

實施加密和QoS的參考指南

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[慣例](#)

[IPSec通訊協定](#)

[AH和ESP](#)

[將GRE通道用於IPSec](#)

[分類資料包](#)

[示例配置](#)

[輸入策略](#)

[輸出策略](#)

[限制和相關問題](#)

[QoS和反重新執行保護](#)

[NBAR](#)

[雙重記帳](#)

[軟體加密和快速交換/CEF](#)

[舊版優先順序隊列和QoS預分類](#)

[硬體加密和QoS](#)

[相關資訊](#)

簡介

隨著VPN發展到包括資料、語音和影片流量，網路中不同型別的流量需要以不同的方式處理。服務品質(QoS)和頻寬管理功能使VPN能夠為語音和影片等對時間敏感的應用程式提供高傳輸品質。每個資料包都經過標籤，以標識其負載的優先順序和時間敏感性，並根據其傳輸優先順序對流量進行分類和路由。Cisco VPN解決方案支援各種QoS功能。

本文檔旨在為在同一網路或一組路由器上配置Cisco IOS[®]加密和QoS功能的使用者提供一個參考。在存在IP安全(IPSec)和通用路由封裝(GRE)隧道時，您會看到輸入和輸出QoS策略的基本配置。本檔案幫助您瞭解組態任務。它還提供有關限制和已知問題的資訊，以確保使用Cisco路由器實現最佳效能並成功實施增強型IP服務。

必要條件

需求

本文檔的讀者應瞭解以下主題：

- IPSec技術

有關IPSec的更詳盡文檔，請參閱[IP安全\(IPSec\)加密簡介](#)。

[採用元件](#)

本文件所述內容不限於特定軟體和硬體版本。

[慣例](#)

如需文件慣例的詳細資訊，請參閱[思科技術提示慣例](#)。

[IPSec通訊協定](#)

有關IPSec協定的詳細討論不在本檔案的範圍之內。但是，本節中提供了概述。請參閱[相關資訊](#)