IPSec の設定

IPsec の概要

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。IPsec をネットワーク インフラストラクチャで設定し、Unified Communications Manager とデバイスとの間では設定しない場合は、IPsec の設定前に、次のことを検討してください。

- IPsec は、Unified Communications Manager 自体ではなく、インフラストラクチャでプロビジョニングすることをお勧めします。
- 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 Cisco IOS 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。

Caution 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の間で IPsec セットアップを構成および管理するには

この章で説明する Unified Communications Manager とゲートウェイまたはトランク間での IPsec の設定については、Cisco Unified Communications Manager アドミニストレーション ガイドを参照してください。