Configuración y verificación del reflector de egreso con CTS Manual

Contenido

Introducción

Este documento describe cómo configurar y verificar un Cisco TrustSec (CTS) con reflector de salida.

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 Release 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 arquitectura de acceso a la red habilitada para identidades que ayuda a los clientes a habilitar una colaboración segura, fortalecer la seguridad y cumplir los requisitos de cumplimiento. También proporciona una infraestructura escalable de aplicación de políticas basada en roles. Los

paquetes se etiquetan en función de la pertenencia del grupo al origen del paquete en el ingreso de la red. Las políticas asociadas con el grupo se aplican a medida que estos paquetes atraviesan la red.

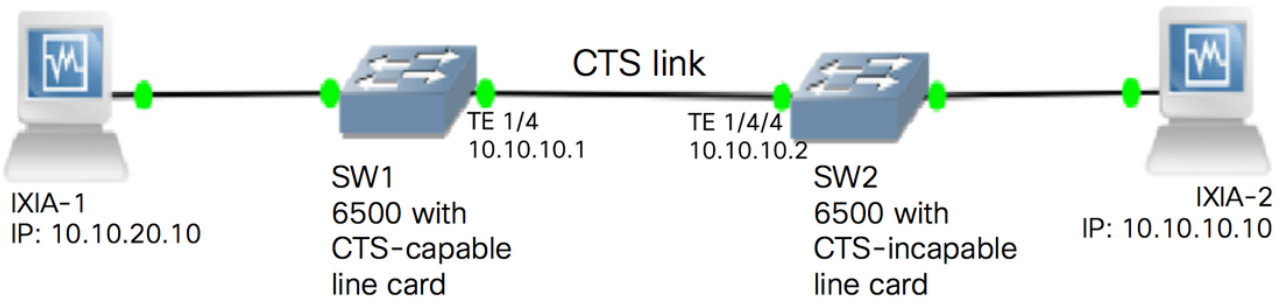
Los switches Catalyst serie 6500 con Supervisor Engine 2T y tarjetas de línea 6900 proporcionan soporte completo de hardware y software para implementar CTS. Para admitir la funcionalidad CTS, hay circuitos integrados específicos de la aplicación (ASIC) dedicados que se utilizan en las nuevas tarjetas de línea de la serie 6900. Las tarjetas de línea antiguas no tienen estos ASIC dedicados y, por lo tanto, no admiten CTS.

El reflector CTS utiliza Catalyst Switch Port Analyzer (SPAN) para reflejar el tráfico de un módulo de switching incapaz de CTS al motor supervisor para la asignación e inserción de Security Group Tag (SGT).

Un reflector de salida CTS se implementa en un switch de distribución con enlaces ascendentes de Capa 3, donde el módulo de conmutación incapaz de CTS se enfrenta a un switch de acceso. Admite tarjetas de reenvío centralizado (CFC) y tarjetas de reenvío distribuido (DFC).

Configurar

Diagrama de la red



Configurar SW1

Configure el manual CTS en el link ascendente a SW2 con estos comandos:

```
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
```

Configurar SW2

Habilite el reflector de egreso en el switch con estos comandos:

```
SW2(config)#platform cts egress
SW2#write memory
```

```
Building configuration...
[OK] SW2#reload
```

Nota: El switch debe recargarse para habilitar el modo reflector de egreso.

Configure CTS Manual en el puerto conectado a SW1 con estos comandos:

```
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
```

Configure una SGT estática en SW2 para la dirección IP de origen 10.10.10.10 desde IXIA.

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

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

El modo CTS actual se puede ver con este comando:

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

El estado del link CTS se puede ver con este comando:

```
show cts interface summary
```

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

```
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
```

Verificar a través de la salida de Netflow

Netflow se puede configurar con estos comandos:

```
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
```

Aplique Netflow en la interfaz de ingreso del switch 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
```

Verifique que los paquetes entrantes estén etiquetados SGT en el switch 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
```

Troubleshoot

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