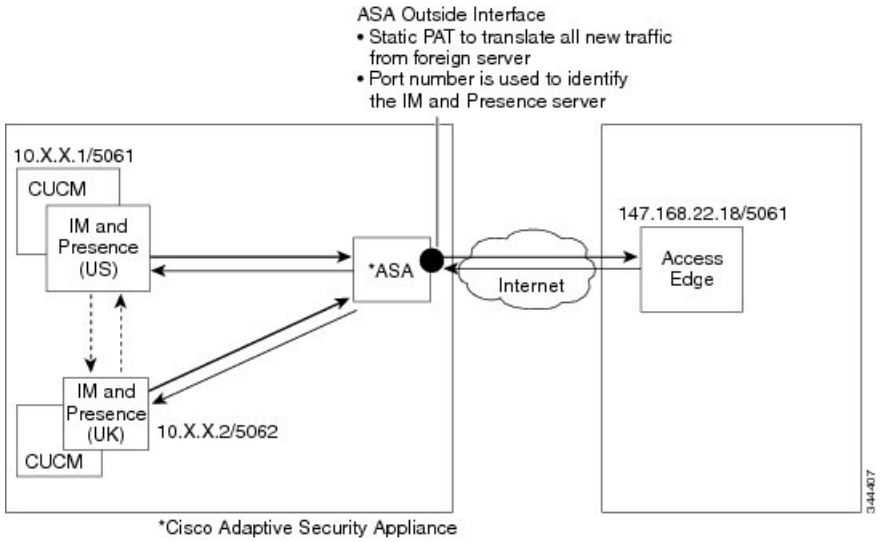
図 *2 : IM* および *Presence* サービスから外部ドメインに発信されるメッセージの *PAT* の例



外部ドメインから IM および Presence サービスに送信された新しいメッセージの場合、Cisco 適応型セキュリティ アプライアンス はスタティック PAT を使用して、IM および Presence サービスのパブリック IP アドレスとポートに送信されたメッセージを、指定された IM および Presence サービス ノードにマッピングします。スタティック PAT を使用すると、実際の IP アドレスをマッピング IP アドレスに変換し、実際のポート番号をマッピング 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または別のポート番号に変換できます。この場合、次の図に示すように、ポート番号はメッセージ要求を処理する正しい IM および Presence サービス ノードを識別します。

（注） ユーザーが IM および Presence サービス ノードに存在しない場合、 IM および Presence サービス ルーティング ノード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。すべての応答は、 IM および Presence サービス ルーティング ノードから Cisco 適応型セキュリティ アプライアンス 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のスタティック *PAT*



プライベートからパブリックへの要求の PAT

この統合では、プライベート メッセージからパブリック メッセージへのアドレス変換に次の構成が含まれます。

- 変換する実際の IP アドレスと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 適応型セキュリティ アプライアンスが内部インターフェイスで受信したすべてのメッセージに NAT アクションを適用する必要があることを示す NAT ルールを構成します。
- グローバル NAT アクションを設定して、外部（外部）インターフェイスを通過するメッセージに使用するマッピング アドレスを指定します。この統合では、アドレスを 1 つだけ指定します（PAT を使用するため）。NAT アクションは、（内部インターフェイスで受信したメッセージの）IP アドレスを IM および Presence サービスのパブリック アドレスにマッピングします。

次の表に、Cisco 適応型セキュリティ アプライアンス リリース 8.2 および 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 および Presence サービス展開と複数の IM および Presence サービス展開の両方に必須です。2 番目の行は、単一の IM および Presence サービス展開専用です。3 番目の行は、複数の IM および Presence サービス展開用です。

表 *1:* グローバル アドレス変換コマンドの例

構成サンプル	Cisco適応型セキュリティ アプライアンス リリース8.2グローバル コマンド	Cisco適応型セキュリティ アプライアンス リリース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 および Presence サービス ノードがあり、他のファイア ウォール トラフィックがない展開で使用できます。	**global (outside) 1** *public_imp_address* **nat (inside) 1 0 0**	**object network obj_any host 0.0.0.0 nat (inside,outside) dynamic** *public_imp_address*
この NAT 設定例は、内部インターフェイスに 1 つの IM および Presence サービス ノードがあり、他のファイアウォール トラフィックがある展開で使用できます。	**global (outside) 1** *public_imp_address* **nat (inside) 1** *private_imp_address* **255.255.255.255 global (outside) 2 interface nat (inside) 2 0 0**	**host** *private_imp_address* **nat (inside,outside) dynamic** *public_imp_address* **object network** *my_inside* **subnet 0.0.0.0 0.0.0.0 nat**（内部、外部）動的インターフェイス
この NAT 構成例は、内部インターフェイスに複数の IM および Presence サービス ノードがあり、他のファイアウォール トラフィックがある展開で使用できます。	**global (outside) 1** *public_imp_ip* **nat (inside) 1** *private_imp_net private_imp_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_imp_address* **object network** *my_inside* **subnet 0.0.0.0 0.0.0.0 nat (inside,outside) dynamic interface**

