

ユニファイド コミュニケーションにおける機密について考えるときは一般に、盗聴などの脅威をいかに防ぐかが問題になります。盗聴を許してしまえば、攻撃者が音声会話を傍受、聴取、録音することができてしまいます。ビジネス リスクという観点から考えると、機密性の欠如は、顧客のクレジットカード番号のような会社の機密情報の損失あるいは盗用につながります。その結果、業界のコンプライアンス規定に違反することになり、事態が公になって、世間の信用も失われるかもしれません。

盗聴は、従来の PBX 環境においても問題となっていました。仮に攻撃者が PBX ネットワーク内のノードのいずれかへのアクセスに成功すれば、会話を聞き、録音することも簡単にできてしまいます。PBX 環境の機密性を確保するには、デバイスや電話回線への物理的アクセスを制限するしかなく、あとはシステム自体の完全性に頼るしかありませんでした。

統合型の IP ベース ユニファイド コミュニケーション ソリューションにおいては、パケット ベースの盗聴ツールが脅威となります。攻撃者は、このツールを使って音声パケットのストリームを傍受し、リアルタイムで聞いて録音するか、パケットを組み立てて後で再生します。対策としては、PC からはアクセスできない独立した VLAN に電話機を配置するという方法があります。こうすれば、音声パケットへのアクセスは難しくなります。けれども、このような対策を取ったとしても確実な保証はありません。

ユニファイド コミュニケーション システムの機密性を確保するには、強力な認証と暗号化のメカニズムを採用する必要があります。たとえ音声会話が傍受されても暗号化の解除は不可能なので、従来の PBX に比べればコミュニケーションの機密性ははるかに高まります。



機密性のオプション

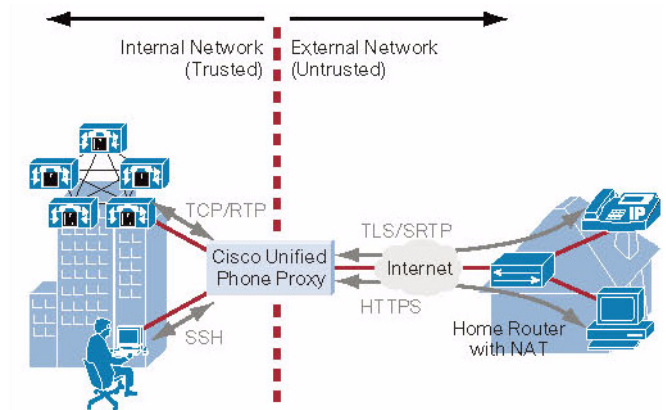
企業キャンパス環境における音声シグナリングとメディアの安全対策としては、ユニファイド コミュニケーションのエンドポイント自体に初めから組み込まれている認証と暗号化の機能を利用するのが一般的です。リモート リンクに対しては、ユニファイド コミュニケーションの認証と暗号化はいっそう重要です。リモート サイト側でアクセス コントロールができるようにするのは困難であるからです。また、認証と暗号化は、インターネット ベースのアクセス手法を使用する場合は必須です。ユニファイド コミュニケーション ネイティブの方式には、音声トラフィックにしか適用できないという欠点があります。つまり、電話機でしか利用できません。リモート サイトでは、さまざまなデバイスからのデータトラフィックも暗号化する必要があります。

このような理由から、リモート WAN やインターネット リンクの保護のためには IPsec (IP Security) VPN および SSL (Secure Sockets Layer) VPN ベースの認証と暗号化を使用するのが一般的です。この方法ならば、データとユニファイド コミュニケーションの両方を保護することができます。

