

セッションボーダーコントローラは、VoIP やユニファイドメッセージングアプリケーションのセキュリティを確保するソリューションとして販売されてきました。しかしながら、セッションボーダーコントローラは、本来はセキュリティゲートウェイとして設計されたものではなく、VoIP ネットワークに公的な IP リンクを安全に追加するために必要なセキュリティレベルを提供することはできません。このアプリケーションレビューでは、セッションボーダーコントローラの限界と代替案について説明します。

ボイスオーバーIP (VoIP) アプリケーション、それに関連するユニファイドメッセージングアプリケーションは、非常に複雑です。この複雑さは、提供するサービスのレンジが広い事とこれらのアプリケーションが直面しているセキュリティに対する脅威の両面から明白です。セッション開始プロトコル (SIP) は、VoIP をはじめビデオやインスタントメッセージ、他のユニファイドメッセージングアプリケーション等幅広く利用されています。このアプリケーションノートでは、このような複雑な状況下の中で、特に、ネットワーク境界でセキュリティが必要とされている場合に、何故セッションボーダーコントローラ (SBC) が SIP ネットワークにおけるセキュリティソリューションとして最適なものではないかを説明します。

セッションボーダーコントローラ

セッションボーダーコントローラ (SBC) という用語は、広範囲の製品タイプに適用されました。元々 SBC は、異なるキャリア間における接続を提供する事を目的に設計されました。この役割において SBC は、たとえ異なる組織が運営・管理しているネットワーク環境下においても、両者間のネットワークをうまく接続する、いわゆる VoIP トラフィックリレーとして機能します。

2つのキャリアネットワークを接続するタスクはほとんどの企業が直面している問題とは、根本的に異なっています。VoIP 及びユニファイドメッセージングサービスを、企業ユーザだけでなく、個人宅で仕事をしている人や、移動しながら働く人達にも SIP トランクの接続を可能にし、安心して利用してもらうためのセキュリティを提供します。これらのサービスは、公の IP ネットワークへの接続が要求され、キャリアのバックボーンのような整然とした環境ではありません。

ほとんどの SBC は、SIP のようなプロトコルが提供している付加価値アプリケーション間での相互接続を提供するのではなく、VoIP という非常に限られたサポートに焦点を合わせています。SIP は、プレゼンス (応答可否) やインスタントメッセージなどの新しいアプリケーションを提供し、データ網でより厳密な統合ができるように設計されました。SBC が VoIP に焦点を合わせるという事実は、これらのより新しいアプリケーションに対しては、何も保証されない事を意味します。

SBC は、SIP ベースの VoIP 及びユニファイドメッセージをセキュアなものにしたいと考えている企業やサービスプロバイダにとって、ほとんど価値が無くなる可能性がある事を意味します。これらの特徴は複数の VoIP プロトコル、プロトコル変換、およびコーデック変換 (コード変換) のサポートを含んでいます。これらの特徴を実現するために、非常に大きく高価なハードウェアを必要とし、\$25K から \$100K の SBC 導入費用がかかります。

ユニファイドメッセージングセキュリティ

企業やサービスプロバイダが直面している課題は、VoIP と他の SIP ベースのアプリケーションにとっての周辺のセキュリティを提供する事です。そしてこれらはユーザのロケーションにかかわらず、すべてのユーザに対し一貫したサービスを提供する必要があります。したがって、ユーザがウェブとメールへの簡単なアクセスを想定するように、彼らは VoIP とユニファイドメッセージングが同じレベルのサービスである事を期待します。ユニファイドメッセージングの主要な利益の 1 つは、ビジネスコミュニケーションの全てのフォームを統合できる能力ですが、これらは効果的なセキュリティコントロール無しには実現できません。

ユニファイドメッセージングアプリケーションは、数多くの脅威にさらされています。

1. WEB や e-mail、他の標準 IP アプリケーションと同様の IP ネットワークレベルの脅威
2. DOS 攻撃や、コールディスラプションアタックを含むアプリケーション及びプロトコルレベルの脅威。これらのアタックは、サービスの品質に重大な影響を与え、最悪サービス停止の引き金になる可能性があります
3. 権限の無いコールモニタリング（盗聴）や、コールフルディング、迷惑電話を含むコンテンツレベルの脅威

料金詐欺などの他の脅威は、アプリケーションとコンテンツの両方のグループになります。SBC はこれらの脅威全てに対する防御手段を持っていません。提供されるセキュリティレベルは、製品に依存しますが、カテゴリとして、SBC は IP ネットワークレベルの脅威に対して、標準ファイアウォールほど有効ではありません。そして、アプリケーションレベルに対しては、部分的な防御しかできず、コンテンツレベルの脅威に対しては、ほとんど防御できません。

リスク

SBC はキャリアネットワークのような比較的制御された環境で動作する事を前提に設計されました。これらは、公の IP ネットワークにはそれほど良く合っていません。ほとんどの SBC は、権限の無いコールモニタリング（盗聴）の防御や、DoS アタックのようなアプリケーションレベルのブロック、他のメッセージングアプリケーションに必要なコンテンツ制御やポリシーの提供機能を持っていません。これらの脅威に対して完全に保護されたというわけではないシステムは、重大な問題を引き起こす場合があります、最悪の場合には、サービスが停止する事になりかねません。

UM Labs

UM Labs が開発した SIP セキュリティゲートウェイは、SIP ベースの VoIP 及びユニファイドメッセージングアプリケーションの包括的なセキュリティを提供するために設計された製品です。UM Labs ゲートウェイの中の、エントリーレベルの製品は、ローミングユーザや、ホームワーカーを対象としており、SIP トランクスにセキュアに接続する事を保証する製品です。そして、より大きな企業やサービスプロバイダ用にはその規模に応じた製品を提供します。それぞれの製品は、VoIP およびユニファイドメッセージングアプリケーションに直面している脅威に対し完全に防御するように設計されています。これは、UM Labs ゲートウェイが SBC より効果的なセキュリティ解決策を持っている事を意味しています。そして、同時にダイレクトセキュリティ機能を持っていないシステムと比較し、数多くの複雑な設定を省略する事ができます。これは、UM Labs が SIP のベースの VoIP とユニファイドメッセージングのセキュリティに対し、どんな SBC よりもはるかに費用効率がよい解決策を提供できる事を意味します。

| 機能 | UM Labs | SBC |
|---------------------------------------|---------|---------|
| 盗聴対策 | ◎ | × |
| 妨害電話、冗雑電話対策 | ◎ | × |
| コールディスラプションアタック対策 | ◎ | × |
| SIP レベル DoS アタック対策 | ◎ | × |
| 他のアプリケーション動作を妨害しない VoIP 動作 | ◎ | ○ |
| 他の SIP ベースアプリケーションの為にポリシーとコンテンツコントロール | ◎ | × |
| Far-End NAT トラバース | ◎ | ◎ |
| ローカル NAT | ◎ | ◎ |
| IP レベルセキュリティ | ◎ | ○ |
| 初期導入費用（概算） | \$2K | \$25K + |

より詳細な情報は、WEB サイトをご覧ください。 <http://www.um-labs.com>