Configuration et vérification du réflecteur de sortie avec CTS Manual

Contenu

Introduction

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

Conditions préalables

Conditions requises

Cisco vous recommande d'avoir une connaissance de base de la solution CTS.

Components Used

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

- Commutateurs Catalyst 6500 avec moteur de supervision 2T sur IOS version 15.0(01)SY
- Générateur de trafic 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.

Informations générales

CTS est une architecture d'accès réseau basée sur l'identité qui aide les clients à sécuriser la collaboration, à renforcer la sécurité et à répondre aux exigences de conformité. Il fournit également une infrastructure évolutive d'application des politiques basée sur les rôles. Les

paquets sont balisés en fonction de l'appartenance au groupe de la source de paquets à l'entrée du réseau. Les stratégies associées au groupe sont appliquées lorsque ces paquets traversent le réseau.

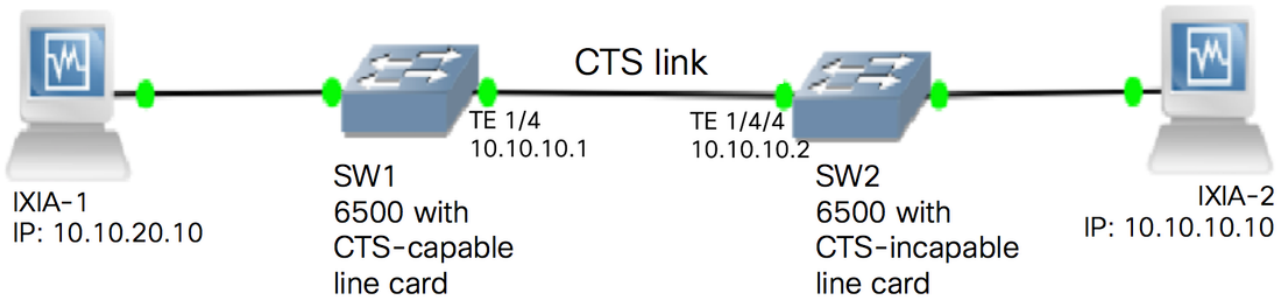
Les commutateurs de la gamme Catalyst 6500 avec cartes de ligne Supervisor Engine 2T et 6900 fournissent une prise en charge matérielle et logicielle complète pour la mise en oeuvre de CTS. Afin de prendre en charge la fonctionnalité CTS, des circuits intégrés spécifiques aux applications (ASIC) dédiés sont utilisés sur les nouvelles cartes de ligne de la gamme 6900. Les cartes de ligne héritées n'ont pas ces circuits ASIC dédiés et ne prennent donc pas en charge CTS.

Le réflecteur CTS utilise l'analyseur de port de commutateur Catalyst (SPAN) pour refléter le trafic d'un module de commutation incapable CTS vers le moteur de supervision pour l'affectation et l'insertion des balises de groupe de sécurité (SGT).

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

Configuration

Diagramme du réseau



Configuration de SW1

Configurez le manuel CTS sur la liaison ascendante vers SW2 avec les commandes suivantes :

```
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
```

Configuration de SW2

Activez le réflecteur de sortie sur le commutateur avec les commandes suivantes :

```
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 manuel CTS sur le port connecté à SW1 à l'aide des commandes suivantes :

```
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 une SGT statique sur SW2 pour l'adresse IP source 10.10.10.10 à partir d'IXIA.

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

Vérification

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Vous pouvez afficher le mode CTS actuel à l'aide de la commande suivante :

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

L'état de la liaison CTS peut être affiché à l'aide de la commande suivante :

```
show cts interface summary
```

Vérifiez que l'état IFC est OUVERT sur les deux commutateurs. Les résultats doivent être les suivants :

```
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
```

Vérification via la sortie Netflow

Netflow peut être configuré avec les commandes suivantes :

```
SW1(config)#flow record rec2
SW1(config-flow-record)#match ipv4 protocol
SW1(config-flow-record)#match ipv4 source address
SW1(config-flow-record)#match ipv4 destination address
SW1(config-flow-record)#match transport source-port
SW1(config-flow-record)#match transport destination-port
SW1(config-flow-record)#match flow direction
SW1(config-flow-record)#match flow cts source group-tag
SW1(config-flow-record)#match flow cts destination group-tag
SW1(config-flow-record)#collect routing forwarding-status
SW1(config-flow-record)#collect counter bytes
SW1(config-flow-record)#collect counter packets
SW1(config-flow-record)#exit
SW1(config)#flow monitor mon2
SW1(config-flow-monitor)#record rec2
SW1(config-flow-monitor)#exit
```

Appliquez Netflow sur l'interface d'entrée du commutateur SW1 :

```
SW1#sh run int t1/4
Building configuration...

Current configuration : 165 bytes
!
interface TenGigabitEthernet1/4
 no switchport
 ip address 10.10.10.1 255.255.255.0
 ip flow monitor mon2 input
 cts manual
  policy static sgt 11 trusted
end
```

Vérifiez que les paquets entrants sont marqués SGT 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
```

Dépannage

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