Cisco Unified Phone Proxy

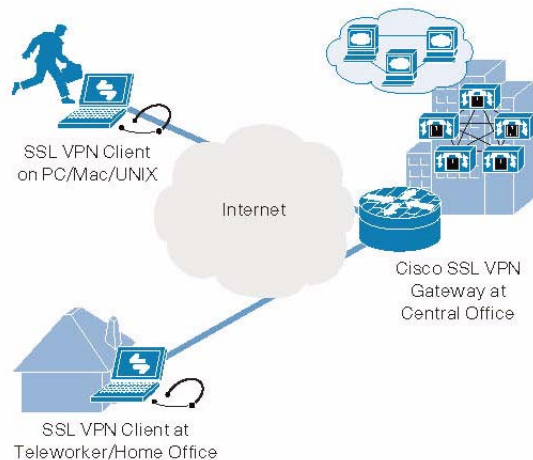
ユニファイド コミュニケーション ネイティブの機密性ソリューションの一つである Cisco Unified Phone Proxy は、認証と暗号化をユニファイド コミュニケーションのエンドポイント (リモート サイトで使われる暗号化機能付き Cisco IP Phone など) で実行するというものです。IP Phone でのシグナリングの暗号化には TLS (Transport Layer Security) が使用され、メディアの暗号化には SRTP (Secure Real-Time Transport Protocol) が使用されます。このように暗号化することで、共有またはパブリックのインフラストラクチャ (インターネットなど) を音声通話が安全に通過できます。リンクの相手側では、Cisco Unified Communications Manager に代わって Cisco Unified Phone Proxy プラットフォームが暗号化を解除します。

音声ユーザに対する Cisco Unified Phone Proxy のサービスは常時実行されますが、このサービスを利用できるのは IP Phone だけです。リモートの FAX 機、プリンタ、コンピュータや、小規模オフィスおよびホーム オフィス (テレワーカー) はサポートされません。



SSL VPN

SSL VPN を利用すればソフト フォンによる通信が暗号化されるので、モバイル ユーザは移動中も音声アプリケーションにアクセスできるようになります。SSL VPN クライアントソフトウェアの導入は容易です。エンド ユーザは、セキュアな Web サイトにアクセスしてクライアント ソフトウェアをインストールします。インストール後は、このクライアントによって音声通信やその他のデータアプリケーションの機密性が確保されるので、企業イントラネットへのアクセスを一本化して機密を維持することが可能になります。

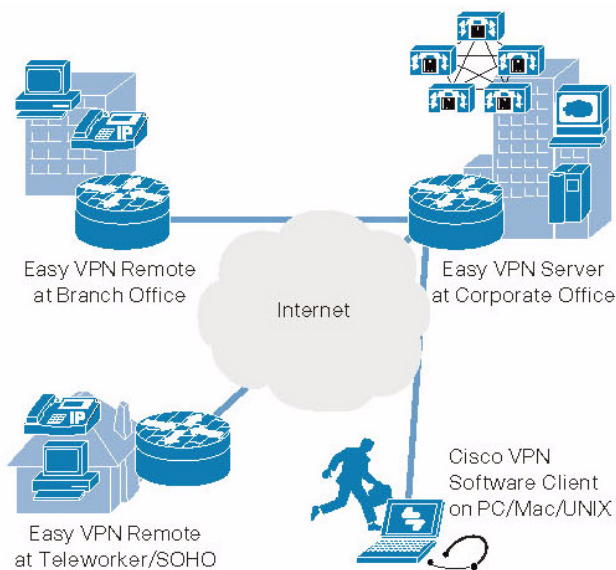


Cisco Easy VPN

数千名のモバイル ユーザやテレワーカーにも対応できるスケラビリティを持つ Cisco Easy VPN は、リモート アクセス展開に理想的なソリューションです。Cisco Easy VPN には、モバイル ユーザをサポートするための Cisco VPN Client ソフトウェア (Windows 版、Mac 版、UNIX 版) が含まれています。小規模オフィスやホーム オフィスでは、シスコのセキュリティルータまたはアプライアンスを利用すれば、電話機、FAX 機、プリンタ、PC に加えて、ワイヤレスクライアントなどのデバイスの通信を暗号化することができます。新しいセキュリティ ポリシーの適用が必要になったときも、本社の Cisco Easy VPN サーバからリモートのユーザやデバイ

