Configurez et vérifiez le réflecteur de sortie avec le cts manual

Contenu

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 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 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 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.

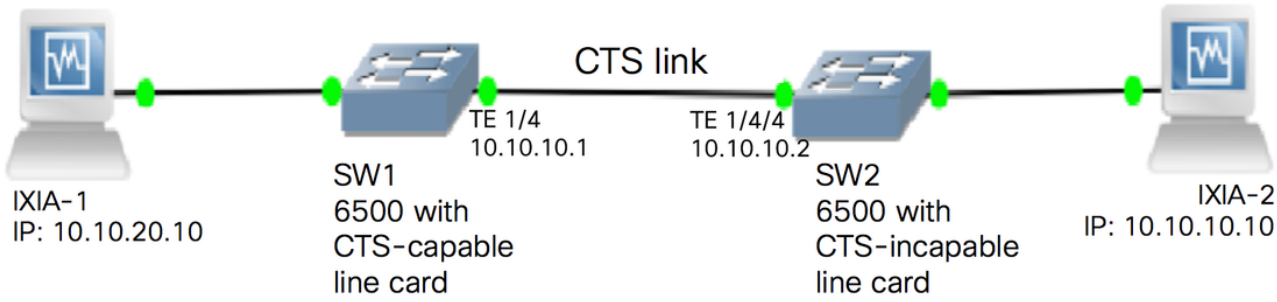
Les Commutateurs de gamme Catalyst 6500 avec l'engine 2T de superviseur et les linecards de gamme 6900 fournissent le matériel et le support logiciel complets pour mettre en application CTS. Afin de prendre en charge la fonctionnalité CTS, il y a les circuits intégrés spécifiques à l'application dédiés (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 CTS (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 CTS 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



Configurez SW1

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

```
SW1(config)#int t1/4
SW1(config-if)#ip address 10.10.10.1 255.255.255.0
SW1(config-if)#no shutdown
SW1(config-if)#cts manual
SW1(config-if-cts-manual)#propagate sgt
SW1(config-if-cts-manual)#policy static sgt 11 trusted
SW1(config-if-cts-manual)#exit
SW1(config-if)#exit
```

Configurez SW2

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

```
SW2(config)#platform cts egress
SW2#write memory
Building configuration...
[OK] SW2#reload
```

Note: 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 :

```
SW2(config)#int t1/4/4
SW2(config-if)#ip address 10.10.10.2 255.255.255.0
SW2(config-if)#no shutdown
SW2(config-if)#cts manual
SW2(config-if-cts-manual)#propagate sgt
SW2(config-if-cts-manual)#policy  static sgt 10 trusted
SW2(config-if-cts-manual)#exit
SW2(config-if)#exit
```

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

```
SW2(config)#cts role-based sgt-map 10.10.10.10 sgt 11
```

Vérifiez

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

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

```
SW2#show platform cts
 CTS Egress mode enabled
```

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

```
show cts interface summary
```

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

```
SW1#show cts interface summary

Global Dot1x feature is Enabled

CTS Layer2 Interfaces
---------------------
Interface  Mode    IFC-state dot1x-role peer-id    IFC-cache    Critical-Authentication
------------------------------------------------------------------------------
Te1/4      MANUAL  OPEN      unknown    unknown    invalid      Invalid

SW2#show cts interface summary

Global Dot1x feature is Enabled
```

```
CTS Layer2 Interfaces
---------------------
Interface  Mode    IFC-state dot1x-role peer-id    IFC-cache    Critical-Authentication
-------------------------------------------------------------------------------
Te1/4/4    MANUAL  OPEN      unknown    unknown    invalid      Invalid
```

Vérifiez par la sortie de NetFlow

Le NetFlow peut être configuré avec ces commandes :

```
SW2#show cts interface summary

Global Dot1x feature is Enabled

CTS Layer2 Interfaces
---------------------
Interface  Mode    IFC-state dot1x-role peer-id    IFC-cache    Critical-Authentication
-------------------------------------------------------------------------------
Te1/4/4    MANUAL  OPEN      unknown    unknown    invalid      Invalid
```

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

```
SW2#show cts interface summary

Global Dot1x feature is Enabled

CTS Layer2 Interfaces
---------------------
Interface  Mode    IFC-state dot1x-role peer-id    IFC-cache    Critical-Authentication
-------------------------------------------------------------------------------
Te1/4/4    MANUAL  OPEN      unknown    unknown    invalid      Invalid
```

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

```
SW1#show 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 35:
```

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

There are no cache entries to display.

Module 34:
  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 33:
  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 20:
  Cache type:                               Normal (Platform cache)
  Cache size:                               Unknown
  Current entries:                               2

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
===============  ===============  =============  =============  =========
=====================  =====================  =======  =============  ==========  ==========
10.10.10.10      10.10.20.10                  0              0  Input
11                       0      255  Unknown        375483970     8162695
10.10.10.2       224.0.0.5                    0              0  Input
4                        0       89  Unknown           6800          85

Module 19: Cache type: Normal (Platform cache) Cache size: Unknown Current entries: 0 There are
no cache entries to display. Module 18: 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
```

Dépannez

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