Configuración de CTS de Capa 3 con reflector de Ingreso

Contenido

Introducción

Este documento describe cómo configurar Cisco TrustSec (CTS) de Capa 3 con Reflector de Ingreso.

Prerequisites

Requirements

Cisco recomienda que tenga conocimientos básicos sobre la solución CTS.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Switches Catalyst 6500 con Supervisor Engine 2T en IOS® Versión 15.0(01)SY
- Generador de tráfico 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.

Antecedentes

CTS es una solución de identidad y control de acceso a la red avanzada para proporcionar conectividad segura de extremo a extremo entre la red troncal de los proveedores de servicios y las redes del Data Center.

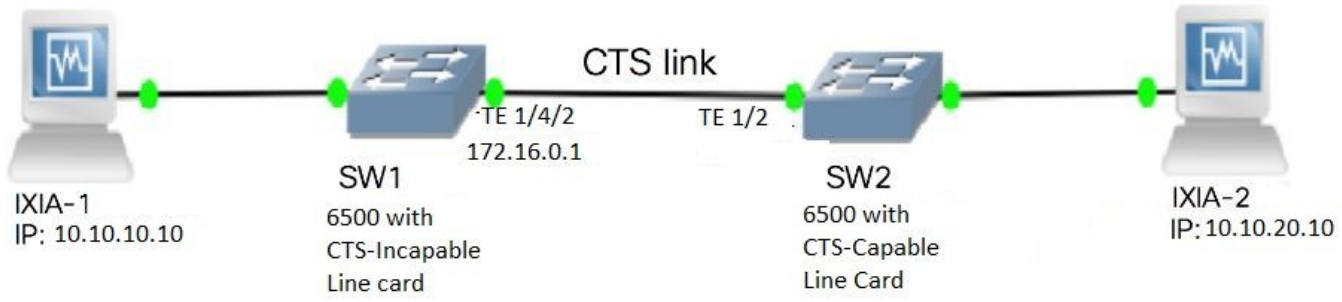
Los switches Catalyst 6500 con las tarjetas de línea Supervisor Engine 2T y 6900 Series proporcionan soporte completo de hardware y software para implementar CTS. Cuando se configura un Catalyst 6500 con las tarjetas de línea Supervisor Engine 2T y 6900 Series, el sistema es completamente capaz de proporcionar funciones CTS.

Dado que los clientes desean seguir utilizando sus switches Catalyst 6500 y tarjetas de línea que ya existen mientras migran a una red CTS, y por esta razón, Supervisor Engine 2T debe ser compatible con ciertas tarjetas de línea que ya existen cuando se implementan en una red CTS.

Para admitir la nueva funcionalidad de CTS, como Security Group Tag (SGT) y el cifrado de enlaces IEEE 802.1AE MACsec, hay circuitos integrados específicos de la aplicación (ASIC) dedicados que se utilizan en el Supervisor Engine 2T y las nuevas tarjetas de línea de la serie 6900. El modo reflector de entrada proporciona compatibilidad entre las tarjetas de línea heredadas que no utilizan CTS. El modo reflector de ingreso soporta solamente el reenvío centralizado, el reenvío de paquetes ocurrirá en la PFC del Supervisor Engine 2T. Solo se admiten tarjetas de línea de la serie 6148 o de la tarjeta de reenvío centralizado (CFC) habilitada para fabric, como las tarjetas de línea 6748-GE-TX. Las tarjetas de línea de la tarjeta de reenvío distribuido (DFC) y las tarjetas de línea de 10 Gigabit Ethernet no se admiten cuando el modo reflector de entrada está activado. Con el modo reflector de ingreso configurado, las tarjetas de línea no admitidas no se encienden. El modo reflector de ingreso se habilita con el uso de un comando de configuración global y requiere una recarga del sistema.

Configurar

Diagrama de la red



Paso 1. Configuración de la Capa 3 de CTS en la Interfaz de Salida entre SW1 y 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
```

Paso 2. Habilitar el reflector de entrada CTS globalmente

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

Conecte una interfaz de una tarjeta de línea compatible con NON CTS 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
```

Asigne SGT estática en el switch SW1 para los paquetes recibidos del IXIA 1 conectado al SW1. Configure la política de permiso para realizar CTS L3 solamente para los paquetes en la subred deseada en el 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
```

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

Verifique que el estado de IFC esté ABIERTO en ambos switches. Los resultados deben tener el siguiente aspecto:

```
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 a través de la salida de Netflow

Netflow se puede configurar con estos 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 netflow en el puerto de ingreso de la interfaz del switch SW2 como se muestra:

```
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
```

Enviar paquetes de IXIA 1 a IXIA 2. Debe recibirse correctamente en IXIA 2 conectado al switch SW2 según la política de tráfico. Asegúrese de que los paquetes estén etiquetados 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
```

Ahora, configure la política de excepciones para saltar CTS L3 para los paquetes a una dirección IP específica en el switch 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
```

Enviar paquetes de IXIA 1 a IXIA 2. Se deben recibir correctamente en IXIA 2 conectado al switch SW2 según la política de excepciones.

> **Nota:** Los paquetes no están etiquetados SGT porque la política de excepciones tiene prioridad **FLOW CTS SRC GROUP TAG=0.**

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.