

# Configurez la couche 3 CTS avec le réflecteur d'entrée

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurez](#)

[Diagramme du réseau](#)

[Étape 1. Installation CTS Layer3 sur l'interface de sortie entre SW1 et SW2](#)

[Étape 2. Réflecteur d'entrée de l'enable CTS globalement](#)

[Vérifiez](#)

[Dépannez](#)

## Introduction

Ce document décrit comment configurer le Cisco TrustSec de la couche 3 (CTS) avec le réflecteur d'entrée.

## Conditions préalables

### Conditions requises

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

### [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 le ® 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.

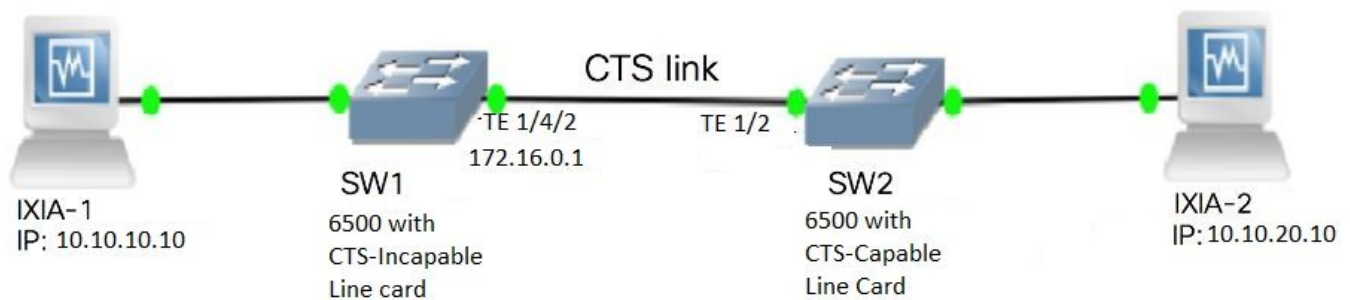
Les Commutateurs de Catalyst 6500 avec l'engine 2T de superviseur et les linecards de gamme 6900 fournissent le matériel et le support logiciel complets afin de mettre en application CTS. Quand un Catalyst 6500 est configuré avec l'engine 2T de superviseur et des linecards de gamme 6900, le système est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

Puisque les clients voudraient continuer à utiliser leurs Commutateurs et linecards de Catalyst 6500 qui existent déjà tandis qu'ils migrent vers un réseau CTS, et pour cette raison, l'engine 2T de superviseur doit être compatible avec certains linecards qui existent déjà une fois déployés dans un réseau CTS.

Afin de prendre en charge la nouvelle fonctionnalité CTS telle que l'étiquette de groupe de sécurité (SGT) 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 qui n'utilisent pas 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 matrice-activé centralisé expédiant des linecards de la carte (CFC) tels que les linecards 6748-GE-TX est prise en charge. Les linecards de la carte de transfert distribué (DFC) 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 mettent pas sous tension. Le mode de réflecteur d'entrée est activé avec l'utilisation d'une commande de configuration globale et exige un rechargement du système.

## Configurez

### [Diagramme du réseau](#)



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

- ```
SW1(config)#int t1/4/2
SW1(config-if)#ip address 172.16.0.1 255.255.255.0
SW1(config-if)# cts layer3 ipv4 trustsec forwarding
SW1(config-if)# cts layer3 ipv4 policy
SW1(config-if)#no shutdown
SW1(config-if)#exit

SW2(config)#int t1/2
SW2(config-if)#ip address 172.16.0.2 255.255.255.0
```

```
SW2(config-if)# cts layer3 ipv4 trustsec forwarding
SW2(config-if)# cts layer3 ipv4 policy
SW2(config-if)#no shutdown
SW2(config-if)#exit
```

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

```
SW1(config)#platform cts ingress
SW1#sh platform cts
CTS Ingress mode enabled
```

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

```
SW1#sh run int gi2/4/1
Building configuration...

Current configuration : 90 bytes
!
interface GigabitEthernet2/4/1
 no switchport
 ip address 10.10.10.1 255.255.255.0
end
```

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.

```
SW1(config)#cts role-based sgt-map 10.10.10.10 sgt 15
SW1(config)#ip access-list extended traffic_list
SW1(config-ext-nacl)#permit ip 10.10.10.0 0.0.0.255 any
SW1(config)#cts policy layer3 ipv4 traffic traffic_list
```

## 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 :

```
SW1#sh cts int summary
```

```
Global Dot1x feature is Enabled
CTS Layer2 Interfaces
```

```
-----
Interface  Mode    IFC-state dot1x-role peer-id    IFC-cache  Critical Authentication
-----
Tel1/4/1   DOT1X   OPEN      Supplic   SW2        invalid    Invalid
Tel1/4/4   MANUAL  OPEN      unknown   unknown    invalid    Invalid
Tel1/4/5   DOT1X   OPEN      Authent   SW2        invalid    Invalid
Tel1/4/6   DOT1X   OPEN      Supplic   SW2        invalid    Invalid
Tel2/3/9   DOT1X   OPEN      Supplic   SW2        invalid    Invalid
```

```
CTS Layer3 Interfaces
```

```

-----
Interface  IPv4 encap      IPv6 encap      IPv4 policy      IPv6 policy
Tel/4/2    OPEN            -----         OPEN             -----

