CHAPTER 13

Cisco Unified Communications プロキシ機能に関する情報

この章では、Cisco Unified Communications プロキシ機能向けに適応型セキュリティ アプライアンスを設定する方法について説明します。

この章の内容は、次のとおりです。

Cisco Unified Communications での適応型セキュリティ アプライアンスに関する情報

この項では、Cisco ASA 5500 シリーズ アプライアンスでの Cisco UC プロキシ機能について説明します。プロキシの目的は、クライアントとサーバ間の接続を終端し、再発信することです。プロキシは、トラフィック インスペクション、プロトコルとの適合性、ポリシー制御など幅広いセキュリティ機能を提供し、内部ネットワークのセキュリティを保証します。プロキシの機能として広く普及しているのが、暗号化された接続を終端して、接続の機密性を維持しながらセキュリティ ポリシーを適用する機能です。Cisco ASA 5500 シリーズ アプライアンスは、統合された通信構成にプロキシの機能を提供する戦略的なプラットフォームです。

Cisco UC Proxy には、次のソリューションが含まれます。

電話プロキシ：シスコ暗号化エンドポイントのセキュアなリモート アクセスと Cisco SoftPhone の VLAN トラバーサル

電話プロキシ機能は、セキュアなリモート アクセスのために Cisco Secure Real-time Transport Protocol（SRTP）および Transport Layer Security（TLS）暗号化エンドポイントの終端をイネーブルにします。電話プロキシを使用すると、大規模な VPN リモート アクセス ハードウェア構成を使用することなく、セキュアな電話を大規模に展開できます。エンドユーザのインフラストラクチャは、VPN トンネルまたはハードウェアを使用しない、単なる IP エンドポイントに制限されます。

Cisco 適応型セキュリティ アプライアンスの電話プロキシは、Cisco Unified Phone Proxy の代わりになる製品です。また、電話プロキシを、ソフトフォン アプリケーションの音声およびデータ VLAN トラバーサルに対して展開できます。Cisco IP Communicator（CIPC）トラフィック（メディアとシグナリングの両方）は、ASA を通じてプロキシで処理できるため、コールは音声 VLAN とデータ VLAN 間を安全に通過できます。

TLS プロキシと電話プロキシの違いについては、次の URL で Unified Communications に関するコンテンツ（ホワイト ペーパーの『TLS Proxy vs Phone Proxy』など）を参照してください。ホワイト ペーパーもあります。

http://www.cisco.com/go/secureuc

TLS プロキシ：Cisco Unified Communications 暗号化シグナリングの復号化と検査

エンドツーエンド暗号化では、ネットワーク セキュリティ アプライアンスがメディアやシグナリング トラフィックに対して「受信停止」になることがよくあります。これにより、アクセス コントロールや脅威回避セキュリティの機能が低下する場合があります。このように可視性が失われると、ファイアウォール機能と暗号化された音声間の相互運用性が失われ、企業では両方の主要なセキュリティ要件に対応できない状態が続く可能性があります。

ASA は、シスコ暗号化エンドポイントから Cisco Unified Communications Manager（Cisco UCM）までの暗号化されたシグナリングを代行受信して復号化し、必要な脅威回避とアクセス コントロールを適用します。また、Cisco UCM サーバへのトラフィックを再暗号化して機密性を保証することもできます。

通常、ASA の TLS プロキシ機能は、構内の統合された通信ネットワークに展開されます。このソリューションは、エンドツーエンド暗号化とファイアウォールを利用して Unified Communications Manager サーバを保護する構成に最も適しています。

モビリティ プロキシ：Cisco Unified Mobility Advantage サーバと Cisco Unified Mobile Communicator クライアント間のセキュアな接続

