暗号設定およびQoS へのレファレンスガイド

内容

概要

VPN がデータ、音声およびビデオ トラフィックを含むようになると、ネットワークではトラフィック タイプに応じて異なる処理を行う必要があります。Quality of service（QoS）と帯域幅を管理する機能によって、VPN では、音声やビデオなどの時間依存型アプリケーション向けの高度な伝送品質を提供できるようになりました。各パケットには、そのペイロードの優先順位および時間の影響の受けやすさを識別するためのタグが付けられ、トラフィックは、その配信優先順位に基づいてソートされ、ルーティングされます。Cisco VPN ソリューションでは、さまざまな QoS 機能をサポートします。

この文書は、同じネットワークやルータ群に対して Cisco IOS® の暗号化と QoS の機能を設定するユーザ向けに、単一のリファレンスとなることを目的として作成されています。この文書によって、IP Security（IPSec）や generic routing encapsulation（GRE; 総称ルーティングカプセル化）トンネルが設定されている場面での、入力および出力 QoS ポリシーの基本的な設定が理解できるようになります。また、この文書では、設定タスクについても説明します。さらに、シスコ ルータを使用した拡張 IP サービスの最適なパフォーマンスと正常な実装を保証するために、制限と既知の問題に関する情報を提供します。

前提条件

要件

このドキュメントの読者は次のトピックについての専門知識を有している必要があります。

- IPSec テクノロジー

IPSec に関するより包括的なマニュアルについては、『IP Security (IPSec) 暗号化の概要』を参照してください。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

表記法

ドキュメント表記の詳細は、「シスコ テクニカル ティップスの表記法」を参照してください。

IPSec プロトコル

IPSec プロトコルの詳細な説明はこの文書の範囲を越えています。そのため、ここではその概要について説明します。詳細については、「関連情報」を参照してください。