```

```

SW2#sh cts int summary
Global Dot1x feature is Enabled
CTS Layer2 Interfaces

```

```

-----
Interface  Mode      IFC-state dot1x-role peer-id      IFC-cache      Critical-Authentication
-----
Tel1/1     DOT1X    OPEN      Authent    SW1         invalid        Invalid
Tel1/4     MANUAL  OPEN      unknown   unknown     invalid        Invalid
Tel1/5     DOT1X    OPEN      Supplic   SW1         invalid        Invalid
Tel1/6     DOT1X    OPEN      Authent    SW1         invalid        Invalid
Te4/5     DOT1X    OPEN      Authent    SW1         invalid        Invalid

```

```

CTS Layer3 Interfaces

```

```

-----
Interface  IPv4 encap      IPv6 encap      IPv4 policy      IPv6 policy
-----
Tel1/2     OPEN            -----         OPEN             -----

```

## Vérifiez par la sortie de NetFlow

Le NetFlow peut être configuré avec ces commandes :

```

SW2(config)#flow record rec2
SW2(config-flow-record)#match ipv4 protocol
SW2(config-flow-record)#match ipv4 source address
SW2(config-flow-record)#match ipv4 destination address
SW2(config-flow-record)#match transport source-port
SW2(config-flow-record)#match transport destination-port
SW2(config-flow-record)#match flow direction
SW2(config-flow-record)#match flow cts source group-tag
SW2(config-flow-record)#match flow cts destination group-tag
SW2(config-flow-record)#collect routing forwarding-status
SW2(config-flow-record)#collect counter bytes
SW2(config-flow-record)#collect counter packets
SW2(config-flow-record)#exit
SW2(config)#flow monitor mon2
SW2(config-flow-monitor)#record rec2
SW2(config-flow-monitor)#exit

```

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

```

SW2# sh run int t1/2
Building configuration...

Current configuration : 166 bytes
!
interface TenGigabitEthernet1/2
 ip address 172.16.0.2 255.255.255.0
 ip flow monitor mon2 input
 cts layer3 ipv4 trustsec forwarding
 cts layer3 ipv4 policy
end

```

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. Assurez-vous 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 0
```

There are no cache entries to display.

```
Cache type: Normal (Platform cache)
Cache size: Unknown
Current entries: 0
```

There are no cache entries to display.

Module 4:

```
Cache type: Normal (Platform cache)
Cache size: Unknown
Current entries: 0
```

There are no cache entries to display.

Module 2:

```
Cache type: Normal (Platform cache)
Cache size: Unknown
Current entries: 0
```

There are no cache entries to display.

Module 1:

```
Cache type: Normal (Platform cache)
Cache size: Unknown
Current entries: 4
```

| IPV4 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       |      |
| <b>10.10.10.10</b> | <b>10.10.20.10</b> | <b>0</b>      | <b>0</b>       | <b>Input</b> |                 |               |      |
| <b>15</b>          | <b>0</b>           | <b>255</b>    | <b>Unknown</b> |              | <b>23726754</b> | <b>515799</b> |      |
| 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             | 5             |      |

Maintenant, stratégie d'exception installée 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 0

```

There are no cache entries to display.

```

Cache type: Normal (Platform cache)
Cache size: Unknown
Current entries: 0

```

There are no cache entries to display.

Module 4:

```

Cache type: Normal (Platform cache)
Cache size: Unknown
Current entries: 0

```

There are no cache entries to display.

Module 2:

```

Cache type: Normal (Platform cache)
Cache size: Unknown
Current entries: 0

```

There are no cache entries to display.

Module 1:

```

Cache type: Normal (Platform cache)
Cache size: Unknown
Current entries: 4

```

| IPV4 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       |           |
| <b>10.10.10.10</b> | <b>10.10.20.10</b> | <b>0</b>      | <b>0</b>             | <b>Input</b>    |               |           |
| <b>15</b>          | <b>0</b>           | <b>255</b>    | <b>Unknown</b>       | <b>23726754</b> | <b>515799</b> |           |
| 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             | 5             |           |

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 0

```

There are no cache entries to display.

Cache type: Normal (Platform cache)  
Cache size: Unknown

Current entries: 0

There are no cache entries to display.

Module 4:

Cache type: Normal (Platform cache)  
Cache size: Unknown  
Current entries: 0

There are no cache entries to display.

Module 2:

Cache type: Normal (Platform cache)  
Cache size: Unknown  
Current entries: 0

There are no cache entries to display.

Module 1:

Cache type: Normal (Platform cache)  
Cache size: Unknown  
Current entries: 3

| IPV4 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.

**Note:** Les paquets ne sont pas SGT étiquetés parce que la stratégie d'exception prend le GROUPE TAG=0 de l'ÉCOULEMENT CTS SRC de priorité.

## Dépannez

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