Cisco Adaptive Securiy Appliance での TLS プロキシ設定

IM and Presence サービス リリース 8.5(2) 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 サービス リリース 8.5(2) 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。

TLS プロキシ設定の最新のリリース情報については、『*Cisco Adaptive Security Appliance Configuration Guide*』を参照してください。

TLS プロキシ

Cisco Adaptive Security Appliance は、IM and Presence サービスと外部サーバの間の TLS プロキシとして機能します。つまり、Cisco Adaptive Security Appliance は、（TLS 接続を開始した）サーバの代わりに TLS メッセージを仲介し、プロキシとしての自分からクライアントに TLS メッセージをルーティングします。TLS プロキシは、着信レッグの TLS メッセージを必要に応じて復号化、検査および変更してから、応答レッグのトラフィックを再暗号化します。

（注） TLS プロキシを設定する前に、Cisco Adaptive Security Appliance と IM and Presence サービス間と、Cisco Adaptive Security Appliance と外部サーバ間に Cisco Adaptive Security Appliance 証明書を設定する必要があります。これを行うには、次の項の手順を実行する必要があります。

- IM and Presence サービスと Cisco Adaptive Security Appliance の間でのセキュリティ証明書交換
- Microsoft CA を使用した Cisco Adaptive Security Appliance と Microsoft Access Edge（外部インターフェイス）の間でのセキュリティ証明書交換

関連トピック

一般的な Cisco Adaptive Security Appliance の問題と推奨される操作

アクセス リストの設定の要件

この項では、単一の IM and Presence サービス導入に必要なアクセス リストの設定をリストします。

（注）
- アクセス リストごとに、対応するクラスマップを設定するとともに、ポリシーマップのグローバル ポリシーにエントリを設定する必要があります。
- IM and Presence サービスのピア認証リスナー ポートを調べるには、**Cisco Unified Communications Manager 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。

表 *1*：単一の *IM and Presence* サービス アクセス リスト設定の要件

項目	説明
配置シナリオ：1 つ以上の外部ドメインと連携する IM and Presence サービス ノード	

項目	説明
設定要件：	IM and Presence サービスがフェデレーションする外部ドメインごとに、次の 2 つのアクセス リストを設定します。 • IM and Presence サービスがポート 5061 で外部ドメインにメッセージを送信できるようにアクセス リストを設定します。 • IM and Presence サービスがポート 5061 で外部ドメインからメッセージを受信できるようにアクセス リストを設定します。Cisco Adaptive Security Appliance リリース 8.3 を使用する場合は、IM and Presence サービスが SIP フェデレーションをリッスンする実際のポートを使用します（IM and Presence サービス ピア認証のリスナー ポートを確認してください）。
設定例：	**access-list** *ent_imp_to_external_server* **extended permit tcp host** *routing_imp_private_address* **host** *external_public_address* **eq 5061** Cisco Adaptive Security Appliance リリース 8.2: **access-list** *ent_external_server_to_imp* **extended permit tcp host** *external_public_address* **host** *imp_public_address* **eq 5061** Cisco Adaptive Security Appliance リリース 8.3: **access-list** *ent_external_server_to_imp* **extended permit tcp host** *external_public_address* **host** *imp_private_address* **eq 5061** （注） 前述のアクセス リストで、5061 は、SIP メッセージングが行われていないかどうかを IM and Presence サービスがリッスンするポートです。IM and Presence サービスがポート 5062 をリッスンする場合は、アクセス リストに 5062 を指定します。
配置シナリオ：クラスタ間展開。これは、マルチノード展開にも適用されます。	
設定要件：	クラスタ間 IM and Presence サービス ノードごとに、次の 2 つのアクセス リストを設定します。 • IM and Presence サービスがポート 5061 で外部ドメインにメッセージを送信できるようにアクセス リストを設定します。 • IM and Presence サービスが任意ポート 5061 で外部ドメインからメッセージを受信できるようにアクセス リストを設定します。Cisco Adaptive Security Appliance リリース 8.3 を使用する場合は、IM and Presence サービスが SIP フェデレーションをリッスンする実際のポートを使用します（IM and Presence サービス ピア認証のリスナー ポートを確認してください）。

