ゲートウェイおよびトランクの暗号化の設定

この章では、ゲートウェイとトランクの暗号化の設定について説明します。

Cisco IOS MGCP ゲートウェイの暗号化

Unified Communications Manager は、MGCP SRTP パッケージを使用するゲートウェイをサポートしています。MGCP SRTP パッケージは、ゲートウェイがセキュア RTP 接続上でパケットを暗号化および復号化するときに使用されます。コールセットアップ中に交換される情報によって、ゲートウェイがコールに SRTP を使用するかどうかが決まります。デバイスが SRTP をサポートしている場合、システムは SRTP 接続を使用します。少なくとも1つのデバイスが SRTP をサポートしていない場合、システムは RTP 接続を使用します。SRTP から RTP へのフォールバック（またはその逆）は、安全なデバイスから安全ではないデバイスへの転送、会議、トランスコーディング、保留音などの場合に発生する可能性があります。

システムが 2 台のデバイス間で暗号化 SRTP コールを設定する場合、Unified Communications Manager はセキュアコール用のマスター暗号化キーと salt を生成し、SRTP ストリーム専用のゲートウェイに送信します。Unified Communications Manager は SRTCP ストリーム用のキーと salt を送信しませんが、ゲートウェイはこれらもサポートします。これらのキーは、MGCP シグナリング パスを介してゲートウェイに送信されます。このパスは IPSec を使用して保護する必要があります。Unified Communications Manager は IPSec 接続が存在するかどうかを認識しませんが、IPSec が設定されて

いない場合、システムはゲートウェイにセッションキーをクリアテキストで送信します。セッション キーがセキュアな接続を介して送信されるよう、IPSec 接続が存在することを確認します。

ヒント SRTP 用に設定されている MGCP ゲートウェイが、認証済みデバイス（たとえば、SCCP を実行している認証済み電話機）とのコールに関与している場合、 Unified Communications Managerがコールを認証済みとして分類するため、電話機に保護アイコンが表示されます。 Unified Communications Managerは、デバイスの SRTP 機能がコールのネゴシエートに成功した場合、コールを暗号化として分類します。MGCP ゲートウェイが、セキュリティ アイコンを表示できる電話に接続されている場合、コールが暗号化されているときは電話に鍵アイコンが表示されます。

次に、MGCP E1 PRI ゲートウェイについての説明を示します。

- SRTP 暗号化の MGCP ゲートウェイを設定する必要があります。コマンド **mgcppackage-capabilitysrtp-package** を使用してゲートウェイを設定します。
- MGCP ゲートウェイでは、[高度な IP サービス（Advanced IP Services）] または [高度な企業サービス（Advanced Enterprise Services）] イメージを指定する必要があります。

  たとえば、**c3745-adventerprisek9-mz.124-6.T.bin** など。
- 保護ステータスは、COCP PRI Setup、Alert、および Connect の各メッセージで独自の FacilityIE を使用して、交換用の CP E1 PRI ゲートウェイと交換されます。
- Unified Communications Manager は、Cisco Unified IP 電話 でのみセキュア通知トーンを再生します。ネットワーク内の PBX は、コールのゲートウェイ側にトーンを再生します。
- Cisco Unified IP 電話 と MGCP E1 PRI ゲートウェイの間のメディアが暗号化されていないと、コールはドロップされます。

（注） MGCP ゲートウェイの暗号化の詳細については、使用している Cisco IOS ソフトウェアのバージョンの『*Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways*』を参照してください。

H.323 ゲートウェイおよび h.323/h.323/.h トランク暗号化 (h.323)

セキュリティをサポートする H.323 ゲートウェイおよびゲートキーパー、または非ゲートキーパー制御の H.225/H.323/H.245 トランクは、Cisco Unified Communications Operating System で IPSec アソシエーションを設定した場合、Unified Communications Manager に対して認証できます。Unified Communications Manager とこれらのデバイスの間での IPSec アソシエーション作成については、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

H.323、H.225、およびH.245デバイスでは暗号キーが生成されます。これらのキーは、IPSec で保護されたシグナリング パスを介して Unified Communications Manager に送信されます。Unified Communications Manager は IPSec 接続が存在するかどうかを認識しませんが、IPSec が設定されていない場合、セッションキーは暗号化されずに送信されます。セッションキーがセキュアな接続を介して送信されるよう、IPSec 接続が存在することを確認します。