Cisco Unified Mobility ソリューションには、企業向け通信アプリケーションとサービスを携帯電話に拡張する、モバイル ハンドセット用の使いやすいソフトウェア アプリケーションである Cisco Unified Mobile Communicator（Cisco UMC）と Cisco Unified Mobility Advantage（Cisco UMA）サーバが含まれています。Cisco Unified Mobility ソリューションは通信のエクスペリエンスを効率化し、単一番号リーチおよびモバイル エンドポイントの Unified Communications インフラストラクチャへの統合を実現します。

セキュリティ アプライアンスはプロキシとして機能し、Cisco UMC と Cisco UMA 間の TLS シグナリングを終端し、再発信します。プロキシ セキュリティ機能の一部として、Cisco UMC と Cisco UMA 間のプロトコルである Cisco UMA Mobile Multiplexing Protocol（MMP; モバイル多重化プロトコル）に対するインスペクションがイネーブルになります。

プレゼンス フェデレーション プロキシ：Cisco Unified Presence サーバとシスコまたは Microsoft 社のプレゼンス サーバ間のセキュアな接続

Cisco Unified Presence ソリューションは、ユーザの可用性とステータスに関する情報（ユーザが特定の時間に IP 電話などの通信デバイスを使用しているかどうかなど）を収集します。また、Web コラボレーションやビデオ会議がイネーブルになっているかどうかなど、通信機能に関する情報も収集します。Cisco Unified Presence でキャプチャされたユーザ情報を使用すると、Cisco Unified Personal Communicator や Cisco UCM などのアプリケーションで、ユーザは最も効率のよい協調的な通信方法を確認して同僚との接続を効率化できるので、生産性が向上します。

ASA をセキュア プレゼンス フェデレーション プロキシとして使用すると、企業は Cisco Unified Presence（Cisco UP）サーバをシスコまたは Microsoft 社の他のプレゼンス サーバに安全に接続し、企業間通信をイネーブルにできます。セキュリティ アプライアンスは、サーバ間の TLS 接続を終端し、サーバ間の SIP 通信に対するポリシーを検査および適用できます。

Cisco Intercompany Media Engine Proxy：異なる企業内の Cisco UCM サーバ間での IP 電話トラフィック用のセキュアな接続

統合された通信が多くの企業内で展開されるにつれ、企業間コールの両側で統合された通信が使用され、その間に Public Switched Network（PSTN）が存在するケースが一般的になりつつあります。すべての外部コールが回線を介して電話のプロバイダーに到達し、そこからすべての外部の宛先に配信されます。

Cisco Intercompany Media Engine は、ビジネス間にダイナミックで、暗号化された VoIP 接続を徐々に作成します。それにより、連携する企業の集合は、それらの間にセキュアな VoIP 相互接続を持つ 1 つの巨大なビジネスと見なすことが最終的にできるようになります。

企業内での Cisco Intercompany Media Engine 配置には、Cisco Intercompany Media Engine サーバ、コール エージェント（Cisco Unified Communications Manager）、および Cisco Intercompany Media Engine Proxy を稼働している ASA からなる 3 つのコンポーネントがあります。

ASA は、企業間のシグナリング接続を暗号化し、不正なコールを防ぐことにより、境界セキュリティを提供します。Cisco Intercompany Media Engine Proxy を稼働している ASA は、インターネット ファイアウォールとして配置することも、Cisco Intercompany Media Engine Proxy として DMZ（通常のインターネット トラフィックのパス外）に配置することもできます。

Cisco Unified Communications での TLS プロキシ アプリケーション

表 13-1 に、ASA で TLS プロキシを使用する Cisco Unified Communications アプリケーションを示します。

表 13-1　TLS プロキシ アプリケーションおよびセキュリティ アプライアンス

アプリケーション	TLS クライアント	TLS サーバ	クライアント認証	セキュリティ アプライアンス サーバの役割	セキュリティ アプライアンス クライアントの役割
電話プロキシおよび TLS プロキシ	IP 電話	Cisco UCM	Yes	自己署名したまたは内部 CA によるプロキシ証明書	ASA CA によって署名されたローカル ダイナミック証明書（電話プロキシ アプリケーションには証明書は不要な場合がある）
モビリティ プロキシ	Cisco UMC	Cisco UMA	No	Cisco UMA 秘密キーまたは証明書偽装の使用	任意のスタティックな設定済み証明書
プレゼンス フェデレーション プロキシ	Cisco UP または MS LCS/OCS	Cisco UP または MS LCS/OCS	Yes	自己署名したまたは内部 CA によるプロキシ証明書	Cisco UP 秘密キーまたは証明書偽装の使用

