

Capa 3 CTS de la configuración con el reflector del ingreso

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Diagrama de la red](#)

[Paso 1. Configuración CTS Layer3 en la interfaz de egreso entre el SW1 y el SW2](#)

[Paso 2. Reflector del ingreso del permiso CTS global](#)

[Verificación](#)

[Troubleshooting](#)

Introducción

Este documento describe cómo configurar la capa 3 Cisco TrustSec (CTS) con el reflector del ingreso.

Prerequisites

Requisitos

Cisco recomienda que usted tiene conocimiento básico de la solución CTS.

Componentes Utilizados

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

- Catalyst 6500 Switch con el Supervisor Engine 2T en la versión 15.0(01)SY IOS®
- Generador de tráfico IXIA

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Antecedentes

El CTS es una solución del control de acceso y de la identidad de la red avanzada para proporcionar la conectividad segura de punta a punta a través de la estructura básica de los

proveedores de servicio y de las redes del centro de datos.

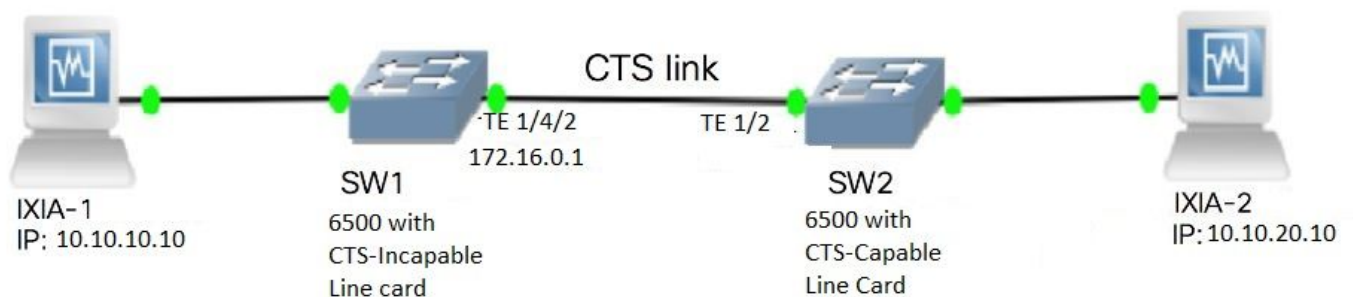
Los Catalyst 6500 Switch con el linecards de las 2T y 6900 Series del Supervisor Engine proporcionan el soporte del hardware y software completo para implementar el CTS. Cuando un Catalyst 6500 se configura con el linecards de las 2T y 6900 Series del Supervisor Engine, el sistema es completamente capaz de proporcionar a las características CTS.

Puesto que los clientes quisieran continuar utilizando sus Catalyst 6500 Switch y el linecards que existen ya mientras que emigran a una red CTS, y por este motivo, el Supervisor Engine 2T necesita ser compatible con cierto linecards que existe ya cuando está desplegado en una red CTS.

Para soportar las nuevas funciones CTS tales como etiqueta del grupo de seguridad (SGT) y cifrado de link de IEEE 802.1AE MACsec, hay circuitos específicos de la aplicación dedicados (Asics) usados en el Supervisor Engine 2T y el nuevo linecards de las 6900 Series. El modo reflector del ingreso proporciona la compatibilidad entre el linecards de la herencia que no utiliza el CTS. El modo reflector del ingreso soporta solamente la expedición centralizada, reenvío de paquete ocurrirá en el PFC del Supervisor Engine 2T. Solamente las 6148 Series o el linecards centralizado tela enabled del indicador luminoso LED amarillo de la placa muestra gravedad menor de la expedición (CFC) tal como el linecards 6748-GE-TX se soportan. El linecards del Distributed Forwarding Card (DFC) y el linecards de los Ethernet de 10 Gigabit no se soportan cuando habilitan al modo reflector del ingreso. Con el modo reflector del ingreso configurado, el linecards NON-soportado no acciona para arriba. Habilitan con el uso de un comando global configuration y requiere al modo reflector del ingreso una recarga del sistema.

Configurar

Diagrama de la red



Paso 1. Configuración CTS Layer3 en la interfaz de egreso entre el SW1 y el 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. Reflector del ingreso del permiso CTS global

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

Conecte una interfaz de un linecard soportado CTS NON con el 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 estático en el Switch SW1 para los paquetes recibidos del IXIA 1 conectado con el SW1. Directiva del permiso de la configuración para hacer CTS L3 solamente para los paquetes en la subred deseada en el authenticator.

```
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 IFC-estado esté ABIERTO en ambo Switches. Las salidas deben parecer esto:

```
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
```

```
Tel/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
Tel/1	DOT1X	OPEN	Authent	SW1	invalid	Invalid
Tel/4	MANUAL	OPEN	unknown	unknown	invalid	Invalid
Tel/5	DOT1X	OPEN	Supplic	SW1	invalid	Invalid
Tel/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
Tel/2	OPEN	-----	OPEN	-----

Verifique a través de la salida del Netflow

El 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 el 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
```

Envíe los paquetes de IXIA 1 a IXIA 2. Debe ser recibido correctamente en IXIA 2 conectado con el Switch SW2 según la política de tráfico. Asegúrese de que los paquetes sean SGT marcados con etiqueta.

```
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	0	148121702	3220037	
10.10.10.10	10.10.20.10	0	255	Unknown	0	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, directiva puesta de la excepción para saltar CTS L3 para los paquetes a una dirección IP específica en el Switch del authenticator.

```
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	

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

Envíe los paquetes de IXIA 1 a IXIA 2. Deben ser recibidos correctamente en IXIA 2 conectado con el Switch SW2 según la directiva de la excepción.

Note: Los paquetes no son SGT marcados con etiqueta porque la directiva de la excepción toma el **GRUPO TAG=0 del SRC del FLUJO CTS de la precedencia.**

Troubleshooting

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