（注） 表の最後の行に示されている構成例は、Cisco 適応型セキュリティ アプライアンス の背後に複数の IM および Presence サービスノードがあり、これらの IM および Presence サービス ノードがすべて同じサブネット上にあることを前提としています。具体的には、すべての内部 IM および Presence サービス ノードが 2.2.2.x/24 ネットワーク上にある場合、NAT コマンドは **nat (inside) 1 2.2.2.0 255.255.255.0** です。

新しい要求のスタティック PAT

この統合では、プライベート メッセージからパブリック メッセージへのアドレス変換に次の構成が含まれます。

- 次のポートの TCP でスタティック PAT コマンドを構成します。5060、5061、5062、および 5080。

- ポート 5080 の UDP で別のスタティック PAT コマンドを構成します。

この統合では、次のポートを使用します。

- 5060：Cisco 適応型セキュリティ アプライアンス は、このポートを汎用 SIP インスペクションに使用します。
- 5061：SIP 要求がこのポートに送信され、TLS ハンドシェイクがトリガされます。
- 5062、5080： IM and Presence Service は、SIP VIA/CONTACT ヘッダーでこれらのポートを使用します。

（注） IM and Presence Service のピア認証リスナー ポートを確認するには、 **Cisco Unified CM IM and Presence Administration** にログインし、**[システム（System）] > [アプリケーション リスナー（Application Listeners）]** を選択します。

関連情報 -

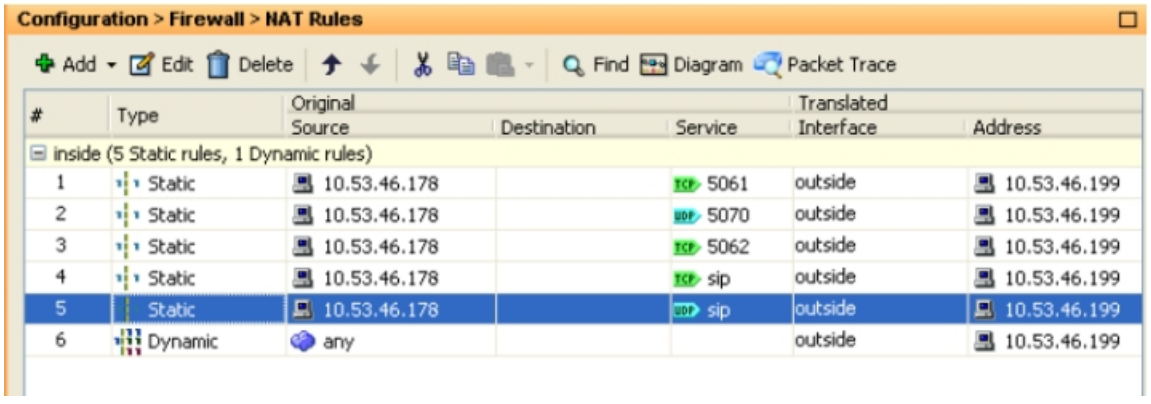
スタティック PAT コマンドの例

Cisco 適応型セキュリティ アプライアンス の構成例

ASDM の NAT ルール

ASDM で NAT ルールを表示するには、**[Configuration（構成）] > [Firewall（ファイアウォール）] > [NAT Rules（NAT ルール）]** を選択します。次の図に示す最初の 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 エントリは発信トラフィックをパブリック IM and Presence Service の IP アドレスとポートにマッピングする発信 PAT 構成です。

図 *4: ASDM* での *NAT* ルールの表示



関連情報

スタティック PAT コマンドの例

Cisco 適応型セキュリティ アプライアンス の構成例

スタティック PAT コマンドの例

（注） ここでは、Cisco 適応型セキュリティ アプライアンス リリース 8.3 およびリリース 8.2 のコマンド例を示します。フェデレーション用に Cisco 適応型セキュリティアプライアンス の新しい設定を行う場合は、これらのコマンドを実行する必要があります。