IPSec アソシエーションの設定に加えて、Unified Communications Manager Administration のデバイス設定ウィンドウにある [SRTP 許可（SRTP Allowed）] チェックボックスにマークを付ける必要があります。これはH.323 ゲートウェイ、H.225 トランク（ゲートキーパー制御）、クラスタ間トランク（ゲートキーパー制御）、およびクラスタ間トランク（非ゲートキーパー制御）の設定ウィンドウなどに存在します。このチェックボックスをオンにしない場合、Unified Communications Manager は RTP を使用してデバイスと通信します。このチェックボックスをオンにする場合、Unified Communications Manager は SRTP がデバイスに対して設定されているかどうかに応じて、セキュア コールと非セキュア コールを許可します。

注意 Unified Communications Manager Administration で [SRTP Allowed] チェックボックスをオンにする場合は、セキュリティ関連情報が暗号化されずに送信されることを防ぐために、IPSec を設定することを強く推奨します。

Unified Communications Manager は、IPSec 接続が正しく設定されたかどうかを確認しません。接続を正しく設定しないと、セキュリティ関連の情報がクリアテキストで送信されることがあります。

セキュア メディア パスまたはセキュア シグナリング パスを確立でき、デバイスがSRTP をサポートする場合、システムはSRTP 接続を使用します。セキュア メディア パスまたはセキュア シグナリング パスを確立できないか、1 つ以上のデバイスが SRTP をサポートしない場合、システムは RTP 接続を使用します。SRTP から RTP へのフォールバック（またはその逆）は、安全なデバイスから安全ではないデバイスへの転送、会議、トランスコーディング、保留音などの場合に発生する可能性があります。

ヒント コールがパススルー対応 MTP を使用し、リージョン フィルタリングの後でデバイスの音声機能が一致し、どのデバイスについても [MTP Required] チェックボックスがオンになっていない場合、Unified Communications Manager はそのコールをセキュアとして分類します。[MTP Required] チェックボックスがオンの場合、Unified Communications Manager はコールの音声パススルーを無効にし、コールを非セキュアとして分類します。MTP がコールに関係しない場合、Unified Communications Manager はデバイスの SRTP 機能に応じてそのコールを暗号化済みに分類することがあります。

Unified Communications Manager は、そのデバイスの [SRTP Allowed] チェックボックスがオンで、そのデバイスの SRTP 機能がコールに対して正常にネゴシエートされれば、コールを暗号化済みに分類します。 コールを暗号化済みとして分類します。前述の条件を満たさない場合、Unified Communications Manager はコールを非セキュアとして分類します。デバイスが、セキュリティ アイコンを表示できる電話に接続されている場合、コールが暗号化されているときは電話機に鍵アイコンが表示されます。

Unified Communications Manager は、トランクまたはゲートウェイ経由の発信 FastStart コールを非セキュアとして分類します。Unified Communications Manager Administration で [SRTP Allowed] チェックボックスをオンにした場合、Unified Communications Manager は **[Enable Outbound FastStart]** チェックボックスをオフにします。

Unified Communications Manager の一部の種類のゲートウェイおよびトランクでは、共有秘密キー（Diffie-Hellman キー）やその他の H.235 データを 2 つの H.235 エンドポイント間で透過的にパススルーさせることができます。このため、これら 2 つのエンドポイントではセキュア メディア チャネルを確立できます。

[H.235 data] の通過を有効にするには、次のトランクおよびゲートウェイの構成時の設定で [**h.235 パススルーを許可**する] チェックボックスをオンにします。

- 「-225 Trunk」
- ICT ゲートキーパー制御
- ICT 非ゲートキーパー制御
- H.323 ゲートウェイ

トランクとゲートウェイの設定の詳細については、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

SIP トランクの暗号化

SIP トランクは、シグナリングとメディアの両方でセキュアなコールをサポートできます。TLS はシグナリング暗号化を提供し、SRTP はメディア暗号化を提供します。

トランクのシグナリング暗号化を設定するには、SIP トランクセキュリティプロファイル ([**システム** > **セキュリティプロファイル** > **(sip trunk security profile)**] ウィンドウで) を設定するときに、次のオプションを選択します。

