Guide de référence de l'implémentation de Crypto et QoS

Contenu

Introduction

Comme les VPN deviennent incluez les données, Voix, et le trafic visuel, les différents types de trafic doit être traité différemment dans le réseau. Le Qualité de service (QoS) et les fonctions de gestion de la bande passante permettent à un VPN pour fournir la qualité de transmission élevée pour des applications sensibles au temps telles que la Voix et le vidéo. Chaque paquet est étiqueté pour identifier la sensibilité prioritaire et de temps de sa charge utile, et le trafic est trié et conduit basé sur sa priorité de la livraison. Les solutions VPN de Cisco prennent en charge un large éventail de caractéristiques de QoS.

Ce document est conçu pour servir de seule référence aux utilisateurs qui configurent le cryptage de Cisco IOS® et les caractéristiques de QoS sur le même réseau ou ensemble de routeurs. Vous verrez des configurations de base des stratégies QoS d'entrée et sortie en présence de la sécurité IP (IPSec) et des tunnels d'Encapsulation de routage générique (GRE). Ce document vous aide à comprendre les tâches de configuration. Il fournit également des informations sur des restrictions et des problèmes connus, pour assurer des performances optimales et l'implémentation réussie des Services IP améliorés utilisant des Routeurs de Cisco.

Conditions préalables

Conditions requises

Les lecteurs de ce document devraient avoir connaissance des sujets suivants :

- Technologie d'IPSec

Pour un document plus exhaustif sur IPSec, référez-vous à une introduction au cryptage de sécurité IP (IPSec).

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Conventions

Pour plus d'informations sur les conventions de documents, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Protocoles IPsecs

Une analyse détaillée des protocoles IPsecs est hors de portée de ce document. Cependant, un aperçu est fourni dans cette section. Voyez les informations relatives