ASA は、さまざまな音声アプリケーションに対して TLS プロキシをサポートします。電話プロキシの場合、ASA で実行中の TLS プロキシには、次の主要な機能があります。

- ASA は、Cisco UCM クラスタがノンセキュア モードであっても、インターネットを介して電話プロキシに接続しているリモートの IP 電話を、強制的にセキュア モードにする。
- TLS プロキシは ASA に実装されて、IP 電話からの TLS シグナリングを代行受信する。
- TLS プロキシはパケットを復号化し、NAT リライトおよびプロトコルへの適合性を行うインスペクション エンジンにパケットを送信する。また、オプションでパケットを暗号化し、それらのパケットを Cisco UCM に送信するか、IP 電話が Cisco UCM でノンセキュア モードになるよう設定されている場合はクリア テキストでパケットを送信することもできます。
- ASA は、必要に応じてメディア ターミネータとして機能し、SRTP および Real-time Transport Protocol（RTP）メディア ストリーム間で変換を行う。
- TLS プロキシは、TLS クライアント、プロキシ（ASA）、および TLS サーバ間で信頼できる関係を確立することで動作する透過的なプロキシである。

Cisco Unified Mobility ソリューションでは、TLS クライアントは Cisco UMA クライアントになり、TLS サーバは Cisco UMA サーバになります。ASA は、Cisco UMA クライアントと Cisco UMA サーバの間にあります。（TLS プロキシとして実装された）Cisco Unified Mobility のモビリティ プロキシでは、クライアントとのハンドシェイク中にサーバ プロキシに対してインポートされた PKCS-12 証明書を使用できます。ハンドシェイク中、Cisco UMA クライアントは証明書（クライアント証明書ではない）を提示する必要はありません。

Cisco Unified Presence ソリューションでは、ASA は、Cisco UP サーバと外部サーバ間の TLS プロキシとして機能します。これにより、ASA は、TLS 接続を開始したサーバの代わりに TLS メッセージをプロキシ処理し、プロキシ処理した TLS メッセージをクライアントにルーティングします。ASA は、サーバとクライアントの証明書トラストポイントを保存し、これらの証明書を TLS セッションの確立時に提示します。

Cisco Unified Communications プロキシ機能のライセンス

ASA でサポートされる Cisco Unified Communications プロキシ機能には、次の Unified Communications Proxy ライセンスが必要です。

- 電話プロキシ
- 暗号化音声インスペクションの TLS プロキシ
- プレゼンス フェデレーション プロキシ
- Intercompany Media Engine Proxy

（注）　バージョン 8.2(2) 以降では、Mobility Advantage Proxy に Unified Communications Proxy ライセンスは必要ありません。

次の表に、電話プロキシ、暗号化音声インスペクションの TLS プロキシ、およびプレゼンス フェデレーション プロキシの Unified Communications Proxy ライセンスの詳細をプラットフォーム別に示します。