IM and Presence サービス ノードをルーティングするための PAT 構成

次の表に、ピア認証リスナーポートが 5062 である IM and Presence Service ノードをルーティングするための PAT コマンドを示します。

（注） Cisco 適応型セキュリティ アプライアンス8.3 の設定では、オブジェクトを 1 回定義するだけで、複数のコマンドでそのオブジェクトを参照できます。同じオブジェクトを繰り返し定義する必要はありません。

表 *2 : IM and Presence* サービス ノードをルーティングするための *PAT* コマンド

Cisco 適応型セキュリティ アプライアンス リリース 8.2 のスタティック コマンド	Cisco 適応型セキュリティ アプライアンス
static (inside,outside) tcp *public_imp_ip_address* **5061** *routing_imp_private_address* **5062 netmask 255.255.255.255** ルーティング IM and Presence Service 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_imp_ip_address* **5061** *routing_imp_private_address* **5061 netmask 255.255.255.255** **static (inside,outside) tcp** *public_imp_ip_address* **5080** *routing_imp_private_address* **5080 netmask 255.255.255.255** **static (inside,outside) tcp** *public_imp_ip_address* **5060** *routing_imp_private_address* **5060 netmask 255.255.255.255**	**object network** *obj_host_public_imp_ip_* **network** *obj_host_10.10.10.10*) **#host** *pu* **object network** *obj_host_routing_imp_pr* *routing_imp_private_address* **object service** *obj_tcp_source_eq_5061* **object service** *obj_tcp_source_eq_5062* **nat (inside,outside) source static** *obj_host_routing_imp_private_address ob* **service** *obj_tcp_source_eq_5062 obj_tcp* ルーティング IM and Presence Service ピア認 の場合は、次のコマンドを使用します。 **nat (inside,outside) source static** *obj_host_routing_imp_private_address ob* **service** *obj_tcp_source_eq_5061 obj_tcp*
--	**object service** *obj_tcp_source_eq_5080* **nat (inside,outside) source static** *obj_host_routing_imp_private_address ob* **service** *obj_tcp_source_eq_5080 obj_tcp*

Cisco 適応型セキュリティ アプライアンス リリース 8.2 のスタティック コマンド	Cisco 適応型セキュリティ アプライアンス リード
--	**object service** *obj_tcp_source_eq_5060* **ser** （注） 5060 は、サービス オブジェクトで「 **nat (inside,outside) source static** *obj_host_routing_imp_private_addres* *obj_host_public_imp_ip_address* **serv** *obj_tcp_source_eq_5060 obj_tcp_sou*
static (inside,outside) tcp *public_imp_ip_address* **5062** *routing_imp_private_address* **5062 netmask 255.255.255.255**	**nat (inside,outside) source static** *obj_host_routing_imp_private_address obj_h* **service obj_tcp_source_eq_5062 obj_tcp_so**

クラスタ間またはクラスタ内 IM および Presence サービス ノードの PAT 構成

マルチノードまたはクラスタ間 IM and Presence Service 展開で、 IM and Presence Service クラスタの非ルーティング ノードが Cisco 適応型セキュリティ アプライアンスと直接通信する場合は、これらのノードごとに一連のスタティック PAT コマンドを構成する必要があります。次に示すコマンドは、単一ノードに設定する必要がある一連のスタティック PAT コマンドの例です。

未使用の任意のポートを使用する必要があります。対応する番号を選択することを推奨します（例：5080 は未使用の任意のポート X5080 を使用）。X は、IM and Presence Service クラスタ間またはクラスタ内サーバに一意にマッピングされる番号に対応します。たとえば、45080 は 1 つのノードに一意にマッピングされ、55080 は別のノードに一意にマッピングされます。

次の表に、非ルーティング IM and Presence Service ノードの NAT コマンドを示します。それぞれの非ルーティング IM and Presence Service ノードのコマンドを繰り返します。

（注） Cisco 適応型セキュリティ アプライアンス8.3 の設定では、オブジェクトを 1 回定義するだけで、複数のコマンドでそのオブジェクトを参照できます。同じオブジェクトを繰り返し定義する必要はありません。

