SSL および TLS のコンテンツ セキュリティ アプライアンス モデル データ暗号化

目次

概要

このドキュメントでは、セキュア ソケット レイヤ（SSL）および Transport Layer Security（TLS）の暗号化方式の定義を示し、使用方法を説明します。

SSL および TLS の概要

SSL および TLS 暗号化方式は、ネットワークのストリームまたは転送セッションでデータ暗号化のために最もよく使用されている 2 つの方式です。

SSL 暗号化方式は、インターネットを経由するセキュア HTTP 通信のために当初は Netscape によって開発され、1990 年代に利用が広まりました。 SSL バージョン 2.0 が最初に一般公開され、間もなく SSL バージョン 3.0 が続いてリリースされました。バージョン 3.0 では旧バージョンの重大なセキュリティ欠陥が解決されています。

TLS バージョン 1.0 は SSL バージョン 3.0 の後継プロトコルです。 セキュリティ アルゴリズム、アラート、および仕様拡張を提供しました。 ささいな変更があっても、2 つのプロトコルで相互に互換性があることは画期的でした。 その後、TLS 暗号化方式は、Advanced Encryption Standard（AES）など、より安全なキー生成アルゴリズムの暗号スイートで改善されました。 現時点で最新のバージョンは TLS バージョン 1.2 です。

> **注:** AsyncOS 8.5.6 時点では、TLS v1 のみサポートされています。 TLS v1.1、1.2 はサポートされていません。 CLI で **sslconfig** を確認し、**GUI**、**INBOUND**、または **OUTBOUND** を選択して、利用可能な暗号メソッドを表示してください。

SSL および TLS の利用方法

現在、Simple Mail Transfer Protocol（SMTP）および HTTPS トランザクションのようなセキュアな転送を利用するほとんどのクライアント/サーバ プログラムは、SSL バージョン 3.0 や TLS バージョン 1.x に基づいています。 多くのアプリケーションには SSL や TLS などのセキュアな転送のサポートが組み込まれていますが、あらゆるプログラムがセキュア トンネルに引き継ぐことができます。 このため、Session Initiation Protocol（SIP）や VPN などのセキュアな電話機の通信など、多くの新しいアプリケーションが発展を遂げました。これらは、UDP 型 IP パケット（dTLS）から引き継がれた、改良された TLS 暗号化方式を使用しています。

SSL と TLS という用語は同じ意味で使用されることがありますが、プロトコルは同一ではありません。 主な違いは、クライアントとサーバによってネゴシエートされる暗号スイート（暗号化タ

イプ) に関連した問題解決にあり、それらの暗号の選択メソッドも異なっています。 基本的に、TLS は、開発がオープンで堅牢であり、IETF で標準化されているため、ネットワーク通信の暗号化手段として好まれています。

注: TLS バージョン 1.2 の仕様の詳細については、RFC 5246 を、SSL バージョン 3.0 については SSL インターネットドラフトを参照してください。