# Contenu



# Introduction

Ce document décrit le Cisco TrustSec de la couche 3 (CTS) avec la configuration et la vérification de réflecteur d'entrée.

# 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

CTS est une solution de contrôle d'accès et d'identité de réseau avancé pour fournir la connectivité sécurisée de bout en bout à travers le circuit principal de fournisseurs de services et les réseaux de Data Center.

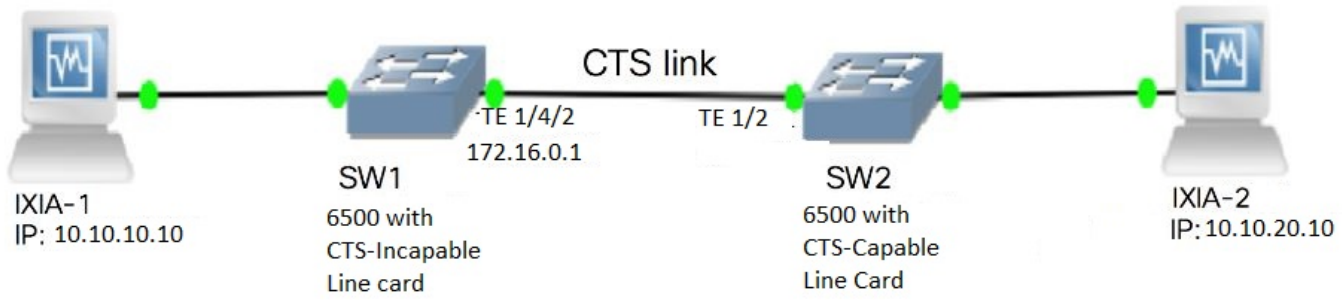
Les Commutateurs de Catalyst 6500 avec l'engine 2T de superviseur et les linecards de gamme 6900 fournissent le matériel et le support logiciel complets pour mettre en application CTS. Quand un Catalyst 6500 est configuré avec l'engine 2T de superviseur et des linecards de gamme 6900, le système est entièrement capable de fournir des caractéristiques CTS.

Puisque les clients voudraient continuer d'utiliser leurs Commutateurs et linecards existants de Catalyst 6500 tandis que migrer vers un réseau CTS et pour cette raison engine 2T de superviseur doit être compatible avec certains linecards existants une fois déployé dans un réseau CTS.

Pour prendre en charge la nouvelle fonctionnalité CTS telle que l' et le chiffrement de voie d'IEEE 802.1AE MACsec, il y a les circuits intégrés spécifiques à l'application dédiés (ASIC) utilisés sur l'engine 2T de superviseur et les nouveaux linecards de gamme 6900. Le mode de réflecteur d'entrée fournit la compatibilité entre les linecards existants non capables d'utiliser CTS. Le mode de réflecteur d'entrée prend en charge seulement l'expédition centralisé, transfert de paquet se produira sur le PFC de l'engine 2T de superviseur. Seulement la gamme 6148 ou les linecards matrice-activés CFC (centralisé expédiant la carte) tels que les linecards 6748-GE-TX est prise en charge. Les linecards DFC (carte de transfert distribué) et des linecards d'Ethernet 10 gigabits ne sont pas pris en charge quand le mode de réflecteur d'entrée est activé. Le mode de réflecteur d'entrée étant configuré, les linecards non-pris en charge ne mettront pas sous tension. Le mode de réflecteur d'entrée est activé utilisant une commande de configuration globale et exige un rechargement du système.

# Configurez

## Diagramme du réseau




---

### Étape 1. Installez CTS Layer3 sur l'interface de sortie entre SW1 et SW2

### Étape 2. Réflecteur d'entrée de l'enable CTS globalement.

Connectez une interface NON d'un linecard pris en charge par CTS à l'IXIA.

Assignez SGT statique dans le commutateur SW1 pour des paquets reçus de l'IXIA 1 connecté à SW1. Stratégie d'autorisation d'installation pour faire CTS L3 seulement pour des paquets dans le sous-réseau désiré sur l'authentificateur.

# Vérifiez

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

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

## Vérification par la sortie de NetFlow

Le NetFlow peut être configuré avec ces commandes :

Appliquez le NetFlow sur le port d'entrée de l'interface commutateur SW2 comme affiché :