（注）　この機能は、ペイロード暗号化機能のないモデルでは使用できません。

モデル	ライセンス要件[1]
ASA 5505	基本ライセンスと Security Plus ライセンス：2 セッション。 *オプション ライセンス：24 セッション。*
ASA 5510	基本ライセンスと Security Plus ライセンス：2 セッション。 *オプション ライセンス：24、50、または 100 セッション。*
ASA 5520	基本ライセンス：2 セッション。 *オプション ライセンス：24、50、100、250、500、750、または 1000 セッション。*
ASA 5540	基本ライセンス：2 セッション。 *オプション ライセンス：24、50、100、250、500、750、1000、または 2000 セッション。*
ASA 5550	基本ライセンス：2 セッション。 *オプション ライセンス：24、50、100、250、500、750、1000、2000、または 3000 セッション。*
ASA 5580	基本ライセンス：2 セッション。 *オプション ライセンス：24、50、100、250、500、750、1000、2000、3000、5000、または 10,000 セッション。*[2]
ASA 5512-X	基本ライセンス：2 セッション。 *オプション ライセンス：24、50、100、250、または 500 セッション。*
ASA 5515-X	基本ライセンス：2 セッション。 *オプション ライセンス：24、50、100、250、または 500 セッション。*
ASA 5525-X	基本ライセンス：2 セッション。 *オプション ライセンス：24、50、100、250、500、750、または 1000 セッション。*
ASA 5545-X	基本ライセンス：2 セッション。 *オプション ライセンス：24、50、100、250、500、750、1000、または 2000 セッション。*
ASA 5555-X	基本ライセンス：2 セッション。 *オプション ライセンス：24、50、100、250、500、750、1000、2000、または 3000 セッション。*
ASA 5585-X（SSP-10）	基本ライセンス：2 セッション。 *オプション ライセンス：24、50、100、250、500、750、1000、2000、または 3000 セッション。*
ASA 5585-X（SSP-20、-40、または -60）	基本ライセンス：2 セッション。 *オプション ライセンス：24、50、100、250、500、750、1000、2000、3000、5000、または 10,000 セッション。*[2]
ASASM	基本ライセンス：2 セッション。 *オプション ライセンス：24、50、100、250、500、750、1000、2000、3000、5000、または 10,000 セッション。*[2]

1. 次のアプリケーションでは、接続時に TLS プロキシ セッションを使用します。これらのアプリケーションで使用される各 TLS プロキシ セッション（およびこれらのアプリケーションのみ）は UC ライセンスの制限に対してカウントされます。
   - 電話プロキシ
   - プレゼンス フェデレーション プロキシ
   - 暗号化音声インスペクション

   TLS プロキシ セッションを使用するその他のアプリケーション（ライセンスが不要な Mobility Advantage Proxy、個別の IME ライセンスが必要な IME など）では、UC 制限に対してカウントしません。

   UC アプリケーションによっては、1 つの接続に複数のセッションを使用する場合があります。たとえば、プライマリとバックアップの Cisco Unified Communications Manager を電話に設定した場合は、TLS プロキシ接続が 2 つあるため、UC Proxy セッションも 2 つ使用されます。

   tls-proxy maximum-sessions コマンドを使用して TLS プロキシの制限を独立して設定できます。モデルの制限を表示するには、**tls-proxy maximum-sessions ?** コマンドを入力します。デフォルトの TLS プロキシ制限よりも高い UC ライセンスを適用する場合、ASA では、その UC 制限に一致するように TLS プロキシの制限が自動的に設定されます。UC ライセンスの制限よりも TLS プロキシ制限が優先されます。TLS プロキシ制限を UC ライセンスよりも少なく設定すると、UC ライセンスですべてのセッションを使用できません。

   注：「K8」で終わるライセンス製品番号（たとえばユーザ数が 250 未満のライセンス）では、TLS プロキシ セッション数は 1000 までに制限されます。「K9」で終わるライセンス製品番号（たとえばユーザ数が 250 以上のライセンス）では、TLS プロキシの制限はコンフィギュレーションに依存し、モデルの制限が最大数になります。K8 と K9 は、エクスポートについてそのライセンスが制限されるかどうかを示します。K8 は制限されず、K9 は制限されます。