項目	説明
設定例：	**access-list** *ent_intercluster_imp_to_external_server* **extended permit tcp host** *intercluster_imp_private_address* **host external public address eq 5061** Cisco Adaptive Security Appliance リリース 8.2: **access-list** *ent_external_server_to_intercluster_imp* **extended permit tcp host** *external_public_address* **host** *imp* **public address eq** *arbitrary_port* Cisco Adaptive Security Appliance リリース 8.3: *ent_external_server_to_intercluster_imp* **extended permit tcp host** *external_public_address* **host** *imp_private_address* **eq** *5061* 前述のアクセス リストで、5061 は、SIP メッセージングが行われていないかどうかを IM and Presence サービスがリッスンするポートです。IM and Presence サービスがポート 5062 をリッスンする場合は、アクセス リストに 5062 を指定します。

関連トピック

Cisco Adaptive Security Appliance の設定例
TLS プロキシ インスタンスの設定, （4 ページ）
クラス マップを使用したアクセス リストと TLS プロキシ インスタンスの関連付け, （6 ページ）
TLS プロキシの有効化, （7 ページ）

TLS プロキシ インスタンスの設定

本統合を実現するには、2 つの TLS プロキシ インスタンスを作成する必要があります。最初の TLS プロキシでは、IM and Presence サービスが開始した TLS 接続を処理します。ここでは、IM and Presence サービスがクライアント、外部ドメインはサーバです。この場合、Cisco Adaptive Security Appliance が、IM and Presence サービスをクライアントとする TLS サーバとして機能します。2 番目の TLS プロキシでは、外部ドメインによって開始された TLS 接続を処理します。ここで、外部ドメインはクライアントで、IM and Presence サービスがサーバです。

TLS プロキシ インスタンスは、サーバとクライアントの両方に対して「トラストポイント」を定義します。TLS ハンドシェイクが開始された方向によって、サーバおよびクライアントのコマンドで定義されるトラストポイントが決定されます。

- TLS ハンドシェイクが IM and Presence サービスから外部ドメインに向かって開始された場合は、サーバ コマンドで指定するトラストポイントには、Cisco Adaptive Security Appliance 自己署名証明書を含めます。クライアント コマンドで指定するトラストポイントには、Cisco Adaptive Security Appliance と外部ドメインの間の TLS ハンドシェイクで使用される Cisco Adaptive Security Appliance 証明書を含めます。

- ハンドシェイクが外部ドメインから IM and Presence サービスに向かって開始された場合は、サーバ コマンドで指定するトラストポイントには、Cisco Adaptive Security Appliance と外部ドメインの間の TLS ハンドシェイクで使用する Cisco Adaptive Security Appliance 証明書を含めます。クライアント コマンドで指定するトラストポイントには、Cisco Adaptive Security Appliance 自己署名証明書を含めます。

はじめる前に

- アクセス リストの設定の要件, （2 ページ）の手順を実行します。

手順

ステップ 1 コンフィギュレーション モードを開始します。

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

ステップ 2 IM and Presence サービスによって開始された TLS 接続に対して、TLS プロキシ インスタンスを作成します。次の例では、imp_to_external という TLS プロキシ インスタンスが作成されます。

```
tls-proxy ent_imp_to_external
server trust-point imp_proxy
client trust-point trustpoint_name
client cipher-suite aes128-sha1 aes256-sha1 3des-sha1 null-sha1
```

ステップ 3 外部ドメインによって開始された TLS 接続に対して、TLS プロキシ インスタンスを作成します。次の例では、foreign_to_cup という TLS プロキシ インスタンスが作成されます。

```
tls-proxy ent_external_to_imp
server trust-point trustpoint_name
client trust-point imp_proxy
client cipher-suite aes128-sha1 aes256-sha1 3des-sha1 null-sha1
```