Envoyez les paquets de l'IXIA 1 à l'IXIA 2. Il doit être reçu correctement sur l'IXIA 2 connecté au commutateur SW2 selon la stratégie de trafic. Notez que les paquets sont SGT étiquetés.

```
SW2#sh flow monitor mon2 cache format  table  Cache type:                              Normal
Cache size:                              4096  Current entries:
0  High Watermark:                             0  Flows added:
0  Flows aged:                                 0    - Active timeout      (  1800 secs)
0    - Inactive timeout    (    15 secs)       0    - Event aged
0    - Watermark aged                          0    - Emergency aged
0There are no cache entries to display.  Cache type:                                 Normal
(Platform cache)  Cache size:                          Unknown  Current entries:
0There are no cache entries to display.Module 4:  Cache type:
Normal (Platform cache)  Cache size:                          Unknown  Current entries:
0There are no cache entries to display.Module 2:  Cache type:
Normal (Platform cache)  Cache size:                          Unknown  Current entries:
0There are no cache entries to display.Module 1:  Cache type:
Normal (Platform cache)  Cache size:                          Unknown  Current entries:
4IPV4 SRC ADDR    IPV4 DST ADDR    TRNS SRC PORT  TRNS DST PORT  FLOW DIRN  FLOW CTS SRC GROUP
TAG  FLOW CTS DST GROUP TAG  IPPROT  ip fwd status                bytes
pkts===============  ===============  =============  =============  =========
======================  ======================  =======
=======================================  ==========1.1.1.10         2.2.2.10
0              0  Input                          10                     0      255  Unknown
148121702     3220037 10.10.10.10      10.10.20.10                  0              0  Input
15                       0      255  Unknown                      23726754
515799 10.10.10.1       224.0.0.5                  0              0  Input
2                        0       89  Unknown                      9536          119172.16.0.1
224.0.0.5                    0              0  Input                          0
0       89  Unknown                       400           5
```

Installez maintenant la stratégie d'exception pour ignorer CTS L3 pour des paquets à une adresse IP spécifique dans le commutateur d'authentificateur.

```
SW2#sh flow monitor mon2 cache format  table  Cache type:                              Normal
Cache size:                              4096  Current entries:
0  High Watermark:                             0  Flows added:
0  Flows aged:                                 0    - Active timeout      (  1800 secs)
0    - Inactive timeout    (    15 secs)       0    - Event aged
0    - Watermark aged                          0    - Emergency aged
0There are no cache entries to display.  Cache type:                                 Normal
(Platform cache)  Cache size:                          Unknown  Current entries:
0There are no cache entries to display.Module 4:  Cache type:
Normal (Platform cache)  Cache size:                          Unknown  Current entries:
0There are no cache entries to display.Module 2:  Cache type:
Normal (Platform cache)  Cache size:                          Unknown  Current entries:
0There are no cache entries to display.Module 1:  Cache type:
Normal (Platform cache)  Cache size:                          Unknown  Current entries:
4IPV4 SRC ADDR    IPV4 DST ADDR    TRNS SRC PORT  TRNS DST PORT  FLOW DIRN  FLOW CTS SRC GROUP
TAG  FLOW CTS DST GROUP TAG  IPPROT  ip fwd status                bytes
```

```
pkts===============  ===============  =============  =============  =========
=====================  ======================  =======
=======================================  ==========1.1.1.10         2.2.2.10
0               0  Input                             10                       0      255  Unknown
148121702     3220037 10.10.10.10      10.10.20.10                   0              0  Input
15                       0      255  Unknown                         23726754
515799 10.10.10.1       224.0.0.5                    0              0  Input
2                        0       89  Unknown                        9536          119 172.16.0.1
224.0.0.5                     0              0  Input                            0
0       89  Unknown                         400           5SW2#sh flow monitor mon2 cache format
tableCache type:                               Normal  Cache size:
4096  Current entries:                               0  High Watermark:
0  Flows added:                                    0  Flows aged:
0    - Active timeout      (  1800 secs)          0    - Inactive timeout    (    15 secs)
0    - Event aged                                 0    - Watermark aged
0    - Emergency aged                             0There are no cache entries to display.  Cache
type:                                Normal (Platform cache)  Cache size:
UnknownCurrent entries:                                   0There are no cache entries to
display.Module 4:  Cache type:                                 Normal (Platform cache)  Cache
size:                             Unknown  Current entries:
0There are no cache entries to display.Module 2:  Cache type:
Normal (Platform cache)  Cache size:                               Unknown  Current entries:
0There are no cache entries to display.Module 1:  Cache type:
Normal (Platform cache)  Cache size:                               Unknown  Current entries:
3IPV4 SRC ADDR    IPV4 DST ADDR    TRNS SRC PORT  TRNS DST PORT  FLOW DIRN  FLOW CTS SRC GROUP
TAG  FLOW CTS DST GROUP TAG  IP PROT  ip fwd status                  bytes
pkts===============  ===============  =============  =============  =========
=====================  ======================  =======
=======================================  =========1.1.1.10         2.2.2.10
0               0  Input                             10                       0      255  Unknown
1807478       39293 10.10.10.10      10.10.20.10                 0              0  Input
0                        0      255  Unknown                       1807478       39293 10.10.10.1
224.0.0.5                     0              0  Input                            2
0       89  Unknown                        164           2
```

Envoyez les paquets de l'IXIA 1 à l'IXIA 2. Ils doivent être reçus correctement sur l'IXIA 2 connecté au commutateur SW2 selon la stratégie d'exception.

> Remarque: Veuillez noter que les paquets ne sont pas SGT étiquetés parce que la stratégie d'exception prend le GROUPE TAG=0 precedence.FLOW CTS SRC

# Dépannez

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