

实施Crypto 和 QoS 的参考指南

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[IPsec 协议](#)

[AH和ESP](#)

[以IPSec使用GRE隧道](#)

[分类数据包](#)

[配置示例](#)

[输入策略](#)

[输出策略](#)

[限制与相关问题](#)

[QoS 和反重放保护](#)

[NBAR](#)

[双重记帐](#)

[软件加密和快速交换/CEF](#)

[传统优先级排队和 QoS 预先分类](#)

[硬件加密和 QoS](#)

[相关信息](#)

简介

VPN成长为请包括数据、语音和视频流量，不同类型的流量需要不同处理在网络。服务质量(QoS)和带宽管理功能允许VPN提供时间敏感的应用程序的传输质量例如语音和视频。每数据包被标记识别其有效负载优先级和时间区分，并且流量根据其交付优先级排序并且路由。Cisco VPN解决方案支持各种各样的QoS功能。

本文设计起单个参考作用对于配置Cisco IOS加密和QoS功能在同一网络或一组路由器的用户。您在IP安全面前将看到输入和输出QoS策略和通用路由封装(GRE)通道基本配置。本文帮助您了解配置任务。使用Cisco路由器，它在限制和已知问题也提供信息，保证增强的IP RTP优先策略服务最佳性能和成功实施。

先决条件

要求

本文档的读者应掌握以下这些主题的相关知识：

- IPSec技术

对于在IPSec的更多详尽的文档，参考[IP安全](#)。

[使用的组件](#)

本文档不限于特定的软件和硬件版本。

[规则](#)

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

[IPsec 协议](#)

IPSec协议的详细讨论是超出本文的范围之外。然而，概述在此部分提供。请参阅[相关信息](#)