Cisco Adaptive Security Appliance（ASA）での TLS プロキシの設定

（注） TLS プロキシの設定に関する最新のリリース情報については、http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_configure.html にある『Cisco Adaptive Security Appliance Configuration Guide』を参照してください。

（注） IM and Presence Release 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 Release 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

Cisco Adaptive Security Appliance（ASA）は、IM and Presence 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（ASA）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（ASA）と IM and Presence 間の Cisco Adaptive Security Appliance（ASA）セキュリティ証明書と Cisco Adaptive Security Appliance（ASA） と外部サーバ間のセキュリティ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 と Cisco Adaptive Security Appliance（ASA）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（ASA）と Microsoft アクセス エッジ（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 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。
- [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。

導入シナリオ：	1 つ以上の外部ドメインとのフェデレーションを行う IM and Presence サーバ
設定要件：	IM and Presence 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 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 が SIP フェデレーションがないかリッスンする実際のポート（Cisco Adaptive Security Appliance（ASA）Release 8.3 を使用している場合。IM and Presence のピア認証リスニング ポートをチェックします）かポート 5061 で、IM and Presence が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。

設定例：	`access-list ent_cup_to_foreign_server extended permit tcp host <routing cup private address> host <foreign public address> eq 5061`
	
	Cisco Adaptive Security Appliance（ASA）Release 8.2：
	
	`access-list ent_foreign_server_to_cup extended permit tcp host <foreign public address> host < CUP public address> eq 5061`
	
	Cisco Adaptive Security Appliance（ASA）Release 8.3：
	
	`access-list ent_foreign_server_to_cup extendedpermit tcp host <foreign public address> host <CUP 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 がリッスンするポートです。 IM and Presence 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。

導入シナリオ：	クラスタ間導入 （これはマルチノード導入にも適用されます）
設定要件：	クラスタ間 IM and Presence サーバごとに、次の 2 つのアクセス リストを設定します。 • IM and Presence 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 が SIP フェデレーションがないかリッスンする実際のポート（ Cisco Adaptive Security Appliance（ASA）Release 8.3 を使用している場合。IM and Presence のピア認証リスニング ポートをチェックします）か任意のポート 5061 で、 IM and Presence が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。

設定例：	`access-list ent_intercluster_cup_to_foreign_server extended permit tcp host <intercluster cup private address> host <foreign public address> eq 5061`
	
	Cisco Adaptive Security Appliance（ASA）Release 8.2：
	
	`access-list ent_foreign_server_to_intercluster_cup extended permit tcp host <foreign public address> host <cup public address> eq <arbitrary port>`
	
	Cisco Adaptive Security Appliance（ASA）Release 8.3：

	ent_foreign_server_to_intercluster_cupextended permit tcp host <foreign public address> host <cup 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 がリッスンするポートです。 IM and Presence 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（ASA）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, （5 ページ）
TLS プロキシの有効化, （6 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 によって開始された TLS 接続を処理します。ここで、IM and Presence はクライアントで、外部ドメインがサーバです。 この場合、Cisco Adaptive Security Appliance（ASA）が、IM and Presence 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 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 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（ASA）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（ASA）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（ASA）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 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（ASA）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（ASA）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（ASA）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 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 IM and Presence 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、cup_to_foreign という TLS プロキシ インスタンスが作成されます。

```
tls-proxy ent_cup_to_foreignserver trust-point cup_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_foreign_to_cupserver trust-point <trustpoint_name>
client trust-point cup_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, （5 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

TLS プロキシ インスタンスの設定, （4 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 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。 選択する TLS プロキシは、クラス マップが IM and Presence から外部ドメインへのメッセージなのか、外部ドメインから IM and Presence へのメッセージなのかによって異なります。
次の例では、IM and Presence から外部ドメインに送信されるメッセージのアクセス リストが、「ent_cup_to_foreign」という IM and Presence 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_cup_to_foreignmatch access-list ent_cup_to_foreign
```

次の例では、外部ドメインから IM and Presence に送信されるメッセージのアクセス リストが、「ent_cup_to_foreign」という外部ドメイン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_foreign_to_cupmatch access-list ent_foreign_to_cup
```

ステップ 3 クラスタ間 IM and Presence 導入を使用している場合は、各 IM and Presence サーバにクラス 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_cup_to_foreignmatch access-list
ent_second_cup_to_foreign
class-map ent_foreign_to_second_cup
match access-list ent_foreign_to_second_cup
```

次の作業

TLS プロキシの有効化, （6 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（ASA） 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

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, （5 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 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
!SIP Inspection Parameters
```

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_policyclass ent_cup_to_foreign
inspect sip sip_inspect tls-proxy ent_cup_to_foreign
```

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

クラスタ間 IM and Presence 導入では、IM and Presence サーバを**追加するたびに**、Cisco Adaptive Security Appliance（ASA）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 サーバ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（ASA）セキュリティ証明書を作成し、IM and Presence サーバにインポートします。

ステップ 3 IM and Presence セキュリティ証明書を作成し、Cisco Adaptive Security Appliance（ASA）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 と Cisco Adaptive Security Appliance（ASA）の間でのセキュリティ証明書交換
IM and Presence と Cisco Adaptive Security Appliance（ASA）の間でのセキュリティ証明書交換