次の作業

クラス マップを使用したアクセス リストと TLS プロキシ インスタンスの関連付け, （6 ページ）

クラス マップを使用したアクセス リストと TLS プロキシ インスタンスの関連付け

クラス マップ コマンドを使用して、以前に定義した各外部ドメイン アクセス リストに TLS プロキシ インスタンスを関連付ける必要があります。

はじめる前に

の手順を実行します。 TLS プロキシ インスタンスの設定, （4 ページ）

手順

ステップ 1 コンフィギュレーション モードを開始します。

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

ステップ 2 各アクセス リストに、クラス マップが使用する TLS プロキシ インスタンスを関連付けます。クラス マップが IM and Presence サービスから外部ドメインへのメッセージ用か、外部ドメインから IM and Presence サービスへのメッセージ用かによって、選択する TLS プロキシが異なります。次の例では、IM and Presence サービス外部ドメインへ送信されたメッセージのアクセス リストが、IM and Presence サービスによって開始された TLS 接続の「ent_imp_to_external」という TLS プロキシ インスタンスに関連付けられます。

```
class-map ent_imp_to_external match access-list ent_imp_to_external
```

次の例では、外部ドメインから IM and Presence サービスに送信されるメッセージのアクセス リストが、「ent_external_to_imp」という外部サーバによって開始された TLS 接続の TLS プロキシ インスタンスと関連付けられます。

```
class-map ent_external_to_imp match access-list ent_external_to_imp
```

ステップ 3 クラスタ間 IM and Presence サービス導入を使用している場合は、各 IM and Presence サービス ノードにクラスマップを設定し、以前に定義したサーバの該当するアクセスリストに関連付けます。次に例を示します。

```
class-map ent_second_imp_to_external match access-list ent_second_imp_to_external
class-map ent_external_to_second_imp match access-list ent_external_to_second_imp
```

次の作業

TLS プロキシの有効化, （7 ページ）

TLS プロキシの有効化

ポリシー マップ コマンドを使用して、前の項で作成したクラス マップごとに TLS プロキシを有効化する必要があります。

（注） フェデレーテッド導入に対し、Cisco Adaptive Security Appliance で高レベル セキュリティの sip-inspect ポリシー マップは、設定しても失敗するため使用できません。低レベル/中のセキュリティ ポリシー マップを使用する必要があります。

はじめる前に

の手順を実行します。クラス マップを使用したアクセス リストと TLS プロキシ インスタンスの関連付け，（6 ページ）

手順

ステップ 1 コンフィギュレーション モードを開始します。

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

ステップ 2 sip-inspect ポリシー マップを定義します。次に例を示します。

```
policy-map type inspect sip sip_inspectParameters
```

ステップ 3 グローバル ポリシー マップを定義します。次に例を示します。

```
policy-map global_policy class ent_cup_to_external inspect sip sip_inspect tls-proxy
ent_cup_to_external
```

Cisco Adaptive Security Appliance のクラスタ間導入用設定

クラスタ間 IM and Presence サービス導入では、IM and Presence サービス ノードを追加するたびに、Cisco Adaptive Security Appliance で次の設定を行う必要があります。

手順

ステップ 1 IM and Presence サービス ノードに対する追加アクセス リストを作成します。

ステップ 2 Cisco Adaptive Security Appliance セキュリティ証明書を生成し、IM and Presence サービス ノードにインポートします。

ステップ 3 IM and Presence サービス セキュリティ証明書を生成し、Cisco Adaptive Security Appliance にインポートします。

ステップ 4 外部ドメインごとにクラス マップを設定します。

ステップ 5 クラス マップをグローバル ポリシー マップに追加します。

関連トピック

IM and Presence サービスと Cisco Adaptive Security Appliance の間でのセキュリティ証明書交換
IM and Presence サービスと Cisco Adaptive Security Appliance の間でのセキュリティ証明書交換
クラス マップを使用したアクセス リストと TLS プロキシ インスタンスの関連付け, （6 ページ）
TLS プロキシの有効化, （7 ページ）
クラスタ間展開とマルチノード展開