

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurez](#)

[Diagramme du réseau](#)

[Configuration SW1](#)

[Configuration SW2](#)

[Vérifiez](#)

[Vérification par la sortie de NetFlow](#)

[Dépannez](#)

Introduction

Ce document décrit comment configurer et vérifier un Cisco TrustSec (CTS) avec le réflecteur de sortie.

Conditions préalables

Conditions requises

Cisco recommande que vous ayez la connaissance de base de la solution de Cisco TrustSec.

[Composants utilisés](#)

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Les Commutateurs de Catalyst 6500 avec l'engine 2T de superviseur sur l'IOS libèrent 15.0(01)SY
- Générateur du trafic d'IXIA

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

[Informations générales](#)

Le Cisco TrustSec est une architecture identité-activée d'accès au réseau qui aide des clients à activer la Collaboration sécurisée, à renforcer la Sécurité, et à adresser des conformités aux réglementations. Il fournit également une infrastructure d'application de stratégie basée par rôle extensible. Des paquets sont étiquetés ont basé sur l'adhésion à des associations de la source de

paquet au d'entrée du réseau. Des stratégies associées avec le groupe sont appliquées pendant que ces paquets traversent le réseau.

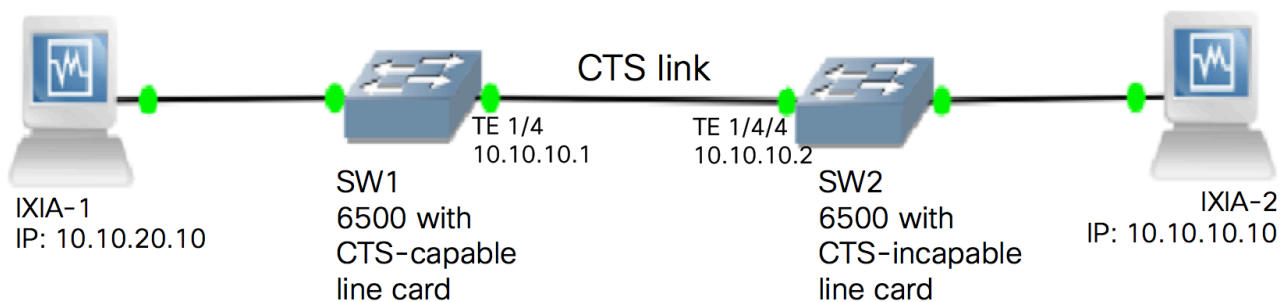
Les Commutateurs de gamme Catalyst 6500 avec l'engine 2T de superviseur et les linecards de gamme 6900 fournissent le matériel et le support logiciel complets pour mettre en application CTS. Afin de prendre en charge la fonctionnalité CTS, il y a les circuits intégrés spécifiques à l'application dédiés (ASIC) utilisés sur les nouveaux linecards de gamme 6900. Les linecards existants n'ont pas ces ASIC dédiés et donc, ne prenez en charge pas CTS.

Analyseur de port de commutateur Catalyst d'utilisations de réflecteur de Cisco TrustSec (ENVERGURE) pour refléter le trafic d'un module de commutation CTS-incapable à l'engine de superviseur pour le transfert et la mise en place de la balise de groupe de sécurité (SGT).

Un réflecteur de sortie de Cisco TrustSec est mis en application sur un commutateur de distribution avec des liaisons ascendantes de la couche 3, où le module de commutation CTS-incapable fait face à un commutateur d'accès. Il le prend en charge centralisé expédiant les cartes (CFC) et les cartes de transfert distribué (DFC).

Configurez

[Diagramme du réseau](#)



Configuration SW1

Configurez le cts manual sur la liaison ascendante à SW2 avec ces commandes :

Configuration SW2

Activez le réflecteur de sortie sur le commutateur avec ces commandes :

Remarque: Le commutateur doit être rechargé afin d'activer le mode de réflecteur de sortie.

Configurez le cts manual sur le port connecté à SW1 avec ces commandes :

Configurez un SGT statique sur SW2 pour l'adresse IP source 10.10.10.10 de l'IXIA.

Vérifiez

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Le mode du courant CTS peut être visualisé avec cette commande :

L'état de lien CTS peut être visualisé avec cette commande :

Vérifiez que l'IFC-état est OUVERT sur les deux Commutateurs. Les sorties devraient ressembler à ceci :

Vérification par la sortie de NetFlow

Le NetFlow peut être configuré avec ces commandes :

Appliquez le NetFlow sur l'interface d'entrée du commutateur SW1 :

Vérifiez que les paquets entrant sont SGT étiquetés sur le commutateur SW1.

Dépannez

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.