# Configurar CTS de Camada 3 com Refletor de Entrada

## Contents



## Introduction

Este documento descreve como configurar o Cisco TrustSec (CTS) de Camada 3 com Refletor de Entrada.

## Prerequisites

### Requirements

A Cisco recomenda que você tenha conhecimento básico da solução CTS.

### Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Switches Catalyst 6500 com mecanismo de supervisão 2T no IOS® versão 15.0(01)SY
- Gerador de tráfego IXIA

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Informações de Apoio

O CTS é uma solução avançada de controle de acesso à rede e identidade para fornecer conectividade segura de ponta a ponta em redes de backbone e de data center de provedores de serviços.

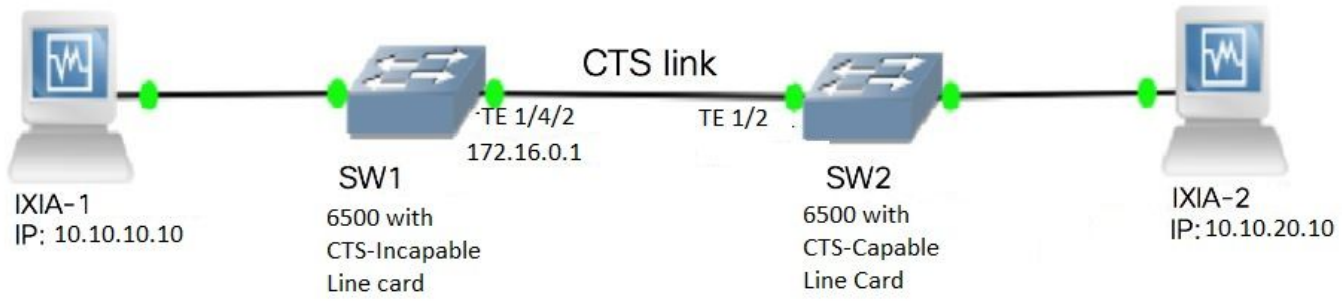
Os switches Catalyst 6500 com placas de linha do mecanismo de supervisão 2T e 6900 Series fornecem suporte completo de hardware e software para implementar o CTS. Quando um Catalyst 6500 é configurado com as placas de linha do Supervisor Engine 2T e 6900 Series, o sistema é totalmente capaz de fornecer recursos CTS.

Como os clientes gostariam de continuar a usar seus switches Catalyst 6500 e placas de linha que já existem enquanto migram para uma rede CTS, e por esse motivo, o mecanismo de supervisor 2T precisa ser compatível com determinadas placas de linha que já existem quando instaladas em uma rede CTS.

Para suportar novas funcionalidades CTS, como a Security Group Tag (SGT) e a criptografia de link IEEE 802.1AE MACsec, há circuitos integrados específicos de aplicativos (ASICs) dedicados usados nas placas de linha do Supervisor Engine 2T e 6900 Series. O modo refletor de entrada fornece compatibilidade entre placas de linha legadas que não usam CTS. O modo refletor de entrada suporta apenas encaminhamento centralizado; o encaminhamento de pacotes ocorrerá no PFC do mecanismo de supervisão 2T. Apenas as placas de linha 6148 Series ou Placa de encaminhamento centralizado (CFC - Centralized Forwarding Card) habilitada para matriz, como as placas de linha 6748-GE-TX, são suportadas. As placas de linha da placa de encaminhamento distribuído (DFC - Distributed Forwarding Card) e as placas de linha 10 Gigabit Ethernet não são suportadas quando o modo refletor de entrada está ativado. Com o modo refletor de entrada configurado, as placas de linha não suportadas não ligam. O modo refletor de entrada é ativado com o uso de um comando de configuração global e requer uma recarga do sistema.

# Configurar

## Diagrama de Rede




## Etapa 1. Configurar CTS Layer3 na interface de saída entre SW1 e 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
```

### Etapa 2. Ativar o refletor de entrada CTS globalmente

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

Conecte uma interface de uma placa de linha NON CTS suportada a 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
```

Atribua SGT estático no switch SW1 para pacotes recebidos do IXIA 1 conectados ao SW1. A configuração permite que a política faça CTS L3 somente para pacotes na sub-rede desejada no autenticador.

```
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
```

# Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Verifique se o estado IFC está ABERTO em ambos os switches. Os resultados devem ser assim:

```
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
------------------------------------------------------------------------------
Te1/4/1    DOT1X   OPEN      Supplic    SW2        invalid  Invalid
Te1/4/4    MANUAL  OPEN      unknown    unknown    invalid  Invalid
Te1/4/5    DOT1X   OPEN      Authent    SW2        invalid  Invalid
Te1/4/6    DOT1X   OPEN      Supplic    SW2        invalid  Invalid
Te2/3/9    DOT1X   OPEN      Supplic    SW2        invalid  Invalid

CTS Layer3 Interfaces
---------------------
Interface   IPv4 encap       IPv6 encap       IPv4 policy      IPv6 policy
Te1/4/2     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
------------------------------------------------------------------------------
Te1/1      DOT1X   OPEN      Authent    SW1          invalid     Invalid
Te1/4      MANUAL  OPEN      unknown    unknown      invalid     Invalid
Te1/5      DOT1X   OPEN      Supplic    SW1          invalid     Invalid
Te1/6      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
------------------------------------------------------------------------
Te1/2       OPEN             ----------       OPEN             -----------
```

## Verificar através da saída do Netflow

O Netflow pode ser configurado com estes comandos:

```
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
```

Aplique o netflow na porta de entrada da interface do switch SW2 como mostrado:

```
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
```

Envie pacotes de IXIA 1 para IXIA 2. Ele deve ser recebido corretamente no IXIA 2 conectado ao switch SW2 de acordo com a política de tráfego. Verifique se os pacotes estão marcados com SGT.

```
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
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           5
```

Agora, configure a política de exceção para ignorar o CTS L3 para pacotes em um endereço IP específico no switch do Autenticador.

```
SW1(config)#ip access-list extended exception_list
SW1(config-ext-nacl)#permit ip 10.10.10.0 0.0.0.255 any
SW1(config)#cts policy layer3 ipv4 exception exception_list


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
```

Envie pacotes de IXIA 1 para IXIA 2. Eles devem ser recebidos corretamente no IXIA 2 conectado ao switch SW2 de acordo com a política de exceção.

> **Note**: Os pacotes não são marcados com SGT porque a política de exceção tem precedência **FLOW CTS SRC GROUP TAG=0.**

# Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.