- **[デバイス セキュリティ モード（Device Security Mode）]** ドロップダウンリストから、「[暗号化済（Encrypted）]」 を選択します。
- **[着信転送タイプ（Incoming Transport Type）]** ドロップダウンリストから 「[TLS]」 を選択します。
- **[発信転送タイプ（Outgoing Transport Type）]** ドロップダウンリストから 「[TLS]」 を選択します。

SIP トランクセキュリティプロファイルを設定したら、そのプロファイルをトランクに適用します ([**Device** > **trunk** > **sip trunk** configuration] ウィンドウ)。

トランクに対してメディア暗号化を設定するには、**[SRTPを許可（SRTP Allowed）]** チェックボックスをオンにします（**[デバイス（Device）][トランク][SIP トランク（SIP Trunk）]** 設定ウィンドウでも同様です）。

⚠

注意 このチェックボックスをオンにする場合は、キーやその他のセキュリティ関連情報がコールネゴシエーション中に公開されないように、暗号化された TLS プロファイルを使用することを推奨します。非セキュアプロファイルを使用する場合でも SRTP は機能しますが、キーはシグナリングおよびトレースで公開されます。この場合、 Unified Communications Managerとトランクの接続先間でネットワークのセキュリティを確保する必要があります。

関連トピック

SIP トランク セキュリティ プロファイルの設定

セキュアゲートウェイとトランクのセットアップ

この手順は、 *CiscoIOS* のメディアおよびシグナリングの認証および暗号化機能と組み合わせて使用します。これにより、セキュリティのためにCiscoIOS MGCP ゲートウェイを設定する方法に関する情報が提供されます。

手順

Step 1 **ctls ctl** コマンドを実行してクラスタを混合モードに設定したことを確認します。

Step 2 電話機が暗号化用に設定されていることを確認します。

Step 3 IPSec を設定します。

ヒント ネットワークインフラストラクチャで IPSec を設定することも、 Unified Communications Managerとゲートウェイまたはトランクとの間でIPSecを設定することもできます。IPSec を設定するために 1 つの方式を実装する場合、他の方式を実装する必要はありません。

Step 4 H.323 IOS ゲートウェイおよびクラスタ間トランクの場合、Unified Communications Manager で [SRTPを許可する（SRTP Allowed）] チェックボックスをオンにします。

[SRTPを許可する（SRTP Allowed）]チェックボックスは、[トランクの設定（Trunk Configuration）]ウィンドウまたは[ゲートウェイの設定（Gateway Configuration）]ウィンドウに表示されます。これらのウィンドウを表示する方法については、Cisco Unified Communications Manager アドミニストレーション ガイドのトランクおよびゲートウェイに関する章を参照してください。

Step 5 SIP トランクの場合、SIP トランク セキュリティプロファイルを設定し、トランクに適用します（この処理を行っていない場合）。また、**[デバイス（Device）] > [トランク（Trunk）] > [SIP トランク（SIP Trunk）]** の設定ウィンドウで **[SRTP を許可する（SRTP allowed）]** チェックボックスを必ずオンにします。

注意 **[SRTP を許可する（SRTP Allowed）]** チェックボックスをオンにする場合、コール ネゴシエーション中にキーやその他のセキュリティ関連情報が公開されないようにするために、暗号化されたTLSプロファイルを使用することを推奨します。非セキュアプロファイルを使用すると、SRTPは機能しますが、キーはシグナリングおよびトレースで公開されます。この場合、 Unified Communications Managerとトランクの接続先間でネットワークのセキュリティを確保する必要があります。

Step 6 ゲートウェイでセキュリティ関連の設定タスクを実行します。

詳細については、『*Media and Signaling Authentication and Encryption Feature for Cisco IOS MGCP Gateways*』を参照してください。

関連トピック

Cisco CTL クライアントの設定
Unified Communications Manager とゲートウェイまたはトランク間の IPsec の設定, on page 7
ネットワーク インフラストラクチャ内の IPSec 設定, on page 6
電話機のセキュリティ
デフォルトのセキュリティ機能
SIP トランク セキュリティ プロファイルの設定

ネットワーク インフラストラクチャ内の IPSec 設定

このセクションでは、IPSec の設定方法については説明しません。代わりに、ネットワーク インフラストラクチャでIPsecを設定する際の考慮事項と推奨事項について記載されています。ネットワーク インフラストラクチャ内で IPsec を設定する予定であり、Unified Communications Manager とデバイスの間では設定しない場合、IPsec の設定前に次の情報を検討してください。

