Configure y verifique el reflector de la salida con el manual CTS

Contenido

Introducción

Este documento describe cómo configurar y verifiy Cisco TrustSec (CTS) con el reflector de la salida.

Prerequisites

Requisitos

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

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 del IOS 15.0(01)SY
- 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

Cisco TrustSec es una arquitectura identidad-habilitada del acceso a la red que ayuda a los

clientes a habilitar la Colaboración segura, a consolidar la Seguridad, y a dirigir los requisitos de la conformidad. También proporciona una infraestructura basada papel scalable de la aplicación de políticas. Se marcan con etiqueta los paquetes basaron en la membresía del grupo de la fuente del paquete en el ingreso de la red. Las directivas asociadas al grupo se aplican mientras que estos paquetes atraviesan la red.

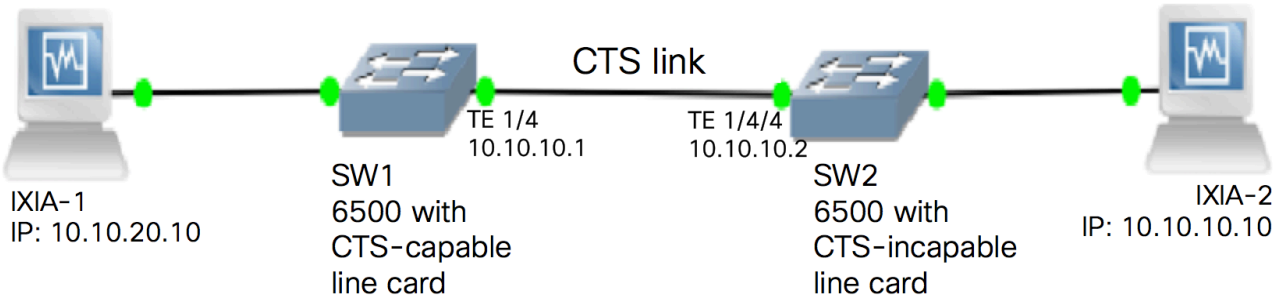
Los Catalyst 6500 Series Switch con el linecards de las 2T y 6900 Series del Supervisor Engine proporcionan el soporte del hardware y software completo para implementar el CTS. Para soportar las funciones CTS, hay circuitos integrados específicos a la aplicación dedicados (Asics) usados en el nuevo linecards de las 6900 Series. El linecards de la herencia no tiene éstos Asics dedicado y por lo tanto, no soporte el CTS.

(SPAN) del analizador del puerto del switch Catalyst de las aplicaciones del reflector de Cisco TrustSec para reflejar el tráfico de un módulo de switching CTS-incapaz al Supervisor Engine para la asignación y la inserción de la etiqueta del grupo de seguridad (SGT).

Un reflector de la salida de Cisco TrustSec se implementa en un switch de distribución con el uplinks de la capa 3, donde el módulo de switching CTS-incapaz hace frente a un switch de acceso. Soporta centralizado remitiendo los indicadores luminosos LED amarillo de la placa muestra gravedad menor (CFC) y distribuido remitiendo los indicadores luminosos LED amarillo de la placa muestra gravedad menor (DFC).

Configurar

Diagrama de la red



Configuración SW1

Configure el manual CTS en el uplink al 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
```

Configuración SW2

Reflector de la salida del permiso en el Switch con estos comandos:

```
SW2(config)#platform cts egress
SW2#write memory
Building configuration...
[OK] SW2#reload
```

Note: El Switch tiene que ser recargado para habilitar al modo reflector de la salida.

Configure el manual CTS en el puerto conectado con el 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 un SGT estático en el SW2 para la dirección IP de origen 10.10.10.10 del 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 actual CTS 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 IFC-estado esté ABIERTO en ambo Switches. Las salidas deben parecer esto:

```
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
```

Verificación a través de la salida del Netflow

El 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 el 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 sean SGT marcados con etiqueta 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

Troubleshooting

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