スに自動的にポリシーをプッシュすることができるので、リモート デバイスに物理的にアクセスすることなく、常にポリシーを最新の状態に維持できます。

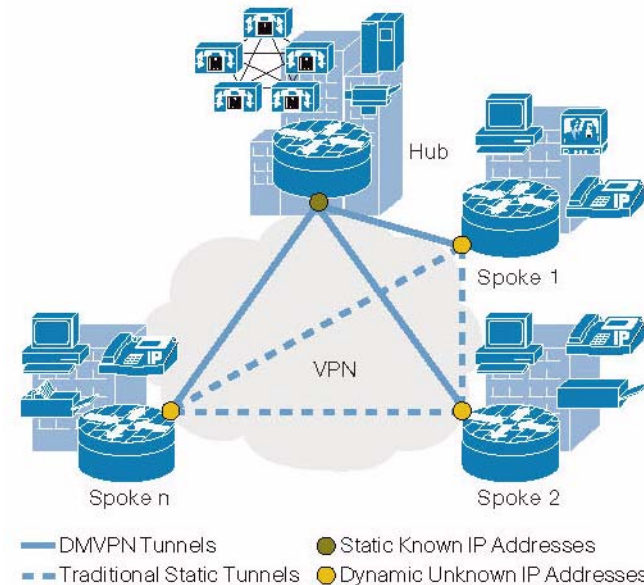
Cisco IOS[®] ソフトウェア ベースのルータには、Enhanced Easy VPN が組み込まれています。この機能は高度な QoS (Quality of Service) 統合を特長としており、トンネル固有の属性に加えてユーザごとの差別化が可能になります。このような機能を利用して、少数のユーザによる帯域幅独占を抑制すれば、重要度の低いデータよりもユニファイド コミュニケーショントラフィックを優先させることができます。



Cisco DMVPN

Cisco DMVPN (Dynamic Multipoint VPN) は、プライベート WAN またはインターネット リンクを介して接続された多数のリモート サイトの音声およびデータ通信の機密性を守るための、拡張性と管理性に優れたテクノロジーです。Cisco Easy VPN と同様に、Cisco DMVPN も IP Phone やソフト フォンをはじめとするさまざまなタイプのデバイスの暗号化をサポートしています。

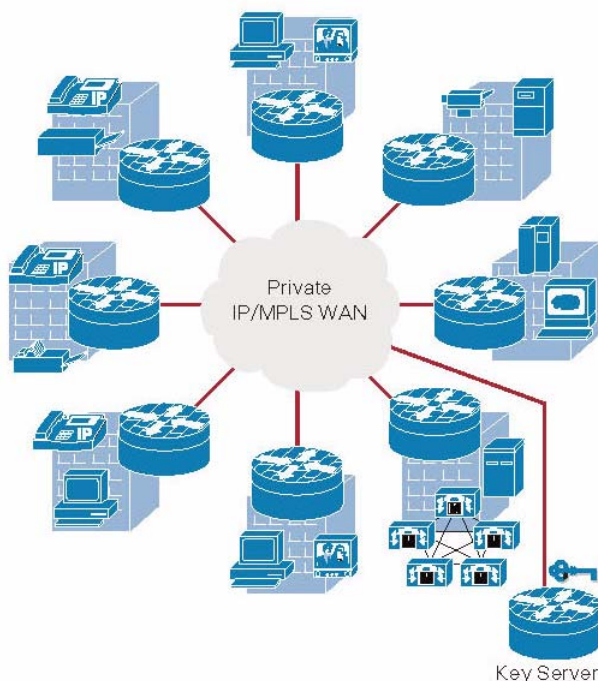
ほとんどのデータ アプリケーションのトラフィックは、一般にリモート サイト (スポーク) から中央のハブへと流れます。音声トラフィックの場合は、通話の両端がいずれもリモート サイトということもあるため、ホップと遅延が増えます。Cisco DMVPN を利用すれば、スポーク間の直接接続が可能です。シスコ セキュリティルータ間には、暗号化されたトンネルが必要に応じて自動的に構築されるので、管理のオーバーヘッドを最小に保ちながら暗号化音声通信のパフォーマンスを最適化することができます。このオンデマンドトンネルは、使用されないときは削除されるので、小型リモート ルータのリソースが節約されると共に、ソリューションの拡張が容易になります。Cisco IOS の QoS オプションを幅広く活用する Cisco DMVPN は、インターネットでリモート サイトを接続する大規模なユニファイド コミュニケーション展開に最適なソリューションです。