表 *3 :* 非ルーティング *IM and Presence Service* ノードの *NAT* コマンド

Cisco 適応型セキュリティ アプライアンス リリース 8.2 のスタティック コマンド	Cisco 適応型セキュリティ アプライアンス
static (inside,outside) tcp *public_imp_address* **45062** *intercluster_imp_private_address* **5062 netmask 255.255.255.255** クラスタ間 IM and Presence Service ピア認証リスニング ポートが 5061 の場合は、 コマンドを使用します。 **static (inside,outside) tcp** *public_imp_address* **45061** *intercluster_imp_private_address* **5061 netmask 255.255.255.255**	**object network** *obj_host_intercluster_imp intercluster_imp_private_address* **object service** *obj_tcp_source_eq_45062* **s** **nat (inside,outside) source static** *obj_host_intercluster_imp_private_addre obj_host_public_imp_ip_address* **service** *obj_tcp_source_eq_45062* クラスタ間 IM and Presence Service ピア認証 の場合は、 コマンドを使用します。 **object service** *obj_tcp_source_eq_45061* **s nat (inside,outside) source static** *obj_host_intercluster_imp_private_addre obj_host_public_imp_ip_address* **service** *obj_tcp_source_eq_45061*
static (inside,outside) tcp *public_imp_ip_address* **45080** *intercluster_imp_private_address* **5080 netmask 255.255.255.255**	**object service** *obj_tcp_source_eq_45080* **s nat (inside,outside) source static** *obj_host_intercluster_imp_private_addre obj_host_public_imp_ip_address* **service** *obj_tcp_source_eq_45080*
static (inside,outside) tcp *public_imp_ip_address* **45060** *intercluster_imp_private_address* **5060 netmask 255.255.255.255**	**object service** *obj_tcp_source_eq_45060* **s nat (inside,outside) source static** *obj_host_intercluster_imp_private_addre obj_host_public_imp_ip_address* **service** *obj_tcp_source_eq_45060*

関連情報 -

新しい要求のスタティック PAT

IM and Presence サービス ノードをルーティングするための PAT 構成

既存の展開での Cisco 適応型セキュリティアプライアンスのアップグレード オプション

Cisco 適応型セキュリティ アプライアンス リリース 8.2 からリリース 8.3 にアップグレードする場合、Cisco 適応型セキュリティ アプライアンス はアップグレード中に既存のコマンドをシームレスに移行します。

（注） IM and Presence Service リリース 9.0 にアップグレードしたら、Cisco 適応型セキュリティ アプライアンスの背後にある IM and Presence Service 9.0 ノードごとに、Cisco >適応型セキュリティ アプライアンスのポート 5080 を開く必要があります。これは、Cisco 適応型セキュリティ アプライアンス もアップグレードしたかどうかには関係ありません。

既存のフェデレーション展開で IM and Presence Service と Cisco 適応型セキュリティ アプライアンス 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ます。

アップグレード手順オプション 1：

1. IM and Presence Service をリリース 9.0 にアップグレードします。
2. Cisco 適応型セキュリティ アプライアンスでポート 5080 の NAT ルールを構成します。
3. IM and Presence Service のアップグレード後に、展開でフェデレーションが機能していることを確認します。
4. Cisco 適応型セキュリティ アプライアンス をリリース 8.3 にアップグレードします。
5. Cisco 適応型セキュリティ アプライアンス のアップグレード後に、展開環境でフェデレーションが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 Service ノードをリリース 9.0 に、Cisco 適応型セキュリティ アプライアンス をリリース 8.3 にアップグレードします。
2. 両方のアップグレード後に、Cisco 適応型セキュリティ アプライアンスでポート 5080 の NAT ルールを構成します。
3. 展開環境でフェデレーションが機能していることを確認します。

これらは、Cisco 適応型セキュリティ アプライアンス の背後にある IM and Presence Serviceリリース 9.0 ノードごとにポート 5080 を開くために必要なコマンドです。

表 *4 :* ポート *5080* を開く *Cisco ASA* コマンド

Cisco 適応型セキュリティ アプライアンス リリース 8.2 のスタティック コマンド	Cisco 適応型セキ
static (inside,outside) tcp *public_imp_ip_address* **5080** *routing_imp_private_address* **5080 netmask 255.255.255.255** **static (inside,outside) tcp** *public_imp_ip_address* **45080** *intercluster_imp_private_address* **5080 netmask 255.255.255.255** （注） クラスタ間 IM and Presence Service 9.0 ノードごとにこれらのコマンドを構成し、それぞれに異なる任意のポートを使用します。	**object service** **nat (inside,outs** *obj_host_public* **object service** **nat (inside,outs** *obj_host_public* （注） クラスタ間 れに異なる

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。