- Ciscoでは、Unified Communications Manager 自体ではなく、インフラストラクチャの中でIPsecをプロビジョニングすることを推奨します。
- IPsec を設定する前に、既存の IPsec 接続または VPN 接続、プラットフォームの CPU への影響、帯域幅への影響、ジッターや遅延などの評価指標について考慮します。
- 『*Voice and Video Enabled IPsec Virtual Private Networks Solution Reference Network Design Guide*』を参照します。

- 『*Cisco IOS Security Configuration Guide, Release 12.2*』（またはそれ以降）を参照します。
- IPsec 接続のリモートエンドをセキュアな CiscoIOS MGCP ゲートウェイで終端します。
- テレフォニーサーバが存在するネットワークの信頼された球体内のネットワークデバイスでホストの終端を終端します。たとえば、ファイアウォール、アクセスコントロールリスト(ACL)、またはその他のレイヤ3デバイスの背後にあります。
- ホスト側IPsec接続の終端に使用する機器は、ゲートウェイの数とそれらのゲートウェイに予想されるコールの量とによって決まります。たとえば、Cisco VPN 3000 シリーズ コンセントレータ、Catalyst 6500 IPsec VPN サービス モジュール、Cisco サービス統合型ルータなどがあります。
- セキュアゲートウェイとトランクの設定に関連するトピックで指定されている順序で手順を実行します。

注意 IPsec接続を設定してその接続がアクティブであることを確認しないと、メディアストリームのプライバシーが損なわれる可能性があります。

Unified Communications Manager とゲートウェイまたはトランク間の IPsec の設定

Unified Communications Manager と、この章で説明されているゲートウェイやトランクとの間の IPSec の設定に関する情報については、『*Administration Guide for Cisco Unified Communications Manager*』を参照してください。

Cisco Unified Communications Manager Administration を使用した SRTP の許可

[SRTP を許可する（SRTP Allowed）] チェックボックスは、Unified Communications Managerの次の設定ウィンドウに表示されます。

- H.323 ゲートウェイの設定ウィンドウ
- [H.225 Trunk (Gatekeeper Controlled) Configuration] ウィンドウ
- [Inter-Cluster Trunk (Gatekeeper Controlled) Configuration] ウィンドウ
- [Inter-Cluster Trunk (Non-Gatekeeper Controlled) Configuration] ウィンドウ
- [SIP トランクの設定 (SIP Trunk Configuration)] ウィンドウ

H.323 ゲートウェイ、ゲートキーパー制御または非ゲートキーパー制御の H.323/H.245/H.225 トランク、SIP トランクの [SRTP Allowed] チェックボックスを設定するには、次の手順を実行します。

手順

Step 1 Unified Communications Managerの説明に従って、ゲートウェイまたはトランクを検索します。

Step 2 ゲートウェイまたはトランクの設定ウィンドウを開いた後、[SRTP を許可する（SRTP Allowed）] チェックボックスをオンにします。

注意 SIP トランクの **[SRTP を許可する（SRTP Allowed）]** チェックボックスをオンにする場合は、キーや他のセキュリティ関連の情報がネゴシエーション中に公開されないように TLS 暗号化プロファイルの使用を推奨します。非セキュア プロファイルを使用すると、SRTP は機能しますが、キーはシグナリングおよびトレースで公開されます。この場合、Unified Communications Managerとトランクの接続先間でネットワークのセキュリティを確保する必要があります。

Step 3 [保存（Save）] をクリックします。

Step 4 デバイスをリセットするには、[Reset] をクリックします。

Step 5 IPSec が H323 に対して正しく設定されていることを確認します。(SIP の場合は、TLS が正しく設定されていることを確認してください)。

関連トピック

ゲートウェイとトランクの暗号化に関する詳細情報の入手先, on page 8

ゲートウェイとトランクの暗号化に関する詳細情報の入手先

- 認証、整合性、および許可
- 暗号化

関連トピック

認証、整合性、および許可
暗号化
Cisco IOS MGCP ゲートウェイの暗号化, on page 1
H.323 ゲートウェイおよび h.323/h.323/.h トランク暗号化 (h.323), on page 2
SIP トランクの暗号化, on page 4
セキュアゲートウェイとトランクのセットアップ, on page 5
ネットワーク インフラストラクチャ内の IPSec 設定, on page 6
Unified Communications Manager とゲートウェイまたはトランク間の IPsec の設定, on page 7