RC-2100
トランク及びリモート接続における SIP セキュリティコントローラ

UM Labs が提供する SIP セキュリティコントローラは、VoIP や他のユニファイドメッセージングアプリケーションにおける強固なセキュリティ対策を簡単かつ低価格にて実現します。各製品は、VoIP やユニファイドメッセージにおける全てのレンジのセキュリティ脅威を排除するために、アプリケーションや、特定のコントローラと共に強固なファイアーウォールセキュリティと結合します。

製品の特徴

セキュリティプロテクション(機密保持)、リモートユーザと SIP トランクにおける安全な環境提供

防御:

対 VoIP/SIP セキュリティの脅威
- SIP /RTP DoS アタック
- スプーフィング
- Media 異常 Anomalies
- 不正 SIP messages
- ワイヤータッピング

対 IP レベルセキュリティの脅威
- ステートフル IP ファイアーウォール
- RTP ストリームにおけるダイナミックピンホーリング

コントロール:

オペレーティングシステム
- ファイアーウォールグレードセキュリティ
- VoIP サービスにおける最適化

サービス:

NAT トラバーサル
- ローカル NAT
- Far-End NAT トラバーサル (STUN を使用しないで実現)

機密性
- SIP-over-TLS, 256 ビット AES 暗号化方式
- SDES 鍵交換における SRTP サポート
- ZRTP 鍵交換における SRTP サポート（追加ライセンスが必要)
- SRTP ゲートウェイ(終端機能含)
- SRTP パススルー
- 全ての SIP 要求に対する HTTP ダイジェスト認証

チャレンジ

ユニファイドメッセージングは、e-mail やインスタントメッセージ、VoIP やビデオ会議のように非常に広範囲にわたるアプリケーションを統括しなければなりません。これらのアプリにとって重要なことは、相手ユーザに今応答できるかどうかのシグナルを出せる事と、コールやメッセージを最も効率よくルーティングする方法を確立することです。
これらのアプリケーションは、全て IP ネットワーク上で動作するものですが、それらのセキュリティ要件は、全く異なっています。
インスタントメッセージのセキュリティ要件は、e-mail のようなコンテンツフィルタリングや、スパムに対する防御となる一方、VoIP やビデオ会議のためのセキュリティコントロールは、リアルタイムにアプリケーション種別を認識し、コールフルッディングに対する防御や、認証されていないコールをモニタリングする必要があります。
VoIP とユニファイドメッセージアプリケーションのセキュリティ要件は、一般の目的に使用されているファイアーウォールより複雑です。汎用ファイアーウォールでは、VoIP やユニファイドメッセージに関わる全ての脅威を防ぐ事ができません。
VoIP とユニファイドメッセージアプリケーションにとっての有効なセキュリティは、アプリケーションによる強固なファイアーウォールセキュリティ制御と満足させる特別なセキュリティの結合です。UM Labs のセキュリティゲートウェイは、ネットワークの全てのタイプにおける VoIP 及びユニファイドメッセージに関するセキュリティを費用効率よく配置できるよう設計されています。

ビジネス要件

VoIP と UM アプリケーションの主要な恩恵の１つは、Voice Telephony と Video 会議を他のメッセージングアプリケーションと統合して、組織の全ての部分にその統合サービスを広げる事ができる点です。VoIP サービスはあらゆる SIP アドレスに対し直接コールおよびトランク接続コールができるため、標準の電話サービスを置き換える事が可能です。
この事による利点を最大限に引き出すためには、２つの要件が必要です。第一に、音声とデータネットワークの完全な統合。第二に、既存のセキュリティに対し VoIP トラフィックを通すように変更し、SIP トランクへの接続を支店にいるユーザやリモートユーザに対して許可するようにしなければなりません。しかしながら、現在の多くの VoIP システムでは、この設計と実装を両立できない状況で、音声とデータを別々のネットワークに実装する、もしくはファイアーウォールが VoIP トラフィックを遮断してしまうため、VoIP アプリが正常に動作しないというのが現状です。

The Solution

UM Labs の RC-2100 は、VoIP やビデオ会議、SIP ベースのインスタントメッセージやプレゼンスベースのアプリケーション等の遠隔 SIP 接続に必要なセキュリティ管理のフルセット機能を持った、非常に費用対効果の高い、SIP セキュリティゲートウェイとして設計されました。RC-2100 は、音声とデータを安全に統合するためのセキュリティを提供します。

©UM-Labs Ltd, 2008

RC-2100
トランク及びリモート接続における SIP セキュリティコントローラ

管理方法

- セキュアかつ直感的な GUI
- リモート Syslog
- 効率的なソフトウェアアップグレード方式を採用

仕様

- 10/100 Fast Ethernet ポート (RJ-45)：３ポート
- RS-232 コンソールポート:1 ポート
- 動作パーツ無し：ファンレス
- エコ製品
- ハードウェア監視装置
- ハードウェア乱数ソース

準拠規格

ハードウェア
- RoHS
- WEE

ソフトウェア
- RFC 3261
- RFC 3711
- RFC 4568
- RFC 2617

ライセンス及び出荷時期

- 同時 20 接続 (登録リモートユーザもしくは、SIP トランクライン)
- ライセンス拡張可能
- 2008 年４月出荷開始

連絡先

UM Labs Ltd
Heathrow Blvd 4
280 Bath Road
West Drayton
UB7 0DQ
UK

Email: info@um-labs.com
VoIP: sip:info@um-labs.com

Revision 1.2 February 2008

RC-2100 は、SIP アプリケーションや、コンテンツコントロールを行う上で必要なネットワークセキュリティ機能（ファイアーウォール機能）と、暗号化されたコールセットアップやメディアトラフィックを通過させるゲートウェイとしての機能を提供します。これらの管理は、シグナリング(SIP)とメディア(RTP)の両方において、認証サービスと共に提供されるべきで、すべてのリモート接続のための完全なプライバシーと機密性を確実にしなければなりません。

RC-2100 は、どのような環境下においても設置可能な、低騒音、低消費電力を実現したハードウェアです。このシステムは、継続操作を確実にするためのハードウェア監視機能および、シグナリングとメディア暗号化の両方における高品質な暗号化キーを発生させるためのハードウェア乱数機能を含んでいます。

特長

- リモートユーザ及び SIP トランクにおける包括的なセキュリティを低価格にて実現
- SIP アプリケーションのセキュリティ、管理、暗号化、認証機能を完全な IP ファイアーウォール機能とともに提供できるため、設定を簡単にかつ設置までの時間を極力短くする事が可能です。
- VoIP アプリケーションレベルのゲートウェイ及びファイアーウォールに特化して動作しているため、すでに設定しているファイアーウォールをあるアプリケーションの為に変更するといった事が必要ありません。
- 標準規格に完全適合していますので、あらゆる VoIP フォンや PBX との相互運用性を持っています。
- ローカル NAT 及びファーエンド NAT トラバーサルをサポートしていますので、リモートユーザが、サードパーティのファイアーウォールや、他の NAT ゲートウェイを経由して接続している場合においても、特別なプロトコルサポートを必要とする事なくサービスを提供できます。

設置

RC-2100 の強固な IP ファイアーウォールセキュリティ層は、汎用のファイアーウォール製品と並べて設置する事が可能です。この構成は、既存のファイアーウォールセキュリティレベルを下げずに、VoIP トラフィックに専念したセキュリティを確保し、コール品質を保護する事が可能なため、非常に好都合です。

RC-2100 は、既存のファイアーウォールの DMZ に接続する事も可能です。

©UM-Labs Ltd, 2008