Configurer CTS de couche 3 avec réflecteur d'entrée

Contenu

Introduction

Ce document décrit comment configurer Cisco TrustSec (CTS) de couche 3 avec Inbound Reflector.

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 Supervisor Engine 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 solution avancée de contrôle d'accès au réseau et d'identité qui fournit une connectivité sécurisée de bout en bout sur les réseaux fédérateurs et de data center des fournisseurs de services.

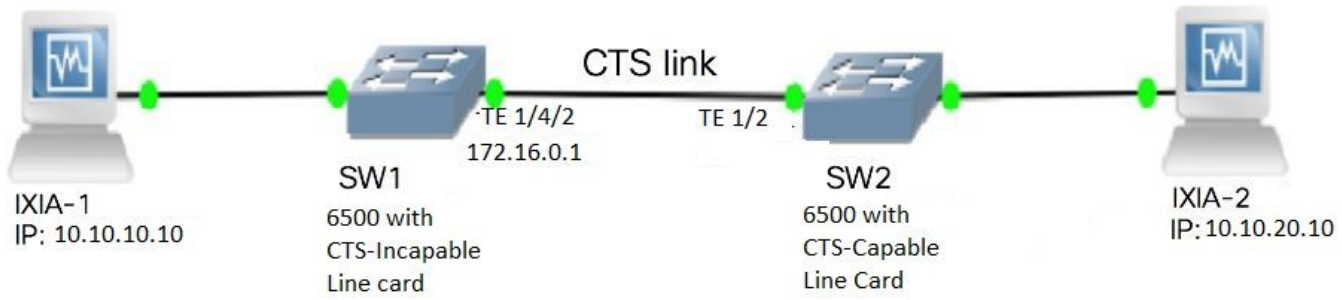
Les commutateurs Catalyst 6500 équipés de cartes de ligne Supervisor Engine 2T et 6900 fournissent une assistance matérielle et logicielle complète pour la mise en oeuvre de CTS. Lorsqu'un Catalyst 6500 est configuré avec les cartes de ligne Supervisor Engine 2T et 6900, le système est entièrement capable de fournir des fonctionnalités CTS.

Puisque les clients souhaitent continuer à utiliser leurs commutateurs Catalyst 6500 et leurs cartes de ligne qui existent déjà lors de leur migration vers un réseau CTS, et pour cette raison, Supervisor Engine 2T doit être compatible avec certaines cartes de ligne qui existent déjà lorsqu'elles sont déployées dans un réseau CTS.

Afin de prendre en charge de nouvelles fonctionnalités CTS telles que Security Group Tag (SGT) et le cryptage de liaison MACsec IEEE 802.1AE, des circuits intégrés spécifiques aux applications (ASIC) sont utilisés sur le Supervisor Engine 2T et les nouvelles cartes de ligne de la gamme 6900. Le mode de réflecteur d'entrée assure la compatibilité entre les cartes de ligne héritées qui n'utilisent pas CTS. Le mode de réflecteur d'entrée prend uniquement en charge le transfert centralisé, le transfert de paquets se produit sur le PFC du Supervisor Engine 2T. Seules les cartes de ligne CFC (Central Forwarding Card) de la gamme 6148 ou de la matrice, telles que les cartes de ligne 6748-GE-TX, sont prises en charge. Les cartes de ligne DFC (Distributed Forwarding Card) et les cartes de ligne 10 Gigabit Ethernet ne sont pas prises en charge lorsque le mode de réflecteur d'entrée est activé. Avec le mode de réflecteur d'entrée configuré, les cartes de ligne non prises en charge ne s'allument pas. Le mode de réflecteur d'entrée est activé à l'aide d'une commande de configuration globale et nécessite un rechargement du système.

Configuration

Diagramme du réseau



Étape 1. Configuration de 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. Activer le réflecteur d'entrée CTS dans le monde entier

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

Connectez une interface d'une carte de ligne non prise en charge CTS à 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
```

Attribuez une SGT statique dans le commutateur SW1 pour les paquets reçus de l'IXIA 1 connecté à SW1. Configurez la stratégie d'autorisation pour exécuter CTS L3 uniquement pour les paquets du sous-réseau souhaité 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
```

Vérification

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Vérifiez que l'état IFC est OUVERT sur les deux commutateurs. Les résultats 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
-------------------------------------------------------------------------------
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             -----------
```

Vérification via la sortie Netflow

Netflow peut être configuré avec les commandes suivantes :

```
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 netflow sur le port d'entrée de l'interface du commutateur SW2 comme indiqué :

```
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 des paquets de IXIA 1 à IXIA 2. Il doit être reçu correctement sur IXIA 2 connecté au commutateur SW2 conformément à la politique de trafic. Assurez-vous que les paquets sont étiquetés 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
```

Maintenant, configurez la stratégie d'exception pour ignorer CTS L3 pour les paquets à une adresse IP spécifique dans le commutateur Authenticator.

```
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
```

Envoyez des paquets de IXIA 1 à IXIA 2. Ils doivent être reçus correctement sur IXIA 2 connecté au commutateur SW2 conformément à la politique d'exception.

> **Note**: Les paquets ne sont pas marqués SGT, car la stratégie d'exception a la priorité **FLOW CTS SRC GROUP TAG=0.**

Dépannage

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