   注：（たとえば **clear configure all** コマンドを使用して）コンフィギュレーションをクリアすると、TLS プロキシ制限がモデルのデフォルトに設定されます。このデフォルトが UC ライセンスの制限よりも小さいと、tls-proxy maximum-sessions コマンドを使用したときに、再び制限を高めるようにエラー メッセージが表示されます。プライマリ装置でフェールオーバーを使用して、**write standby** コマンドを入力して強制的にコンフィギュレーションの同期を行うと、セカンダリ装置で **clear configure all** コマンドが自動的に生成され、セカンダリ装置に警告メッセージが表示されることがあります。コンフィギュレーションの同期によりプライマリ装置の TLS プロキシ制限の設定が復元されるため、この警告は無視できます。

   接続には、SRTP 暗号化セッションを使用する場合もあります。
   - K8 ライセンスでは、SRTP セッション数は 250 までに制限されます。
   - K9 ライセンスに制限はありません。

   （注） メディアの暗号化/復号化を必要とするコールだけが、SRTP 制限に対してカウントされます。コールに対してパススルーが設定されている場合は、両方のレッグが SRTP であっても、SRTP 制限に対してカウントされません。
2. 10,000 セッション UC ライセンスの場合、組み合わせたセッション数は合計 10,000 までですが、電話プロキシ セッションの最大数は 5000 です。

表 13-2 に、TLS セッションのデフォルト数と最大数の詳細をプラットフォーム別に示します。

表 13-2　セキュリティ アプライアンス上での TLS セッションのデフォルト数と最大数

セキュリティ アプライアンス プラットフォーム	TLS セッションのデフォルト数	TLS セッションの最大数
ASA 5505	10	80
ASA 5510	100	200
ASA 5520	300	1200
ASA 5540	1000	4500
ASA 5550	2000	4500
ASA 5580	4000	13,000

次の表に、Intercompany Media Engine Proxy の Unified Communications Proxy ライセンスの詳細をプラットフォーム別に示します。

（注）　この機能は、ペイロード暗号化機能のないモデルでは使用できません。

モデル	ライセンス要件
すべてのモデル	Intercompany Media Engine ライセンス Intercompany Media Engine（IME）ライセンスをイネーブルにすると、TLS プロキシ セッションを設定された TLS プロキシの制限まで使用できます。また、Unified Communications（UC; ユニファイド コミュニケーション）ライセンスがインストールされており、その制限数がデフォルトの TLS プロキシの制限数より多い場合、お使いのモデルに応じて、ASA が UC ライセンスの制限数にまでセッション数を加えた制限を設定します。**tls-proxy maximum-sessions** コマンドを使用して TLS プロキシの制限を手動で設定できます。モデルの制限を表示するには、**tls-proxy maximum-sessions ?** コマンドを入力します。UC ライセンスもインストールすると、UC で使用できる TLS プロキシ セッションは IME セッションでも使用可能になります。たとえば、設定された制限が 1000 TLS プロキシ セッションの場合、750 セッションの UC ライセンスを購入すると、最初の 250 IME セッションまでは、UC に使用可能なセッション数に影響を与えません。IME に 250 を超えるセッションが必要になると、プラットフォームの制限の残りの 750 セッションが UC と IME によって先着順に使用されます。 • 「K8」で終わるライセンス製品番号の場合、TLS プロキシ セッションは 1000 までに制限されます。 • 「K9」で終わるライセンス製品番号の場合、TLS プロキシ制限は、使用する設定とプラットフォーム モデルに依存します。 **（注）**　K8 と K9 は、エクスポートについてそのライセンスが制限されるかどうかを示します。K8 は制限されず、K9 は制限されます。 接続には、SRTP 暗号化セッションを使用する場合もあります。 • K8 ライセンスの場合、SRTP セッションは 250 までに制限されます。 • K9 ライセンスの場合、制限はありません。 **（注）**　メディアの暗号化/復号化を必要とするコールだけが、SRTP 制限に対してカウントされます。コールに対してパススルーが設定されている場合は、両方のレッグが SRTP であっても、SRTP 制限に対してカウントされません。

ライセンスの詳細については、一般的な操作のコンフィギュレーション ガイドの Chapter 5, “Managing Feature Licenses,” を参照してください。