Cisco GET VPN

Cisco Group Encrypted Transport VPN (GET VPN) は、プライベート WAN または MPLS (Multiprotocol Label Switching) WAN インフラストラクチャを介してリモート サイトとの間で行われる音声通信およびデータ通信の機密性を守るテクノロジーです。Cisco GET VPN の暗号化にはトンネルは使用されないため、MPLS インフラストラクチャの上にポイントツーポイントの IPsec トンネルを構築する必要がなくなり、複雑さや拡張性の制限とも無縁です。

Cisco GET VPN では、MPLS インフラストラクチャ固有の QoS、ルーティング、およびマルチキャストのサービスが使用されるので、すでに MPLS で標準化されている環境へのセキュアなリモート音声アプリケーションの導入が可能になります。Cisco GET VPN によって暗号化がサポートされるデバイスは、IP Phone やソフト フォンなど多岐にわたります。



リモート展開のシナリオ

遠隔地の拠点に導入するユニファイド コミュニケーションサービスの機密性を守る方法は、導入先の規模によって異なります。

中～大規模のリモート サイトまたはブランチ

これに該当する拠点のセキュリティを確保するには、サイト間 VPN と呼ばれる方法を使用します。多くの場合は、動的ルーティング プロトコル アップデートを統合できることが必要になります。このシナリオで使用されるテクノロジーには、Cisco DMVPN、Cisco Easy VPN (スタティック ルーティングのみ)、Cisco GET VPN (プライベート WAN IP/MPLS のみ) などがありません。

小規模オフィスまたはホーム オフィス (テレワーカーなど)

ユーザやデバイスの数が少ない小規模な環境では一般に、動的ルーティング プロトコルは不要です。したがって、セキュリティ確保の選択肢が増えます。このシナリオで使用されるテクノロジーには、Cisco Easy VPN、Cisco DMVPN、Cisco Unified Phone Proxy などがありません。

モバイル ユーザ

モバイル ユーザには一般に、ハードウェア ベースの VPN ソリューションは不要です。モバイル ユーザのユニファイド コミュニケーションのセキュリティを確保する手段としては一般的に、音声とデータのトラフィックを統合する VPN クライアント ソフトウェアがあります。これと同時に、多数のエンドユーザ デバイスのセキュリティ ポリシーを動的かつ自動的に更新する手段が必要です。このシナリオで使用されるテクノロジーには、Cisco Easy VPN や SSL VPN などがありません。

リモート デバイスのサポートに関する要件

認証と暗号化に関するサポートが必要なデバイスが何種類も遠隔拠点に存在することも珍しくありません。これに該当するデバイスには、IP Phone、ソフト フォン (モバイル ユーザに一般的に使用される PC ベースのソフトウェア)、データ デ

バイス (FAX 機、プリンタ、PC、サーバなど) があります。複数の種類のデバイスの保護が可能か方法を選ぶことが必要です。



ユニファイド コミュニケーションの機密性を守る方法の要約

次の表は、リモート ユニファイド コミュニケーションの機密性を守るためのソリューションをまとめたものです。

リモート ユニファイド コミュニケーションの機密性	Phone Proxy	SSL VPN	Cisco Easy VPN	Cisco DMVPN	Cisco GET VPN
リモート ロケーション					
中規模～大規模のリモートサイトまたはブランチ オフィス	×	×	スタティックルーティングのみ	○	○
小規模または自宅オフィス (在宅勤務を含む)	電話のみ	ソフトフォンのみ	○	○	×
モバイル ユーザ	×	○	○	×	×
サポートするデバイス					
IP 電話機	○	×	○	○	○
ソフトフォン	認証のみ	○	○	○	○
データ デバイス (Fax、プリンタ、PC)	×	×	○	○	○

©2008 Cisco Systems, Inc. All rights reserved.
Cisco、Cisco Systems、および Cisco Systems ロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の一定の国における登録商標または商標です。
本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。
「パートナー」または「partner」という用語の使用は Cisco と他社との間のパートナーシップ関係を意味するものではありません。(0809R)
この資料に記載された仕様は予告なく変更する場合があります。